Security adaptation in highly dynamic wireless networks

EL MALIKI, Tewfiq

Abstract
On remarque un manque de protocoles d’adaptation de sécurité génériques pour gérer des conditions de sécurité extrêmement dynamiques et des performances dans le contexte des Réseaux auto-organisés. Nous avons proposé un référence moniteur à sécurité adaptative (SARM) pour les environnements mobiles et sans fil qui vise à offrir un Framework générique capable d’intégrer efficacement les nouvelles technologies émergentes telles que la bio-sécurité et green IT afin de traiter efficacement la sécurité des systèmes complexes. Grâce à l’intégration des principes de l’Autonomic Computing, SARM règle finement, via la boucle rétroactive, les moyens sécuritaires basés sur la cryptographie et le suivi du contexte, y compris l’environnement de l’utilisateur et la consommation d’énergie. L’approche matériel et les simulations extensives basées sur la programmation par agents ont également été menées afin de valider SARM en présence d’attaquants. Les résultats montrent clairement que le SARM est efficace en termes de survie, de l’utilisation du réseau et la consommation d’énergie -QoS [...]
SECURITY ADAPTATION IN HIGHLY DYNAMIC WIRELESS NETWORKS

THÈSE
présentée à la Faculté des sciences économiques et sociales
de l’Université de Genève
par
Tewfiq EL MALIKI
sous la direction de
Dr. Jean-Marc Seigneur et prof. Dimitri KONSTANTAS
pour l’obtention du grade de
Docteur ès sciences économiques et sociales
mention systèmes d’information

Membres du jury de thèse:

M. Dimitri KONSTANTAS, Professeur
Mme. Giovanna Di Marzo SERUGENDO, Professeur, président du jury
M. Sviatoslav VOLOSHYNOVSKIY, Professeur
M. Yanjun ZUO, Professeur, University of North Dakota

Thèse no 847
Genève, 3 juin 2014
La Faculté des sciences économiques et sociales, sur préavis du jury, a autorisé l'impression de la présente thèse, sans entendre, par là, émettre aucune opinion sur les propositions qui s'y trouvent énoncées et qui n'engagent que la responsabilité de leur auteur.

Genève, le 3 juin 2014

Le doyen
Bernard MORARD

Impression d'après le manuscrit de l'auteur
# Table of Contents

Table of Contents ........................................................................................................ iii
Résumé .......................................................................................................................... vii
Abstract ......................................................................................................................... ix
Acknowledgments .......................................................................................................... xi
Biographical Sketch ...................................................................................................... xii
List of Figures ................................................................................................................. xiii
List of Tables .................................................................................................................. xv
List of Abbreviations ..................................................................................................... xvi
List of Definitions ......................................................................................................... xxi
List of Symbols .............................................................................................................. xxvii

## Chapter 1. Introduction
  1.1 Motivation .............................................................................................................. 1
  1.2 Thesis Statement
    1.2.1 Adaptive Security for highly dynamic networks ............................................. 6
  1.3 Overview and main contributions ...................................................................... 8
  1.4 Publications .......................................................................................................... 9
  1.5 Structure of the thesis ......................................................................................... 10
  1.6 REFERENCES ................................................................................................. 11

## Chapter 2. Related Work and State of the art
  2.1 Background and Literature Review ................................................................ 13
    2.1.1 Introduction ................................................................................................. 13
    2.1.2 Context of Wireless Networks .................................................................. 14
    2.1.3 Security Technology ................................................................................. 18
  2.2 State of the art .................................................................................................. 26
    2.2.1 Autonomous systems ............................................................................... 29
    2.2.2 Trust and reputation .................................................................................. 32
    2.2.3 Synthesis and open problems ................................................................... 39
  2.3 Conclusion and Summary ................................................................................. 40
  2.4 REFERENCES ................................................................................................. 41

## Chapter 3. Problem Statement and Methodology ................................................. 49
  3.1 Problem statement overview ........................................................................... 49
  3.2 Self-Organizing Networks ................................................................................. 49
    3.2.1 Introduction to the security of highly dynamic networks ....................... 49
    3.2.2 MANET ..................................................................................................... 50
    3.2.3 VANET ..................................................................................................... 51
    3.2.4 WSN ........................................................................................................ 52
    3.2.5 Synthesis .................................................................................................. 52
  3.3 Attackers’ Classification .................................................................................... 54
    3.3.1 A synthesis of SON Attacks .................................................................... 55
    3.3.2 Physical attacks ....................................................................................... 56
Table of Contents

3.3.3 Active attacks.............................................................. 57
3.3.4 Attacks on VANET.......................................................... 59
3.4 Problem formulation ......................................................... 60
  3.4.1 Mathematical formulation................................................. 61
  3.4.2 Complexity of exact mathematical formulation...................... 62
3.5 Methodology of the Approach ............................................. 62
  3.5.1 Adaptive security Framework........................................... 64
  3.5.2 Trust........................................................................... 64
  3.5.3 Reputation ..................................................................... 65
  3.5.4 Trust and Network .......................................................... 66
3.6 Conclusion and Summary ................................................... 67
3.7 REFERENCES ..................................................................... 68

Chapter 4. Autonomic Computing for adaptive security .................. 75
  4.1 Introduction ..................................................................... 75
  4.2 The Autonomic System........................................................ 76
    4.2.1 Background................................................................. 76
    4.2.2 Autonomic properties.................................................... 78
    4.2.3 Issues in autonomic communications: SmartCity ............... 79
    4.2.4 Discussion ................................................................. 82
    4.2.5 Architecture of autonomic system................................. 82
  4.3 Adaptive security .............................................................. 84
    4.3.1 Introduction to adaptive security.................................... 84
    4.3.2 Definition Adaptive Security......................................... 85
    4.3.3 Adaptive security architecture..................................... 85
  4.4 Summary ........................................................................... 89
  4.5 REFERENCES ..................................................................... 91

Chapter 5. Design and Methodology Description of the Framework .... 93
  5.1 Motivation ....................................................................... 93
    5.1.1 Complex adaptive Systems in Security Design.................. 95
  5.2 Adaptivity model .............................................................. 96
    5.2.1 Justifications .............................................................. 96
    5.2.2 Adaptive Framework................................................... 98
  5.3 Discussion of SARM.......................................................... 100
    5.3.1 Security Means........................................................... 101
    5.3.2 Trust and reputation as means of SARM......................... 103
    5.3.3 Digital identity as means in SARM................................. 107
    5.3.4 Summarizing Table for identity management................... 108
  5.4 High level SARM ............................................................. 109
    5.4.1 Methodology Design Approach..................................... 109
    5.4.2 Verification of Methodology........................................ 109
  5.5 Discussion and summary .................................................... 109
  5.6 REFERENCES ..................................................................... 110

Chapter 6. Implementation and experiments ................................ 113
  6.1 Introduction ...................................................................... 113
    6.1.1 Analysis of Resource costs for security ......................... 114
    6.1.2 Assumptions and experiments...................................... 115
    6.1.3 Metrics and Measurements Methods.............................. 116
    6.1.4 Results and Discussion ............................................... 118
# Table of Contents

6.2 Conclusion ............................................................................................................. 123  
6.2.1 Summary ........................................................................................................... 123  
6.3 REFERENCES ....................................................................................................... 124  

Chapter 7. Simulation and Evaluations ................................................................. 125  
7.1 Validation process ............................................................................................... 125  
7.1.1 Simulation tools: ............................................................................................. 126  
7.1.2 Model Set-up .................................................................................................. 126  
7.1.3 Experiment methodology for Wi-Fi .................................................................. 126  
7.2 Use case: Wi-Fi hotspot simple approach ......................................................... 127  
7.2.1 System Model .................................................................................................. 128  
7.2.2 Decision-Making Function ............................................................................ 128  
7.2.3 SARM evaluation ............................................................................................ 129  
7.2.4 State-chart and context .................................................................................. 130  
7.2.5 Scenarios ......................................................................................................... 131  
7.2.6 Results Analysis .............................................................................................. 131  
7.2.7 Results ............................................................................................................. 135  
7.3 Use case: Hotspots, trust & reputation ............................................................. 135  
7.3.1 Context: ......................................................................................................... 135  
7.3.2 Approach ........................................................................................................ 136  
7.3.3 The security problem and related work ......................................................... 137  
7.3.4 Wi-Fi Trust and reputation solutions .............................................................. 139  
7.3.5 Trust and reputation ....................................................................................... 140  
7.3.6 State-chart and context .................................................................................. 142  
7.3.7 Scenarios ......................................................................................................... 144  
7.3.8 Results Analysis .............................................................................................. 145  
7.3.9 Synthesis ......................................................................................................... 146  
7.4 Use case: SARM in WSN .................................................................................... 147  
7.4.1 WSN-SARM .................................................................................................... 148  
7.4.2 Goal of SARM-WSN ...................................................................................... 149  
7.4.3 WSN-SARM Description .............................................................................. 149  
7.4.4 State chart and context .................................................................................. 153  
7.4.5 Validation Methodology .................................................................................. 153  
7.4.6 Scenarios ......................................................................................................... 157  
7.4.7 Metrics ............................................................................................................ 158  
7.4.8 Results Analysis .............................................................................................. 158  
7.5 Use case: SARM in service of Green 2.0 .......................................................... 163  
7.5.1 Sensor Energy Consumption ......................................................................... 164  
7.5.2 The Main Problem: use case ......................................................................... 165  
7.5.3 Implementation of Green-SARM ................................................................. 166  
7.5.4 Implementation and Validation Methodology .............................................. 168  
7.5.5 Results Analysis .............................................................................................. 171  
7.5.6 CONCLUSION ................................................................................................. 177  
7.6 General conclusion ............................................................................................. 178  
7.7 Related Work and comparison ......................................................................... 178  
7.7.1 Motivation and evaluation .............................................................................. 178  
7.7.2 Comparison ..................................................................................................... 180  
7.8 Summary ............................................................................................................. 185  
7.9 REFERENCES ..................................................................................................... 186
### Chapter 8. Conclusions and Future Work

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1</td>
<td>What have we learned?</td>
<td>189</td>
</tr>
<tr>
<td>8.2</td>
<td>Conclusions</td>
<td>190</td>
</tr>
<tr>
<td>8.3</td>
<td>Overall Conclusion</td>
<td>191</td>
</tr>
<tr>
<td>8.4</td>
<td>Contributions</td>
<td>191</td>
</tr>
<tr>
<td>8.5</td>
<td>Future research</td>
<td>193</td>
</tr>
<tr>
<td>8.6</td>
<td>Final summary</td>
<td>193</td>
</tr>
</tbody>
</table>
Résumé

Comme les réseaux sans fil et mobiles sont devenus de plus en plus hétérogènes, complexes et particulièrement dynamiques, les exigences en termes de sécurité sont devenues d'autant multiples et doivent être abordées d'une manière souple et dynamique afin de faire face au contexte d'exécution en constante changement.

En outre, les réseaux de capteurs WSN devraient également être en mesure de remplir leur mission dans des milieux hostiles, tels que les environnements sous attaques dites "Sinkholes". En effet, la sécurité dans les WSN est devenue un sujet de recherche d'actualité, en raison de son déploiement à grande échelle et le nombre croissant de nouvelles attaques auxquelles elle doit faire face.

Nous observons que les protocoles de sécurité classiques basés sur la résolution des problèmes de sécurité en mode statique, ne peuvent plus faire face à des attaques dynamiques. En outre, ils freinent l'utilisation efficace des ressources de capteurs en compromettant, inévitablement, l'efficacité globale du réseau. Partant, l'objectif de l'informatique verte basée sur l'initiative (Green 1.0) n'est pas rempli.

Les exigences des nouveaux mécanismes de sécurité doivent donc être traitées de manière flexible.

En effet, il y a un manque de protocoles dynamiques et génériques qui adaptent leur sécurité pour faire face à des conditions extrêmement dynamique, et pour satisfaire les performances exigées dans le cadre de réseaux mobiles et sans fil (MWSN), où la fiabilité et la survie globale du réseau sont des critères essentiels pour de nombreuses applications.

Sans aucun doute, un moniteur de référence, qui adapte sa sécurité hautement dynamique, doit être basé sur un système bio-inspiré. Ceci pour faire face aux conditions extrêmement dynamiques de sécurité en satisfaisant les performances exigées, y compris la qualité de service.

Nous avons proposé un Moniteur de référence de sécurité adaptable (SARM) pour les environnements sans fil et mobiles, visant à offrir un Framework capable d'intégrer efficacement les nouveaux domaines émergents tels que la biosécurité, la confiance et green IT - afin de faire face efficacement à la sécurité des systèmes complexes.

En effet, le SARM est basé sur un système dit "Autonomic Computing" utilisant une boucle rétroactive pour choisir le meilleur moyen de sécurité via la rétroaction. Ce faisant, nous pouvons peaufiner le choix, en temps réel, des contre réactions adéquates aux différentes attaques dynamiques.

Ces moyens peuvent être des systèmes cryptographiques choisis selon l'évolution du contexte, l'environnement de l'utilisateur et les aspects de la consommation d'énergie. En particulier, notre système est basé sur les caractéristiques bio-inspirées telles que l'autogestion et l'auto-optimisation.

Des simulations approfondies utilisant une approche basée sur la programmation par agent ont également été menées afin de vérifier la
performance de SARM dans le cas de MWSN en présence de différents attaquants. Les résultats montrent clairement que le SARM est efficace en termes de survie "Survivability", de l'utilisation globale du réseau et la consommation d'énergie.

Une autre contribution importante de cette recherche a été la mise en œuvre et l'évaluation des SARM pour choisir le point d'accès le plus fiable grâce à l'utilisation de systèmes de confiance et réputés.

Des études de performances énergétiques ont été entreprises pour comparer les consommations de différents moyens sécuritaires utilisés dans le Framweork. Les résultats et les analyses de cette expérience indiquent que les fonctions de gestion de sécurité sont correctes et que la sécurité globale est assurée efficacement pour les différents comportements d'attaques. Ceci permet d'obtenir une avancée conséquente dans le domaine des systèmes de sécurité vert bio-inspirés.
Abstract

Since wireless and mobile networks have become increasingly heterogeneous, complex and particularly dynamic, multiple security requirements must be addressed in a flexible and dynamic manner in order to cope with the changing runtime context. In addition, Wireless Sensor Networks (WSN) should also be capable of fulfilling their mission in hostile milieux such as in sinkhole attack environments. Indeed, security in WSN has become a hot research topic due to their widespread deployment and the increasing number of new runtime attacks that they must face. We observe that conventional security protocols address security problems in a static fashion, and cannot deal with dynamic attacks. Moreover, they limit the efficient use of sensor resources and inevitably, overall network efficiency is not guaranteed. Thus, the objective of the green computing (Green 1.0) initiative is not fulfilled. The requirements of new security mechanisms must therefore be addressed in a flexible manner. Indeed, there is a lack of generic security adaptation protocols to deal with extremely dynamic security conditions and performances in the context of Mobile Wireless Networks (MWSN) where reliability and survivability are critical criteria for many applications. Definitely, a generic high level security adaptation reference monitor must be developed based on a bio-inspired system in order to deal with the extremely dynamic security conditions and also with performance, including Quality of Service. We have proposed a Security Adaptation Reference Monitor (SARM) for wireless and mobile environments that aims to offer a Framework capable of effectively integrating new, emerging domains -such as bio-security, trust and green IT- in order to deal efficiently with the security of complex systems.

Indeed, SARM is based on an autonomic computing security feedback loop regulation system, which fine-tunes security means from counteraction schemes and cryptography strength based on monitoring of the context, including the user environment and energy consumption aspects. In short, it is based on self-x bio-inspired characteristics, such as self-management and self-optimization.

Extensive simulations using an agent-based approach have also been conducted in order to verify the performance of SARM in the case of MWSN in the presence of attackers. The results clearly show that SARM is efficient in terms of survivability, overall network utilization and power consumption.

Another key contribution of this research has been the implementation and evaluation of SARM in selecting the best Access Point through the use of trust and reputation paradigms. Energy performance analysis have been undertaken to compare the consumption of different security methods used in the Framework.

The results and analysis of the experiments indicate that the security management functions properly and that security is provided efficiently for diverse behaviors. This provides a strong milestone in the field of bio-inspired green security of complex systems.
Acknowledgments

First, I would like to acknowledge the Grace of God, mainly for his blessings. I am very glad to also be able to thank my parents and friends, who have supported me not only during the thesis, but also throughout my life.

I would next like to thank Prof. Dimitri Konstantas. It is my great good fortune to have met him, because he has had the aptitude to encourage me in starting as well as in finishing this thesis. He gave me the opportunity to do my PhD research in his excellent Advanced Systems Group. I am thankful for his kindness and patience with me over the years.

This work would not have been possible without the guidance of my mentor, the enlightened Dr. Jean-Marc Seigneur, because he has taken it upon himself to lead my path. Indeed, Dr. Seigneur has guided my way over the past few years not only with his intellect and knowledge, but also with real thoughtfulness about my research subject.

I have benefited greatly from each conversation with him about security, networking and all other subjects. Dr. Seigneur in particular was the person who really suggested that I should take up the study of the subject of my thesis.

I would like to thank the thesis jury Prof. Giovanna Di Marzo Serugendo, Prof. Sviatoslav Voloshynovskiy, and particularly Prof. Yanjun Zuo for his relevant and grateful remarks, suggestions and references in the fields of moving target defense and adaptive multi-agent systems.

I would not be truly grateful if I did not thank my students who participated in this research. There are many whom I would like to thank, including Oliver Oudoum, Michael De Azevedo and others. I would especially like to thank Andrés Revuelta for his active help, as this has meant that I have had time to continue this thesis.

Finally, I would like to thank Dr. Ciaran Burke for his relevant and meticulous dissertation corrections.
Biographical Sketch

Tewfiq EL MALIKI was born in 1967 in Morocco and received his Baccalaureate with honors in mathematics before becoming an Electrical Engineer (M.S. Telecommunication orientation) at the Swiss Federal Institute of Technology in Lausanne (EPFL), Switzerland in 1992. He started as a research and development engineer in the field of TV setup-box cryptography at Nagra-vision. In 1995, he worked as a research assistant in the telecommunication lab of the EPFL and was in charge of the assessment of the Telecom PTT research on xDSL systems in access networks.

Later, he worked as a product manager and was also a new telecommunications technologies instructor at Swisscom. In 1999, he became a project manager at the Federal Office of Communications, mainly managing unbundling projects within the local loop and the introduction of LRIC-based pricing for interconnection.

He is currently working as a Professor in the Department of ICT at the Geneva University of Applied Sciences, Switzerland.

His research interests include mobile and sensor network security, data security, simulation and teletraffic. At the moment, he is working on research projects in the field of digital identities and security in mobile and Wireless Sensor Networks.
List of Figures

Figure 1: Internet of Thing a new dimension of AAA ........................................... 2
Figure 2: Internet of Thing a new dimension of AAA ........................................... 3
Figure 3: The many facets of privacy protection ....................................................... 4
Figure 4: Security management triangle .................................................................. 4
Figure 5: General model of autonomic Adaptation architecture ............................. 7
Figure 6: Spider map of the Major contribution areas of the Thesis ....................... 8
Figure 7: Major domains and articles related to state-of-the art of the thesis ......... 9
Figure 8: Number of World wide mobile subscribers .............................................. 14
Figure 9: Road map for next generation mobile cellular network ......................... 16
Figure 10: Mapping of wireless networks - mobility and range ............................. 17
Figure 11: Road map to 5G .................................................................................. 18
Figure 12: Risk is a combination of probability, threat and impact ...................... 20
Figure 13: Threat is a combination of Actor, Motivation and Vulnerability ............ 20
Figure 14: Security countermeasures display a decrease in returns related to effort beyond optimum (effort*, security*) ................................................................. 22
Figure 15: A Taxonomy of Security-Related Requirements .................................. 23
Figure 16: Security model .................................................................................... 25
Figure 17: Reference Monitor model ..................................................................... 27
Figure 18: MAPE-K : Autonomous element ......................................................... 31
Figure 19: trust layer in security systems ............................................................... 33
Figure 20: Reputation topology ............................................................................ 34
Figure 21: Goals of trust and reputation systems for SONs ................................... 36
Figure 22: Trust relationship ................................................................................. 65
Figure 23: Soft security ......................................................................................... 66
Figure 24: Inter-relationship among trust constructs [McKnight and Chervany] 67
Figure 25: an urban Autonomic system scenario in a Smart City ....................... 81
Figure 26: Description of autonomic system ......................................................... 83
Figure 27: Control Loop description of autonomic system with details ............... 84
Figure 28: Moving toward continuous security protection .................................. 86
Figure 29: plot of Cost security function for k=1 .................................................. 88
Figure 30: Risk management related to autonomic and security adaptation systems ................................................................. 89
Figure 31: level of security adaptation ................................................................. 96
Figure 32: General model of autonomic Adaptation architecture ....................... 97
Figure 33: Breakdown of Adaptive quintuple model ............................................ 99
Figure 34: Foundations of our adaptive security Framework ................................ 100
Figure 35: Security Means details ....................................................................... 102
Figure 36: Security adaptation Framework .......................................................... 103
Figure 37: A model for rating process, with ratings by agents from set A for a given object, O ................................................................. 104
Figure 38: A network of three vertex and oriented edges .................................... 105
Figure 39: Josang belief represented as triangle .................................................... 106
Figure 40: Architecture of SC-SD ........................................................................ 114
Figure 41: Scheme of experimental energy consumption circuit ......................... 116
Figure 42: Experimental test-bed energy consumption ........................................ 117
Figure 43: Download time of different files (sec, non-sec.) .................................. 118
Figure 44: Configuration of SARM experiments ........................................... 119
Figure 45: Power for idle mode ................................................................. 120
Figure 46: Power for voice transmission without encryption .......................... 121
Figure 47: Power for AES voice encryption ................................................. 121
Figure 48: Power for different cases of voice encryption .............................. 122
Figure 49: Animation interface and results ............................................... 127
Figure 50: Simulation scenario WIFI ......................................................... 129
Figure 51: State-charts: Movement and Status of agents .............................. 130
Figure 52: Performance of Light SARM and references ................................ 132
Figure 53: Min-Max & std-dev. for Light-SARM & References ...................... 133
Figure 54: Effect of threshold on overall utilization 1st Scenario ................. 133
Figure 55: Effect of threshold on overall utilization 2nd Scenario ................. 134
Figure 56: A normal Wi-Fi access user interface ....................................... 136
Figure 57: New Wi-Fi user access interface with trust ranking .................... 137
Figure 58: Trust model overview ............................................................. 139
Figure 59: State-chart: Fixed APs and mobile users .................................. 143
Figure 60: Comparison of low and high density APs in the first scenario ...... 145
Figure 61: Comparison of low and high density APs in the second scenario .. 146
Figure 62: WSN-SARM Modules ............................................................. 150
Figure 63: Context of WSN-SARM .......................................................... 151
Figure 64: Animation interface of Arranged WSN-SARM ......................... 152
Figure 65: State-charts: “Transmission” of agents “SensorStateR” and “TF” .. 153
Figure 66: Animation interface and results of Random WSN-SARM .......... 157
Figure 67: Reliability of references for the 3 scenarios .............................. 159
Figure 68: Reliability of WSN-SARM for the 3 scenarios ......................... 159
Figure 69: Long-term reliability of WSN-SARM for second scenario ........... 160
Figure 70: Reliability of WSN-SARM for the second scenario .................... 161
Figure 71: Energy Loss of SARM for the second scenario, No Trust ............ 162
Figure 72: Reliability and Energy Loss of WSN-SARM for the second scenario .................................................................................. 163
Figure 73: Adapted SARM: Green-SARM ............................................... 166
Figure 74: Communication protocol based on soft security ......................... 167
Figure 75: State chart of sensors .............................................................. 169
Figure 76: Animation of Model Context .................................................... 170
Figure 77: 1000 sensors for the first scenario (Green-SARM) .................... 172
Figure 78: Network of 1000 Sensors for the first scenario (without SARM) ... 173
Figure 79: 500 sensors for the first scenario (without SARM) ..................... 173
Figure 80: Gain in terms of survivability for 20% rate of attackers for [100,1000] of sensors .................................................................................. 174
Figure 81: graph of 100 sensors for the second scenario using Green-SARM 176
Figure 82: graph of 100 sensors for the second scenario (without-SARM) .... 176
Figure 83: Survivability of 100 sensors for different scenarios .................... 177
Figure 84: Dimensions of the security services perspective ....................... 179
Figure 85: Dimension of the adaptation method perspective ....................... 179
Figure 86: Evaluation of SARM related to security services perspectives ...... 183
Figure 87: Main dimensions of SARM adaptation method .......................... 184
# List of Tables

Table 1: Four aspects of self-management as they are now and as they would be with autonomic computing .......................................................... 29
Table 2: Classification of trust and reputation measures [61] .................... 35
Table 3: Comparison of different trust models [96] .................................. 40
Table 4: WLAN principal parameters .................................................... 53
Table 5: MANET principal parameters ............................................... 53
Table 6: WSN principal parameters ................................................... 53
Table 7: VANET principal parameters .................................................. 54
Table 8: Shows the attacks and associated layer .................................... 55
Table 9: Active SON attacks and counterattacks references .................... 58
Table 10: Passive SON attacks and counterattacks references .................. 57
Table 11: Major 20 Autonomic characteristics and description ............... 78
Table 12: Adaptive security model description ................................... 99
Table 13: Evaluation of identity 2.0 technologies .................................. 108
Table 14: Main characteristics of experiments ..................................... 116
Table 15: Energy consumption for mobile networks (20s, 50 KB) ............. 122
Table 16: User behavior and recommended actions to neighbors .............. 129
Table 17: Access Point Behaviors ...................................................... 144
Table 18: Initialization and effect of our variables .................................. 145
Table 19: Statistics for average number of connections in the second scenario .................................................................................................................. 146
Table 20: Statistics for average number of connections in the second scenario .................................................................................................................. 147
Table 21: Behavior and recommended actions sent by Base Station to a Sensor under sinkhole attack ........................................................................ 150
Table 22: Characteristic data for the Mica2dot sensor platform: 3V, 4MHz, 915MHz transceiver, transmit power 5 dBm ........................................... 164
Table 23: Behavior and recommended value sent by Base Station to Sensor for Sinkhole and Jammer attacks ......................................................... 166
Table 24: The main characteristics of SARM and of 4 other frameworks .... 182
Table 25: Main characteristics of SARM in Autonomic system ............... 183
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAAA</td>
<td>Anyone, Anytime, Anyone, Anything</td>
</tr>
<tr>
<td>AODV</td>
<td>Ad hoc On-Demand Distance Vector</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
</tr>
<tr>
<td>BAN</td>
<td>Body Area Network</td>
</tr>
<tr>
<td>BS</td>
<td>Base station</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>CONFIDENT</td>
<td>Cooperation Of Nodes: Fairness In Dynamic Ad-hoc</td>
</tr>
<tr>
<td>CORE</td>
<td>COllaborative Reputation</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>DARPA</td>
<td>Defense Advanced Research Projects Agency</td>
</tr>
<tr>
<td>DCS</td>
<td>Data Centric Sensor</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed DoS</td>
</tr>
<tr>
<td>DMF</td>
<td>Decision Making Function</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DRBTS</td>
<td>Distributed Reputation-based Beacon Trust System</td>
</tr>
<tr>
<td>DSR</td>
<td>Dynamic Source Routing</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>EDGE</td>
<td>Enhanced Data Rates for GSM Evolution</td>
</tr>
<tr>
<td>ENISA</td>
<td>European Network and Information Security Agency</td>
</tr>
<tr>
<td>EPFL</td>
<td>Ecole Polytechnique de Lausanne</td>
</tr>
<tr>
<td>GPRS</td>
<td>General packet radio service</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile</td>
</tr>
<tr>
<td>Gx</td>
<td>Global system for mobile Generation x</td>
</tr>
<tr>
<td>HSCSD</td>
<td>High-Speed Circuit-Switched Data</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technology</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electro-technical Commission</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Thing</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
</tbody>
</table>
IPTV  IP Television
ISO  International Standard Organization
ITSEC  Information Technology Security Evaluation Criteria
ITSEC  Information Technology Security Evaluation Criteria
ITU  International Telecommunications Union
LRIC  Long Run Incremental Cost
LTE  long-term evolution
MANET  Mobile Ad-hoc NETwork
MAPE-K  Management, Analyze, Plan, Execute, Knowledge
MP  Mobile Phone
MWSN  Mobile Wireless Sensor Network
NASA  National Aeronautics and Space Administration
NIST  National Institute of Standards and Technology
OCEAN  Observation Based Cooperation Enforcement in Mobile adHoc Network
OS  Operating System
P2P  Peer to Peer
PAN  Personal Area Network
PCM  Pulse Code Modulation
PDC  Personal Digital Cellular
pdf  Probability density function
PKI  Public Key Infrastructure
QoC  Quality of Context
QoE  Quality of Experience
QoS  Quality of Service
QoSS  Quality of Service and Security
RFID  Radio Frequency Identity
RFSN  Reputation-based Framework for Sensor Network
RFSN  Reputation based framework for sensor networks
RM  Reference Monitor
RREP  Route REPlay
RSS  Robust Reputation System
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTP</td>
<td>Real Time Protocol</td>
</tr>
<tr>
<td>RWP</td>
<td>Random WayPoint</td>
</tr>
<tr>
<td>SAML</td>
<td>Security Assertion Markup Language</td>
</tr>
<tr>
<td>SARM</td>
<td>Security Adaptation Reference Monitor</td>
</tr>
<tr>
<td>SD</td>
<td>Secure Digital</td>
</tr>
<tr>
<td>SDSI</td>
<td>Simple Distributed Security Infrastructure</td>
</tr>
<tr>
<td>SIL</td>
<td>Security Importance Level</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol</td>
</tr>
<tr>
<td>SIP ID</td>
<td>SIP Identity</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message System</td>
</tr>
<tr>
<td>SN</td>
<td>Sensor Node</td>
</tr>
<tr>
<td>SON</td>
<td>Self Organizing Network</td>
</tr>
<tr>
<td>SPKI</td>
<td>Simple Public Key Infrastructure</td>
</tr>
<tr>
<td>SSID</td>
<td>Service Set IDentifier</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Session layer</td>
</tr>
<tr>
<td>TA</td>
<td>Trust Authority</td>
</tr>
<tr>
<td>TCAODV</td>
<td>Trust Computing</td>
</tr>
<tr>
<td>TCP</td>
<td>Transport Control Protocol</td>
</tr>
<tr>
<td>TF</td>
<td>Trust Function</td>
</tr>
<tr>
<td>ToIP</td>
<td>Telephony over IP</td>
</tr>
<tr>
<td>TPM</td>
<td>Trusted Platform Module</td>
</tr>
<tr>
<td>TTL</td>
<td>Time To Live</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UML</td>
<td>Unified Modeling Language</td>
</tr>
<tr>
<td>UML-RT</td>
<td>Unified Modeling Language- Real Time</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunication System</td>
</tr>
<tr>
<td>VANET</td>
<td>Vehicular Ad-hoc NETwork</td>
</tr>
<tr>
<td>WCDM</td>
<td>Wideband Code Division Multiple Access</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Wireless Fidelity</td>
</tr>
<tr>
<td>WiMax</td>
<td>Worldwide Interoperability for Microwave Access</td>
</tr>
<tr>
<td>WISPss</td>
<td>Wireless Internet service providers</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>WMESH</td>
<td>Wireless Mesh</td>
</tr>
<tr>
<td>WMN</td>
<td>Wireless Mesh Network</td>
</tr>
<tr>
<td>WPAN</td>
<td>Wireless Personal Area Network</td>
</tr>
<tr>
<td>WSN</td>
<td>Wireless Sensor Network</td>
</tr>
<tr>
<td>x</td>
<td>One of</td>
</tr>
<tr>
<td>xDSL</td>
<td>One of Digital Subscriber Line</td>
</tr>
<tr>
<td>xG</td>
<td>One of Cellular Generation</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
</tbody>
</table>
List of Definitions

access control
Enable authorized use of a resource while preventing unauthorized use or use in an unauthorized manner.

accountability
The security objective that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

adaptive system
an autonomic system that is be able to choose the best configuration according to its objectives, policies and users' preferences

assurance
Grounds for confidence that the other four security objectives (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. "Adequately met" includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or by-pass.

automaticity
the heart of a control feedback system and its ability to adapt its internal functions and means

autonomic system
is a system that operates and serves its purpose by managing its own self without external intervention even in case of environmental changes

authentication
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.

authorization
The granting or denying of access rights to a user, program, or process.

availability
The security objective that generates the requirement for protection against intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise cause a denial of service or data.

awareness
This property will adapt the system in response to context or state changes. In fact, an autonomic system must be able to sense its environment as well its internal state in order to assess its control feedback in respect of its objectives.

computing security methods
Computing security methods are security safeguards implemented within the IT, using the networking, hardware, software, and firmware of the IT. This includes (1) the hardware, firmware, and software that implements security functionality and (2) the design, implementation, and verification techniques used to ensure that system assurance requirements are satisfied.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>confidentiality</td>
<td>The security objective that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and while in transit.</td>
</tr>
<tr>
<td>data integrity</td>
<td>The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.</td>
</tr>
<tr>
<td>data origin authentication</td>
<td>The verification that the source of data received is as claimed.</td>
</tr>
<tr>
<td>denial of service</td>
<td>The prevention of authorized access to resources or the delaying of time-critical operations.</td>
</tr>
<tr>
<td>domain</td>
<td>See security domain.</td>
</tr>
<tr>
<td>entity</td>
<td>Either a subject (an active element that operates on information or the system state) or an object (a passive element that contains or receives information).</td>
</tr>
<tr>
<td>freshness</td>
<td>Data freshness ensures that the data is recent and that no old messages have been replayed in order to protect data aggregation schemes against replay attacks.</td>
</tr>
<tr>
<td>identity</td>
<td>Information that is unique within a security domain and which is recognized as denoting a particular entity within that domain.</td>
</tr>
<tr>
<td>identity-based security policy</td>
<td>A security policy based on the identities and/or attributes of the object (system resource) being accessed and of the subject (user, group of users, process, or device) requesting access.</td>
</tr>
<tr>
<td>integrity</td>
<td>The security objective that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).</td>
</tr>
<tr>
<td>IT Security Architecture</td>
<td>A description of security principles and an overall approach for complying with the principles that drive the system design; i.e., guidelines on the placement and implementation of specific security services within various distributed computing environments.</td>
</tr>
<tr>
<td>IT security objective</td>
<td>See “Security objective”.</td>
</tr>
<tr>
<td>IT-related risk</td>
<td>The net mission/business impact (probability of occurrence combined with impact) from a particular threat source exploiting, or triggering, a particular information technology vulnerability. IT related-risks arise from legal liability or...</td>
</tr>
</tbody>
</table>
mission/business loss due to:
1. Unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information.
2. Non-malicious errors and omissions.
3. IT disruptions due to natural or man-made disasters.
4. Failure to exercise due care and diligence in the implementation and operation of the IT.

non-computing security methods

Non-computing methods are security safeguards which do not use the hardware, software, and firmware of the IT. Non-computing methods include physical security (controlling physical access to computing resources), personnel security, and procedural security.

object

A passive entity that contains or receives information. Note that access to an object potentially implies access to the information it contains.

QoS

International Telecommunication Union (ITU) Recommendation E.800 “Totality of characteristics of a telecommunications service that bear on its ability to satisfy stated and implied needs of the user of the service”.

reference monitor

The security engineering term for IT functionality that (1) controls all access, (2) cannot be bypassed, (3) is tamper-resistant, and (4) provides confidence that the other three items are true.

residual risk

The remaining, potential risk after all related security measures are applied. There is a residual risk associated with each threat.

risk

Within this document, synonymous with “IT-related risk.”

risk analysis

The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.

risk assessment

See risk analysis

risk management

The total process of identifying, controlling, and mitigating information technology related risks. It includes risk analysis; cost-benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission/business and constraints due to policy, regulations, and laws.

rule-based security policy

A security policy based on global rules imposed for all subjects. These rules usually rely on a comparison of the sensitivity of the objects being accessed and the possession of corresponding attributes by the subjects requesting...
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>security</td>
<td>Security is a system property. Security is much more that a set of functions and mechanisms. Information technology security is a system characteristic as well as a set of mechanisms which span the system both logically and physically.</td>
</tr>
<tr>
<td>security domain</td>
<td>A set of subjects, their information objects, and a common security policy.</td>
</tr>
<tr>
<td>security goal</td>
<td>The IT security goal is to enable an organization to meet all mission/business objectives by implementing systems with due care consideration of IT-related risks to the organization, its partners, and its customers.</td>
</tr>
<tr>
<td>security objectives</td>
<td>The five security objectives are integrity, availability, confidentiality, accountability, and assurance.</td>
</tr>
<tr>
<td>security policy</td>
<td>The statement of required protection of the information objects.</td>
</tr>
<tr>
<td>subject</td>
<td>An active entity, generally in the form of a person, process, or device, which causes information to flow among objects or changes the system state.</td>
</tr>
<tr>
<td>system integrity</td>
<td>The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.</td>
</tr>
<tr>
<td>survivability</td>
<td>For a system, this is the capacity to fulfill its mission in a timely manner, in the presence of intrusions, attacks, accidents and failures.</td>
</tr>
<tr>
<td>threat</td>
<td>The potential for a “threat source” (defined below) to exploit (intentional) or trigger (accidental) a specific vulnerability.</td>
</tr>
<tr>
<td>threat analysis</td>
<td>The examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.</td>
</tr>
<tr>
<td>threat source</td>
<td>Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) the situation and method that may accidentally trigger a vulnerability.</td>
</tr>
<tr>
<td>tolerance</td>
<td>Is the process of masking runtime failures of a system by eliminating faulty components, limiting the fault effect, and allocating valid substitutes.</td>
</tr>
<tr>
<td>traffic analysis</td>
<td>The inference of information from observation of traffic flows (presence, absence, amount, direction, and frequency).</td>
</tr>
<tr>
<td>traffic flow confidentiality</td>
<td>A confidentiality service to protect against traffic analysis.</td>
</tr>
</tbody>
</table>
vulnerability  A weakness in system security procedures, design, implementation, internal controls, etc., that could be accidentally triggered or intentionally exploited and result in a violation of the system’s security policy.
List of Symbols

a parameter
A Component framework model
A = {} Set of agents
AS = (A,X,Q,TUp,Uf) Adaptive security 5-tuple
CM Countermeasures
Cost (.) Cost Function
Cost '(.) Cost Derived function
d distance
F Failures
k Constant
M Security Means
Neg Negative Trust Value
Neu Neutral Trust Value
O={o} Set of Object
p(.) frequency distribution
P(.) Power
Pos Positive value
Pr Probability
Q() General Criterion Function
Q Adaptness
qi,j Criterion Function
ρ rating
ρik represents the rating by agent ai on object Ok
ρij be the rating that agent i has for agent j
S Security
Si Sensor i
TF(.) Trust Function
Tj Tasks
Ti,vj(vij) Trust of values vij (i packets) sent by the BS to sensor z about his neighbor sensor j
<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust()</td>
<td>General Trust Function</td>
</tr>
<tr>
<td>$T_x(v,T)$</td>
<td>Evaluation Function for a threshold T and the result x</td>
</tr>
<tr>
<td>U</td>
<td>User</td>
</tr>
<tr>
<td>$U_f$</td>
<td>Utility function (adaptation strategy)</td>
</tr>
<tr>
<td>$U_p$</td>
<td>User Preferences</td>
</tr>
<tr>
<td>V</td>
<td>Vector</td>
</tr>
<tr>
<td>$v_{ij}$</td>
<td>Value of ij coordinates</td>
</tr>
<tr>
<td>$\Omega { T }$</td>
<td>Set of Tasks</td>
</tr>
<tr>
<td>X</td>
<td>Context</td>
</tr>
<tr>
<td>$A(S)$</td>
<td>Non security component</td>
</tr>
<tr>
<td>$A(QP)$</td>
<td>Quality proprieties</td>
</tr>
<tr>
<td>$A(SP)$</td>
<td>Security proprieties</td>
</tr>
</tbody>
</table>
Chapter 1. Introduction

“Security is, I would say, our top priority because for all the exciting things you will be able to do with computers - organizing your lives, staying in touch with people, being creative - if we don't solve these security problems, then people will hold back.”

-Bill Gates, Microsoft CEO.

1.1 Motivation

More than ever, we have become dependent on Information and Communication Technology (ICT). Many aspects of our daily lives are dependent on ICT, among others energy, transport, education, police, military and business. Therefore, there are major reasons why both individuals and civil or military organizations have to be vigilant in keeping information and communication systems secure. Indeed, security looms as a significant issue in our everyday lives, even for services the primary functions of which do not relate to security [2]. Thus, it is a part of the cement that holds societies together. Without security, no business or state can hold. [3]

Likewise, the use of wireless networks has become more widespread in civil and military domains. Nevertheless, wireless networks are vulnerable to a greater number of security problems than any other form of network, as they are mainly mobile or Ad Hoc networks [3, 4]. In wireless networks, the transmission channel is open to the air, and attackers find it easier to interrupt transmission and/or break into the network to access information. If the network security is not strong enough, the network will suffer from worms, viruses, spam and so on [7], or the entire network will be put out of use. In fact, threats come with the classic security problems in addition to other problems related to the wireless nature of the networks, as well as their complexity and energy limitations. These properties can represent major security vulnerabilities [4].

Moreover, the Internet of Things (IoT), a network of billions of addressable, smart and mobile devices, will have a real effect on our daily lives in the near future. It is a technological revolution that represents the future of computing and communications, and it is based on dynamic technical innovation in a number of important fields, from wireless sensors to nanotechnology. In this respect, it is a new dimension that has been added to the world of ICT: from anytime, anyplace connectivity for anyone, we will now have connectivity for anything (Figure 1)[5]. In addition, IoT lays the foundations for modernizing our lives through global machine-to-machine interactions and global connectivity between physical objects.

The three major communications related to IoT are based on the three major technology areas: RFID (identifying things), sensors (sensing things) and embedded systems (reading things). These are new and complex systems.
Therefore, what would previously have been a simple communication system is becoming ever more complex, and nowadays involves a huge number of interactions with different environments, the security of which are difficult to ensure. Applications cannot be aware of the need for security mechanisms or indeed of the presence of dynamic, changing forms of attack. It is critical to maintain overall security in relation to configuration complexity and the changing runtime context. Accordingly, any concept that needs to cope with this new security challenge has to be based on, amongst other things, a sufficiently dynamic adaptation security system in order to satisfy overall performance aspects such as power consumption, this being a key issue in mobile networks, especially in sensor networks or the internet of things [6].

In these last networks mentioned, the data at risk could be sensitive and the networks may operate in hostile environments. It is imperative to address these problems from the earliest point of the system’s design. All software development projects need a well-balanced amount of security awareness, right from the beginning. [7]

However, due to the different constraints on and limited power of the abovementioned networks, new security challenges have arisen that are entirely distinct from the conventional ones. In addition, in order to gain widespread acceptance, there are still some barriers that must be surmounted. People are rightly concerned about data privacy, which is a tridimensional subject, as illustrated in Figure 3. Concerns have also been raised about the capacity of smart devices to operate robustly in remote locations with limited power supplies [2]. Another issue is the balancing of security against cost and risk. Indeed, it is

\[\text{Figure 1: Internet of Thing a new dimension of AAA}\]
nonsense to give high levels of protection to data which is not valuable, or to overprotect data at a cost greater than its value.

Therefore, what would previously have been a simple communication system is becoming ever more complex, and nowadays involves a huge number of interactions with different environments, the security of which are difficult to ensure. Applications cannot be aware of the need for security mechanisms or indeed of the presence of dynamic, changing forms of attack. It is critical to maintain overall security in relation to configuration complexity and the changing runtime context. Accordingly, any concept that needs to cope with this new security challenge has to be based on, amongst other things, a sufficiently dynamic adaptation security system in order to satisfy overall performance aspects such as power consumption, this being a key issue in mobile networks, especially in sensor networks or the internet of things [6].

In these last networks mentioned, the data at risk could be sensitive and the networks may operate in hostile environments. It is imperative to address these problems from the earliest point of the system’s design. All software development projects need a well-balanced amount of security awareness, right from the beginning. [7]

However, due to the different constraints on and limited power of the abovementioned networks, new security challenges have arisen that are entirely distinct from the conventional ones. In addition, in order to gain widespread acceptance, there are still some barriers that must be surmounted. People are rightly concerned about data privacy, which is a tridimensional subject, as

**Figure 2: Internet of Thing a new dimension of AAA**
illustrated in Figure 3. Concerns have also been raised about the capacity of smart devices to operate robustly in remote locations with limited power supplies [2]. Another issue is the balancing of security against cost and risk. Indeed, it is nonsense to give high levels of protection to data which is not valuable, or to overprotect data at a cost greater than its value.

![Figure 3](image3.png)

**Figure 3 : The many facets of privacy protection**

In general, security should manage three connected vertexes: usability, cost and risk, as illustrated in Figure 4. This is why security must be adaptable in order to manage the total requirements.

![Figure 4](image4.png)

**Figure 4: Security management triangle**

There is actually enormous research potential in the field of wireless and sensor network security, particularly in relation to limitations of power and performance constraints, but a lot is still to come.

On the other hand, sustainable development has promoted efficiency in the use of resources, which is one of the fundamental principles of green computing (Green 1.0). Its main goal is to reduce the environmental footprint of devices so
that they can process data in a more ecologically balanced way, which will most often lead to energy savings. Indeed, it studies practices which use computing resources efficiently, motivated by the need to reduce the use of materials that are harmful to nature, maximize energy efficiency and productivity, promote recycling and biodegradability, and avoid any increase in manufacturing waste [11, 12].

Security in this field is no exception because it actually leads to the consumption of greater and greater amounts of resources. Another step forward is the Green IT (2.0) initiative, which is also a good means of catalyzing economies of energy. Indeed, in the smart 2020 report [20], the scale of IT’s potential as a force to drive greater efficiency across the economy and help significantly in delivering savings of 15% of global emissions by 2020 are illustrated. By using ICT within the SmartCity concept, we hope to help dramatically in reducing energy consumption, for example by controlling and intelligently managing pollution from big cities. One of the biggest challenges is overcoming the lack of information about the emissions impact of products and services, especially in the context of complex configurations and integration. Also, for the first time, the importance of ICT in terms of its indirect contribution to reducing the greenhouse effect has been highlighted. Thus, the first concerns in the field of ubiquitous computing must relate to energy consumption in adapting security. It is obvious that wireless sensor networks and mobile networks - such as the Mobile Ad-hoc NETwork MANET and Vehicular Ad-hoc NETwork VANET - are very special networks, in the sense that they operate under many more constraints than traditional networks [8, 9, 10]:

a. Severe limitation of available resources
b. Highly dynamic networks
c. Open to a wide variety of security vulnerabilities and threats

The above discussion leads us to draw two conclusions.

a. The first conclusion is that, due to the levels of system and network complexity, an adaptive security system dealing with energy consumption and survivability cannot be a basic static component that might contain some state-of-the-art solutions. Moreover, it is difficult to deploy conventional security solutions in attempting to tackle new, emerging forms of attack - and new vulnerabilities. However, we could potentially borrow some fundamentals and classical mechanisms if we consider the depths of their environmental constraints and identify their weaknesses as well as their strangeness.

b. Our second conclusion is that the high level of dynamism and the volatility of the network’s topology and components need ab initio a well designed and flexible framework in order to respond to runtime environmental changes that have the potential to cause the failure of the entire network.

To overcome the abovementioned problems, properties have been developed known as self-x, which refers particularly to the self-management, self-configuration and self-networking elements of communication infrastructures,
collectively referred to as the autonomous communication paradigm, which in recent years has become a key research area because of direct economic and industrial interest [12]. Taking an analogy from the autonomic human nervous system, which regulates homeostatic functions without conscious intelligent control, autonomous communication seeks to simplify the management of complex communication structures and reduce the need for human intervention.

1.2 Thesis Statement

This thesis has investigated methods mainly based on autonomic computing in order to build an adaptive security framework capable of determining appropriate runtime security means for a highly dynamic wireless network with respect to the context-aware, self-management, self-optimization and self-protection paradigms of an autonomic system. In addition, the secure and adaptive framework which has guided the security design since its starting point will exhibit improvement with respect not only to security, survivability and performance, but also to policies and users’ preferences.

1.2.1 Adaptive Security for highly dynamic networks

In order to validate our thesis, we must carry out an implementation, measurements and simulations, as well as some evaluations of our security framework based on its adaptability to different Networks (Mobile Networks: Gx; MANETs, VANETs, WSNs).

The specific problem being addressed concerns the tradeoffs happening between security, performance and efficiency in relation to current and proposed security protocols. These objectives are particularly pertinent in relation to wireless networks, which have constrained network capacity and limited access to resources. Our Framework must fine-tune dynamically the efficient security means (Identity management, PKI, Trust and so on) and network access connections based on the particular context with respect to the policies and vulnerabilities of the network. Therefore, devices and nodes will be able to self-organize into a network using appropriate security protocols and adequate energy consumption components, not only to safeguard security, survivability and performance, but also policies and users’ preferences.
Conclusions and Future Work

According to [14] a common model of adaptive security is described in Fig. 4.

A common model of adaptive security can be defined as a Control Object and a Control Device, the latter of which controls the object and consists of a Detector Device which senses data and collects it, an Analyzer Device which processes the adaptive requirements, and a Response Device which provides the resulting control action. As a result, we have a feedback loop composed of a Detector Device (Sensing), an Analyzer Device (Analyzing and Deciding), and a Responder Device (Acting). This is the basic model of an autonomic element.

Note that the user is also a participant in the autonomic loop, since he can set his preferences and policies as well as being able to react in case of a security attack.

Figure 5 describes the adaptive security architecture principle addressed in this dissertation.

**The fundamental problem to address is**: How to provide the best security means in relation to policies, vulnerabilities, energy consumption, survivability and overall performance, in highly dynamic networks?

Other difficulties relate to the wireless environment, users’ mobility and the heterogeneity of access networks. Moreover, the access context is typically one beyond that of 3G, where many types of access networks may have borders at the same time (UMTS, Wi-Fi, WiMax, LTE and so on). But, the access context might also be one of a Self-organizing network, where each network service unfortunately has its own characteristics such as bandwidth, security policies and vulnerabilities, and provides a different level of security and Quality of Service (QoS) to the running device. Therefore, achieving a balance between all resources is crucial. A useful approach consists of designing a framework capable of striking the best balance between all security means, access
networks and QoS in order to meet user policy and preferences without compromising overall security. Supporting security and QoS simultaneously in this way is a challenging issue, since they compete for the same resources. Thus, an adaptation security framework based on an autonomic system and an adaptive control system is an adequate solution.

1.3 Overview and main contributions

The work of this thesis contributes to the state of the art of many areas, and particularly to four:

First, to adaptive security related to autonomic systems;

Second, to survivability and energy saving in relation to Mobile and Wireless networks;

Third, to Trust and identity management related to Mobile and wireless networks.

Finally, the integration of all of these areas has led to a Security Adaptation Reference Monitor (SARM) Framework that we have deployed for different networks in order to guarantee their overall security. This Framework is used in self-organizing networks (SON) to mitigate the consequences of a substantial number of runtime threats in instances when it does not completely eliminate them.

Figure 6: Spider map of the Major contribution areas of the Thesis
Figure 6 and Figure 7 describe the major contribution areas and major domains and articles related to the state of the art of the thesis respectively. The legend of the two figures is the same and is explained in Figure 5 in the upper left corner. In brief, autonomic system design, security adaptation, SON Networks, mobile identity management and trust and reputation are the principal contribution areas.

1.4 Publications


1.5 Structure of the thesis

This thesis is organized into eight chapters and an appendix that are distributed in three blocks: related works and problem statement (chapters 2 and 3); Framework design and conception (chapters 4 and 5); and implementation description, evaluation and conclusions (chapters 6, 7, 8).

- Chapter 1. : Introduction
- Chapter 2. : Related Work and State of the art, p. 13
- Chapter 3. : Problem Statement and Methodology, p. 49
- Chapter 4. : Autonomic Computing for adaptive security, p. 75
- Chapter 5. : Design and Methodology Description of the Framework, p. 93
- Chapter 6. : Implementation, p. 113
- Chapter 7. : Simulation and Evaluations, p. 125
- Chapter 8. : Conclusions and Future Work, p. 189
1.6 REFERENCES


Chapter 2. Related Work and State of the art

“In listening to any state of the art’s speaker, it’s hard to believe there’s much else that can be done to improve the subject”

- Unknown

In this chapter, we review relevant related work and the state of the art in the field of wireless networks, as well as for their security and related fields.

The chapter is divided into three sections. The first provides a background and literature review, and the second is dedicated to the state of the art. Finally, a conclusion and a summary of the chapter can be found in section 2.3.

2.1 Background and Literature Review

2.1.1 Introduction

There is actually enormous research potential in the field of wireless network security, especially in relation to power limitations and performance constraints. A wireless or mobile network is a special network due to the constraints particular to it, in comparison with a traditional computer network. Therefore, it is difficult to deploy conventional security solutions as things stand. However, taking inspiration from some fundamentals and classical mechanisms, if these are well understood, might be an excellent starting point for designing an adapted security system.

Our study is about analyzing the security constraints within wireless and mobile networks in order to find a solution to the various security problems related to the constantly changing behavior of attackers.

Indeed, the most critical issue in terms of security in mobile networks is that of dealing with the multitude of security challenges, including those attacks based on consuming unnecessary power, and finding a solution capable of responding in runtime to these special attacks.

This solution must reflect the fact that the security means must be proportional to the potential network attacks and, as stated in chapter one, that security should manage three vertexes (risk, cost, usability) in a triangular approach to find the most suitable balance. A generic security adaptation mechanism as a compelling solution to this problem would thus be greatly helpful.

The security deployment must not be based on the classical layered security scheme, which has been shown to be an inadequate and non-optimal solution. As a matter of fact, the deployment of a cross-layer solution would be the most suitable and could greatly extend both the lifespan of the network and the global network utilization.

Our work is inspired by the concept of the Reference Monitor (RM), which was developed for data access [1], autonomous systems [2], and trust and reputation
mechanisms [3], and has commonly been used for the first theme for more than 40 years, and for the second and third themes only in recent decades. It has given efficient results in terms of data access in the security domain and also in the telecommunication domain.

### 2.1.2 Context of Wireless Networks

Before discussing the security of wireless networks, it is important to take a broad look at the major wireless networks which will be used in this work.

**Introduction to different Wireless Network**

![Figure 8: Number of World wide mobile subscribers](source: ITU World Telecommunication ICT Indicators database)

First of all, mobile telecommunication has advanced considerably in the last few years. According to ITU, more than 6 billion people now own mobile phones. Figure 8 depicts a forecast of mobile subscribers for the end of 2013, which is estimated to reach 6.8 billion subscribers. In addition, mobile wireless communication is probably the most active domain in the field of computing and communications. To make it easy for the reader, we present a synthesis description of each important network as well as some of their principal properties. Then, they are mapped in order to highlight their tendencies.

Wireless networks may be divided into the following:

**Cellular networks**: Cellular networks were originally designed to address voice and/or data transport requirements.

**WLAN networks**: WLAN are generally used as extensions to existing wired infrastructure and provide an interface between wireless clients and base stations or access points.

**Ad hoc Networks**: Each device or node in an ad hoc network is free to move independently in any direction, and will therefore change its links to other devices frequently. Each node must forward traffic unrelated to
its own use, and must therefore serve as a router. Thus, energy is fundamental in this network, predominantly for mobile devices.

**Range and mobility**

Now, we will explicate the various wireless networks according to their range and number of users.

**Body Area Networks** (BANs): These are all networks that communicate between different devices attached to one body. The range is thus in the order of one meter. BANs are subsets of PANs. The standard is IEEE 802.15.4, which is developing according to IEEE, a communication standard optimized for low power devices in operation on, in or around the human body (but not limited to humans) to serve a variety of applications including medical, consumer electronics/personal entertainment and others.

**Personal Area Networks** (PANs): These include networks that achieve distances of up to about ten meters, covering the close environment of a single user. The range is small and thus the number of devices is smaller. The standard is IEEE 802.15.4, charted according to IEEE to investigate a low data rate solution with multi-month to multi-year battery life and very low levels of complexity. It operates in an unlicensed, international frequency band. However, another IEEE standard - P802.15.3 - aims to draft and publish a new standard for higher rates (20Mbit/s or greater) for Wireless Personal Area Networks (WPANs).

**Wireless Local Area Networks** (WLANs, IEEE 802.11x): the range of these networks can be up to a hundred meters. The number of users could be larger but the bit rate per user will decrease, which is why the number by cell will be limited to about 10. Likewise, cordless phones have a range of up to 300 meters and the number of phones connected to one base station is large.

**Cellular Systems** (GSM, UMTS, LTE): these have a range that is larger, varying from a few meters up to a radius of 10km or even 30 km. The bit rate is usually between 9kbit/s and 5 Mbit/s.

**Satellite systems** (Iridium, Thuraya): These provide even larger cell sizes, usually covering many countries and even continents. The cell size is related to the relevant satellite’s orbit, e.g. a geostationary satellite provides a 1000 km radius.

As mobility is a key issue in this field, we have made a division related to mobility:

**Nomadic devices**: These are placed at a specific location for a limited period of time and are then moved to another location. The device is identical to a fixed network for that period and may then be moved to a new environment.

**Low mobility Pedestrian network**: Many communication devices operate at pedestrian speeds. Therefore, the handover is rarely operated.

**High mobility**: These often operate at vehicular speed, from 30 km/h up to about 100 km/h.
**Extremely high mobility**: This relates mainly to high speed trains and airplanes, at speeds up to 1000 km/h.

In addition, the continuing growth in use of IP protocol, such as voice over IP and IPTV, pushes operators to deploy more and more IP and related networks, rather than old switching networks. This emphasizes the rapid convergence between Voice-Data and Mobile-Fix on one hand, and wireless, IP and multimedia networks on the other hand. Furthermore, these trends are enabled by a multitude of wireless technologies operating within the ranges of BAN, PAN, LAN, WAN, Gx, and Satellite. This is a fundamental reason for the spread of mobile and wireless communications -as well as computing- across all possible forms, including intra-, extra- persons and systems. Therefore, this has led to ubiquitous access to a converged mobile wireless infrastructure based on Anywhere, Anytime, Anything, Anyone (AAAA) paradigms. The overlapping of all this convergence is illustrated in Figure 9.

![Figure 9: Road map for next generation mobile cellular network](image-url)
**Wireless networks trends**

![Figure 10: Mapping of wireless networks - mobility and range](image)

In Figure 11, we have recapitulated the range and mobility of the wireless networks. Note that the trends are moving towards global wireless communication.

Some trends in Mobile cellular networks are outlined below:

4G is an integrated wireless solution offering customized personal service and mobile multimedia, anywhere and at any time, with global mobility support [4]. However, 5G will be a complete wireless communication system, integrating all access networks and referred to as Real world wireless. Likewise, the 6G mobile system for global coverage will integrate the fifth generation satellite network. These satellite networks consist of telecommunications satellite networks, earth imaging satellite networks, and navigation satellite networks [5]. From then on, satellite networks will be used from 6G mobile communication systems. The general trend would suggest that the cost of a call will be reduced and lower level users will benefit. In short, mobile cellular networks have thus far provided mass services for anyone and will soon come to dominate all networks. That is the reason why their penetration rate will be the highest.
Figure 10 summarizes the evolution of mobile cellular networks from the second generation towards the next, 5G. The trend is clearly moving towards a completely wireless system.

**Summary**

This section provides outlines of some basic wireless and mobile networking standards such as IEEE 802.11, 802.15.x, and Gx cellular networks. Other standards are not discussed but can be found in reference [97]. The major trends are moving towards complete convergence in wireless systems based on AAAA paradigms as well as satellite networks.

### 2.1.3 Security Technology

One of the most popular engineering success stories of the last few decades is that of the wireless network. Indeed, in addition to the civil and military influence of these technologies, they have impacted on all sectors, including social, financial and scientific.

The recent history of ICT has shown that if the security of any network is not correctly designed from the point of the system’s conception, the consequences
in terms of malicious users’ exploitation of vulnerabilities can cost a lot in terms of both money and reputation. In addition, any system upgrade which may be undertaken in order to reinforce security or to fix flaws could be a very difficult and expensive process. Furthermore, the security of a mobile network is more difficult to achieve, notably because of the potential for exposure of the radio link to attackers, the limited resources and protection of each node, and the highly dynamic, changing topology.

Actually, security requirements really depend on the kind of mission that the network is designed for, in addition to its operating environment. Of course, a military environment is different from a civil one. The same user might want to change the system security requirements of their device (such as a military device) from a low level (in peace time) to a high level (in war time). Conventional security systems were developed without any consideration for this dynamic element. However, modern security systems must have basic dynamical requirements such as self-testing capacities, active assessment etc.

Before discussing the security of wireless networks, however, it is important to have a broad look at security as a whole.

**Security definition**

The Oxford Advanced Learner’s Dictionary contains the following definition of the noun security:

**Protection**

[UNCOUNTABLE] the activities involved in protecting a country, building or person against attack, danger, etc.;

[UNCOUNTABLE + SINGULAR OR PLURAL VERB] the department of a large company or organization that deals with the protection of its buildings, equipment and staff;

[UNCOUNTABLE] protection against something bad that might happen in the future;

**Feeling happy, safe**

[UNCOUNTABLE] the state of feeling happy and safe from danger or worry.

We can see, based on these definitions, that security means safety from attack, danger, worry or from something bad happening. However, in the ICT domain, security is related to information assets, communication infrastructure, and functioning [98].

In answer to the question, “why do we need ICT security?”, the response must simply be “to protect investment - and also life, if we consider the workings of terrorism”. More importantly, if we do not secure ICT, the potential loss could be devastating.
Security requirements cost

There is serious debate - and divergence - among the security community about the definitions of information security terms in the field. ISO, IEC, NIST and ENISA disagree about many of these definitions, such as that of vulnerability. This is why we will choose the clearest definitions in relation to standard organization.

As indicated in the glossary, the following definitions are used:

Vulnerability (ITSEC): The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.

Vulnerability (NIST): Any weakness of the security system that could be unintentionally triggered or intentionally exploited and result in a violation of the system’s security policy.

Threat source (NIST): Either (1) intent and method targeting the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability.

Threat (NIST): The potential for a “threat source” to exploit (intentional) or trigger (accidental) a specific vulnerability.

NIST defines a “threat-source” as the interaction of an actor and motivation, and a “threat” as an interaction between a “threat-source” and a vulnerability.

Figure 12: Risk is a combination of probability, threat and impact
Figure 13: Threat is a combination of Actor, Motivation and Vulnerability

Figure 12 and Figure 13 depict the risk and threat analysis and dependencies.
Risk (ISO): The potential that a given threat will exploit the vulnerabilities of an asset or group of assets and thereby cause harm to the organization. A risk might consist of

- Unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information.
- Non-malicious errors or omissions.
- ICT disruptions due to natural or man-made disasters.
- Failure to exercise due care and diligence in ICT implementation and operation.

Cost

The cost of a security mechanism is determined by two factors: the cost of a failure and the cost of putting countermeasures in place. The more energy spent on appropriate countermeasures, the lower the possibility of loss due to failure. Therefore the total cost of security can be obtained by totaling up these two cost factors. Assuming that greater effort means greater expenditure on countermeasures and smaller subsequent losses due to security breaches, functions that show the cost of countermeasures and the cost of security failures intersect at the level of effort with the optimum cost level, because that is where the total cost is minimal. [8]

In Figure 14, it is shown that the level of security is dependent on the effort required to achieve it. We could prove that the inflexion point is within the optimum couple (security*, effort*). In fact, within this segment it is possible to get more security for little extra effort; but afterwards, any relatively small increase in security takes huge amounts of extra effort.
Related Work and State of the art

Figure 14: Security countermeasures display a decrease in returns related to effort beyond optimum (effort*, security*)

Otherwise, beyond the optimum level (security*, cost*), the cost of implementing extra security countermeasures increases dramatically and the efficiency of the whole security system declines.

In brief, security should be maximized, but relative to the cost that it generates. In addition, the optimum should be exceeded only if the value of the protected assets can justify it. Unfortunately, the optimum is variable and depends on the evolution of the system in its environment. For a system to be optimal or at least suboptimal, it should be controlled at runtime.

**Security goals and security objectives**

ICT security is resource-consuming, which is why it is important to understand the ins and outs of implementing a large-scale security system.

The goal of security as stated by NIST recommendations:

The goal of information technology security is to enable an organization to meet all of its mission/business objectives by implementing systems with due care and consideration of IT-related risks to the organization, its partners and customers.

Security goals can be achieved through due consideration of security requirements and polices. [9]

A taxonomy of security requirements is thoroughly described in reference [10].
Figure 14 illustrates a taxonomy of security related requirements. The two sets of 4 subtypes of security requirements in the upper right part of the figure combine to produce 16 different types of pure security requirements. The 5 different types of non-security requirements along the upper left side of the

Figure 15: A Taxonomy of Security-Related Requirements

Figure 14 illustrates a taxonomy of security related requirements. The two sets of 4 subtypes of security requirements in the upper right part of the figure combine to produce 16 different types of pure security requirements. The 5 different types of non-security requirements along the upper left side of the
figure with a security integrity level (SIL) from 1 to 5 are part of security-significant requirements.

The security system requirements in the lower right part of the figure are those system requirements that are allocated to security subsystems. Finally, the security constraints are shown on the right side of the figure as a subtype of ordinary constraints; in fact, these are typically mandated security policies or countermeasures, such as mandates for specific approaches to ensure security requirements are met or requirements for specific configuration levels when using a countermeasure.

It is possible to find different classifications of security requirements, among them one from NIST that covers all the security issues, and then groups them properly. These are explored in the next paragraphs [7].

**Availability**: assures that the system works properly and that services are available or not denied to authorized users.

**Integrity**: comprises two aspects relevant to ICT – data integrity and system integrity.

**Confidentiality**: confidentiality of data or system information means that only the intended users receive information; that this information is not disclosed to any unauthorized individual. The confidentiality principle applies to data in storage, processing, and in transmission.

**Accountability**: the requirement that the actions of an entity must be uniquely traceable to that entity. This requirement has become more and more important as businesses have become increasingly dependent on IT. Accountability is of great significance for issues like non-repudiation, fault isolation, intrusion detection and prevention, after-action recovery and legal action.

**Assurance**: a requirement to show that security measures have been properly implemented and work as intended. In the course of an implementation, if the functionality has been correctly implemented, sufficient protection has been provided against unintentional errors and sufficient resistance to intentional penetration is present, then the objectives can be considered to be adequately met.
Conclusions and Future Work

Figure 16: Security model

The five security objectives described above are interrelated and interdependent. It is not possible to achieve one without considering the others. They are referred to as ‘first level security’ and are shown in Figure 16, which gives a good overview of security and security services.

The five security objectives are not enough for dynamic security network. Other definitions are introduced in this text.

**Cryptographic key management:** Cryptographic keys must be securely managed when cryptographic functions are implemented in various other services.

**Security administration:** The security features of the system need to be administered in order to meet the needs of a specific installation and to account for changes in the operational environment.

**System protections:** Underlying the various security functional capabilities is a base of confidence in the technical implementation. This represents the quality of the implementation from both the perspective of the design processes used and the manner in which the implementation was accomplished.

**Authorization:** The authorization service enables specification and subsequent management of the allowed actions for a given system.
Tolerance [99]: The tolerance is the process of masking runtime failures of a system by eliminating faulty components, limiting the fault effect, and allocating valid substitutes.

Freshness [11]: Data freshness ensures that the data is recent and that no old messages have been replayed in order to protect data aggregation schemes against replay attacks.

Attacks could be fabricated by replaying correct information, or by flooding the nodes within the network in order to block the entire network or parts thereof. Thus the freshness of information is also a requirement within highly dynamic networks, such as WSN.

Survivability: for a system, this is the capacity to fulfill its mission in a timely manner, in the presence of intrusions, attacks, accidents and failures [12, 13].

For WSN security, the network should satisfy confidentiality, integrity and availability requirements. However, these requirements are not always possible due to the fact that these networks are deployed in hostile environments, and sensor nodes have to supply their objective even though they may be under attack. For example, Selfish nodes utilize the network on one hand, but do not cooperate on the other hand, so as to protect their own interest, and save battery life for their own communications. In fact, they do not intend to damage other nodes directly. On the other hand, malicious nodes aim to damage other nodes, for example, by causing network congestion when saving battery life is not a priority. That is why survivability has been introduced to deal with these problems.

2.2 State of the art

The concept of adaptation security in wireless networks is used to mitigate the consequences of a substantial number of runtime threats when it does not completely eliminate them.

Many systems which are rated at the higher levels of data security are implemented according to the reference monitor concept. First introduced by James Anderson [1], the reference monitor is a concept that has proven to be a useful tool for computer security experts. It is the only effective tool known for describing the abstract requirements of secure system design and implementation.
Conclusions and Future Work

Figure 17: Reference Monitor model.

Figure 17 describes the principal elements of the reference monitor model. Unfortunately, it does not have the ability to adapt its behavior because it is deterministic, like all static security systems. Therefore, a new paradigm must be developed in order to deal with dynamic attacks, such as those from selfish or malicious nodes.

In [14], Ganz introduced a form of security broker architecture for WLANs. This framework uses security services to execute the security requirements specified by the user and maintain the available network performance as well as ensuring the performance of security routines.

Reference [15] has also proposed an adaptive security application in mobile ad-hoc networks, where network conditions play a role in choosing the relevant runtime security mechanisms.

Chigan et al. [16] report that highly secure mechanisms often inevitably consume large amounts of system resources, which may unintentionally lead to a security attack. Consequently, a suitable security service is provisioned in a progressive way in order to achieve the maximum overall security services, balanced against network-performance services throughout the course of WLAN and Sensor network operation.

In article [17], Niedermayer et al. explicit that the performance of the security services has an important influence on the QoS of the communication, which leads to the question of the performance impact of security protocols. A number of frameworks base their choices of security services on performance values and security ratings. The term Quality of Security Service (QoSS) is introduced and represents the dependency that exists between security algorithms and quality of service values.

Saxena published in [18] an article on the adaptation of security mechanisms
within WLANs. The required security level is directly dependent on the trustworthiness of the environment, but also on how hostile one might expect the environment to become. The article argues that excess processing and transmission resources are wasted in mobile environments if security is over-provisioned. Therefore, the trade-off between security and performance looms large over the choice of security services.

Adaptive security mechanisms can also be found in flexible protocol stacks for wireless networks [19], context-aware access control systems [20] and security architectures [21]. This has prompted a new strategy- the implementation of a completely reconfigurable architecture [21], which is fundamental for the adaptation of architecture to the terminal and network variability of the context, particularly in the security field [22].

Individual sensor nodes in a WSN have inherent limitations in terms of resources, which make designing security procedures more complicated. Each of these limitations is due in part to the two greatest constraints: limited energy and physical size [23].

Security in sensor networks is complicated by the constrained capabilities of sensor node hardware and the properties of the deployment [24, 25, 26].

All aspects of wireless sensor networks are being examined, including secure and efficient routing [27, 28, 29, 30], data aggregation [31, 32, 33, 34], group formation [35, 36] and so on. Although some existing architectures for WSN can be seen to partially solve these problems, it is still possible to pinpoint neglected aspects that can be considered crucial for the creation of a satisfactory security system.

Chigan et al. [17] have proposed an approach to increase the availability of WSNs, but they need additional hardware, which would generate more cost. Until now, only a few approaches have been available, and more studies in these areas are needed.

The literature has also reported on the interaction between QoS and security. Certain articles have studied the impact of security on QoS in WLAN. For example, in [38] Liang and Wan examine the influence of security on overall system performance in terms of authentication, latency and call dropping probability.

Shen and Thomas [39] have stated that QoS and security have been considered separately, but that they have many impacts on each other. Therefore, they propose a model for a distributed dynamic management system, which aims to maximize QoS and/or security while maintaining a minimum user-acceptable level of QoS and/or security even when the network resource availability changes.

Stefan et al. in [40] investigate how security can be treated as yet another QoS parameter through the use of tunable security services. Users can specify a tradeoff between security and performance through the choice of available security configuration(s).

Other security issues include [23] security-energy assessment, data assurance,
survivability, Trust, end-to-end security, security and privacy support for Data Centric Sensor networks (DCS) and node compromise distribution. It's very important to study these areas because of the special characteristics of the sensor network, such as battery limitation, high failure probability nodes, more easily compromised nodes, unreliable transmission media, etc.

### 2.2.1 Autonomous systems

In 2001, IBM [2] introduced the concept of autonomic computing, taking inspiration from the autonomic nervous system, which manages the most complex functions of our body without our conscious coordination. IBM proposed that complex systems should deal with their managing functions in the same way. Thus IBM suggested autonomic properties for the management of regular maintenance and optimization tasks so as to reduce the need for administrative intervention. IBM has also attributed the main properties of the autonomic system based on self-management to self-configuration, self-optimization, self-healing and self-protection. Kephart and Chess give brief description, taken from Ref. [63, 64], which is explicated in Table 1.

**Table 1: Four aspects of self-management as they are now and as they would be with autonomic computing**

<table>
<thead>
<tr>
<th>Concept</th>
<th>Current computing</th>
<th>Autonomic Computing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-configuration</td>
<td>Installation, configuration, and integration of the system are time consuming and error-prone</td>
<td>Automated configuration of components and systems follows high-level policies. The rest of the system adjusts automatically and efficiently.</td>
</tr>
<tr>
<td>Self-optimization</td>
<td>Systems have hundreds of manually set, nonlinear tuning parameters, and their numbers increase with each release</td>
<td>Components and systems continually seek opportunities to improve their own performance and efficiency</td>
</tr>
<tr>
<td>Self-healing</td>
<td>Problem determination in large, complex systems can take a team of programmers weeks</td>
<td>Automatic system detection, diagnosis, and repair of localized software and hardware problems</td>
</tr>
<tr>
<td>Self-protection</td>
<td>Manual detection of and recovery from attacks and cascading failures</td>
<td>Automatic system defense against malicious attacks or cascading failures. Use of early warnings to anticipate and prevent system wide failures</td>
</tr>
</tbody>
</table>

The autonomic paradigm is an emerging discipline and has yielded many interesting results. Among others factors, there are still many research challenges in bringing it to realization for many fields [64]. In addition, the
concept is still under discussion [65].

The aim of the notion of the autonomic system is to improve a system to the extent that it becomes autonomous, with a simultaneous aim to minimize the need for human intervention. The first use of the term in relation to computing was in describing a self-managing system [63]. Nevertheless, the concept itself is not new. In fact, it was previously used in a self-managing military project initiated by DARPA in 1997. The major objective of this project was to create personal communication and location devices for soldiers on the battlefield. The devices needed to be able to communicate in hostile environments and to collect data from unattended ground sensors and so on, and to transmit this data autonomously to all participants concerned. At the same time, the potential for enemy interception of this information had to be minimized [66].

Many other DARPA projects have been based on, among other things, self-regenerative systems [67]. In addition, in 2005 NASA launched an interesting project called Autonomous NanoTechnology Swarm, which was to deal with ensuring that craft that survived after entering the asteroid belt would be capable of working.

In the field of video streaming, there are projects based on Self-Adaptive systems which ensure the QoS of video or audio in the absence of bandwidth fluctuations. However, the autonomic community does not identify them as autonomic if the system is based on only one of the Self-x proprieties [68].

This is why IBM has proposed a reference model for autonomic control loops [62] to identify an autonomic system. This loop is called MAPE-K (Management, Analyze, Plan, Execute, Knowledge) autonomic loop, which is likely inspired by the generic agent model proposed by Russel in 2003 [69]. Figure 18 illustrates the principal of MAPE-K for autonomous elements. Moreover, the autonomic system is also inspired by natural biological systems, which are nondeterministic but scalable and robust at a high level, while at a lower level their behavior and context are unpredictable. This is the case of both cellular systems and insect colonies [70].
Conclusions and Future Work

The autonomic system was exploited in many other fields, such as security, adaptation, and routing. For example, J-M Seigneur [95] has introduced autonomic security patterns in his security design - but only at the authentication level.

In this respect, the autonomic paradigm can be exploited perfectly within SON networks. In fact, in these networks, the dynamism and unpredictable changeability need a high-level, self-managing system. The key issue in the case of WSN is that sensing and processing are cheap, but communication is costly. That is why sensors are battery driven and the major issue lies in controlling the wireless interface. The node in WSN follows the same autonomic model as the MAPE-K loop [71, 72]. Another approach is to embed the autonomic qualities into the OS of the nodes. Accordingly, this would provide self-management at the lowest level of the stack. This is the trend of self management in ad hoc sensor networking [73]. Routing is one of the main issues in WSN. One of the more autonomic routing techniques consists of electing cluster heads dynamically, depending on availability, or spreading the packets fairly across all nodes, depending on battery power and consumption [74].

Autonomic Communication is the field where self-management and self-optimization can be seen to fit absolutely. These capabilities can be provided in a timely fashion if we investigate the context aware approach. Indeed, to improve the overall performance of the network, the system concerned must be autonomic and context aware. The typical context involves mobility services, location, identity, ad hoc communication, and adaptation of QoS changes depending on mobility and services [75]. Indeed, to be classified as having self-adaptive behavior, an autonomic system must be able to interpret its behavior as

![Figure 18: MAPE-K: Autonomous element](image-url)
well as its context and generate feedback as a result [76].

In this respect, the number of sophisticated network attacks is increasing exponentially, and these are launched with great frequency. In addition, they are becoming riskier as regards overall system security due to the extreme complexity of their asynchronous behavior, which could potentially lead to catastrophic results. Therefore, the conventional security measures and techniques are not capable of dealing with them, because they attack largely interconnected and interdependent complex systems [77]. This is why many research challenges could be solved thanks to autonomic systems. In fact, self-healing and self-stabilizing systems have inherently secure architectures in term of survivability (i.e., one of the security requirements of WSN).

Moreover, multilateral communication happens among self managing partners in autonomic networks; this is why there is a pressing need for suitable models to maintain trust between them. Therefore, trust is an important aspect for making decisions concerning the security of networks, particularly in relation to highly dynamic networks such as SON. Trust management is an approach to managing distributed networks through a combination of policies and logical deduction. This is why the highly dynamic nature of the autonomic system requires novel dynamic trust management models in order to establish trust relationships and manage access. [78]

A number of frameworks have been developed for designing trust management systems. These mainly focus on different aspects of trust by adopting different notions of trust relationships and thus implementing different mechanisms for propagating trust and deducing new security statements.

In the next section, we will introduce trust and reputation work, discuss both concepts, and explore their application to security in SON networks.

2.2.2 Trust and reputation

Security and trust

Josang describes trust in security systems in Ref. [61]. He was really the first to attribute the notion of ‘soft security’ to trust and reputation systems. Security in general is provided by tools and mechanisms which protect a system against malicious parties. Indeed, conventional security mechanisms typically protect resources from malicious users by restricting access to allow authorized users only. However, in many situations, we have to protect the system from those who offer resources if they act fraudulently by providing false or corrupted information. In such cases, conventional security mechanisms are unable to protect against these attacks. In Ref. [60], Raya and al. introduce hard security for conventional security mechanisms, such as those for authentication and privacy, as opposed to soft security measures for trust and reputation systems.
ICT trust

Computer security trust is the assurance level relating to high risk concerning current interactions in highly sensitive applications. It ensures that the data and the system are protected from being adversely affected by malicious and non-authorized parties.

Figure 19 depicts the three layers of the security approach to achieving economic and social prosperity for ICT services.

Communication security includes encryption of channels and so on. Authentication provides identity trust for identity claims over a communication channel. To verify an identity via a communication channel, a Certificate Authority (CA) is needed. In fact, a CA is also called a “trust provider”, and is used to authenticate the service provider and to support all security mechanisms for managing identities.

Actually, reputation is a context-dependent quality. For example, an engineer might have a good technical reputation and a bad social reputation. Seigneur in [95] proposed a formal model of context-dependent reputation. Some reputation systems provide one reputation rating per transaction, which may help mitigate fraud.

Trust and privacy

In [81], Seigneur addressed the inherent conflict between trust and privacy in interacting environments and proposed a method to achieve a balanced trade-off between trust and privacy by ensuring minimal trade of privacy for the required level of trust. Moreover, he surveyed in article [82] different means of
identifying individuals’ virtual identities and showed how to transfer them into his trust engines based on adaptability, security, usability and privacy.

Moreover, in article [83], Wei et al. have used pseudonyms to achieve identity privacy and anonymity in the virtual computing environment. They have showed the positive results of their approach through simulations.

**Reputation topology**

Reputation can be viewed as a global or a personalized quantity. Many reputation systems rely on global reputation. In the case of Amazon or eBay, reputation is based on the cumulative ratings of users by others. In fact, in this case reputation is referred to as individual reputation.

For the case of personalized reputation, Zacharia and Maes studied this subject in depth in 1999 [84]. In Ref. [80], Mui argues that an agent is likely to have a different reputation in the eyes of others, relative to their reputation in an embedded social network. In the same text, we find a reputation topology very useful to the understanding of the notion of reputation and its relationship with social network. Besides, it is assumed that reputation is context dependent. This topology is illustrated in Figure 20.

![Figure 20: Reputation topology](image-url)

At the top level of reputation, we can describe reputation as related to an agent (individual) or a group of agents (individuals). The majority of reputation systems focus on the reputations of individuals. This would be the case for eBay, Amazon and others [85]. Beyond this, individual reputations can be divided into facts based on direct observations and inferences based on information collected indirectly (second-hand evidence).

Afterwards, reputation is also divided into directly observed reputation [86] and reputation derived from direct observation [87].
For indirect reputation, prior beliefs about strangers can be used specifically to affect value to new agents [84]. Then, a group-derived reputation can be extended to provide prior reputation estimates for agents. In the [88] article Sabater and Sierra have postulated different ways of mapping the link between the initial individual reputation of a stranger and the group from which he/she comes. Ultimately, the evaluating agent can only estimate the stranger’s reputation based on information garnered from others within the environment [89].

**Trust Management**

Blaze et al. [90] were almost first to propose the notion of trust management in the field of security. This was defined as a tool with which to specify and interpret security policies and relationships in order to authorize critical security actions. Indeed, they divided security into two themes: System Security and trust management. The latter allows certain keys to take certain actions when presenting security credentials without verification of the identity of the user whose credentials they are. This approach was implemented in the PolicyMaker software, and later in KEyNote.

Moreover, the small world principle, when applied to social networks and peer-to-peer computing [91], enables paths from a source node to a destination node to be found efficiently. Based on this, Zhu et al. [92] engaged in a practical approach to compute trust in wireless networks based on graph and computed trust values.

In this respect, a security solution to enable effective security decisions to be made relating to data protection, secure routing and other network activities based on trust evaluation is proposed in reference [93] by Cubaleska et al.

<table>
<thead>
<tr>
<th></th>
<th>Specific</th>
<th>General, Synthesized</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Subjective</strong></td>
<td>Survey Questionnaires</td>
<td>eBay, voting</td>
</tr>
<tr>
<td><strong>Objective</strong></td>
<td>Technical Product tests</td>
<td>Synthesized general scores from product tests</td>
</tr>
</tbody>
</table>

**Trust and Reputation related work**

Mui has proposed a computation rating model based on reciprocity, trust and reputation [80]. He has studied the relative strengths of different notions of reputation in depth, and has proposed relevant computation models.

Josang [61] has explained different models and notions of trust and reputation in great detail. He has proposed his own approach called ‘metrics belief models’ based on the belief theory framework which is related to probability theory, but the total probability - which is the sum of probabilities of all events - is not necessarily 1, but is in fact less than that, and the remainder is affected in uncertain ways.
In [93], Cubaleska and Schneider propose a method to identify malicious hosts in order to build a policy. In [94], Liang and Shi present a personalized conception of trust for building cooperation in P2P networks. They define long term reputation and provide a short risk evaluation and base their performance criteria on sensitivity, hit ratio, effectiveness, and applicability in a P2P shared web server. They also build a trust based routing framework based on a combination of adaptive Trust and an economic approach.

Wireless, SON and mobile networks are becoming very complex and thus their security is also becoming a difficult, complicated issue [41]. While self-x systems are considered to be one of the major features of SON, these properties do not come naturally, and need to be enforced. The entire chain of a SON system must be capable of coping with variable conditions, fault nodes and malicious entities. In addition, attacks must be considered and treated during runtime. According to Srinivasan et al [43], trust can solve some problems that are beyond the power of traditional cryptographic security measures. The authors argue that trust management is the key to building trustworthy and reliable WSN. Indeed, a Trust Management system is one of the most adequate approaches that can be used to enforce the security mechanisms in wireless networks, and particularly in SON networks.

**SON security: trust and reputation**

Trust and reputation have been formally studied for more than a decade in order to establish the ways in which they can affect decision making abilities in uncertain conditions [42]. It is only recently that they have been adapted within wireless networks. The importance of reputation- and trust- based systems in Self-organizing wireless networks has been recognized in many articles [42, 43]. In these articles, the authors have proposed the goals of trust and reputation systems. Their essential properties have also been identified, such as those illustrated in Figure 21.

<table>
<thead>
<tr>
<th>Capable of coping with any kind of misbehavior</th>
<th>Encourage nodes to cooperate and become trustworthy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimize the impact of any insider attack</td>
<td>Provide information to allow nodes to discriminate between trustworthy and untrustworthy nodes</td>
</tr>
<tr>
<td></td>
<td>Discourage untrustworthy nodes from participate to any activity.</td>
</tr>
</tbody>
</table>

**Figure 21 : Goals of trust and reputation systems for SONs**

In SON, the trust system must also have three other characteristics:

i. A relation to long living entities

ii. The capacity to capture and distribute feedback about cooperation and to assure its availability in the future
iii. The use of feedback for trust

The use of reputation and trust systems in internet, e-commerce and P2P networks has proven their efficiency and usability, whereas in the field of SON they are novice applications - but have nonetheless had some good results. We will provide some related works in this field.

Rasmusson and Jansson [44] have shown the influence of the migration of an agent within a network. In fact, an agent can often move faster than any negative information pertaining to his behavior. Furthermore, Grandison and Sloman in [45] have discussed the notion of a node behaving well or badly in a network at great length. They conclude that a global judgment would be inaccurate due to the dynamism of the network, even though a centralized authority exists within the network. Consequently, every node should have its own notion of what constitutes a bad and a good node. This is an old and established problem in the field of agents, and is known as “logical omniscience” [46].

In Ref. [47], Mejia et al. establish a good survey of trust models in mobile ad hoc networks. Indeed, it provides a nomenclature and gives an excellent comparison of trust models.

Pirzada and McDonald [48] have proposed an approach to implement trust relationships in ad hoc networks. The trust in this scenario is based on a combination of weighted values which are attributed to all observed receiving and forwarding activities of a node. The compound trust values are used as a link when defining routes based on the shortest path routing algorithm. This allows the most trustworthy paths within a network to be discerned.

In article [49], Yan et al. have presented trust as a measure of uncertainty. Their trust model is based on entropy and probability capable of solving concatenation and multipath trust propagation in MANET.

Yan and al. have proposed a trust framework which offers a security solution mainly to ensure data protection and secure routing in ad hoc networks [50]. Their model is based on logical and computational trust and utilizes factors such as neighbors’ recommendations, experience, statistics, IDS, etc.

Article [51] contains a survey of the trust related to MANET routing protocols. The authors stress the difficulties in detecting security flaws due to the dynamic changing infrastructure and the degree of mobility in MANET. Then, they conclude that trust is a key for the establishment of secure routing protocols.

Jarrett and Ward in [52] have proposed a trusted routing schema that extends AODV routing protocol to exclude any untrustworthy nodes from participating in routing. Their proposal is trust computing AODV, referred to as TCAODV. It prevents malicious and selfish nodes from misusing resources. It is based on public cryptography and a trusted root.

Other models propose trust management systems, such as the Davis trust management scheme, which is based on a structured hierarchical model and addresses the revocation of certificates [53]. The model is robust due to the use of digital certificates to establish trust. In order to be trusted, a node must have a
Related Work and State of the art

valid certificate.

In article [54], Momoni et al. survey the state of the art of trust-based systems in WSN and highlight the differences between WSN and MANET as conventional ad hoc networks. Next, they gather together different trust definitions and characteristics. They extend the definition of trust to include a data trust component, as well as reliability, and then propose a model that it is expected to guarantee robustness.

In article [55], Singh et al. stressed the importance of trust management for security in MANET and proposed an algorithm to satisfy security requirements.

Michiardi and Molva [56] have proposed the CORE (which stands for COllaboration REputation) mechanism to enforce cooperation among nodes. CORE differentiates between observations of subjective reputation, indirect reputation and functional reputation. All of them are weighted in order to arrive at a combined reputation value, which forms the foundation of the decision as to whether to collaborate with a node or be isolated from it gradually. CORE is based on community nodes that have to collaborate continually; otherwise their reputation diminishes gradually, to the point of exclusion.

As a matter of fact, CORE is a distributed reputation system which uses first- and second-hand information to update reputation, which is quantified as being between minus one and plus one (–1 and +1). It uses Dynamic Source Routing (DSR) protocol for routing over a bi-directional symmetrical communication.

CONFIDENT [57] is another security reputation system which was proposed by Buchegger and Le Boudec in order to discard misbehavior in MANET on the bases of altruism and utilitarianism. It uses DSR routing protocol as well as first- and second-hand information to evaluate reputation. Indeed, CONFIDENT uses instant reciprocal altruism to encourage collaboration because it forces nodes to behave well without any delay. Unfortunately, the system is vulnerable to false accusations of attacks by malicious nodes because only negative information is exchanged between nodes. Furthermore, nodes which have been excluded for misbehavior are allowed to be readmitted to the system after a certain amount of time. Therefore, they have the potential to attack repeatedly unless the temporary exclusion is extended.

OCEAN is an extension of DSR protocol which was proposed by Bansal and Baker [58] and is based on monitoring and reputation systems whereby nodes rely only on their own observations. The reputation of neighbors is updated depending on their actions and whenever the value goes below a certain threshold, that particular node is added to a faulty list. A timeout is used to allow faulty nodes to reenter the network if they have been wrongfully excluded.

An amelioration of CONFIDENT which is proposed by the same authors is called the Robust Reputation System (RRS) and is based on the Bayesian framework with Beta distribution for updating reputation. Every node has two metrics - trust and reputation. Trust discriminates between trustworthy and untrustworthy nodes, whereas reputation discriminates between normal and abnormal nodes. Unlike CORE and OCEAN, RSS gives greater weight to current behavior as it exchanges only fresh information. In fact, this choice forces the malicious nodes
Conclusions and Future Work

A Reputation-based Framework for Sensor Networks (RFSN) has been proposed by Ganeriwal and Srivastava [59]. This is a distributed reputation framework for high integrity sensor networks based on the classification of nodes as cooperative or non-cooperative and on first- and second-hand information. It uses Beta-pdf for reputation representation, updates and integration, as well as watchdog mechanisms, which are combined to compute a trust value. Based on a comparison between this value and a particular threshold, the observed node’s cooperation or lack thereof is decided.

Srinivasan et al. [43] have proposed a distributed security system called a Distributed Reputation-based Beacon Trust System (DRBTS) that models a WSN as an undirected graph and makes use of both first- and second-hand information. It presents a set of techniques to detect and remove malicious nodes that are misleading about their location. In fact, the nodes are divided to BSs and SNs: nodes within the first group monitor each other and provide information to nodes in the other (SNs) group, which can then decide whether or not to trust based on voting mechanisms. Unfortunately, this system only resolves the problem of beacon nodes’ misbehavior. However, it could easily be extended to other problems.

Table 3 compares various trust and reputation mechanisms issued in wireless Self-Organizing Networks.

Trust and revocation have been studied by Raya et al. [60]. They present data-centric trust in ephemeral ad hoc networks in general, and discuss VANETs as a case study. Also in reference [37], Raya et al. present local revocation in a game theoretic model instead of alternative reputation. Finally, they derive optimal parameters.

### 2.2.3 Synthesis and open problems

Research in the field of reputation and trust based systems for SONs is still in the incubation phase. There are many open issues in the field.

Trust modeling is really complicated due to the uncertainty that might be dealt with based on probability theory. So far, there has not been a complete probabilistic answer to the problem. In addition, a reliable and robust framework for SONs has not yet been completely solved. The trend in WSN is to propose a simple and efficient model for an energy consuming problem when integrating trust in nodes.
<table>
<thead>
<tr>
<th>Characteristics</th>
<th>CONFIDENT</th>
<th>CORE</th>
<th>RFSN</th>
<th>DRBTS</th>
<th>OCEAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architecture</td>
<td>Distributed</td>
<td></td>
<td></td>
<td></td>
<td>Standalone</td>
</tr>
<tr>
<td>Type of data collection</td>
<td>Reputation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data distribution</td>
<td>Negative to friends</td>
<td>Positive from RREP</td>
<td>Yes</td>
<td>BN to SN SN to SN</td>
<td>No</td>
</tr>
<tr>
<td>Misbehavior detection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Selfish routing</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Malicious routing</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### 2.3 Conclusion and Summary

In this chapter, we presented an overview of mobile and wireless networks, as well as the trends within these spheres. An overview was also given of definitions relating to the security field. We then described the state of the art related to adaptive security for highly dynamic networks. Finally, we emphasized two major paradigms which are applied to SONs (trust and reputation, and the autonomic system) due to their strong link to adaptation and security. Now that we have a complete sense of both the background and the state of the art, we can proceed to state the problem and the methodology of approach.
2.4 REFERENCES


4. S. Akhtar, “2G-5G Networks: Evolution of Technologies, Standards, and Deployment”, Information Technology Department, Clayton State University


Advances in mobile Communication networks, Computer Communications, Vol. 23, issued 5-6, March 2000


Conclusions and Future Work

91. A. Oram. “Peer-to-Peer: Harnessing the Power or Disruptive Technologies”, O'Reilly & associates, March 2001
98. P. Lamsal, “Understanding Trust and Security”, Department of Computer Science, University of Helsinki, Finland 2001
Chapter 3. Problem Statement and Methodology

“A problem is half-solved if properly stated”
- John Dewey

This chapter discusses the problem addressed in this research and the methodology used to address it. Firstly, Section 3.1 gives an overview of the problem statement and in section 3.2 the scope of this research is outlined. Then, section 3.3 provides an exhaustive classification of attacks in SON networks. In section 3.4, the problem formulation is detailed. Thereafter, in section 3.5 the methodology of the approach is described, and all the trust and reputation background information used in the thesis is examined. Finally, section 3.6 contains a conclusion and summary.

3.1 Problem statement overview

In this dissertation, we present a solution to deal with the security requirements of highly dynamic networks, such as self-organizing networks (SONs: MANET, VANET, MWSN, WSN, and WMN). These networks present conflicting minimum security requirements. To meet all of these requirements, the system must be able to balance many variables. Taking security considerations into account early on in the system’s design and maintaining this awareness during each stage of development is surely a way to avoid many risks. In addition, any minimum change should push people to rethink the whole security system, from the beginning. This is why a well-designed security framework will provide a structure and guidelines for all security system designers to enable them to handle security issues properly early on, without having to introduce safeguards for different security vulnerabilities during the project. The difficulty in designing and developing a universal security system is evident in this field. Indeed, every complex system is particular and needs a special and individualized approach. Adaptive security systems are a key issue in this field; it is necessary to develop an efficient solution for dynamic environments without complex mathematical or physical modeling. The only difficulty is the complexity involved in implementing such adaptive security systems - mainly in highly dynamic networks such as SONs - because we must have solid knowledge of the environments, security objectives and requirements, as well as trends. This is why the fundamental security objectives and requirements will be outlined in the next section.

3.2 Self-Organizing Networks

3.2.1 Introduction to the security of highly dynamic networks

SONs are boosted by the growing number of devices that are coming into existence each day in different fields of life. In addition, the extent of their interaction and mobility and so on is turning communication itself into a highly complex system. Accordingly, we are moving towards the omnipresence of mobile ICT. The IoT is the major trend and progress in ubiquitous system field.
Almost all devices now support multiple channel communication, with this being mainly wireless, such as through Bluetooth, Zigbee, WiFi or WiMax, or infrared. Even if a device is not connected to the internet, one of its network’s nodes or a device in its vicinity is, for example a Bluetooth headset connected to a phone. Thus, eavesdropping is ordinary and normal, and so security is jeopardized if any conventional form of attack is launched, such as a man-in-the-middle, worm, virus, denial of service, etc. This is why all conventional counterattacks occur on behalf of security engineers. However, there are also many constraints which add to the difficulties of these attacks - among others, the heterogeneity of requirements, energy consumption, low CPU capacity and small memory. Therefore, the traditional counterattacks have become obsolete. Moreover, new attacks are challenging security, on one hand due to the nature of these new networks and the dynamic quality of mobile ad-hoc networks (MANET), and on the other hand due to the non-technical background of the majority of users. In this last case, conventional security is compromising usability.

These challenges are pushing researchers to review all of these networks in order to explain and clarify their characteristics, constraints and security requirements, as well as the forms of attack that they could potentially encounter.

In the next section, we provide summarized descriptions of the principle emerging self-organizing networks, as well as of relevant security issues and counterattacks. Four of the most common types of SON networks will be addressed: Mobile Ad-hoc NETworks (MANET), (Mobile) Wireless Sensor Networks ((M)WSN), Wireless Mesh Networks (WMN) and Vehicular Ad hoc NETworks (VANET).

Anyway, the high level security goals are not so different from other networks: most typically, they concern authentication, confidentiality, integrity, availability, and non repudiation (definitions of all of these notions are provided on page 19), but these requirements can change from one state to another (normal state, critical state, etc.) and from one context to another (with this being mainly the case for military networks).

3.2.2 MANET

Objective of MANETs

The goal of MANET is to provide a flexible way of developing ubiquitous wireless broadband access, allowing a mobile network to be deployed without any prior infrastructure [1].

An ad hoc network is a collection of nodes or terminals capable of

i. communicating autonomously between each other;

ii. forming a multi-hop radio network; and

iii. maintaining connectivity in a decentralized manner.

Each node has the potential advantage of being a host and/or a router. More critically, the network topology is dynamic. In fact, the degree of connectivity
Conclusions and Future Work

between the nodes may vary over time due to node departures, new node arrivals, and the possibility of having mobile nodes.

**MANET security requirements**

The MANET security requirements as described in reference [2] (Book of Levente Buttyán) consist of:

i. Confidentiality
ii. Integrity
iii. Non-repudiation
iv. Authentication
v. Access control
vi. Privacy

3.2.3 VANET

**Objectives of VANETs**

The goal of the deployment of a VANET is to enhance the safety and efficiency of a transport system. Reference [3] (Book of Al-Sakib Khan Pathan) has listed some prominent services which can be provided through VANET:

i. Traffic updates: drivers can access real-time, precise information about traffic in order to make correct decisions in avoiding congestion
ii. Route suggestion: comparative analysis to suggest different routes to destination
iii. Emergency warning signals: propagation of warnings to inform if the car ahead suddenly brakes
iv. Commercial purpose: road side shops might advertise to drivers
v. Environmental warning signals: warnings concerning environmental hazards (e.g. ice on the road)

**VANET security requirements**

The basic requirements are discussed in reference [2] (Book of Levente Buttyán). The major security requirements in VANET are:

i. Authentication
ii. Message integrity
iii. Message non-repudiation
iv. Entity authentication
v. Access control
vi. Message confidentiality
vii. Privacy
viii. Availability
ix. Real-time guarantees

3.2.4 WSN

Objectives of WSN
A WSN [4] is a wireless network composed of elements which are able to make measurements, elaborate upon them and send them to a sink point. This must be done within a dynamic network, using limited energy and at a large scale, even in instances where communications problems or hostile environmental conditions are present, in order to:

i. reduce cost
ii. ensure event detection
iii. guarantee network connectivity
iv. maximize the lifetime of the network

WSN security requirements
WSN security requirements relate to:

i. Data confidentiality
ii. Data Authentication
iii. Data Integrity
iv. Data Freshness
v. Availability (ensuring that services offered by a whole WSN or by a single sensor node must be available whenever they are required)

3.2.5 Synthesis

WLAN
The IEEE 802.11 standards define a wireless local area network. IEEE 802.11 specifies both physical and media access control layers. These networks are generally used as extensions to wired networks through base stations; however, wireless access has introduced security issues. Many threats and vulnerabilities are specific to this type of network and are addressed by Pradip et al. in Ref. [5].

A WLAN hotspot is a variant of indoor WLANs. These networks are usually dynamically configured in order to manage mobile users. Table 4 shows the parameters of a WLAN network.
### Conclusions and Future Work

### Table 4: WLAN principal parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Energy Requirement</strong></td>
<td>Low, high or supplied</td>
</tr>
<tr>
<td><strong>Network size</strong></td>
<td>Small to large</td>
</tr>
<tr>
<td><strong>Node Range</strong></td>
<td>Medium - up to hundreds of meters</td>
</tr>
<tr>
<td><strong>Link data rate</strong></td>
<td>Up to 300 Mbit/s</td>
</tr>
<tr>
<td><strong>Network Configuration</strong></td>
<td>Static (generally)</td>
</tr>
<tr>
<td><strong>Session length</strong></td>
<td>Minutes to hours</td>
</tr>
<tr>
<td><strong>QoS</strong></td>
<td>None</td>
</tr>
</tbody>
</table>

### MANET

A MANET is an autonomous system that is self-organizing so as to overcome its lack of infrastructure. Any communication between two nodes is accomplished via intermediate nodes that act as routers. MANETs, however, are deployed with the purpose of allowing communication between nodes on the move. The mobility of the nodes makes the topology dynamic. This network might be connected to a backbone network via gateways [6].

### Table 5: MANET principal parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Energy Requirement</strong></td>
<td>High</td>
</tr>
<tr>
<td><strong>Network size</strong></td>
<td>Small to medium</td>
</tr>
<tr>
<td><strong>Node Range</strong></td>
<td>Short - 1 to 10 meters</td>
</tr>
<tr>
<td><strong>Link data rate</strong></td>
<td>Less than 11 Mbit/s</td>
</tr>
<tr>
<td><strong>Network Configuration</strong></td>
<td>Static or Dynamic</td>
</tr>
<tr>
<td><strong>Session length</strong></td>
<td>Minutes to hours</td>
</tr>
<tr>
<td><strong>QoS</strong></td>
<td>None, or High for military fields</td>
</tr>
</tbody>
</table>

### WSN

WSNs have emerged as one of the technologies that combine automated sensing, embedded computing and wireless networking in tiny, embedded devices. Sensor Networks are used to gather physical information about an object or area and relay that information back to an access point (sink) [7].

### Table 6: WSN principal parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Energy Requirement</strong></td>
<td>Low to High (Duration)</td>
</tr>
<tr>
<td><strong>Network size</strong></td>
<td>Small to very large (thousands)</td>
</tr>
<tr>
<td><strong>Node Range</strong></td>
<td>Short - 2 to 20 meters</td>
</tr>
</tbody>
</table>
Table 7: VANET principal parameters

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy Requirement</td>
<td>Low to High (Duration)</td>
</tr>
<tr>
<td>Network size</td>
<td>Small to very large (thousands)</td>
</tr>
<tr>
<td>Node Range</td>
<td>Short - 2 to 20 meters</td>
</tr>
<tr>
<td>Link data rate</td>
<td>Less than 1 Mbit/s</td>
</tr>
<tr>
<td>Network Configuration</td>
<td>Static or Dynamic</td>
</tr>
<tr>
<td>Session length</td>
<td>Very short</td>
</tr>
<tr>
<td>QoS</td>
<td>None or medium (medical apps)</td>
</tr>
</tbody>
</table>

**VANET**

One goal of a VANET, which is a particular form of MANET, is to enable the dissemination of information pertaining to traffic and road conditions, such as local congestion or surface ice, as detected by independent moving vehicles. This activity, which is known as an information warning function, is useful for vehicles on major highways and motorways, enabling early reactions to potential threats.

**Summary of SON**

Self-organizing networks are clearly highly dynamic and need special handling and treatment, not only to achieve their objectives and security requirements, but also for the sake of the QoS of the overall network. Moreover, one of the principle objectives is to save energy, which is a key issue in WSN. Security requirements fall across a broad spectrum depending on the services and network. However, the survivability of the network is also a must for all SONs.

**3.3 Attackers’ Classification**

Attackers can be internal or external. This means that the model used here distinguishes between attacks launched from within a network and those coming from outside [8]. Any internal authorized node, i.e. an insider, can jeopardize an entire network’s security due to the fact that the network is inherently distributed.

It is a good idea to have an overview of attacks in order to classify them according to TCP-IP protocol stack. References [9, 10, 11] detail some attacks on the Protocol stack which are reported in Table 8.
Conclusions and Future Work

Table 8: Shows the attacks and associated layer

<table>
<thead>
<tr>
<th>Layers</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Data corruption, viruses, malicious code repudiation and worms</td>
</tr>
<tr>
<td>Transport</td>
<td>TCP/UDP SYN flood, session hijacking</td>
</tr>
<tr>
<td>Network</td>
<td>Hello word, black-hole, grey-hole, wormhole, link spoofing, replay, location disclosure</td>
</tr>
<tr>
<td>Data Link</td>
<td>Malicious behavior, selfish behavior, monitoring, traffic analysis</td>
</tr>
<tr>
<td>Physical</td>
<td>Eavesdropping, active interference: jamming and so on</td>
</tr>
</tbody>
</table>

3.3.1 A synthesis of SON Attacks

First of all, we will list the different attacks which have taken place against MANET in order to have a global vision. Pradip et al. in Article [5] give a broad description of attacks against MANET, reference [12] (Book of Al-Sakib Khan Pathan) does the same for WSN and reference [13] does likewise for SON, particularly VANET. In addition, Karlof in article [14] focuses on routing security within WSN. It discusses different attacks and countermeasures as well as the major routing protocols and energy saving topology maintenance. Sinkholes and Hello flooding attacks are also presented as new forms of attack.

We will now perform a complete inventory of all plausible attacks on SON networks related to the literature.

1. Jamming attack
2. Wormhole attack
3. Blackhole attack
4. Byzantine attack
5. Traffic analysis
6. Routing Attacks:
   1) Routing Table Overflow
   2) Routing Table Poisoning
   3) Packet Replication
   4) Route Cache Poisoning
   5) Rushing Attack
7. Resource consumption attack
8. IP Spoofing attack
9. State Pollution attack
10. Sybil attack
11. Fabrication
12. **Modification**
13. **Session Hijacking attack**
14. **Repudiation attack**
15. **Denial of Service attack**
16. **Location disclosure attack**
17. **Flooding attack**
18. **Impersonation or Spoofing attack**
19. **Colluding misrelay attack**
20. **Device tampering attack**
21. **Gray hole attack**
22. **Link spoofing attack**
23. **Neighbor attack**
24. **Jellyfish attack (Subset blackhole)**
25. **Packet dropping attacks**
26. **Sleep deprivation torture**
27. **SYN Flooding attack**
28. **Malicious code attacks**
29. **Illusion attack**
30. **Link withholding attack**
31. **Bogus attack**
32. **Identity disclosure attack**

Other attacks related to moving target defense are presented in [87].

### 3.3.2 Physical attacks

These attacks are hardware oriented and are simple to execute.

As stated in by Yau in reference [11], we can divide external threats into two major categories: passive eavesdropping, where the adversary simply listens to transmitted signals; and active interference, where the opponent sends signals or data designed to disrupt the network in some way.

Node compromise is described in reference [9-10] respectively by Şen and Kong, and it is the easiest form of attack against WSN because nodes are placed in an open environment. Through these, an attacker might view and/or alter data or even damage hardware. Tamper resistant packages and camouflage are among the solutions that aim to prevent such attacks.

**Eavesdropping attacks** [12]: these are passive attacks by external and internal nodes. They compromise privacy just by detecting that a signal is present.
**Conclusions and Future Work**

**Jamming attacks** [10, 11]: These are a kind of denial of service (DoS) attack, which is defined by NIST as an attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting the available resources. In fact, jamming represents the most serious security threat in the field of Wireless Sensor Networks (WSNs) [15], as it can easily throw even WSNs utilizing strong high-layer security mechanisms out of order, simply because it is often ignored in the initial WSN design. The critical issue of jamming in WSNs is covered by article researchers using notions such as frequency hopping and spread spectrum communication [89], but is still open to other research issues in this field.

**Traffic analysis** [14]: This is a network based attack against distributed systems. The goal of this attack is to be invisible, as thereby the attacker does not need to compromise any nodes nor break a cryptographic design. Indeed, it traces a packet flow using timing and other eavesdropped routing information [90]. For example, through timing analysis, it can be revealed that two packets coming in and out of an explicit forwarding node at times (t) and (t+dt) are likely to be from the same packet flow. Thus, this attack may reveal details which would compromise location privacy, anonymity/identity privacy and motion pattern privacy, as well as providing details of route tracing. In the end, the authors conclude that ad hoc networks deployed in hostile environments need new countermeasures in order to be able to resist to such passive attacks.

**Table 9: Passive SON attacks and counterattacks references**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Akyildiz [22]</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Sabbah et al.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[23,24]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key distribution</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[26]</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Chen et al [27]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deng et al [25]</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Conner et al. [28]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Xi [29]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tamper resistance and camouflaging [16]</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

**3.3.3 Active attacks**

These attacks cause unauthorized changes to the network. The major threat from them is a denial of service (DoS) attack, caused by the blocking of the wireless communication channel. These attacks are always launched by users or authorized nodes operating within the network. The success of such attacks depends on their duration, and the routing protocol used.

We could classify active attacks as being separable into four groups:
Dropping: selfish nodes intentionally drop all packets. This attack could lower a network’s performance. One derivative attack is selective dropping, which hides itself from detection by only dropping some packets.

**Modification:** an intruder attacker modifies packets in order to disrupt the network. Likewise, a sinkhole attacker makes itself more attractive in order to start a dropping attack.

**Fabrication:** the intruder fakes his own packet to disturb the network.

**Timing:** an attacker gives other nodes the impression that it is closer to them than is actually the case in order to manipulate the topology of the network. Hello flood attacks use this technique.

### Table 10: Active SON attacks counterattacks references

<table>
<thead>
<tr>
<th>Categories/response</th>
<th>Active attacks ↓</th>
<th>Dropping</th>
<th>Modification</th>
<th>Fabrication</th>
<th>Timing</th>
<th>impersonation</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flooding [30] [22]</td>
<td>☑</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yi [30, 31]</td>
</tr>
<tr>
<td>Compromising routing information [17,23]</td>
<td>☑ ☑ ☑</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ARRIVE [32]</td>
<td></td>
</tr>
<tr>
<td>Selective forwarding [33]</td>
<td>☑</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Trust-based Abu-Ghazaleh [36], Gago [38]</td>
<td></td>
</tr>
<tr>
<td>Sinkhole [33], Grayhole [34]</td>
<td>☑ ☑</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Trust P2P applied to WSN [35], Al Shurman [38]</td>
<td></td>
</tr>
<tr>
<td>Byzantine (Colluding misrelay)[39]</td>
<td>☑ ☑ ☑</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Crépeau [40]</td>
<td></td>
</tr>
<tr>
<td>Sybil attacks [23]</td>
<td>☑</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Authentication [41]</td>
<td></td>
</tr>
<tr>
<td>Wormhole [42] [43] (Rushing)[44]</td>
<td>☑ ☑</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>[36], Hu [42, 44]</td>
<td></td>
</tr>
<tr>
<td>HELLO flood attacks [43]</td>
<td>☑ ☑ ☑</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>[36]</td>
<td></td>
</tr>
<tr>
<td>Acknowledgment spoofing[43]</td>
<td>☑ ☑ ☑</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>[19], Adjih[45]</td>
<td></td>
</tr>
<tr>
<td>False data injection to disrupt data aggregation[50]</td>
<td>☑</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Wagner [51], [19] authentication &amp; key distribution, [50]</td>
<td></td>
</tr>
<tr>
<td>Spoofing location [33], VANET [49]</td>
<td>☑</td>
<td>☑</td>
<td></td>
<td></td>
<td></td>
<td>Sastry [48], Jian [46], VANET[49]</td>
<td></td>
</tr>
<tr>
<td>Link spoofing[45]</td>
<td>☑ ☑</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Rafto [47]</td>
<td></td>
</tr>
</tbody>
</table>

Probably the most serious type of denial of service attack is a sleep deprivation torture attack [13], whereby node energy is deliberately wasted. It is based on making service requests of any kind in order to waste the limited power and resources of a node. It has been emphasized in the literature that this is the
Conclusions and Future Work

most powerful DoS attack. Security capable of dealing with such attacks has been extensively studied and has already been developed by the military for use in packet radio networks. Spread spectrum technology is designed to be resistant to noise, interference, jamming, and unauthorized intrusion [23].

Any protection in the physical layer cannot furnish protection against sleep deprivation torture, even though power constraints are indeed a physical layer attribute, because power levels influence all ad hoc network operations and make securing such networks particularly difficult.

There are also threats to integrity, e.g. when an external attacker attempts to replay old messages, or to change the order of messages. Old messages may be replayed to reintroduce out-of-date information. Out-of-date routing information could lead to further denial of service attacks as nodes attempt to use old but invalid routes, or even delete current, valid routes. If the routing protocol utilizes neighbor-sensing by monitoring received data packets, the replaying of old packets may falsely lead nodes to believe that an ‘old’ link with a neighbor has become active and usable again.

Additionally, we should also have an overview about the misuse goals of attackers. Indeed, they try not to follow the routing protocols’ specifications in disrupting network communication. In addition, we must take into account their capabilities that affect the attackers [13].

Route disruption: causing routing loops and pushing the network towards non optimal use.

Node isolation: isolating one or more nodes from the network in order to partition the network.

Resource consumption: misuse of resources in order to worsen performance in terms of energy, bandwidth, and so on.

Attackers’ achievement of their objectives is directly affected by:

i. Computation power
ii. Deployment capability
iii. Location control
iv. Mobility
v. Degree of physical access

3.3.4 Attacks on VANET

A VANET is considered by the literature to be a special case of MANET. However, it has some specific characteristics such as high levels of dynamism and volatility, mainly regarding its network topology, participants and communication links. Whereby, the security requirements of VANET are slightly different from those of MANET.

Although this survey provides a good insight about the state of security in VANET, it does not dwell on the specifics of various types of attacks or various
attack models that can be used for threat assessment.

IEEE 1609.2 standard specifies security services for Wireless Access in Vehicular Environments (WAVE). A good survey about VANET was carried out by Stampolis and Chai [106]. We could find the methods that were proposed so far to secure VANET in 1609.2 security functions recommendations:

i. IEEE Draft Std 1609.2-2006 was issued July 6, 2006
ii. It contains formats for secured messages
iii. Signed and encrypted
iv. Elliptic curve cryptography (bandwidth)
v. It contains mechanisms for identified authentication
vi. It contains certificate issues and expiry mechanisms

3.4 Problem formulation

Generally, much ongoing work is concerned with providing layered security such as the Holistic security Approach [52]. But there is a principal withdrawal from this approach because of the redundancy of implementation of security in the absence of a systemic view. Thus, wastage of resources is introduced – resources such as energy, CPU power, and -predominantly- time. As a matter of fact, economizing battery power and managing resources are especially important factors in today’s communications technology.

Actually, communication systems are resource consuming, particularly in relation to battery power [53]. This is because a lot of smart and useful mobile applications need significant amounts of power, mainly on account of GPS for geo-localization. In order to reduce power and resource consumption, however, users turn their security means off. Indeed, when designing a wireless network, the problems of significant consumption of power and resources, to power a processor, for example, are considered to be limiting factors. This is why it is widely acknowledged that users and designers have a tendency to avoid security measures in mobile devices in attempting to reduce their power and resource consumption, thus putting not only a particular user’s security at risk but also that of other users in cases of DDOS attacks [54].

It is highly critical to maintain overall security due to the configuration complexity and the changing runtime context. Accordingly, the concept that will be able to cope with this new security challenge must be based on a dynamic adaptation security system in order to satisfy overall performance in areas such as power consumption, this being a key issue in mobile networks, and especially in sensor networks.

In this last network, the data could be sensitive and the network could operate in a hostile environment. It is imperative to address these problems ab initio. However, due to different constraints and power limitations, security poses new challenges that are really very different from those affecting traditional networks.

There is actually enormous research potential in the field of wireless and sensor
network security, especially in relation to power limitations and performance constraints. Indeed, these networks are special due to the many restrictions they find themselves bound by in comparison with traditional computer networks. Therefore, it is difficult to deploy only conventional security solutions.

Our study is about analyzing the security constraints within wireless networks and sensor networks and finding a solution to the various security problems related to the constantly changing behavior of attackers.

Indeed, the most critical problem relating to security in mobile networks is dealing with all of these security challenges - including attacks based on consuming unnecessary power - and finding a solution that is able to respond in runtime to these various changing attacks.

1. Proportionality: The solution must be based mostly on the fact that security means must be proportional to the potential likelihood of network attacks.

2. Generic security adaptation framework: A generic security adaptation mechanism mainly based on an autonomic system as a compelling solution for this problem will be greatly helpful.

3. Cross-layer or optimal-layer: The security scheme must not be based on a classical layered security scheme, which has been shown to be an inadequate and non-optimal solution.

4. Survivability: The solution must extend the lifespan of the network as well as the global network utilization.

5. Reference monitor for data protection: Our work is inspired by the concept of the Reference Monitor (RM) which was developed for data access [55] and has been widely used for more than 30 years. Its efficiency in data access is widely exploited in the security domain and is also largely accepted.

6. Component based security: Security measures must be also provided to all the components of a system as well as to the network. We should secure the whole chain.

7. Realistic Design: The design must take into account the limited resources and practical aspects.

8. QoS with security: Security must be treated as a crucial aspect of QoS, stated in many articles as QoSS.

### 3.4.1 Mathematical formulation

A very fundamental definition for adaptation security problem based on security means was proposed [56]:

Let $M_1, M_2, \ldots, M_k$ be alternative security means for class $\Omega = \{ T_j \}$ set of tasks. Any mean $M_i$ is related to a vector of parameters $\mathbb{U} \rightarrow M_i = M_i(\mathbb{U})$.

The criterion function intended for the estimation of specific objective (e.g. efficiency, survivability) applied to a specific task $T_j \in \Omega$:

Conclusions and Future Work
Problem Statement and Methodology

$q_{i,j} = q(T_j, M_i)$.  

Equation 1

The importance of adaptation arises when the criterion function can only be calculated at runtime. The goal to achieve is to select an efficient security means by minimizing the following of integral criteria for specific tasks, using only observations of its values:

$Q(M) = \int q(T, M)p(T)dT$  

Equation 2

Where $p(T)$ is frequency distribution of tasks $T$.

Security adaptation is now mathematically formulated, like the majority of other subjects.

### 3.4.2 Complexity of exact mathematical formulation

Unfortunately, the exact mathematical approach is unrealistic for a practical implementation. In this respect, the complexities of network and security design, implementation and upgrades are barriers to any practical system, particularly in highly dynamic environments. Indeed, the complexity of implementing formulas such as those of equations 1 and 2 would be time and energy consuming, which would contradict the objectives of SON networks. This is why it is appropriate to use empirical adaptive technologies to deal with this problem. In addition, this approach allows for the development of systems that function also efficiently in dynamic environments without the need for complete mathematical models of the system.

### 3.5 Methodology of the Approach

For a long time, security has been treated as a static component in system design, with a static security assessment assumed to able to protect the system throughout its lifetime, under the assumption that energy is unlimited. However, this assumption no longer holds, because some devices are disconnected from a power line and are thus in a battery mode that has a limited lifespan. Reference [57] declares that Wi-Fi devices consume 30% more energy than devices in normal mode. A complete study of the energy consumption of mobile phones, where it has been proved that a 3G connection consumes six times more energy than Wi-Fi, is presented in [58] by Balasubramanian. In addition, the problem of energy is a key issue in sensor network [59]. Therefore, the security cannot be considered without other contextual aspects, especially energy awareness.

Some solutions have already been implemented but are based on fixed security schemes and may be inadequate for systems exposed to diverse operating contexts [60], like those found in wireless environments. However, as greater security consumes more energy, in the case of contexts where attacks cannot happen, security means should be stopped in order to save battery power. In order to do this, the policies need a high level of coordination for proper security policy provision.

Applications for adaptive security have been proposed in areas such as mobile
Conclusions and Future Work

ad-hoc networks, where the current network conditions play a role in choosing the relevant security mechanisms during runtime [14]. In WLAN the same principle can be applied and evaluated to ensure security and performance. Some proposals have been made to provide adaptive security framework systems [61], but none of them have taken the energy consumption into account. Another contribution to the adaptation of security mechanisms in WLANs was published by Saxena in [62]: the required security level depends mainly on the level of trust within the environment, and how hostile one expects the environment to become.

We argue that spare processing and transmission resources are wasted in mobile environments if security is over-provisioned. Hence the trade-off between security and performance is essential in the choice of security services. Adaptive security mechanisms are also found in flexible protocol stacks for wireless networks [63], context-aware access control systems [64] and security architecture [65]. This prompted us to enable the implementation of a completely reconfigurable architecture [66], which would be fundamental for adapting the architecture to allow for the terminal and network variability of the context, particularly in the security field [67].

Flexible security mechanisms are needed in order to respond to new types of attacks and to meet different network setting-specific protection requirements. The required flexible security assessment can be achieved by introducing a generic autonomic computing security framework, according to David Chess [69, 70]. He describes the importance of automatically configuring the security of various parts of the system and automatically making various security trade-offs according to the value of the assets being protected and the cost of the measures being employed to protect them.

Because of the following limitations [71], layered security solutions are inadequate and/or inefficient:

I. **Redundant Security Provisioning**: systematic security at each layer consumes more resources than necessary

II. **Non-adaptive Security Services**: because attacks on a WSN can come from any layer and any protocol, a countermeasures scheme at only one layer is unlikely to guarantee security all of the time.

III. **Power Inefficiency**: energy efficiency must be addressed because it is a crucial issue in WSN. The power efficiency design cannot be addressed wholly within any single layer in the networking stack.

The new approach to solve the inefficiency of layer security is to use a cross-layer approach. In the case of sensor networks, the sensors usually forward their messages to a base station (gateway) [72] in a hop-by-hop fashion because they are resource-constrained in terms of energy; the amount of energy expended increases dramatically with the range of transmission. It is quite easy for an attacker like a Sinkhole [73] to defeat the WSN purpose by dropping messages when they are received rather than forwarding them, or by making other sensors run out of energy by asking them to send information. Many solutions have been proposed for non-mobile WSN but there is a lack of
literature for MWSN. Indeed, it is harder to deal with mobile attackers.

3.5.1 Adaptive security Framework

We propose a generic Framework called a Security Adaptation Reference Monitor (SARM) as a compelling solution to this problem, because it is feedback loop control system which has been developed especially for highly dynamic wireless networks.

Implementing this security scheme at each application level is not feasible because the change will interfere with each communication program in each device. The best way to overcome this constraint is to implement it in the kernel and consequently to have overall security control - or even better - to do it based on a cross-layer approach.

Because of the constraints imposed in sensor networks, such as energy limitation, decentralized collaboration and fault tolerance, the algorithms for network security tend to be quite complex and usually defy analytical methods that have been proved to be fairly effective for traditional networks. Furthermore, the application of new methods and mechanisms in real networks would be very difficult and is not operational. It appears that simulation is the only feasible approach to the quantitative analysis of new algorithms in wireless networks.

We have conceived SARM for wireless environments based on an autonomic computing security feedback loop control system, which fine-tunes security means based on monitoring of context, including the user environment and energy consumption aspects. It aims to offer a global adaptation security scheme for any application instead of a classical layered security mechanism.

Trust and reputation will now be introduced and defined. Thereafter, we will apply them in our adaptive security Framework.

3.5.2 Trust

Trust and reputation might be well understood during face-to-face trade or in a virtual community. Reputation refers to the perception that an agent has of another’s intentions and norms. Reputation has been used by biologists [74], economists [75] and computer scientists [76]. We will concentrate in this section on trust and reputation for computer sciences.

The first trust definition [77] (reliability trust) states that trust is the subjective probability by which an individual A expects that another individual B will perform a given action on which its welfare depends.
Figure 22: Trust relationship

Figure 22 shows the Trust notion which reflects the relationship between a trusting (trustor) and a trusted agent (Relaying party, trustee) for a specific context.

Trust is also related to the perception of risk that a person has when dealing with another. McKnight & Chevany [78] have given a definition:

Definition 2 (Decision Trust): Trust is the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible.

3.5.3 Reputation

Definition 3 (Reputation): Reputation is what is generally said or believed about a person’s or thing’s character or standing.

This definition fits well with the social trust definition. Reputation can also be considered as a collective measure of trustworthiness based on recommendations or ratings from members of a community.

The main difference between trust and reputation systems is that trust is a value which reflects a subjective view of a subject between two agents; whereas reputation is seen as a value given by the whole community.

Resnick et al. [79] declare that reputation systems must have three properties in order to operate at all:

- **Longevity** (no identity changing): entities must live long, so that with every interaction there is always an expectation of future interactions
- **Diffusion of current ratings**: ratings about current interactions must be captured and distributed
- **Ratings influence past-present**: ratings about past interactions must guide decisions about current interactions.
- **Trust transitivity propriety** (Reliability trust):
If A trusts B and B trusts C, then A trusts C. This assertion is not always true. Nevertheless, it might give A the opportunity to derive a measure of trust in C. Anyway, there are semantic constraints for the transitive trust derivation to be valid among others. Indeed, the trust must be for the same purpose [80].

Rasmusson and Jansson [81] consider that trust is the concern of soft security, as opposed to traditional hard security mechanisms. They see each agent as responsible for managing his own security using social control mechanisms. Their work shows clearly that trust is a more complex processing problem here than would be the case for conventional security situations.

3.5.4 Trust and Network

There are general types of trust [82]: basic, general, and situational. This distinction can be applied in any network. Basic trust is related to the previous experience of a node in all situations; whereas general trust does not relate to a particular situation but is more of a generally held opinion. Situational trust is related to a particular situation or context. This last form of trust is the most important in SON such as MANET and WSN.

McKnight and Chervany [83] have presented the relationships among the six trust constructs of a node in a self-organizing network, which are:

I. Dispositional trust of a node: a general expectation about others
II. Situational decision to trust a node: occurs when a node interacts with a new node and might need to trust a third party to communicate
III. System trust in a node: occurs when nodes believe that the structures encourage successful interactions

Trust belief in a node: the belief that a particular node is trustworthy in a specific context.
I. Trusting intention of a node: voluntary dependence on a node despite knowing the risk involved

II. Trusting behavior of a node: voluntary dependence in a specific situation despite the existence of some risks

Figure 24: Inter-relationship among trust constructs [McKnight and Chervany]

3.6 Conclusion and Summary

In this chapter, we stated the problem which is addressed in this research. Then, we presented an overview of a SON’s security requirements with an exhaustive classification of attacks on SON networks. Next, we gave the mathematical formulation for adaptive security and explained its implementation complexity. Finally, we described the trust and reputation background related to our thesis. The mathematical Trust approach was a good help in implementing a trust and reputation system progressively within our Framework. This began with the study of an analytical trust and reputation approach. As soon as we had some solid foundations, we implemented them within our Framework using analytical checking mechanisms for simple cases. Thereafter, we implemented a trust and reputation system using simulation tools.
3.7 REFERENCES


15. A. Mpitziopoulos, Damianos Gavalas, Charalampos Konstantopoulos, and Grammati Pantziou “A Survey on Jamming Attacks and
Conclusions and Future Work

Countermeasures in WSNs” IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 11, NO. 4, FOURTH QUARTER 2009


34. A. A. Pirtada and C. Mcdonald, “Establishing trust in pure ad-hoc networks”, in proceedings on Computer Sciences, 2004


45. C. Adjih, D. Raffo, and P. Muhlethaler, “Attacks against OLSR: Distributed key management for security”, OLSR Workshop, 2005


49. P. Golle, D. Greene, and J. Staddon “Detecting and Correcting Malicious Data in VANETs”, ACM, VANET’04, October 1, 2004


58. N. Balasubramanian, A Balasubramanian, and A. Venkataramani, “Energy Consumption in Mobile Phones”, IMC’09, 2009


75. D. M. Kreps and R. Wilson, "Reputation and imperfect information," Journal of Economic Theory, Elsevier, 1982 vol. 27(2), pages 253-279,

77. In Gambetta (ed.) “Can we trust trust?”, 213-237, 1988


Chapter 4. Autonomic Computing for adaptive security

“Civilization advances by extending the number of important operations which we can perform without thinking about them”

-Alfred North Whitehead, “Introduction to Mathematics”.

“Water shapes its course according to the nature of the ground over which it flows; the soldier works out his victory in relation to the foe whom he is facing”

-Sun Tzu, “On the art of War”.

In this chapter, we introduce two subjects- autonomic and security adaptation systems. We start with an introduction in section 4.1. Next, we give a background picture with a definition and some information on historical origin, as well as on the complexity of an autonomic system. In subsections, we discuss the subject, provide a set of all system properties, introduce the Smart City initiative which is based on autonomic communication, and finish up with a system design and architecture. Section 4.3 introduces the principle of adaptive security. Then, in subsections, we describe the architecture of this approach, and define a security adaptation system and risk management. Finally, we summarize this chapter in section 4.4.

4.1 Introduction

Today, ubiquitous computing is becoming an important domain that impacts on real life, focusing on simplifying our daily lives through the use of smart phones, RFID tags, networks based on sensors and smart homewares/clothes, etc. The Internet of things is one of these components. Recently, the popularity of a number of trends and applications has grown at such a great pace that these applications are now increasingly common. Nowadays, all delivered services are sophisticated and must be reliable in terms of time-to-market, in addition to having rapid response times for customer inquiries. Thereby, up to 80% of an average company’s ICT budget is currently spent on maintaining its existing applications [1].

This spreading has put computing, networking systems, applications and services beyond the passing level of complexity that a normal, untrained human - or even a group of humans - could deal with; and a fortiori this extends to the design and maintenance of a system’s operations, and to solving runtime problems. The increasing levels of complexity and heterogeneity of systems and dynamism of networks and applications have made static security mechanisms seem fragile in terms of their capacity to tackle changing runtime attacks. This
evolution leads to unforeseen threats and vulnerabilities, and thus, the protection of users and things according to high level policy is becoming a major concern.

The need to investigate and explore other alternatives and opportunities in order to find new paradigms for system and application design has been looming for years now. Therefore, many fields, mainly those based in biology, have been catapulted into the domain of security to solve this problem. Autonomic computing, based on strategies used by biological systems, seeks to improve the design of systems and applications and catalyzes their survivability. In fact, the autonomic system is here to combat the issue of complexity [2]. It functions in a way that mirrors how the autonomic nervous system regulates and protects our bodies without our conscious involvement. Many fields have been identified as research opportunities, amongst other things, predictive and continuous optimization, self-protecting, self-learning security implementations and context awareness. In brief, the autonomic system seeks to improve the manageability of security in our lives. This is the main goal of our work.

4.2 The Autonomic System

4.2.1 Background

**Autonomic definition**

The autonomic system is an emerging discipline [2] because, amongst other reasons, there are still many research challenges ahead on the road to making it a practical reality [3]. More fundamentally, however, the interpretation of the concept itself is still under discussion [4]. Drawing from the dictionary definition, autonomic essentially means a “self-governing”, “self-managing” or “adaptive” system, and is derived from the noun autonomy.

**Definition**

An Autonomic System is a system that operates and serves its purpose by managing its own self without external intervention even in case of environmental changes.

Therefore, an autonomic system must be able to customize itself in response to changes in policies or mission; or in order to adapt to its deployment environment.

**Autonomic computing and system complexity**

Because of the scale of the complexity, heterogeneity and dynamism of networks, systems and applications, infrastructure is becoming fragile and vulnerable. This is why the investigation to find an alternative paradigm to deal with these challenges is of such immediate significance. The main goal of this approach is to find a new paradigm to promote a self-managing system according to a high level of human guidance.
Indeed, the autonomic computing paradigm is inspired by biological systems such as the autonomic human nervous system, which inspires the development of self-managing, self-aware, self-optimizing and context aware systems and applications.

In this respect, the IBM [6] manifesto stated that the most important barrier to further progress in IT is a looming software complexity crisis. The administration of such complex systems is beyond individual software environments. Thus, it would be best if we could handle all complexity and uncertainties with minimal human intervention.

Autonomic systems will be interactive collections of autonomic elements – individual system constituents that contain resources and deliver services to human and/or other autonomic elements.

They will manage their internal behavior and their relationships with other autonomic elements in accordance with policies that humans or other elements have established. System self-management will arise at least as much from the innumerable interactions between autonomic elements as it will from the internal self-management of the individual autonomic elements – just as the social intelligence of an ant colony arises largely from interactions between individual ants. A distributed, service-oriented infrastructure will support autonomic elements and their interactions.

**The road to the Autonomic system**

*The Nervous System*

The Autonomic Computing Paradigm has been inspired by the human autonomic nervous system which is, to the best of our knowledge, the most sophisticated example of autonomic behavior that exists in nature today [7].

In fact, observation of the natural world has given us the opportunity to formulate theories about nature [8]. This was the case for both Newton’s laws and Kepler’s model. At the same time, models inspired by nature have also been successful, as in the cases of Velcro and bulletproof vests. Nowadays, computer science contributes to the comprehension and study of biological systems. The interaction between the two sciences has given engineers new opportunities. Indeed, in order to tackle the many diverse technical problems which have not been solved – either at all or in part - engineers have always tapped into natural patterns, such as neural network paradigms, evolutionary algorithms, fuzzy systems, and classification systems. As such, we have taken inspiration from biological systems in order to provide solutions to tackle a wide range of problems. This natural inspiration is a major motivation for the development of artificial immune systems [10]. This technique utilizes metaphors from immune systems in order to solve problems in a new field of research called a bio-inspired system.

*Ashby’s Ultrastable System*

A huge number of variables are enclosed within every real machine, and a human system might be represented by the same sets of variables. In order to survive, it is necessary to keep the most important variables within viable limits;
otherwise there is disequilibrium, leading to disintegration or loss [10].

The management of such a system entails working together constantly to maintain its essential variables within their reasonable limits. Ashby states that any behavior that maintains the essential variables within their limits in the viability zone will be an adaptive form of behavior.

Likewise, ICT can be modeled as a set of variables that are necessary to maintain stability within limits; otherwise the system will be unstable and out of control. Further reflections might also be made as regards security, the main objective of which is to maintain an acceptable level of risk to the system according to policies. This is why a Generic framework design must be based on this principle.

Two important observations can be made about the field of autonomic systems:

I. whenever a system’s environment pushes it towards disequilibrium, the system will manage to return to a state of equilibrium; and

II. the goal of adaptive behavior is linked to the survivability of the system.

### 4.2.2 Autonomic properties

We have synthesized all of the characteristics of an autonomic system that have been stated in the literature. Indeed, these are the properties that will be used for comparative purposes. They are exposed and explained briefly in Table 11.

<table>
<thead>
<tr>
<th>Autonomic characteristics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all secure layer</td>
<td>&quot;deny all&quot; policy access on a need-to-know basis, foundation of &quot;defense-in-depth&quot; multiple security layers</td>
</tr>
<tr>
<td>Anomaly detection</td>
<td>automatic recognition of and reaction to abnormal behavior, anticipation of threats before their manifestations</td>
</tr>
<tr>
<td>Autonomy</td>
<td>security mechanisms functioning in an autonomous fashion</td>
</tr>
<tr>
<td>Disposability</td>
<td>a sacrificial system to guarantee overall system survivability</td>
</tr>
<tr>
<td>Distributivity</td>
<td>distribution of elements reduces attack surface</td>
</tr>
<tr>
<td>Diversity</td>
<td>control mechanisms</td>
</tr>
<tr>
<td>Dynamically changing coverage</td>
<td>a means to intelligently predict and anticipate what threat-response mechanisms must be deployed</td>
</tr>
<tr>
<td>Fault tolerance</td>
<td>changing response mechanisms to respond to threats for which they would not be prepared</td>
</tr>
<tr>
<td>Immune learning</td>
<td>adaptivity – the ability to learn threats over time</td>
</tr>
</tbody>
</table>
Conclusions and Future Work

<table>
<thead>
<tr>
<th><strong>Autonomic characteristics</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Immune memory</td>
<td>capacity to remember threats over time</td>
</tr>
<tr>
<td>Integration with other systems</td>
<td>defense-in-depth strategy helping to achieve flexibility</td>
</tr>
<tr>
<td>Multilayered</td>
<td>implementation of multiple security measures to overcome the risk of individual measures being compromised</td>
</tr>
<tr>
<td>Noise tolerance</td>
<td>recognition of threats without an absolute signature match</td>
</tr>
<tr>
<td>Pattern recognition</td>
<td>pattern matching to identify normal and abnormal behavior</td>
</tr>
<tr>
<td>Predator-Prey pattern response</td>
<td>scaling up of responses, triggering and feedback as the number of attackers increases</td>
</tr>
<tr>
<td>Resilience</td>
<td>The reliability of the resilient system means it continues to function in spite of reduced capacity</td>
</tr>
<tr>
<td>Robustness</td>
<td>linked to diversity and distributivity</td>
</tr>
<tr>
<td>Self Identity</td>
<td>distinguishing between self and no self; isolating and eliminating according to policy (Trust)</td>
</tr>
<tr>
<td>Self organization</td>
<td>threat-response controls must be capable of adjusting their behavior in a similar manner so as to choose the best countermeasures</td>
</tr>
<tr>
<td>Uniqueness</td>
<td>each system has unique behavior in order to prevent monoculture and to avoid generalized identical attacks</td>
</tr>
</tbody>
</table>

**4.2.3 Issues in autonomic communications: SmartCity**

**Definition [20]**

Autonomic Communication is an integrated technology platform for sensing, communicating, decision making and reacting in future networking and networked businesses.

Autonomic communication is centered around networking selfware, a novel approach to perform network control, management, middleware communication, etc. based on principles of high evolvability and generic network instrumentation. [20]

In autonomic telecommunication, protocols are now designed by applying some part of self* proprieties to avoid human intervention. These protocols are isolated and are not yet designed at high level due to the difficulty of dealing with all interactions. To tackle this problem, we need to have a sustain network by allowing protocols and procedures to operate in an autonomic manner.
**Smart City**

Demographic trends that have already largely been determined will contribute to a substantial reshaping of the global landscape between now and 2050. Indeed, people will be far more concentrated in urban areas. Accordingly, by 2015, and for the first time in human history, the majority of the world’s human population will live in cities. According to UN projections, nearly two-thirds of the population of the developing world will live in cities by 2025. [11]

Emerging technologies will be used in the service of humans in cities, causing the rapid expansion of digital networks and services, often offering connections to all form of Wireless sensors - essentially IoT, which is already blooming in our cities. These emerging technologies must be guided towards sustainable ends, and must therefore be accompanied by a scalable and intuitive universal access strategy to all kinds of real-time information, in a safe and reliable manner.

To date, the various networks in urban services have been completely unaware of each other, because while they carry isolatable information from source to destination, the methods of transmission and processing of transmissions from different networks are incompatible with each other.

Smart City is an R&D initiative based around IoT scalable architectures, using future technologies for the realization of networked real-time secure platforms and applications in order to help utilities (fire departments and other emergency services, traffic management, etc.) to improve their management and coordination of resources in these innovative areas. One of the major challenges for this initiative is the integration of so many networks. The security and management requirements entailed by such large volumes of data, such as video monitoring, must also be emphasized, as these would ideally go through the smart grid.

Indeed, this global communication network offers both dramatic advantages and significant challenges [12] for:

I. Industry
II. Operators
III. Developers
IV. Users.

Considering the potentially gargantuan number of components that could be connected to a Smart City information system and their physical distribution across a large area, most smart cities will face network complexity issues. A great many challenges will inevitably arise in securely enabling the integration and deployment of the IPv6-based IoT architecture in smart cities with so many heterogeneous networks.

In IoT, one of the main challenges is to deal with the large number of devices and users, as this requires both specific and scalable solutions. Furthermore, IoT does not rely on standard distributed networks. Here, the network is composed of non-standard IT equipment which can also be located in accessible public places, particularly in the context of smart cities, and so is less
secure. So, the heterogeneity of such devices and users make the challenges even more difficult. In addition, many IoT nodes have limited resources in terms of CPU, memory and energy, which also limits and even discards some well-known effective solutions.

Hence, SmartCity cannot just rely on off-the-shelf solutions but has to carefully consider the specific context. It can adopt some state-of-the-art solutions but this will need careful study so that the right choices and the necessary adaptations will be made. Hence a good evaluation will need to be completed beforehand, through accuracy assessments, in order to achieve not only the security requirements but also overall system efficiency.

From a security perspective, the main objective is to guarantee related system properties from the earliest stages of development in order to be faced with any problems \textit{ab initio}, which will thus need to be urgently fixed. So, the goal is to have security in place from the beginning and thus to avoid explosions of small fixes afterwards. Therefore, the main security issues must be analyzed in order to provide a well-tailored solution. However, there is no global solution to the adaptive management of overall security in this global, specific communication network.

\textbf{Figure 25: an urban Autonomic system scenario in a Smart City}

Figure 25 shows the greater density of the smart city of the future, where IoT will be widespread. In Smart City architecture, the degree of complexity is due to the greater density at each level, which causes a lack of security. This is why security at each level and for each component part must be taken into account; otherwise the Smart City will be chaotic.
Therefore, security is considered to be a key issue. One of the most important solutions will be based on autonomic systems and adaptive security because they fit exactly with the security requirements and goals of the Smart City.

### 4.2.4 Discussion

Dependable, resilient and highly dynamic networks, such as SONs applied to a Smart City, are considered relevant to autonomic systems because they need to achieve both low levels of management effort and high survivability on the basis of unsupervised methods. It is highly relevant to notice that these networks often behave autonomously and collectively at high levels but are not based on autonomic elements at lower levels.

An autonomic system is fundamentally self-managed and is able to respond to attacks, problems, and condition changes. In this respect, it is a reactive system when countering attackers, as well as having the capacity to be a passive system when its power is low in order to manage its own survivability - or even to self-destruct, e.g. in military applications. This behavior might seem contradictory, which is why these systems need special care to be taken during their design as well as to be programmed with smart behavior combinations in order to reach a solution of compromise.

In addition, at least a minimum aggregate of properties must be defined as a foundation set for an autonomic system to fulfill its mission, even though the behavior of autonomic systems can vary from system to system. [13]

- **Automaticity**: This is at the heart of a control feedback system and its ability to adapt its internal functions and means.
- **Adaptivity**: An autonomic system must be able to choose the best configuration according to its objectives, policies and users’ preferences. This behavior is an essential property in dealing with runtime attacks and in adapting the means to reflect the system’s evolution in a timely fashion, in both the long and the short term.
- **Awareness**: This property will adapt the system in response to context or state changes. In fact, an autonomic system must be able to sense its environment as well its internal state in order to assess its control feedback in respect of its objectives.

### 4.2.5 Architecture of autonomic system

An autonomic system is based on rapid and dynamic resource integration evolving in an environment where a federation of heterogeneous systems has no central authority. The pervasive and ubiquitous systems function in the same manner. [12]

David M. Chess [20] describes the importance of Autonomic Security and explains that it is important for the configuration of the security of various parts of the system to happen automatically and for various security tradeoffs to automatically be made according to the value of the assets being protected and the cost of the measures being employed to protect them.
An autonomic system requires a sensor channel as well as motor channels in order to react and counter the effects of changes in the environment.

In this respect, the autonomic system is directly dependent on its mission, policies, and users’ preferences. Its control system would be implemented as a feedback loop to manage an error function or a heuristically assisted system such as a fuzzy system. In this respect, a trust and reputation system might be a good combined solution.

Three principal components are identified in the design of an autonomic system: the first is a Functional unit, which performs operational functions; the second is a Management unit, which controls the functional unit; and the final component consists of inputs/outputs, as described in Figure 26.

![Figure 26: Description of autonomic system](image)

More precisely, an autonomic system is divided into a functional unit that performs operational functions and a management unit that controls the functional unit, inputs and outputs [12]. Thereby, the autonomic system forms a feedback loop. The system collects information by sensing the variety of sources and the user context. Thereafter, they are analyzed and modeled as a basis for adaptation decisions. Then, we apply these decisions and actualize them through the loop, as described in Figure 27.
The above model is also consistent with the principles of a control system. These properties are fully compatible with adaptive technologies based on a practical control system, which might be implemented as fully compatible with an autonomic system. The next section will introduce the foundations of adaptive security and then explain the design of an adaptive security system.

4.3 Adaptive security

4.3.1 Introduction to adaptive security

The trends in mobile networks are moving towards greater mobility and wireless access, and more pervasive networking environments. Because of these trends, devices can roam through heterogeneous networks and interact with multiples devices using many complex protocols. Accordingly, the characteristics of the system are unpredictable in terms of resources, context, user needs and preferences. Moreover, the system is continuously under changing forms of attack, depending on the context and the environment. Self-adaptivity is a key issue in an autonomic system as it can respond to the unpredictable fluctuations of resources in highly complex systems. Indeed, achieving self-adaptivity in the current context, including in relation to security measures and countermeasures, will overcome the traditional weaker static model of security and also guarantee...
Conclusions and Future Work

overall QoS.

In the past few years, serious interest in adaptive computing systems has skyrocketed in many fields because of the system’s potential to adapt dynamically to its environment, particularly in the security field.

A lot of work has been done to shift toward adaptivity but more effort is still needed in order to build a broad, adaptive architecture for security mechanisms. Indeed, without this specific architecture, mechanisms might still interfere with each other and thus be counterproductive. In order to tackle runtime attacks and apply countermeasures (to confine compromised components), we must use an adaptive security system.

4.3.2 Definition Adaptive Security

In reference [14], Adaptive security is described as the capability of a system to automatically or semi-automatically change its security policies and mechanisms to reflect the internal or external environment.

4.3.3 Adaptive security architecture

Motivation

The duration of an entire cycle of an attack can be estimated at anywhere between a millisecond and a second, whereas the security countermeasures could take many hours and will at least take minutes. Likewise, an attacker only needs to locate one or more exposed vulnerability, which contrasts sharply with a security system that needs to address as many as hundreds, or even thousands [15]. It is clear at this point that this is no longer a field where any old manner of security approach can be applied. That’s why new manners are needed in order to reinforce compliance with security policies and user preferences.

We can also define the fundamental reasons for adaptive security:

I. the conventional, static security architecture is unable to cope with the dynamic, changing nature of security;

II. any system which has had its lifetime extended will be unable to deal with future threats and attacks by static mechanisms which are built-in from the beginning;

III. offensive attacks are generated and spread more rapidly than countermeasures can be developed to deal with them;

IV. to cope with the immense complexity of ICT systems, attacks and threats.

Foundations

Three revolutions in the computing and communication fields are driving the development of autonomous and adaptive systems [16].
First is the emergence of the IoT in addition to the AAA paradigms, which are extending the traditional boundaries of interactions between computers/humans and things. For example, a sensor node must fulfill its requirements in a hostile environment, adapt to variable contexts, communicate with neighbors and at the same time conserve its limited battery life (see Smart City p.79).

Second is the growing demand for autonomic computing, which focuses on the development of systems that can self-manage to address unpredictable changes while hiding their intrinsic complexity from users and protecting themselves with only high-level human guidance. This capability is especially important to security systems when dealing with attacks.

Third is the increasing complexity of systems, protocols and devices - but also of attacks - which must be addressed in timely manner.

Figure 28 shows the evolution of a security system through real time integration to its ultimate goal of attaining Self-X principles, which are the objectives of an autonomic system.

- **Survivability and security adaptation**

Survivability is defined as a system’s capability to fulfill its mission in a timely manner in the presence of attacks, failures or accidents [17]. Basically, the definition states that all computer systems have an explicit or implicit mission, which must succeed in the face of adverse events. Achieving survivability involves four key properties, which include [17]:

- Attack resistance: defines strategies for repelling attacks, such as firewalls and user authentication
- Attack recognition: identifies attacks and includes techniques like intrusion detection and system logging
- System recovery: concerns restoration of compromised system data or replacing parts of the system
- System adaptation: the enhancement of survivability in response to adverse events, which could include system patches or intrusion signature updates.
• Security adaptation and risk management

When a system is simple, its characteristics can largely be ascertained, either analytically or empirically. However, a complex system cannot be addressed using analytical tools. Another method must be developed to address this problem. To secure a system, it is necessary to ensure that it satisfies a set of rules and maintains a set of characteristics. Communication networks are complex and need further security protection. A model is needed and must be developed to apply a decision function in order to adapt security means to threats in real-time. Early approaches to calculating security risks used static mechanisms. Unfortunately, these approaches are not sophisticated or flexible enough to allow risk management to tolerate some (small) risks and thus gain time while minimizing costs. Hence, techniques to dynamically variable risks have been developed. We will develop some simple models to illustrate the general approach of adaptation security.

Simple model

As stated on page 21, the cost of security is the sum of the cost of the implementation and deployment of security means (countermeasures) plus the cost of failure.

\[ \text{Cost}(S) = \text{Cost}(CM) + \text{Cost}(F) \]

Equation 3

With S: Security, CM: Countermeasures, and F: Failures

Let’s assume that more effort means greater expenditure on countermeasures and smaller subsequent losses. In addition, we assume that we have an inversely proportional relation with a factor \( k \).

\[ \text{Cost}(CM) = S \text{ and Cost}(F) = \frac{k}{S} \]

Equation 4

Then, the function of security cost will be:

\[ \text{Cost}(S) = S + \frac{k}{S} = \frac{S^2 + k}{S} \]

Equation 5

Now, if you would prefer to minimize this function in order to obtain a lower cost, you can use the first derivative test to check whether you have a minimum, or neither an inflection point.

Let’s study the sign of the first derivative function:

\[ \text{Cost}'(S) = 1 - \frac{k}{S^2} \text{ and Cost}'(S) = 0 \]

\[ S = \sqrt{k} \]

Equation 6
Conclusion: the minimum is located at the point where the cost of security is equal to the cost of the countermeasures if \( k = 1 \). However, in reality, the cost of implementing countermeasures is not directly proportional to the cost of failure, but is more complicated function, and one which is more dependent on time. Minimizing this simplified function is not an easy task in real-time. This is why it is necessary to implement an adaptive system which aims to adapt security means based on a suboptimal but rapid solution. In the next section, we will see that the solution to the exact model is NP-hard.

**Risk management**

There is an important similitude between the tasks facing security adaptation architecture and the concept of risk management. In fact, adaptive security tries to minimize risk at below or at least equal to the level of an accepted requirement. In order to reduce the impact and magnitude of an attack, adaptive security modulates the counterattacks during runtime in a timely fashion. As adaptive security methods are an iterative, ongoing amelioration process, we will introduce a feedback control loop to actively adapt the process.

In order to achieve timely security management, man is confronted with the need to identify what risks the system faces, where its vulnerabilities lie, the impact of potential threats and the chances of a threat actually taking place.

To achieve the best possible security mechanism choice, the system must look for the best possible balance between the cost of security and the cost of insecurity in order to protect the maximum amount of assets. This means that the system must make compromises continuously: this is what is called risk
Conclusions and Future Work

Management. This exercise is not a trivial one, and its resolution is an optimization problem stated, in computational complexity theory, as NP-hard (Non-deterministic Polynomial-time hard).

Besides, the measurement of these risks is not a trivial exercise either, due to the difficulty in estimating risks and their potential effects.

Risk is in general analyzed as a function of threats and their likelihood, which represents the frequency of hazard [19]. Also, hazard can be broken down into threat and vulnerability components. Each vulnerable element is coupled with an associated safeguard. Finally, risk management is formulated as the maintenance of a set of requirements framed as constraints on the aforementioned factors. If the level of risk falls below a threshold then no action will be taken other than a re-sampling of risk; otherwise, some predefined action will be launched in order to protect assets, and the safeguards related to vulnerabilities will be reviewed. [18]

Indeed, the system’s security must be tightened. The level of security must be monitored continuously if the risk dictates. The frequency must also be fixed at a value that is sufficient to allow for reaction when using counteraction measures. These principles are illustrated in Figure 30.

![Figure 30: Risk management related to autonomic and security adaptation systems](image)

### 4.4 Summary

This chapter gives a brief overview of Autonomic concepts and their application in communication and network fields which can be applied to our specified
networks. Next, we will shift our focus onto the current and possible future applications of autonomic systems. Finally, we discuss how the fundamental properties of Autonomic computing comply with the basic design requirements for adaptation security in different highly dynamic networks, such as SON Networks.
4.5 REFERENCES


Chapter 5. Design and Methodology Description of the Framework

“This theory is a self-fulfilling prediction that orders experience into the framework it provides”

-Ruth Hubbard, Theory

This chapter discusses the design of our Framework, the Security Adaptation Reference Monitor (SARM). First, Section 5.1 reviews the motivation and background of the subject and how they relate to SARM. Section 5.2 then describes the adaptive modeling and autonomic system based on which SARM is designed. Next, Section 5.3 presents an analysis of SARM architecture. In Section 5.4, a brief high-level overview of SARM is provided. Finally, Section 5.5 summarizes the overall design.

5.1 Motivation

Security in the recent past was usually treated as a static component in system design, with static security assessments assumed to be able to protect the system throughout its lifetime. As a matter of fact, in most cases the main problem with conventional security frameworks and mechanisms is that they are static; whereas the networks are dynamic systems where conditions are changing rapidly. Moreover, the ongoing changing attacks are generally known at runtime.

The increasing diversity of wireless communication networks and indeed the heterogeneity of access networks have contributed strongly to complicating the task of fulfilling security requirements. Indeed, users can change their environments in a very short space of time and roam through these different networks, interacting with different contexts.

Some solutions have already been implemented but these are based on old ‘one-time’ security schemes and may not be adequate for systems exposed to diverse operating contexts.

This traditional standalone concept of communication security cannot cope with such continuously evolving systems and would not be able to respond to all the forms of attack that a system could possibly encounter during the context changes of runtime. One possible solution would be to have different security settings and policies such that each one could be used to deal with attacks coming from each context. However, these policies may not be sufficiently coherent and need strong coordination to achieve the best security policy provisioning.

Applications for adaptive security [1] (see chapter 4) have been proposed in areas such as mobile ad-hoc networks, where the particular network conditions play a role in choosing the relevant security mechanisms at runtime [2]. The same principle can be applied and evaluated in WLAN in order to ensure
security and performance [3]. There have also been proposals to provide adaptive security systems through system-event monitoring [4]. Therefore, sensing, regular feedback loop, real-time risk evaluation, and acting to deliver what exactly is needed, are the major functionalities.

The global solution is to develop a system that could overcome this security complexity through a thorough integration of security systems for communication infrastructure, allowing any kind of device to connect transparently to any access wireless network in any context.

Flexible security mechanisms are needed in order to respond to new types of attacks and to meet different network setting-specific protection requirements. The required flexible security assessment can be achieved through the introduction of a generic framework.

Besides, the implementation of an adaptive security system becomes a necessity to cope with the large variety of new dynamic attacks. The above-mentioned discussion about security enables us to come up with the new concept of framework adaptive system.

Adaptive mechanisms and architecture might be chosen according to abovementioned reasons.

In the development of consumer software, the component paradigm is generally not a priority in all phases of the software life cycle, from requirements, implementations, and tests to deploy and manage adaptive systems.

The proposed approaches are based on context-aware adaptation models that allow through an autonomic control loop to choose on runtime the most appropriate means. The ultimate goal of these approaches is to ensure security of applications in terms of usability and reliability with respect to dynamic changing and user needs. Most papers consider that security can be viewed as a dimension of QoS. Furthermore, trade-offs between QoS and security are neither taken in account simultaneously nor timely in adaptation process.

**Design approach to an Adaptive Security Model**

How can we process to implement adaptive security architecture? We will outline an approach detailed in [25] but it would be a better approach if it is integrated into security and QoS of the large overall system, network and also to ensure that all components are complying with overall security policy.

I. Define a priority list of threats and designate the desirable ones to avoid or destroy. Similarly, characteristics of these threats are described by an attribute structure or behavior

II. Identify acceptable behavior, trusted components and actions that must not be misunderstood as a threat.

III. Define triggers to monitor for threats and to invoke the countermeasures response.

IV. Implement redundancy for critical functions (corollary to the notion of survivability)
V. Define threat response mechanisms

VI. Define a recovery process to restart themselves in case of compromising threat

VII. Define feedback capability that allows the threat response mechanisms to validate threats so that they only respond to legitimate and realistic threats. This enables the adaptive behavior.

Not every component must have defined every threat characteristics. The objective is to have different threat responses widespread over the system to facilitate the survivability of the ecosystem.

**Adaptive Security Processing**

Recent adaptive security approaches are based in general on the concept of autonomic computing and communication.

The approach of adaptive security involves the chain of threats detection, analysis and response based on:

I. Gathering and monitoring of information

II. Correlation: the evaluation of telemetry data; the ability to correlate information into actions is the crux of adaptive security.

III. Response: actions to prevent or react to threats

In [26], Alia and Lacoste give a description of an adaptive model based on component paradigm using component models and frameworks such as fractal [27]. This system is a reconfigurable recursive component composition. It is also compatible from high level perspective with autonomic approach such IBM’s autonomic architecture [28].

### 5.1.1 Complex adaptive Systems in Security Design

There is a statement very accepted in the field of security design “complexity is the enemy of security”. But at the same time, we would like to argue that complexity is the enemy of static security measures [29].

Complexity is the major obstacle in designing a secure system. Dan Geer et al. argue [30] that systems are becoming so complex that they are rarely entirely understood by members of their design teams, let alone by users. This is why these systems are seldom partially understood; and are *a fortiori* complete complex systems. As such, no one person can analyze the whole system and predict all the ways in which it could potentially be compromised by an attacker in order to prevent insecure operating modes [5]. Therefore, this state will lead to great vulnerability and inevitably to breaches, and security will cost a lot. Indeed, on one hand, the defender has to counter every possible attack; on the other hand, the attacker has to locate at least one vulnerability. In short, there is a great sense of disequilibrium as a matter of course, and this is to the advantage of the attacker. To facilitate the goal of an adaptive security system, it would be very practical to divide the system into many levels in order to construct a consistent one.
Figure 31: level of security adaptation

Figure 31 shows a security adaptation level architecture taken from reference [6], which is divided into 4 levels.

I. The first level is the lowest and is based on formal methods and algorithms.
II. The second level consists of the local system
III. The third level consists of the local network
IV. The last level consists of the distributed network and is based on communication protocols as well as special software and hardware.

5.2 Adapting model

5.2.1 Justifications

The more variable the environment, the more difficult it becomes to enforce security guidelines. This rule becomes a burden mainly when changes occur due to time pressure. In these situations, the new implementation may often contain new or unobserved vulnerable elements because it has been developed under pressure. The new system presents possibly the weakest link for security.

The major problem with conventional security mechanisms is that they are fixed in advance; whereas nowadays, networks are highly dynamic. As stated in chapter 4, regular feedback, constant monitoring, risk management, and real-time evaluation are key concepts in a dynamic environment. Adaptive security is seen as an extension of conventional security. In addition, risk management leads to the selection of safeguards, and feedback is needed in order to choose adequate ones. ISO Reference [7] has confirmed these statements.

The implementation of adaptive security management with logging and reporting is a basic foundation for auditing, which is a potential cost- and time-saving measure.
Defining priorities and identifying cost constraints from the beginning might help in addressing residual risk. An adaptive security system will also help to address this - but in a dynamic way, based on context sensing, user preferences and defined policies. Indeed, some forms of attack very rarely occur in some contexts. Moreover, the system could learn from past events and respond to other incidents. As a matter of course, it is always possible to counter attackers, but never possible to avoid an attack which is yet to be launched.

Some solutions to the problem of providing dynamic security in complex systems exist [8]. Still though, some questions have been raised. One of the important questions could be formulated as: how should a security system capable of analyzing and adapting functions and components to deal with large security tasks, systems and contexts be designed?

Firstly, this question is explicitly a cross disciplinary issue that impedes the development of a common solid system. However, solid foundations exist for further research and development [9].

Our work is based principally on reference monitors [10], adaptive security frameworks [11], and control theory [12].

The model already described is illustrated in Figure 32

![Figure 32: General model of autonomic Adaptation architecture](image)

Here we have a feedback loop composed of a detector device (sensing), analyzer devices (analyzing and deciding), and a responder device (acting). This is the basic model of an autonomic element.
We will aim to answer the question of how security aspects should be handled at the distributed level. We will design a foundation for a generic security adaptation framework.

### 5.2.2 Adaptive Framework

As described before, current systems either suffer from a number of drawbacks in terms of their overall security capacity and dynamism, or else they are highly specific, addressing a single security issue. Hence with the current setup, total security is far from achievable. We propose a security adaptation framework for wireless environments which we call a Security Adaptation Reference Monitor (SARM).

The concept of isolating various functions and restricting their access to specific systems can also be applied to security in wireless environments, integrated within the operating system itself, using a cross-layer security approach. The main focus of our concern is the adaptation of the successful concept of reference monitor to deal with mobile and wireless communication security. Moreover, the best way to overcome the unrealistic goal of implementing the framework for each communication program would be to integrate it in the kernel, and consequently have overall security control. Thus, all communication programs would have to interact with the SARM in order to gain access to communication resources.

**Why a generic framework**

To implement and choose an adaptive security system depends on a number of factors, which are correlated [13]:

1. Cost of acquisition
2. Cost of maintenance
3. Usability
4. Effectiveness

We need a structured approach in order to tackle the problem of satisfying the abovementioned requirements, and thus implementing an efficiency security system. The approach must be based on modular building block methodology so as to allow easy integration and to hide the complexity of the internal adaptive security system. Moreover, this approach allows for gradual expansion to meet the requirements of ongoing expansion elsewhere. In order to react in real-time to any threat, feedback information is needed. This would also reduce the amount of human intervention, which generates human errors.

**The system**

Three principal components of the autonomic system (p.83, Figure 26) have been identified in the design of our Framework. These have been extended based on adaptation security architecture.

We might describe an adaptive security system as a quintuple system [14]:

---

**Design and Methodology Description of the Framework**
Design and Methodology Description of the Framework

AS = (A,X,Q,Up,Uf)

**Table 12 : Adaptive security model description**

<table>
<thead>
<tr>
<th>Quintuple : AS</th>
<th>Description</th>
<th>Splitting</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Component framework model</td>
<td>Components and set of properties</td>
</tr>
<tr>
<td>X</td>
<td>Context</td>
<td>Computing, Physical, User</td>
</tr>
<tr>
<td>Q</td>
<td>Adaptivity model</td>
<td>QoS and security related dimensions</td>
</tr>
<tr>
<td>Up</td>
<td>User preferences</td>
<td>User security satisfaction level</td>
</tr>
<tr>
<td>Uf</td>
<td>Adaptation strategy</td>
<td>Utility function to maximize performance</td>
</tr>
</tbody>
</table>

**Figure 33: Breakdown of Adaptive quintuple model**

In Figure 33, we find the component breakdown of the adaptive system model:

- **A** is composed of components of the system and a set of properties. These components belong to either a set of non security related components or to a set of security components. The components are annotated with properties related to QoS or to security.

- The context refers to the circumstance of any interaction between a user and the system.

- Adaptivity dimensions: QoS and security dimensions provide a high-level network user's view of the system.

- The User Preferences express user constraints and requirements (a sort of wish list).

- The utility function expresses the quality of adaptation for a given user/users.

Now that we have explicitly defined the elements of an adaptive system, we will map them into an autonomic system. For the Functional unit, we add user preferences and divide the security means into those that are application dependent and those that are not (application independent). Afterwards, we add...
a sensing element to factor in the context.

For the Management unit, we add policies and logs for short- and long-term security or QoS security analysis and monitoring. The block risk, vulnerabilities and performances are based on the risk management module defined in Figure 30 of Chap.4.

![Figure 34: Foundations of our adaptive security Framework](image)

We have depicted our generic Framework in Figure 34. It is comprised of two units which are based on the concept of the reference monitor so as to ensure the security of any network.

### 5.3 Discussion of SARM

The key challenge for SARM is to adapt the Reference Monitor (RM) and autonomic system concepts to wireless communication and beyond, including data access control. The goal of a RM is to enforce security by preventing all processes and users from accessing any data except through the reference itself. The security kernel is managed by security policies. We have also chosen to apply the autonomic computing security pattern [15] in the design of SARM by
dividing it into a functional unit and a monitoring unit. The Framework is adapted to a cross-layer security approach. As a result, the Framework will reduce overheads even at very high levels.

To reduce the system’s complexity and to make the system incremental, we propose a feedback loop framework as introduced in [16] at the authentication level, that is, the system will automatically tune to its best configuration based on its particular monitored context, thus avoiding any static decision making. Hence, the SARM is split into two units looped in a servo control system model in order to fine tune the adequate security measures/means, which we will discuss later. One unit, called the management or monitoring unit, monitors the context by evaluating and analyzing risks, performance, and energy consumption, which are significant for detecting attacks, and tunes the adequate security means using the second module, which is called the functional unit.

### 5.3.1 Security Means

As depicted in Figure 35, security means are defined as any algorithm or mechanism that could ensure security but that also has the capacity not to take security action unless it is actually necessary. It also includes the choice of adequate network access, because some network communication technologies are more secure, with higher levels of energy consumption, while others are less secure, with lower levels of energy consumption. Security means can be application-dependent, as in the case of localized trust [17, 18] or distributed trust [19], or application-independent, as with cryptographic protocols. Indeed, localized and distributed forms of trust are good paths to explore because they generate low-computing charges (less energy consumption) and in some cases give better results. Thus they fit the context of WSN, for example, perfectly.

Let’s start with a use case of the Framework for WSN: firstly, the application uses communicative means. The default preferences relating to the chosen application are followed. Secondly, the context gathering module collects all information about the application’s current context. This information is then sent to the Monitoring/Management Unit, which is responsible for all security analysis in accordance with the security policies based on log files at a first stage, and risks, vulnerabilities, and energy consumption at a second stage. The logs are used to store all the information about the system, but mainly about security problems. Risk, performance, and energy consumption analysis with policies is a key issue in the Framework because it is responsible for detecting potentially unsecure contexts, probable energy wasting environments, and/or particularly vulnerable applications.

Thus, the analysis could delve into a trade-off between all these constraints to choose an efficient action to tune the functional unit.
Our second use case is for WI-FI: we start firstly with a user who chooses an application that could be a location-based service, or a gaming, banking or other application that needs a communication interface. The user has personal preferences for the chosen application. Secondly, the Context Gathering module gathers all information about the context in which the application is being used. This information is then sent to the monitoring unit. Thirdly, the monitoring unit is responsible for all security analysis in accordance with the security policies at the first stage, and risks, vulnerabilities and performances at the second stage. The security policy is expressed in a standard form in order to offer a number of potential advantages. This policy should be deployed and maintained so as to save time and complexity and make centralized system management more feasible. In addition, risk, performance and vulnerability analysis is a key issue in the Framework because it is responsible for detecting potentially insecure contexts, environments that are potentially wasteful of energy, and/or particularly vulnerable applications. Thus, the analysis could attempt a trade-off between all of these constraints in order to choose an efficient action in the adaptation action to tune the functional unit.

In the end, the functional unit is responsible for selecting adequate security means, like efficient network access. The device will then adapt its security so as to have the most efficient mechanisms. In doing so, the loop will make the communication system more self-managing in terms of security and more accurate in coping with any dynamic changes in context.

This autonomous security Framework is thus well-adapted to react dynamically during runtime, depending on the security parameters and context. In fact, a trade-off between security and performance is also carried out.
Moreover, the control system of this Framework is ideal for a collaborative environment wherein the decision making function of security must interact with other users in order to come to an adequate decision.

5.3.2 Trust and reputation as means of SARM

How to build reputation Network Architectures

There are two main forms of reputation architecture: centralized and distributed. The first of these is a reputation system that gives information about the performance of a particular agent after collecting ratings from other agents and evaluating his reputation. Indeed, the central authority is responsible for collecting ratings from other agents about their direct experiences with the evaluated agent. The second system is a distributed system which has no central procedure for the submission or receipt of ratings. However, each agent rates his own experiences, and whenever one agent wants to know the reputation of another, he must look for distributed scores or try to obtain ratings from as many agents with direct experience of that agent as possible.
Formalizing the rating process

The environment is a field of many agents connected by a network. Trust can be computed based on personal experience or second hand information, or a combination of both.

A model for the abstract rating process is taken from [20] proposed by Mui:

Two sets of elements, agents and objects, exist together in an environment. Objects can represent agents.

\[ A = \{a_1, a_2, \ldots, a_m\} \]
\[ O = \{O_1, O_2, \ldots, O_n\} \]

\[ \rho: A \times O \rightarrow S \]  \hspace{1cm} \text{Equation 7} \]

The rating is \( \rho \), where \( \rho_{ij} \) represents the rating by agent \( a_i \) on object \( O_j \).

Reputation learning

The reputation of an agent is calculated according to ratings from other agents based on encounters between them. Updating trust is done with respect of a rule.

Let \( \rho_{ij} \) be the rating that agent \( i \) gives to agent \( j \) with respect to a particular context. Assume that \( \rho_{ij} \) has been updated. \( \rho_{ij} \) and \( \rho_{jk} \) are agent \( i \)'s ratings of agent \( j \) and agent \( j \)'s ratings of agent \( k \), respectively. Agent \( i \)'s rating of agent \( k \) can be expressed as:

\[ \rho_{ik} = f(\rho_{ij}, \rho_{jk}) \]  \hspace{1cm} \text{Equation 8} \]

Where \( f(\cdot) \) is a rating function for inference across 2 edges.
Centrality based Rating (Thesis)

![Network Diagram](image)

Figure 38: A network of three vertex and oriented edges

\[ \rho: A \times O \rightarrow S \]

\[ A_{3 \times 3} = \begin{bmatrix} 1 & 0.2 & 0 \\ 0 & 1 & 0.8 \\ 0.4 & 0.9 & 1 \end{bmatrix} \]

The ratings that can be represented by matrix A and \( a_{ij} \) are agent i’s ratings of agent j, assuming the fact that each agent has a positive view regarding his rating. Then, the diagonal of the matrix A is always 1.

If \( x \) is the vector of reputation values for the network overall and \( x \) the reputation value for agent i, let \( n \) be the number of agents.

Reputation vector is \( x=[x_1, x_2, \ldots, x_n]^T \)

The rating process by the entire network for agent i is:

\[ x'_i = a_{1i} + a_{2i} + \ldots + a_{ni} = A^T x \]

Equation 10

The problem can be solved by its stationary values based on the eigenvalue \( \lambda = 1 \):

\[ (A^T - \lambda I)x = 0 \]

Equation 11

The main problem is that Equation 11 does not always have a steady state solution due to the fact that eigenvalue 1 may not exist.

Like the Markov matrix, the A matrix has an eigenvalue 1 if each column is normalized to a sum of 1. Therefore, the related eigenvector is the reputation of the corresponding agent. All agents that have higher values are selected as very reputable agents and are recommended to all members of the network.

Quantitative models

The subjective logic of Josang [21] is defined below.

The model enables ratings to be formulated based on four basic values:

b: belief (trust)

d: disbelief (distrust)
Where \( b+d+u = 1 \) and \( b, d, u \) and \( a \in [0,1] \).

The opinion about the truth of \( x \) is a \( w \) \( (b, d, u, a) \).

The probability expectation value of an opinion is defined as \( E = b + a.u \)

![Figure 39: Josang belief represented as triangle](image)

The opinion might be practically represented as an equilateral triangle. A point inside the triangle represents a \( (b, d, u) \) triple. The \( b, d, u \)-axes run from one edge to the opposite vertex indicated by the Belief, Disbelief or Uncertainty label within \([0, 1]\). For example, a strong positive opinion is represented by a point towards the bottom right; \( E \) is formed by projecting the opinion onto the base, parallel to the base rate projector line. Beta distribution B-pdf are normally denoted as Beta (\( a, b \)) where \( a \) and \( b \) are its two parameters. The Beta distribution of an opinion is defined in Equation 12.

\[
\beta(\alpha, \beta) \text{ where } \begin{align*}
\alpha &= \frac{2b}{u} + 2a \\
\beta &= \frac{2d}{u} + 2(1-a)
\end{align*}
\]  

Equation 12

Thereafter, average and variance values can be used based on Beta pdf. Furthermore, different opinions are combined via operators that manipulate the basic values of trust.

**Binary Ratings**

We have \( \rho_i(c) \), denoting agent \( i \)'s rating of context \( c \), and let \( \rho_j(c) \) be agent \( j \)'s rating of context \( c \). If \( \rho_j(c) \in \{0, 1\} \) then the rating is binary, 0 for disapproval and 1 for approval. We considered the function that indicates whether \( i \) approves of \( j \):

\[
\rho_{ij} = \begin{cases} 
1 & \text{if } \rho_i(c) = \rho_j(c) \\
0 & \text{otherwise}
\end{cases}
\]  

Equation 13

The inference function \( f(.) \) can be derived from 2 links, see below.

\[
\rho_{ij}(c) = f(\rho_{ij}(c), \rho_{jk}(c)) = \rho_{ij}(c).\rho_{jk}(c) + (1 - \rho_{ij}(c)).(1 - \rho_{jk}(c))
\]  

Equation 14
Using recursivity, we can calculate the propagated rating for agents that are more than 2 links away.

**Simple Summation (Binary Ratings)**

The simplest way to compute reputation is to add up all the positive scores and subtract the negative scores. In this way, anyone can understand the function of trust.

In this model, only 2 ratings are possible, positive equal to 1 and negative equal to 0. The set is $\mathbb{S} = \{0, 1\}$ and the rating is $\rho_i \in \{0, 1\}$.

This is the principle of eBay's reputation forum which is described in detail in [22]. Another model is proposed in [23] and computes the reputation score as the average of all ratings; a similar model is used by Amazon, for example.

**Other Approaches**

There are many other Trust and reputation approaches, such as Continuous Rating, Bayesian Systems, Discrete trust and the Fuzzy model. Article [24] gives a good summary.

### 5.3.3 Digital identity as means in SARM

To ensure safety and security when accessing a system, a mechanism to identify both the users and the system was introduced that was to be exploitable by everyone, everywhere. Moreover, this solution put the user at the center of the system, which is the fundamental of the user-centricity requirement.

All the identity systems will be able to coexist and each of them offer sufficiently unique capabilities that will allow them to flourish independently to some extent. In spite of these unique capabilities, there is a significant degree of duplication of functionality across the various systems. Convergence between the systems would eliminate such duplication and result in a simpler identity landscape. Higgins and the Liberty Alliance project offer positive conceptions of convergence.

The identity management panorama is changing rapidly. On one hand, classic identity management components are consolidating; on the other hand, new components and standards are emerging, like identity federations and user-centricity.

Identity management is also gaining importance. In the future, identity management solutions based on federated architecture and user-centric paradigms combined with mobility will play a more central role in the IT industry, mainly in the mobile field. This is why a mobile identity management system must be integrated into the means of SARM.

For practical reasons, we have in article [31] a survey of identity management and mobility. In this article, the ongoing research into identity management and mobility is discussed. We define a research problem and outline a basic model. We indicate the necessity of mobility and the importance of identity in the field of
future ambient intelligent environments. The research target is any mobile service provider; however the first beneficiary is the user due to the facts of usability, privacy and mobility. We move forward in our research and define Mobile identity management requirements. The MId implementation must support a wide range of information technologies and devices with the critical goals of high scalability, reliability and usability. The emergent technologies should also be taken into account when building the concept of mobile identity 2.0, mainly in the field of ambient intelligent environments. Thereafter, a summary of the identity management initiative is provided.

### 5.3.4 Summarizing Table for identity management

The 10 requirements at the top of the following table are those discussed in the article [31]. In this table, white means that the requirement is not covered, grey that it is partially so, and black, that it has been fully fulfilled.

At the moment, designers have to choose between many authentication and identity management systems and users are left to face the inconvenience of a variety of digital identities. While the main initiatives have different priorities and some unique advantages, they overlap in many areas. The most pressing requirements for users are interoperability, usability and user-centricity principles. Thanks to Higgins, the majority of identity requirements are guaranteed. Therefore, the user is free to visit all access systems without having to worry about the identity management system used by the provider.

<table>
<thead>
<tr>
<th>Requirements</th>
<th>XRI/XDI</th>
<th>ID/WSF</th>
<th>Shibboleth</th>
<th>CardSpace</th>
<th>OpenID</th>
<th>SXIP</th>
<th>Higgins</th>
</tr>
</thead>
<tbody>
<tr>
<td>Empowering users’ total control of over their privacy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Usability, as users can use the same identity for each identity transaction</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Giving a consistent user experience thanks to uniformity of identity interface</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Limiting identity attacks, i.e. Phishing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Limiting reachability / disturbances, such as spam</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reviewing policies on both sides when necessary, identity providers and service providers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Huge scalability advantages as the Identity Provider does not have to have any prior knowledge of the Service Provider</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assuring secure conditions when exchanging data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Decoupling digital identity from applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pluralism of Operators and Technologies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5.4 High level SARM

5.4.1 Methodology Design Approach

The methodology was designed using a high level, top-down approach in order to find the most suitable solutions. We have characterized each wireless network studied in order to appreciate the objective and security requirements of each one, while using the same framework to test them. This might be done through theoretical tests, simulations or field tests. Metrics are needed during these tests in order to analyze the impact of security on resources.

5.4.2 Verification of Methodology

For the purpose of verification of the methodology, a validation and consolidation process should be run for the designed Framework. The Framework also needs to be compared to other frameworks, or to approaches in other areas of research. Our Framework is based on Autonomic computing and adaptive security. The background of the methodology is described more completely in Chapter 1 and 4.

5.5 Discussion and summary

Our Framework is intended to provide adaptive architecture, mechanisms and algorithms to satisfy overall performance. As such, it provides adequate security protection at all levels. Our Framework attempts to provide reasonable means and solutions for environments where devices operate under constraints and are thus unable to provide sufficient security. As a matter of fact, our Framework aims to offer the most adequate security level. Degradation of security is then possible if the policy, user preferences and energy requirements can be satisfied. Moreover, our Framework is designed to adapt security levels based on application security requirements. Accordingly, the system functions with minimum security requirements, despite the threats and vulnerabilities, in accordance with overall performance and constraints.

This chapter describes the design of SARM and explains its internal architecture, which consists of three modules (control system): a functional unit, a management unit and a context sensing unit. The context sensing unit gathers information from the environment. The functional unit is responsible for choosing adequate security means as well as for efficient network access. The management unit is responsible for all security analysis in accordance with the security policies at the first stage, and risks, vulnerabilities and performance at the second stage. The intended security means in the Framework is presented for two cases: a. trust and reputation, and b. identity management initiatives.
5.6 REFERENCES


4. D. Djenouri and N. Badach, “A Survey on Security Issues in Mobile Ad hoc Networks” Research report, Computer Science Department, University of Science and technology, Algiers, Algeria, 2004


Chapter 6. Implementation and experiments

“...education fails in so far as it does not stir in students a sharp awareness of their obligations to society and furnish at least a few guideposts pointing toward the implementation of these obligations.”

-Mary Barnett Gilson, “Social responsibility education”.

The previous chapters describe a methodology intended for the use of users or system developers to determine *ab initio* the most suitable adaptive security and access means for different categories of wireless networks. This chapter will describes some principal resource costs for security and some applications of SARM. The results of section 6.2 will be used in the simulations of the next chapter.

6.1 Introduction

As mobile and wireless networks have become increasingly heterogeneous and particularly dynamic, the requirements in terms of security and performance must be addressed in a flexible manner but also in a dynamic way to deal with the evolution of the system in real time according to its context. In addition, the evolution of using smart phones privately and professionally highlights the urgent need of improving security of communication and data.

Currently, mobile phones have become real computers, but unfortunately, with less security. Hence the existence of multiple flaws such as ease of misuse of resources, total control of communications, especially SMS, etc...

The increasing number of applications and devices make security more relevant in this field. However, providing security faces challenges because of the severe limitation of CPU utilization related to communications, memory and resources. In fact, security is resources consuming, particularly in wireless Sensor Networks.

The basic idea is to integrate SARM in phones to deal with extremely dynamic security conditions while maximizing performance based on policies, preferences and risks associated with different contexts.

The overall objective of our work is the exploration of SARM to secure transmissions, voice, data of mobiles phone such as Android. The principal objective is to use external cryptographic tamper-proof system based on Smart Card (SC) SD, which supports data encryption mechanisms and protected memory.

SC is a card that securely manages and stores information separately from the rest of the device’s components.

In a SC-SD, man can find security platform delivered through a secure microSD
processor. The main objective is to integrate SARM in this smart card to protect voice and data infrastructure, preventing loss or theft of sensible data, vital information and proprietary assets. Another objective aims to increase the awareness of the costs using encryption and access networks.

Figure 40: Architecture of SC-SD

6.1.1 Analysis of Resource costs for security

Motivation

For a long time, security has been treated as a static component in system design, with static security assessment assumed to protect the system throughout its lifetime and assuming that energy is unlimited. However, this assumption does not hold anymore because devices are disconnected from power line and they are in battery mode that has limited live time. Reference [3] declares that Wi-Fi devices consume 30% more energy than normal mode. In [4], we find a complete study of energy consumption in mobile phones and it is proved that a 3G connection consumes from 5 to 10 times more energy than Wi-Fi. In addition, the problem of energy is a key issue in sensor network [5]. Therefore, the security cannot be considered without other context aspects especially energy awareness.

Data and telephony

Data security has become a major concern for all users, particularly for applications in Self-Organization Network field, because they require many security features adapted to their wireless transmission. Different kind of security mechanisms and strong cryptographic algorithms are available to prevent any violation of data security. Unfortunately, these security capabilities are time and
energy consuming. Indeed, certain algorithms and mechanisms are strong enough to protect largely the data but at the same time reduce severely battery lifespan. That’s why an adaptable platform for mobile device will save energy and reduce the delay to fit to the limits of a real time range; mainly for telephony application.

In this respect, to deploy VoIP so that users receive an acceptable level of voice quality, VoIP traffic must be guaranteed certain compensating bandwidth, Jitter, and packet loss.

According to G.729 [1], codec requires packet loss far less than 1% to avoid audible errors. ITU G.114 [1] specification recommends less than 150 ms one-way end-to-end delay for high-quality real-time traffic, such as voice; and for Jitter buffers, varying delay, further add to the end-to-end delay, and are usually effective only on delay variations of less than 100 ms.

Thereby, the delay must be less than 100 ms, which is a significant constraint for mobile device.

The goal of our analysis is to integrate cryptographic algorithms and security mechanisms in SARM in order to implement them in a SC-SD memory card. Thereby, our SARM means will be chosen perfectly according to context. This will help designers and developers to fit timely the users’ preferences and policy in order to have efficiency application and security system. That’s why we have carry out experimental measures to compare energy consumption of different algorithms and access networks. Based on the results, we could adapt timely our SARM means to policy and user’s preferences. In this respect, we increase the efficiency and validation of the Framework.

6.1.2 Assumptions and experiments

There are three techniques for performance evaluation:

I. Analytical
II. Simulation
III. Measurement

Simulations offer less accuracy than measurements. For this matter, we have previously developed hardware and software to measure energy consumption. That’s why we have privileged the measurement instead of analytical or simulation methods. Analytical technique is complicated due to the fact that this method needs more precision and required more time. We have made several assumptions to limit the scope of the study and also to keep the implementation and complexity reasonable. Anyway, further studies are needed to consider an overall evaluation.

We use commercially available mobile phones with a SC-SD for the SARM.
### Table 14: Main characteristics of experiments

<table>
<thead>
<tr>
<th>Phone</th>
<th>Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Galaxy S3; GT9300</td>
<td>WLAN or Cellular network</td>
</tr>
<tr>
<td>Android version 4.1.2</td>
<td>803.11g; GSM/UMTS/G4</td>
</tr>
<tr>
<td>Battery: 3.8 V; 2100 mAh</td>
<td>Protocols: Data channel (SIP/RTP); SMS;</td>
</tr>
<tr>
<td></td>
<td>switched channel, voice PCM G.711 (64 kbit/s)</td>
</tr>
</tbody>
</table>

#### 6.1.3 Metrics and Measurements Methods

Our focus is to determine the impact of cryptographic algorithms and use of different access networks on battery resources. We will explain the methodology of the measurements.

**Encryption Latency**

We will evaluate the latency of some means in SARM, such as identity. The latency is the time to encrypt a block cipher or a file calculated based on a time function.

**Energy Consumption**

![Figure 41: Scheme of experimental energy consumption circuit](image-url)
To measure the current level, we have developed an electronic card capable to measure a low current level via low precision resistor \((r=50\, \text{mOhm})\) in series between battery and the mobile phone. The electronic card uses many low noise amplifiers \((\text{gain } =200)\) and has an USB interface in order that data will be directly accessed from a PC. The equivalent circuit scheme is shown is Figure 41.

The most known problem of battery detection mechanisms was bypassed by using all four battery’s connectors; otherwise they will be no power. At the same time, to avoid battery fluctuations we have connected the battery to DC adapter. The time of a single measure is 2500 times by a second. The Figure 42 illustrates the details of the experiments.

![Image of experimental setup](image)

**Figure 42: Experimental test-bed energy consumption**

To calculate the power via our method we must:

Take the measured voltage via the PC \(V_{PC}(t)\) and divide it by the amplifier gain 200 to have \(V(t)\)

\[
V(t) = \frac{V_{PC}(t)}{200} \quad \text{Equation 15}
\]

then apply the equation

\[
P(t)=V(t) \cdot V(\text{battery } = 3.8) / r(50\, \text{mOhm}) \quad \text{Equation 16}
\]

Finally, we use Equation 17 to calculate the power:

\[
P(t)= V_{PC}(t) \times 0.38 \quad \text{Equation 17}
\]
6.1.4 Results and Discussion

Identity management

We have studied all Identity management platforms [6] and we have had a good background in this field as a means in our Framework.

We have implemented a test-bed based on WLAN network and mobile phones. The main goal is to know the time consuming difference between a secure and non-secure connection. The results are shown in Figure 43. The requirements of this experience are:

I. E65 telephone
II. WLAN 802.11b, D-link Access Point
III. Tomcat server
IV. SAML [2 ]Token and SSL secure connection

![Download time](chart.png)

**Figure 43: Download time of different files (sec, non-sec.)**

Figure 43 shows the download time average difference between secure and non-secure for different file sizes. In all cases, the difference between secure and non-secure is ranged from 10% to 15%. For each measure, the specific file download is done 30 times. The standard deviation is less than 1.7%.
Energy

Voice Communication energy cost
We have carried out an end to end voice encryption, which is very important to secure in mobile network mainly that any telephony call is not protected at all inside the GSM network.

![Configuration of SARM experiments](image)

Figure 44: Configuration of SARM experiments

We have implemented the system with these elements:
I. Commercially smart card SD for encryption,
II. SIP protocol for signaling,
III. RTP for ToIP, and
IV. Data channel.

Results and analysis
All energy metrics are based on experiments with Samsung S3 Galaxy.
The graphs in Figure 46 through Figure 47 each shows power consumption for a voice encryption. A voice packet is based on 20ms and 64kbit/s, which gives a 160bytes size.

In Figure 48 illustrates that Blowfish cipher has the highest encryption energy
Implementation and experiments

Consuming for 20ms encryption block which seems to be less efficiently with small block, because it uses one function to process the entire buffer of plaintext. For larger files, Blowfish is more efficient which is more adequate for voice encryption.

AES is the more energy consuming for long block. However, it is the strongest in term of cryptographic properties.

In all cases, the difference between secure and non-secure is ranged from 12% to 20%. Moreover, for each measure, the specific measures are done 30 times. The standard deviation is less than 1%.

Figure 45: Power for idle mode
Implementation and experiments

Figure 46: Power for voice transmission without encryption

Figure 47: Power for AES voice encryption
Access network energy consumption

We must have an overall view about the energy consumption of security utilization in order to tune the best security means and also to choose the best access network depending on the context, user preferences and policies. [3,4,5]

Table 15: Energy consumption for mobile networks (20s, 50 KB)

<table>
<thead>
<tr>
<th>Network</th>
<th>Energy consumption [J]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bluetooth</td>
<td>~2</td>
</tr>
<tr>
<td>2G (max)</td>
<td>5</td>
</tr>
<tr>
<td>WIFI</td>
<td>(7.6) 30% more than 2G</td>
</tr>
<tr>
<td>3G</td>
<td>(12.5) 2 to 6 times WIFI</td>
</tr>
<tr>
<td>4G (our approach)</td>
<td>(20) 2 to 3 times 3G</td>
</tr>
</tbody>
</table>

Table 15 describes the power consumption for different mobile networks. We can see clearly that the power consumption is going increasingly within the new cellular network generations. We argue that the next satellite cellular generation will consume more energy. That's why we see the importance of applying our Framework to data and telephony communications, particularly in SONs.
6.2 Conclusion

This chapter was a foundation for all simulations and evaluations of the next chapter. Indeed, it gives us a solid background to launch the simulations of the Framework SARM based on the tuning of the security means related to the accurate energy and access network consumption tradeoffs. Besides, the experiments have given us the opportunity to study a full end-to-end secure telephony connection based also on SARM and SC-SD and thus to have an overview about the real application of SARM. Nevertheless, we need further studies of the Framework for real applications, different contexts, and diverse access networks and energy consumption.

6.2.1 Summary

In chapter is a set of measurements of SARM are launched based on implementation in the field of security. We establish a secure connection based on a tamper resistance SC-SD secure card. The energy consumption is accurately evaluated. In short, the proof of concept of SARM was based on implementing it in a tamper resistant security module based on a Secure Digital Card.
6.3 REFERENCES

1. ITU-T recommendations to find at http://www.itu.int


Chapter 7. Simulation and Evaluations

“An indirect quotation, we can usually expect to rate only as better or worse, more or less faithful, and we cannot even hope for a strict standard of more and less; what is involved is evaluation, relative to special purposes, of an essentially dramatic act.”

-Willard Van Orman Quine, “speech acts”

“Good critical writing is measured by the perception and evaluation of the subject; bad critical writing by the necessity of maintaining the professional standing of the critic”

-Raymond Chandler

This chapter describes some implementations of SARM with the intention of providing some validation. The simulation tools are used to validate and animate different user cases relating to different networks and environments. The simulations and analysis demonstrate the feasibility, potential uses, and limitations of SARM and its associated concepts.

The chapter is divided into six main sections. Firstly, we explain the validation process of SARM. Section 7.2 describes the first validation context of Wi-Fi. Then, in Section 7.3 we depict the trust and reputation approaches applied to Hotspots rated and ranked with SARM. Section 7.4 discusses the use case of applying SARM in WSN networks. Next, Section 7.5 describes the use case of SARM in the service of Green 2.0. Then in Section 7.6, we conclude our simulations work. Section 7.7 is fully to comparison of SARM with relevant works.

Finally, Section 7.8 summarizes the overall validation process.

7.1 Validation process

We have tested our Framework for different cases: means and contexts.

The validation process in this work was executed through simulation and collection of measurements (see last chapter). However, simulation typically provides less accurate results than analytical evaluation, which was ruled out due to the high level of precision and large amount of time it would require.

We have chosen simulations because they are less costly and time consuming, particularly if the simulation tools can be mastered. In this respect, we have lengthy experience (more than 10 years since the first version) in using and developing simulations through Anylogic, which is a strong simulation tool. It is used by more than 200 universities and in many industries around the world.
7.1.1 Simulation tools:

AnyLogic is a simulation tool that supports all the most common simulation methodologies in place today: System Dynamics, Process-centric (a.k.a. Discrete Event), and Agent Based modeling. It is based on Real-time UML and Java object-oriented language. AnyLogic is a programming and simulation environment, mainly aimed at the modeling of hybrid systems. The unique flexibility of the modeling language enables the user to capture the complexity and heterogeneity of social systems with any desired level of detail. These characteristics matched our simulation development needs exactly. Moreover, AnyLogic’s graphical interface, tools, and library objects allow for quick modeling in diverse areas, such as network management, resource optimization, and consumer and/or patient behavior.¹

In our case, we have used Agent Based modeling because it corresponds to our final goal of simulating the overall characteristics by only describing the behavior of each category of devices described in table 1. Moreover, the mobility is based on a random mobility model and excludes other locations within the chosen area of Geneva, such as the lake.

7.1.2 Model Set-up

The basic element of an Agent Based model is the agent itself. This is done in AnyLogic by creating a new class than behaves as an Access Point. Each device is associated with a given agent matching its location. As the device is not static, we have modeled its mobility using X and Y random variables.

The movement and the status of our agents are controlled by state-charts which represent the exact behavior of the device.

Setting up our security model, it is possible to take advantage of state charts in order to control agents’ behavior. Using AnyLogic as an implementation platform, agents and especially state-charts can be programmed very conveniently. In particular, modifications and/or extensions of the final model can be handled in a simple way.

7.1.3 Experiment methodology for Wi-Fi

In all the experiments conducted for Wi-Fi, we validated the proposed mechanisms and analyzed the extended performance based on a range of varying mobility scenarios. All of the simulations were run using a wireless network composed of 1,000 nodes moving over a rectangular 8.69km x 6.08km topography, and operating over one day of simulation time. In our simulations, we considered that the APs were those taken from Geneva Hotspots. We also considered that the WLAN APs showed greater reliability than mobile nodes, in having an unlimited amount of energy and a uniform transmission range. The communication range of APs was configured to be 100 meters. Each mobile device was also configured to have a communication range equal to 100 meters.

¹ http://www.xjtek.com/anylogic/
We deployed the APs in an incremental mode, from AP1 to APn, in the exact position taken from the true GPS position. Thus we estimated the impact of our mechanisms for an existing network based on the behavior of mobile devices and on overall network performance.

The movement pattern of mobile clients was totally random, to conform to a real Hotspot application. To achieve this, we used the Random WayPoint (RWP) mobility model [1] with pause time equal to the time needed for network access and data transfer. In our simulation, each mobile device initially published its security value and calculated its own Decision Making Function in order to decide whether or not to use a secure channel. In the case of a security failure, the device was ranked as compromising security and in the case of power failure it was ranked as energy wasting.

We carried out our experiments for thirty cases. In each studied case, the simulations were conducted using different Decision Making Functions. Our performance evaluation was the result of 1000x30 different simulations.

The first step was to assign to each Agent a state according to a predefined percentage fixed in our scenarios.

Figure 49 shows a very powerful animation interface created using AnyLogic. Note that the Access Points and forms of devices are described in Figure 50. In the background of the animation, the Hotspots APs are located according to their GPS coordinates on the map of Geneva.

7.2 Use case: Wi-Fi hotspot simple approach

In the past few years, Wireless Local Area Networks (WLANs) have become the
major wireless networks in many cities. Their spread in many locations like airports, cafes, businesses and university campuses has expanded their utilization. This ongoing spreading, coupled with the inherent vulnerabilities of the deployed protocols, has brought about more breaches of security. In addition to the typical network threats, wireless networks present several challenges and potential forms of attack. This is due to the broad, open air nature of the channel which allows for more attacks, as well as bandwidth limitations and constant topology changes on account of node mobility. In such networks, the security requirements are high because of the vulnerability to so many kinds of attack. In this case, the basic security mechanisms may not be sufficient.

SARM’s Decision Making Function (DMF) is utilized to deal with the problem. Indeed, we tackle the abovementioned constraint issues by implementing a simple adapted security mechanism, respecting overall performance.

7.2.1 System Model

In IEEE 802.11, the privacy of devices in a given radio domain can be compromised if the AP identity is spoofed. This security breach is now very easy to deploy by using a soft AP. In addition, there is a great temptation to use PKI to secure the channel. However, it would be so time and energy consuming that a more easily deployable solution should be proposed.

Some solutions could be implemented based on trust management [2, 3], but they need to hold and manage a lot of values. Simple solutions should be implemented, evaluated and eventually strengthened in order to save energy and maximize the use of the network’s resources overall.

As some values should be published in order to decide whether or not to use security, one might be tempted to cheat by behaving maliciously, firstly by forcing users to secure their connection even if no security is necessary because there is no risk of depleting the mobile user device energy; secondly to push users not to be secured in order to compromise their privacy or security in general. This dissertation investigates how to determine when to use a secure connection and when to use a non-secure connection, especially in light of the trade-offs between security and performance.

7.2.2 Decision-Making Function

We assume that each AP periodically collects information related to active users during short intervals of time that we have called monitoring periods (their length is not discussed in this dissertation). A series of binary values are published by each user, and we can assume that some of them are collected by each AP. The Decision Making Function (DMF) then handles these values and decides whether a secure connection is necessary or not.

This method presents several advantages. First, the tests are very simple, and consume minimal time and energy. Second, new tests could easily be added to mitigate other malicious behavior.

The DMF is typically a statistical test that determines the security of the connection between the AP and the users. Trust values are collected previously
in order to judge whether a transfer should be secured or not. The DMF can do something as simple as comparing two values or can mean the use of a more complicated technique.

The main objective of this use case is to apply SARM in order to support mobile clients' security and their ability to seamlessly access the Internet near public WLAN Hotspots, even when some attacks happen. The locations of Hotspot APs in our simulation correspond to real positions based on GPS coordinates of Geneva.

7.2.3 SARM evaluation

We have evaluated SARM in the context of proximity based wireless networks through the Anylogic simulation tool for the case of Geneva hotspot locations. The results show that SARM is efficient in terms of security, overall network utilization and power consumption.

![Figure 50: Simulation scenario WIFI](image)

Before using an AP, each device will publish a binary value and will read the published values of other devices within range of the access point.

<table>
<thead>
<tr>
<th>User Behavior</th>
<th>Recommended action for neighbors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>Don’t secure: 0</td>
</tr>
<tr>
<td>Trying to waste neighbors’ energy</td>
<td>Secure : 1</td>
</tr>
<tr>
<td>Trying to compromise neighbors’ security</td>
<td>Don’t secure : 0</td>
</tr>
</tbody>
</table>

Our solution consists of choosing a function that predicts whether or not to use a secure connection based on the average of the published values of each device.
within range.

\*T_a(v, threshold) = \text{Sum(value/number of devices within a given range)}; \text{if } T_a(v) > \text{threshold then a secure connection should be used; if not, a non-secure connection can be used.}

There are other interesting functions that can also be taken as references:

The first is security in every case, even when there is no threat and the second is no security in any case. Another interesting case is a randomly chosen value that determines whether or not to use security. Ultimately, we introduce a security case with a 50% threshold which is useful for comparative purposes.

\*T_1(v) = 1 \text{ the result is equal to one for whatever value are published by users; secure connection in all cases}

\*T_0(v) = 0 \text{ the result is equal to zero for whatever value are published by users; non-secure connection in all cases}

\*T_r(v) = \text{random (0,1) for any published value; if } T_r(v) = 1 \text{ then we use a secure connection and if } T_r(v) = 0 \text{ then we use a non-secure connection}

\*T_a(v, 50\%) = \text{Sum(value/number of devices within a given range); if } T_a(v) > 50\% \text{ then we use a secure connection; if not, we use a non-secure connection.}

7.2.4 State-chart and context

![State-chart](image)

**Figure 51 : State-charts: Movement and Status of agents**

In Figure 51, all Agents start simultaneously in a “Temporary” state in the “Movement” and “Status” state-charts. The Agents switch to their relative states (Normal, Security compromising, Energy consuming). A number of these are Access Points, so they are switched to the state “Fix” and placed on the map
according to their GPS positions taken from Swiss hotspots, in footnote 2. All others are considered as mobile nodes and each of them follows a random mobility model. They are then added to a list of Access Points whenever they are within the range of this AP.

We used Agents that had one of 3 statuses:

a. Normal state
b. Security compromising state or
c. Energy wasting state.

Each Agent was then processed based on the value of the Decision Making Function. Therefore, each Agent either changed to another Status or remained in the same state. When completing the transfer, each Agent returned to its initial state.

### 7.2.5 Scenarios

We have used two scenarios to validate our model. In the first scenario, devices (agents) which had access to APs were divided into three categories.

Those with normal behavior, which represented 50% of all devices. Note that half of these were mobile devices (25% of the total).

Those with energy wasting behavior – in looking for unnecessary security access, these were devices that tried to push other devices to waste energy. These represented 25% of devices.

Those with security compromising behavior - attempting not to use security in accessing the network in order to compromise the privacy and security of everyone within a given range, leaving the connection out-of-use during a period of time equal to the time needed for network access and data transfer. That was the case for 25% of devices.

In the second scenario, we fixed the percentage of devices for each category:

80% with normal behavior, half of these being mobile devices
10% with energy wasting behavior
10% with security compromising behavior

### 7.2.6 Results Analysis

During our analysis, we firstly studied the performance of Light SARM in the case of the Geneva Hotspots network in terms of relative utilization, wastage of energy and security compromise under the constraint of a fixed percentage (25%) of devices operating in energy wasting states and *idem* in security compromising states (25%). Four references were taken for evaluation. Secondly, we studied the same performance indicators for the case of our

---

second scenario, which is based on 10% of devices being wasteful of energy and 10% of devices compromising security.

For purposes of comparison, we plotted the Light SARM and four references and their relative average number of Agents’ states in Figure 52 for the first scenario.

![Figure 52: Performance of Light SARM and references.](image)

Please note: there are significant differences between each case and 250 devices are in a “security compromising” state in the All-secure case, as 25% of devices are by default in this state in the first scenario.

As we can see from the results depicted in Figure 52 the most efficient overall solution for all constraints is the DMF which is implemented in the Light SARM, and all other references are inefficient. The best relative utilization rate happened in the case of “non-secure”, but unfortunately this result is compromised by the huge amount of security compromising devices (out-of-use). On the other hand, “All-secure” is, as a matter of course, efficient in security compromising terms but is worst in terms of energy wastage. For more details, the minimum-maximum and the standard deviation for the same average results are plotted in Figure 53.
Moreover, the results in the second scenario are similar to those in the first scenario, in the sense that Light SARM makes the best choice in accordance with policy and user preferences. Indeed, Light SARM constitutes a good trade-off for all of the studied cases, because it simultaneously allows high overall utilization and lower wastage of energy. Therefore, it shows that our Framework is efficient in this context and is the best trade-off between security and performance.

**Figure 53: Min-Max & std-dev. for Light-SARM & References.**

Moreover, the results in the second scenario are similar to those in the first scenario, in the sense that Light SARM makes the best choice in accordance with policy and user preferences. Indeed, Light SARM constitutes a good trade-off for all of the studied cases, because it simultaneously allows high overall utilization and lower wastage of energy. Therefore, it shows that our Framework is efficient in this context and is the best trade-off between security and performance.

**Figure 54: Effect of threshold on overall utilization 1st Scenario**
The “Random” values related to the three categories are well distributed and almost equal. However, the utilization rate is lower than both Averages and the energy wasting rate is higher than “Average 5%”. This last “Average” constitutes a good trade-off for all studied cases because it offers simultaneously a high overall utilization and a lower energy wasting. Therefore, it is interesting to plot the three categories for different threshold values to find the exact value that optimizes the overall network utilization.

Figure 54 illustrates the evolution of our three categories when we varied the threshold value between 0% (“All-secure”) to 100% (“Non-secure”). We also plotted the overall utilization for two cases under the constraint of our first scenario. In one case, we counted only 80% of the energy wasting devices in the overall utilization, and in the other case only 60%. Indeed, when a device is in energy wasting status, only a part of its offered bandwidth and allocated time are used. That was the reason why we counted only a part of them.

In the Figure 55, we plotted the same case as in Figure 54 with the only difference being that the second scenario was applied. The results showed that our SARM was optimal in term of overall utilization. It improved the overall utilization by 10% in the case of 60% of energy wasting devices. Almost no improvement was realized in the case of 80% of energy wasting devices.

![Overall utilization graph](image-url)

**Figure 55: Effect of threshold on overall utilization 2nd Scenario**

The overall utilization was better for SARM when the threshold was in the interval of [0:0.2]. The overall utilization difference was clear when using SARM instead of “All-secure” method. The obtained gain of SARM was almost 10%. The threshold in this case was 0.01.
7.2.7 Results

WLAN has been increasingly deployed in various locations because of the convenience of wireless communication and decreasing costs of the underlying technology. However, the existing security mechanisms in wireless communication are vulnerable to attacks, seriously threaten privacy and are particularly resource consuming. The emergence of wireless networks brings many open issues to network designers.

Therefore, several challenges are opened particularly in the field of security and energy consumption. This dissertation presents the simulation of a new dichotomy mechanism of SARM in WLAN applied to Geneva Hotspots network Access Points based on random mobility and AnyLogic simulations. Our work shows that SARM is in many cases optimal in term of overall network utilization, almost a gain of 10%. The “All secure” Decision Making Function has got the best overall security compromising rate but it is the worst case in utilization. On the other hand, “Non-secure” has got the best relative utilization rate but it is the worst case in energy wasting. Our work shows that our solution is optimal in term of overall utilization rate because it tackles at the same time the worst cases of “Non-secure” and “All-secure”. These results encourage us to further research on other strategies that could automatically optimize the trade-off between security and performance particularly in energy consumption and overall network utilization.

7.3 Use case: Hotspots, trust & reputation

7.3.1 Context:

The number of access points in the world is increasing significantly: they have spread into many locations like airports, cafes, businesses and university campuses. This ongoing spreading, coupled with the inherent vulnerabilities of the technologies deployed, has resulted in more security breaches. In addition to the typical network threats, wireless networks present several challenges and are vulnerable to more forms of attack. This is due to the broad, open air nature of the channel, which makes more attacks possible, as well as due to bandwidth limitations and constant topology changes because of node mobility.

Furthermore, many security breaches have been registered, such as Service Set Identifier (SSID) spoofing using soft AP. In order to steal credit card numbers and other personal information, thieves use a ‘soft AP’ to masquerade as a legitimate Internet AP. For instance, it has been reported [4] that fake Wi-Fi networks have been set up in airports in order to capture users’ sensitive information while they surf the Web. In cases like this, the basic security mechanisms may not be sufficient.

It is important to know whether a Wi-Fi network within range is trustworthy or not. For instance, we can take the example of a young man who wants to send an email to inform his wife that his plane will be late, or that of a businessman who must make a banking transaction using the Internet. In these two cases, it is crucial to notice that the requisite level of security is not the same.
According to the opinions of those who have used APs, it is important to inform future users as to whether or not they can rely on these APs. In some locations, it is common to have the option of connecting to more than five Wi-Fi networks.

Instead of having just the access points and their received power level as depicted in Figure 56, it is useful and more interesting to have with them a trust ranking as depicted in Figure 57.

![Figure 56: A normal Wi-Fi access user interface](image)

### 7.3.2 Approach

In order to tackle the abovementioned constraint problems, we need new and easily deployable security-adapted mechanisms in respect of overall performance.

One question to answer is how SARM should be integrated in a mobile phone (MP) in order to secure access to a Wi-Fi hotspot that could potentially be faked?

The idea is to use trust from SARM’s means in order to rank any available access points according to their reputations. This way, the user will have evidence of the levels of security of particular access point hotspots.
The security problem and related work

The number of Wi-Fi networks is growing very quickly because of the increasing demand for shared, personal and commercial Wi-Fi access. In most public Wi-Fi networks, solutions are not based on security or optimized energy consumption. It is very important for network operators and users to find ways to improve network utilization and energy consumption.

For instance, a user who wants to connect to an AP and has very little battery life in his/her mobile phone will not be able to use the network for very long. Another pertinent example would be a case in which a user wants to transfer money via online banking and needs to use an AP which he/she can trust.

The goal of this work is to present an easy deployable solution that:

- evaluates the level of trust pertaining to the security of the AP;
- minimizes energy consumption; and
- encourages the owner of the AP to act correctly.

Related work

Salem et al. [5] propose a reputation system to enable users to choose the best hotspots and to discourage wireless Internet service providers (WISPs) from providing a poor quality of service to mobile nodes. In their dissertation, they consider a mobile node MN, which is affiliated with a home network H, and wants to connect to the Internet via a hotspot managed by a wireless Internet service provider. The behavior of each WISP in this model is characterized by
what they call a reputation record. This record represents an evaluation of the reputation of the WISP and is generated and signed by a trusted central authority. The reputation mechanism is maintained by the same trusted central authority. When a WISP first enters the network, the trusted central authority provides it with an initial reputation record that can thereafter increase (i.e. getting a better reputation) or decrease, depending on the behavior of the WISP. If MN has two neighboring WISPs proposing equivalent offers, i.e. the same QoS and price, MN will logically choose to connect to the access point managed by the WISP with the best reputation record. A micropayment scheme is used to make sure that Mobile Nodes pay for the services they receive.

Our solution is similar in some regards, but different as well because it can work for free or fee-based AP. Our solution also takes the energy consumption into account, which is an important criterion where mobile devices are concerned. Our work focuses on detecting the APs that want to cheat by stealing sensitive information or cause the user to consume a lot of battery life.

In [6], Ben-Salem et al. establish selection algorithms focus on AP signal strength as an important metric. An extensive field study was conducted across three neighborhoods in Chicago, and showed that choosing an AP based on signal strength bypasses significant opportunities for Internet connectivity. The design and implementation of Virgil, an automatic AP discovery and selection system, were presented. Virgil quickly associates with each AP found during a scan, and runs a battery of tests designed to discover the AP’s suitability for use by estimating the bandwidth and round-trip-time to a set of reference servers. Virgil also probes for blocked or redirected ports, to guide selection in favor of preserving any application services currently in use. The use of Virgil was evaluated in five different neighborhoods across three different cities. The results show that Virgil finds a usable connection between 22% and 100% more often than selections based on signal strength alone. Virgil improves both performance and accuracy for neighborhoods where the user commonly travels, by caching AP test results. The work in this study focused on estimation of bandwidth and round-trip-time to assess APs. Our solution focuses on two other aspects - security and energy consumption - in order to assess APs.

Ormond et al. [7] further examine network selection decisions in wireless heterogeneous networks based on a user-centric approach, which they say enables a user to choose the network that best meets their requirements. Their network selection algorithm predicts the data rate for each interface available to the mobile node and decides based on these predictions. Their approach is very interesting because they focus on user requirements and preferences, but do not consider security and energy consumption as we do.
As shown in Figure 58, the trust model and the variable Trust functions are defined as follows:

I. \( U \) is the user,

II. \( n \) is the number of friends that \( U \) has,

III. \( v \) is the trust value of the AP \( N \) rated by user \( U \)

IV. The value \( T \) is the sum of recommendations from friends of \( U \); and

V. \( N \) is the Access Point AP.

The solution will be given in next sections.

### 7.3.4 Wi-Fi Trust and reputation solutions

**Our Solution and its Assumptions**

We now consider a mobile phone (MP) with integrated Wi-Fi technology. A user wants to connect his MP to the Internet via a Wi-Fi AP. There are different APs which are available in his vicinity. In our solution, a reputation mechanism is used to discourage the APs from cheating: the trust/reputation value of an AP is used during the selection process to choose the best AP for the user from those available. Thanks to our reputation-based mechanism, the APs are encouraged to behave: they do not steal sensitive data from connected users or force users to consume large amounts of energy when connected, for example by forcing
strong levels of encryption even if this is unnecessary.

**Attacker Model Assumptions**

Trust and reputation evidence is maintained by a Trusted Authority (TA). We assume that:

- the TA is trusted by the other parties;
- the user is not able to create multiple identities in order to cheat, for example via Sybil attacks [2], and also that the MP has a SIM card which unambiguously authenticates the identity of the user with a provider;
- there is a social networking web site for mobile users whereby they can specify who their friends are;
- communication between users/mobile clients can take place using the web site;
- the connection to the mobile web site will be made through GPRS or GSM;
- the AP has an unlimited amount of energy and a uniform transmission range;
- the trust value of an AP will be in the range of [0…1].

### 7.3.5 Trust and reputation

Our solution proposes a form of trust management in order to help users to choose the most trustworthy AP. Two thresholds are used: trust_value_min. and trust_value_max.

We have defined three cases:

**First case:** the MP will connect to an AP using an encrypted connection if the trust value of the AP falls between two values which will be explained later in this dissertation.

**Second case:** the MP will not connect to an AP if its trust value is less than the trust_value_min.

**Third case:** the MP will connect to an AP without encrypting data if the trust value of the AP is greater than the trust_value_max.

**Reputation model**

The behavior of each AP in our model is characterized by what we call a reputation record.

This record represents an evaluation of the reputation of the AP in terms of its security and energy consumption, and this evaluation is generated and signed by a trusted authority, denoted TA.
When an AP first enters a network, the TA provides it with an initial reputation record that can later improve (i.e. gaining a better reputation) or worsen, depending on the AP’s behavior.

Users have the option of asking friends as to their recommendations about an AP. A user can do this by using a mobile web site where he can store all his information about the APs used by him and his friends. These recommendations are useful when a user has no information about an AP. After using an AP, the user can rate it according to three possible values: Positive, Negative or Neutral. We assume that two functions are implemented in MPs: one for detecting a security breach during a session and the other for detecting excessive energy consumption.

Note that the four functions to calculate Trust and Reputation were proposed by Xavier TITI from the University of Geneva. They are based on theory developed in paragraph 5.3.2 about Trust and reputation as means of SARM

**Trust Function 1**

It is responsible to compute the trust value of an AP by taking into account an evaluation from a friend of a user. But we have defined different levels of friendship. We consider that:

the user is $U$; $n$ is the number of friends that $U$ has; $v$ is the trust value of APs stored in $U$’s MP; $T$ is the value of the sum of recommendations coming from $U$’s friends; and $N$ is the AP.

This function is implemented within the MP. The results of this function will be applied to the two thresholds (trust_value_min. and trust_value_max.) in order to ascertain the relevant case.

$$Trust(U \rightarrow N) = \sum_{i}^{n} \frac{Friendshipfactor \ast Trust(Ui \rightarrow N)}{n}$$

Equation 18

**Trust Function 2**

This is responsible for computing recommendations from friends of a user’s friends.

$Ui$ represents all of $U$’s friends

*Friendshipfactor* is a factor of friendship that is explained in function 3.

$n$ is the number of friends that $U$ has,

$v$ is the trust value of the AP $N$ rated by user $U$

The value $T$ is the sum of recommendations from friends of $U$; and $N$ is the Access Point AP.

This function is implemented on the mobile web site. When a user asks for this form of recommendation, the web site will compute its value and send it to the
user. We have chosen to allocate this function to the web site in order to lighten the MP's load, and the user will nevertheless receive the recommendation value so as to be able to compute the trust value of the AP.

\[
TrustUpdate (U \rightarrow N) = \begin{cases} 
  v & \text{if } n = 0 \\
  \frac{n(v + T) + v}{2 * (n + 1)} & \text{otherwise}
\end{cases} \quad \text{Equation 19}
\]

**Trust Function 3**

This is responsible for computing the *Friendship factor* of the user. We use *nblink* to represent the level of friendship. nblink must be less than or equal to 6, taking into account the Small World theory [8]. A and B are users and friends. This function is used to help the computation of the recommendation by calculating the *Friendship factor*. This function is also implemented on the mobile web site, hence the MP only receives the factor.

\[
\text{Friendship factor } A \rightarrow B = \begin{cases} 
  1 & \text{if } A \text{ is a friend of } B \\
  \frac{1 + \frac{nblink}{2}}{nblink + \frac{1}{2}} & \text{else}
\end{cases} \quad \text{Equation 20}
\]

**Trust Function 4**

This is responsible for computing the trust value of an AP. Pos represents good feedback, Neg represents bad feedback and Neu represents neutral feedback. The trust value is certified by the TA and stored in the AP. As already stated, we assume that this value cannot be changed by the user. This function is implemented in the AP. When the user finishes using the AP, he can choose between three different forms of feedback (Pos, Neg, Neu). This function will also be implemented in the MP in order for the phone to have a record of its own experiences with the AP.

\[
Trust_{Network(AP)} = \frac{\sum_{i=0}^{n} Pos + \frac{1}{2} \sum_{i=0}^{p} Neu}{\sum_{i=0}^{n} Pos + \sum_{i=0}^{m} Neg + \sum_{i=0}^{p} Neu} \quad \text{Equation 21}
\]

**7.3.6 State-chart and context**

The movement and the status of our agents are controlled by a state-chart which represents the exact behavior of the device as depicted in Figure 59.
Each agent starts in a “Temporary” state on the state-chart. Some of our agents were APs, so they switched to the “Fixed” state. These agents were placed on the map according to their GPS positions in footnote 3. The rest of our agents were considered to be mobile nodes and each of them followed a random mobility model and was switched to the Walking state. Whenever they come within an AP’s range, they are added to this AP’s list. The processing state evaluates the trust function and chooses the best value from all the APs nearby.

We used agents that were in one of the 6 states:

- **Transmit**: a normal connection is completed without encryption or problems (green)
- **Energy Wasting**: an encrypted connection is established although the encryption is unnecessary (blue)
- **Energy Saving**: a non-encrypted connection is established despite the AP’s requests for encryption (dark green)
- **Security Compromising**: the AP compromises security because the connection is not encrypted (red)
- **Utilization Lost**: a connection is not established because the Trust value is below the minimum threshold although there is no danger (magenta)

---

Simulation and Evaluations

Other: there is no AP within a fixed range (yellow)

Every agent can fall into one of those six states. After that, the agent will follow the state Statistics to accomplish all necessary measures before going back in his initial state.

Setting up our security model using Table 17, we can take advantage of the state chart by monitoring agents' behavior. The behavior of APs is summarized in Table 4.

<table>
<thead>
<tr>
<th>Table 17: Access Point Behaviors</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Behaviour</strong></td>
</tr>
<tr>
<td>Normal Transmit</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Energy wasting</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Security compromising</td>
</tr>
</tbody>
</table>

**7.3.7 Scenarios**

For our first scenario, we fixed the percentages of users in motion, APs and the percentage for each category of AP:

- 60% are users in motion
- 40% are APs
- 10% of APs have Energy wasting behaviour
- 10% of APs have Security compromising behavior
- 80% of APs have Transmit behavior

For our second scenario, we fixed the percentages of users in motion, APs and the percentage for each category of AP:

- 60% are users in motion
- 40% are APs
- 25% of APs have Energy wasting behaviour
- 25% of APs have security compromising behavior
- 50% of APs have Transmit behavior

The two scenarios were run using a wireless network composed of 600 users and 300 APs in the case of high density, and 400 users and 40 APs in the case of low density.
7.3.8 Results Analysis

In this section, we present the results of the validation of our solution by using a simulation. Firstly we endeavor to find the best trust value to initialize the AP and to find the best value for the two thresholds - trust_value_min. and trust_value_max.

Table 18: Initialization and effect of our variables

<table>
<thead>
<tr>
<th>Threshold min – max</th>
<th>0.1–0.3</th>
<th>0.2–0.4</th>
<th>0.3–0.5</th>
<th>0.4–0.6</th>
<th>0.5–0.7</th>
<th>0.6–0.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initialisation of AP value</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>0.1</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>0.2</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>0.3</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>0.4</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>0.5</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>0.6</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>0.7</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>0.8</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>0.9</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>1</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

The results of Table 18 show that the best value for our thresholds is 0.3 for the trust_value_min. and 0.5 the for trust_value_max., because in this case we are able to detect the malicious AP after a number of connections to this AP. The best initial trust values for AP are between [0.8 and 1].

Figure 60: Comparison of low and high density APs in the first scenario

Figure 60 shows that with our solution, in the case of high AP density, we can detect a malicious AP in roughly 20 connections. However, in the case of low AP density, we can only detect a malicious AP with our solution in roughly 90 connections. This is due to the fact that there are many isolated APs which are evaluated without comparison to any other APs’ trust values. In other words, in the first case users can evaluate the trust values of the APs and choose the best one more easily than in the second case. Therefore, our solution is well-adapted to accommodate a rapid rise in the number of APs, mainly in cities, in the near future.
Figure 61 illustrates the evolution of the percentage of normal users for the second scenario (25% Security compromising, 25% Energy wasting) for low and high AP density. In the case of high density, the number of connections required to detect a malicious AP is around 21 connections and in the case of low density, it is around 142 connections. We can deduct that there is not a big difference between the two scenarios for high AP density because a user can detect a malicious AP using approximately the same number of connections in each case. However in the case of low AP density there is a big difference between the two scenarios because the number of connections required for scenario 2, for instance, is significantly higher than that for scenario 1.

7.3.9 Synthesis

Our solution provides a way to find the number of connections made by different users in attempting to detect malicious APs, taking into account the fact that there are no attackers.

Table 19: Statistics for average number of connections in the second scenario

<table>
<thead>
<tr>
<th></th>
<th>High density</th>
<th>Low density</th>
<th>Ratio LD/HD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average number of connections made to detect malicious AP</td>
<td>20.81</td>
<td>96.87</td>
<td>4.66</td>
</tr>
<tr>
<td>Standard deviation</td>
<td>4.13</td>
<td>23.68</td>
<td>5.74</td>
</tr>
<tr>
<td>Number of connections for 99% confidence level</td>
<td>30.41</td>
<td>151.95</td>
<td>5.00</td>
</tr>
</tbody>
</table>

In Table 19, we found the average amount of connections needed to detect malicious APs in the cases of high AP density and low AP density for 30 samples. Then, we calculated the ratio of low density to high density. We also calculated the standard deviation (SD) and the confidence interval in order to...
show the reliability of our results. Indeed, for 99% of the time, the estimated number of connections for convergence will be less than or equal to the average, plus 2.326 to account for standard deviation (A + 2.326 * SD). For high density, the number of connections needed to detect a malicious AP is less than for low density; the ratio is around 1:5.

**Table 20: Statistics for average number of connections in the second scenario**

<table>
<thead>
<tr>
<th></th>
<th>High density</th>
<th>Low density</th>
<th>Ratio LD/HD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average number of connections made to detect malicious AP</td>
<td>27.78</td>
<td>154.00</td>
<td>5.54</td>
</tr>
<tr>
<td>Standard deviation</td>
<td>5.31</td>
<td>35.34</td>
<td>6.66</td>
</tr>
<tr>
<td>Number of connections for 99% confidence level</td>
<td>40.12</td>
<td>240.86</td>
<td>6.00</td>
</tr>
</tbody>
</table>

In Table 20, the average values for high density and low density and the ratio of low:high are provided for the scenario whereby 25% of APs are Security compromising and 25% of APs are Energy wasting. We also calculated the standard deviation and the confidence interval, which indicate how reliable our results are. The detection of malicious APs in the case of low AP density takes between 5 and 6 times longer than in cases of high AP density, depending on whether the first or second scenario is used.

These results provide encouragement to engage in further research into other strategies that could automatically optimize the trade-offs between security and energy consumption in other important application domains, such as in wireless sensor networks. Therefore, we have carried out studies to evaluate SARM in WSN.

### 7.4 Use case: SARM in WSN

A Wireless Sensor Network (WSN) consists of a large number of low-power and multifunction sensor nodes that communicate as single hop, multi-hop, or cluster-based models to send data to one or more base stations (BSs) through wireless links. These BSs are endowed with a large amount of energy. WSNs represent a challenging and interesting research area due to the constraints involved. The sensors’ small size and the networking capabilities increase the appeal of WSNs for use in daily life. Distributed computing and routing could be well applied in the case of multi-hop and cluster-based models. These capabilities enable WSNs to provide significant advantages for many applications that would not have been possible in the past. A WSN is built by deploying sensing nodes in the area of interest to then form a self-configured network and start acquiring the necessary information. The unique properties of WSNs increase the level of flexibility and reduce user involvement in operational tasks. Use in battlefield surveillance, forest fire detection, and smart
environments are some of their more well-known applications. Since the nodes in WSNs are battery operated and have limited operating lifetimes, there is a growing need for the development of energy aware security algorithms with low computational loads in order to preserve the networks’ lifetimes.

WSNs involve a huge number of interactions with their particular environments during which security is difficult to ensure against the dynamic changing attacks. Indeed, it is seriously challenging to maintain overall security at the highest level due to the configuration complexity and the changing runtime context. In addition to the security challenge, data transfer in WSNs is more susceptible to loss due to the nature of sensors (power and processing, etc.) and the high error rate of wireless links. Moreover, sinkhole attackers cause the packet loss to skyrocket by means of dynamic changing behavior. Therefore, the most crucial constraint in WSNs - reliability - is not at all guaranteed.

In general, most applications cannot operate in cases of high packet loss. Thus reliability, being a key issue in sensor networks, is definitely one of the most important criteria for evaluating the quality of WSNs. Accordingly, we will apply SARM for WSNs under sinkhole attack. Please note: security is used as a general term, to include availability, reliability, and survivability.

7.4.1 WSN-SARM

In order to validate SARM, we have applied an adapted version of SARM, called WSN-SARM, to the application domain of wireless sensor networks.

Validation Application Domain Main Problem

In Wireless Sensor Networks (WSN), one of the main constraints is the need to minimize energy consumption in order to maximize the lifespan of the network. Indeed, sensor nodes are usually battery powered. In order to increase the lifetime of sensor networks, various energy saving schemes have been proposed.

One of the known possibilities for prolonging network life is energy balancing, which is the approach that we have implemented in our SARM Framework for WSN. In an energy-balanced network, all the nodes’ energy depletes at the same rate. It is an efficient method for implementing a data-gathering algorithm for WSNs.

Indeed, a data-gathering WSN is deployed over the region that is to be monitored and when a sensor detects an event, it needs to report to the BS, which is not limited in terms of energy for the purposes of our case study.

Messages are sent to the BS using a hop-by-hop routing method. This method seeks to minimize overall network energy utilization, since the received power $P$ is depending on at least the squared distance of a hop.

$$P(d)=k d^a$$  \hspace{1cm} \text{Equation 22}

where $k$ is a constant, $d$ distance of a hop and $a$ is a parameter between 2 and 5.
This heavy traffic relating to nodes near the BS causes their energy to deplete rapidly.

Thus, it creates bottleneck regions in the network. Unfortunately, when too many of these nodes run out of energy, the sink becomes disconnected from the network. This can lead to the network being put out of service, even though there may be plenty of energy remaining in nodes at a distance from the sink. Therefore, it seems that energy balancing is a particularly promising way of maximizing the lifespan of a network that is accomplishing a data-gathering task.

Another problem that challenges all the proposed solutions is the issue of sinkhole attacks. Indeed, it compromises the balancing effect on the lifespan of any WSN. That is why a countermeasure is necessary in this case.

We propose our SARM Framework, with its feedback mechanisms and its Trust Function, as an efficient solution to balance the energy of all reachable nodes in order to overcome sinkhole attacks. Then, we compare it with simple equidistribution (uniform packet repartition) without any feedback.

### 7.4.2 Goal of SARM-WSN

The goal of this validation is to show that SARM adapts security as efficiently as possible by:

1. maintaining a level of security appropriate to the context;
2. maximizing overall utilization; and
3. minimizing power consumption.

### 7.4.3 WSN-SARM Description

In Figure 62, we describe, module by module, how SARM is applied to the application domain of our validation, becoming the WSN-SARM version.
First of all, the uniform packet repartition, unbalanced neighbors’ packet repartition and the set of suboptimal distance paths are all security means which can be tuned by SARM. The application preference serves to maximize the usage time while maintaining sufficient security. The gathering context module is used to collect and distribute trust values between the Base Station and the nodes (sensors). These values represent a sensor’s trust in its neighbors. They are summarized in the following table:

**Table 21: Behavior and recommended actions sent by Base Station to a Sensor under sinkhole attack**

<table>
<thead>
<tr>
<th>Sensor Behavior towards neighbors</th>
<th>Recommended action to Sensor by BS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>If packet is received then add (1)</td>
</tr>
<tr>
<td>Sinkhole action with neighbors because of not sending packet</td>
<td>If packet is lost then add (-1)</td>
</tr>
</tbody>
</table>

The values are sent to the management unit for analysis using a Trust Function (TF) which will declare whether an algorithm has to be used or not. In addition, the performance is fixed as energy saving in accordance with the Application
Preference, which is lifespan maximizing.

Each sensor sends packets uniformly to a number of sensors within a defined range according to the threshold used as policy. Thanks to its context gathering module, the Trust Function has all the necessary information to evaluate the level of trust. Figure 63 provides a representation of the context of each sensor, as well as of some of their behavior.

The management unit will integrate the Trust Function (TF), which predicts whether to use uniform or unbalanced connections based on the output of the TF, depending on historical values $v_{ij}$ (i packets) sent by the BS to sensor z about his neighbor, sensor j, within a defined range.

$$T_{jz}(v_{ij}) = \frac{\sum_{i=1}^{N} v_{ij}}{N}$$  \hspace{1cm} \text{Equation 23}

[T_{jz}(v_{ij}): sensor z’s trust in sensor j and vi are sent by BS as ACK, N: number of all packets sent by sensor z and received by the BS]

Threshold = rand()

For all j sensors,

- if $T_{jz}(v_{ij}) > 0$
- TF is the summation of all positive Trust relating to j neighbors
- if (TF=0)

  \text{then \{we send uniformly\}}
or else, if \(TF > \text{threshold}\)
then \{we send the packet to sensor \(j\)\}

End of for loop

The system consists of between one and many sensors with different behaviors that could potentially change at random. Therefore, it would have been preferable to analyze the overall system characteristics in a real world scenario, but that would have been very difficult. The complexity of analysis comes from the fact that every node acts independently from others. Therefore, our model will be studied using simulation tools in order to compare it with reference cases.

Figure 64: Animation interface of Arranged WSN-SARM

Figure 64 shows a very powerful animation interface created using AnyLogic. The BS is placed in the upper left side of the square.

Arranged sensors are sensors that are placed at a distance equidistant from the BS, as depicted in Figure 64. Random sensor repartition means that the sensors are randomly placed.

The sensors are spread over a square topology with a 520 meter side length, and operate over one day of simulation time. In our simulations, we considered the Base station to be taken as the origin. The Base Station covers the entire network. We ranged the number of communicating neighbors from 1 to 7. Indeed, depending on the topology of the network (arranged or randomly distributed sensor positions), each sensor was configured to have a maximum
communication range of 50 meters. We deployed the sensors incrementally, from $S_1$ to $S_n$. The number of sensors can be selected at anywhere between 10 and 1000 and their arrangement can be chosen as uniform or random.

### 7.4.4 State chart and context

Using AnyLogic, which is a strong simulation tool, as an implementation platform agent, state-charts particularly can be programmed very conveniently. Specifically, modifications and/or extensions of the final model can be handled in simple ways.

![State chart diagram](image)

**Figure 65**: State-charts: “Transmission” of agents “SensorStateR” and “TF”

In Figure 65, each Agent (sensor) starts simultaneously in a “Transmission” state in the “SensorStateR” and “Trust Function” state-charts. The Agents are switched to their relative state (Sinkhole, Base Station, Sensors). They are then added to a list of sensors whenever they are within this range.

We used Agents with one of the following forms of behavior:

- a. Normal state and
- b. Sinkhole.

Each Agent is then processed based on the monitoring unit’s decision to choose security means - or not. Therefore, an Agent could change to another state or remain in the same state. When completing a transfer, the Agent returns to its initial state, and so on. The state-chart Trust updates the trust each time the Base Station sends an acknowledgment (ACK). As a matter of course, a BS is not limited in terms of energy and thus is not subject to attack from any sinkhole.

### 7.4.5 Validation Methodology

In our experiments, we have validated our proposed solution and analyzed the extended performance for a range of various scenarios.
We have carried out simulations based on 0%, 20% and 50% of devices being sinkhole attackers. Furthermore, the network topology was set to random spreading or arranged uniform spreading of sensors. We have taken uniform packet distribution across neighbors as a reference. In addition, a Time-To-Live (TTL) counter is used to avoid a packet remaining within a network forever and to guarantee that the energy consumed is limited to a maximum value when a packet is sent from the farthest sensor to the BS.

To minimize the transit delay and the energy consumption, we have also introduced suboptimal routing paths as all paths that have the shortest Euclidean distance to the BS. Indeed, if the topology of sensors is uniformly distributed and the sensors are not at the border of the square, there are 3 sensors that are placed at the shortest distance from the BS.

Normally, the BS is in the middle of a network so as to minimize the distance to the farthest sensor. Additionally, 90 degree sector antennas are used to cover each of four squares in order to lengthen the BS’s range and minimize energy consumption. Sector directional antennas can be also added to sensors to help take advantage of this technique for purposes of energy consumption [9]. Therefore, we do not lose any generality if we put the BS at the upper left side of the square; rather, we gain in terms of the survivability of the WSN.

In our experiments, we have validated our proposed solution and analyzed its extended performance for various scenarios. All sensors are spread out over a square (520m²) topology and operate over one day of simulation time. In our simulations, we considered the Base station to be taken as the origin. The Base Station coverage ranges across the entire network. The connection number with neighbors varies from 1 to 7. Indeed, depending on the topology of the network (whether in arranged or randomly distributed sensor positions), each sensor was configured to have a maximum communication range of 50 meters. We deployed the sensors in an incremental mode, from S1 to Sn.

We have also used an algorithm in the Base Station to calculate each sensor’s suboptimal routing hops to the BS. This would need to send packet step-by-step power emission and could be implemented by using a sector antenna.

The number of sensors can be anything from 10 to 1000 and their display can be arranged uniformly or randomly.
Figure 66 shows a very powerful animation interface using AnyLogic. Note that the BS and sensors' forms are described in Figure 63. Arranged sensors means that they are placed equidistantly to each other, as depicted in the last figure.

Randomly distributed sensors means that they are situated in a random manner, as depicted in the last figure.
We carried out our experiments for thirty cases. In each case studied, we ran our simulations under different conditions. Our performance evaluation was the result of different simulations.
Figure 66: Animation interface and results of Random WSN-SARM

7.4.6 Scenarios

We have used three scenarios to validate our model. In our scenarios, sensors (agents) were divided into two categories:

- those with normal behavior, which account for x% of all sensors;
- those with energy wasting/sinkhole behavior, which account for (1-x)% of all sensors.

In the first scenario, we fixed the percentages at:

- 100% with normal behavior and
- 0% with sinkhole behavior.

In the second scenario, we fixed the percentages at:

- 80% with normal behavior and
- 20% with sinkhole behavior.

In the third scenario, we fixed the percentages at:

- 50% with normal behavior and
- 50% with sinkhole behavior.
7.4.7 Metrics

Energy metrics are Packet loss ratio, which affects energy loss per node, and whole network energy loss, which is important for evaluating energy efficiency in transport protocol.

Assuming that dropped packets have a direct relation to energy wastage, the energy loss per node can be measured thus [58]:

\[
E(i) = \frac{\text{nbr of packets dropped by node}}{\text{all packets rvd node}} \quad \text{Equation 24}
\]

Whereas the energy loss for the whole network can be calculated using the total number of packets received, thus:

\[
E_{\text{net}} = \frac{\text{nbr of packets dropped by net}}{\text{all packets rvd BS}} \quad \text{Equation 25}
\]

The reliability of the entire network is defined as:

\[
R_{\text{net}} = \frac{\text{nbr of packets rvd by BS}}{\text{total packets send by all}} \quad \text{Equation 26}
\]

Please note, \( R_{\text{net}} = \frac{1}{E_{\text{net}} + 1} \) and rvd = received by;

7.4.8 Results Analysis

During our analysis, we firstly studied the performance of WSN-SARM in the three defined scenarios where sensors were arranged either uniformly or at random. The performance metrics are network reliability ratio and overall network energy loss within the constraints:

(thanks to TTL) almost the same average energy consumption for any packet, and overall traffic must be balanced across all neighbors to guarantee the network’s survivability.

Secondly, we studied the rapidity of convergence to 100% (How WSN-SARM tends to 1) and compared it to the suboptimal routing paths.

Thirdly, we studied the long-run convergence of the TF used in WSN-SARM.

For purposes of comparison, we plotted the WSN SARM in Figure 67 and uniform balancing (no trust: uniform packet distribution across neighbors) in Figure 68 for the same three predefined scenarios. We can easily conclude that SARM is largely better than uniform balancing; a ratio of 20:1 is reached in a short time – 50 seconds. Indeed, we have obtained the SARM’s feedback mechanism’s desired effect.
Figure 67: Reliability of references for the 3 scenarios.

Figure 68: Reliability of WSN-SARM for the 3 scenarios.
In Figure 69, we plotted the long-term convergence trend of SARM for the second scenario. Unfortunately, the convergence is very long due to the use of links with many hops. Moreover, in the second and third scenarios, with 20% and 50% of sinkhole attackers respectively, the degree of reliability of SARM exceeds that of the 0% sinkhole because sensors within the Base Station detect any sinkhole neighbor and eliminate it from its connections.

![Convergence of SARM, 200 Arranged Sensors](image)

**Figure 69: Long-term reliability of WSN-SARM for second scenario**

For purposes of comparison, we plotted the WSN-SARM based on 20% of sensors being sinkhole attackers (the second scenario) using our Trust Function and also without trust in Figure 70. We have used all suboptimal routing paths to the Base Station. The results clearly demonstrate that the level of convergence is boosted.
Figure 70: Reliability of WSN-SARM for the second scenario
In Figure 71, we have depicted the Network Energy Loss as defined by our metrics. We have an average ratio of 5.2:1 between the two cases. We can conclude that using SARM with the Trust Function converges more rapidly than without trust. Thereby, the reliability is guaranteed and the overall energy cost is minimized even with 20% of sensors as sinkhole attackers.

Please note: there are significant differences between Trust used by WSN-SARM and uniform packet distribution reference.
We have depicted in Figure 72 the proof that WSN-SARM is converging towards 100% in terms of Reliability and towards 0% in terms of Network Energy Loss.

All the results show the clear advantages of WSN-SARM arranged sensor network or random sensor network even when 50% of sensors are sinkhole attackers. We can conclude that our security monitor helps the WSN to operate even if 50% of sensors are sinkhole attackers thanks to the feedback control system connected to the context gathering monitor and the Trust Function.

7.5 User case: SARM in service of Green 2.0

Ubiquitous computing is becoming increasingly widespread, mainly through the Internet of Things, which is highlighted by large-scale embedded sensor devices. Indeed, trends are best observed through the use of sensors and RFID in everyday life, such as in cars or refrigerators, or even for animals, to keep track of useful information about them. This overflow of information coming from sensing and communication fits squarely within a complex system and autonomic computing. Furthermore, the mobility of these devices exposes them to different security vulnerabilities.

However, there will be no acceptance of these new paradigms without apt security methods, which are a main concern for both industry and consumers.
The increasing complexity of communication systems and also of attacks make conventional static security almost obsolete, given how high its resource consumption would need to be to maintain the required security level. The overhead costs would be impractically high. Thus, new mechanisms need to be established in order to achieve the principle of adaptative security based on autonomic systems in the field of security relating to the Internet of Things.

On the other hand, sustainable development has promoted greater efficiency in terms of resource use, which is one of the fundamental principles of green computing (Green 1.0). Indeed, it focuses on the efficient use of computing resources in practice, motivated by the need to reduce the use of materials harmful to nature, and maximize energy efficiency and life product [11]. In addition, the Green IT (2.0) [12] initiative is a good means of indirectly contributing to catalyzing economies of energy by using smart protocols and communications to reduce the emissions coming from other technologies and business sectors. In short, we would like to minimize the overall energy consumption of security mechanisms (Green 1.0), as well as to use ICT to contribute indirectly to reducing emissions (Green 2.0).

In this section, we introduce our SARM Framework for Green IT 2.0 and explain its components and functionalities. In addition, we have evaluated the Framework based on a case study of pollution detection in Geneva through a mobile WSN with the intention of managing transport traffic and thus energy consumption.

Adapted SARM for Green 2.0

We have used an adapted version of SARM called Green-SARM for the application domain of wireless sensor networks applied to a case study of pollution detection in the city of Geneva, which is an application for both Green 1.0 and 2.0 initiatives.

7.5.1 Sensor Energy Consumption

A typical sensor node processor operates at 8 MHz, with 4KB of RAM, 128KB flash and ideally 916 MHz of radio frequency [13]. Table 23 shows that receiving data utilizes almost half the amount of energy used for sending, which is between 5 and 25 times the average energy needed for computing. This is why the computing energy needed for our trust and detection functions is really insignificant in comparison with that needed for transmission.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective data rate</td>
<td>12.4 kbps</td>
</tr>
<tr>
<td>Energy to transmit</td>
<td>59.2 μJ/byte</td>
</tr>
<tr>
<td>Energy to receive</td>
<td>28.6 μJ/byte</td>
</tr>
</tbody>
</table>
7.5.2 The Main Problem: use case

Geneva is an international city, a financial hub and a worldwide center for diplomacy and for the UN. Geneva is the most popular and the second most populous city in Switzerland.

During summer, traffic jams unfortunately make the city polluted. To apply the objectives of Green IT 1.0 and 2.0, we seek to minimize this pollution by implementing the following:

1. A sensor network will be deployed based on cheap Zigbee transmitters to monitor the level of pollution (CO2).
2. Every transmitter will be attached to a car or a pedestrian.
3. There will be multiple fixed base stations that will collect information on CO2 from the sensors.
4. Some information will be exchanged within a fixed range and an evaluation of data consistency will be rated as a trust.
5. The data obtained will be aggregated by weighted averages according to the trust based on the collected information.
6. Thereafter, recommendations will be disseminated among drivers and walkers to enable them to avoid places where the pollution surpasses a certain level, and simultaneously, trust information about every transmitter will be send to the participants.
7. Finally, the traffic will be managed in real time through the use of action plans capable of reducing the volume of emissions and thus avoiding peaks in pollution in advance.
7.5.3 Implementation of Green-SARM

The control system of the SARM Framework is ideal for a collaborative environment whereby the decision making trust function of the security element must interact with other users in order to come to an adequate decision. In Fig. 70, we describe module by module, how SARM is applied to the application domain of our validation, becoming the Green-SARM version. First of all, the security means, which can be tuned by SARM, are used to block connections to rejected sensors. However, the application could potentially use authentication and encryption methods with all rejected sensors. The application preference is to maximize the usage time while maintaining sufficient security. The context gathering module is used to collect and distribute trust values between the Base Station (BS) and the nodes (sensors). These values represent a sensor’s trust of its neighbors. They are summarized in Table 23.

Table 23: Behavior and recommended value sent by Base Station to Sensor for Sinkhole and Jammer attacks

<table>
<thead>
<tr>
<th>Sensor behavior towards neighbors</th>
<th>Recommended value to Sensor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>Good (1) = Pos</td>
</tr>
<tr>
<td>Sinkhole or jamming of neighbors</td>
<td>Bad (-1) = Neg</td>
</tr>
<tr>
<td>“Who are you?”</td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td>Neutral (0.5) = Neu</td>
</tr>
</tbody>
</table>
Attackers are detected when they come within a given range of a BS. The network is configured with messages following a given communication protocol to establish connections, as described in Figure 74. In fact, according to the protocol, only BSs and attackers send messages asking "who are you?". As the BSs are too far from each other, if a message of this type is received, it means that it is sent by an attacker. In this case, the base sends a "Bad" message to everyone to indicate that an intruder is present and the BS updates its trust using a centralized database.

![Communication protocol based on soft security](image)

The values are sent to the management unit for analysis using a Trust Function (TF) that will assert whether or not an algorithm has to be used, and which one if so. In addition, the performance is fixed as energy saving in accordance with the Application Preference, which is to maximize the lifespan.

One of our uses of the TF is explicated in Equation 28:

$$ TF_j = \frac{(2\text{Pos}-2\text{Neg})}{(2\text{Pos}+2\text{Neg}+ \text{Neu})} \quad \text{Equation 28} $$

For all j sensors
if (TF$_j$ > threshold )
Accept connection
or else, if { TF$_j$ <= threshold}
then {reject connection and use encryption and authentication if required}
End of for loop

The TF will be used to calculate the weighted average of pollution values gathered from the sensors and also to minimize the overall energy consumption.
Implementation and analysis of the system would be difficult and complex. This stems from the fact that every sensor acts independently of the others. Therefore, our model will be studied using simulation tools in order to compare it with reference cases. Indeed, each sensor sends data packets to a number of sensors within a defined range according to the threshold used as policy. Thanks to its context gathering module, the TF has all the information with which to evaluate the trust.

**Attackers**

The behavior of a node is fixed at the start of the simulation based on uniform distribution, which has an average equal to the rate of attackers. There are many forms of attack but we will consider only two:

- Jamming attack: given the sensitivity of the wireless medium to noise, a node can cause a denial of service just by transmitting signals at a certain frequency. This form of attack is implemented just by sending a packet repeatedly.
- Sinkhole attack: the node tries to attract most of the paths to itself, like a concentrator, in order to have control over most of the data flowing through the network. To do this, the attacker must appear very attractive to others, presenting optimal routes. This is implemented by imitating a BS or any good node.

Note that we do not treat Sybil attacks.

**Metrics**

Due to the characteristics of a WSN, its major objective is to fulfill its mission, even though some of its nodes may be out of use due to attackers. Indeed, this means to ensure the WSN’s survivability, which can be defined as its “capability to fulfill its mission, in a timely manner, in the presence of intrusions, attacks, accidents and failures” [14].

The gain in terms of survivability is the ratio of:

- the amount of time that elapses before 75% of the total number of nodes run out of battery due to attacks, without using our Framework to
- the amount of time that elapses before 75% of the total number of nodes run out of battery when using our Framework.

### 7.5.4 Implementation and Validation Methodology

We have implemented Green-SARM and validated it through the use of a mobile sensor wireless network simulation developed using AnyLogic, which is a simulation tool that supports all different simulation methodologies. It is based on Real-time UML, Java object-oriented language and an agent based model.
**Model Set-up**

Each Sensor is associated with a given agent matching its location and behavior.

Setting up our security model using Table 23, we can take advantage of state charts by monitoring the behavior of agents. The state of our agents is controlled by state charts, which represent the exact behavior of sensors, as shown in Figure 75. Using AnyLogic as an implementation platform, agents and state charts can be programmed very conveniently. Particular modifications and/or extensions of the final model can be handled in a simple way.

![State chart of sensors](image)

**Figure 75: State chart of sensors**

In Figure 75, each Agent (Sensor) starts at state Init. The Agents are switched to their relative states (Sinkhole, Jamming, Base Station, Sensors) according to the percentage of attackers, BS and Sensors. They are then added to a sensor’s list whenever they are within its range.

We used Agents with one of the following behaviors:
1. Normal state
2. Sinkhole and Jamming behavior (as attackers)

Each Agent is then processed based on the monitoring unit’s decision as to whether or not to choose a security means. Thus, an Agent could transit to another state or remain in the same state. When arriving at a minimum defined level of Energy according to the sensor’s real consumption (see Table 22) the Agent transits to Sensor_low; and then transits to Sensor_off when the Agent has insufficient energy to transmit data. The Agent transits to Rejected state when its TF is lower than the Threshold. The state chart Trust updates the trust each time the Base Station receives information about a sensor. Of course, the BS is not limited in energy and also has access to a trust database to spread it across its range.

In order to study the model thoroughly, we have introduced factors:
ImmunityRate: when the TF of a Sensor reaches this value, it has double the influence on its “Good” values. This is a catalyst to accelerate convergence.

   a. Limit: this is the TF’s threshold for rejecting sensors.
   b. JudgementError: this defines an error rate among the large number of messages received and helps to study the robustness of the model. It is useful in our case where errors are very frequent due to the media utilized.

**Validation Methodology**

We have carried out simulations based on 0%, 20%, 40%, 60% and 80% half-and-half sinkhole and jammer attackers. Furthermore, the network topology was set to a random distribution of sensors. We have distributed uniformly the received packets over the neighbors.
Normally, the BSs are spread randomly across the network. In our experiments, we have validated our proposed solution and analyzed its extended performance based on a range of various scenarios, where we have fixed up to ten BSs. All sensors are spread over a square topology and operate over one day of simulation time. The Base Station coverage extends to a large circle but has no contact with the coverage of other BSs. We have deployed the sensors in an incremental mode, from S1 to Sn. As the device is not static, we have modeled its mobility using a random variable model. The movement pattern of mobile clients was totally randomized in order to reflect a real application. To achieve this, we used the Random WayPoint (RWP) mobility model [1]. All the nodes are mobile and their pause time is a randomly uniform variable. The time is measured in minutes and is in a range [0:50,000] adapted to sensors' batteries.

**Scenarios**

We have used three scenarios to validate our model. In our scenarios, sensors (agents) are divided into four categories.

Those with normal behavior are designated N sensors set in the range of [100; 1000]. The trust threshold has been optimized, after many series of simulations, to 0.3.

Sinkhole and jammer attackers account for the same amount of sensors.

In the first scenario, we fixed the number of sensors at: N have normal behavior, plus 10% of N are sinkhole attackers and 10% of N are jammer attackers.

In the second scenario, we fixed the number of sensors as: N have normal behavior, plus 20% of N are sinkhole attackers and 20% of N are jammer attackers.

In the third scenario, we fixed the numbers of sensors as: N have normal behavior, plus 40% of N are sinkhole attackers and 40% of N are jammer attackers.

**7.5.5 Results Analysis**

During our analysis, we firstly studied the performance of Green-SARM in the three defined scenarios, where sensors were arranged at random. Secondly, we studied the scalability of the model. Thirdly, we studied the robustness of the model based on the Error factor. For comparison purposes, we plotted the Green-SARM for 1000 sensors in Figure 77 and did the same, but without trust, in Figure 78 for the first scenario. We can easily conclude that SARM is largely better than would normally be the case without security trust; a ratio of 6.5:1 is reached and we can see this in a relatively short time – 1000 minutes, compared to the maximum time of 50,000 minutes. Indeed, the SARM's feedback mechanism has the desired effect. An example of 500 sensors without Green-SARM security is plotted in Figure 79. We can clearly see that attackers can quickly diminish the survivability of a network.
Figure 77: 1000 sensors for the first scenario (Green-SARM)
Figure 78: Network of 1000 Sensors for the first scenario (without SARM)

Figure 79: 500 sensors for the first scenario (without SARM)
In Figure 80, we plotted the scalability of the model as a function of a number of sensors using Green-SARM for the first scenario. This graph clearly shows that our model is scalable. As the number of sensors goes up, the network survivability also increases.

Figure 80: Gain in terms of survivability for 20% rate of attackers for \([100,1000]\) of sensors

For purposes of comparison, we plotted the Green-SARM based on 20% of sensors being sinkhole attackers (the second scenario) using our TF in Figure 81, and also without trust in
Simulation and Evaluations

Figure 82. We have contracted the figures so that they fit onto one page. The results clearly demonstrate that the level of survivability is boosted.
Figure 81: graph of 100 sensors for the second scenario using Green-SARM

Figure 82: graph of 100 sensors for the second scenario (without-SARM)
In Figure 83, we plotted the gain in terms of survivability of the model as a function of the percentage of attackers using Green-SARM. Therefore, we have proof that Green-SARM can ameliorate the level of survivability up to a rate of about 2 when a network is coming under more frequent attack as compared to a passive security network.

The JudgmentError factor, which defines errors of the TF, was set to 10%, but the variation in the results was less than 1%. This illustrates the robustness of the Green-SARM Framework.

All the results show the clear advantages of Green-SARM, even if 80% of sensors are sinkhole or jammer attackers. We can conclude that our security monitor helps the WSN to operate even when it comes under attack from 80% of its sensors (attackers) thanks to the looping system connected to the context gathering monitor and the TF.

### 7.5.6 CONCLUSION

We have proposed a Security Adaptation Reference Monitor based on security adaptation and Green IT concepts and the Autonomic Computing Security pattern in order to support both context monitoring and behavior control. This chapter also presents the validation of SARM for the sphere of WSN. The results clearly show that Green-SARM copes with survivability and network energy loss even coming under sinkhole and jamming attack from 80% of sensors. Indeed, Green-SARM constitutes a good platform within a Base Station to detect any sinkhole, eliminate it from its connections and put it into a log file, thanks to the context gathering monitor and the looped regulation system. Therefore, we show
that our Framework is efficient in this context and is tuned to achieve the best trade-off between security and performance according to application preferences. In addition, the network is well balanced in terms of energy.

7.6 General conclusion

We launched a set of measurements and used cases simulation studies to evaluate our Framework for different environments and contexts. Herein, we presented the validation of SARM in the following cases:

I. Wi-Fi contexts in proximity based wireless networks
II. Wi-Fi confidence levels based on the trust and reputation approach applied to Hotspots rated and ranked with SARM.
III. WSN networks during a number of famous attacks
IV. Finally, Mobile WSN during certain attacks in service of the green IT initiative.

The results show that SARM copes with a dynamic security changing environment and efficiently responds in terms of adjusting the adequate security means whilst ensuring survivability and preserving battery life. At this stage, we have carry out a proof of concept of our Framework. However, a comparison with other works is needed and that is the next section purpose.

7.7 Related Work and comparison

The most relevant papers found related to resources computational efficiency when providing security, particularly for data encryption are highlighted below.

7.7.1 Motivation and evaluation

Firstly, there are some developments in security systems that integrate ab initio adaptive mechanisms at the hardware, operating system, network and application levels, but there is a general awareness that the subject is relevant and is in need of additional research and development [15]. This author presented methodologies designed to adapt security in order to respond to dynamically changing behavior during runtime.

Indeed, Elkhodary indicates the need for further research on the trade-off between security and efficiency in using computational resources. In addition, he emphasizes the fact that security typically generates overheads regarding resources.

Focusing on applications for mobile devices, where the context is constantly changing and requires continuing adaptation, this work presents guidelines for adaptive security systems. Elkhodary [15] and McKinley [16] highlight the fact that security must react adaptively not only at the application level but also at the operating system level. Accordingly, it adapts the means of response at different layers when the threat level changes due to certain contextual events.

Elkhodary et al. have the same opinion as others about the complexity of ICT
systems. As a matter of fact, they make the complexity the more important barrier to robust security system. Therefore, they proposed to use adaptive security system and classification schemes. Indeed, they extended the McKinley classification scheme, which are both exploited in Figure 86 and Figure 87 to evaluate SARM.

First, McKinley identified three perspectives of adaptive security services. He did not look only for the presence of the three services but also for them to be adaptive (see Figure 84). Then, Elkhodary had extended this approach to evaluate an adaptive method. In this respect, he defined the adaptive method perspective, which examines the reconfiguration mechanism employed by adaptive system in terms of three dimensions: computational paradigm, reconfiguration scale, and conflict handling [15] (see Figure 85).

![Figure 84: Dimensions of the security services perspective](image1)

![Figure 85: Dimension of the adaptation method perspective](image2)

Secondly, Chen et al. in [17] introduce a model that provides a balance between security and quality of service.
This model assumes that the cryptographic algorithms are evaluated by key size and uses weights according to their computational complexity in order to define the level of confidence provided.

Chen’s model integrates the performance impact caused by the processing of these algorithms in wireless networks, due to the overheads in the allocation of resources.

7.7.2 Comparison

The references that are used for comparison purposes are the following:

Firstly, for WSN, a mechanism of dynamic adaptation is found in reference [18], which adapts the security gradually via the selection of cryptographic algorithms. The authors argue that QoS should be supported while optimizing security and power consumption. According to the authors, their model aims to provide priority-based delivery packets, while optimizing security requirements subject to specific energy constraints.

Their work also highlights the fact that one of the most relevant topics in the literatures is the complexity of adapting security, especially during runtime. The authors then propose a mechanism that dynamically handles adaptation security in accordance with the security requirements of the applications and the relevant power constraints. Based on the principle of adequate security technologies – which argues that information must be protected at a consistent rate depending on the value of the information – the authors applied a security adaptation model in accordance with the context [18].

Secondly, other works utilize adaptation techniques for smart devices with limited resources. They investigate some algorithms, considered in a number of given scenarios. [19]. Hamad et al. describe an experiment to investigate the computational requirements for some of the most popular cryptographic algorithms, with reference to power and to consumption of resources. In order to prevent attackers from gaining access to sensitive information, security levels are defined within a network, based upon threats and the value of the protected assets. Security policies impose the compulsory usage of several mechanisms that protect the information.

Thirdly, a service of adaptive encryption is proposed by Izquierdo et al. [20]. This model takes into account the limitations of processing power and security requirements. It consists of data encryption architecture, using more than one algorithm to encrypt multiple blocks of information. When it comes to confidentiality (achieved through encryption techniques), we find that the special characteristics of block cipher modes force us to employ “all-or-nothing” approaches. The authors present a novel solution for this problem, which confronts performance and security problems using concepts taken from partial encryption and parallel encryption modes.

Fourthly, focusing on performance, Rocha et al. [21] propose an adaptive middleware capable of dynamically selecting security protocols in the link layer, which uses parameters based upon the wireless network, system resources and security levels. These different types of data are accompanied by specific
Finally, our SARM (Security Adaptation Reference Monitor) has been proposed in order to deal with dynamic wireless network environments, and also supports an approach using flexible methods in order to deal with security dynamically, at runtime and making use of context gathering principles. We propose a generic adaptive security reference monitor in order to consider performance with respect mainly to energy consumption. The Framework also makes use of an adaptation security runtime in the wireless network in order to mitigate the consequences of the substantial number of threats in cases when one cannot eliminate them entirely, because there is no awareness of what security mechanism should be used in certain applications in order to protect against threats in a sufficiently dynamic manner. Therefore, it is glooming to choose dynamically the best adequate means in accordance with adaptive security objective.

**Evaluation**

We have used the abovementioned evaluation criterions to point out the advantages and drawbacks of SARM and to compare it with other approaches. We have carried out three evaluation processes of SARM.

Elhodary et al. share the opinion of Dan Geer et al in this area about complexity. As a matter of fact, they situate the characteristic of complexity as the principal barrier to achieving a robust security system. Therefore, they propose to use adaptive security systems and related classification schemes. Indeed, they extended the McKinley classification scheme, which is exploited latter, in order to evaluate SARM.

The first comparison is relative to some other approaches and their relative requirements. Therefore, we have dressed Table 24, which illustrates the main adaptive security aspects of SARM, which respects the security requirements of highly dynamic networks. Indeed, due to the fact of genericity of our Framework it covers almost all adaptivity requirements, mainly an efficient use of resources and the approach of cross layer are widely assimilated in SARM compared to other approaches.

In Table 24, we show that some aspects considered in SARM covers many adaptive security requirements of highly dynamic networks compared to other frameworks, notably cross-layer approach and independence from application.
Table 24: The main characteristics of SARM and of 4 other frameworks.

(F: Fully; N: None; P: partially; U: undefined)

<table>
<thead>
<tr>
<th>Approaches proposals</th>
<th>Survivability</th>
<th>Security scalability</th>
<th>Sensitive to Context</th>
<th>Economy of resources</th>
<th>Keeps always level of security higher</th>
<th>Dynamic Adaptation</th>
<th>Cross layer</th>
<th>Independent from application</th>
</tr>
</thead>
<tbody>
<tr>
<td>El Maliki</td>
<td>F</td>
<td>P</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>P</td>
<td>F</td>
</tr>
<tr>
<td>Taddeo</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>P</td>
<td>F</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Hamad</td>
<td>U</td>
<td>F</td>
<td>N</td>
<td>F</td>
<td>F</td>
<td>P</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Izquierdo</td>
<td>U</td>
<td>U</td>
<td>F</td>
<td>F</td>
<td>P</td>
<td>F</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Rocha</td>
<td>U</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>P</td>
<td>F</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>

Secondly, we have also evaluated SARM related to 20 major autonomic characteristics describe in Chapter 4., Table 11. We have dressed a grid to assess SARM in respect the fundamental requirements of autonomic system.

Table 24 represents an evaluation grid used to assess SARM related to the fundamental requirements of autonomic systems. SARM fulfills the majority of the requirements thereof. Nevertheless, some requirements are not covered in any way whatsoever due to the design of SARM, which requires an extension to cover fault tolerance and recovery at node level.
### Table 25 Main characteristics of SARM in Autonomic system

<table>
<thead>
<tr>
<th>Autonomic characteristics</th>
<th>F Full, P partially, N None</th>
</tr>
</thead>
<tbody>
<tr>
<td>all secure layer</td>
<td>F</td>
</tr>
<tr>
<td>Anomaly detection</td>
<td>P</td>
</tr>
<tr>
<td>Autonomy</td>
<td>F</td>
</tr>
<tr>
<td>Disposability</td>
<td>F</td>
</tr>
<tr>
<td>Distributivity</td>
<td>F</td>
</tr>
<tr>
<td>Diversity</td>
<td>F</td>
</tr>
<tr>
<td>Dynamically changing coverage</td>
<td>F</td>
</tr>
<tr>
<td>Fault tolerance</td>
<td>N</td>
</tr>
<tr>
<td>Immune learning</td>
<td>P</td>
</tr>
<tr>
<td>Immune memory</td>
<td>P</td>
</tr>
<tr>
<td>Integration with other systems</td>
<td>P</td>
</tr>
<tr>
<td>Multilayered</td>
<td>P</td>
</tr>
<tr>
<td>Noise tolerance</td>
<td>F</td>
</tr>
<tr>
<td>Pattern recognition</td>
<td>P</td>
</tr>
<tr>
<td>Predator-Prey pattern response</td>
<td>P</td>
</tr>
<tr>
<td>Resilience</td>
<td>P</td>
</tr>
<tr>
<td>Robustness</td>
<td>F</td>
</tr>
<tr>
<td>Self Identity</td>
<td>F</td>
</tr>
<tr>
<td>Self organization</td>
<td>F</td>
</tr>
<tr>
<td>Uniqueness</td>
<td>P</td>
</tr>
</tbody>
</table>

Thirdly, we have carried out an evaluation related to McKinley and Elkhodary perspective dimensions.

![Diagram](image)

**Figure 86: Evaluation of SARM related to security services perspectives**

Figure 86 depicts the adaptivity of SARM related to McKinley perspectives. In
fact, SARM provides a very generic and simple mechanism for implementing adaptive security means. User might define polices, authentication and authorization are in the scope of SARM. Nevertheless, the details of their functionalities are beyond the scope of the framework. However, tolerance at node level is not in the scope of the current design of SARM. It should be addressed in the future work, even though tolerance is admitted at network level.

Figure 87 illustrates the evaluation of SARM related to Elkhodary approach. In fact, SARM is good at conflict handling and reconfiguration scale. However at computation paradigm, it is at component-based composition level, which is the ability to rewire different implementation of a well-defined component at runtime without recompilation, which is the main adaptation paradigm supported by SARM for composing security component to application level. Indeed, our Framework is based on means that are components considered as black boxes that can be added or removed at runtime and thus is not at all oriented to a full computational paradigm.

The conflicts at node level in SONs network are not covered by SARM, but at network level the conflicts are handled autonomously. In fact, it detects conflicts among nodes and manages them at a network level. Nevertheless, we could also manage the conflicts at an interactive level, which is a compromising solution between autonomous and user-driven.

**Discussion**

The primary objective of SARM is fully achieved, namely designing and implementing a generic adaptive security Framework for the experts, designers and developers of security systems. In fact, it is an effective and user-friendly
tool helping them to meet the security requirements of highly dynamic networks and to have a methodical and systemic approach to ensure interoperability, efficiency, and adaptability of countermeasures to face various attacks and security breaches.

SARM is divided into a functional unit and a monitoring unit linked by a feedback control system. The Framework is adapted to a cross-layer security approach. As a result, it will reduce overheads even at very high levels.

To reduce the system’s complexity and to make the system incremental, we propose a feedback loop framework, that is, the system will automatically tune to its best configuration based on its particular monitored context, thus avoiding any static decision making.

However, our Framework does not satisfy the full range of the requirements indentified by the scheme. It needs a further research to investigate other axes of adaptive security and to resolve, amongst other things, policies conflict by using for example formal methods based on policy language and to implement tolerance at node level.

7.8 Summary

This chapter describes the implementation of SARM and related validations. The validation process and some experiments provide proof of the concept of the feasibility of SARM. Indeed, we have shown that SARM adapts the security means to security requirements of each dynamic network.

Four different use cases applied to different scenarios were used in this research. Simulations were used to evaluate the four cases. The results and analysis of the simulations indicate that SARM is a foundation framework in the field of security adaptation in SON.

Finally, we have carried out a comparison process to evaluate relatively the performances of SARM and stated that further evaluations are also needed to extend the spectrum of our proof of the concept.
7.9 REFERENCES


4. G. Preston, “Don't fall victim to the 'Free Wi-Fi' scam” In: ComputerWorld Networking & Internet, 2007


Chapter 8. Conclusions and Future Work

“You have to start with the truth. The truth is the only way that we can get anywhere. Because any decision-making that is based upon lies or ignorance can't lead to a good conclusion.”
— Julian Assange

8.1 What have we learned?

We have provided a large review of the state of the art security in the field of SONs and cellular networks. In addition, we have studied both the actual and future trends in these networks and have presented with details their security requirements and as well as an exhaustive study of attacks. Then, we have emphasized on two major paradigms applied to SONs (trust and reputation, and autonomic system) due to their strong link to adaptation security.

Actually, there are extant studies in the field of adaptive security and their applications but they are not addressing the majority of attacks. Indeed, conventional security approaches, largely applied, are constructed on static basics without much regard to actual threats. These treats need a formal dynamic approach to tackle them. In fact, the majority of attacks are changing on runtime and a holistic security approach is energy and time consuming. In addition, the majority of wireless devices are running on limited battery energy, particularly in highly dynamic networks such as SONs.

To address these inadequacies, we have firstly proposed a generic adaptive security framework named Security Adaptation Reference Monitor (SARM), based on the Reference Monitor concept and the Autonomic Computing Security pattern, in order to support both context monitoring and behavioral control.

Secondly, we have enhanced the Framework with diverse means such as digital identity management, PKI and trust. Our energy experiments and SC-SD implementation have given a solid foundation for all our simulations.

Thirdly, we presented the validation of SARM in different contexts, mainly in that of highly dynamic networks, such as WSN and MANET. We have addressed in this dissertation diverse adaptive security issues and challenges, and we have established a milestone on the road toward a complete solution to adaptive security challenges. We hope that our work will be evolutionary in the field of security and will help designers and developers to tackle timely security problems in highly dynamic networks.

Therefore, we have learned that the trends in cellular networks are toward satellite wide coverage and more energy consuming. In addition, trends in wireless networks are towards both dynamism and mobility, in addition to the devices limited energy. Then, we have found that the attacks on SONs networks
are diversified and no security system is adapted to all these attacks and threats. Indeed, their security requirements are so diversified that they need new mechanisms in order to satisfy them. We have also learned that system complexities as well as largely deployed conventional static security approaches are the principal barriers to achieving a robust security system to tackle dynamic attacks, mainly when changing on runtime. As a matter of fact, due to the levels of system and network complexity, an adaptive security system dealing with energy consumption and survivability cannot be a basic static component that might contain some state-of-the-art solutions. Moreover, it is difficult to deploy conventional security solutions in attempting to tackle new, emerging forms of attack - and new vulnerabilities. Then, we have learned that the high level of dynamism and the volatility of the network’s topology and components need ab initio a well designed and flexible framework in order to respond to runtime environmental changes. Next, we have also found that autonomic system characteristic and adaptive security approach are the ideal security solutions to meet the SONs’ security requirements at the beginning. In addition, Trust management system is one of the most adequate approaches that can be used to enforce the security mechanisms in SONs and solve problems that are beyond the power of traditional cryptographic security measures. We have then established a generic Framework called SARM capable of adapting dynamically on runtime adequate security countermeasures based on above-mentioned paradigms and approaches.

8.2 Conclusions

A single security solution does not represent an efficient means of dealing with all wireless networks and all devices. We thus require an appropriate means of dealing with each specific attack in each specific wireless network. Static networks or those that display a low level of variability relative to their normal characteristics could be securely managed with the classical approach. On the contrary, a highly dynamic network requires an adaptive solution in order to tackle the changing requirements in real-time. The design of such a framework, one that is context aware and that adapts the means based on the context and polices is looming on the horizon.

In this thesis, we tackled this challenging problem of adapting adequate security means that are capable of matching application requirements, user preferences and policies, while optimizing system performance such as energy consumption. Firstly, we introduced the subject and treated the fundamental questions involved in brief. Then, we gave a background assessment regarding wireless and mobile networks, including a literature review, constituting a state of the art of the subject. Next, we demonstrated the dynamism of SON networks. Therein, we stated their objectives and listed their security requirements, as well as discussing attacks on SONs. Secondly, we addressed the problem statements and the methodology of our approach. In so doing, we introduced the Framework and trust and reputation mechanisms. Thirdly, we focused on two main subjects, namely autonomic systems and adaptive security. Fourthly, we argued for the importance of having an adaptive security means in a dynamic network and presented the design and methodology description of the
framework. Furthermore, by using adaptation policies, it is possible to tune the adaptation mechanism and to customize it according to specific applicative scenarios.

Finally, we launched a set of measurements and used cases simulation studies to evaluate our Framework for different environments and contexts.

Herein, we presented the validation of SARM in the following cases:

I. Wi-Fi contexts in proximity based wireless networks
II. Wi-Fi confidence levels based on the trust and reputation approach applied to Hotspots rated and ranked with SARM.
III. WSN networks during a number of famous attacks
IV. Finally, Mobile WSN during certain attacks in service of the green IT initiative.

Indeed, we validated different means within our Framework. The results show that SARM copes with a dynamic security changing environment and efficiently responds in terms of adjusting the adequate security means whilst preserving battery life. Indeed, Chapters 6 and 7 illustrate the implementation of our Framework for different use cases. The results also demonstrate that the solution using trust and reputation is more efficient to eliminate undesired and distrusted access points and malicious nodes.

8.3 Overall Conclusion

Our research reached three main goals:

Firstly, we provided a Framework that can be used to determine the suitable security means for a specific wireless network application under certain constraints, including those concerned with performance or/and minimizing energy consumption,

Secondly, we used up-to-date autonomic and adaptation security paradigms in order to craft a bespoke framework reinforced by trust and reputation mechanisms

Thirdly, we have implemented the Framework for WSN. The results clearly show that SARM copes with reliability and survivability of network energy loss under sinkhole attack, even when faced with higher rates of attackers. Indeed, we have evaluated our Framework via simulation and experiment in a specific context, using the trust and reputation functions in order to counter different security attacks. In this respect, we not only proposed the gradual adaptation approach, but we also demonstrated its feasibility by simulating the Framework during the first stage, and then by implementing it in tamper resistance devices during the second stage.

8.4 Contributions

Our research represents a contribution in the field of security and efficiency of mobile networks in the following ways:
This research demonstrates how wireless networks can be separated into different types of networks as well as their relative trends. Classifying wireless networks based on their requirements and objectives into distinct categories is aiming to identify attacks and threats and attributed then to their relative category. This has led to the ascertainment that the conventional security approaches are outdated to tackle the new dynamic attacks and threats during runtime. This kind of classification facilitates finding adequate security schemes for a given network.

This research has also led to an approach that intends to define a generic Framework to tackle correctly the dynamic attacks and to assess all performances, particularly the overhead energy consumption.

The difference between SARM and most of other approaches is that we address the security as a general and global problem based on autonomic system and adaptive security approach. Furthermore, our generic Framework can be easily adapted to diverse situation without losing its generalities. Indeed, SARM requires context to provide its control loop system with relevant information to perform the adequate security actions related to the specified attacks, context and so on. The benefits of applying SARM are gains in performance and energy efficiency on one hand, and respects of policies and user preferences on the other hand. These last parameters are providing SARM with more flexibility as well as precision, accuracy and finesse.

Our Framework is open and generic enough to deal with all security or/and energy consumption objectives, and even to incorporate new objectives or risks thanks to its risk management apparatus and policies.

We have defined an operational means with respect to performance. New mobile network applications can be easily integrated into our framework.

Thanks to reference monitoring, the Framework is incremental and provides a feedback control loop.

Many other control systems, such as fuzzy control, nonlinear control, analytic hierarchy processes or even any new control system, can be explored as a feedback control loop.

SARM as a context-aware and adaptive mobile network framework was designed, and was then implemented and evaluated for different networks in order to perform a precise efficiency set-point within a control system.

Our Framework defines parameter boundaries for the chosen security methodology. We have also defined the limit of virus propagation or eradication in mobile networks.

We achieved a realistic implementation model by integrating the Framework in a cryptographic Smart card SD for two mobile phones in order to secure integrally all their communications, and in the future, such technology could be directly integrated in the OS.

Security and protocol designers as well as system developers can use the Framework to determine how to secure their system appropriately and to secure it efficiently when the context is known. Finally, adaptive security means
combined with the control loop system can help to conserve resources and to
lengthen the survivability of the network.

8.5 Future research

Although this dissertation has answered how we design and address the
problem of dynamic on runtime threats with respect to adaptive security
objective including policies and user preferences, it opens up more research
opportunities and questions that are still unanswered.

Future work includes the extension of our Framework to support more
adaptation parameters (such us processor and memory usage) as well as
implementing SARM in a tamper resistant device that might be able to deal with
concurrent policies. Moreover, an internal feedback loop to control the internal
behavior of the device is needed in order to prevent misuse of the device or
node on the one hand; and to apply fault tolerance and recovery, on the other
hand.

More researches had to be carried out to extend our approach by integrating
SARM into SC-SD, particularly by implementing for example SARM directly in
the OS.

Another hot subject in mobile networks is virus propagation. The Framework
presented in this dissertation is a good mean to tackle this problem and to
define, amongst other things, the propagation limit rate of virus and their
eradication in any mobile networks.

Several other potential areas of research involve SARM and its components. For
example, different authentication and authorization mechanisms might be
included in the means, and many decision-making functions, such as fuzzy and
nonlinear functions, could enhance the flexibility of SARM. Our research can be
applied to any mobile network or device.

In addition, different learning methods would be researched for the adaptiveness
of the Framework to reach fruition. For the control loop system, increasing the
number of context related information to be processed at decision making
function will increase the energy consumption. A deep research has to be held
over this subject to ameliorate the usability of the framework. Strong context
metrics have to be also introduced as a global objective. Next, the functional and
management units can be potentially improved by integrating other components
to deal with fault tolerance. In addition, any contradiction raised by the policies,
user preferences and system decision must be addressed in real-time, which is
not cover at all. The scalability of SARM has also to be tested more deeply to
improve the credibility of the framework.

8.6 Final summary

This dissertation has reviewed past literature on cellular and wireless networks
(particularly self-organization networks), as well as autonomic and adaptive
security systems. We have designed a generic Framework called SARM that
can be used to find a suitable and efficient scheme in order to address
dynamically different attacks and threats for different types of wireless networks. We have shown how SARM adapts security means depending on its context, polices and user preferences. Finally, we have implemented SARM for diverse dynamic networks use cases and thus performed a proof of concept study.

Lausanne, 15th of Mai 2014

Tewfiq EL MALIKI