Leonardo Augusto Martucci

The Identity-Anonymity Paradox

On the Relationship between Identification, Anonymity and Security in Mobile Ad Hoc Networks

Karlstad University Studies
2006:36

Leonardo Augusto Martucci. *The Identity-Anonymity Paradox – On the Relationship between Identification, Anonymity and Security in Mobile Ad Hoc Networks*

Licentiate thesis

Karlstad University Studies 2006:36
ISBN 91-7063-067-4
ISSN 1403-8099

Distribution:
Karlstad University
Division for Faculty of Economy, Communication and IT
Department of Department of Computer Science
SE–651 88 KARLSTAD
SWEDEN
+46 54 700 1000

www.kau.se

Printed at: Universitetstryckeriet, Karlstad 2006

“ ‘Would you tell me, please, which
way I ought to go from here?’

‘That depends a good deal on where
you want to get to,’ said the Cat.

‘I don’t much care where—’ said Alice.

‘Then it doesn’t matter which
way you go,’ said the Cat. ”

Alice’s Adventures in Wonderland
Lewis Carrol

The Identity-Anonymity Paradox

On the Relationship between Identification, Anonymity and Security
in Mobile Ad Hoc Networks

LEONARDO AUGUSTO MARTUCCI
D*epartment of Computer Science, Karlstad University*

Abstract

In mobile ad hoc networking, every device is responsible for its own basic computer services, including packet routing, data forwarding, security and privacy. Therefore, most of the protocols employed in hardwired networks are not suitable for mobile ad hoc environments, since they were designed for static environments with defined borders and highly specialized devices, such as routers, network addressing provisionment servers, firewalls and intrusion detection systems. This work concentrates on the achievement of network security and privacy.

The main goal of this licentiate thesis is the discussion about the impact of the definition of identity and identifiers on mobile ad hoc network security and privacy aspects and the definition of the *identity-anonymity paradox*. Even though the concepts of anonymity and identifiers are often understood as opposites, we show in this thesis that reliable anonymity is not achievable in mobile ad hoc environments without trusted, unique and persistent identifiers since network security must also be guaranteed.

Furthermore, this thesis discusses the consequences of the deployment of different mobile ad hoc network security solutions to the provisioning of privacy and also to the definition of a digital identity in these environments.

Keywords: network security; mobile ad hoc networks; identity; privacy; and anonymous communication mechanisms.

Acknowledgments

My licentiate thesis is now complete. It sounds odd to me to call this work as mine, since so many contributed to its achievement, not only from the academic and research perspective, but also in the personal sphere. It would be unfair not to mention those who somehow contributed to the completion of this thesis.

First, I have Prof. Simone Fischer-Hübner to thank for giving me the opportunity to pursue my doctoral studies under her supervision, for introducing me to the research field of computational privacy, and for providing my with advice and directions whenever I need them. I am privileged for having her as my supervisor.

I am thankful for have been given the chance of working with so many wonderful people with whom I share not only the authorship of the papers include in this thesis, but also problems, solutions, ideas and so many hours of fruitful discussions. They are: Prof. Simone Fischer-Hübner, Prof. Tereza Cristina Carvalho, Prof. Wilson Ruggiero, Dr. Yeda Venturini, Dr. Christiane Schweitzer, Dr. Armin Mittelsdorf, Fernando Redigolo and Christer Andersson. They all have my deepest respect.

I would like to thank all my colleagues at the Department of Computer Science for providing me such a nice and friendly work environment. Thanks to Irina Persson, for reviewing my reference list. I also want to thank all members of the Privacy and Security Group, especially Stefan Lindskog, Reine Lundin, Hans Hedbom and my co-advisor, Thijs J. Holleboom. I am honored to be part of such fine group.

I am also grateful for having made such good friends in the last two and half years, who had definitely helped me in several aspects during my adaptation process. I would consider my thesis incomplete if I do not name at least some of them. First, I want to thank my dear friends Ximena Dahlborn and Torbjörn Andersson for being so nice and helpful. I am fortunate to have Christer Andersson as a great friend, with whom I have been sharing the office since the first day of my doctoral studies in Karlstad. I owe a great deal also to my good friend Albin Zuccato, who taught me a lot about Sweden and its idiosyncrasies, helped to review this thesis, and with whom I had long talks about everything that could possibly be discussed.

I am thankful for the friendship and support of my brother, Daniel Martucci, and my other brothers, Paulo de Andréa, Carlos E. Santoro (Bidu), Bruno Galiotto and Fernando Szterling, which whom I had the opportunity and luck to meet during my life.

All my gratitude goes to my parents, Moacyr and Olga Martucci, for their unconditional support and love. For everything, I have only you to thank.

Karlstad, August 2006 Leonardo A. Martucci

List of Appended Papers

This thesis is comprised of the following five peer-reviewed papers. References to the papers will be made using the Roman numbers associated with the papers such as Paper I.

I. Yeda R. Venturini, Christiane M. Schweitzer, Leonardo A. Martucci, Fernando F. Redigolo, Armin W. Mittelsdorf, Wilson V. Ruggiero, and Tereza C. M. B. Carvalho. Security Model for Ad Hoc Networks. In *Proceedings of the 2002 International Conference on Wireless Networks (ICWN 2002)*, pages 185–191. Las Vegas, Nevada, USA, 24–27 Jun 2002.

II. Leonardo A. Martucci, Christiane M. Schweitzer, Yeda R. Venturini, Tereza C. M. B. Carvalho, and Wilson V. Ruggiero. A Trust-Based Security Architecture for Small and Medium-Sized Mobile Ad Hoc Networks. In Ian F. Akyildiz, Erdal Cayirci, Eylem Ekici, and Giacomo Morabito, editors, *Proceedings of the 3rd Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2004)*, pages 278–290. Bodrum, Turkey, 27–30 Jun 2004.

III. Leonardo A. Martucci, Tereza C. M. B. Carvalho, and Wilson V. Ruggiero. A Lightweight Distributed Group Authentication Mechanism. In Steven M. Furnell and Paul S. Dowland, editors, *Proceedings of the 4th International Network Conference (INC 2004)*, pages 393–400. Plymouth, Devon, United Kingdom, 6–9 Jul 2004.

IV. Christer Andersson, Leonardo A. Martucci, and Simone Fischer-Hübner. Requirements for Privacy-Enhancements in Mobile Ad Hoc Networks. In Armin B. Cremers, Rainer Manthey, Peter Martini, and Volker Steinhage, editors, *3rd German Workshop on Ad Hoc Networks (WMAN 2005), Proceedings of INFORMATIK 2005 - Informatik LIVE! Band 2*, pages 344–348. Lecture Notes in Informatics (LNI), Volume P-68, Gesellschaft für Informatik (GI), Bonn, Germany, 19–22 Sep 2005.

This paper extends results reported in:

- Leonardo A. Martucci. Comparison of Anonymous Communication Mechanisms for Ad Hoc Networks. In Günter Müller and Sven Wohlgemuth, editors, *FIDIS Section 5.3 from Deliverable 3.3: Study on Mobile Identity Management*, 9 May 2005. Also available as http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.3.study_on_mobile_identity_management.pdf.

V. Leonardo A. Martucci, Christer Andersson, and Simone Fischer-Hübner. Chameleon and the Identity-Anonymity Paradox: Anonymity in Mobile Ad Hoc Networks. To be published. In *Short Paper Proceedings of the 1st International Workshop on Security (IWSEC 2006)*. Kyoto, Japan, 23–24 Oct 2006.

Part of this paper summarizes results reported in:

- Leonardo A. Martucci. Identification in Mobile Ad Hoc Networks. In Denis Royer, editor, *FIDIS Section 6.1.1 from Deliverable 11.1: Collection of Topics and Clusters of Mobility and Identity - Towards a Taxonomy of Mobility and Identity*, 9 Jun 2006. Also available as http://internal.fidis.net/fileadmin/fidis/workpackages/wp11/D11.1_Taxonomy/fidis-wp11-del11.1.mobility_and_identity.pdf.
- Leonardo A. Martucci, Christer Andersson and Simone Fischer-Hübner. Towards Anonymity in Mobile Ad Hoc Networks: The Chameleon Protocol and its Anonymity Analysis. In *Karlstad University Studies 2006:35*, Karlstad University, Sweden, Aug 2006.

Minor editorial changes have been made to Papers I, II and III.

Comments on my Participation

Concerning Paper I, its main contribution, a security model for mobile ad hoc networking, was the result of a collective effort of the authors. The writing was mainly done by me, Dr. Yeda Venturini and Dr. Christiane Schweitzer. Prof. Wilson Ruggiero and Prof. Tereza Cristina Carvalho both supervised the work. In Paper II, the security architecture for mobile ad hoc networking described in the paper was the result of the collective effort of all authors and the writing and contextualization of the work was mainly done by me. Regarding Paper III, I am responsible for both content and writing, while Prof. Tereza Cristina Carvalho and Prof. Wilson Ruggiero both supervised the work.

Regarding paper IV, I am responsible for the idea, for the first version of the requirements for anonymous communications mechanisms and also for the initial evaluation of four anonymous peer-to-peer communications mechanisms in the context of mobile ad hoc networks. This initial version was later extended by both me and Christer Andersson, who was the main responsible for the paper editing. Prof. Simone Fischer-Hübner supervised the work by discussing and reviewing the paper contents.

Regarding paper V, I am the responsible for the identity-anonymity paradox, for the initial idea of designing an overlay anonymous communication mechanism for mobile ad hoc network environment and for the first sketch of the protocol, which was later properly described using state transition diagrams and flowcharts by me and Christer Andersson. I was the main responsible for describing the protocol while Christer Andersson was the responsible for theoretical analysis. Prof. Simone Fischer-Hübner took part in the discussions regarding the protocol functionality and the theoretical analysis. She also supervised the work.

Other Papers

Apart from the papers included in this thesis, I have also authored the following papers.

1. Leonardo A. Martucci, Tereza C. M. B. Carvalho, and Wilson V. Ruggiero. Domínios Virtuais para Redes Móveis Ad Hoc. In *Proceedings of the 21st Brazilian Symposium on Computer Networks (SBRC 2003)*, pages 599–614. Natal, RN, Brazil, 19–23 May 2003.

2. Leonardo A. Martucci, Hans Hedbom, Stefan Lindskog and Simone Fischer-Hübner. Educating System Testers in Vulnerability Analysis: Laboratory Development and Deployment. In Cynthia Irvine, Matthew Rose, and Naomi Falby, editors, *Practical and Experimental Approaches to Information Security Education, Proceedings of the 7th Workshop on Education in Computer Security (WECS7)*, pages 51–65. Monterey, CA, USA, 4–6 Jan 2006.

Contents

Introductory Summary [redacted]

1 Introduction

Ubiquitous computing consist of computational environments providing information instantaneously through invisible interfaces[1], allowing unlimited spreading and sharing of information and offering an invaluable support for many aspects of the society and its institutions. This futuristic scenario is foreseen to be materialized with the advent of seamless communication networks combined with pervasive computing and natural human-computer interfaces, ultimately leading to an omnipresent distributed computing environment. These environments represent a paradigm shift from the current networking and computer model. However, the realization of such environments is dependent on the development of new solutions and protocols.

The research presented in this thesis is focused on a single, but fundamental core technology needed to enable ubiquitous computing: mobile ad hoc networks. Mobile ad hoc networks consist of mobile computers that establish on the fly network connections through their wireless interfaces, enabling instantaneous networking independently of the presence or aid of any central devices. The advent of mobile ad hoc networks is a paradigm shift per se from the current network infrastructure model, on which the network has defined borders and where the basic network services, such as addressing, routing and security, are provided by specific devices.

In mobile ad hoc networking every device is responsible for its own basic services, including packet routing, data forwarding, security and privacy. Therefore, most of the protocols employed in hardwired networks are not suitable for mobile ad hoc environments, since they were designed for static environments with defined borders and highly specialized devices, such as routers, network addressing provisionment servers, firewalls and intrusion detection systems.

Among the several challenges included on deploying mobile ad hoc networks, this work concentrates on the achievement of network security and privacy. Moreover, this thesis discusses the consequences of the deployment of different mobile ad hoc networks security solutions for the provisioning of privacy and also to the definition of a digital identity in these environments.

Network security can be defined as the achievement of the five security services (authentication, access control, confidentiality, integrity and non-repudiation) specified in the Telecommunications Standardization Sector of the International Telecommunications Union (ITU-T) Recommendation X.800 [2] along with the provisioning of availability [3]. A standard definition of security services is found in the Internet Engineering Task Force (IETF) RFC 2828 [4], which describes a security service as: a processing or communication service that is provided by a system to give a specific kind of protection to system resources.

[1] The term invisible interface was coined at the Computer Science Laboratory at XEROX Palo Alto Research Center (PARC). In this context, invisibility means that the technology (i. e. the user interface) should be only used as an enabler to the accomplishment of the task, and never as the tasks' centerpiece [1]. From this aspect, ubiquitous computing was understood as the opposite of virtual reality in terms of interfaces.

In this thesis, the topic of the first three papers is network security. Papers I and II describe a security model and a security architecture for mobile ad hoc networks respectively. The goals of these papers are the description of a comprehensive security model and the development of an architecture that can provide security services and limited privacy protection to a controlled set of devices. In this architecture, mobile devices may belong to multiple administrative authorities, also called virtual domains. Paper III presents a lightweight distributed group authentication mechanism which main goal is the identification of devices belonging to a known virtual domain, along with the non-disclosure of the device and group identities to individuals outside the trusted group. Another goal of this mechanism is to mitigate the effects of attacks targeting the battery resources of mobile devices.

Privacy is a concept that is not easily defined, since the understanding of privacy is basically a cultural construct, and, hence, subjective, changing significantly between different societies [5]. Although it seems not to be possible to provide a precise and universal understanding of privacy, it is feasible to identify the three underlying aspects that construct the concept of privacy independently of the cultural background. These aspects of privacy are [6]: informational privacy, territorial (or spatial) privacy and privacy of the person. Informational privacy is related to the a person's right to determine when, how and to what extent information about him or her is communicated to the others [7]. Territorial privacy refers to the ability of controlling the information that enter and leaves the personal sphere, i. e., the close physical area surrounding an individual [8]. Finally, privacy of the person describes the people's right to be protected against physical undue interference [6].

In this thesis, informational privacy is the topic of Papers IV and V, which focus on the achievement of anonymous communication in mobile ad hoc networks. The former paper presents an evaluation of several peer-to-peer anonymous communication mechanisms and their adequacy to mobile ad hoc requirements, while the latter proposes an anonymous communication mechanism for mobile ad hoc networks and also introduces the identity-anonymity paradox. Furthermore, in this thesis, we discuss the utter importance of an appropriate definition of identities and identifiers in computer systems, and the impact of this definition related to security and privacy, especially in mobile ad hoc network environments.

Providing security and privacy is a keystone factor for the take up and success of mobile ad hoc networking, and, consequently, to omnipresent distributed computing environments. Therefore, the deployment of suitable security mechanisms and privacy-enhancing technologies in mobile ad hoc networking is of major importance to achieve users' trust, especially if confidential or private information is being dealt with and, thus, potentially under threat of being disclosed to unauthorized parties.

In principle, security and privacy are two complementary properties that may naturally be implemented together. Digital security techniques, such as encryption, can be employed to empower privacy for example. However, a clear conflict exists between the provisioning

of certain security and privacy properties together[2] [6]. Although we do not solve this conflict in this thesis, we point out that the the lack of trusted identifiers is not an answer for the provisioning of anonymous communications and we show that the connection between the provisioning of security and anonymous communications in mobile ad hoc networks is the definition of the network identifiers.

The remainder of this section succinctly presents the goals of this thesis in Section 1.1, followed by the structure of this thesis in Section 1.2.

1.1 Objective

The definition of the identity-anonymity paradox and the impact of this paradox on security and privacy on mobile ad hoc network are the main goals of this thesis. The accomplishment of this objective is supported, either directly or indirectly, by the papers included in this thesis.

Each of the papers encompassed in this thesis has, of course, its own objectives, findings, conclusions and discussions. However, in the context of this thesis, each of these papers provide an invaluable contribution to the discussion of the impact of identities and identifiers and their relation to security and privacy in mobile ad hoc environments.

The security model, architecture and the lightweight distributed authentication mechanisms for mobile ad hoc networks, described in the Papers I-III of this thesis, were mainly designed for closed groups in mobile ad hoc networks (i. e., devices belonging to one or more autonomous systems). In the aforementioned papers, we indirectly concluded that trusted identification is essential to the provisioning of security in mobile ad hoc networks. Even though not included in these papers, problems regarding unidentifiable devices were discussed before the achievement of the presented results. In particular, from the findings and discussions regarding these first three publications we concluded that device identification is critical for the provisioning of security in mobile ad hoc networks, as it is in hardwired networks. The need of identification also appeared in Paper IV during the evaluation process of anonymous communication mechanisms in the light of mobile ad hoc networks and in Paper V on the proposal of Chameleon, an overlay anonymous communication mechanism suitable for mobile ad hoc environments.

In conclusion, the five publications encompassed in this thesis were fundamental for the discussion about the impact of the definition of identity and identifiers on mobile ad hoc network security and privacy aspects and, later, for the formulation of the identity-anonymity paradox, to be presented in this thesis.

[2]For instance, preventive security, or the ability of predict and preempt malicious activities, has gained momentum in the beginning of this decade at the cost of anonymity provisioning for instance. The modus operandi of preventive security generally includes electronic surveillance by the monitoring and eavesdropping of personal communication data en masse, which some understand as the price to be paid for a secure society, while others see it as a violation of privacy rights, and even the beginning of the Orwellian society.

1.2 Structure

This licentiate thesis presents an introductory summary regarding a collection of five peer-reviewed papers in the area of security and privacy in mobile ad hoc networks that were either authored or co-authored by the writer of this thesis.

The remainder of the introductory summary is organized as follows. Section 2 presents the research questions underlying this thesis and the research methodology employed to address those questions. Section 3 provides theoretical background and the related work regarding this thesis, which includes a taxonomy of security models proposed for mobile ad hoc networks in Section 3.1 and the description of anonymous communication mechanisms for mobile ad hoc network environments in section 3.2. Section 4 presents and discusses the identity-anonymity paradox, which demonstrates why identities are needed to achieve reliable anonymity. By reliable anonymity we understand the ability of an anonymous communication mechanism to offer the claimed anonymity properties even in the presence of malicious nodes. The contributions of this work are outlined in Section 5, while Section 6 summarizes the contents of the five papers included in this thesis. Finally, concluding remarks and an outlook of the future research directions are provided in Section 6.

2 Research Issues

In this section, the underlying research questions and the research methodology, used to address these questions, are presented and discussed.

2.1 Research Questions

As presented in Section 1.1, the main objective of this thesis is the discussion about the impact of the definition of identity and identifiers on mobile ad hoc network security and privacy aspects. Therefore, the research questions involved in this work reflect the underlying research activities necessary for the achievement of the goal of this thesis.

The answers to the first two questions provide a fundamental background for answering the third research question, which refers to the main goal of this thesis. The overall research questions for this thesis are:

1. *How to provide network security in mobile ad hoc networks?*

   Answering this question demands the definition of an acceptable trade-off between performance, usability and security. In Papers I and II we define a set of trade-offs and propose a security model and architecture designed for mobile ad hoc environments. Paper III presents a detailed description of a lightweight distributed group authentication protocol especially designed and implemented as part of the architec-

ture presented in Paper II. In addition, in Section 3.1 we present a taxonomy of proposed security models for ad hoc networks and in Section 4 we evaluate the strength of these models from the point of view of a specific attack regarding the problem of uniqueness of network identifiers, the Sybil attack [9]. We concluded from this question that trustworthy identifiers are a prerequisite for security in mobile ad hoc networks.

2. *What are the requirements and how to provide anonymous communication in mobile ad hoc networks? Can existing peer-to-peer anonymous communication mechanisms be directly deployed in mobile ad hoc networks?*

This question is investigated in Paper IV, which presents a set of requirements for anonymous communication mechanisms and also a set of properties of mobile ad hoc environments. We concluded that no proposed peer-to-peer anonymous communication mechanism could be directly implemented in mobile ad hoc networks. Therefore, we proposed, in Paper V, Chameleon, an anonymous communication mechanism for mobile ad hoc networks, which extends the Crowds protocol [10] to make it suitable for the requirements of mobile ad hoc networks. We concluded from this question that the uniqueness of identification demands the deployment of trustworthy identifiers, as required in most anonymous communication protocols while other mechanisms based on unidentifiable devices are susceptible to Sybil attacks.

3. *What is the relationship between anonymous communication, security and identification in mobile ad hoc networks?*

This question is analyzed in both Paper V and in Section 3 of this thesis. The relationship between those three parameters led us first to a taxonomy of the security models in mobile ad hoc networks, in Section 3.1, to a classification of anonymous communication mechanisms for mobile ad hoc networks in Section 3.2 and later to considerations regarding the usage of unidentified (anonymous) devices in mobile ad hoc networks in Section 4. Finally, the combination of these findings are extended to achieve the main goal of this thesis: the analytical formulation of the identity-anonymity paradox, in Section 4.

2.2 Research Method

The scientific research method used during the research that led to this thesis had the (recurrent) steps: literature study, problem statement, hypothesis formulation, testing and evaluation, and conclusions. This research method is classified as deductive research [11], since hypotheses (or theories, according to the deductive research terminology) were proposed and afterwards tested in order to verify the validity of their claims.

Hypotheses testing was either done with the implementation of prototypes, simulation or by analytical methods. For the evaluation of these hypotheses, we used the following

methods: live network results (under a controlled environment after the implementation of a prototype) in Papers II and III; simulation in Paper III, and; logical analytical evaluation in all papers. Hypothesis falsification was used as analytical evaluation tool, mainly in Paper IV.

The model presented in Paper I led to the architecture presented in Paper II. The problem statement for those two papers were, in general, the same: the provisioning of security in mobile ad hoc networks. The model aspects were evaluated against the particular characteristics of mobile ad hoc networks. In Paper II, we tested the functionality and usability of the system architecture prototype, a proof of concept implementation, and also the fluctuations of the trust parameters to check if they follow the expected behavior from the analytical model. The architecture was also analytically evaluated during the conception process.

In Paper III, we present a lightweight group authentication mechanism that could deny the exposure of the digital certificates that identify one network entity (user or device). The mechanism presented in Paper III was designed as an answer to this problem. Functional tests were performed over a proof of concept prototype, which was later added to the prototype presented in Paper II. In addition, the security properties of the protocol proposed in Paper III were analytically evaluated according to a set of security attacks. Finally, simulation was used to verify the randomness properties of the pseudo-random number generator (PRNG) embedded for the development of the mechanism presented in Paper III[3].

In Paper IV, we studied the compatibility of proposed peer-to-peer (P2P) anonymous communication mechanisms in mobile ad hoc environments. In this paper we had to state a hypothesis for every mechanism analyzed (i. e. this mechanism is compatible with the requirements of mobile ad hoc networks) and analytically evaluate it. Therefore, in this paper, we basically used falsification to evaluate the P2P anonymous communication mechanisms in the light of the mobile ad hoc network requirements. We concluded, using analytical evaluation, that none of the existing P2P anonymous communication mechanisms available nowadays is fully suitable for ad hoc networks.

The original underlying problem that led us to Paper IV was the achievement of anonymous communications in mobile ad hoc networks. The conclusion that none of current existing P2P anonymous communication mechanisms is suitable for mobile ad hoc network environments led us to the design of Chameleon, an anonymous communication mechanism for mobile ad hoc networks, presented in Paper V, which functionality is based on the Crowds protocol [10]. This paper also includes the results of the analytical evaluation of Chameleon. Results regarding the network performance of Chameleon are planned to be achieved through the means of simulation in the near future.

The ambiguity on the definition of mobile ad hoc networks in the RFC 2501 [13] was studied in order to define the (in)dependence of a mobile ad hoc network from any trusted third-party (TTP), from the point of view of the network security and privacy. We con-

[3]The simulation results of the PRNG testing do not appear in Paper III, but they are published in [12].

cluded that a TTP is needed to provide both security and anonymity in mobile ad hoc networks, since the uniqueness of identifiers could not be guaranteed without a trusted party. The extension of this rationale led us to the proposal of the identity-anonymity paradox in Section 4, which is also presented in Paper V.

3 Security and Privacy in Mobile Ad Hoc Networks

Mobility is very likely the key factor behind the success of wireless devices. It is a common belief that the prospect of having access to information anywhere at anytime is pushing the popularity of wireless networks. The dissemination of wireless data networks has been increasing in an astonishing rate since the first release of the IEEE 802.11 standard [14] in late 1999. Figures regarding the wireless expansion are barely needed since the increase on the amount of wireless hot spots available in public areas, such as airports, high-speed trains and hotels, is easily noticeable in the last few years. Recently, wireless access points had become cheap enough that domestic wireless local area networks are not uncommon anylonger. In parallel, wireless personal network technologies, such as Bluetooth [15], are becoming more popular and widespread in high-end mobile devices. Furthermore, with the upcoming of IEEE 802.16 [16] certified products in the beginning of 2006, this last mile broadband wireless access technology will certainly increase the demand and, consequently, the market for wireless solutions. Thus, the growth and importance of the wireless market is undeniable.

The aforementioned wireless technologies were originally designed to operate in single-hop scenarios and in controlled environments, since the related standards cover physical and data link aspects only. However, in order to achieve multi-hop wireless networks in an environment with potential high dynamic topologies and nodes with limited resources that may vanish and reappear in a different geographical locations, special routing algorithms are needed. The IETF Mobile Ad Hoc Network (manet) Working Group was created with the purpose of developing and standardizing IP routing for these environments [13]. Other pioneering research efforts on multihop packet radio networks were led by U. S. governmental and military agencies, such as the U. S. Army's Task Force XXI Advanced Warfighting Experiment, the U. S. Navy and Marines' Extending the Littoral Battlespace and the DARPA[4] Global Mobile [17]. However, the mobile ad hoc networking paradigm shift demands far more than just appropriate routing protocols. Suitable solutions are also needed for different aspects such as network addressing, security and privacy.

The security mechanisms included in the wireless technology standards are not suitable for mobile ad hoc networking, and, consequently, for ubiquitous computing, because they depend on the constant presence of centralized services deployed in the hardwired network. In addition, only data link security is sometimes provided by central devices usually located in the hardwired network. For instance, the Enterprise Mode of the IEEE 802.11i

[4]Defense Advanced Research Projects Agency.

amendment for wireless networks needs an RADIUS (Remote Authentication Dial-In User Service) server for authenticating devices [18, 19]. Therefore, security models and architectures suitable for mobile ad hoc network environments are needed.

The same underlying rationale is valid for privacy. The existing anonymous communication mechanisms available for hardwired networks are not suitable or directly applicable for mobile ad hoc networks, since they rely either on the constant presence of centralized services and/or on a constant network traffic flow, which implies traffic contention during periods when the amount of traffic is higher than the expected amount of traffic, or the usage of dummy traffic when this amount is below the expected. Relying on the assumption of the constant presence of a centralized service does not meet with the requirements for a mobile ad hoc network [13]. Moreover, keeping a constant traffic flow in the network may compromise the network performance or shorten the device lifetime due to excessive transmissions of dummy traffic.

The remainder of this section is divided in two parts: first, a taxonomy classifying the security mechanisms for mobile ad hoc networks is introduced along with a brief description of the mechanisms that belong to each group of solutions; finally, the anonymous communication mechanisms are briefly introduced and classified according to their functionality regarding their placement in the TCP / IP stack.

3.1 A Taxonomy of Security Models for Mobile Ad Hoc Networks

In this section, a taxonomy of mechanisms for securing mobile ad hoc networks is presented. The purpose of a taxonomy is to provide a classification of the security mechanisms proposed to mobile ad hoc networks according to a given metric. In this taxonomy, the security models are classified into three families regarding the way that identifiers are generated, obtained and, eventually, transferred.

i. *intermittently connected to an established infrastructure* — security models belonging to this group assume that mobile ad hoc networks connect periodically (or at least occasionally) to an established infrastructure, such as the Internet. Therefore, it is possible to rely on the established security infrastructure that already exists in the Internet, such as a Public Key Infrastructure (PKI), and therefore, distribute digital certificates among the participants of a mobile ad hoc network. Security schemes in this group include proposals that rely on constant or periodic access to the Internet [20] and others combining crypto-based techniques [21, 22] with digital certificates;

ii. *setting a Certificate Authority in the mobile ad hoc network* — the assumption is that one or more devices have a special role in the network, such as personal Certificates Authorities (CA) and repositories. These CA are responsible for issuing certificates or credentials to devices in the mobile ad hoc networks. There are two basic approaches to set one or more CA in mobile ad hoc networks:

(a) one or more devices have a special role in the network, such as issuing certificates and publishing certificate revocation lists, for instance. To this approach belongs the Resurrecting Duckling model [23, 24] and its variants, such as [25], which are based on a central device that have privileges over other devices and controls the ad hoc network. The usage of a secure side-channel for certificate distribution is a common assumption for these protocols;

(b) a set of ad hoc network devices has parts of a private key that is used to issue certificates usually based on threshold cryptography. As long as a sufficient part of these nodes is the network range, digital certificates can be issued. Threshold cryptography was first proposed in the context of ad hoc networks by Zhou and Haas [26] and later extended by Luo et al. [27]. How many nodes and which nodes are needed to issue a certificate is usually implementation dependent;

iii. *PGP-like (Pretty Good Privacy) security models* — the assumption is that every device has one or more public / private key pairs and that every device can issue its own certificates and distribute them as well. Security often relies on the concept of web of trust. Such solutions are distributed enough to operate in complete isolation from any deployed infrastructure, however there are absolute no guarantees regarding protection against Sybil attacks[5] [9]. This is a major drawback of security models belonging to this family, such as the École Polytechnique Fédérale de Lausanne paper series on security in mobile ad hoc networks [28–30], for instance.

The three aforementioned groups are not necessarily disjointed. To the best of our knowledge, there are no published models that can be classified as a hybrid solution. However, sketching one is not an impossible task. For instance, local scope certificate authorities may be deployed to establish several secure networks under the control of a single entity (e. g., a person or a family); and the interconnection between mobile ad hoc networks under different authorities may be achieved using a PGP-like system.

In Paper II of this thesis, a security architecture is presented relying on multiple CA-like devices that control and secure a service-oriented ad hoc network. This solutions can operate isolated from an established infrastructure, although one or more nodes play a special role regarding security.

3.2 Mobile Ad Hoc Networks and Anonymous Communications

In this section, we limit our scope to anonymous communication mechanisms in mobile ad hoc networks, which is an aspect of informational privacy. Anonymity is defined as “the

[5] In a Sybil attack, malicious users assume multiple identities, preventing the usage of security mechanisms based on filters, reputation or trust assumptions. The consequences of Sybil attacks and their countermeasures are further discussed in Section 4.

state of being not identifiable within a set of subjects, the anonymity set" [31]. Current proposals for achieving anonymity in mobile ad hoc networks can be classified in two different groups regarding their level of functionality: either in the network layer (i. e., anonymous ad hoc routing protocols) or as a middleware between the application and the transport layers (i. e., overlay anonymous communication mechanisms).

The advantages of implementing anonymity in the routing protocol are the complete transparency towards the application layer and also probable better network performance in comparison to overlay anonymous communication mechanisms (but worse compared to standard ad hoc routing protocols), since data travel directly from the source to the destination, using the route assigned by the anonymous routing protocol (if assuming that the routing protocol works as expected by determining an adequate network path).

On the other hand, a major disadvantage is the incompatibility with standard ad hoc routing protocols, what may result in a reduced anonymity set (containing the devices running the anonymous routing protocol) since it is not expected that all mobile ad hoc network users would have an anonymous routing protocol running instead of a standard protocol. Although it is technically possible to have several routing protocols running in the same device, the routing priority is given to the protocol with the lowest cost, which is a local defined parameter. Changing this parameter to force the selection of the anonymous routing protocol would require some sort of upper-layer intervention, which would void the advantage of the transparency property. In addition, even if a reasonable amount of devices prioritizes the anonymous routing protocol over the standard routing, a set of devices running only standard ad hoc routing protocols may degrade the anonymity of other devices, since they will not be able to reply to packets encoded according to the anonymous routing protocol and force anonymous nodes to disclose information. Furthermore, since messages are directly transferred from source to destination, connection information (e. g., for TCP, the connection tuple: IP source address, IP destination address, TCP source port and TCP destination port) may potentially expose the relationship between two communicating nodes and compromise some anonymity properties, such as the sender anonymity and sender-receiver unlinkability[6], for instance.

Several anonymous ad hoc routing protocols have been proposed and published recently. A non-exhaustive list of protocols may include: ANODR (Anonymous On Demand Routing) [32], SDAR (Secure Distributed Anonymous Routing) [33], PPR (Privay Preserving Routing) [34], and MASK [35]. The goal of these mechanisms is to achieve anonymity (and also location privacy, for some protocols such as ANODR and PPR) in the routing layer. All the aforementioned protocols rely on a Trusted Third Party (TTP) for the distribution of identifiers (such as transactional pseudonyms), with the exception of ANODR, which is defines itself as an "identity-free" ad hoc routing protocol.

Overlay anonymous communication mechanisms operate over the transport layer and below the application layer. The advantage of these mechanisms is that they are indepen-

[6] In this work, we will follow the Pfitzmann and Hansen [31] terminology for the definition of privacy related terms such anonymity, unlinkability and pseudonymity, for instance.

dent from the routing layer since they operate on top of the transport layer. Therefore, overlay anonymous communication mechanisms may be deployed along with standard ad hoc routing protocols. On the other hand, the disadvantages include the non-transparency towards the upper layer, since applications must be diverted from the normal data flow towards the overlay network (i. e., using a local proxy for instance). Furthermore, the network performance might be worse compared to anonymous routing protocols, since messages are routed through a set of intermediary overlay nodes and a number of connections must be established before a message is finally delivered to the destination.

To the best of our knowledge, only two overlay anonymous communication mechanisms were proposed so far. Jiang et al. [36] proposal was base on an adaptation of the Chaumian mix concept [37] to mobile ad hoc networks. Jiang et al. claim that their proposal is resistant to global observers[7], but at the cost of bandwidth-consuming dummy traffic. In addition, their proposal does not provide the property of fairness, since the mobile ad hoc network is divided into two sets: the Mix nodes and non-Mix nodes. Obviously, the performance burden is greater over in Mix nodes than in non-Mix nodes, since the former set has to execute all the mixing functions and also relays more data than other nodes. In addition, Mix-based solutions heavily rely on public-key encryption, which is a major performance drawback.

Chameleon [38] is an overlay anonymous communication mechanism designed after the requirements for anonymous communication systems in mobile ad hoc environments described in [39]. Chameleon underlying functionality is based on the anonymous path setting of the Crowds system [10], which uses the toss of a biased coin to determine if a data stream is forwarded directly to the destination or, else, it should be forwarded to relay node instead. Chameleon properties include sender, receiver and relationship anonymity against a defined set of attackers. Further details of Chameleon are described in Paper V.

4 The Identity-Anonymity Paradox

In this section we focus on the problem of identification in mobile ad hoc networks and its consequences for the aspects of security and anonymity in these environments.

According to the RFC 2501 [13], mobile ad hoc networks *may* operate in isolation — that is, in the absence of any fixed infrastructure. Therefore, the concept of autonomous systems is not applicable in mobile ad hoc environments, as there is no entity controlling the network and providing services such as routing, security or addressing[8]. The lack of standardized addressing schemes allows network nodes to change their IP addresses

[7] A global observer is able to eavesdrop all communication channels in the network simultaneously. However, global observers are not able to break public key or symmetric key crypto-systems.

[8] There are currently no standards for IP assignment in mobile ad hoc networks. Recently, the Autoconf Internet Engineering Task Force (IETF) Working Group [40] was assigned to study, among other questions, the problem of addressing in mobile ad hoc networks.

(and MAC addresses as well), or even to have multiple network interfaces (either real or virtual) with multiple identifiers each. Thus, obtaining unique, persistent and trustworthy identifiers from layers below application (regarding the TCP / IP model) is not realistic. The consequence of such fact is that traditional identification systems that rely on the usage of network or data link information are basically useless in such environments.

If the definition of mobile ad hoc networks stated in RFC 2501 [13] is taken to its extreme, i. e. if we understand *may* as a need to work in isolation from any infrastructure at all times, it may turn out that the deployment of unique identification in those environments is impossible to be guaranteed. This impossibility may lead to the fallacious argument that anonymity is naturally achievable in mobile ad hoc networks in all layers below application (regarding the TCP / IP model), since unique identifiers do not exist. In this section we first conclude that security provisioning in mobile ad hoc network needs unique identifiers and then we expose the incorrect reasoning that holds the fallacy that anonymity is naturally achieved without identifiers.

The remainder of this section is organized as follows. First we introduce the connection between anonymous devices and Sybil attacks, discuss the fallacy behind anonymous devices and the provisioning of anonymity properties and present and discuss the current countermeasures against Sybil attacks in mobile ad hoc networks. In the second part of this section, we introduce the identity-anonymity paradox by presenting the connection between network security, anonymous devices and the provisioning of anonymous communications in mobile ad hoc networks. Finally, we identify the consequences of the identity-anonymity paradox in the last part of this section.

4.1 Anonymous Devices and Sybil Attacks

The lack of reliable network and data link identification may give the impression that nodes in mobile ad hoc networks are naturally anonymous, especially if we consider using the Sybil attack as an enabler for achieving anonymity. A Sybil attack is defined as “a small number of network nodes counterfeiting multiple identities so to compromise a disproportionate share of the system” [9]. Therefore, the Sybil attack would allow the usage of multiple identifiers simultaneously, which lifetime would be equivalent to the lifetime of one session or TCP connection, for instance. Therefore, both IP and MAC addresses would constantly change and, in principle, it would not be possible to associate or track those identifiers [41]. The ultimate goal of this approach is to obtain anonymous devices, which cannot be differentiated from other devices in the network, by denying identifiers.

The general goal of deploying anonymous devices (i. e., devices without identifiers) is to achieve location-privacy and untraceability by the means of randomly changing the identifiers associated to a given device immersed in the network. However, the benefits of having random identifiers are not enough to compensate for the disadvantages that arise from the deployment of such technique in mobile ad hoc networks. In fact, {*IP, MAC*} pairs

should not be considered identifiers, since one single device can change them constantly or even have several pairs active at the same time, due to the existing lack of addressing control in mobile ad hoc networks[9].

A disadvantage of anonymous devices in distributed environments is how to correctly identify a given destination (e. g., a device offering a specific service) located in the network. If we assume a service-based mobile ad hoc network, such as a Jini [42], UPnP [43] or Konark [44] networks, any device could easily impersonate any network service. Moreover, the absence of unique identifiers might also disrupt ad hoc routing, since a malicious user could announce false information under different {*IP, MAC*} pairs.

In addition, relying only on anonymous devices is not enough to provide key anonymity properties such as sender-receiver relationship anonymity and sender anonymity against the receiver because senders and recipients establish direct connections between them. Therefore, they could be easily pinpointed and have their relationships exposed and their anonymity properties compromised.

Another drawback of such scheme is its vulnerability to traffic analysis and to physical layers oriented attacks, such as radio fingerprinting, triangulation and signal to noise (S / N) ratio tracking techniques [34], for instance, that could potentially expose the sender's location independently of the {*IP, MAC*} pair selected. Thus, the claimed benefit of protecting users' location privacy by not allocating identifiers to the network devices is not guaranteed. Current countermeasures against Sybil attacks include resource (computational, communication or storage) testing [9], radio source verification, random key pre-distribution, positioning techniques and remote code attestation [45]. However, each of these countermeasures has its own drawbacks:

- Resource testing [9] assumes that devices are limited in resources, either regarding computational power, storage resources or communication capabilities, and therefore, would not able to perform two complex tests simultaneously, if a single test would demand all the device resources. However, the heterogeneity of devices and the need of simultaneously verification of all network nodes prevent resource testing to be feasible in mobile ad hoc networks;

- Radio source verification is a variant of resource testing, which tests the communication capabilities of a network device. It does not test all nodes simultaneously, since only one communication channel can be listened in a given slot of time (if we assume the existence of a single radio in the testing device), and part of devices remain untested. However, technology limitations prevent the usage of several channels simultaneously due to interference between communication channels (e. g. the IEEE 802.11 standard allows the usage of three simultaneous channels at most [14]). In addition, a Sybil attacker could take advantage of the dynamic characteristic of mobile ad hoc networks and mimic the constantly arrival of new (Sybil) nodes in the

[9]Therefore, the properties of {*IP, MAC*} pairs are the same of transactions pseudonyms.

network;

- Random key pre-distribution [45] may work in wireless sensor networks, but are unfeasible in mobile ad hoc networks and, in addition, in this case, there is the need of a trusted entity distributing those keys;

- Remote code attestation relies on the concept that the code running in a Sybil node would be different from the code running in a legitimate node [45]. This method might be useful in sensor networks, if we assume that all nodes run the same set of code. However, it might not be the case in mobile ad hoc networks with heterogeneous devices. In addition, if only the code used for the generation of identities (e. g., network address) is attested, it may still be possible to launch several instances of the same legitimate code and starts several threads running the same code in order to bypass remote code attestation.

- Geographical positioning techniques try to pinpoint devices in order to verify the position of a node. The basic assumption relies on the law of physics that states that two bodies of mass cannot occupy the same space at the same time. Therefore, only one identifier should exist in a give geographical location. A variant of this scheme verifies the whereabouts of a node and checks if the density of nodes in a given geographical location is higher than the expected, which might indicate the presence of Sybil nodes [45]. The drawback of this technique is clear: in multi-hop wireless ad hoc networks it may be unfeasible to verify the exact position of a given device, especially without the aid of other devices, which might be non-legitimate or colluding nodes.

4.2 Defining the Identity-Anonymity Paradox

A clear conflict between mobile ad hoc network security and anonymous devices exists regarding the uniqueness of identification and the vulnerability to Sybil attacks. The usage of anonymous devices prevents, in theory, to associate a given device to a given logical identifier at a given time slot. On the other hand, security can only be provided in mobile ad hoc networks if the uniqueness of identification[10] can be guaranteed (by the means of trusted identifiers) and, therefore, the network is protected against Sybil attacks.

Network security is necessary to keep the network sanity, by preventing the network disruption, in the presence of malicious users. Without uniqueness of identification, attackers could assume multiple identities in the mobile ad hoc network and compromise basic network services, such as routing, and bypass reputation systems, for instance. Therefore, mobile ad hoc network security models that are not vulnerable to Sybil attacks and anonymous devices cannot be deployed in the same network.

[10] Uniqueness of identification is the ability to associate one logical identifier to one device.

Anonymous communication mechanisms, on the other hand, share a similar requirement with security models for mobile ad hoc networks: they both rely on unique identifiers to provide their services.

It means that a relationship between devices and trusted identifiers must exist, as otherwise a Sybil attack could be easily deployed in the network. Anonymous communications provide, in general, anonymity properties at the cost of network performance. The trade-off between the achieved level of anonymity and the network performance usually correspond to the main difference between the proposed anonymous communications. For instance, anonymous communication protocols that offer protection against global attackers usually rely on traffic contention, dummy traffic and broadcasting to achieve their goals, while other mechanisms that offer protection against an attacker model that excludes the global eavesdropper usually provide a better performance.

In conclusion, even though the concepts of anonymity and identifiers are often understood as opposites, reliable anonymity is not achievable in mobile ad hoc environments without trusted, unique and persistent identifiers since network security must also be guaranteed. Overlay anonymous communication mechanisms usually rely on unique identifiers and are a natural candidate for the provisioning of anonymity in mobile ad hoc networks since they can be deployed in conjunction with mobile ad hoc network security architectures. We named the need of unique identification for the provisioning of anonymity as the *identity-anonymity paradox*, since the concepts of identity seems to contradict the concept of anonymity, but, as shown in this section, the deployment of anonymity demands trusted identifiers.

4.3 The Consequences of the Identity-Anonymity Paradox

The consequences of this paradox and its relation with the Sybil attack lead to clear interpretation of the definition of mobile ad hoc networks in the RFC 2501 [13] regarding the operation in isolation and a better understanding of the foundations behind the issue of identifiers in proposed security mechanisms for mobile ad hoc environments. A list of conclusions can be drawn when putting the aforementioned taxonomy, the RFC 2501 definition and identity-anonymity paradox into the same picture:

- the usage of anonymous devices in mobile ad hoc networks can be harmful to the network security and must be avoided. In addition, anonymity properties, such as relationship anonymity and sender anonymity, are not guaranteed using anonymous devices. Furthermore, the possible benefits of achieving location-privacy are also not guaranteed since physical layer attacks could be used to disclose a devices' location and even also to track and associate their transactional pseudonyms[11].

- security schemes for ad hoc networks need to guarantee the uniqueness of the net-

[11] Transactional pseudonyms are pseudonyms used for one transaction [31].

work identifiers, usually by the means of digital certificates, since Sybil attacks can only be prevented in mobile ad hoc networks with trusted identifiers, usually issued by a TTP[12] (either centralized or distributed). We can conclude that anonymous communication in mobile ad hoc networks can only be achieved if security solutions from families *i* or *ii*, from the taxonomy presented in Section 3.1, are deployed (but not from family *iii*).

- regarding the definition of mobile ad hoc networks in RFC 2501 [13], to our understanding, a mobile ad hoc network may either depend intermittently on some deployed infrastructure (and therefore may operate in isolation for a given time frame) or it could operate in complete isolation from the deployed infrastructure, given that some support system (e. g., a TTP or a CA) is deployed in the mobile ad hoc network. Two important conclusions can be drawn from the previous item:

  – first, security is hardly achievable (if not impossible to be achieved) in complete distributed systems without any trust relationship between devices since the complete absence of a trusted entity may lead to a vulnerability to Sybil attacks;

  – second, in the RFC 2501, the passage "*may* operate in isolation" does not mean, regarding security aspects, that the dependence on a TTP (either centralized or distributed) is completly and utterly impossible to happen. Operating in isolation to the hardwired network does not mean the absence of all trust relationships, or the prohibition of the existence of trusted devices in mobile ad hoc networks.

5 Contributions

This section summarizes the main contributions of this thesis. They are directly related to the research questions presented in Section 2. The contributions are:

- The design of a security model for mobile ad hoc networks and, afterwards, the development, implementation and evaluation of a trust-based security architecture for the same environments that is built on top of a distributed service-based network infrastructure.

- The design, implementation and analytical evaluation of a lightweight distributed group authentication mechanism, based on shared-keys, loose time synchronization and pseudo-random number generation, that is included in the aforementioned security architecture for ad hoc networks.

[12] To the best of our knowledge, the only existing method to provide unique identification is with certificates issued by some sort of a TTP.

- The identification of the requirements for anonymous communication mechanisms under the assumptions of a mobile ad hoc network environments, the conduction of a comparative study and analysis of existing anonymous P2P communication mechanisms and the assessment whether they are suitable for mobile ad hoc networks or not.

- The design and analytical analysis of an overlay anonymous communication mechanism for mobile ad hoc networks.

- The formulation of the identity-anonymity paradox, which states that the provisioning of reliable anonymity is not achievable in mobile ad hoc environments without trusted identifiers and, in addition, the impact of this paradox in the RFC 2501 definition of mobile ad hoc networks from the point of view of proposed security models.

6 Summary of Papers

This section contains short summaries of the papers included in this thesis.

Paper I – Security Model for Ad Hoc Networks

Several new applications and the new emerging technologies that make ad hoc networking possible are pushing the development of ad hoc networks. Securing the ad hoc environment is essential for the success of these new applications as well as for the entire future of ad hoc networking. Several security aspects for ad hoc networks, such as trust management and routing concerns were approached in the last few years, but no comprehensive security models for ad hoc network environments were presented until now. This paper introduces a security model for wireless service-based ad hoc networks.

Paper II – A Trust-Based Security Architecture for Small and Medium-Sized Mobile Ad Hoc Networks

This paper describes a trust based security architecture for small / medium-sized mobile ad hoc networks. We designed and implemented a security architecture that extends the traditional PKI model, assigning variable trust values to digital certificates and issuing credentials to grant access to network services. Trust values are not static; they vary during regular network operation as network users provoke security incidents. Depending on the seriousness of the incidents the trust value associated to the offender's certificate will vary. Eventually, a series of security incidents may end up with the certificate revocation. We also developed a security framework for designing secure applications and built prototypes to

test and validate our architecture. We considered service-oriented ad hoc networks, where every mobile device is classified as service providers or service users.

Paper III – A Lightweight Distributed Group Authentication Mechanism

Identifying trustable devices and establishing secure tunnels between them in ad hoc network environments is a difficult task because it has to be quick, inexpensive and secure. Certificate-based authentication mechanisms are too expensive for small devices. The use of such mechanisms must be controlled and reserved for special situations, (e. g., banking applications) but not for everyday transactions. In addition, indiscriminate use of asymmetric ciphering and certificate-based authentication is a shortcut to battery exhaustion attacks. This paper describes a lightweight distributed group authentication mechanism suitable for ad hoc network devices requirements. We introduce the concept of group authentication, the target of which is not the individual identification of devices, but to verify if a device belongs or does not belong to a trusted group. The proposed mechanism verifies if devices have a pre-shared secret and sets new cipher keys each time it runs. This mechanism requires loose synchronization among the devices' real time clocks to thwart replay attacks. It also mitigates the effects of battery exhaustion attacks due to its lightness.

Paper IV – Requirements for Privacy-Enhancements in Mobile Ad Hoc Networks

This paper formulates requirements for anonymous overlay networks for enhancing the privacy of mobile ad hoc network users. Besides, it analyzes existing peer-to-peer based anonymous overlay networks and shows that none of them are compliant with those requirements. Finally, it outlines the ongoing design of an anonymous overlay network intended for mobile ad hoc environments.

Paper V – Chameleon and the Identity-Anonymity Paradox: Anonymity in Mobile Ad Hoc Networks

In this paper we first present the identity-anonymity paradox, which explains why identities are needed to achieve reliable anonymity. Then, we introduce Chameleon, a novel anonymous overlay network for mobile ad hoc environments, and describe it in details with the support of state transition diagrams. To the best of our knowledge, this is the first low-latency anonymous communication mechanism designed for a mobile ad hoc network setting.

7 Conclusions and Outlook

This thesis is focused in the provisioning of network security and anonymity in mobile ad hoc environments and the discussion about the impact of the definition of identity and identifiers on both security and anonymity.

We conclude that the identity-anonymity paradox is the linkage between the provisioning of security and anonymity in mobile ad hoc networks since it explains that security and anonymity can only be deployed if trusted identifiers exist in the network. Furthermore, the identity-anonymity paradox allow us to have a clear understanding of the RFC 2501 definition for mobile ad hoc networks from the point of view of security models.

Even though each appended paper has its own objectives, their findings proved to be invaluable for the background and discussion of the main goal of this thesis: the formulation of the identity-anonymity paradox and its impact on the definition of identity and identifiers in the aspects of mobile ad hoc network security and privacy.

Future research activities include in the short term the simulation of Chameleon in order to evaluate its performance in relation to varying levels of degrees of anonymity. Some of the parameters that will be tested in our tests include: the end-to-end delay variation introduced by changing a system parameter (the probability of forwarding); and the average number of data link paths used to connect a source to a destination in comparison to a standard routing protocol in order to evaluate the transmission overhead generated by the anonymous communication mechanism, and, consequently, the amount of energy spent in the network per transmitted bit.

Another short term research activity is the evaluation of the possibility of using anonymous credentials [46, 47] for guaranteeing identity uniqueness and simultaneously prevent the disclose of an unique identifier.

In the middle term, we plan to analyze the possible advantages and disadvantages of introducing cross-layer information to increase security and privacy in mobile ad hoc networks. We are particularly interested on the possibility of using the SNMP MIB[13] as a natural repository of cross-layer information that could be potentially used in the advantage of the provisioning of security and privacy in mobile ad hoc environments.

References

[1] Mark Weiser. Creating the Invisible Interface (invited talk). In *Proceedings of the 7th annual ACM Symposium on User Interface Software and Technology (UIST 1994)*, page 1. ACM Press, 2–4 Nov 1994.

[13] The Management Information Base (MIB) [48] of the Simple Network Management Protocol (SNMP) Architecture [49].

[2] Security architecture for open systems interconnection for ccit applications. Recommendation X.800 - International Telecommunications Union, The International Telegraph and Telephone Consultative Committee, Data Communication Networks: Open Systems Interconnection (OSI); Security, Structure and Applications, Mar 1991.

[3] William Stallings. *Cryptography and Network Security: Principles and Practices*. Prentice Hall, Upper Saddle River, NJ, USA, third edition, 2003.

[4] Robert W. Shirey. Internet Security Glossary. RFC-2828, May 2000. See http://www.ietf.org/rfc/rfc2828.txt.

[5] Rolf Lunheim and Guttorm Sindre. Privacy and Computing: a Cultural Perspective. In Richard Sizer, Louise Yngström, Henrik Kaspersen, and Simone Fischer-Hübner, editors, *Proceedings of the IFIP TC9/WG9.6 Working Conference on Security and Control of Information Technology in Society*, pages 25–40. North-Holland, 12–17 Aug 1993.

[6] Simone Fischer-Hübner. *IT-Security and Privacy - Designing and Use of Privacy-Enhanving Security Mechanisms*, volume 1958 of *Lecture Notes in Computer Science*. Springer-Verlag Berlin/Heidelberg, 2001.

[7] Alan F. Westin. *Privacy and Freedom*. Atheneum, New York, NY, USA, 1967.

[8] Christer Andersson. Enhancing Privacy for Mobile Networks, Licentiate Thesis, Karlstad University Studies 2005:53, December 2005.

[9] John R. Douceur. The Sybil Attack. In P. Druschel, F. Kaashoek, and A. Rowstron, editors, *Peer-to-Peer Systems: Proceedings of the 1st International Peer-to-Peer Systems Workshop (IPTPS)*, volume 2429, pages 251–260. Springer-Verlag, 7–8 Mar 2002.

[10] Michael Reiter and Avi Rubin. Crowds: Anonymity for Web Transactions. In *DIMACS Technical report*, pages 97–115, 1997.

[11] Alan F. Chalmers. *What is this thing called Science?* Open University Press, Buckingham, England, third edition, 1999.

[12] Leonardo A. Martucci. Virtual Domains for Mobile Ad Hoc Networks: a security mechanism (from the original title: Domínios Virtuais para Redes Móveis Ad Hoc: um mecanismo de segurança). Master's thesis, Escola Politécnica da Universidade de São Paulo, Oct 2002. In Portuguese.

[13] M. Scott Corson and Joseph Macker. Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. RFC-2501, Jan 1999. See http://www.ietf.org/rfc/rfc2501.txt.

[14] ANSI/IEEE Std 802.11, 1999, Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. ISO/IEC 8802-11 IEEE Std 802.11, Sep 1999. See http://standards.ieee.org/getieee802/download/802.11-1999.pdf.

[15] Bluetooth Special Interest Group (SIG). Specification of the Blutooth System: wireless communications made easy. Core version 1.1, Feb 2001. See http://www.bluetooth.com/.

[16] ANSI/IEEE Std 802.16, 2004, Local and metropolitan area networks - Part 16: Air Interface for Fixed Broadband Wireless Access System. ISO/IEC 8802-16 IEEE Std 802.16, Oct 2004. See http://standards.ieee.org/getieee802/download/802.16-2004.pdf.

[17] James A. Freebersyser and Barry Leiner. *A DoD Perspective on Mobile Ad Hoc Networks*, chapter 2, pages 29–51. Addison-Wesley, Reading, MA, USA, first edition, Dec 2000.

[18] IEEE Std 802.11i, 2004, Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Ammendment 6: Medium Access Control (MAC) Security Enhancements. Ammendment to IEEE Std 802.11, 1999 Edition (Reaff 2003), Jul 2004. See http://standards.ieee.org/getieee802/download/802.11i-2004.pdf.

[19] Nancy Cam-Winget, Tim Moore, Dorothy Stanley, and Jesse Walker. IEEE 802.11i Overview. NIST 802.11 Wireless LAN Security Workshop.

[20] Frank Kargl, Stefan Schlott, and Michael Weber. Identification in Ad Hoc Networks. In *Proceedings of the 39th Hawaiian International Conference on System Sciences (HICSS-39)*. IEEE Computer Society, 4–7 Jan 2006.

[21] Tuomas Aura. Cryptographically Generated Addresses (cga). RFC-3972, Mar 2005. See http://www.ietf.org/rfc/rfc3972.txt.

[22] Gabriel Montenegro and Claude Castelluccia. Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Addresses. In *Proceedings of the Network and Distributed System Security Symposium (NDSS 2002)* [50].

[23] Frank Stajano and Ross Anderson. The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks. In *Proceedings of the 3rd AT&T Software Symposium*, Oct 1999.

[24] Frank Stajano. The Resurrecting Duckling: What Next? In *Revised Papers from the 8th International Workshop on Security Protocols*, volume 2133 of *Lecture Notes in Computer Science*, pages 204–214, London, UK, 3–5 Apr 2001. Springer.

[25] Dirk Balfanz, Diana K. Smetters, Paul Stewart, and Hao Chi Wong. Talking to Strangers: Authentication in Ad Hoc Wireless Networks. In *Proceedings of the Network and Distributed System Security Symposium (NDSS 2002)* [50].

[26] Lidong Zhou and Zygmunt J. Haas. Securing Ad Hoc Networks. *IEEE Network*, 13(6):24–30, 1999.

[27] Haiyun Luo, Petros Zefros, Jiejun Kong, Songwu Lu, and Lixia Zhang. Self-securing Ad Hoc Wireless Networks. In *Proceedings of the 7th IEEE Symposium on Computers and Communications (ISCC 2002)*, pages 567–574, 1–4 Jul 2002.

[28] Jean-Pierre Hubaux, Levente Buttyán, and Srdjan Čapkun. The Quest for Security in Mobile Ad Hoc Networks. In *Proceedings of the 2th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC'01)*, pages 146–155, New York, NY, USA, 4–5 Oct 2001. ACM Press.

[29] Srdjan Čapkun, Jean-Pierre Hubaux, and Levente Buttyán. Mobility Helps Security in Ad Hoc Networks. In *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC'03)* [51], pages 46–56.

[30] Srdjan Čapkun, Levente Buttyán, and Jean-Pierre Hubaux. Self-organized public-key management for mobile ad hoc networks. *IEEE Transactions on Mobile Computing*, 2(1):52–64, Jan–Mar.

[31] Andreas Pfitzmann and Marit Hansen. Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology v0.28, 29 May 2006. See http://dud.inf.tu-dresden.de/literatur/.

[32] Jeijun Kong and Xiaoyan Hong. ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad Hoc Networks. In *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC'03)* [51], pages 291–302.

[33] Azzedine Boukerche, Khalil El-Khatib, Li Xu, and Larry Korba. SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks. In *Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN'04)*, pages 618–624, 2004.

[34] Srdjan Čapkun, Jean-Pierre Hubaux, and Markus Jakobsson. Secure and Privacy-Preserving Communication in Hybrid Ad Hoc Networks. Technical Report IC/2004/10, EPFL-IC, CH-1015 Lausanne, Switzerland, 30 Jan 2004.

[35] Yanchao Zhang, Wei Liu, and Wenjing Lou. Anonymous Communication in Mobile Ad Hoc Networks. In *Proceedings of the* 24*th Annual Joint Conference of the IEEE Communication Society (INFOCOM 2005)*, Miami, FL, USA, 13–17 Mar 2005.

[36] Shu Jiang, Nitin H. Vaidya, and Wei Zhao. A Mix Route Algorithm for Mix-net in Wireless Mobile Ad Hoc Networks. In *Proceedings of the 1st IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS2004)*, 24–27 Oct 2004.

[37] David Chaum. Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. *Communication of the ACM*, 24(2):84–88, Feb 1981.

[38] Leonardo A. Martucci, Christer Andersson, and Simone Fischer-Hübner. Towards Anonymity in Mobile Ad Hoc Networks: the Chameleon Protocol and its Anonymity Analysis. Technical Report 2006:35, Karlstad University, Karlstad, Sweden, Aug 2006.

[39] Christer Andersson, Leonardo A. Martucci, and Simone Fischer-Hübner. Requirements for Privacy-Enhancements for Mobile Ad Hoc Networks. In *3rd German Workshop on Ad Hoc Networks (WMAN 2005), Proceedings of INFORMATIK 2005 - Informatik LIVE! Band 2*, volume 68 of *LNI*, pages 344–348. GI, 19–22 Sep 2005.

[40] IETF Ad Hoc Network Autoconfiguration Working Group. Ad Hoc Network Autoconfiguration (autoconf), 2006. See http://www3.ietf.org/html.charters/autoconf-charter.html.

[41] Marco Gruteser and Dirk Grunwald. Enhancing Location Privacy in Wireless LAN Through Disposable Interface Identifiers: A Quantitative Analysis. In Parviz Kermani, editor, *Proceedings of the 1st ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots (WMASH 2003)*. ACM, 19 Sep 2003.

[42] SUN Microsystems. The Jini Architecture Specification – Version 1.2, 2001. See http://www.sun.com/software/jini/specs/.

[43] UPnP Forum. UPnP Device Architecture, Version 1.0, Jun 2000. See http://www.upnp.org/download/UPnPDA10_20000613.htm.

[44] Sumi Helal, Nitin Desai, Varum Verma, and Choonhwa Lee. Konark - a Service Discovery and Delivery Protocol for Ad Hoc Networks. In *Proceedings of the IEEE Wireless Communications and Networking (WCNC 2003)*, volume 3, pages 2107 – 2113. IEEE, 16–20 Mar 2003.

[45] James Newsome, Elaine Shi, Dawn Song, and Adrian Perrig. The Sybil Attack in Sensor Networks: Analysis & Defenses. In *Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks (IPSN04)*, pages 259–268, New York, NY, USA, 26–27 Apr 2004. ACM Press.

[46] Jan Camenisch and Anna Lysyanskaya. An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In *Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT 2001)*, volume 2045 of *Lecture Notes in Computer Science*, pages 93–118. Springer, 2001.

[47] Jan Camenisch and Els Van Herreweghen. Design and Implementation of the *idemix* Anonymous Credential System. In Vijayalakshmi Atluri, editor, *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS 2002)*, pages 21–30, 18–22 Nov 2002.

[48] Marshall T. Rose. Management Information Base for Network Management of TCP/IP-based internets: MIB-II. RFC-1158, May 1990. See http://www.ietf.org/rfc/rfc1158.txt.

[49] David B. Levi and Paul Levy. Simple network management protocol (SNMP) applications. RFC-3413, Dec 2002. See http://www.ietf.org/rfc/rfc3413.txt.

[50] *Proceedings of the Network and Distributed System Security Symposium (NDSS 2002)*. The Internet Society, Feb 2002.

[51] *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC'03)*, New York, NY, USA, 1–3 Jun 2003. ACM Press.

Paper I [redacted]

Security Model for Ad Hoc Networks

Reprinted from

Proceedings of the 2002 International Conference on Wireless Networks (ICWN 2002)
Las Vegas, NV, USA, 24–27 Jun 2002

Security Model for Ad Hoc Networks

Yeda R. Venturini, Christiane M. Schweitzer,
Leonardo A. Martucci, Fernando F. Redigolo, Armin W. Mittelsdorf,
Wilson V. Ruggiero, Tereza Cristina M. B. Carvalho
{yeda, chrism}@larc.usp.br, leonardo.martucci@kau.se,
{fernando, armin, wilson, carvalho}@larc.usp.br

Abstract

Several new applications and the new emerging technologies that make ad hoc networking possible are pushing the development of ad hoc networks. Securing the ad hoc environment is essential for the success of these new applications as well as for the entire future of ad hoc networking. Several security aspects for ad hoc networks, such as trust management and routing concerns were approached in the last few years, but no comprehensive security models for ad hoc network environments were presented until now. This paper introduces a security model for wireless service-based ad hoc networks.

1 Ad Hoc Networks and Security

An ad hoc network is defined as a set of mobile nodes or platforms that can move arbitrarily in a temporary infrastructure and establish an ephemera network, without the presence of a central entity, using wireless interfaces to switch packets. Ad hoc network nodes can be hosts (i. e., running users applications) or routers (i. e., switching packets to another nodes, extending the network reach) [3, 5, 6].

The same reasons that allow the set up, almost instantaneously, of a wireless ad hoc network, also bring the challenge of controlling and guaranteeing the system security required for the applications and services using such communication infrastructure [4]. The main contribution of this paper is a security model with all the basic requirements to develop secure applications and services in ad hoc network environments.

The rest of this paper is organized as follows. Section 2 presents the security aspects for ad hoc environments and its assumptions. The security model for a service-based ad hoc network is defined and discussed in Section 3. The conclusion, in Section 4, summarizes the work.

2 Ad Hoc Security Aspects

Wireless communications have several characteristics that differ from traditional wired environments; most of them are related to the nature of the communication itself. Wireless communication signals spread through the environment in contrast to wired communication, where the signal is confined in a copper or optical fiber medium. Besides, one of the greatest advantages of wireless systems, the node mobility, may lead to severe security issues [9].

It is important to understand that wireless communication can impact not only to the physical, data link and network layers of the OSI network model. Although the methods of cryptography deployed in wired network can also be applied in wireless network, sometimes they are not appropriate. For example, wireless networks have a greater error rate than wired networks and, therefore, block cryptography mechanisms might be more appropriate than stream cryptography mechanisms.

2.1 Physical Transmission

In wired networks, to avoid that unauthorized users have access to the network, the following precautions are usually taken:

- Devices are physically protected from unauthorized access and the cabling is protected against eavesdropping.
- Firewalls are installed to avoid unauthorized hosts to access controlled services.
- Network access points can be set up as security strongholds.

However, it is not possible to avoid unauthorized devices to reach the wireless network area. Any device within reach of radio-frequency signals can get access to data being transmitted, and also transmit data to other devices using the wireless interface. Interruption and interception attacks are easier to perform in wireless networks than on traditional, wired networks. To avoid this kind of attacks, implementation of services capable of assuring the availability of connection and confidentiality of information are required.

The physical layer mechanism usually deployed is the spread spectrum technique with low power transmission [1, 2, 7]. This technique increases the difficulty to mount signal interruption (e. g., a jamming attack) as well as signal interception (eavesdropping) attacks [8].

2.2 Unauthorized Access

Some characteristics in ad hoc networks may require different security solutions. Private or public network require different levels of security and different solutions as well.

2.2.1 Private Networks

In a private network, devices with authorized connection are known and controlled. These networks are usually created to serve a limited group of users and devices, such as: business networks; domestic networks; domestic automation networks; networks created for conferences or meetings outside the business networking environment and; wireless access providers to the Internet.

In these networks just authorized devices should have access to the network, but in wireless ad hoc networks, this control is not so simple. In order to control the communication and avoid intruders, devices first need to authenticate each other. However, device authentication may not be enough to control the access to the network. Other usual question in these networks is the confidentiality of data being transmitted. The use of cryptography is necessary to critical data transmission because it is not possible to avoid that an intruder could capture signals being transmitted on the air.

2.2.2 Public Networks

The services provided from a public network can be accessed by unknown devices. These networks are usually created for itinerant users. Some examples: information services offered at an airport or a temporary network with an Internet access point deployed in events. This kind of network may or may not require device and user authentication. Equally, the transmitted data can be confidential or not. Usually the need of authentication and cryptography depends on the nature of the service. In public networks, users and devices are unknown, which makes encryption and authentication mechanisms harder to be deployed, if not impossible. The use of public and private key scheme can offer authentication in the application level.

3 Security Model for Service-Based Ad Hoc Networks

In a service-based network, services are offered and requested through the communication infrastructure. The wireless ad hoc network communication infrastructure is composed by wireless devices, which communicate among themselves directly and without any fixed infrastructure. The security model, presented in this work, has the purpose of establishing a service-based ad hoc network on which services interact in a secure way.

3.1 Service-Based Networks

A service-based network is formed by a communication infrastructure and by an entity set that offers and requests services.

3.1.1 Entities

Entities can also be classified according to their physical or logical nature.

Physical entities are equipments with the most diverse complexities. The simplest devices may have one function only, such as air-conditioners, microwaves, etc., while the most sophisticated ones may offer multiple services, such as wireless phones with PBX functions, answering machines with Internet access, and computers that communicate with wireless devices, among others.

Logical entities must be hosted by physical entities to exist. Logical entities are the processes that run in servers or access devices, including the processes that interact with users.

The entities that compose a service-based network can be classified in: *users*, *service providers* (or services) and *devices*. All entities can be identified; this is an important aspect when it is crucial to protect the network against non-legitimate entities.

- *Users* are logical entities that request services to the network services providers. Users are the entities that use the network services and can be identified.

- *Services Providers* are logical entities with capacity, functionality and availability to answer to the service requests presented to them. The service capacity corresponds to the intensity with that a service can be provided. The amplitude of this capacity is related to the amount of resources allocated or associated to the service. The functionality is related to the ability to provide, supply or perform a set of functions. Finally, service availability is related to the periods of time that the device is able to perform its functionality services. A service provider may request services from another entities and may also be identified

- *Devices* are physical entities capable of supporting (hosting) services and users. Devices commonly offer user interfaces, such as displays, keyboards, microphones and touch screens. Devices have physical addresses and may be identified.

Considering the dynamic behavior of the entities, they are either *present* or *absent*, depending on the position in the network's reach-radius and their power status (*on*/*off*).

Devices can also be classified as *permanents* or *guests*. An initial configuration process defines the device's privileges. Permanent devices are those which have long-lived privileges and guest devices have short-lived privileges. Guests can be classified as unidentified, until they are not submitted to an identification process, and identified when they gone through a positive identification process. Guests that go through an identification process can assume generic identities (anonymous) or specific ones (identified guests).

3.1.2 Communication Infrastructure

The communication infrastructure provides the exchange of data between entities in a transparent way. No particular network technology is required for establishing a service-based network. The existence of an ad hoc routing protocol in the network layer will be assumed from now on in this paper.

3.2 Authentication and Authorization

Before a service or function can be used by an entity, a verification of proper permissions for this access may be performed. First, the entity is identified to verify if it is who it claims to be. This process is called *authentication* (or identification). After that, the entity's permission to use the service is verified. This process is called *authorization*.

Entities are classified in the network as a result of an initial authentication process called *registration*. This classification depends on pre-established configurations and may trigger the issuing of one or more certificates that indirectly define the entity's rights.

Actions are entities' individual initiatives, translated in the form of service requests or service replies. Generally, access devices perform service requests and receive replies. Devices that host service providers perform actions that process service requests, and return replies (and/or results).

Permissions are the rights to perform actions. Permissions can have different granularities. Service permissions define the rights to use a service as a whole, while function (or operation) permissions define rights to act on specific functions of the service.

An efficient mapping between services and entities is necessary for permission control and verification. A direct mapping between services and entities may become unpractical in networks with more than a few users or with complex services. Therefore, the proposed model use groups and profiles to simplify the mapping. *Groups* are sets of entities that are created based on common entity characteristics or purposes. *Profiles* define a set of permissions, which can be relative to devices, services or functions. Profiles form a convenient way to group permissions that are later mapped to groups of entities.

Access rights are defined as the relationship that establishes the right of an entity to perform a given action. Access rights are defined and may be verified through the mapping between users, groups, profiles and actions, as presented in Equation 1.

$$Entity \Leftrightarrow Group \Leftrightarrow Profile \Leftrightarrow Action \tag{1}$$

The *action-radius* of an entity is defined by all the actions that it has rights to execute, thus it is derived from the union of all the actions for which it has access rights.

The access rights that a service network assigns to an entity are proportional to the trust level that this network has about this entity. The trust level indicates how much the service

network trusts a particular entity. The trust level can be changed as result of administrator intervention (adding a new device in the network), promotion, demotion, suspect behavior or banishment. Finally, the trust level can be automatically changed through authentication, as when an entity passes from the non-identified to identified state.

The authentication of an entity goes through several steps. The public services network may not require authentication, while critical services, such as document signing or commercial transactions application being executed in home devices may require multiple identification levels. Services may require the appropriate identification procedures according to its own criteria, and in the order and quantity desired, allowing great flexibility and increasing security. Several types of identification procedures may be supported, such as passwords, tokens, certificates and biometrics.

After session establishment, where mutual device identification is required, extra identification requests may be optionally exchanged. The mutual initial identification exchanges the minimal amount of necessary information, to not compromise entities' privacy. Depending of the reply, new requests may be generated as well as messages granting or denying the identification presented to execute an appropriate action.

3.3 Registration Service

The registration service's purpose is to register new entities on the service-based network (i. e., initially authenticating them on the network) and issuing signed digital certificates to these new entities. Certificates should be presented by user entities on every service request for authentication purpose; if the certificate is authentic and valid, the service provider verifies the access rights related to the identified end user.

In order to use the lookup service (which belongs to the basic infrastructure of a service-based network, and contains a list of the available services) as well as general services, an entity must identify itself using the certificates issued by the device hosting the registration service, called the registration authority.

The registration service and the lookup service could be associated, but they do not necessarily coexist in the same device. Both services are essential to the network, but they do not need to be available at all times.

The registration service is mandatory for the security model, and like all services in ad hoc networks, it is not fixed on a device, and may exist in any capable, permanent and previously identified (or announced) network device. These devices could be in a list of the possible registration authorities.

The registration authorities control a mobile database of registered entities, called the *registry*. It should be distributed and shared among the permanent devices capable of being a registration authority. Service providers have to accept certificates signed from any recognized registration authority.

An entry in the registry is indexed through a unique identifier associated to each entity (e. g., a combination of the physical device address and a PIN, for devices). It includes the entities' certification information (e. g., an entity's public key) and, for devices, information regarding the class they belong to (i. e., permanent or identified guest).

When devices register in the registration service, they are classified as anonymous guests, identified guests or permanent users and devices. The registration service classifies the devices based on pre-configured list of devices that should belong to a specific class (e. g., the list of permanent devices) as well as on rules for automatic classification (i. e., if a device fulfills some requirements, it may be automatically classified and registered).

After a period of time away from its permanent (home) network, a device should be capable of recognizing its home network through its registry's logical *id*. This logical *id* should be changed periodically, following a pseudo-random sequence generated from a seed distributed to permanent devices. If the seed's secrecy is compromised, the same could be changed by the active registration service and propagated through the ad hoc network. Devices out of the permanent network range will have to be submitted to a new registry. This method guarantees the users' privacy, avoiding device tracking, and the service network privacy, avoiding identification to a non-authorized user.

The registration service also has a certification revocation list. This list contains the revoked certificates, and each revoked certificate should be at this list until the certification expiration. A service provider may also issue special signed digital certificates, independently from a central registration authority. In this case, these certificates are used to authenticate entities only to the services hosted by the issuer service provider, which becomes a special instance of a registration authority restricted to a set of specific services. When combined with trust distribution mechanisms, a set of such special registration authorities may take the role of a central registration authority.

3.4 Application Security

Many devices, such as notebooks and handheld computers, support the installation, configuration and execution of applications. These activities have potential security risks since they may allow the execution of malicious code, permit virus proliferation and compromise privacy, among other vulnerabilities.

In order to protect against potentially unsafe activities, a security model similar to the Java security model version 2 is proposed, which should:

- be secure against malicious applications: it is necessary to prevent programs from damaging its computational environment. Viruses and Trojan horses are examples of such programs;
- protect against intrusive programs: it is necessary to avoid that private information in the host device to be accessed or disclosed by the running programs;

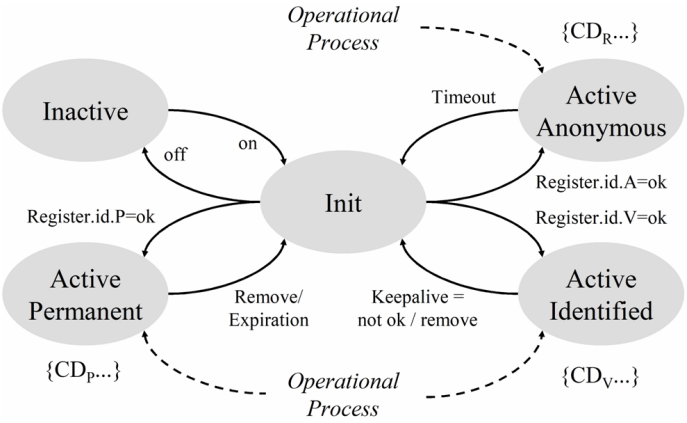

Figure 1: Device Access State Machine.

- support authentication: the author and user identity of the program should be verified;
- use cryptography: all data in transit, i. e., sent or received to / from the network or storage devices (e. g., hard disks and databases), should be encrypted;
- support audits: all potentially sensitive operations should be logged;
- be capable of being verified: rules of operation should be established and the adherence to them must be verifiable;

A virus is not a device's recognized application, since it does not own a valid digital signature (unless the system is configured to do so), and, therefore, it is prevented from executing. When an application needs more privileges, it must be a proper member of a higher privileged group, or an authorized user must modify the system permissions.

3.5 Dynamic Behavior

After the dynamic process of inserting a device in an ad hoc network environment is completed, it is necessary to consider the device's behavior in this environment. As previously seen, when devices register in the network, they are classified as anonymous guests, identified guests or permanent entities. Figure 1 shows the finite state machine related to the device behavior.

When a device accesses the network, it enters in an initial state ("Init"), under an unidentified guest status. If it successfully registers with the registration service, it becomes a network member, and moves to an active state ("Permanent", "Identified" or "Anonymous") according to the classification received from the registration service. The device

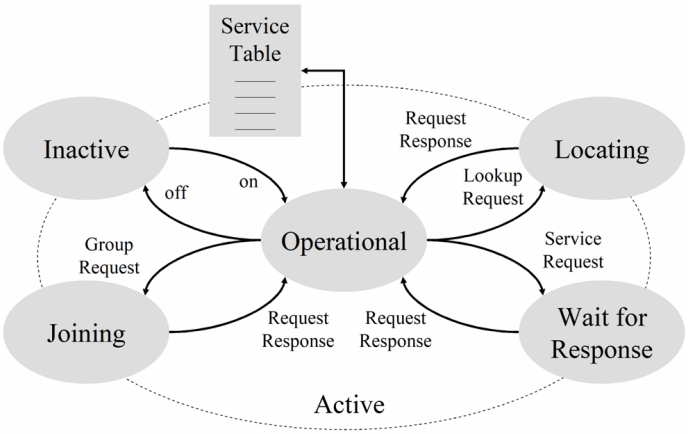

Figure 2: Finite-state machine of service access.

remains on the initial state while it does not successfully register. If it is powered off or leaves the network environment, it leaves the initial state and goes to the “Inactive” state.

If the device is registered as a permanent device (“Register.id.P=ok” transition), it means it has long-lived privileges on the network. It leaves the permanent state when its certificate expires (“Remove/Expiration” transition) or is revoked (i. e., it is removed from the list of permanent devices). When an anonymous guest certificate, which is a short-lived certificate, is issued (“Register.id.A=ok” transition), the device has a pre-defined time to access public network services (those which do not demand any identification), returning to the initial state when it times out. And last, if the device is an identified guest, it can access any network public service and guest specific services (“Register.id.V=ok” transition). It returns to the initial state when it is removed, its certificate expires or it is no longer active (“Keepalive=not_ok/remove” transition).

When a device is in one of the active states, it is necessary to consider its behavior when a service is requested, as shown in Figure 2. In the moment that the device is in an active state (“Operational” state), it can request: the location of a given service from a lookup service (“Locating” state); a service from a service provider (“Wait for Response” state); or a group registration to join additional groups and gain additional privileges. A request response indicates whether or not the request was successful.

Before using a service, a device needs to find it. Through the service location protocol, it requests the location of a service, going to the “Locating” state. It returns to the “Operational” state after receiving the answer.

When a device is in the active state as an anonymous guest, it can only locate public services. When it requests a service, it enters the “Wait for Response” state and exits this state when it receives the reply of the service provider.

3.6 Security Mechanisms

The security model encompasses several security mechanisms, which are used by the entities to interact among themselves in a secure way.

Network Discovery — An entity may belong to different networks (e. g., a home network and a corporate network). Before accessing a service, the entity must discover in which network it is presently in (using the registry *id*, for example), and select the appropriate certificates and credentials for the network services. This task is under responsibility of the network discovery mechanism.

Individual Registration — In order to access a service in a network, an entity needs to go through an individual registration process: new entities in the network should register themselves in the registration service. The registration service, according to its configuration, provides a special certificate, called an individual certificate, to the registering entity. The individual certificate is valid for that specific network and it correctly identifies the entity to the services in the network.

Group Registration — As previously seen, the entities may belong to one or more groups and, depending on which groups it belongs to, the request of service operations may be allowed or denied. In order to join a group, the entity must execute a group registration process: it registers itself to specific groups in the registration service. As a result of the group registration, entities receive group membership credentials, which shall be used to prove to service providers that they are part of one or more groups.

Registration Service Configuration — In order for entities to successfully register and receive individual and group certificates, the registration service must be configured. The registration service configuration mechanism is responsible for defining the rules that should be used in the registration process in order to issue permanent, identified guest or anonymous guest certificates.

Service Setup — Each service must be configured in order to communicate securely. This mechanism is responsible for the configuration of security parameters in a service, such as the access rights related to groups, individual entities and operation profiles as well as the security requirements for the service. All configurations must be signed, for auditing purposes. It is possible that services issue special certificates to identify entities that have access to its functions independently from the registration authority. These certificates are managed through the service setup.

Authentication — A key mechanism in the security infrastructure is the identification of entities, such as users, devices and services. This identification is possible with the individual certificates, which are issued and signed by the registration authority. To identify itself in a network, an entity presents its individual certificate, issued by the registration authority of that network, to another entity.

Session Setup — When an entity wants to communicate with a service provider, it must setup a session between them. A session must provide an encrypted tunnel for communi-

cation in the wireless medium, in order to assure the confidentiality and integrity needed for the secure communication. During the session establishment, there is the authentication phase, where the entity proves its identity to the service provider and vice-versa (if necessary). Once a session is established, an entity may request the desired service operations and, depending on the service configuration, the entity requesting the service may need to provide additional group membership credentials to have a specific operation allowed.

Logging — The network may provide a logging service for non-repudiation and auditing. There must be logging for key security operations, such as individual and group registration and service registration configuration.

Certificate and Credential Revocation — When groups or entities are removed from the network, the individual certificates and group credentials must be revoked. The revocation mechanism is responsible for maintaining and advertising the list of certificates and credentials revoked. It allows to security-tight services a way of instantly verifying if credentials and certificates are still valid as well as allows that services periodically receive this list.

Content Filtering — The content filtering mechanism is responsible for checking that viruses and other malicious code do not enter a device and corrupt services.

Runtime Checking — The processes that implement the services must be executed in a restricted environment, with signed and unsigned code having different restrictions. If malicious code bypass the content filtering mechanism, the runtime checking mechanism must detect new, non-registered services that may appear as a consequence of the malicious code, as well as detecting that a running process has been tampered. Also, if a service tries to interact with other services or the underlying device in a disallowed or unexpected way, the runtime checking procedure must detect and interfere, to avoid potentially dangerous situation.

4 Conclusions

This article presented an overview of a network security model for a service-based ad hoc network. The necessary services in this model are the lookup and registration services. The former is necessary for finding services in the ad hoc network and the latter for providing security. These services can be replicated in many devices and, despite being necessary, do not need to be present at all times, fulfilling ad hoc network requirements.

The model guarantees the security of network resources through certificates issued by the registration services. The individual certificates ensure the authenticity of the entities involved in the communication, while the groups' certificates (credentials), guarantee the access rights to services. The presence of the registration service is not essential after an entity receives its certificates: after receiving them, the entity is capable of identifying itself and the groups it belongs to, without depending on other entities.

Applying this security model it is possible to provide security in a service-based ad

hoc network without being dependent on central elements, which are usually presents at all times in traditional networks.

This security model targets services networks based in Bluetooth and IEEE 802.11b technologies. Futures works will describe the architecture of security model shown in this paper.

References

[1] ANSI/IEEE Std 802.11, 1999, Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. ISO/IEC 8802-11 IEEE Std 802.11, Sep 1999. See http://standards.ieee.org/getieee802/download/802.11-1999.pdf.

[2] Jennifer Bray and Charles F. Sturman. *Bluetooth: Connect without Cables*. Prentice Hall PTR, Upper Saddle River, NJ, USA, Dec 2000.

[3] Raffaele Bruno, Marco Conti, and Enrico Gregori. WLAN Technologies for Mobile Ad Hoc Networks. In *Proceedings of the 34th Hawaiian International Conference on System Sciences (HICSS-34)*, Washington, DC, USA, 3–6 Jan 2001. IEEE Computer Society.

[4] Laura Marie Feeney, Bengt Ahlgren, and Assar Westerlund. Spontaneous Network: an Application Oriented Approach to Ad Hoc Networking. *IEEE Communications Magazine*, 39:176–181, Jun 2001.

[5] Vesa Kärpijoki. Security in Ad Hoc Networks. In *Proceedings of the Seminars on Network Security, Helsinki University of Technology*, 2000.

[6] Charles E. Perkins, editor. *Ad Hoc Networking*. Addison-Wesley, Reading, MA, USA, first edition, Dec 2000.

[7] Bluetooth Special Interest Group (SIG). Specification of the Blutooth System: wireless communications made easy. Core version 1.1, Feb 2001. See http://www.bluetooth.com/.

[8] Marjaana Träskbäck. Security of Bluetooth: an overview of Bluetooth security. Helsinki University of Technology, 2000.

[9] Lidong Zhou and Zygmunt J. Haas. Securing Ad Hoc Networks. *IEEE Network*, 13(6):24–30, 1999.

Paper II [redacted]

A Trust-Based Security Architecture for Small and Medium-Sized Mobile Ad Hoc Networks

Reprinted from

Proceedings of the 3rd Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2004)
Bodrum, Turkey, 27–30 Jun 2004

A Trust-Based Security Architecture for Small and Medium-Sized Mobile Ad Hoc Networks

Leonardo A. Martucci, Christiane M. Schweitzer, Yeda R. Venturini,
Tereza Cristina M. B. Carvalho, Wilson V. Ruggiero
leonardo.martucci@kau.se, {chrism, yeda, carvalho, wilson}@larc.usp.br

Abstract

This paper describes a trust based security architecture for small / medium-sized mobile ad hoc networks. We designed and implemented a security architecture that extends the traditional PKI model, assigning variable trust values to digital certificates and issuing credentials to grant access to network services. Trust values are not static; they vary during regular network operation as network users provoke security incidents. Depending on the seriousness of the incidents the trust value associated to the offender's certificate will vary. Eventually, a series of security incidents may end up with the certificate revocation. We also developed a security framework for designing secure applications and built prototypes to test and validate our architecture. We considered service-oriented ad hoc networks, where every mobile device is classified as service providers or service users.

1 Introduction

Mobile ad hoc networks are notorious for their unusual characteristics, such as the lack of a permanent infrastructure, the sporadic nature of connectivity, the dynamically changing topology and the absence of network frontiers and central entities [7]. Mobile ad hoc networks, due to their singular attributes, demand new protocols and solutions for their open issues, such as suitable routing protocols, convenient QoS designs, applicable network addressing schemes and appropriate security mechanisms, for instance.

Security in mobile ad hoc networks is a matter of scope and environment as its requirements basically depend on the network purpose and on the network goal. For instance, the security requirements of a military ad hoc network are different depending on the scenario. Confidentiality and availability are the most important issues in a battlefield, whereas in a humanitarian rescue mission scenario, availability is far more meaningful than confidentiality. Therefore, the application context defines the security requirements in every case.

This paper presents a security architecture designed for small and medium-sized service-based ad hoc networks whose mobile and fixed devices can be grouped under a same ad-

ministrative authority. Security is achieved by extending the existing PKI (Public Key Infrastructure) model. Non-static trust information was added to digital certificates and new PKI states were defined. A certificate-based authentication procedure is preceded by a group authentication technique, which works with pre-shared keys and symmetric ciphers, verifies if the devices belong to a trusted group. The group authentication is a challenge-response mechanism presented in [9].

An object-oriented application framework implements the trust-based security architecture functionalities. It was built for designing and developing applications for mobile ad hoc networks over a secure foundation provided by the proposed security architecture. This framework is briefly described in this paper.

Two prototype applications (an electronic file signer and a secure slideshow application) were designed and implemented over the application framework in order to test and evaluate the security provided by the architecture. A second, but not least important, reason was to test and evaluate the usability of the framework.

The remainder of this paper is organized as follows: security threats against general ad hoc networks are briefly addressed in Section 2; in Section 3, an overview of the state of art of context-based security for ad hoc networks is provided; in Section 4, the scope of the proposed security architecture and appropriate environments are described; in Section 5, the proposed security architecture is presented; in Section 6, a step-by-step roadmap on how to secure an ad hoc network with the proposed trust-based security architecture is provided; security mechanisms used to secure an ad hoc network running over the secure application framework are presented in Section 7 whereas implementation details, tests and results can be found in Section 8 and 9; Section 10 summarizes the achieved results and also provides a glance of future research activities.

This paper summarizes one of the results of a two-year research project held at University of São Paulo (USP) and corresponds to the third paper to be published regarding the achievements of this project. The first two publications, [9] and [16], described a security model for ad hoc network and a challenge-response mechanism used to identify trusted devices in an ad hoc environment. A fourth paper describing a more refined challenge-response authentication mechanism for ad hoc networks is going to be published in the near future [10].

2 Security Threats in Ad Hoc Networks

Network services available anytime and anywhere and wandering nodes with seamless connectivity are two important ad hoc network characteristics. However, this absolute lack of boundaries is the Achilles heel of such networks, as no network borders exist to be defended, turning security into a fuzzy task. Therefore, every device has to guarantee its own security [6].

Security threats in ad hoc networks are somewhat an extension of the threats found on conventional (wired) networks. Even though these threats are described in several published works, such as [6, 7, 13], we intend to provide a brief description of security threats and their relation with ad hoc network characteristics, in order to deliver enough background for the good understanding of the rest of this paper.

The security taxonomy described in [14] is used to allow the identification of new attacks that concern wireless networks.

2.1 Passive Attacks

Mobile ad hoc networks are passive to eavesdropping (as any wireless network), due to the communication medium nature. Interception of radio frequency carriers and, therefore, the transmitted data (that shall or shall not be ciphered), must be understood as unavoidable. IEEE 802.11 and Bluetooth, two of the most popular wireless communication standards nowadays, rely on spread spectrum (SS) communication with public direct sequence (DS-SS) codes and/or public frequency hopping (FH-SS) patterns, in order to provide interoperability among devices from different vendors. In these standards, SS does not aim to provide security, but only ISM (Industrial, Scientific and Medical) conformance with spectrum band usage rules.

In fact, layer 1 security is hardly an option for open-standard communication technologies because a shared-medium is emulated in the physical layer. However, military communication systems are notorious for relying on long DS-SS codes or long FH-SS patterns in order to thwart passive attacks. This paper will not consider layer 1 security, as our proposed architecture was designed and implemented to be applied over open-standard wireless communication technologies.

Traffic analysis involves the capture of transmitted data, followed by their storage and analysis, in order to extract useful information from ciphered payloads. As previously seen in this section, wireless networks are exposed to eavesdropping. If weak ciphers schemes are used, its combination with passive attacks can lead to very insecure wireless networks - IEEE 802.11 WEP (*Wired Equivalent Protocol*) is an example of a poor security protocol (more about WEP weaknesses in [4]).

2.2 Active Attacks

Active attacks against mobile ad hoc networks are a superset of attacks on conventional networks (see more in [11] and [14]). These attacks can be divided in the following categories:

- Replay attacks involve capturing, storing and retransmission of a message or sequences of messages. Replay attacks often prelude other security attacks. Wireless

networks are highly susceptible to replay attacks, as messages are transmitted "over-the-air" and are, thus, susceptible to be intercepted.

- Masquerade or impersonation attacks occur when one entity pretends to be a different entity. Unprotected or weak authentication mechanisms usually lead to this security threat, as message sequences can be easily replayed. Man-in-the-middle (MitM) attacks often prelude impersonation attacks. Flaws in tunnelled authentication mechanisms for wireless networks using man-in-the-middle attacks were published in [3].

- A message modification attack takes place when a message or a sequence of messages are captured or intercepted, altered and retransmitted. Intentional delaying and message reordering are also considered to be modification attacks. In order to prevent this kind of security attack, data integrity must be guaranteed. Protection against modification attacks is essentially based on the same suite of protocols in wireless and conventional networks. However, mobile ad hoc networks are more susceptible to message modification, as data can be relayed by every node, trusted or not, in the wireless network.

- Denial of service (DoS) prevents or inhibits service provision in computer networks. Logical DoS may be avoided if a strong authentication mechanism is applied, but physical DoS is hard to prevent in standardized communication systems for public usage. Service disruption in wireless networks is easy to perform, as it is possible to jam the frequency range being used by wireless communication (as it is standard defined). However, in order to jam a wireless network, the attacker must be in network range. Wireless network devices are also susceptible to battery exhaustion attacks, a special kind of denial of service that targets battery-driven mobile devices [12].

3 The State of Art of Context-Based Security for Ad Hoc Networks

As presented in Section 1, defining the context and the purpose of a mobile ad hoc network is decisive as it sets the security demands for each specific scenario. This section presents the state of art of security for ad hoc networks, presenting security models, mechanisms and also their target scenarios. The most relevant work concerning the context and the scope of our work (see Section 4 for more information about the scope) is also presented in this section. Nevertheless, we do not have the intention to present an exhaustive list of published papers regarding ad hoc networks security.

The "Spontaneous network" proposal [6], for example, was designed to secure ad hoc networks restricted to a small area, such as a room, where users can share a common secret and set a secure and spontaneous network. A similar approach was proposed in [2], which assumes the same scenario as a starting point, but with a slightly different goal — deriving

strong symmetric keys starting from weak keys. As seen, both proposals were designed for a very specific environment, a small group confined in a closed place, like a meeting room or a conference room. In addition, all users must trust each other, which is a reasonable assumption for a closed context.

An alternative and realistic scenario is an environment where all devices belong to one user or a group of users or even a small office. All these devices are under a same administrative authority and they all belong to the same secure group of devices, which may establish secure communication channels among them. The setting of these groups and the distribution of cryptographic keys among devices that compose a group were the target of several papers. "The Resurrecting Duckling" security model [13] and the following "What's next?" [12] were among the first works to propose a solution for this scenario using a central and portable device, the "cyber representative", which distributes digital certificates to other devices using physical contact, in a process denoted "system imprinting". This model was the first security design that was complete enough to be denoted as security architecture for mobile ad hoc networks to be ever published. It tries to cover all network threats in a single and coherent solution. However, this proposal is far from perfection due to some naïve assumptions, such as an all-mighty device, the absence of a closed scope and the lack of proper solutions for some security questions, such as battery exhaustion attacks.

Zhou and Haas [18] presented a mechanism for key setting and distribution in an ad hoc network distributing pieces of a private key among special devices denoted servers and signing certificates using threshold cryptography. This mechanism was later improved in [8] by allowing a group of nodes that share a common secret to sign a digital certificate. Although none of these two papers specify a target environment, they are obviously meant to be applied in closed environments, where nodes know each other beforehand, as they are supposed to share some sort of common information before starting to issue certificates. Therefore, it is reasonable to assume that both of these mechanisms, even though being designed to secure routing in ad hoc networks, rely on the assumption that at least its first nodes belong to a single user or community of users that share a common interest.

Hubaux, Buttyan and Čapkun [7] proposed a public-key distribution system suitable for self-organized ad hoc networks. Their proposal have some similarities with the PGP (*Pretty Good Privacy*) system, with users issuing their own digital certificates, but with no directory server for public key distribution. In fact, this work suggests that every device should keep a small repository with certificates selected by the user. Public-key checking is done by merging the local repositories of two users/devices and trying to find a certificate path (chain) between them. However, the presence of dishonest users is poorly addressed and new authentication methods are needed to circumvent this problem. This system was designed assuming a network that exhibits a *small world* property (see [17]). The *small world* scenario, applied to the ad hoc networks environment, postulates that these networks have a small average diameter and highly clustered characteristics, which increase the probability of finding a certificate path between two nodes. They assert that their proposal can

be applied in self-organized environments, such as ad hoc networks and peer-to-peer applications, but its usability seems to be very limited to users will, and it seems not suitable for automatic activities (e. g., data synchronization).

Candolin and Kari presented a security architecture for wireless ad hoc networks relying on trust information [5]. Even though no specific environment is explicit in the paper, some architecture details, such as a network establishment along with a certificate issuing procedure, reveal the nature of the target ad hoc scenario (small ad hoc networks that can rely on a single certificate issuer). Trust information is service-oriented, which means that a device should have multiple trust values associated to it and decisions are based on the trust relationship between service provider and user. However, how exactly trust information is first set and also how trust loss occurs is omitted. Furthermore, the revoking method can lead to full-scale DoS attacks against the protected ad hoc network, as a compromised node can falsely declare that a network device is guilty of an offensive action, which may lead to the revocation of the victim's certificate.

In next section, the scope of our security architecture is presented and also its target environment.

4 The Scope and Environment

A trust-based security architecture suitable for small and medium-sized mobile ad hoc networks is the main goal and contribution of this paper. However, before starting to describe the security architecture and its implementation we need to define the term small and medium-sized ad hoc networks.

We consider small and medium-sized networks to be all networks whose devices belong to a single person, a group of persons (e. g., a family) or an organization (e. g., an office, a small community). In fact, we believe that the great majority of future mobile ad hoc networks will fit under the given specification. In addition, we believe that some small administrative work is acceptable to perform some key actions (e. g., joining new devices to the secure network) for an ad hoc network with a limited number of users and devices.

We also considered a service-oriented network (Jini-like [1]), where all devices are classified as service providers or users. Service-oriented networks usually have one or more service directory services, which track and keep a list of all available network services in the neighborhood. We assumed that any network device with enough resources can assume the role of a service directory in the absence of an online directory service. And we assume that mobile devices could be clustered according to their ownership or affinity (i. e., personal devices from employees of one office may belong to the office's secure cluster and also to the employee's home cluster). These secure clusters are named *virtual domains* [9].

We also presupposed that a secure wireless ad hoc network established under the rules of the proposed security architecture is under control of at least one person with admin-

istrative rights (administrator), as it is usual in any existing network. Administrator roles include: initializing and creating a new secure ad hoc network, allowing devices to join a secure network, expelling devices from a secure network, etc.

Even though all devices belonging to a single administrative authority may be scattered and out of radio range, they will still keep their bounds with other devices belonging to the same secure network. In fact, the terms small and medium-sized refer to the size of the secure network only. Moreover, this limitation regarding the dimension of the ad hoc network is given only because some administrative work is needed during system bootstrapping, as described in the following sections. Notice that a secure network can be established and run over an insecure ad hoc network.

5 Trust-Based Security Architecture

The proposed trust-based security architecture for small and medium-sized ad hoc networks assumes a service-oriented network. Network devices "incarnate" network service providers and/or clients.

The proposed architecture is a composition of shared secrets, loose synchronization among devices' real time clocks, symmetric and asymmetric ciphers protocols and trust information embedded in digital certificates. Next, some assumptions about network devices to be secured are made:

- Every device has to run at least one symmetric and one asymmetric cipher and has memory enough to store its own digital certificates;
- Some devices have enough memory to keep a list of all running services in the neighborhood (defined by radio range). All these devices are eligible to host a service directory;
- At least one device has a user-friendly interface and enough memory to keep a digital certificate store.

We stress that the main goal of the proposed security architecture is the achievement of a security architecture blueprint and an application framework as well, in order to provide a platform for implementing new secure applications in such environments.

In this section, we introduce the main components of the proposed security architecture. In Section 5.1 we present the network entities, with a common definition for every physical or logical component of the proposed security architecture. In Section 5.2 we classify these entities according to their status and in Section 5.3 we introduce how trust information is spread in the ad hoc network and translated in our security architecture. Finally, in Section 5.4, we present the new trust states that extend the current PKI model.

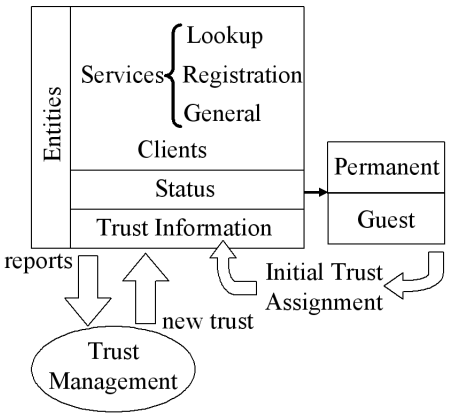

Figure 1: Security architecture items: entities (clients or servers), their related status and trust information.

Figure 1 shows the security architecture components and some relationships between them. It represents generic entities, their contents (*status* and *trust information*) and also how trust information is changed (*reports* and *new trust*). The *trust management* block is actually a service of an existing entity, as seen in this section.

5.1 Network Entities

Logical entities run in physical devices. One device may host one or more logical entities. The proposed security architecture assumes two different entities:

- Clients;
- Services — three different service providers exist: lookup services; registration services; and general service providers.

The term entity will be freely used in this paper to refer services and also clients.

Clients (C) are entities that use services. They may either be a piece of software or a human user interacting with a mobile device. General service providers (P) are entities that deliver services. Services may be provided for public access or restricted to known entities. Peers that request services are denoted clients and peers that receive service requests are denoted service providers.

Lookup services (*LS*) are directories that keep a list of all available network services in the neighborhood, which is defined by radio range of the wireless interface. One or more *LS* may exist at the same time and any device with enough resources in the ad hoc network may run a *LS* if no *LS* is available.

Registration Services (*RS*) are the first service and starting point of every ad hoc network to be secured with our architecture proposal. A device that runs a *RS* needs a friendly user interface and is supposed to be a resourceful mobile device, with memory and processing power enough to keep a small digital certificate database and to issue digital certificates in a reasonable response time. *RS* issue digital certificates with embedded trust information and keep lists of issued certificates and modification of their trust values. *RS* have similarities with PKI's Certificate Authorities (CA). However, *RS* really extend the CA concept. For instance, *RS* can change clients and service providers' privileges by issuing or revoking, upon request, digital certificates that are not only meant for identification purposes, but for refining access-control. We denoted this family of certificates as credentials because they provide restrictions and grant access to network services.

In addition, *RS* may renew certificates and distribute and renew shared secrets among devices that belong to the secure ad hoc network (*virtual domain*).

RS also track the behavior of clients and service providers through security events, which are reports of network offenses, perpetrated by clients or service providers against their peers. Security events may also report nice and good behavior and *RS* translate these events in changes in trust information regarding one entity. Moreover, the starting point of a new secure ad hoc network is a *RS* with a self-signed digital certificate. Furthermore, a *RS* with a self-signed digital certificate can issue certificates to other entities, which could join the secure network, and even to other *RS*, which hold a certificate issued by the first *RS* that allows them to also issue certificates. Other entities can only join a secure network through an interaction with a *RS*. A device may host several services and clients.

5.2 Entity Status

Service providers and clients are classified according to their current entity status:

- Anonymous guests or;
- Identified guests or;
- Permanent entities.

Permanent entities have long-term privileges, which are set during an initial configuration process.

Guest entities are capable of starting a communication channel and use services, but they have few privileges and rights. Identified guest have short-term rights and must be submitted to a registration process. Anonymous guests are users that had not gone through to a registration process and, hence, cannot be identified. In addition, anonymous guests can use only public services.

An initial configuration process sets the entity status and also its privileges. The initial configuration process runs only in *RS*. This process is manual, giving to the network owner

total control over user rights. The initial configuration process is also used to register incoming devices and grant service credentials, providing a better control over the secure ad hoc network. The spread of the configuration data over the network occurs naturally, without any user intervention (details are provided on Section 6).

5.3 Trust Information and the Network Perception

When service providers or clients join a secure ad hoc network, they receive a certificate from a *RS*. A digital certificate received from a *RS* carries more information than a regular certificate (i. e., version, serial number, issuer, expiration date, etc.). It also has a trust value that tells the maximum trust that this entity bearing the certificate in question will have.

As previously and briefly stated in Section 5.1, trust information is important since it works as a service access control parameter, granting or denying network rights for services.

Moreover, trust information translates the *network perception* about one entity. *Network perception* can be understood as a network's common intelligence regarding one entity and it is determined by its behavior towards the rest of the network in terms of security. *RS* are responsible to translate entities behavior in new trust values and also to distribute the new trust information among the network entities.

Therefore, trust regarding one entity may rise or decrease according to its behavior. If a client commits a fault against a network print service for instance (e. g., printing 50,000 high-quality copies of a book — a DoS attack), its trust value may fall. Entities behavior must be reported to a *RS* in order to have their behavior translated into new trust values.

However, in ad hoc network environments, it is not possible to count on specific services to be available at all times, as they can be out of range or even turned off. In order to make our architecture compliant with ad hoc network characteristics without compromising security, two inner mechanisms were designed:

- A *local perception* on every entity, which is an instant reaction mechanism used as immediate response against attacks. It can deny the attacker access to local services as soon as the attack is identified;
- In order to report faults to *RS*, a *gossip mechanism* is used. The *gossip mechanism* works as follows: when an entity is attacked by another entity, it first tries to report the security event to an available *RS*, but, if none is present, it keeps the information regarding the fault and waits a *RS* to be in radio range (if no ad hoc routing protocol is running). Once a *RS* is available in the network neighborhood, the entity sends, or gossips, as we prefer, all stored data regarding network security attacks to the *RS*.

To build the *network perception*, fault reports must be consolidated in order to obtain the current picture of the network trust information. However, if a secure ad hoc network

has two or more *RS*, each *RS* will hold a small piece of the actual network perception. Merging trust information from different *RS* demands synchronization.

RS keep a list of all received security reports. Before synchronization, each *RS* stamps its lists with a version number and its name (e. g., RS^A). When two *RS* meet, they do not only exchange their own report lists, but also verify if one of them has a more recent report from other *RS* that are not currently available in the ad hoc network.

Synchronizing trust information periodically or when a considerable amount of reports is available causes an obvious delay in the *network perception* consolidation process. On the other hand, synchronization every time a new trust report is received can significantly impact the network traffic and cause a waste of battery resources from *RS*. However, in ad hoc network environments, it is not guaranteed that all *RS* of a given *domain* are available at all times. Therefore, report synchronization among *RS* can be delayed or occur not simultaneously among all *RS* (if more than two *RS* exist) what implies having *RS* with different *network perceptions* at the same time.

For instance: if three *RS* exist in a given domain (RS^A, RS^B and RS^C) but only two of them (RS^A and RS^B) are available during synchronization time, these two *RS* exchange their most recent report lists and verify if any of them has a newer version of RS^C's list. If RS^B leaves the ad hoc network and RS^C arrives, RS^A and RS^C can synchronize their lists and, moreover, RS^C will also get an updated version of RS^B report list, as RS^A had obtained this before directly from RS^B. Notice that the *network perception* of all three *RS* is not the same at any moment in this example. In fact, in real ad hoc networks, network perception will hardly be the same in all *RS* as mobile nodes can leave and join the ad hoc network at anytime. And if *RS* are never available at the same time, *RS* may demand that entities with enough memory and processing resources to store a local version of its trust report table, in order to increase the probability of this report list to reach another *RS*. Meanwhile, *RS* will carry its own network perception. This mechanism is only turned on by one *RS* if it considers that trust reports from other *RS* are outdated.

This natural latency in the propagation of trust reports is the trade-off between having an instantaneous picture of the *network perception* and mobility in the trust based security architecture proposed in this paper. However, if the achievement of a unique network perception is hard to obtain, *local perception* is used to thwart attacks and protect a device even if the available network perception is not up to date.

5.4 Trust Information and Certificate Revocation List

Modifications in trust information are published by *RS* using the Trust Information and Certificate Revocation List (*TICRL*), which is an extension of a regular Certificate Revocation List (CRL) from PKI. Besides adding trust information, *TICRL* also supports three more additional states besides the CRL revoked state. *TICRL* lists:

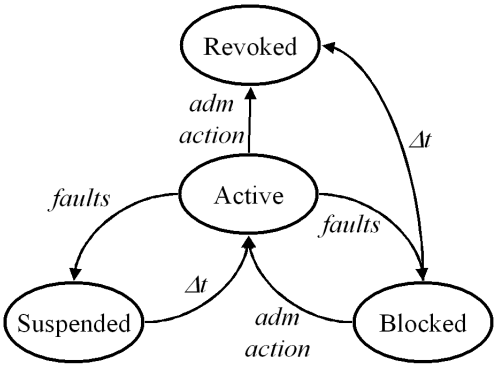

Figure 2: Life cycle of a digital certificate in the proposed security model.

- Active entities are all entities that had any change in its trust information.
- Suspended entities are entities that had a sudden loss of trust in a short period of time and, therefore had all their rights suspended for a determined period of time.
- Blocked entities are entities whose rights were suspended for an undetermined period of time. Only the network owner or one user with administrative rights can unblock an entity.
- Revoked entities are entities whose certificates were revoked. The network perception regarding any entity whose certificate is revoked is of full distrust.

This new form of handle certificate status establishes an extended model for digital certificates life cycle. Figure 2 presents this life cycle.

6 Roadmap to Secure Ad Hoc Networks

In this section we present a step-by-step roadmap on how to secure an ad hoc network with the proposed trust-based security architecture. In Section 6.1 we show how a secure network starts from a *RS*. Section 6.2 presents how a client uses a service and how a report is sent to a *RS*. Finally, in Section 6.3, we show how the *TICRL* are updated.

6.1 Step by Step: Building a Secure Ad Hoc Network

To start a secure ad hoc network, human interference is needed. First, a suitable device with a friendly-user interface must be selected to run a *RS* by the human owner of the

network. After the *RS* application has been started, this primal *RS* self-signs its digital certificate, thus creating a new secure ad hoc network, or *domain*, and produces a long random number that will be used to secretly identify all network entities that belong to its *domain*. After that, the network owner pre-registers in the *RS* all devices that he / she wants to belong to the secure network (e. g., notebooks, palm devices, etc.). All devices that join a domain have an entity status, alias and initial authentication method (which might be a biometric scheme, a weak password or both). The network owner may also add new *RS* to the *domain*. This phase is called *initialization phase*.

For devices with no user input interface, a Bluetooth like approach is recommended (i. e., stamping a random factory short-length code in the device chassis for initial authentication purposes).

When an entity requests to join the domain, the *RS* asks for the tuple "*alias, authentication data*", and if it is correctly provided, the *RS* signs the device's public certificate and sends it along with the random number that identifies the domain back to the requesting entity. This phase is called *joining phase*.

The *initialization phase* is the only operational phase that requires manual intervention or administrative work. In fact, the need of a manual system bootstrapping is the reason of limiting the scope of this security architecture to small and medium sized mobile ad hoc networks, as it is clear that during regular operation the proposed architecture is also suitable to large mobile ad hoc networks.

The public certificate and the random number are both ciphered before being transmitted. The symmetric cipher key is derived from the authentication protocol.

The distribution of digital certificate distribution can also be performed using a secure side-channel, as presented in [15] and [13]. This method requires both devices to be at zero-hop distance. The proposed security architecture applies a simple approach that can be executed at any distance, ciphering the public key of the requesting entity using data derived from the authentication protocol as symmetric key (see more on Section 7).

The initial trust value is defined according to the initial authentication method and the entity status. A permanent entity receives a greater trust value if it was initially authenticated using a biometric method plus a password than another one using only a password as authentication method, for instance. And guest entities always receive a lesser trust value than a permanent entity. A trust-based certificate is shown in Figure 3.

The trust information is a composition of three complementary percentages: trust, distrust and unknown factor. Trust and distrust definitions are straightforward. Unknown factor represents the lack of previous behavior knowledge about a single entity.

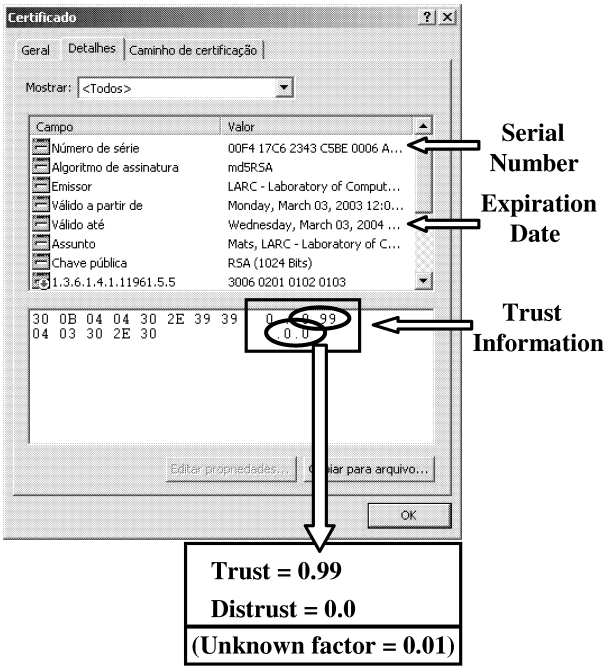

Figure 3: A digital certificate with embedded trust information (initial trust value of 0.99).

6.2 Step by Step: Using a Network Service

After issuing trust-based digital certificates to entities, the network is now able to start offering services over a secure application framework. When a Client (C) wants to use a service, it sets a secure communication with a Lookup Service (*LS*) and requests a network service (e. g., printing), which is provided by a Service Provider (P).

LS keeps a list of all P available in the domain and verifies if the requested P (e. g., P_1) is currently available. If P_1 is available, *LS* sends P_1 address to the requesting client (C_1). Client C_1 establishes a secure communication with service provider P_1, which verifies if C_1 has enough trust to use the requested service and if it has all the needed credentials (if any is needed).

P_1 may also look for an available Registration Service (*RS*) to get the current *network perception* about C_1. The same procedure is followed by C_1 regarding P_1 status. If C_1 and P_1 requirements are both fulfilled, a secure channel is established between them and the service is provided, otherwise communication ends.

If a security attack is detected by either C_1 or P_1, a security report regarding the offender is generated by the offended entity. The offended entity queries *LS* for an available *RS*. If

an *RS* is available at that moment, the security fault is reported; otherwise it is stored and kept until a *RS* becomes available.

Security events are classified in six categories (we understand that six levels of security events offer good granularity and simplicity at the same time):

- Three regarding network offenses (incidents), from critical to light offenses;
- Three regarding nice network behavior (e. g., absence of security faults in a given period of time, extreme security awareness, etc.).

As definition of a security event may change from entity to entity, they are full responsible for classifying network offenses and delights according to the proposed six-level classification.

6.3 Step by Step: Updating Trust Tables

Once a security event is reported to a Registration Service (*RS*), it add it to its Trust Event List (*TEL*), which contains the history of all reported events, and calculates the new trust value for a given device.

If multiple *RS* exist, each *RS* builds one *TICRL* regarding only certificates issued by it. Therefore, if RS^A issued certificates for entities C^{A1}, P^{A1} and P^{A2}, it will only build a *TICRL* regarding these three entities.

However, RS^A may store security events regarding entities with certificates issued by RS^B in its *TEL*. RS^A and RS^B have to synchronize their *TEL* in order to build a unique *TICRL* that can offer a true picture of the current *network perception*.

Figure 4 shows the workflow of trust updating through an example. It starts with a Client requesting a service to a Service Provider, which verifies the Client's access rights, and sends a trust report to the *RS*. The workflow ends with the update of the *TICRL* in the *RS*. Figure 5 illustrates a *TICRL* of a single *domain* with three *RS* (RS^A, RS^B and RS^C).

7 Security Mechanisms

The security mechanisms, used to secure an ad hoc network running over the application framework of the proposed trust-based security architecture for small and medium sized ad hoc networks, are:

- Shared-secret network authentication followed by the establishment of a TLS secure channel and;
- Access-control based on trust information.

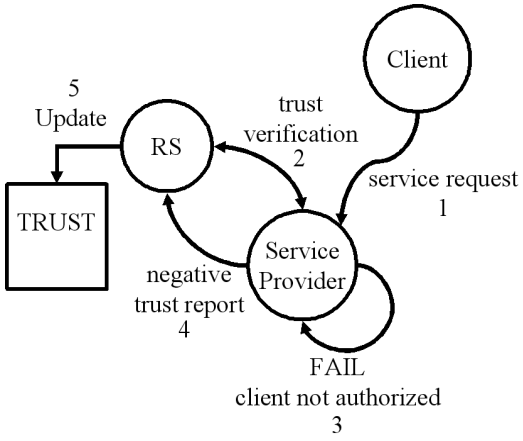

Figure 4: A trust update is represented here. First, a Client requests a service to a Service Provider (1). The Service Provider verifies if Client has enough rights for the requested service consulting a locally stored copy of *TICRL* or requesting it to an available *RS* (2). If the trust associated to the Client is not enough (3), a negative trust report is sent to an available *RS* (4). The *RS* updates its report list and the *TICRL*.

The shared-secret network authentication uses the mechanism described in [9], and it aims to recognize if the communicating parties belong to the same *domain*. Furthermore, this shared-secret network authentication can attenuate battery exhaustion attack attempts, as it is based on a lightweight protocol and occurs before any high power-demanding algorithm, as asymmetric key ciphers.

The network authentication sets a secure tunnel between two entities (that only know that the other communicating party belongs to a known *domain*).

Inside this secure tunnel, a TLS authentication is started, with the certificates travelling ciphered inside the established channel. Therefore, each party can identify its peer univocally, but their identities travel protected from eavesdroppers. In addition, a TLS tunnel is established between the peers and the original channel set using the network authentication mechanism is then abandoned. The service is then requested and provided inside a secure TLS tunnel.

8 Application Framework

The application framework is a software infrastructure designed to provide a platform for implementing new applications over a secure environment.

RS#	Certificate#	State	Trust
RS^A	C^{A1}	**Active**	(%,%)
	C^{A2}	**Suspended**	(%,%)
	P^{A4}	**Active**	(%,%)
	P^{A7}	**Active**	(%,%)
RS^B	C^{B2}	**Blocked**	(%,%)
	P^{B3}	**Revoked**	-
	SL^{B1}	**Blocked**	(%,%)
RS^C	C^{C1}	**Active**	(%,%)
	C^{C2}	**Suspended**	(%,%)
	C^{P3}	**Revoked**	-

Figure 5: *TICRL* translates the network perception of a domain with three *RS*.

It was fully designed in Java in order to be platform independent. The application framework implements the security architecture and its components. It also provides an application program interface (API) for designing network clients (C) and service providers (P) over a secure infrastructure. Figure 6 illustrates the application framework layers. A brief description of the framework layers and its functionalities is presented next:

- A Communication Layer that is used to set TCP connections between mobile devices.
- A Security Mechanism Layer, composed by two sub layers. A network authentication sub layer, which verifies if a communicating party belongs to a known *domain*; and a TLS layer used to exchange digital certificates and establish a secure tunnel.
- A Trust Layer that verifies the trust information regarding a digital certificate. It calculates new trust values from network events (when needed) and also queries the *RS* for the current *network perception*.
- Application Support Layer that has infrastructure for basic network services (*RS* and *LS*) to run and also for network clients and service providers' design. The application program interface (API) for the development of new applications is located over the client and service provider sub layers.

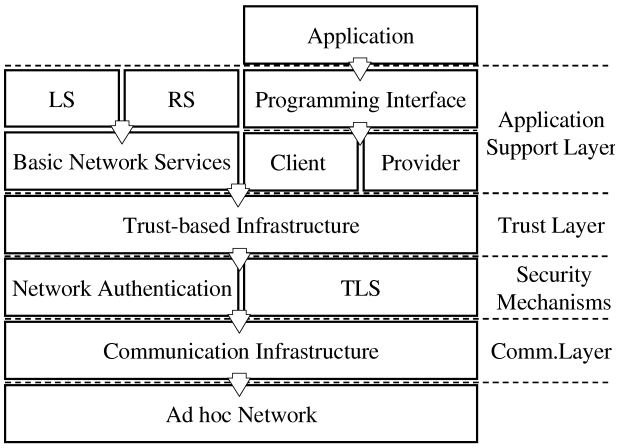

Figure 6: The application frameworks and its several layers.

9 Application Prototypes

Two prototypes were designed to test our application framework usability:

- A digital signer of electronic files. It is composed by a client that requests files to be signed; a signer that receives files, evaluate the network perception of clients, check credentials and enable files to be signed. Signing is only done after approval of the signer owner and a verifier that checks the signature authenticity.

- A secure slideshow that multicasts slides to entities that belong to the same secure ad hoc network. It was designed to be used for education support, in classrooms or meetings rooms.

The implementation of the digital signer was done just after the application framework was developed. It was designed and programmed by the same developing team as the first test of the application framework.

In this prototype, were considered faulty behaviors actions like: clients sending virus infected documents to the digital signer application and non-authorized service requests (i. e., not enough trust). A single programmer developed the second prototype in a two-month period and with almost no assistance. This prototype was built to evaluate the usability of the application framework. Results were encouraging for a two-month period, as the developer had very little experience on Java programming at that date.

In this prototype, insufficient rights to request access to the secure slideshow content were faulty behaviors. From the client point of view, a secure slideshow server could

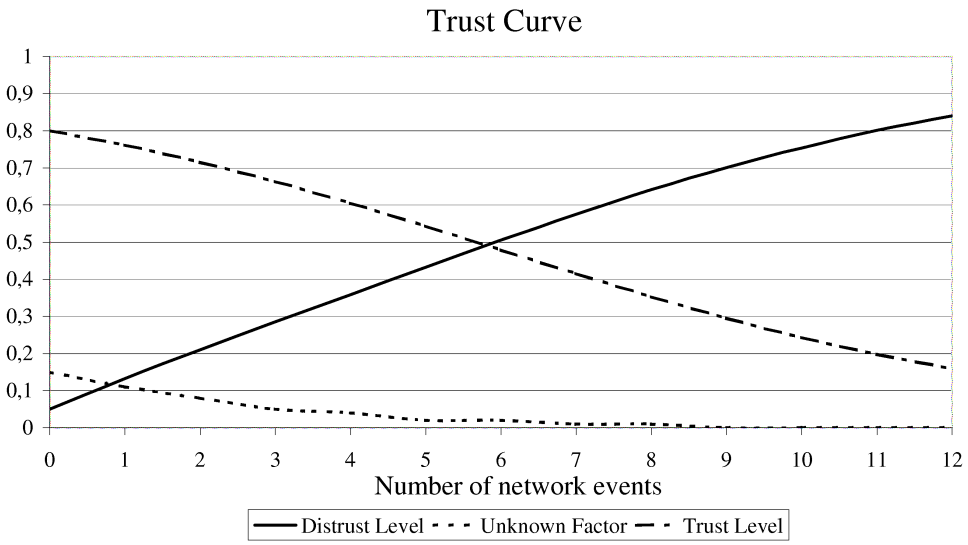

Figure 7: Example of the trust information fluctuation of an offender network user.

present a fault behavior if the announced content did not correspond to the real broadcasted content. In this case, faults were not automatic detected, and user intervention was needed.

Regarding security, both applications performed well. We forced one client to commit several faults, and then checked the client's network perception. Reports were sent from services to *RS* through the gossip mechanism.

The fluctuation of the trust information of this user is presenter in Figure 7. The initial trust value assigned to this device was 0.8 for trust level, 0.15 for unknown factor and 0.05 for distrust level.

After six network offenses (incidents), the trust level and the distrust level are approximately 0.5 each. And after ten incidents the trust level was 0.25 and the distrust level was of 0.75. The unknown factor naturally tends to zero, as more information is obtained about the entity's behavior in the secure network.

In this example, we artificially suppressed the suspended and blocked states of the *RS*, as it would first suspend and then block offender network user before the trust information reaches such low levels, as 0.16, after twelve incidents (or before the distrust level reaches 0.84, after the same twelve network offenses).

10 Conclusion and Summary

In this paper we introduced and described a trust-based security architecture for small and medium sized mobile ad hoc networks. Albeit we have limited the scope of our proposal to small and medium sized mobile ad hoc networks, the proposed security architecture can clearly be applied to larger ad hoc networks with several active *RS* during operation mode. We have limited our scope mainly because system bootstrapping is a manual activity. Therefore, for large ad hoc networks, an initial configuration effort equivalent to the ad hoc network size is needed.

The proposed security architecture is also suitable for ad hoc network characteristics, such as mobility, lack of network borders, dynamic topology changing, etc. (see more in Section 1).

Node mobility mainly impact report synchronization among *RS*, but, as shown, regular entities can be used to propagate report lists among *RS*. Even though latency exists in the consolidation of the *network perception*, a protection mechanism, the *local perception* can be used to protect entities under attack. Other effects of mobility and dynamic topology do not affect security, but only regular usage of network services (e. g., if a client looks for a non-available service, no service can be provided). Regarding the lack of network borders, virtual borders are defined using *domains* as a first stronghold to protect entities against attackers.

Summarizing, first we surveyed the security threats in ad hoc networks, classifying them according to the security taxonomy presented in [14] and focusing on the aspects regarding wireless networks. In addition, we provided the state of art of context based ad hoc networks, listing the most relevant papers in ad hoc network security field, concerning the scope of this work, and their application context.

Furthermore, we have presented and described a trust-based security architecture for small and medium-sized ad hoc networks, which assumes a service-oriented, Jini-like, network environment. We have assumed four basic kind network entities: clients, specific service providers, directory or lookup services and registration services, which extend the certification authority (CA) concept from PKI, as trust information and credentials are added to service access-control. Every entity must belong to one or more secure ad hoc networks (e. g., home network and / or office network, for instance), which is denoted *domain*.

In addition, *RS* track entities behavior using a *gossip mechanism*, where entities report secure events (offenses and also nice network behavior) regarding other network entities. The *RS* then analyze all received security events and reduce or restore entities trust values. Trust information is published in *TICRL* and it reflects the *network perception*. In fact, *TICRL* extends the PKI model, with new states besides the *revoked*, they are: *active*, but with trust loss; *blocked*; and *suspended*. We have also shown how the trust information lists are synchronized among several *RS* in ad hoc environments.

In fact, mobility related characteristics, like leave and join operations, affect the pro-

posed security architecture in trust synchronization only, as it is not possible to guarantee that the network perception of all existing *RS* is the same at all times. Other network entities (*LS*, *P* and *C*) are immune to mobility related characteristics in terms of security. The only effect over those entities is that they will not be able to report faults or nice behavior to the *RS*. Other issues non-related to security are common to any ad hoc environment, such as a client not finding a specific service in the ad hoc network.

The proposed security architecture relies on standard authentication and cryptographic algorithms, such as TLS, and non-standard security mechanisms, such as group authentication (see [9]). We have also briefly described the application framework that was designed after the proposed security mechanism, and also two prototypes that were built over this framework. Finally, as we have observed running the prototypes, the proposed security architecture prevents active attacks against mobile ad hoc networks. We believe the great majority of future ad hoc networks will be of small and medium-sized networks, what makes our solution a very comprehensive one, but we have also shown that the limitation of scope is only due to the manual system bootstrapping needed during *initialization phase*.

Future Work

In the near future we intend to provide a detailed performance evaluation of the trust-based security architecture, including its operational costs and timings. Furthermore, we will also provide other project results, such as results regarding power consumption gains obtained group authentication in hostile environments and others regarding cryptographic performance of the cipher sets applied and also about trust management.

Acknowledgments

We are thankful to our colleagues Armin Mittelsdorf, Fernando Redigolo, Cesar Rossi, Fabio Taroda and Rony Sakuragui for their invaluable contributions to this work. We also thank Mats Näslund and András Mehes for useful comments and discussions and Frank Bodinaud for testing the application framework.

References

[1] Ken Arnold, Bryan O'Sullivan, Robert Scheifler, Jim Waldo, and Ann Wollrath. *The Jini^{TM} Specification*. Addison-Wesley, Reading, MA, USA, 1999.

[2] Nadarajah Asokan and Philip Ginzboorg. Key-agreement in ad hoc networks. *Computer Communications*, 23(17):1627–1637, 2000.

[3] Nadarajah Asokan, Valtteri Niemi, and Kaisa Nyberg. Man-in-the-Middle in Tunneled Authentication Protocols. Technical Report 2002/163, IACR ePrint Archive, Oct 2002. See http://eprint.iacr.org/2002/163/.

[4] Nikita Borisov, Ian Goldberg, and David Wagner. Intercepting Mobile Communications: The Insecurity of 802.11. In *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking (MOBICOM-01)*, pages 180–189, New York, NY, USA, 16–21 Jul 2001. ACM Press.

[5] Catharina Candolin and Hannu Kari. A Security Architecture for Wireless Ad Hoc Networks. In *Proceedings of the Military Communications Conference (MILCOM 2002)*, volume 2, pages 1095–1100, 7–10 Oct 2002.

[6] Laura Marie Feeney, Bengt Ahlgren, and Assar Westerlund. Spontaneous Network: an Application Oriented Approach to Ad Hoc Networking. *IEEE Communications Magazine*, 39:176–181, Jun 2001.

[7] Jean-Pierre Hubaux, Levente Buttyán, and Srdjan Čapkun. The Quest for Security in Mobile Ad Hoc Networks. In *Proceedings of the 2th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC'01)*, pages 146–155, New York, NY, USA, 4–5 Oct 2001. ACM Press.

[8] Haiyun Luo, Petros Zefros, Jiejun Kong, Songwu Lu, and Lixia Zhang. Self-securing Ad Hoc Wireless Networks. In *Proceedings of the 7th IEEE Symposium on Computers and Communications (ISCC 2002)*, pages 567–574, 1–4 Jul 2002.

[9] Leonardo A. Martucci, Tereza Cristina M. B. Carvalho, and Wilson V. Ruggiero. Domínios virtuais para redes móveis ad hoc. In *Proceedings of the 21st Brazilian Symposium on Computer Networks (SBRC 2003)*, pages 599–614, Natal, RN, Brazil, 19–23 May 2003.

[10] Leonardo A. Martucci, Tereza Cristina M. B. Carvalho, and Wilson V. Ruggiero. A lightweight distributed group authentication mechanism. In Steven M. Furnell and Paul S. Downland, editors, *Proceedings of the 4th International Network Conference (INC 2004)*, pages 393–400, Plymouth, Devon, UK, 6–9 Jul 2004.

[11] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Inc., Boca Raton, FL, USA, 1996.

[12] Frank Stajano. The Resurrecting Duckling: What Next? In *Revised Papers from the 8th International Workshop on Security Protocols*, volume 2133 of *Lecture Notes in Computer Science*, pages 204–214, London, UK, 3–5 Apr 2001. Springer.

[13] Frank Stajano and Ross Anderson. The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks. In *Proceedings of the 3rd AT&T Software Symposium*, Oct 1999.

[14] William Stallings. *Cryptography and Network Security: Principles and Practices*. Prentice Hall, Upper Saddle River, NJ, USA, second edition, 1998.

[15] Srdjan Čapkun, Jean-Pierre Hubaux, and Levente Buttyán. Mobility Helps Security in Ad Hoc Networks. In *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC'03)*, pages 46–56, New York, NY, USA, 1–3 Jun 2003. ACM Press.

[16] Yeda R. Venturini, Christiane M. Schweitzer, Leonardo A. Martucci, Fernando F. Redigolo, Armin W. Mittelsdorf, Wilson V. Ruggiero, and Tereza Cristina M. B. Carvalho. Security model for ad hoc networks. In *Proceedings of the International Conference on Wireless Networks (ICWN 2002)*, pages 185–191, Las Vegas, NV, USA, 24–27 Jun 2002.

[17] Duncan J. Watts. *Small Words: the Dynamics of Networks between Order and Randomness*. Princeton University Press, Princeton, NJ, USA, 1999.

[18] Lidong Zhou and Zygmunt J. Haas. Securing Ad Hoc Networks. *IEEE Network*, 13(6):24–30, 1999.

Paper III [redacted]

A Lightweight Distributed Group Authentication Mechanism

Reprinted from

Proceedings of the 4th International Network Conference (INC 2004)
Plymouth, Devon, United Kingdom, 6–9 Jul 2004

A Lightweight Distributed Group Authentication Mechanism

Leonardo A. Martucci,
Tereza Cristina M. B. Carvalho, Wilson V. Ruggiero
leonardo.martucci@kau.se, {carvalho, wilson}@larc.usp.br

Abstract

Identifying trustable devices and establishing secure tunnels between them in ad hoc network environments is a difficult task because it has to be quick, inexpensive and secure. Certificate-based authentication mechanisms are too expensive for small devices. The use of such mechanisms must be controlled and reserved for special situations, (e. g., banking applications) but not for everyday transactions. In addition, indiscriminate use of asymmetric ciphering and certificate-based authentication is a shortcut to battery exhaustion attacks. This paper describes a lightweight distributed group authentication mechanism suitable for ad hoc network devices requirements. We introduce the concept of group authentication, the target of which is not the individual identification of devices, but to verify if a device belongs or does not belong to a trusted group. The proposed mechanism verifies if devices have a pre-shared secret and sets new cipher keys each time it runs. This mechanism requires loose synchronization among the devices' real time clocks to thwart replay attacks. It also mitigates the effects of battery exhaustion attacks due to its lightness.

1 Introduction

Securing ad hoc mobile environments is not easy to be achieved in a quick, inexpensive and secure way. Security cannot rely on central servers, as there are no guarantees that they will be in radio range all times — devices' availability and motion are quite unpredictable in mobile ad hoc networks. Besides, complex configurations must be discarded, as target users of mobile ad hoc applications are the common audience and not security specialists.

In this paper, we propose a simple, but efficient, lightweight distributed group authentication mechanism that can be applied to the following scenario: a set of devices that belong to a single administration authority, such as a single user, a group (e. g., a family) or an enterprise that needs to exchange or synchronize data among devices, with or without the users' concern. In this paper, each set of devices is called *security cluster*. Each security cluster is composed of trusted devices that can recognize participants of known

clusters through a mechanism called *group authentication*. While an individual authentication mechanism tries to identify devices and/or users univocally, group authentication only checks if two devices belong to a same (i. e., trusted) group. It is based on pre-shared secrets, which are distributed among devices of a security cluster (how this is achieved exactly is out of the scope of this paper).

Group authentication may be the only authentication mechanism available, but if a pre-shared secret is exposed in a single device, the whole group is compromised, as the secret is common to the entire group. Group authentication can also precede individual authentication, in order to increase security, save power and even protect users' identities, as shown in this paper.

The idea behind the proposed mechanism is straightforward and intuitive enough even for those not familiar with network security. It is extremely powerful as it can set strong short-term symmetric keys, which are never transmitted over-the-air, between devices. In addition, it is also completely transparent to the end-user. The lightweight distributed group authentication can be applied to ad hoc and non ad hoc networks, but its advantages are noticed on low-resource distributed computer environments.

The proposed distributed authentication mechanism can be applied at any OSI layer (from data link to application) and be bound to other authentication mechanisms, such as certificate based ones. Nevertheless, for specific cases group authentication may be enough (e. g., devices hosting non-critical services, with low processing power or scarce battery resources). However, individual authentication may be necessary for devices hosting sensitive services and/or data. In these cases, the proposed mechanism can drastically reduce the number of unsuccessful authentication attempts using digital certificates and asymmetric keys, saving precious battery power.

This paper is organized as follows. In Section 2, we present the architecture of the distributed group authentication mechanism preceded by a detailed description of how it works and sets new secret keys between devices. Section 3 evaluates the mechanism's security and its lightness compared to other mechanisms. Section 4 gives a survey to the related work, presenting some security mechanisms based on the same assumptions as this. Finally, conclusions are presented in Section 5.

2 Lightweight Distributed Group Authentication Mechanism

Ad hoc networks' future environments (e. g., pervasive computing, sensor networks, etc.) rely on devices with major constraints regarding battery resources, processing power and available bandwidth. Thereupon, security mechanisms suitable for those devices are utterly important, as the establishment of a secure communication channel with a resource-expensive mechanism can lead to a successful battery exhaustion attack [9].

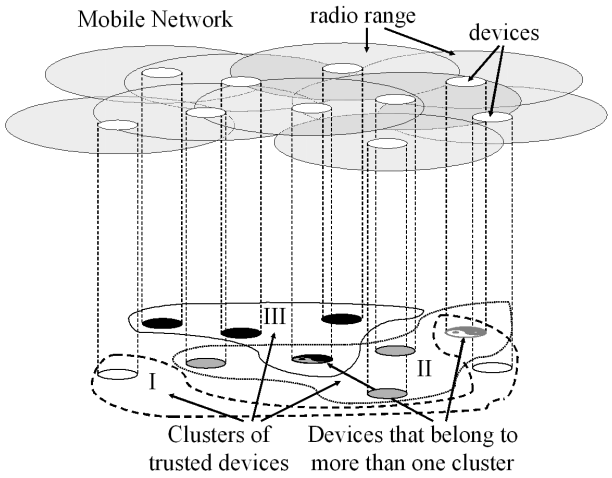

Figure 1: The ad hoc network universe divided in several clusters of trusted devices.

Before describing the proposed mechanism itself, we need to share our foresight of how ad hoc networks will be deployed in short and medium terms, as it will clarify the understanding and the meaning of this mechanism. From our point of view, the great majority of ad hoc networks will be of networks whose devices have something in common, such as their ownerships (e. g., an enterprise, a family, etc.) or placement (e. g., a meeting room, a house or even the streets).

This presumption is reasonable, as several security mechanisms designed for ad hoc networks share this same foresight. In addition, we assume that it is possible to divide the whole ad hoc universe in small clusters of trusted devices (a similar approach can be found in [10]). Furthermore, we assume that it is possible to set a pre-shared key among participant of a security cluster. Naturally, these clusters will overlap, as one device may belong to one or more groups. Figure 1 illustrates a mobile network, composed by several mobile devices divided in three security clusters (I, II and III).

The conclusion seems to be simple: if it is possible to set a pre-shared secret among devices that belong to a same security cluster, it is also possible to set secure sessions among them. However, important issues are concealed and have no easy answers: How are secure sessions going to be established? Is the lightweight distributed group authentication mechanism suitable? And why? This section attempts to provide answers to these questions.

2.1 Authenticating Devices

In a few words, our distributed group authentication mechanism could be described as follows. First, the pre-shared secret k, which was previously set among devices belonging to one security cluster, is used as key input of a secure hash function (HMAC) with the current local time value, t_1, as data input. The output of the HMAC function, called 1^{st} nonce, is divided in three equal parts (a, b, c). After that, the timestamp t_1 and first part a are transmitted in a challenge message. A *nonce* can be set from one or more runs of the HMAC function. This initial step is illustrated below:

$$H_k(t_1) = 1^{st}nonce = (a, b, c) \Rightarrow challengeMessage = (a, t_1) \quad (1)$$

How exactly and to which devices in the ad hoc network this information will be transmitted depends on which OSI layer the mechanism was implemented. On layers 2 and 3, for instance, broadcasting is the best option, but if implemented in layers 4 to 7, a TCP connection should be established before any data can be exchanged (see also Section 3). After having receiving the challenge message, any other device from the same security cluster (shared-secret key k is known) is able to reproduce the 1^{st} nonce using timestamp t_1, and to recognize the slice a of the received challenge message as valid. Every device that receives and recognizes a challenge message generates a 2^{nd} nonce, using the shared-secret k as key input of the HMAC function and a second timestamp t_2 as data input. The 2^{nd} nonce is divided in three parts (x, y, z). The slice z is set as symmetric cipher key and is used to establish a cryptographic tunnel between the devices. Response message is then assembled with x and b and ciphered with z. Notice that the symmetric cipher key z was generated in run-time. The timestamp t_2 is also added to the message. This response message is sent back to the first device. Notice that only peer-to-peer (and no multiparty) authentication exists, as different t_2 are expected from different devices. This sequence is presented below:

$$H_k(t_2) = 2^{nd}nonce = (x, y, z) \Rightarrow responseMessage = (E_z[x, b], t_2) \quad (2)$$

The first device can reproduce the 2^{nd} *nonce* from the received timestamp t_2 and generate the symmetric key z. After that, it must decipher the message payload and check its contents, x and b. It then assembles the last message of our authentication mechanism. The *last* message contents are c and y, both ciphered using z as symmetric key.

$$responseMessageRecognized \Rightarrow lastMessage = (E_z[y, c]) \quad (3)$$

The *last* message is used for confirmation purposes. After receiving the *last* message, the second device is sure that the first device really knows the symmetric key z and, hence, y and k. When this protocol ends, two devices from a same security cluster can securely exchange data using z as temporary symmetric cipher key. The protocol described above can also be restarted at any moment in order to re-authenticate both ends and set a new, fresh temporary cipher key z', which is also never transmitted over-the-air and with only two HMAC additional runs. A deeper evaluation of the mechanism from the security point of view is provided in Section 3.

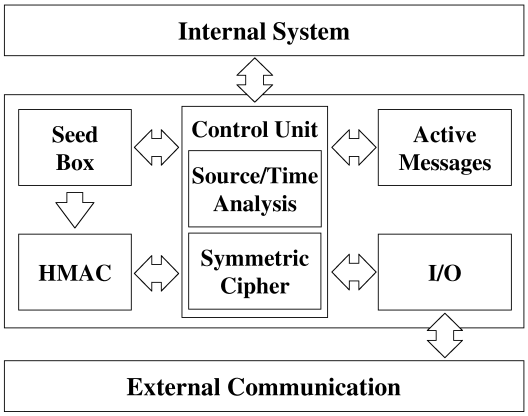

Figure 2: The architecture of the lightweight distributed authentication mechanism.

2.2 The System Architecture

The proposed mechanism should be placed between the internal system (e. g., software application) and the external communication (e. g., wireless interfaces), as a security middleware (see Section 2.4). Figure 2 shows the architecture of the proposed mechanism and its internal building blocks.

HMAC is a suitable sequence generator for our mechanism, as its inputs are: a secret key and a data input (timestamps in our case). Moreover, it has a 160-bit long hash value output (with SHA-1 as embedded hash function). The two basic requirements for sequence generator candidates were:

- It must be cryptographic secure, or polynomial-time unpredictable.
- It must accept an arbitrary value as input parameter (the timestamp).

The *Seed Box* is a storage unit responsible to hold all known pre-shared keys k_n, where each k_n corresponds to one different secure cluster. Each k_n receives a mnemonic name, assigned by the device's owner, to be easily associated to a secure cluster.

The I/O is the building block responsible for the communication of the mechanism with the network communication interfaces (the layer just below the mechanism).

The *Control Unit* has four functions: the first is to be an interface between the mechanism itself and applications from upper levels; the second regards re-keying; and the last two are directly related with security: source address and timestamp verification and message ciphering. Messages are only considered valid if their timestamps values are within the lower and upper bounds of a *time window* set around the device's current time given by its real time clock.

The *Active Messages* is a storage unit responsible to store all valid sent messages, the timestamps and *nonces*. This block is particularly useful to prevent message fabrication attacks (see in Section 3). Every message sent is considered valid if it is not expired. Expiration is determined by messages' timestamps. *Active Messages* storage blocks also checks if timestamp information is used more than once and discards messages with repeated timestamps, in order to increase security.

2.3 Loose Synchronization among Devices and Modular Security

Devices belonging to the same security cluster must have their clocks loose synchronized; otherwise their peers may discard authentic challenge messages if the message's timestamp is out of the bounds defined by the time window. Therefore, time windows should not be set too narrow if no time synchronization service is available in the network (e. g., a local NTP — Network Time Protocol — running for members of a security cluster only).

The design of our distributed group authentication mechanism is completely modular. Therefore, it can be associated with other security mechanisms. If individual authentication is mandatory, a certificate-based authentication can happen just after the setting of the secure tunnel between the devices that had already gone through the lightweight group authentication. This fact is particularly important when dealing with mobile devices, because their resources are often scarce and the indiscriminate use of expensive functions, as certificate-based authentication, must be reserved to very special situations or critical applications only.

2.4 Re-Authentication, Re-Keying and Implementation Layer

Any peer can request at anytime a renewal of the group authentication procedure to set a new symmetric cipher key z between the devices. The re-keying is transparent to upper layer applications and is made inside the secure tunnel already set, thus the re-keying procedure is concealed from outsiders (that are not aware of the re-keying procedure). In addition, re-authentication frequency is not fixed, and shall be agreed between communicating devices.

Group authentication mechanism can be implemented at any layer of the OSI protocol (from data link to application), but security aspects change regarding to the chosen OSI layer. For instance: a data link layer implementation can only offer data link security, what can be used to conceal the device's hardware address and, thus, prevent tracking. On the other hand, upper-TCP implementations offer end-to-end security and can be used to tie applications to security clusters, in order to increase control over applications network access.

3 Security Evaluation

In this section, we provide a security evaluation of the proposed distributed group authentication scheme using an attack-oriented approach. We also emphasize its lightness and estimate how much power can be saved by its deployment along with a certificate-based solution, instead of relying on certificate-based solution only. Theoretical attacks against our mechanism are performed to evaluate its efficiency to thwart them, protect devices and transmitted data.

The most relevant security attacks against our mechanism are: fabrication (including replay attack), man-in-the-middle (MitM) and brute-force attacks. All them proved infeasible against our mechanism. We had also implemented a prototype of the proposed mechanism using Java and 64-bit UTC (Universal Coordinated Time) timestamps. Our prototype runs over TCP and precedes a TLS procedure, allowing the certificates to be exchanged by the devices communicating inside a secure tunnel, protecting users' identities from potential attackers. The implementation is a peer-to-peer application, suitable for ad hoc networks.

3.1 Man-in-the-Middle (MitM) and Replay Attacks

A *man-in-the-middle* attack, or just MitM, happens when an attacker device E places itself in the middle of two legitimate devices A and B and masquerade as B to A and as A to B. Our proposed scheme thwarts MitM attacks as symmetric key k is set on both ends A and B and the rest of the communication between both ends is done inside a secure tunnel. Therefore, intermediary nodes only forward ciphered packets (with the very exception of *challenge* messages).

Replay attacks are a combination of two different network attacks: a passive attack (interception) and a fabrication attack. An attacker E can easily capture valid messages being exchanged between two devices, A and B, that belong to the same security cluster S, without being noticed. After that, E may try to reuse this information by sending it to a fourth device, C, that also belong to S. The protection against replay attacks is provided by the use of timestamps as HMAC data input. The *Control Unit* block ignores challenge messages with timestamps that were already used and the *Active Messages* block, in association with *Control Unit* block, prevents *response* or *last* messages to be received without being related with a *challenge* message. In addition, only messages with a valid timestamp (within device's time window) are accepted. Therefore, a captured *challenge* message have to be retransmitted before its validity expires, otherwise it is useless.

3.2 Brute-Force Attack

A brute force attack consists of trying every possible key until the right one is found. If an attacker captures a *challenge* message, it can produce and send multiple *response* messages

back to the originator. The lifetime of the *challenge* message is used to protect the device against this attack, as no response shall be expected to an expired message. Lifetime defines the period susceptible to brute-force attacks. The *Control Unit*'s source analysis tracks the source address of the incoming response messages and checks if multiple answers are coming from a single device (and, eventually, blocking messages arriving from it). Intercepted messages may also be submitted to a brute-force attack in order to obtain the shared-secret k. However, finding out a shared-secret key of 160 or 512-bit long is extremely expensive. If we assume that generating one *nonce* and comparing its first part with another part captured from a *challenge* message takes around 1000 cycles (950 cycles for SHA-1 [3] and 50 more for other digital operations needed), a state-of-art 3GHz microprocessor fully committed on finding a 160-bit long key k would take approximately $7.7 * 10^{33}$ years to find it out (assuming that the attacker discover k in $\frac{n}{2}$ attempt, where n is the maximum number of attempts). On the other hand, the effectiveness of a brute-force attack over the symmetric cipher key z depends on the length of z, and on the output length of HMAC.

3.3 Lightweight Power-Saving Mechanism

Lightness may sound a bit strange for a security evaluation section, although it is a fundamental security matter when we aim ad hoc network devices with low battery resources. Power saving is a need and the proposed mechanism spends it wisely. Small devices running applications that don't need individual authentication can establish secure tunnels without the need of asymmetric ciphers as new shared-key are set between devices with only two HMAC runs. However, if a service truly demands individual authentication, certificates are exchanged as soon as the secure tunnel is set. This procedure helps devices to save battery power, as a high percentage of arriving certificates are expected to be valid, as they already had gone through group authentication, mitigating battery exhaustion attacks effects.

4 Related Work

Our lightweight power-saving distributed group authentication mechanism is based on the association of shared-secret and a secure sequence generator that takes as input parameter public information (timestamp) and a secret. Authentication mechanisms that rely on the same assumptions and authentication systems for mobile communications are reviewed in this section.

SecurID authentication [1] is also based in a pseudo-random number generator and time information, although it is not a distributed solution, since it relies on a centralized authentication server. Moreover, SecurID uses tokens working as number generators, and passwords. SecurID and our mechanism goals are not the same, as SecurID pursues user authentication, while ours seeks group device authentication. Furthermore, our group

mechanism is transparent to end-users, and also sets a secure tunnel between devices.

The SIM (*Subscriber Identity Module*) is another authentication system, used in GSM mobile systems based on a one-way hash function module [8]. SIM relies on challenge-response procedures, with 128 bits keys, but only 32 bits of response. SIM is transparent to end-users and also lightweight, suitable for mobile devices, but it relies on centralized servers to verify incoming responses message.

IEEE 802.11 WEP is based on a PRNG that generate sequences to be used to cipher messages. However, the RC4 PRNG using a secret key of 40 bits is considered weak, and several attacks over WEP were published in the last few years [2], and even open-source tools to break it are freely available. The IEEE 802.11i next-generation security protocol for wireless networks being evaluated is the TKIP (*Temporary Key Integrity Protocol*) [4]. TKIP masks WEP weaknesses, encrypting data with secret keys of 128 bits, periodically renewing the symmetric cipher key and preventing IV (*Initialization Vector*) to be repeated with the same cipher key. However, the re-keying relies on an EAP-based server, a centralized device. Moreover, IEEE 802.11i CCMP (*Counter Mode with CBC-MAC Protocol*) proposal also has its key management relying on an EAP-based server. Therefore, none of these two IEEE 802.11i security proposals are suitable for an ad hoc network unless every device on the ad hoc network runs an EAP-based authentication server. Furthermore, the only EAP that meets all IEEE 802.11i requirements is the EAP-TLS, which works with digital certificates and asymmetric cryptography.

IKE with a pre-shared key [6] can also be used as pre-authentication mechanism. Its advantage is that no loose synchronization among devices real-time clock is needed. In addition, only three messages are needed with IKE authentication with pre-shared keys in aggressive mode (the same amount needed by the pre-authentication mechanism described previously). However, IKE with pre-shared keys has a major drawback that impacts power-consumption: messages can be replayed. Even though a replay attack will not succeed, as attackers do not have the pre-shared-key, replayed challenge messages are always replied, as there is no time information in the message payload. Therefore, a replayed challenge message will, initially, pass as authentic for the IKE Responder and will be replied, causing battery power to be spent (data transmission mode is the most expensive mode in terms of energy consumption [5]). In conclusion, it is not difficult to foresee that IKE authentication with pre-shared keys spends more battery power than the pre-authentication mechanism presented in the previous subsection when submitted to a battery-driven attack.

SKEME with a pre-shared-key [7] is also a candidate for pre-authentication mechanism. SKEME with a pre-shared key advantages are basically the same of IKE with a pre-shared key: real time synchronization among device's real time clock is not needed and only four messages are exchanged between mobile devices. However, its disadvantages are also the same as IKE with a pre-shared key: replayed messages will be answered, and battery power spent. The conclusion is exactly the same of IKE with pre-shared keys: it will spend more battery power than the pre-authentication mechanism presented in the previous subsection when submitted to a battery-driven attack.

5 Summary & Conclusions

In this paper, we have proposed an efficient lightweight distributed group authentication mechanism as a feasible solution to secure mobile ad hoc networks. We have shown how group authentication works and how it is implemented, assuming that it is possible to distribute a secret among trustable devices. We also have explained how a secure tunnel is set between each pair of mobile devices and how a symmetric cipher key is derived from an initial pre-shared secret. We also illustrated how we renewed the symmetric cipher key automatically in a distributed environment. We associated a name to each security cluster to make it intuitive and straightforward even for the common audience.

Group authentication provided by the proposed mechanism can be sufficient for almost every wireless device. Moreover, we believe that individual authentication is restricted to few applications, and the lightness provided by our mechanism when compared with certificate-based mechanisms, justifies its use as everyday solution for security. We have also illustrated how the proposed mechanism thwarts security attacks, such as MitM and replay attacks. On purpose, we have not selected a specific symmetric key cipher for the proposed mechanism, as we were aiming an open solution that works with any kind of mobile devices, even with legacy and simple devices with very few resources and computational power. We emphasize that the proposed mechanism is not only an ad hoc networks secure solution, and can be set on any kind of computer networks, offering a light and distributed security solution.

References

[1] RSA SecurID Authentication: a better value for a better ROI. Whitepaper, 1 Dec 2001.

[2] Nikita Borisov, Ian Goldberg, and David Wagner. Intercepting Mobile Communications: The Insecurity of 802.11. In *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking (MOBICOM-01)*, pages 180–189, New York, NY, USA, 16–21 Jul 2001. ACM Press.

[3] Antoon Bosselaers, René Govaerts, and Joos Vandewalle. Fast Hashing on the Pentium. In Neal Koblitz, editor, *CRYPTO'96: Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology*, volume 1109 of *Lecture Notes in Computer Science*, pages 298–312, London, UK, 18–22 Aug 1996. Springer-Verlag.

[4] Nancy Cam-Winget, Tim Moore, Dorothy Stanley, and Jesse Walker. IEEE 802.11i Overview. NIST 802.11 Wireless LAN Security Workshop.

[5] Laura Marie Feeney and Martin Nilsson. Investigating the Energy Consumption of a Wireless Network Interface in an Ad Hoc Networking Environment. In *Proceedings of the* 20^{th} *Annual Joint Conference of the IEEE Communication Society (INFOCOM 2001)*, volume 3, pages 1548–1557, Anchorage, AK, USA, 22–26 Mar 2001.

[6] Dan Harkins and Dave Carrel. The Internet Key Exchange (IKE). RFC-2409, Nov 1998. See http://www.ietf.org/rfc/rfc2409.txt.

[7] Hugo Krawczyk, Mihir Bellare, and Ran Canetti. HMAC: Keyed-Hashing for Message Authentication. RFC-2104, Feb 1997. See http://www.ietf.org/rfc/rfc2409.txt.

[8] Bertil Schmidt, Manfred Schimmler, and Wael Adi. Area Efficient Modular Arithmetic for Mobile Security. In *Proceedings of the International Conference on Wireless Networks (ICWN 2002)*, pages 208–214, Las Vegas, NV, USA, 24–27 Jun 2002.

[9] Frank Stajano and Ross Anderson. The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks. In *Proceedings of the* 3^{rd} *AT&T Software Symposium*, Oct 1999.

[10] Srdjan Čapkun, Jean-Pierre Hubaux, and Levente Buttyán. Mobility Helps Security in Ad Hoc Networks. In *Proceedings of the* 4^{th} *ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC'03)*, pages 46–56, New York, NY, USA, 1–3 Jun 2003. ACM Press.

Paper IV [redacted]

Requirements for Privacy-Enhancements for Mobile Ad Hoc Networks

Reprinted from

3rd German Workshop on Ad Hoc Networks (WMAN 2005)
Proceedings of INFORMATIK 2005 - Informatik LIVE! Band 2
Lecture Notes in Informatics (LNI), Volume P-68
Bonn, Germany, 19–22 Sep 2005

Requirements for Privacy-Enhancements in Mobile Ad Hoc Networks

Christer Andersson, Leonardo A. Martucci, Simone Fischer-Hübner
{christer.andersson, leonardo.martucci, simone.fischer-huebner}@kau.se

Abstract

This paper formulates requirements for anonymous overlay networks for enhancing the privacy of mobile ad hoc network users. Besides, it analyzes existing peer-to-peer based anonymous overlay networks and shows that none of them are compliant with those requirements. Finally, it outlines the ongoing design of an anonymous overlay network intended for mobile ad hoc environments.

1 Introduction

Mobile ad hoc networks are constituted of mobile platforms that establish on-the-fly wireless connections among themselves, and ephemera networks without central entities to control it. Mobile ad hoc networks are an important building block in the fields of ubiquitous computing and sensor networks, two upcoming technologies that promise revolutionary services for the everyday citizen, as they allow instant networking between mobile devices without the interference or aid of central devices for network establishment.

However, applications based on mobile ad hoc networks also provide many challenges to privacy. When running applications on top of mobile ad hoc networks, vast amounts of possibly sensitive data are being transmitted among the participating mobile devices. Also, traffic information generated inside such networks can reveal sensitive information about the users, such as behavioral patterns or the locations of their communication partners. Finally, since MobileIP allows users to utilize existing web applications inside mobile ad hoc networks, users also run the risk of being profiled or pinpointed by web servers.

The purpose of this paper is to analyze how privacy can be enhanced in mobile ad hoc networks with the means of anonymous overlay networks, which are outlined in section 2. A number of requirements are derived in section 3 that an anonymous overlay network must fulfill in order to be suitable for mobile ad hoc environments. As peer-to-peer (P2P) based interactions are preferred to client-server based interactions in mobile ad hoc environments, section 4 analyzes to what degree existing proposals for P2P-based anonymous overlay networks are compliant with the characteristics of mobile ad hoc networks. Finally,

section 5 briefly discusses the ongoing design of an anonymous overlay network intended for mobile ad hoc environments.

2 A Possible Solution: Anonymous Overlay Networks

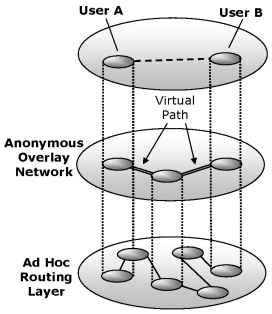

Figure 1: Anonymous communication between two nodes using an anonymous overlay network.

As a countermeasure against potential privacy problems in mobile ad hoc networks, we introduce an *anonymous overlay network* between the ad hoc routing layer and the application layer (see Figure 1) to provide anonymous communication services. Generally, an *overlay network* is a virtual network that is built on top of an existing network in order to implement network services not available in the existing network. In our case, the purpose of the overlay network is to provide all participants in the mobile ad hoc network with the means of anonymous communication. Being "anonymous" could imply both that a person's actions cannot be linked to his identity, and that it is hidden with whom he is communicating.

Many different kinds of overlay networks exists for providing anonymous communication, ranging from Chaum's classical Mixes [1] for email communication to newer P2P-based approaches, such as MorphMix [7] and Herbivore [4]. Most of them work by routing encrypted messages through chains of nodes, often called *virtual paths*, in order to hide both the identity of the sender and the relation between the sender and the recipient. On its path to the recipient, the outlook of a message is usually changed at each intermediate node by the means of encryption. In the cases when an anonymous overlay network employ a P2P-based model, it is the users themselves that constitute the nodes in the virtual paths.

Making use of an anonymous overlay network in mobile ad hoc environments would allow a user to be anonymous towards both other members of the anonymous overlay network (who may or may not be a part of that user's virtual path) and people in the whereabouts not participating in the network. It would also allow a user to be anonymous towards parties that are not part of the mobile ad hoc network, but still involved in the transactions, such as web servers on the Internet.

3 Requirements for Anonymous Overlay Networks

The most relevant characteristics of mobile ad hoc networks include: (1) heterogeneous mobile devices with different capabilities regarding embedded resources, (2) on-the fly es-

tablishment of network data links through wireless interfaces without the aid of any central entity or dynamic topologies, (3) resource availability and network services are defined by the network devices themselves, and finally (4) end devices are responsible to provide routing and packet forwarding while also guaranteeing their own security. Taking these characteristics into consideration, a number of requirements can be defined that an anonymous overlay network should meet in order to be suitable for mobile ad hoc environments:

- `Requirement R1:` *The anonymous overlay network must scale well.* The network must function well even with a large number of participants.
- `Requirement R2:` *The anonymous overlay network must provide strong ano-nymity properties.* For example, the network must provide adequate protection against malicious users and local (and preferably also global[14]) attackers.
- `Requirement R3:` *The anonymous overlay network must be fair regarding the distribution of workload among the participants.* Alternatively, some incentives must be given to accept a higher portion of the work load.
- `Requirement R4:` *The anonymous overlay network must provide acceptable performance.* Thus, the network should preferably be "lightweight" (for example, generate few messages and few public key operations).
- `Requirement R5:` *The anonymous overlay network must employ a P2P model.* Dependency on central hardware/services is not allowed in ad hoc networks.
- `Requirement R6:` *The overlay network must handle an dynamic topology.* In a mobile ad hoc network, nodes are frequently entering or leaving the network.

4 An Evaluation of State-of-the-Art Anonymous Overlay Networks

As stated above, the anonymous overlay network in our proposal should employ a P2P model. The most notorious anonymous overlay networks that rely on P2P interactions include: Crowds, Hordes, Tarzan, MorphMix, Herbivore and P^5. Crowds [6] is a lightweight overlay network that achieves anonymity by hiding one user's action within the actions of many users (in a so-called "crowd"). The crowd then issues requests to end servers on behalf of its members. Hordes [9] functions essentially like Crowds when sending messages to the web server, but uses multicast on the way back. Unlike Hordes and Crowds, Tarzan [3] uses layered encryption and cover traffic to be resistant against a global attacker. MorphMix [7] tries to provide strong anonymity without the use of cover traffic[15]. Herbivore [4] combines an approach based on Chaum's DC nets [2] with a hierarchical topology

[14] A global attacker has the possibility to eavesdrop on all traffic circulated in the overlay network.
[15] Traffic (lacking meaningful content) primarily employed to confuse potential eavesdroppers.

in which the users are grouped into smaller subsets (so-called "cliques"). In P^5 [8], participants send fixed length packets onto hierarchically tree-structured broadcasts channels at a fixed rate.

Table 1 below highlights the main results[16] that were generated when the aforementioned anonymous communication mechanisms were evaluated against the requirements listed in section 3. The table lists all the requirements that seem problematic to fulfill for each studied technology together with a brief motivation. In conclusion, it seems that none of the studied anonymous communication mechanisms are fully suitable for use in mobile ad hoc environments.

Table 1: Evaluation of P2P-based anonymous overlay networks.

Crowds	R2-	The attacker model in Crowds does not consider global attackers. Also, since each intermediary node decrypts and re-encrypts each packet, the level of confidentiality towards other nodes on the virtual path is limited.
	R5-	Crowds does not employ a true P2P-model as membership management and key distribution are handled by a centralized server.
Tarzan	R2-	The mechanism in Tarzan preventing malicious nodes from colluding (based on IP subnets) is not compliant with mobile ad hoc environments.
	R4-	Tarzan relies on cover traffic to protect against a global attacker.
Hordes	R2-	Hordes offers the same anonymity properties as Crowds, and thus, does not consider a global attacker.
	R5-	Similar to Crowds, membership management and key distribution are handled by a central server.
MorphMix	R2-	The attacker model assumes that a global attacker does not exist, and therefore does not protect against such an attacker.
	R3-	When building a virtual path between a node *a* and *b*, an additional node *w*, which is not part of the virtual path, must always act as a "witness".
	R4-	MorphMix transmits many messages when establishing its virtual paths, namely $6L + (L-2)(L+1)$ messages, where L is the number of nodes in the virtual path. Moreover, it needs four times more public key operations than Tarzan when constructing the paths.
	R6-	Path rebuilding is not efficiently done when a node leaves. Instead, the whole virtual path is rebuilt.

[16] Preliminary results of an earlier version of this evaluation is available at http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.3.study_on_mobile_identity_management.pdf.

Table 1: (continued)

Herbivore	R4-	Practical experiments in [4] indicate a high latency when many nodes are sending simultaneously.
	R5-	The minimum and maximum size of a clique needs to be centrally administrated.
	R6-	Although constituting an interesting concept, especially in the context of interconnected ad hoc domains, Herbivore's current topology based on cliques does not seem to be suitable for highly dynamic topologies.
P^5	R3-	Users near the root of the P^5 tree have a greater workload (and a stronger level of anonymity) than those located in the leaves of the tree. However, it is not possible to increase the desired level of anonymity during operation by migrating towards the root, since once the desired level of anonymity is chosen, it cannot be increased.
	R4-	P^5 relies heavily on cover traffic. Moreover, one public-key operation is required at a node for each received packet.
	R5-	In order to set the centrally administrated a-priori value determining the depth of the P^5 binary three, the expected number of participants in the anonymous overlay network is required beforehand.

5 Conclusions & Outlook

In order to guarantee privacy in usage scenarios based on mobile ad hoc networks, novel anonymity technologies must be developed, or existing ones need to be accordingly adapted. We are currently designing an anonymous overlay network suited for mobile ad hoc environments. Based on the analysis in previous section, the lightweight protocol Crowds seemed an appropriate choice for an underlying base. This initial version of the protocol will then be modified to make it fully suitable for mobile ad hoc environments. For example, new key distribution solutions [5] will be used to remove the need for a central server, and if a node in the path is leaving the network, the path will be rebuilt using as few operations as possible. Besides, we will elaborate on how to protect against global eavesdroppers without significantly reducing the performance. Finally, we will study how to hinder a malicious user from compromising an anonymous overlay network by using multiple IP addresses per device in order to increase the proportion of malicious nodes in the network (for example by using virtual interfaces).

References

[1] David Chaum. Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. *Communication of the ACM*, 24(2):84–88, Feb 1981.

[2] David Chaum. The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. *J. Cryptography*, 1(1):65–75, 1988.

[3] Michael J. Freedman and Robert Morris. Tarzan: A Peer-to-Peer Anonymizing Network Layer. In Vijayalakshmi Atluri, editor, *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS 2002)*, 18–22 Nov 2002.

[4] Sharad Goel, Mark Robson, Milo Polte, and Emin Gün Sirer. Herbivore: A scalable and Efficient Protocol for Anonymous Communication. Technical Report 2003-1890, Cornell University, Ithaca, NY, 14850, USA, Feb 2003.

[5] Leonardo A. Martucci, Christiane M. Schweitzer, Yeda R. Venturini, Tereza C. M. B. Carvalho, and Wilson V. Ruggiero. A Trust-Based Security Architecture for Small and Medium-Sized Mobile Ad Hoc Networks. In *Proceedings of the 3rd Annual Mediterranean Ad Hoc Networking Workshop, Med-Hoc-Net*, pages 278–290, Jun 2004.

[6] Michael Reiter and Avi Rubin. Crowds: Anonymity for Web Transactions. In *DIMACS Technical report*, pages 97–115, 1997.

[7] Marc Rennhard and Bernhard Plattner. Introducing Morphmix: Peer-to-Peer based Anonymous Internet Usage with Collusion Detection. In *Proceedings of the Workshop on Privacy in Electronic Society (WPES02)*, 21 Nov 2002.

[8] Rob Sherwood, Bobby Bhattacharjee, and Aravind Srinivasan. P^5: A Protocol for Scalable Anonymous Communication. In *Proceedings of the 2002 IEEE Symposium on Security and Privacy*, pages 55–70, 12–15 May 2002.

[9] Clay Shields and Brian Neil Levine. A Protocol for Anonymous Communication Over the Internet. In *Proceedings of the 7th ACM Conference on Computer and Communications Security*, pages 33–42, Nov 2000.

Paper V [redacted]

Chameleon and the Identity-Anonymity Paradox: Anonymity in Mobile Ad Hoc Networks

To be published

Proceedings of the 1st International Workshop on Security (IWSEC 2006)
Short Paper, Kyoto, Japan, 23–24 Oct 2006

Chameleon and the Identity-Anonymity Paradox: Anonymity in Mobile Ad Hoc Networks

Leonardo A. Martucci, Christer Andersson, Simone Fischer-Hübner
{leonardo.martucci, christer.andersson, simone.fischer-huebner}@kau.se

Abstract

In this paper we first present the identity-anonymity paradox, which explains why identities are needed to achieve reliable anonymity. Then, we introduce Chameleon, a novel anonymous overlay network for mobile ad hoc environments, and describe it in details with the support of state transition diagrams. To the best of our knowledge, this is the first low-latency anonymous communication mechanism designed for a mobile ad hoc network setting.

1 Introduction

Mobile ad hoc networks are constituted of mobile platforms that establish on-the-fly wireless connections among themselves, and ephemera networks without central entities to control it. The quest for privacy in mobile ad hoc networks is currently focused on introducing anonymity in the network layer, with several anonymous routing protocols being recently proposed [5, 11, 22]. However, such solutions prevent the usage of standardized ad hoc routing protocols, meaning, in practice, that all network nodes must run a non-standard routing protocol. Our proposal, Chameleon, is an anonymous overlay network tailored for mobile ad hoc environments, aiming, with reasonable performance costs, to provide sender anonymity against recipients and relationship anonymity against local observers. In addition, Chameleon provides conditional anonymity against malicious Chameleon users, as well as protection against single attackers trying to compromise large portions of a network by assuming multiple identities. Chameleon builds on a flexible design that provides isolation and independence from both the application and transport layers, allowing the usage of standardized mobile ad hoc routing protocols. To the best of our knowledge, Chameleon is the first low-latency anonymous overlay network being applied in a mobile ad hoc setting. Another overlay anonymous communication mechanism was recently presented by Jiang *et al.* [9], who propose a number of adaptations to make Chaum's classical mix concept [6] suitable for ad hoc networks. However, their solution is not low-latency, since it uses stop-and-go mixes and suggests the usage of bandwidth-consuming dummy-traffic.

Chameleon was specially designed with the characteristics of mobile ad hoc environments in mind. Therefore, when designing Chameleon, key characteristics of those environments, such as limited battery lifetime, user mobility and vanishing nodes, for instance, were taken into account. The core functionalities of Chameleon are inspired by the traditional Crowds system [15] for anonymizing HTTP traffic. This decision was made according to a previous evaluation of Peer-to-Peer (P2P) based anonymous overlay networks in the context of ad hoc networks [3]. Although none of the studied techniques were fully compliant with the characteristics of mobile ad hoc networks, the Crowds system [15] was deemed as an appropriate choice for a foundation upon which Chameleon could be developed. A number of adaptations to Crowds were made. For example, Chameleon enables end-to-end encryption between a sender and a recipient, employs certificates to hinder attackers from assuming multiple identifies, and acts as a general overlay network accepting all messages from the application layer.

The rest of this paper is organized as follows. Section 2 presents a discussion regarding identification and anonymity in mobile ad hoc networks, which we called the identity-anonymity paradox. In Section 3 we introduce Chameleon by describing its architecture and assumptions. In Section 4 we present a detailed description of Chameleon with the support of state-transition diagrams. Section 5 presents the theoretical analysis of the Chameleon protocol. Finally, Section 6 presents concluding remarks and future research plans.

2 The Identity-Anonymity Paradox

In order to implement identities in Chameleon, each Chameleon node owns a set of certificates used to authenticate against other Chameleon nodes. We assume that certificates are obtained either by a side-channel, or when the nodes are in contact with the certificate authority, possibly located in a fixed network. This section discusses why digital certificates were selected as identifiers in Chameleon, and also why we consider that the most reasonable option for all anonymous communication mechanisms and also security models for mobile ad hoc networks to be proposed from now on.

By definition [7], mobile ad hoc networks *may* operate in isolation — that is, in the absence of any fixed infrastructure. Therefore, the concept of autonomous systems is not applicable in mobile ad hoc environments, as there is no entity controlling the network and providing services such as routing, security or addressing[17]. The lack of standardized addressing schemes allows network nodes to change their IP addresses (and MAC addresses as well), or even to have multiple network interfaces (either real or virtual) with multiple identifiers. Thus, obtaining unique, persistent and trustworthy identifiers from layers below application (regarding the TCP/IP model) is not realistic. The consequence of such

[17]There are currently no standards for IP assignment in mobile ad hoc networks. Recently, the Autoconf Internet Engineering Task Force (IETF) Working Group [2] was assigned to study, among other questions, the problem of addressing in mobile ad hoc networks.

fact is that traditional identification systems that rely on the usage of network or data link information are basically useless in such environments.

The lack of reliable network and data link identification might give the impression that nodes in mobile ad hoc networks are naturally anonymous, especially if we consider using the Sybil attack[18] [8] as an enabler for achieving anonymity. The Sybil attack would allow the usage of multiple identifiers simultaneously with a lifetime equivalent to the lifetime of one session or TCP connection, for instance. Therefore, both IP and MAC addresses would constantly change and, in principle, it would not be possible to associate or track those identifiers.

Although the concepts of anonymity and identities can be understood as opposites, without identities, reliable anonymity is not achievable in mobile ad hoc environments. First, because such scheme would be vulnerable to traffic analysis and positioning techniques. Furthermore senders and recipients could be easily pinpointed and their relationships exposed since both senders and receivers establish direct connections, thereby, having their anonymity properties compromised. In addition, the lack of persistent identities is harmful for the network sanity, since all security mechanism for mobile ad hoc networks would hold without some form of trustworthy identifiers. We named this need of identifiers to achieve anonymity as the *identity-anonymity paradox*.

The consequences of this paradox and its relation with the Sybil attack lead to a clear interpretation of the definition of mobile ad hoc networks in the RFC 2501 regarding the operation in isolation and a better understanding of the foundations behind the issue of identifiers in proposed security mechanisms for mobile ad hoc environments. A taxonomy of such mechanisms is presented below, where security models are classified into three families regarding the way that identifiers are generated and obtained:

i. *intermittently connected to an established infrastructure* — security models belonging to this group assume that mobile ad hoc networks connect periodically (or at least occasionally) to an established infrastructure, such as the Internet. Therefore, it is possible to rely on the established security infrastructure that already exists in the Internet, such as a PKI (Public Key Infrastructure), and therefore, distribute digital certificates among the participants of an ad hoc network. Security schemes in this group include proposals that rely on Internet access [10] and proposals combining crypto-based techniques [4] with digital certificates;

ii. *setting a Certificate Authority in the mobile ad hoc network* — the assumption is that one or more devices have a special role in the network, such as personal Certificates Authorities (CA) and repositories. These CA are responsible for issuing certificates or credentials to devices in the mobile ad hoc networks. There are two basic approaches to set one or more CA in a mobile ad hoc network:

[18] In a Sybil attack, malicious users assume multiple identities, preventing the usage of security mechanisms based on filters or trust assumptions.

(a) one or more devices have a special role in the network, such as issuing certificates and publishing revocation lists, for instance. Solutions such as the Resurrecting Duckling model [17] are based on a central device that controls the network. In Martucci *et al.* [13], a security architecture is presented using multiple CA-like devices that control and secure a service-oriented ad hoc network. These solutions can operate isolated from an established infrastructure, although one or more nodes play a special role regarding security;

(b) a set of ad hoc network devices has parts of a private key that is used to issue certificates usually based on threshold cryptography. As long as a sufficient part of these nodes is the network range, digital certificates can be issued. Threshold cryptography was first proposed in the context of ad hoc networks in Zhou and Haas [23]. How many nodes and which nodes are needed to issue a certificate is usually implementation dependent;

iii. *PGP-like (Pretty Good Privacy) security models* — the assumption is that every device has one or more public/private key pairs and that every device can issue its own certificates and distribute them as well. Security often relies on the concept of web of trust. Such solutions are distributed enough to operate in complete isolation from any deployed infrastructure, however there are absolute no guarantees regarding protection against Sybil attacks, what is a major drawback of security models belonging to this family, such as the proposal of Capkun *et al.* [19] for instance.

Several conclusions can be drawn when putting the aforementioned taxonomy, the RFC 2501 definition and identity-anonymity paradox into the same picture. First, security schemes for ad hoc networks need to guarantee the uniqueness of the network identifiers, usually by the means of digital certificates. Second, the provisioning of reliable anonymous communication for nodes in a mobile ad hoc network, persistent identifiers are also needed. Third, to achieve reliable certificate distribution in ad hoc networks to prevent Sybil attacks, some sort of trusted third party (either centralized or distributed) is needed, which includes solutions from families *i* and *ii*, but not from family *iii*. Finally, regarding the RFC 2501 definition, to our understanding, a mobile ad hoc network may either depend intermittently on some deployed infrastructure (and therefore may operate in isolation for a given time frame) or it could operate in complete isolation from the deployed infrastructure, given that some support systems (a third trusted party) is deployed in the mobile ad hoc network.

Given all the aforementioned reasons, identities in Chameleon are implemented as digital certificates. The strategy for issuing and distributing identifiers depends on the security model chosen. From the point of view of the security model, Chameleon is an add-on for providing anonymous communication.

3 Chameleon: an Anonymous Overlay Network

The idea of Chameleon is that one user's action is hidden within the actions of many other users. By sending messages through virtual paths, a user can participate in a communication session while at the same time hiding his identity among the identities of the other users in the mobile ad hoc network.

A virtual path functions by routing encrypted messages through chains of nodes. To protect against traffic analysis, the appearance of the messages is changed at each node in the path through encryption. Generally, there are two main strategies for constructing virtual paths for anonymous overlay networks. One approach, applied in layered encryption approaches, is to let the first node decide the whole path by wrapping a message in several layers of encryption — one for each intermediary node along the path. These layers are thereafter peeled off (by decryption), one by one, at each subsequent node on the path. In the second strategy, the first node decides its successor, and then the intermediate nodes decide their respective successors, until some node decides to end the path, based on some criteria, and then forwards the message to the destination.

To deal with high mobility and to enable efficient path repairing in case of disappearing nodes, Chameleon employs the latter strategy for establishing virtual paths. Therefore, during path establishment, the decision of extending the path or not depends on the result of the toss of a biased coin, which bias is determined by a "probability of forwarding" p_f, where p_f is bounded by the interval $[0.5, 1)$. With the probability $(1 - p_f)$, the path is ended and a connection is established with the destination; otherwise the path is extended to another randomly chosen node, at which the same process is repeated. The path length L is thus probabilistic and denotes the sum of the appearances for each node on the path (excluding the destination node), and $\min(L) = 2$. The expected path length, L_{exp}, is given in equation (1) [15]:

$$L_{exp} = (p_f)/(1 - p_f) + 2 \tag{1}$$

Virtual paths are bidirectional, meaning that messages can travel forward (towards the destination) or backward (towards the source). As in Crowds, the destination's IP address is known only to the nodes belonging to the path, and path rebuilding is performed in the forward direction only (to enable path rebuilding also in the backward direction, intermediary nodes would require greater knowledge about the path and, eventually, the identity of the sender). To provide better protection against local observers, link encryption is employed between the nodes in the virtual path. Unlike Crowds, conditionally on the destination type, end-to-end encryption may also be applied between the sender and destination (see Section 4). Finally, Chameleon relies on the following assumptions:

i. It is expected that certificates are obtained a priori from a third trusted party, which is, most likely, located in a fixed network. Whether this assumption collides or not with the definition of mobile ad hoc networks in RFC 2501 [7] is polemic among authors in the field. In our opinion, it is expected for a node in a mobile ad hoc network

to have occasional contact with a fixed network and, therefore, to a set of trusted devices. This assumption is also present in other papers dealing with the problem of anonymity in ad hoc networks, such as [5, 11, 22];

ii. Chameleon assumes that it is possible to establish secure sessions in the transport layer, with mutual authentication using digital certificates and symmetric key establishment. Secure sessions can be achieved using standard protocols, such as TLS.

iii. Since the IP and hardware addresses are not necessarily unique identifiers that can be linked, with a long-term one-to-one relationship, to a corresponding user, we assume that the mobile ad hoc environment is a service-based network, such as Jini [14], SLP (Service Location Protocol) [20] or UPnP [18] networks. Therefore, all network services, including potential anonymity services, are announced through a localization (or directory) service, such as Jini's Lookup Server.

4 Chameleon Protocol Description

In the remainder of this paper, we use the following notation for describing the networks nodes in a Chameleon scenario:

i. Ψ denotes the set of nodes $\{\psi_1, \psi_2, ..., \psi_n\}$ situated in the mobile ad hoc network;

ii. Γ denotes the set of Chameleon users $\{\gamma_1, \gamma_2, ..., \gamma_n\}$, where $\Gamma \subset \Psi$. A virtual path is defined as a path connecting the sender, γ_s, with the last node before the destination, γ_{last}, where γ_s and γ_{last} are interconnected by zero or more nodes from Γ. When we describe the protocol, γ_i denotes the current node. The cardinality of Γ is denoted $|\Gamma|$ (where $|\Gamma| \in \mathbb{N}$), and $min(|\Gamma| = 3)$, since this is the minimum amount of members needed to provide some level of anonymity;

iii. D denotes the destination, which can be classified in three disjoint sets: $D_{\overline{sec}}$ accepts only unencrypted requests; D_{sec} accepts secure requests using a standard secure transport protocol between γ_{last} and D, and; D_Γ understands Chameleon protocol messages, enabling end-to-end encryption between γ_s and D;

iv. $\Phi \subset \Gamma$ denotes a set of decentralized directory servers $\{\phi_1, \phi_2, ..., \phi_n\}$ announcing the set of network addresses of the nodes in Γ, IP_Γ, along with their digital certificates, to other nodes in Γ. To reveal as little as possible information to Φ, each node in Γ requests IP_Γ at regular time intervals. The restriction $\Phi \subset \Gamma$ decreases the likelihood of corrupted directory servers announcing false information, since they can be detected as malicious nodes and filtered out by other Chameleon users. The announcement of IP_Γ follows one of the main principles of zero configuration networking [21], which assumes the existence of a service discovery system in network environments such

as mobile ad hoc networks. The nodes in Φ act as a distributed version of the blender in Crowds.

The following notation is used for the messages types in Chameleon:

i. θ denote application data passed to Chameleon from the application layer;

ii. m_{γ_i,γ_j} denote messages passed between Chameleon nodes γ_i and γ_j via the lower layers. The messages m_{γ_i,γ_j} are link encrypted between γ_i and γ_j using the symmetric key $E_{k_{\gamma_i,\gamma_j}}$ (established using a secure transport layer protocol). For the cases where $D \in D_{sec}$ or $D \in D_{\overline{sec}}$, the payload of m_{γ_i,γ_j} includes: IP_D — the IP address of D; $p\#_{\gamma_i,\gamma_j}$ — a path identifier (a randomly generated integer for identifying packet streams between nodes γ_i and γ_j); and the data payload θ — see equation (2), where $\cdot$ denotes concatenation. For the case where $D \in D_\Gamma$, m_{γ_i,γ_j} has two optional fields to achieve end-to-end encryption and data integrity — see equation (3). The first field contains a symmetric key $k_{\gamma_s,D}$, which is encrypted with the D's public key, Pu_D. The symmetric key $k_{\gamma_s,D}$ is used to set an end-to-end secure channel between γ_s and D. The second field is used to send the output of a keyed-hash function for message integrity, with input data θ and key $k_{\gamma_s,D}$;

$$m_{\gamma_i,\gamma_j} = E_{k_{\gamma_i,\gamma_j}}[p_{\#\gamma_i,\gamma_j} \cdot IP_D \cdot \theta] \tag{2}$$

$$m_{\gamma_i,\gamma_j} = E_{k_{\gamma_i,\gamma_j}}[p_{\#\gamma_i,\gamma_j} \cdot IP_D \cdot E_{k_{\gamma_s D}}[\theta] \cdot E_{Pu_D}[k_{\gamma_s D}] \cdot hash_{k_{\gamma_s,D}}(\theta)] \tag{3}$$

iii. An acknowledgment message is generated in γ_{last} and sent towards γ_s to inform that a message has reached its destination. Equation (4) describes the $ack\gamma_{i+1}, \gamma_i$ acknowledgement message sent from γ_{i+1} to γ_i.

$$ack_{\gamma_{i+1},\gamma_i} = E_{k_{\gamma_{i+1},\gamma_i}}[p_{\#\gamma_{i+1},\gamma_i}] \tag{4}$$

Each node in Chameleon maintains a routing table with the following entries: the destination's IP address (IP_D); the backward and forward path identifiers ($p_{\#\gamma_{i-1},\gamma_i}$ and $p_{\#\gamma_i,\gamma_{i+1}}$); the address of the preceding and succeeding nodes in the virtual path ($IP_{\gamma_{i-1}}$ and $IP_{\gamma_{i+1}}$) and; the time-to-live (TTL) counter, a decremental counter indicating the remaining lifetime of a given entry in the table. The path identifiers are managed in the same way as the *path_id* in Crowds [15]. In Chameleon, the tuple $[IP_{\gamma_i}, IP_{\gamma_{i+1}}, p_{\#\gamma_i,\gamma_{i+1}}]$ identifies a path connection between two nodes γ_i and γ_{i+1}. A Chameleon node can be described as a local proxy server following the state transition diagram in Figure 1. Its role is threefold; first, it may serve as the user's local proxy to which the user's applications forward their data, θ. In this case the node constitute the first node on the virtual path, γ_s. This situation is represented by the "Handle forward θ" state in Figure 1, which in turn can be expanded to the diagram in Figure 2. In the second case, a node can be an intermediary peer in one or more virtual paths. This situation is represented by the "Handle forward $m_{\gamma_{i-1},\gamma_i}$" (which can be expanded to

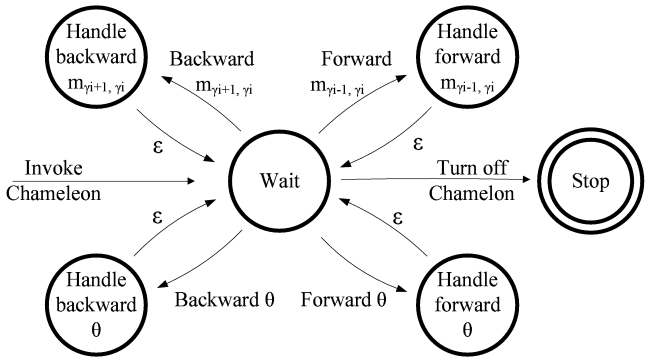

Figure 1: The Chameleon main state transition diagram for each node in Chameleon. A node can play the roles of γ_s, γ_i, or γ_{last}, depending on the type the incoming message.

the diagram in Figure 3) and "Handle backward $m_{\gamma_{i+1},\gamma_i}$" state in Figure 1 depending on the message direction. Finally, a node can act as the last peer in a virtual path, γ_{last}. In this case, it acts as a proxy server towards *D*.

In the remainder of this section, we key out the protocol details by (1) describing virtual path establishment, (2) describing how data is sent from γ_s to *D*, and, (3) describing how virtual paths are repaired in the event of a path break.

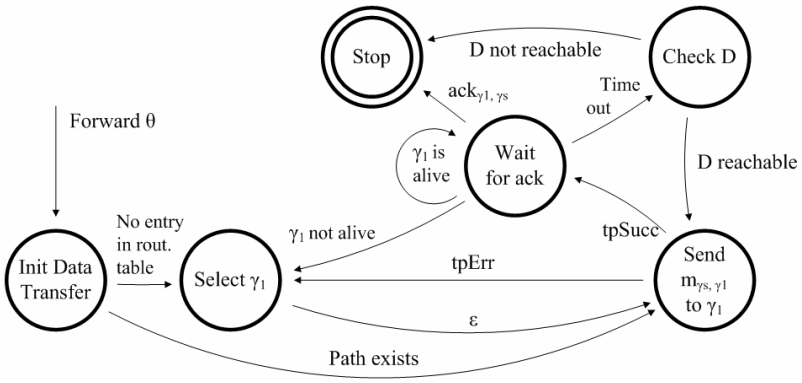

Figure 2: State transition diagram for a node γ_s receiving data from the application layer. The acronyms *tpSucc* and *tpErr*, used in this section, denote transitions indicating whether the sending of a message was accomplished successfully (*tpSucc*) or not (*tpErr*) in the transport layer.

A. *Building virtual paths.* In Chameleon, virtual paths are constructed as follows, as-

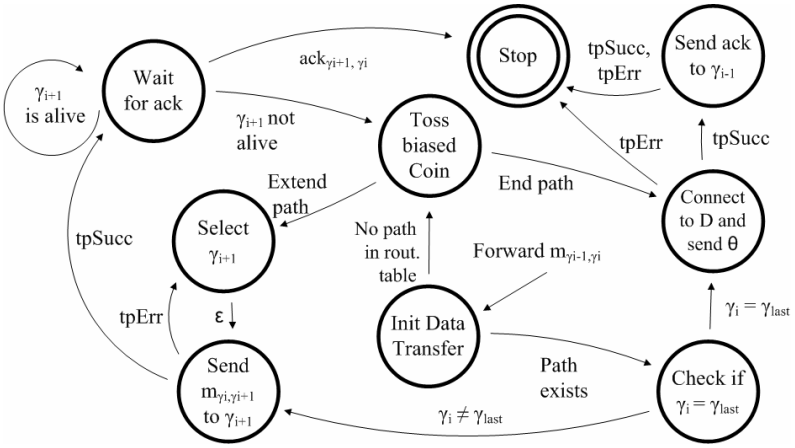

Figure 3: State transition diagram for a node γ_i receiving a message $m_{\gamma_{i-1},\gamma_i}$, including path repairing.

suming that there is no entry in the routing table for the designated IP_D:

(i) Path establishment is initiated when a node γ_s receives θ from the application layer. Then, γ_s randomly selects[19] a node γ_1 from Γ, as visualized in the "Select γ_1" state in Figure 2. Then, γ_s and γ_1 establish a secure session in the transport layer, exchanging a symmetric key k_{γ_s,γ_1} for link encryption. The sender γ_s then assembles and encrypts m_{γ_s,γ_1} (in which θ is piggy-backed) and forwards m_{γ_s,γ_1} to γ_1 ("Send m_{γ_s,γ_1} to γ_1" state in Figure 2). In cases when γ_s cannot send m_{γ_s,γ_1} to γ_1, it selects another new random node γ_1 from Γ and repeats the process;

(ii) Now, γ_i (i. e., $i = 1$), triggers the state transition diagram in Figure 3, and starts by decrypting $m_{\gamma_{i-1},\gamma_i}$. Assuming there is no corresponding entry for $m_{\gamma_{i-1},\gamma_i}$ in the Chameleon routing table of γ_i, a biased coin is tossed ("Toss biased coin" state in Figure 3). If the decision of the coin toss is to end the path, θ (encapsulated in $m_{\gamma_{i-1},\gamma_i}$) is forwarded to D. In this case, γ_i becomes the last node in the virtual path, γ_{last}. Otherwise, the path is extended one hop and a new node γ_{i+1} is selected randomly from Γ. The message $m_{\gamma_i,\gamma_{i+1}}$ is then encrypted and forwarded to γ_{i+1}, where this process is repeated. Eventually, a path will be established between γ_s and γ_{last}, where γ_s and γ_{last} are interconnected by zero or more intermediary Chameleon nodes.

[19] If γ_s posses no recent information about Γ, it contacts a directory server ϕ_i and requests this information. The nodes γ_s and ϕ_i mutually authenticate using their certificates.

B. *Sending and forwarding data*. In Chameleon, data is passed from γ_s to D in the following way, assuming that a virtual path is already established:

   (i) When γ_s receives θ from an application, γ_s assembles and encrypts m_{γ_s,γ_1}, and sends it to γ_1, as depicted in the "Send Message m_{γ_s,γ_1} to γ_1" state in Figure 2;

   (ii) Regarding the intermediary nodes, an incoming $m_{\gamma_{i-1},\gamma_i}$ is treated according to the state transition diagram depicted in Figure 3. At each node, $m_{\gamma_{i-1},\gamma_i}$ is decrypted, and $m_{\gamma_1,\gamma_{i+1}}$ is generated and encrypted before being forwarded. Eventually, the last node on the path, γ_{last}, will receive $m_{\gamma_{last-1},\gamma_{last}}$. Then, γ_{last} sends θ to D (either encrypted or unencrypted, depending on the destination type, see Section 4). Provided that the connection with D was successful, $ack_{\gamma_{last},\gamma_{last-1}}$ is sent backwards along the path to acknowledge γ_s that D did receive θ;

   (iii) The sending of data in the backward direction is initiated when γ_{last} receives θ from D. Then, γ_{last} encapsulates θ in $m_{\gamma_{last},\gamma_{last-1}}$ and sends it to γ_{last-1} on the virtual path. Since messages travelling in the backward direction are not acknowledged, the state transition diagram in Figure 1 always returns to the "Stop" state, independent of whether or not it was possible to send the message to γ_{last-1}. This process is repeated at each intermediary node until the message eventually reaches γ_s. If a timeout threshold is exceeded, the "Check D" state is invoked (Figure 2), where γ_s checks the status of D (this is possible since the ad hoc network is a service-based network). The timeout should be large enough to allow intermediary nodes to conduct path repairing, but, on the other hand, not too large, since this would risk to compromise the protocol performance.

C. *Repairing virtual paths.* Path repairing is initiated in two situations: first, when γ_i fails to send $m_{\gamma_i,\gamma_{i+1}}$ to γ_{i+1}, and, second, when γ_i waits for $ack_{\gamma_{i+1},\gamma_i}$ and notices that γ_{i+1} is not alive (γ_i polls γ_{i+1} at regular intervals during the "Wait for $ack_{\gamma_{i+1},\gamma_i}$" state to assert that γ_{i+1} is still alive, as illustrated in Figures 2 and 3). The node γ_i tosses a biased coin and either forwards θ directly to D or selects a new node γ_{i+1} as its successor in the path. In this way, the path is restored from the point where it was broken, and not from the beginning. No explicit path destruction is conducted after the communication session via the virtual paths has ended. Instead, the TTL field in the routing table ensures that inactive path entries are deleted.

5 Theoretical Analysis

Six different requirements were defined in [3] which an anonymous overlay network should adhere to (at least to an acceptable degree, since the requirements are not orthogonal) in order to be suitable in mobile ad hoc network environments. Next, we list these requirements, and discuss to what extent Chameleon meets them:

1. *Scalability*: the workload on each participant in Chameleon remains virtually constant as the number of participants grows, as in Crowds [15]. It is proved in [15] that for each node in the network, the expected number of virtual paths a node will be appearing on at a particular time is given by: $\frac{1}{(1-p_f)^2} * (1 + \frac{1}{|\Gamma|})$;

2. *Strong anonymity properties*: an anonymous overlay network should provide adequate protection against, for instance, malicious users and different types of eavesdroppers. The Chameleon attacker model is more complete and suitable for mobile ad hoc networks than the one used in Crowds. It assumes that all nodes (attackers included) have the same radio range. The following types of attackers are included:

   (a) *Local observer* ($\psi_{obs} \in \Psi$): a passive observer whose radio range covers γ_s;

   (b) *Malicious insiders* ($\Gamma' \subset \Gamma$): this attacker is represented by $|\Gamma'|$ (collaborating) malicious members of Γ, aiming to occupy all positions on the virtual path;

   (c) *Malicious outsider* ($\psi' \in \Psi$): this is a malicious node aiming to control an intermediary node linking a pair of Chameleon nodes in a given virtual path;

   (d) *Destination* (D): this attacker attempts to disclose the identity of γ_s;

   (e) *Malicious directory servers* ($\phi' \subset \Phi$): these constitute attackers hosting directory services for the purposes of misusing information about Γ, by the means of announcing different subsets of Γ in different instances of ϕ' and then mount a partition attack. Or, alternatively, announce a reduced set of Γ in order to increase the percentile of Γ' nodes in the announced set.

   The metric used is the same metric used for evaluating the anonymity properties of Crowds [15]. In this metric, each user is considered separately, and the resulting value spectra is a function of (among other parameters) the size of the anonymity set, the probability of forwarding and the amount of malicious insiders. The degree of anonymity for a subject γ_i can be expressed on a continuous scale ranging from `absolute privacy` to `provably exposed` via `beyond suspicion`, `probable innocence`, `possible innocence` and `provably exposed`. Chameleon offers sender and relationship anonymity against local observers. Unlike Crowds, Chameleon enables both link-to-link and end-to-end encryption for certain destination types. However, due to performance reasons Chameleon does not protect against a global observer[20]. In Table 1, the offered degrees of anonymity in Chameleon are summarized. The proof for these values can be found in [12]. Malicious directory servers are not included in the table since their goal is to compromise the anonymity level by supporting other malicious users. Possible countermeasures against ϕ' include the usage of redundant servers or cycling through Φ. In the extreme case, every node could run an instance of ϕ, but the performance trade-off would be high;

[20] Protection against a global observer can only be achieved if all nodes transmit in a constant rate independently of the real data traffic (i. e., demands the usage of dummy traffic).

Table 1: Degrees of anonymity in Chameleon.

	Sender Anonymity	*Receiver Anonymity*	*Relationship Anonymity*
Local observer (ψ_{obs})	possible innocence	beyond suspicion (for large networks)	beyond suspicion (for large networks)
Malicious insiders (Γ')	probable innocence if $\lvert\Gamma\rvert \geq \frac{p_f}{(p_f-\frac{1}{2})} * (\lvert\Gamma'\rvert + 1)$	P(absolute privacy) $= \left(\frac{\lvert\Gamma\rvert-\lvert\Gamma'\rvert}{\lvert\Gamma\rvert}\right)^{L_{exp}-1}$	probable innocence
Malicious outsider (ψ')	probable innocence if $L_{exp} \geq 4$	probable innocence if $L_{exp} \geq 4$	beyond suspicion
Destination	beyond suspicion for $\lvert\Gamma\rvert \geq 3$	–	beyond suspicion

3. *Fair distribution of work*: an anonymous overlay network should be fair regarding the distribution of workload among the participants. A possible source for unfairness in Chameleon is the workload implied for the operators of the directory servers Φ. However, this is dependent of the service-based network technology selected.;

4. *Performance-wise lightweight solution*: in order to reduce computational overhead and increase battery lifetime, an anonymous overlay network should generate few messages and perform few public key operations. Chameleon uses public key encryption sparsely and avoids layered encryption. The protocol overhead is low; assuming knowledge about Γ, $2L$ public key operations and $2L-1$ Chameleon messages are needed to establish a path, where L denotes the path length. In comparison, MorphMix [16] generates $6L + (L-2)(L+1)$ messages and needs at least $13L$ public key operations when establishing a path. Additionally, in contrast to Chameleon, the earlier mentioned mix-based proposal by Jiang *et al.* [9] uses nested public key encryption for both path establishment and message transfer. Lastly, no performance consuming dummy traffic is used;

5. *Adherence to the P2P-model*: mobile ad hoc networks are most often assumed to function without the aid of central services [7]. Unlike e. g., Crowds, Chameleon is a P2P-compliant protocol, although all nodes in Γ need to agree on the value of p_f;

6. *Manage a dynamic topology*: in most proposed mobile ad hoc network scenarios, it is assumed that nodes frequently enter and leave the network. Chameleon addresses dynamic topologies by, among other things, an optimized path repairing process in the forward direction. A virtual path is repaired only from the point of breach, in contrast to other approaches that rebuild a broken path entirely from scratch.

6 Conclusions

This paper introduced Chameleon, a low-latency anonymous overlay network tailored for mobile ad hoc networks that provides, for instance, efficient path repairing, and a reduced amount of control messages in comparison to other anonymous overlay networks. Chameleon does not rely on dummy traffic or layered encryption and it was inspired by the Crowds system, although it differs from Crowds in a number of ways, including: end-to-end encryption between the sender and recipient, certificate-based protection against Sybil attacks, and a distributed service discovery mechanism (and also an attacker model consistent with mobile ad hoc networks). We also presented the identity-anonymity paradox, which states the need of persistent identifiers to achieve reliable anonymity in mobile ad hoc networks. Current research plans include analyzing protocol performance by the means of simulation.

References

[1] *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC'03)*, New York, NY, USA, 1–3 Jun 2003. ACM Press.

[2] IETF Ad Hoc Network Autoconfiguration Working Group. Ad Hoc Network Autoconfiguration (autoconf), 2006. See http://www3.ietf.org/html.charters/autoconf-charter.html.

[3] Christer Andersson, Leonardo A. Martucci, and Simone Fischer-Hübner. Requirements for Privacy-Enhancements for Mobile Ad Hoc Networks. In *3rd German Workshop on Ad Hoc Networks (WMAN 2005), Proceedings of INFORMATIK 2005 - Informatik LIVE! Band 2*, volume 68 of *LNI*, pages 344–348. GI, 19–22 Sep 2005.

[4] Tuomas Aura. Cryptographically Generated Addresses (cga). RFC-3972, Mar 2005. See http://www.ietf.org/rfc/rfc3972.txt.

[5] Azzedine Boukerche, Khalil El-Khatib, Li Xu, and Larry Korba. SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks. In *Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN'04)*, pages 618–624, 2004.

[6] David Chaum. Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. *Communication of the ACM*, 24(2):84–88, Feb 1981.

[7] M. Scott Corson and Joseph Macker. Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. RFC-2501, Jan 1999. See http://www.ietf.org/rfc/rfc2501.txt.

[8] John R. Douceur. The Sybil Attack. In P. Druschel, F. Kaashoek, and A. Rowstron, editors, *Peer-to-Peer Systems: Proceedings of the 1st International Peer-to-Peer Systems Workshop (IPTPS)*, volume 2429, pages 251–260. Springer-Verlag, 7–8 Mar 2002.

[9] Shu Jiang, Nitin H. Vaidya, and Wei Zhao. A Mix Route Algorithm for Mix-net in Wireless Mobile Ad Hoc Networks. In *Proceedings of the 1st IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS2004)*, 24–27 Oct 2004.

[10] Frank Kargl, Stefan Schlott, and Michael Weber. Identification in Ad Hoc Networks. In *Proceedings of the 39th Hawaiian International Conference on System Sciences (HICSS-39)*. IEEE Computer Society, 4–7 Jan 2006.

[11] Jeijun Kong and Xiaoyan Hong. ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad Hoc Networks. In *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC'03)* [1].

[12] Leonardo A. Martucci, Christer Andersson, and Simone Fischer-Hübner. Towards Anonymity in Mobile Ad Hoc Networks: the Chameleon Protocol and its Anonymity Analysis. Technical Report 2006:35, Karlstad University, Karlstad, Sweden, Aug 2006.

[13] Leonardo A. Martucci, Christiane M. Schweitzer, Yeda R. Venturini, Tereza C. M. B. Carvalho, and Wilson V. Ruggiero. A Trust-Based Security Architecture for Small and Medium-Sized Mobile Ad Hoc Networks. In *Proceedings of the 3rd Annual Mediterranean Ad Hoc Networking Workshop, Med-Hoc-Net*, pages 278–290, Jun 2004.

[14] SUN Microsystems. The Jini Architecture Specification – Version 1.2, 2001.

[15] Michael Reiter and Avi Rubin. Crowds: Anonymity for Web Transactions. In *DIMACS Technical report*, pages 97–115, 1997.

[16] Marc Rennhard and Bernhard Plattner. Introducing Morphmix: Peer-to-Peer based Anonymous Internet Usage with Collusion Detection. In *Proceedings of the Workshop on Privacy in Electronic Society (WPES02)*, 21 Nov 2002.

[17] Frank Stajano and Ross Anderson. The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks. In *Proceedings of the 3rd AT&T Software Symposium*, Oct 1999.

[18] UPnP Forum. UPnP Device Architecture, Version 1.0, Jun 2000.

[19] Srdjan Čapkun, Jean-Pierre Hubaux, and Levente Buttyán. Mobility Helps Security in Ad Hoc Networks. In *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC'03)* [1], pages 46–56.

[20] John Veizades, Erik Guttman, Charles E. Perkins, and Scott Kaplan. Service Location Protocol. RFC-2165, Jun 1997. See http://www.ietf.org/rfc/rfc2165.txt.

[21] IETF Zero Configuration Networking Working Group. Zero Configuration Networking (zeroconf), 2003. See http://www.zeroconf.org/zeroconf-charter.html.

[22] Yanchao Zhang, Wei Liu, and Wenjing Lou. Anonymous Communication in Mobile Ad Hoc Networks. In *Proceedings of the* 24^{th} *Annual Joint Conference of the IEEE Communication Society (INFOCOM 2005)*, Miami, FL, USA, 13–17 Mar 2005.

[23] Lidong Zhou and Zygmunt J. Haas. Securing Ad Hoc Networks. *IEEE Network*, 13(6):24–30, 1999.