University *POLITEHNICA* of Bucharest
Faculty of Automatic Control and Computers, Computer Science and Engineering Department

PhD Thesis

in Computer Science, Information Technology and System Engineering

Security in Wireless Networks

Securitatea rețelelor mobile

presented by

Drd.ing. Alexandra-Elena MIHĂIȚĂ (MOCANU)

supervised by

Prof.dr.ing. Florin POP

2020
Bucharest, Romania

Contents

List of Figures

List of Tables

1 | Introduction

1.1 Research statement and thesis objectives

Starting with a successful connection between a client and a server made by Sir Timothy John Berners-Lee in 1989, the Internet has quickly evolved to a 4.57 billion of interconnected people. According to the Statistica website in [Cle20], this number of interconnected people encompasses more than 59% of the world population. More than 50% of the global Internet traffic is made by mobile devices, throught different wireless connections (2G, 3G, WiFi *etc*).

The increased number of users, the constant changing topology, the limited resources and the heterogeneity of the devices have made challenging granting security in wireless mobile networks. Attacks like sybil [JZE+19], clone node [NSK+20], intelligent spoofing [GNF+20], denial of sleep [FFBY20] and denial of service [PS20] in wireless mobile networks are the focus of research nowadays.

In the domain of wireless mobile networks, we decided to focus our research into the field of VANET, participatory sensing and wireless mobile networks where we study the prospect of securing each of these networks. Each use case of wireless mobile network has different topologies, types of communication and protocols among the nodes. These factors along with particularities of each of the use cases have determined different security approaches with different results, each presented in the following chapters. The results we have reached are based on the research questions and objective established in Table 1.1.

Therefore, the main objective of this doctoral thesis is the research, development and evaluation of a novel security model for wireless mobile networks.

We have identified three scenarios that can benefit from our research and solutions:

- vehicular ad hoc networks,
- wireless sensor networks,
- participatory sensing.

In order to find the best solutions, we have tried to answer a couple of research questions like:

1. **How can we secure a wireless mobile networks without affecting its performances regarding quality of service? (RQ1)**

   The answer to this question is addressed in every chapter of this thesis. In order to propose security for a wireless mobile network, we have to properly define the main attributes of the network and analyse its restraints. After that, we have to take into account the characteristics of the type of wireless communication used like range and propagation protocols. These specifications help in the choice of a security model.

2. **What is the impact on performance regarding quality of service when adding an encryption based security module in wireless mobile networks? (RQ2)**

   An encryption-based security module for wireless mobile networks is challenging due to both the overload in the network and the existing time-constraints. This thesis tries to prove that adding such a security model can be done but, at the cost of lost or incomplete communication between the nodes of the network.

3. **Can we define a trust model for VANET to ensure the security of the users involved the network? (RQ3)**

   Various models have already been proposed for trust and reputation model in VANET. The model we proposed is one of the most common: public-key based, using the .X509 certification standard to authenticate users and monitoring devices to determine the good or bad behaviour of the nodes in the network. The efficiency of the model has been tested by simulation using a UPB VANET Simulator.

4. **How do different scenarios of wireless mobile networks influence the definition a trust and reputation model? (RQ4)**

   To find the answer to this question, we have analysed multiple wireless mobile networks and have proposed different security models. These models have tried to answer the necessities of VANET, wireless sensor networks and participatory sensing.

5. **Should the wireless aspect of the communication in wireless mobile networks be treated as an integrated part of the network or should it be addressed separately? (RQ5)**

   When studying the different type of wireless mobile networks and proposing the various security models, we noticed the importance of the wireless aspect of the networks. Therefore, we proposed a model for treating the wireless aspect separately and another model which considers it a part of the node's behaviour. The results of this comparison are presented further on in the thesis.

1.2 Thesis outline

This thesis focuses on wireless mobile networks, their various applications and applicabilities and researches novel models to secure each of the use-cases addressed. The multiple security solutions are presented with their advantages and disadvantages. In Chapter 2 we present the main attributes and technologies which make possible the existence of wireless mobile networks, along with the main routing protocols and several known attacks. In the Chapter 3 we describe in detail existing attacks and their damage on the networks. Also, the comparative results of implementing several encryption algorithms both abstractly and in wireless mobile networks can be read. These experiments were made in order to show that performances depend greatly on the environment where they are made. In Chapter 4 the discussion is focused on the particular type of wireless mobile networks called vehicular ad hoc networks. A survey of existing approaches is presented along with the the security model proposed. In Chapter 5 we deal with a different type of wireless mobile network called participatory sensing. This application is discussed with respect to elder reintegration and proposes a security model tested stochastically. In Chapter 6 we deal with the wireless sensor network type of wireless mobile networks by proposing a Markov-based approach for security. In Chapter 7 we present the main conclusions of the research of this thesis with the main advantages and shortcoming of each of the security approach.

The thesis ends with the references that are in number of 177.

Research question	Research objective	Research methodology	Use case
RQ1	To emphasize the importance of the main attributes of wireless mobile networks like constant changing topology, limited time for interactions and limited resource capabilities and the fact that each addition to the network's structure reflects in the quality of service.	Proven stochastically and through simulations	The proper answer to this question is the entirety of this thesis, the main focus of our research being securing VANET, PS and WSN. Each of the security models proposed in this thesis has achieved some security properties at a cost of the performance of the networks where it was applied.
RQ2	To emphasize that the characteristic of a security method and the algorithm used varies greatly in performance according to the scenario where it is applied.	Proven by simulations	To answer this question, we implemented several encryption algorithms in an independent environment and then implemented each of these algorithms for encrypting messages exchanged between the users in a VANET in a simulated environment. The time for encryption and decryption of the messages between the users in VANET determined a huge drop in the total number of packets sent in the network. Details about implementation approach and results are provided in chapter 3 and in paper [MDM+15]
RQ3	To emphasize the importance of choosing the security properties which we want to grant. If privacy is important, then an encryption algorithm might be the best approach, but if authentication is the main goal, then public key cryptography might do best. A lot of research has been conducted towards securing VANET, most of which being user oriented.	Proven stochastically and through simulations	The answer to this question involved the implementation of a complex security model for VANET which aimed at solving most of the security attributes, through various methods, at the cost of network performances. More details about the increased duress on the network and its performances after adding an elaborate security model can be read in chapter 4 and in paper [MDP+17b]
RQ4	To show the strong correlation between the characteristics of the type of wireless mobile network and the trust and reputation based security model chosen.	Proven stochastically	To provide an insightful response to this question we analyzed various different approaches and then proceeded to proposed novel models to address the shortcoming of the existing models. In doing so, we proposed, implemented and tested various trust model in multiple scenarios like VANET, PS and WSN. The results of these security models can be read further in chapters 4,5 and 6 and in paper [MDP+17a]
RQ5	To show that trust in wireless mobile networks can be seen as a accumulation of user-based trust and communication-based trust.	Proven stochastically and through simulations	To address this question we proposed a user-only trust model in participatory sensing as a part of wireless mobile networks. We, then, analyzed the variations in trustfulness of the user when problems with the communication appeared. Those variations led to the belief that communication trust should be addressed separately. The implementation of a Markov-based trust model for wireless sensor networks as part of wireless mobile networks showed the importance of trust communication and addressed the shortcoming of the previous approach.More details can be read in chapters chapter 5 and 6 and in paper [MPME20]

Table 1.1. Thesis objectives and methodology.

2 | Wireless mobile networks

During the last decade, the wireless aspect of communication has passed from the stage of novelty to that of commodity. Nowadays, not being wireless connected to the Internet or having access to other devices has become the odd thing. Whether it be Bluetooth, WiFi, Satellite or 4G, 5G we all want easy access to our devices and to be able to remote control everything.

In this chapter, we present a survey of wireless technologies used in wireless mobile networks 2.1, then we address the security issues each type of wireless communication brings in 2.2. In section2.3 we present some of the tools used for simulating real-time conditions of wireless communication in wireless mobile networks. The result of these studies can be read in 2.4.

2.1 Wireless mobile communication technology in wireless mobile networks

In this chapter we discussed the importance of the The wireless based communication was first recognized and standardized internationally in 1997 and since then has known continuous evolution, developing subsequent amendments in the years that came.

The initial 802.11 standard, obsolete today, had two possible data rates of 1 or 2 megabits per second and forward error correction. As for the how, it could transmit over infrared at 1 MB/sec, using frequency hopping spread spectrum or direct sequence spread spectrum at 1 Mbit/s or 2 Mbit/s.

The 802.11a standard uses the 5 GHz frequency, less popular for usage but with serious environmental attenuation problems that degrease significantly the range of usage.

The 802.11b wireless networking standard reaches to 11Mbit/s and represents the first real-connection with the users, being the first widely available solution for users to buy. Its frequency for communication is in the band of 2.4 GHz.

The 802.11g standard s provides a theoretical maximum speed of 54Mbps at the frequency band of the 802.11b standard of 2.4 GHz frequency.

The 802.11n standard operates at data rates from 54 Mbps to 600 Mbps, and can use the 2.4 and 5 GHz frequencies. The 802.11n standard's main novelty is the increased speed of connection. This was able by allowing for bonded channels which doubles the radio spectrum of an 802.11a type of connection, and in turn doubles the data rates. Another speed enhancing technology is MIMO (multiple input multiple output) which uses multiple antennas on the client devices and on the provider's wireless access points in order to achieve diversity gain and reduce fading.

2.2 Shortcoming in wireless mobile communication technology

In order to secure the communication over any of the subsequent of the 802.11 standard, one can use a protocol like Wired Equivalent Privacy (WEP), Wi-Fi Protected Access or Wi-Fi Protected Setup (WPS). Each of these has had security breaches, which is why the Wi-Fi Alliance has updated its test plan and certification program.

The WEP protocol is vulnerable because it uses RC4 symmetric stream cipher algorithm which xores a stream of bits: the secret key with the plaintext into obtaining the ciphered text. This is then transmitted to the receiver where it is xored with the same secret key into obtaining the plaintext. The problem is the fact that a zero plaintext xored with a key results in the key itself.

The Wi-Fi Protected Access(WPA) protocol uses two keys: an integrity message check of 64 bits and an encryption key of 128 bits, both derived from a master key. This protocol has resolved the main issues of the WEP protocol but has been proven to be weak against dictionary attacks. These attacks imply the successive testing with words from a predefined list called dictionary and are different from brute force attack because they try only the most probable passwords.

The Wi-Fi Protected Access II(WPA2) protocol introduced the use of counter cipher block chaining message authentication code protocol (CCMP) and uses either the advanced encryption standard(AES) or the temporary key integrity protocol(TKIP). The second implementation was added in order to allow WPA compatibility.

The Wi-Fi Protected Setup(WPS) protocol is used in order to secure the settings of the access point along with those of the devices trying to connect to that access point.

Protocol	Encryption	Authntication	Data Integrity	Vulnerabilities	Complexity
WEP	RC4	WEP-Open and WEP-Shared	CRC-32	Chopchop, Bittau fragmentation, FMS, PTW, DoS	low
WPA	TKIP	WPA-PSK and WPA-Enterprise	Michael	Chopchop, WPA-PSK, Reset, DoS	high for WPA-Enterprise
WPA 2	CCMP and AES	WPA2-Personal and WPA2-Enterprise	CBC-MAC	DoS, MAC spoofing, Offline dictionary in the WPA2-Personal	high for WPA2-Enterprise

Table 2.1. Security Comparison between Wireless Protocols.

2.3 Wireless mobile network simulation tools

When trying to determine the best way analyze the performances of the security models proposed in this thesis, we faced the challenge of multiple existing simulator in wireless mobile networks.

A survey on wireless sensor networks in [MZ12] revealed free or open source simulators classified based on their main focus as follows:

- **emulator and code level oriented simulators**. These simulators are focused on the hardware element of the networks. In this category fall: ATEMU [PBM+04], Avrora [TLP05], EmSIm [TRJ02], Freemote Emulator [KMKW11], MSPSim [EÖF+09], TOSSIM [LLWC03] and VMNet [WLZN07];

- **topology oriented**. This category focuses on the ability to test algorithms and routing protocols. The only known simulator to the authors in this category is Ataraya [MZ12];
- **environment and wireless communication oriented**. These simulators are focused on the wireless aspect of the networks and emulate environmental issues that may occur in real life. In this sense, the authors mention Prowler [Szt04], Wireless Sensor Network Localisation Simulator and WSNet [JYX+18];
- **network and application level simulators**. These simulators make possible " transporting and processing gathered data". We mention AlgoSenSim [MF09], NetTopo [SWZ+08], SENSE [CBP+05], Sensor Security Simulator (S3), SHAWN [FKFP07], SIDnet-SWANS [GGD+07], Sinalgo [ANDK+18] and TRMSim-WSN [MP09];
- **cross-level**. These simulators make possible simulations of the wireless network at various degrees of abstraction. In this category we mention COOJA [EÖF+09], J-Sim [SHK+06] and Sensor Network Package [RKMC16], SENS [SKA04] and WSN-Sim [MZ12];
- **TCP, routing and multicast protocols oriented**. In this category are simulators mainly based on the NS-2 network simulator like: Mannasim [PRG15], NRL Sensorsim [BE19] and RTNS [PCL07];
- **software environmental oriented**. These simulators are OMNeT++ based and include: Castalia [Bou07], MiXiM [WSKW09], NesCT [VH08], PAWiS [MGH06] and SEN-SIM [LW82];
- **actor oriented**. In this category Ptolemy II based simulators can be observed like Viptos [CLZ05] and VisualSense [BKL+05].

Although, there were multiple choices available, the UPB VANET Simulator is, to the best of our knowledge, the first to implement security in VANET. Another simulator used in the process of analyzing the security model proposed in this thesis is TRMSim-WSN which is a specialized simulator for trust and reputation models in wireless sensor networks.

UPB VANET Simulator Sim2Car is the first simulator used for data testing and security emulation of the models proposed in the thesis. The university Politehnica Bucharest's simulator represents an 802.11b Wireless MAC layer, an UDP transport layer simulator whose routing and addressing schemes have been changed to depend on geographical position. The input of the simulator consists of vehicle mobility models according to which the vehicles are positioned on the map. Their trace is updated periodically in order to keep a realistic view of the grid. An interesting fact is that it takes into account trace rules and multiple types of driver behaviors.

TRMSim-WSN represents the second simulator we choose for testing and evaluating the trust and reputation model proposed in this thesis. Each trust and reputation model has its own specific characteristics and particularities. However, most of them share the same abstract schema or pattern about what steps have to be given in order to complete a whole transaction in a distributed system making use of a trust and/or reputation model. The main advantage of this simulator is its generic structure which allows versatility and provides wasiness of implemention of different trust and reputation models over wireless sensor networks.

2.4 Conclusions

In this chapter, we presented the most important aspects of the wireless aspect of the wireless mobile networks. In 2.1, we presented a short survey of current technologies in wireless communication. Each of the most common wireless technologies has shortcoming which are addressed in 2.2. A short description of several tools used in simulating wireless mobile networks was made in 2.3, focusing on the Sim2Car and TRMSim-WSN.

3 | Security approaches in wireless mobile networks

This chapter discusses various attacks on wireless mobile networks and multiple existing methods to counteract them. Firstly, we discuss about the Bouncy Castle library and the encryption algorithms implemented in this library. We make a comparison between them in terms of performances and also analyze their performance in a wireless mobile networks simulator. Secondly we discuss about the multiple trust and reputation models which can be applied in wireless mobile networks emphasizing their strengths and their lacking.

3.1 Attacks in wireless mobile networks

Raya and Hubaux [RH05] present a critical analysis of the evolution of vehicular security, from the early solutions designed to cope with tachometers, all the way to the use of GPS tracking devices and applications for smartphones.

Coming from a military background, the wireless sensor networks (WSN) have slowly, but steadily gained interest from user-perspective considering their low costs for securing different environments.

Authors in paper [SSV13] have made an analysis of the security challenges and attributes of a WSN by layers, while authors in paper [PLH06] describe the role of different security techniques in WSN.

An interesting classification of the main goals of adding security on WSN was made by authors in [PS^{+}09], emphasizing primary and secondary goals in table 3.1.

Main goal	Attributes	Description
Primary goal	confidentiality	ability to hide the contect of a packet from third parties.
	authentication	ability to trace each packet in the network to its source
	integrity	ability to grant that a received packet is the same as the sent packet, without alterations
	availability	ability to ensure that a node is ready and able to communicate its data using network resources
Secondary Goal	data freshness	ability to decide the accuracy of the packets received, even after determining that confidentiality and integrity goals are achieved.
	self organization	ability to recover and find new routes in order to send data
	time syncronisation	ability to make sure that all the nodes in the WSN are working accordingly to the same timestamps and therefore make accurate pathtracking
	secure tracking	ability to accurately know the location of a sensor in order to determine if a sensor is malicious, broken or under attack.

Table 3.1. A list of security attributes required in WSN.

Paper [Che15] presents a very well structured classifications of the main attacks present in WSN based on their approach. A summary of that classification can be seen in table 3.2.

Authors in paper [DBFH09] state that the main form of abuse can come from a malicious node in the network in the form of Sybil attacks or pollution and/or fabrication of information. Their solution toward the problem is an Angel-based approach which aims at providing data confidentiality and integrity. Their limitations come from the high dependency on the platform's

Goal Oriented Attacks	Active	Jamming, Blackhole, Sybil, DoS, DDoS, Man in the middle
	Passive	Traffic monitoring, Eavesdropping, Traffic analysis
Performed Oriented Attacks	Inside	Mole, Blackhole, Grayhole, Malicious attack, On-off attack
	Outside	Eavesdroping, DoS, DDoS, Resource exhaustion
Layer Oriented Attacks	Phisycal	Jamming, Eavesdropping
	Data link	Channel exhaustion, Traffic analisys, Sybil
	Network	Blackhole, Resource exhaustion, Node capture, Eavesdroppping
	Transport	Desyncronisation, DoS, Flooding, Resource exhaustion
	Application	Data coruption, Repudiation, Malicious node, BS path DoS

Table 3.2. A list of security attacks in WSN based on their approach.

computational capability.

According to users in paper [CRKH11] the main concern when talking about participatory sensing should be user privacy and how sensor data disclosure might affect it. They even try and redefine the term in order to better reflect the realities of participatory sensing networks as being the guarantee that participants maintain control over the release of their sensitive information. This includes the protection of information that can be inferred from both the sensor readings themselves as well as from the interaction of the users with the participatory sensing system.

Authors in [MMH+15] split attacks into the main vulnerability which they address.

3.2 Encryption algorithms testing for secure communication in wireless mobile networks

Obtaining security through cryptography is obtained by encrypting and decrypting all the data in the network. Taken into consideration all the implementation requirements and the main goal of this research's purpose (privacy), the symmetrical encryption is chosen due to being less computational challenging and time consuming.

Several symmetric cryptographic algorithms have been selected for message encryption: AES, AES Fast, AES Light, Blowfish, Camellia, Camellia Light, Tea and Twofish.

Algorithm	**Key sizes(bits)**	**Block sizes(bits)**	**Rounds**
AES	128	128	10,12 or 14
AES Light	128	128	10,12 or 14
AES Fast	128	128	10,12 or 14
Blowfish	32-448	64	16
Twofish	128,192 or 256	128	16
Camellia	128, 192 or 256	128	18 or 24
Camellia Light	128, 192 or 256	128	18
Tea	128	64	Variable(64 recommended)

Table 3.3. Symmetric encryption algorithms comparison

The **Advanced Encryption Standard (AES)** is an encryption algorithm which has three versions based on the key lengths of 128, 192 and 256 bits; the length, in turn, determines the number of encryption rounds (which can be 10, 12 and 14). The **AES Fast** algorithm is an optimized version of the AES algorithm in the sense that it uses 8KB of static tables to store precomputed round calculation. The **AES Light** algorithm is an optimized version of the AES algorithm in terms of footprint. It has no static tables, and therefore it is the slowest version of the AES algorithm. **Blowfish** has 16 rounds, and uses block sizes of 64-bits and keys with variable length between 32 bits and 448 bits. **Twofish** is one of Blowfish's successors. It has 16 rounds, and can support three possible key block sizes of 128, 192 and 256 bits, with data blocks of 128 bits. **Camellia** is another symmetric algorithm made by Mitsubishi. It has 18 or 24 rounds, and three possible key dimensions of 128, 192 and 256 bits, with fixed data blocks of 128 bits. The **Light version of the Camellia** cipher is optimized for size and therefore has a smaller implementation. The **Tiny Encryption Algorithm (TEA)** is one of the simplest in description. It has a variable number of rounds, although 64 rounds are recommended.

3.3 Trust and reputation security approaches in wireless mobile networks

Authors in [FZC+20] address the need for security in wireless sensor networks by splitting the problems into two large categories: outside and inside attacks. The outside attacks are said to be easily mitigated by using authentication and message encryption but, the inside attacks are the ones who can destroy completely the network. Authors mention trust and reputation models as the best security approach against the inside attacks by limiting the impact a user can have on the whole network.

The importance of wireless sensor networks and the need for security is emphasized also by authors in [PA13]. They mention both military and civilian applications and classify the possible attacks on wireless sensor networks as routing attacks and data traffic attacks.

The authors of paper [WCC+16] presented CATrust, a regression-based trust management model that evaluated resilience, accuracy and coverage properties through simulation and demonstrates that fact the CATrust model outperforms the existing approaches in missing good services and missing bad services probabilities.

Another interesting approach is cluster based, thus splitting trust in two: inter-cluster and intra-cluster [KSH+19]. In this paper, the authors make a clear difference between data trust and communication trust, a similar approach as the one proposed in this paper where we deal with user trust and communication trust.

Authors in paper [SKS20] present a more elaborate survey and taxonomy on energy management schemes in wireless sensor networks. The taxonomy presents both energy management approaches and energy preserving algorithms.

Trust and reputation based security for wireless mobile networks has become more popular and one of the most commonly used approaches. The use of cryptography-based security models for wireless sensor networks has become more and more unpopular, as cited in [NMBG20], due to the heavy computational load on the network.

Marmol *et al.* [MP10] propose a standardization of trust and reputation models in wireless mobile networks like ad hoc or wireless sensor networks. They emphasize common elements while trying to provide a set of preliminary steps for standardisation.

3.4 Experimental results of different security approaches

The algorithms described in section 3.2 have been tested in an independent benchmark, Crypto++ 5.6.0 [com20]. Crypto++ uses C++ language, the Microsoft Visual Studio 2005 compiler and an Intel Core 2 1.83GHz processor. The capabilities of the processor are very poor compared to those of current computers but not compared to the processor of wearable devices.

Taking into considerations the characteristics of the simulator as well as the characteristics of the algorithms, several implementation of security modules were made, one for each algorithm. These implementations have been made in order to create a comparative analysis between the performances of the algorithms both independently and within the Sim2Car simulator. The interest in this comparative analysis was to reveal how much does the choice of an encryption algorithm relies on the design of the application in which it will be used. The tests performed for this scope have shown different results. The performance of the algorithms were different in the two cases.

The computer on which the test have been conducted has the following configuration: 8 GB RAM of memory, Intel Core i5-3230M 2.6GHz Processor and Microsoft Windows 8.1 64 bit Operating System.

The tests for encrypting the smallest block size (1908 bytes) the best performance was that of the Blowfish algorithm, while the worst was that of the Camellia Light algorithm. The difference between the two algorithms is quite impressive, the worst having 4 times the time of the best. Encrypting the greatest data block (2480400 bytes) determined the AES to be the best algorithm and the Tea algorithm as the worst. The difference between the best and the worst algorithms is twice the time.

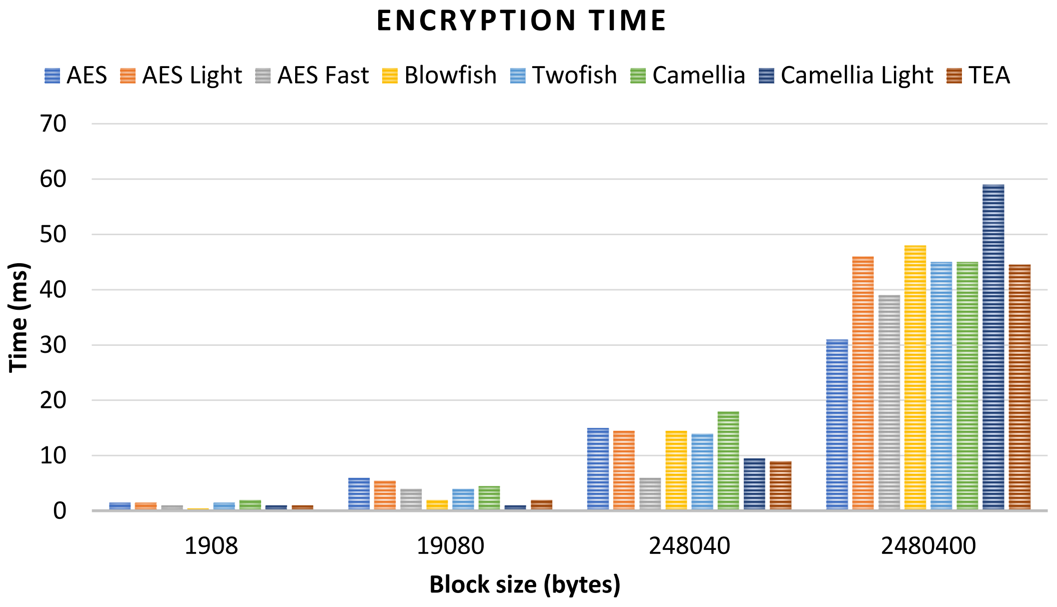

Figure 3.1. Encription time vor various data lengths.

The tests for decryption the smallest block size (1908 bytes) the best performance was that of the Camellia algorithm, while the worst was that of the AES algorithm. The difference between the two algorithms is quite impressive, the worst having 3 times the time of the best.

The decryption of the greatest data block (2480400 bytes) determined the AES to be the best algorithm and the AES Light algorithm as the worst. The difference between the best and the worst algorithms is very thin, only 7microseconds.

For small packets of data, the Blowfish algorithm proves to be the fastest, whereas the largest amount of data to be encrypted has revealed AES as being the fastest. These results are somewhat expectable since Blowfish is known to be a fast block cipher for small amount of data since it does not need to change the keys so often. The change of keys is the more time consuming in the cipher and when encrypting large amount of data the change of keys brings delays.

The simulation ran on the UPB's simulator have had the goal of monitoring the numbers of messages exchanges between the cars with each of the ciphers. The average packet size of the messages exchanged between cars is 220 bytes.

The result of the simulations has revealed a much larger number of messages exchanges between vehicles when using the TEA cipher. The simulation using this cipher has had the maximum number of messages exchanged at a certain point almost 4 times greater the number of messages exchanged with the other algorithms. The least efficient cipher was Camellia Light.

This shows that even though in an independent application the Blowfish cipher produced better time results, in the application the TEA cipher is more useful. The answer can be that for a limited amount of time, the time that two cars stay in each other's proximity, the fast time for both encrypting and decrypting the data blocks, allows more messages.

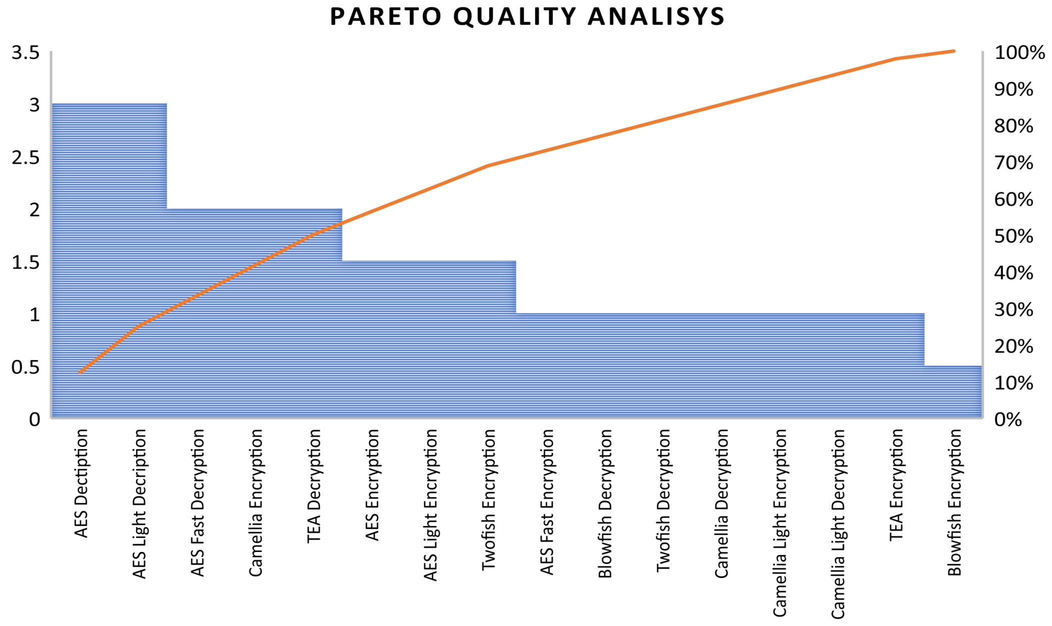

Figure 3.2. Comparison of the number of packets sent between multiple algorithms.

3.5 Conclusions

In this chapter, we discussed the various existing methods for obtaining security in wireless mobile networks. Firstly, in section 3 we discuss about the Bouncy Castle library and the encryption algorithms implemented in this library. In 3.3 we make an evaluation of current trends in trust and reputation models. In 3.2, a comparison between them in terms of performances and also analyze their performance in a wireless mobile networks simulator. A similar comparison is made for trust and reputation models emphasizing their strengths and their lacking.

4 | Security in VANET

Generically, as stated in the guidelines IEEE 1471-2000 and ISO/IEC 42010 and described in [LLZ^{+}15], the VANET architecture consists of three large domains: mobile, infrastructure and generic. The mobile part refers to the constantly moving elements of the network, whether they be vehicles or other mobile devices like phones. The infrastructure contains both the roadside part like traffic lights, as well as the centers where the traffic data is analyzed. The generic domain refers to the internet infrastructure as well as the private domains which allow access to the gathered information.

In VANET there are two types of communications: vehicle-to-vehicle(V2V) and vehicle-to-infrastructure(V2I). The V2V is considered to be locally, its main focus being on preemptive behaviour like prevention of accidents or preserving the integrity of the vehicle in the proximity of other obstacles or vehicles. The V2I communication is considered to have a more globally aspect since it can help create and gather information about the entire network, not just about the environment in the close proximity of the vehicle. This type of communication is used for the exchange of critical information about the network and can help create accurate estimates of future levels of traffic. Both these types of information are important in order to create a safe environment on the streets.

The proposed model is cryptography based using a public key infrastructure(PKI) to distribute and validate vehicles in the network. The communication between each two vehicles is secured by encrypting the messages using a common key obtain using the Diffie-Hellman key exchange algorithm. The V2I communication is secured using .X509 certificates.

In this chapter, firstly we present the theoretical concepts and challenges. In section 4.1 are presented the Equation and models for the trust management followed by the main results obtain threw simulation in section 4.2. The chapter concludes with the advantages and disadvantages of the proposed security model, as well as possible improvements in section 4.4.

4.1 A trust and reputation security approach in VANET

The concept of trust refers to who are the peers in one's group, which of them can be trusted and based on what can they be trusted. The first element refers to the vehicles or users in the network, the second element is a bit more difficult to define. In a subordinated hierarchy there is a root certificate authority that authorizes several descendants and only the certificates given by these entities are recognized as trust-worthy. In a cross-certified mesh, there are a various number of CA that may authorize any other CA, “except if and as naming constraints are applied" [Lin00]. The trustworthiness of this type of network is not uniform, and it varies greatly on the length of the certification chain. The trust lists are a trust design in which the peer is given an initial set of public keys of trusted CA and in order to be validated successfully it must use one of the CA from that set. The final element needs to take into consideration whether or not there are prior trusted peers, inactive peers or if the issue of maliciousness is taken into consideration.

Generically, trust management models are overviews of networks in terms of the confidence-risks ratio. The most common models for trust management are: public-key systems, resurrecting duckling and distributed trust management. The first model implies the existence of a certificate authority based upon peers can authenticate between themselves. The second model is based on the idea of master-slave, where the master send commands and the slaves have to obey. The third model is based on the idea that trust has to be earned and, moreover, it has to be earned for each peer because it is transitive only if it meets several condition.

Trust management in the context of mobile ad hoc networks has more challenges given the opportunistic communication and the ad hoc nature of the network. Ad hoc networks rely on the active cooperation between all peers for routing and packet forwarding. Communication distance, bandwidth or threshold are various parameters that can influence a peer to act selfishly in the sense that it will only listen to the data from its proximity without forwarding it.

The proposed security approach implements a hybrid form of trust model between the public key systems and the distributed trust management. In the beginning, the infrastructure gives each node the benefit of a doubt, so they are all considered to be “kind and selflessly“. Using the information gathered by the monitoring devices, a list of misbehavior is made. Once a node exceeds a given threshold, like Friedrich Nietzsche said, it will not be trusted again.

The Cooperative MAC protocol is a multi-rate compatible 802.11 standard protocol based on the idea that users in a VANET have different transfer speeds between sender and receiver. Given low speed communication between a sender and a receiver, if there is a third user between the two that has higher transmission speeds then that user will act as forwarder in order to speed up the overall transmission and decrease the general throughput.

The general usage means that every station needs to find out how close it is to its pair along with the channel and speed at which it is going to communicate. Therefore, Request to Send (RTS) and Clear to Send (CTS) frames need to be introduces in the system for collision avoidance and channel reservation(NAV).

Say there is a peer that wants to send data(Sender), a peer to whom is designated the data(Receiver) and two peers that happen to be in the area(Helper1 and Helper2) like in figure 4.1. The transmission of the data follows the pattern below:

- the Sender sends a RTS packet;
- each peer in the area receives the RTS packet and verifies if the Sender address exists in the proximity table. If it is not, it will be added. Then, each peer computes the data rate at which it could transfer data and stores it along with the MAC address in the proximity table;
- if a peer receives the RTS packet without errors it becomes a posible helper. Each helpers asses if their data rates can improve the transfer. If it can, it will send a helper-ready-to-send (HTS) packet. The helper with the best proximity is chosen as intermediary. Note: HTC is identical to a CTS type of message;
- the Receiver sends a CTS in order to reserve the channel. If there is a helper, it reserves the channel for the time necessary for a transfer with the helper, otherwise it reserves the channel for the time necessary for direct communication;
- the Sender starts sending the data. If received without errors, the Receiver transmits ACK packet. This step repeats until the end of transmission.

The Cooperative Mac Protocol (CoopMAC) presents advantages like higher spatial diversity since any damage in communications between two nodes can be taken over by a third one with better signal power and higher data rates with both nodes.

The protocol has shortcomings like the fact that the helper might not want to be so helpful

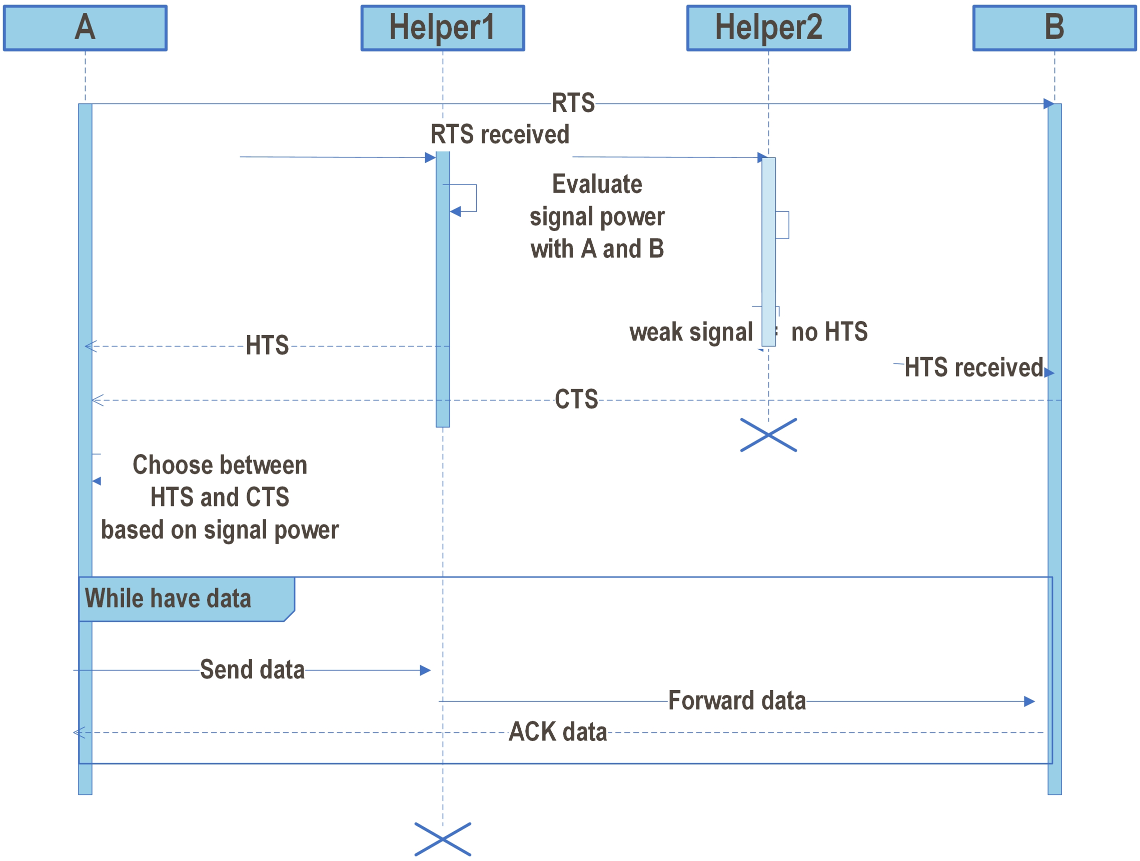

Figure 4.1. The Cooperative MAC protocol for transferring data.

and refuse to forward frames, simply dropping them when they come. In this case, the sender has to notice the lack of helpfulness and find another intermediary or, if there are no, to send the frames itself despite the low data rate.

Another potential issue that might come from the helper if it turns malicious is the attempt to deny service to the source by dropping packets received from the sender but spoofing ACKs on behalf of the destination. But that is not the worst that could happen; the helper turned malicious could end up modifying the payload of the messages and the forward them. This is very hard to detect from the sender's point of view because it does not know anything is wrong with the intermediary in order to change it or to send the frames itself.

4.2 Encryption based security model aspects in VANET

This chapter presents the validation of the security mechanism proposed by simulation using Sim2Car. The algorithms used for testing are AES, AES Light and AES Fast. The “classic” version is an implementation of the AES (Rijndael) algorithm from FIPS-197 that uses one static table of 256 word table for each encryption and decryption for a total of 2KBytes. It thus adds 12 rotate operations per round the values contained in the other tables from the contents of the first.

The “fast” version is an implementation of the AES (Rijndael) algorithm from FIPS-197 optimized by Dr. Brian Gladman in terms of time consumption by using 8KBytes of static tables for round precompilation.

The “light” version is an implementation of the AES (Rijndael) algorithm from FIPS-197 optimized by Dr. Brian Gladman in terms of memory usage by using no static tables for round precomputation, which has as result the smallest foot print.

Given the fact that the minimum packet size is 9 bytes, the maximum packet is 614 bytes and the average packet size is 177 bytes and the fact that for relative small input size the “fast” version has the best performances, it is recommended to use the “fast” implementation of the AES algorithm. That decision was cemented by the incresed number pf messages exchanged in the network.

The advantage brought in throughput for the CoopMAC protocol a mathematical demonstration does the deal in paper [LTP05]. The fundamental assumption for which the demonstration is made is that all stations are uniformly distributed in the coverage area.

The maximum assumed transmission rages $r_{11}, r_{5.5}, r_2$ and Sr_1 are defined for 11 Mbps, 5.5 Mbps, 2Mbps and 1 Mbps transition rates.

The transition time of a a data packet for a fixed data transition rate of x Mbps is presented in the flowing Equations:

$$T_{11} = T_{count}(n) + T_{overhead} + \frac{8L}{R_{11}} \text{ (1)}$$
$$T_{5.5} = T_{count}(n) + T_{overhead} + \frac{8L}{R_{5.5}} \text{ (2)}$$

where $T_{overhead}$ is defined as

$$T_{overhead} = T_{PLCP} + T_{DIFS} + T_{RTS} + T_{CTS} + 3T_{SIFS} + T_{TACK}$$

and $T_{count}(n)$ is defined as the amount of time necessary for a successfully connection

Moreover, for 2Mbps transition rates the transmitting time if the helper is not available is defined in the flowing Equations:

$T_2 = T_{count}(n) + (P_{11,11} + P_{5.5,11} + P_{5.5,5.5})T_{CoopOH} + \frac{16P_{11,11}L}{R_{11}} + \frac{8P_{5,11}L}{R_{11}} + \frac{8P_{5,11}L}{R_{5.5}} + \frac{16P_{5.5,5.5}L}{R_{5.5}} + (1 - P_{11,11} - P_{5.5,11} - P_{5.5,5.5})(T_{overhead} + \frac{8L}{R_2})$ (4)
where $R_x = xMbps$ and $T_{CoopOH} = 2T_{PLCP} + T_{DIFS} + 5T_{SIFS} + T_{RTS} + 2T_{CTS} + T_{ACK}$. (5)

Based on the Equations presented above it can be written in similar mode the equations for average transmission time T_1.

The CSMA/CA protocol guarantees the fact that each station in the network have the same number of packet for a long period of time. Therefore the average transmission time per packet is calculated as:

$$T = f_{11}T_{11} + f_{5.5}T_{5.5} + f_2T_2 + f_1T_1 \text{ (6)}$$

where

$$f_{11} = \frac{r_{11}^2}{r_1^2} \text{ (7)}$$
$$f_{5.5} = \frac{(r_{5.5}^2 - r_{11}^2)}{r_1^2} \text{ (8)}$$
$$f_2 = \frac{(r_2^2 - r_{5.5}^2)}{r_1^2} \text{ (9)}$$
$$f_1 = \frac{(r_1^2 - r_2^2)}{r_1^2} \text{ (10)}$$

Taking into account equation (6) and the fact that the maximum range is about $r_{11} \simeq 36m < r_{5.5} \simeq 45m < r_2 \simeq 48m < r_1 \simeq 51m$ we can say that the CoopMac average time is better than T_1 and T_2 but worse than T_{11} and near to T_{55}. Given the fact that the CoopMAC is used for bad communication speed transfers, thus interfering in the T_1, T_2 and more rarely to T_5 we can state that the method improves both timing and throughput.

4.3 Experimental results regarding architectural choices and criptographic performances in VANET

In order to demonstrate the validity of the proposed security mechanism, several simulation have been made using 802.11 p technology with two different map scenarios: San Francisco($121km^2$) and Beijing($16.807.8km^2$).

The test have taken into account a number of 500 vehicles and 10 infrastructure point on the map. A number of 50 vehicles has been randomly chosen and their results plotted in the simulation.

The decreased number in the tiles exchanged both between the vehicles and between vehicles and the infrastructure is motivated by the increased overhead that the security mechanism has introduced to the network. An average length of the message without the security mechanism was computed as being around 100 bytes, whereas with the security mechanism has increased the number of bytes of the message to 177 bytes.

A survey of the way the previously attacks are addressed by the security mechanism presented in this chapter, we summarise as follows:

- alteration attacks occur when the messages exchanged are different from the receiver to the destination, thus creating a false image of the traffic. This type of attack has been resolved by introducing a hash of the message along with the message which is verified at the destination. If the computed hash of the message is different from the sent hash, then the message is dropped. This solution has considered that communication error are of at most 2 bits and can be resolved automatically by the wireless transceiver;
- replay attacks are the ones that collect data over a time slot only to reuse that data at later times in order obtain certain privileges. This attack has been resolved by the introduction of pair of GPS position into the encrypted data filed and the message packet ID, therefor, if a helper wants to resend information the GPS encrypted data will show that the location is different from the receiver's location and that the difference between the timestamp of the message and the current time is more that one minute. Thus the messages will be dropped;
- sybil attacks are part of the impersonating attacks and happen when an attacker uses a different set of identification at the same time. This attack was limited by imposing that all messages should be signed and the message data has information about the GPS location of the emitter. In order to apply this attack, one should get the certificates of more than one vehicle from the network which means attacking the infrastructure. This type of attack has not been treated because of the unlimited resource capability of the infrastructure;
- ID disclosure attack adds prejudice to users privacy, revealing their secret data. This type of attack is possible only if the attacker is in the proximity of the victim at all times and it corresponds with it at the discovery stage;
- eavesdropping occurs when an attacker listens to the communications from the network in order to get confidential information. This attack is useless in the network in the message exchange phase because of the shared key algorithm imposed which determine the use of a different key at all times.

Attacks like the ones stated below have been taken into consideration and the solution found was to introduce monitoring devices in the network which should detect the misbehavior and signal to the infrastructure. This, in turn, will add the vehicle to a revocation list or a blacklist and announce it to all the vehicle in the network in order to prevent further malicious acts. The disadvantage of the proposed solution is that the elimination of malicious vehicles is made in time and therefor their actions can affect the network for a longer time.

- denial of service or distributed denial of service are attacks meant to make the network unavailable and thus users uninformed about the traffic status. This attack is very hard to mitigate because it does not affect the security of the system, but the availability of it. It does not rely on the system's cryptography weaknesses but on the wireless communication environment;
- fabrication attacks happen when a user creates false information in order to obtain certain privileges. These bogus information inserted into the system are mitigated at the infrastructure level when correlating the information from various sources. The vehicles that uses this approach will be found by the signature of the message. Messages that have been stored from other users lose their viability if the sender to the infrastructure is not the same as the message generator vehicle.

The proposed solution for attacks like DoS or Fabrication is to introduce monitoring devices in the network which should detect the misbehavior and signal to the infrastructure. This, in turn, will add the vehicle to a revocation list or a blacklist and announce it to all the vehicle in the network in order to prevent further malicious acts. The disadvantage of the proposed solution is that the elimination of malicious vehicles is made in time and therefor their actions can affect the network for a longer time.

4.4 Conclusions

The security mechanism described in the thesis is based on wireless communicating devices in which vehicles act like clients that send information about their GPS location or from their sensors and clients that need to receive information from a higher instance about the bigger picture of the network, that bigger picture being the infrastructure.

In this chapter we proposed a security model for VANET based on .X509 certificates for user to authenticate in the network, a CoopMac algorithm to increase communication through third parties, Diffie-Hellman exchange in order for each pair of two user to share a secret key for encrypting the messages exchanged.

The main disadvantage to the network is the fact that it cannot grant anonymity, and that the infrastructure can restore any paths of the participating vehicles. Also, the real-time constraints of the security mechanism was barely met because the number of packets transferred in the network dropped drastically. This issue could not be resolved, but a walk around it was found by adding a cooperation model to the network which increases the distance and, therefor, also the time slot. If an attack takes place on the server side, and the infrastructure cannot resist, it will reveal data about the participants, along with the identity of those who have monitoring devices.

5 | A participatory sensing security approach for elder reintegration in wireless mobile networks

When talking about elder reintegration as a particular case study for trust in participatory sensing several aspects must be cleared: why participatory sensing, why is trust important in these applications and further more, why elder reintegration.

Participatory sensing applications represent a community in which user choose to gather and share data from their sensors for aggregation. Unlike opportunistic networks, the users are aware of the active application and sharing sensors data is done, not when the conditions fit, but when the users allow it. The opportunistic approach has the disadvantage of uncontrollable sharing data while the participatory sensing application has the disadvantage of many user interrupts. In order to better address the everyday user's needs a mixture of these two model of application has been proposed: users decide when and where they share data without the application having to constantly check for user agreement.

Trust management is a key technique to protect ICT solutions from internal attacks, and is a valuable solutions for the mentioned problem. It consists in determining a trustworthiness degree of an opinion provider,and assessing the trustfulness of the provided opinions. Our work provides a new approach for trust management by monitoring not only what a user says, but also its knowledge in saying that.

The chapter is structured in the following sections: in section 5.1 we describe in details the trust management with its problems and proposed solutions. Further on, in section 5.2 presents the proposed approach for trust management in a participatory system. Experimental results regarding the proposed approach are presented in section 5.3. The final section 5.4 presents the main conclusions of the proposed approach.

5.1 A trust and reputation based security approach in participatory sensing

The proposed approach tries to solve trust management issues in participatory sensing applications based on human experience: elder reintegration. The current approach takes into account the elders's recommendations for tourists regarding fastest paths, shortest path or the one with most touristic objectives.

The main components of the architecture are the users of the system, the initial generated information formed by a set of predefined touristic objectives and maps and the user knowledge about those objectives. The system is based on request from some users and responses from others. These represent actual recommendations based on the comparison between the users profiles and between the prior two categories: known information and the certain one.

The proposed architecture takes into account two types of users: the givers and the receivers. The givers are the elders which choose to share their knowledge about city status: fastest paths, shortest paths and moreover, the most relevant sightseeing in an area of interest. The receivers are the visitors that need assistance when it comes to choosing what is worth seeing in a foreign city. A user can be either a receiver or a giver, but not both.

Elder Reintegration has a peer-to-peer architecture where users communicate via request and responses. The peer activity is made through dedicated mobile application TERI - Trust Elder ReIntegration. The system is based on the premises that the receiver has a smartphone with enabled GPS which is active during sightseeing. Each giver's GPS monitors computes how much does the user follow a suggested path and, at the end of the path or when the application is closed, it sends back to the giver the resulted percentage. The givers complete challenges and make recommendations via smartphone or tablet.

Each recommendation given by an elder to a tourist can be time, distance or sightseeing oriented. Based on this orientation, the profile of the giver and the profile of the receiver the recommendation is asserted a score. The higher the score, the higher the compatibility between the giver and the receiver in accordance to the orientation of the request.

The exchange of information is divided in 4 phases: initializing, learning, recommendation and adjustment phase. Each phase is important for the correction of the data and the trust computation of the user. The stages represent the actual flow of information that a user brings to the application: first a user must declare what it knows and what its interests are. Then, the system finds out how much does the user really know about its interests. After creating a profile of the residents of a city, they can begin to suggest paths to visitors. The final phase is that of correcting the recommendation. Each of these phases is further described in details.

Each user of the system has a trust with values between 0 and 1 where 0 means untruthful and 1 means total trust. Each feedback represents a score that the receiver shares about the quality of the recommendation of the giver and is between 0 and 10 where 0 represents bad recommendation and 10 represents a good, liked one. When entering the system, each user receives a value representing its initial trust which is further explained in the next chapter. Also, each giver stores a list of the receivers with which it has been in contact along with their percentage of availability to follow the suggested path whereas each receiver stores the list of all the givers with which it has been in contact along with their resulted trust. This way, each user can compute the trust of the others but not its own. Also, by not knowing if the other user gave a good or bad score, one can not alter the associated trust value without influencing its own trust.

The main advantage of the proposed approach is the ability to make suggestions for tourists not only in terms of fastest or shortest path but also for sightseeing along with a new trust management approach. The mobile application brings high mobility at the user side.

5.2 Trust and reputation management for elder reintegration in participatory sensing

The proposed trust model is broken into several perspective: it monitors how much does the user trust what it knows, how much does the system trust what the user says it knows and how much do the other users trust what he said he knew. These perspective correspond to different phases of the system and are presented next.

In the initialization phase, each user has to complete a user profile stating where he lives, what cities does he know and at what degree, the time spent in each city and preferably the neighborhoods which are most familiar. These information create an initial level of trust of the user in terms of credibility. This information helps create the initial trust of the givers and the main interest of the receivers for later suggestions.

In the learning phase, each giver has to fill out a set of challenges where at first they state their interests and afterwards are tested regarding their knowledge in those areas. Categories of interests may be museums, theaters, hospitals, restaurants, florists *etc.* The second degree of trust has to be influential enough to reflect the user knowledge but without eliminating the importance of feedback. The challenges represent a virtual map of the city where they have to set as many touristic objectives in their area of interest as possible and afterward to respond to a set of choosing the best path to a place. The number of recognized objectives of the total number known by the system in that area of interest determines an second degree of trust of the giver. The deviation of the path suggested by the giver to the path suggested by a GPS application can determine the degree of knowledge in terms of fast traveling. This also represents a part of the second degree of trust of the giver. The receiver must also complete a set of challenged regarding their interests and the complete a set of challenges regarding those interests. This phase contributes to the computation of the score of a recommendation. The resulted trust after phase one and two represents initial trust (TI) represented by Equation 5.1. The percentages of each element in the Equation of trust computing have been determined stochastically.

$$TI = \beta \times TInitialize + (1 - \beta) \times TLearning, where \quad \beta = 0.1 \tag{5.1}$$

After the learning phase starts the actual communication phase. At this point, the system accepts request from receivers and responses from elders. The system also accepts an emergency profile where it gives a user basic information about hospitals or public transport stations.

The recommendation and feedback phases work hand in hand, in the sense that for each recommendation a feedback is to be made. But, the given feedback must also take into consideration the profile of the receiver. Based on the degree of similarity the feedback can have a bigger or smaller importance on the final result. If a total compliance of the suggested path means 100% valid opinion from the receiver (feedback vale), then 50% compliance of it should have only half the importance of the feedback. Considering the fact that trust has a value between 0 and 1 while feedback (F) has a value between 0 and 10, a division by 10 must be made in order to remain in stated interval of trust. More explicitly, considering feedback (F) a value between 0 and 10 representing the receiver satisfaction toward a suggested path and an obedience percentage (OP), a value between 0 and 1, representing the degree with which the receiver has followed the suggested path, the Equation for trust communication between two users is stated in Equation 5.2.

$$TrustFeedbackperRequest/Response = 0.1 \times OP \times F \tag{5.2}$$

The trust computation of the users has to reflect as best possible their knowledge so it has to be best divided between the system phases. For example, if the initial phase has a percentage higher that the learning phase, users that have lived for longer period of time in a place with lower knowledge would have greater score that a user with actual knowledge but has not lived there for as long. Also, a balance between the trust the system gives the user and the trust computed via the feedback received must be made. For example, if the feedback percentage is small, a giver with high level of trust can then send bad recommendations because it does not affect the general result. On the other hand, a user with good system trust that meets bad receivers could be destroyed if the percentage of feedback is too high. Therefore, the initial and learning phases must counter balance the feedback phase. Generically, a user's trust is composed of 55% initial trust (TI), which is gathered in the first and second phases, and 45% the trust from the other N number of users feedback (TF). The computation of the trust of other users feedback can be seen in Equation 5.3.

$$TF = \frac{\sum_{I=1}^{n} 0.1 \times OP_{IR} \times F_{RI}}{|G|} \tag{5.3}$$

where |G| is the cardinal of the list of givers that have previously had contact with. This Equation can be rewritten as follows:

$$TF = 0.1 \times \frac{\sum_{I=1}^{|G|} OP_{IR} \times F_{RI}}{|G|} \tag{5.4}$$

The proposed approach for trust computation of a user therefore depends on what he think he knows (5.5 %), on what the system knows he knows (49,5%) and on the trust given by the other users (45%), summing it up in Equation 5.5:

$$TotalTrust = \alpha \times TI + (1 - \alpha) \times TF, where \quad \alpha = 0.55 \tag{5.5}$$

The percentages of the trust levels after each phase in the Equation 5.5 have been stochastically chosen based on the assumption that malicious majority must not influence decisively the total trust of a good user.

5.3 Experimental results

For the purpose of testing the computational approach for trust in participatory sensing a sample of 12 users was taken into consideration and mathematically modeled. Of these users, 7 have been considered givers and 5 have been considered receivers. For each of these users an initial trust value has been appointed and several random generated routes have been put in place in order to compute the user feedback trust.

The second phase named learning phase represents a set of challenges that the user has to complete. The second phase has also been mathematically modeled and user profiles have been randomly generated.

For the third and fourth phase, recommendations and feedback, random requests and responses have been made. These request and responses have been made in 3 iterative steps in order to determine how accurate does one user influence another.

Closing the application by the receiver without sharing the path taken with the giver is reflected by a 0 in the obedience percentage. This strong negative value is used in order to discourage the users from getting information from the system without feedback. A value of -1 means that the user has not had any requests/responses and therefore the feedback is null. Similar pairs of requests and responses are generated for second and third iteration.

An evolution of the total user trust after each stage is presented in diagram 5.1. The system phases presented are: initialization in the system, learning in the system, first iteration of interactions, second iteration of interactions and third iteration of interactions. In this diagram it can be observed that the first phase introduces a weak starting point but it can not be eliminated because it is necessary for setting the challenges of phase two. As it can be seen in the diagram, phase two has a catalysis role for balancing the general user trust without letting it be strongly influenced by good or bad reviews. The next three phases represent iterations at with user interact and evaluate each other. The fact that the other user does not know the evaluation of the other helps maintaining a balance of trustfulnesses. This is done by the fact that a receiver does not

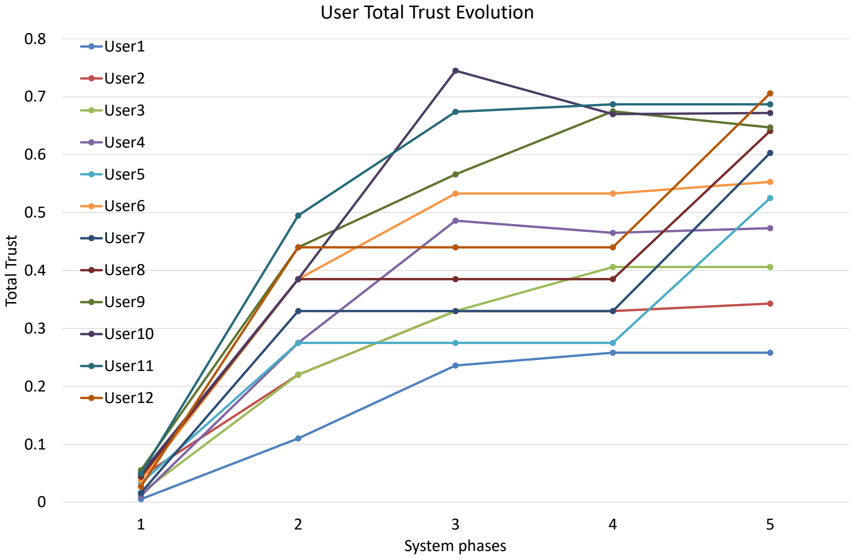

Figure 5.1. User trust evolution after each phase of the trust and reputation security model.

know how much its grade influences the total trust of the iteration as neither does the giver.

5.4 Conclusions

In this chapter we have presented a new type of application for path optimization using cloud based services in participatory sensing systems based on elder reintegration. The motivation behind this theme is that the pervasiveness of the ICT and the availability of reliable and powerful Internet access everywhere allows people to always be reachable by everyone, despite the respective physical distance among two individuals. An evolution of the total user trust after each stage is presented in diagram 5.1 where it can be observed that the first phase introduces a weak starting point but it can not be eliminated because it is necessary for setting the challenges of phase two.The second phase is important for making a balanced general user trust. The third and fourth phases represent iterations at with user interact and evaluate each other giving mutual trust feedback.

The proposed trust management model was statistically evaluated. The main diagram shows a balanced network where strong feedback is attenuated by user history.

The chapter has been structured as following: in section 5.1 we described in details the trust management with its problems and proposed solutions. Further on, in section 5.2 was presented the proposed approach for trust management in a participatory system. Experimental results regarding the proposed approach were then discussed in section 5.3. The final section 5.4 presents the main conclusions of the proposed approach.

6 | Security in WSN

Authors in [ARH19] claim that one of the main problem when dealing with wireless sensor networks is the high computational cost of the nodes. This, along with their limited resources leads to an increased level of vulnerability to attacks and even, environmental impact. Trust and reputation models can therefore be a viable alternative.

This chapter introduces a novel method for trust management based on Markov chains for wireless sensor networks (Section 6.1) and an adaptive method trust management with respect to QoS concerns (Section 6.2). Finally, we present the obtained results through simulation. (Section 6.3).

6.1 A Markov-based trust and reputation security approach in wireless sensor networks

The proposed trust model helps emulate the behaviour of the communication between two users or, moreover, their ability to communicate or be defective. That fault is that any given node can be offline for an undefined period of time. Each node fails according to a sum of exponentially distributed function with parameter α and recovers according to a sum of exponentially distributed function with parameter β. In the system, each node can have one of three states: online and available for communication, offline and non-existing and volatile in which the node has recovered from an offline state but it is still not available for communication. The volatile state can be assimilated to the error diagnosis state after a sudden shut down of a node.

The proposed model represents an optimist approach and therefore grants each node full trust when entering the system. The trust and reputation value of any node in the system, at starting point, is 1.

The trust and reputation value of a node in the system for this proposed model is computed based solely on first hand information. Further work on the proposed model will include analysing if second hand information adds robustness to the system, as references [BB03] and [MGLB00] suggest.

For this model of trust and reputation, we suggest using a hybrid approach of both event-trigger and time-based for updating the trustworthiness of a node. The event-trigger update refers to the oscillating state of the node between online and offline and between the states offline and volatile. The time-based aspect of the proposed model refers to the fact that, if a node is in the volatile state for a period of time larger than a set threshold τ, then it will be automatically placed in the online state again. Along with resetting the state of the node from volatile to online, the trust and reputation value of the node will be restored to 1, therefore allowing a node to redeem from a bad behaviour. That bad behaviour in this proposed model is represented by a bad connection, either from subjective causes like battery drainage or objective one like weather events.

The time during which the node is offline is considered down time. We consider that the down time of a node is according to a sum of exponentially distributed function with parameter β.

Parameter β, as well as α, can have either a fixed value for the lifespan of the node or a variable one, thus generating two different scenarios (Figure 6.1). These two scenarios can be assimilated in real life to the power supply a node may have. For example, the fixed parameter can be used to map, for example, a node which is constantly power plug and, thus, has little-to-no variations during it's lifespan, while a battery based node may vary according to the battery usage curve.

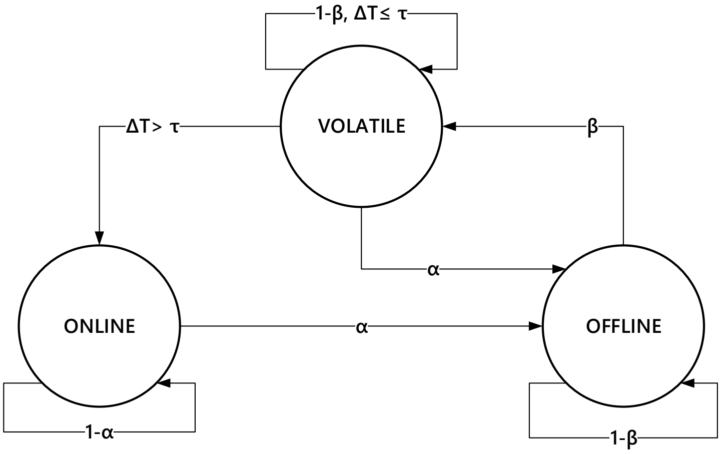

Figure 6.1. Multi-state security approach. Each node fails with a probability based on α parameter and recovers to an online state with a probability based on β parameter.

For research purposes, we consider that only one node recovers at a time as well as the fact that the nodes' variations between the state of online, offline and volatile are independently and that the state of one node does not influence that of those surround it. Therefore, for each node i from the N number of nodes existing in the network there is a different α and β generically referred to as α_i and β_i. The premises previously stated represent an adaptation of a model presented in [Gla14].

Given the previous premises, one of the main objectives of this chapter is to discover what is the probability that a given number of nodes i, smaller than N, are online at any given time t in the WMN. To this respect, firstly we modeled the proposed WMN as a Markovian system. We introduce

$$\gamma_i = \frac{\alpha_i}{\beta_i} \tag{6.1}$$

where α_i and β_i are the coefficients for the exponentially distributed functions which represent the states when a node is offline, respectively online.

Given the equation 6.1 and knowing the total number of nodes N in the network, we can state the probability that a given number i of nodes, smaller than N, are online at any given time t, from balance equations of continuous time Markov chain as follows in equation 6.2.

$$P_i = \frac{\gamma_i}{i! \sum_{j=1}^{N} \frac{\gamma_j}{j!}} \tag{6.2}$$

Another goal of this thesis is to estimate what is the average down time rate (i.e. the average number of nodes that breaks down per time unit) as well as the average failure rate for our given WMN.

Considering P_N the probability that all the nodes in the network are online, then we can state that the average down time rate ($P_{down.rate}$) can be computed as the improbability of P_N happening. Knowing the value P_N, then the probability of the whole network to be down can be expressed in equation 6.3.

$$P_{down.rate} = 1 - P_N \tag{6.3}$$

In order to estimate the average failure rate ($\lambda_{fail.rate} \epsilon [0; 1]$) of a network with N number of nodes, we have to take into consideration both the down time of each node in the system as well as the probability of having i nodes online in the WMN. To this respect, we use the conditional expectation calculation to compute equation 6.4.

$$\lambda_{fail.rate} = \sum_{i=1}^{N} i \times \alpha_i \times P_i \tag{6.4}$$

If we know the percentage of time when nodes are unavailable, then we can compute the average number of online nodes in the WMN as stated in equation 6.5.

$$N_{avg} = \sum_{i=1}^{N} i \times P_i \tag{6.5}$$

Trying to find the equation for the average down time rate, a new challenge has arisen. If we can determine what the average number of online nodes is in a network, could we address the problem in reverse and find out what would be the minimum number of nodes that a WMN would have to have in order to ensure that at any given time there are at least N nodes online? The mathematical equation which can estimate the lowest number M of nodes which can guarantee at least N online nodes can be stated as follows $N_{avg}(M) \geq N$. The extended computation of that inequality can be observed in equation 6.6 .

$$\sum_{i=1}^{M} \frac{i \times \gamma_i}{i! \sum_{j=1}^{M} \frac{\gamma_j}{j!}} \geq N. \tag{6.6}$$

We choose the variable w to express the probability that an offline node can not go online immediately, thus remaining in the volatile state. It's value can be computed as the ratio of the rate of node break-downs that can not go online immediately, over the total average rate of node break-downs as shown in equation 6.7.

$$w = \frac{\sum_{j=1}^{N-1} \alpha_j \times P_j}{\sum_{j=1}^{N} \alpha_j \times P_j}. \tag{6.7}$$

We can define the trust of a node i in a WMN with M nodes, an average number of N_{avg} online nodes with a probability w that after a break down they cannot become immediately online, after k number of transitions as follow in equation 6.8.

$$T_i^k = \frac{1}{k} \times \left((1 - w) \times T_i^{k-1} + w \times \frac{N_{avg}}{M} \right) \tag{6.8}$$

6.2 Experimental results

For a wireless sensor network with 10 which can switch their state between online and offline independently, we consider each of the node's initial trust to be 1 ($T_0 = 1$). That is to say that all the nodes start from the presumption of being fully reliable, with capabilities to be a part of the network (online). Each transition to offline and online again affect the reliability of the node and therefore it's trust.

The equations proposed in section 6.1 have been tested and validates mathematically and in simulation using TRMSim-WSN.

During the validation we have observed that a low rate a failure, stated by a low value of parameter *alpha*, along with a high recovery rate, translated in a high value of parameter *beta*, increase the probability of i number of nodes to be online in the network. These simulation results can be observed in Figure 6.3.

In Figure 6.2 we show the dependency of the probability of having a certain number of nodes online in the network according to the existing number of failed nodes. As seen, the value of the probability P is decreasing significantly with the number of offline nodes.

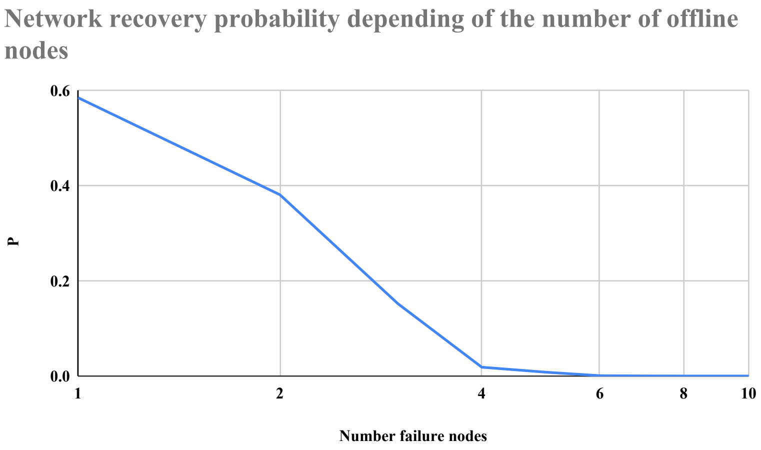

Figure 6.2. Values of the probability P of having a certain number of online nodes in the network with respect to the number of failed nodes.

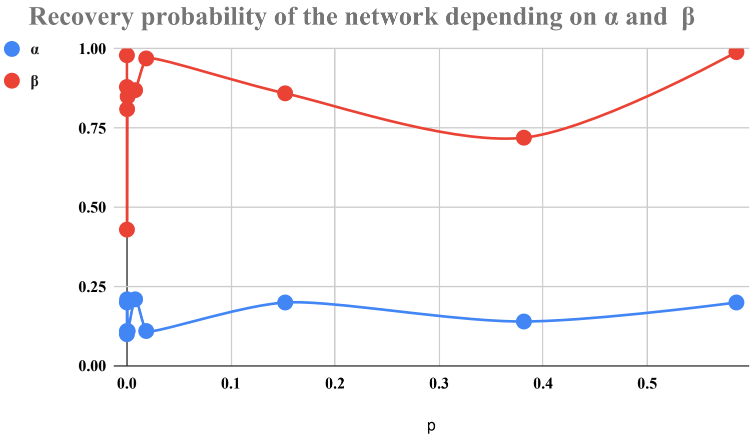

Figure 6.3. Values of the probability P of having a certain number of online nodes in the network with respect to the α and β parameters.

Furthermore, we evaluate the proposed trust method using a randomly generated sample values for parameters α and β. In Figure 6.4 we show the obtained results where it can be seen that the trust value for each nodes decreases in the same manner as the value of the probability P of having a certain number of nodes online in the network.

If after a certain number of transitions during the volatile state, a node will remain stable, the trust and reputation model allows the possibility of redemption by reinstating its trust value to the initial one, $T_0 = 1$. Further work will determine how long does the time τ has to be in order to properly represent that a node has become stable and available.

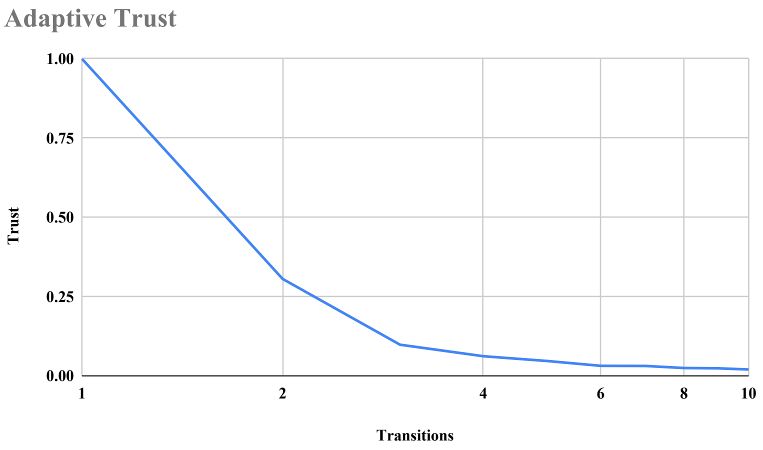

Figure 6.4. Evolution of trust with respect to the number of failed nodes in the network.

6.3 Conclusions

Taking into consideration the heterogeneous devices in a network along with the different operating systems and all-changing topology, it becomes difficult and consuming in terms of resources (time, money *etc.*) to implement classical security models with respect to QoS.

In this chapter, we have proven that a trust and reputation based new paradigm of security may be able so solve these issues in an efficient way. The Markov based approach for trust and reputation in WMN proposed in this thesis manages to compute trust values of the nodes that are dynamic,asymmetric, context sensitive, subjective and partial transitive. Each node in the system can have one of three states: online and available for communication, offline and non-existing and volatile in which the node has recovered from an offline state but it is still not available for communication. The volatile state can be assimilated to the error diagnosis state after a sudden shut down of a node. The trust and reputation model proposed represents an optimist approach and therefore grants each node full trust when entering the system. The trust and reputation value of any node in the system, at starting point, is 1.Each update of the trust and reputation value is computed based solely on first hand information using a hybrid approach of both event-trigger and time-based for updating the trustworthiness of a node. The obtained results of the proposed trust and reputation model present great potential regarding further simulations and determining the accuracy of the proposed algorithm.

Our statements are as follow: the trust model is defined in section 6.1 and tested with results presented in 6.2 . The trust model proposed considers that the adaptive factor, w, is changing over time and that fact in reflected in the trust computation of a node.

7 | Conclusions and future directions

7.1 Conclusions

During the research for this thesis, we have tried to find a way to implement a security model in wireless mobile networks, presenting multiple solutions with their advantages and disadvantages.

7.2 Main contributions

O1 We implemented and tested various cryptographic algorithms independently and in the UPB's Sim2Car Simulator in order to make a performance evaluation;

O2 We proposed, implemented and tested in a simulator environment an encryption-based security model for VANET;

O3 We proposed, implemented and tested stochastically a trust and reputation model for participatory sensing networks. This model addresses user trust;

O4 We proposed, implemented and tested stochastically and in a simulator environment a trust and reputation model for wireless sensor networks. This model addresses communication trust.

7.3 List of publications

The main results of this thesis were presented to various conferences, journals and books. We have 7 publications, 4 as first author and 3 as co-author. My publications list consists in 1 book chapter (Advances in Mobile Cloud Computing and Big Data in the 5G Era), 1 articles in international journals(Information Sciences) and 5 papers in well-established international conferences (International Conference on Green, Pervasive, and Cloud Computing; P2P, Parallel, Grid, Cloud and Internet Computing; International Conference on Testing Software and systems).

The authors would like to thank the reviewers for their time and expertise, constructive comments and valuable insight

Previous published papers:

1. **Mocanu (Mihăiță), Alexandra-Elena**; Dobre, Ciprian; Pop, Florin; Mavromoustakis, Constandinos X; Mastorakis, George; "Secure Opportunistic Vehicle-to-Vehicle Communication","Advances in Mobile Cloud Computing and Big Data in the 5G Era",229-268,2017,Springer

2. **Mocanu (Mihăiță), Alexandra-Elena**; Dobre, Ciprian; Mocanu, Bogdan; Pop, Florin; Cristea, Valentin; "Analysis of security approaches for vehicular ad-hoc networks","P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2015 10th International Conference on",304-309,2015,IEEE

3. Mocanu, Bogdan; Pop, Florin; **Mocanu (Mihăiță), Alexandra-Elena**; Dobre, Ciprian; Cristea, Valentin; "Spider: A bio-inspired structured peer-to-peer overlay for data dissemination","P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2015 10th International Conference on",291-295,2015,IEEE

4. Mocanu, Bogdan; Pop, Florin; **Mocanu (Mihăiță), Alexandra-Elena**; Dobre, Ciprian; Castiglione, Aniello; "Data fusion technique in spider peer-to-peer networks in smart cities for security enhancements", "Information Sciences",479,607-621,2019,Elsevier

5. Mocanu, Bogdan; Pop, Florin; **Mocanu (Mihăiță), Alexandra-Elena**; Dobre, Ciprian; Cristea, Valentin; Castiglione, Aniello; "Flaw Recovery in Cloud Based Bio-inspired Peer-to-Peer Systems for Smart Cities","International Conference on Green, Pervasive, and Cloud Computing",338-352,2017,Springer

6. **Mocanu (Mihăiță), Alexandra-Elena**; Dobre, Ciprian; Pop, Florin; Mocanu, Bogdan; Cristea, Valentin; Esposito, Christian; "A trust application in participatory sensing: Elder reintegration","International Conference on Green, Pervasive, and Cloud Computing",596-610,2017,Springer

7. **Mocanu (Mihăiță), Alexandra-Elena**; Mocanu, Bogdan; Esposito, Christian; Pop, Florin; "Trust is in the air: a new adaptive method to evaluate mobile wireless networks","IFIP International Conference on Testing Software and Systems",135–149,2020, Springer

7.4 Projects

During the PhD period, I was member of various projects for which I am thankful, offering me the context to build real world use cases for my thesis and also the opportunity to interact with different researchers. These projects were:

1. *DataWay*: Real-time Data Processing Platform for Smart Cities: Making sense of Big Data in romanian: Platforma de procesare a datelor in timp real pentru Orase Inteligente: Dand sens Big Data., Project Code PN-II-RU-TE-2014-4-2731, Period: October 2015 - September 2017, Director: Prof.dr.ing. Florin POP

2. *MobiWay* - Mobility beyond Individualism (PN-II-PT-PCCA-2013-4-0321)

3. *Sectoral Operational Programme Human Resources Development 2007-2013 of the Ministry of European Funds through the Financial Agreement POSDRU187 1.5S155536*

Bibliography

[ANDK⁺18] Phan Minh Linh An, Thang Nguyen-Duc, Taejoon Kim, Taehong Kim, JaeSeang Lee, and HyungSeok Choi. An enhancement of sinalgo simulator for mobile network scenario. *Wireless Networks*, pages 504–505, 2018.

[ARH19] Usama Ahmed, Imran Raza, and Syed Asad Hussain. Trust evaluation in cross-cloud federation: Survey and requirement analysis. *ACM Computing Surveys (CSUR)*, 52(1):1–37, 2019.

[BB03] Sorav Bansal and Mary Baker. Observation-based cooperation enforcement in ad hoc networks. *arXiv preprint cs/0307012*, 2003.

[BE19] BI Bakare and JD Enoch. A review of simulation techniques for some wireless communication system. *International Journal of Electronics Communication and Computer Engineering*, 10(2), 2019.

[BKL⁺05] Philip Baldwin, Sanjeev Kohli, Edward A Lee, Xiaojun Liu, Yang Zhao, CT Ee, Christopher Brooks, NV Krishnan, Stephen Neuendorffer, Charlie Zhong, et al. Visualsense: Visual modeling for wireless and sensor network systems. Technical report, Citeseer, 2005.

[Bou07] Athanassios Boulis. Castalia: revealing pitfalls in designing distributed algorithms in wsn. In *Proceedings of the 5th international conference on Embedded networked sensor systems*, pages 407–408, 2007.

[CBP⁺05] Gilbert Chen, Joel Branch, Michael Pflug, Lijuan Zhu, and Boleslaw Szymanski. Sense: a wireless sensor network simulator. In *Advances in pervasive computing and networking*, pages 249–267. Springer, 2005.

[Che15] Kahina Chelli. Security issues in wireless sensor networks: Attacks and countermeasures. In *Proceedings of the World Congress on Engineering*, volume 1, 2015.

[Cle20] J. Clement. Mobile internet usage worldwide - statistics & facts, 2020.

[CLZ05] Elaine Cheong, Edward A Lee, and Yang Zhao. Viptos: a graphical development and simulation environment for tinyos-based wireless sensor networks. In *SenSys*, volume 5, pages 302–302, 2005.

[com20] Crypto++ community. Crypto++ library 5.6.0 release 2020, 2020.

[CRKH11] Delphine Christin, Andreas Reinhardt, Salil S Kanhere, and Matthias Hollick. A survey on privacy in mobile participatory sensing applications. *Journal of Systems and Software*, 84(11):1928–1946, 2011.

[DBFH09] Akshay Dua, Nirupama Bulusu, Wu-Chang Feng, and Wen Hu. Towards trustworthy participatory sensing. In *Proceedings of the 4th USENIX conference on Hot topics in security*, pages 8–8, 2009.

[EÖF⁺09] Joakim Eriksson, Fredrik Österlind, Niclas Finne, Nicolas Tsiftes, Adam Dunkels, Thiemo Voigt, Robert Sauter, and Pedro José Marrón. Cooja/mspsim: interoperability testing for wireless sensor networks. In *Proceedings of the 2nd International Conference on Simulation Tools and Techniques*, pages 1–7, 2009.

[FFBY20] Reza Fotohi, Somayyeh Firoozi Bari, and Mehdi Yusefi. Securing wireless sensor networks against denial-of-sleep attacks using rsa cryptography algorithm and interlock protocol. *International Journal of Communication Systems*, 33(4):e4234, 2020.

[FKFP07] Sándor P Fekete, Alexander Kroller, Stefan Fischer, and Dennis Pfisterer. Shawn:

The fast, highly customizable sensor network simulator. In *2007 Fourth International Conference on Networked Sensing Systems*, pages 299–299. IEEE, 2007.

[FZC+20] Weidong Fang, Wuxiong Zhang, Wei Chen, Tao Pan, Yepeng Ni, and Yinxuan Yang. Trust-based attack and defense in wireless sensor networks: A survey. *Wireless Communications and Mobile Computing*, 2020, 2020.

[GGD+07] Victor Gradinescu, Cristian Gorgorin, Raluca Diaconescu, Valentin Cristea, and Liviu Iftode. Adaptive traffic lights using car-to-car communication. In *2007 IEEE 65th vehicular technology conference-VTC2007-Spring*, pages 21–25. IEEE, 2007.

[Gla14] Ioannis Glaropoulos. Queuing theory 2014-exercises, 2014.

[GNF+20] Ning Gao, Qiang Ni, Daquan Feng, Xiaojun Jing, and Yue Cao. Physical layer authentication under intelligent spoofing in wireless sensor networks. *Signal Processing*, 166:107272, 2020.

[JYX+18] Xiaojie Jin, Yingzhen Yang, Ning Xu, Jianchao Yang, Nebojsa Jojic, Jiashi Feng, and Shuicheng Yan. Wsnet: Compact and efficient networks through weight sampling. In *International Conference on Machine Learning*, pages 2352–2361. PMLR, 2018.

[JZE+19] Mojtaba Jamshidi, Ehsan Zangeneh, Mehdi Esnaashari, Aso Mohammad Darwesh, and Mohammad Reza Meybodi. A novel model of sybil attack in cluster-based wireless sensor networks and propose a distributed algorithm to defend it. *Wireless Personal Communications*, 105(1):145–173, 2019.

[KMKW11] Raphaël Kummer, Timothée Maret, Peter Kropf, and Jean-Frédéric Wagen. Freemote: A wireless sensor networks emulation system. In *Proceedings of 7th MINEMA workshop*, 2011.

[KSH+19] T. Khan, K. Singh, L. Hoang Son, M. Abdel-Basset, H. Viet Long, S. P. Singh, and M. Manjul. A novel and comprehensive trust estimation clustering based approach for large scale wireless sensor networks. *IEEE Access*, 7:58221–58240, 2019.

[Lin00] John Linn. Trust models and management in public-key infrastructures. *RSA laboratories*, 12, 2000.

[LLWC03] Philip Levis, Nelson Lee, Matt Welsh, and David Culler. Tossim: Accurate and scalable simulation of entire tinyos applications. In *Proceedings of the 1st international conference on Embedded networked sensor systems*, pages 126–137, 2003.

[LLZ+15] Wenshuang Liang, Zhuorong Li, Hongyang Zhang, Shenling Wang, and Rongfang Bie. Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends. *International Journal of Distributed Sensor Networks*, 11(8):745303, 2015.

[LTP05] Pei Liu, Zhifeng Tao, and Shivendra Panwar. A cooperative MAC protocol for wireless local area networks. In *Communications, 2005. ICC 2005. 2005 IEEE International Conference on*, volume 5, pages 2962–2968. IEEE, 2005.

[LW82] Ki-Won Lee and Kensall D Wise. Sensim: A simulation program for solid-state pressure sensors. *IEEE Transactions on Electron Devices*, 29(1):34–41, 1982.

[MDM+15] A. Mihaita, C. Dobre, B. Mocanu, F. Pop, and V. Cristea. Analysis of security approaches for vehicular ad-hoc networks. In *2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, pages 304–309, 2015.

[MDP+17a] Alexandra Mihaita, Ciprian Dobre, Florin Pop, Bogdan Mocanu, Valentin Cristea, and Christian Esposito. A trust application in participatory sensing: Elder reintegration. In *International Conference on Green, Pervasive, and Cloud Computing*, pages 596–610. Springer, 2017.

[MDP+17b] Alexandra-Elena Mihaita, Ciprian Dobre, Florin Pop, Constandinos X Mavromoustakis, and George Mastorakis. Secure opportunistic vehicle-to-vehicle communication. In *Advances in Mobile Cloud Computing and Big Data in the 5G Era*, pages 229–268. Springer, 2017.

[MF09] A Marculescu and J Fontignie. Algosensim: an algorithm oriented sensor networks simulator. *Retrieved May*, 3:2009, 2009.

[MGH06] Stefan Mahlknecht, Johann Glaser, and Thomas Herndl. Pawis: towards a power aware system architecture for a soc/sip wireless sensor and actor node implementation. In *Fieldbus Systems and Their Applications 2005*, pages 129–134. Elsevier, 2006.

[MGLB00] Sergio Marti, Thomas J Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 255–265, 2000.

[MMH+15] Hayam Mousa, Sonia Ben Mokhtar, Omar Hasan, Osama Younes, Mohiy Hadhoud, and Lionel Brunie. Trust management and reputation systems in mobile participatory sensing applications: A survey. *Computer Networks*, 90:49–73, 2015.

[MP09] Félix Gómez Mármol and Gregorio Martínez Pérez. Trmsim-wsn, trust and reputation models simulator for wireless sensor networks. In *2009 IEEE International Conference on Communications*, pages 1–5. IEEE, 2009.

[MP10] Félix Gómez Mármol and Gregorio Martínez Pérez. Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems. *Computer Standards & Interfaces*, 32(4):185–196, 2010.

[MPME20] Alexandra Mihaita, Florin Pop, Bogdan Mocanu, and Christian Esposito. Trust is in the air: a new adaptive method to evaluate mobile wireless networks. In *INTERNATIONAL CONFERENCE ON TESTING SOFTWARE AND SYSTEMS*. Springer, 2020.

[MZ12] Bartosz Musznicki and Piotr Zwierzykowski. Survey of simulators for wireless sensor networks. *International Journal of Grid and Distributed Computing*, 5(3):23–50, 2012.

[NMBG20] Henry Nunoo-Mensah, Kwame Osei Boateng, and James Dzisi Gadze. Pstrm: Privacy-aware sociopsychological trust and reputation model for wireless sensor networks. *Peer-to-Peer Networking and Applications*, pages 1–21, 2020.

[NSK+20] Muhammad Numan, Fazli Subhan, Wazir Zada Khan, Saqib Hakak, Sajjad Haider, G Thippa Reddy, Alireza Jolfaei, and Mamoun Alazab. A systematic review on clone node detection in static wireless sensor networks. *IEEE Access*, 8:65450–65461, 2020.

[PA13] M. M. Patel and A. Aggarwal. Security attacks in wireless sensor networks: A survey. In *2013 International Conference on Intelligent Systems and Signal Processing (ISSP)*, pages 329–333, 2013.

[PBM+04] Jonathan Polley, Dionysus Blazakis, Jonathan McGee, Daniel Rusk, and John S Baras. Atemu: a fine-grained sensor network simulator. In *2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004.*, pages 145–152. IEEE, 2004.

[PCL07] Paolo Pagano, Mangesh Chitnis, and Giuseppe Lipari. Rtns: an ns-2 extension to simulate wireless real-time distributed systems for structured topologies. In *Proceedings of the 3rd international conference on Wireless internet*, pages 1–8. Citeseer, 2007.

[PLH06] Al-Sakib Khan Pathan, Hyung-Woo Lee, and Choong Seon Hong. Security in wireless sensor networks: issues and challenges. In *2006 8th International Conference Advanced Communication Technology*, volume 2, pages 6–pp. IEEE, 2006.

[PRG15] Rodolfo Miranda Pereira, Linnyer Beatrys Ruiz, and Maria Luisa Amarante Ghizoni. Mannasim: A ns-2 extension to simulate wireless sensor network. *ICN 2015*, page 107, 2015.

[PS+09] Dr G Padmavathi, Mrs Shanmugapriya, et al. A survey of attacks, security mechanisms and challenges in wireless sensor networks. *arXiv preprint arXiv:0909.0576*, 2009.

[PS20] M Premkumar and TVP Sundararajan. Dldm: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks. *Microprocessors and Microsystems*, 79:103278, 2020.

[RH05] Maxim Raya and Jean-Pierre Hubaux. The security of vehicular ad hoc networks. In *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, pages 11–21. ACM, 2005.

[RKMC16] Madhupreetha L Rajaram, Elias Kougianos, Saraju P Mohanty, and Uma Choppali. Wireless sensor network simulation frameworks: A tutorial review: Matlab/simulink bests the rest. *IEEE Consumer Electronics Magazine*, 5(2):63–69, 2016.

[SHK+06] Ahmed Sobeih, Jennifer C Hou, Lu-Chuan Kung, Ning Li, Honghai Zhang, Wei-Peng Chen, Hung-Ying Tyan, and Hyuk Lim. J-sim: a simulation and emulation environment for wireless sensor networks. *IEEE Wireless Communications*, 13(4):104–119, 2006.

[SKA04] Sameer Sundresh, Wooyoung Kim, and Gul Agha. Sens: A sensor, environment and network simulator. In *37th Annual Simulation Symposium, 2004. Proceedings.*, pages 221–228. IEEE, 2004.

[SKS20] Jaspreet Singh, Ranjit Kaur, and Damanpreet Singh. A survey and taxonomy on energy management schemes in wireless sensor networks. *Journal of Systems Architecture*, page 101782, 2020.

[SSV13] Anitha S Sastry, Shazia Sulthana, and S Vagdevi. Security threats in wireless sensor networks in each layer. *International Journal of Advanced Networking and Applications*, 4(4):1657, 2013.

[SWZ+08] Lei Shu, Chun Wu, Yan Zhang, Jiming Chen, Lei Wang, and Manfred Hauswirth. Nettopo: beyond simulator and visualizer for wireless sensor networks. *ACM SIGBED Review*, 5(3):1–8, 2008.

[Szt04] J Sztipanovits. Probabilistic wireless network simulator (prowler), 2004.

[TLP05] Ben L Titzer, Daniel K Lee, and Jens Palsberg. Avrora: Scalable sensor network simulation with precise timing. In *IPSN 2005. Fourth International Symposium on Information Processing in Sensor Networks, 2005.*, pages 477–482. IEEE, 2005.

[TRJ02] TK Tan, A Raghunathan, and Niraj Kumar Jha. Emsim: An energy simulation framework for an embedded operating system. In *2002 IEEE International Sympo-*

sium on Circuits and Systems. Proceedings (Cat. No. 02CH37353), volume 2, pages II–II. IEEE, 2002.

[VH08] András Varga and Rudolf Hornig. An overview of the omnet++ simulation environment. In *Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops*, page 60. ICST (Institute for Computer Sciences, Social-Informatics and . . . , 2008.

[WCC$^+$16] Yating Wang, Ray Chen, Jin-Hee Cho, Ananthram Swami, Yen-Cheng Lu, Chang-Tien Lu, and Jeffrey Tsai. Catrust: Context-aware trust management for service-oriented ad hoc networks. *IEEE Transactions on Services Computing*, 2016.

[WLZN07] Hejun Wu, Qiong Luo, Pei Zheng, and Lionel M Ni. Vmnet: Realistic emulation of wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 18(2):277–288, 2007.

[WSKW09] Karl Wessel, Michael Swigulski, Andreas Köpke, and Daniel Willkomm. Mixim: the physical layer an architecture overview. In *Proceedings of the 2nd International Conference on Simulation Tools and Techniques*, pages 1–8, 2009.