Identity Deployment and Management in Wireless Mesh Networks

Leonardo A. Martucci[1], Albin Zuccato[2] and Simone Fischer-Hübner[1]

[1] Karlstads University, Department of Computer Science
{leonardo.martucci, simone.fischer-huebner}@kau.se
[2] TeliaSonera, R&D Informations Security
albin.zuccato@teliasonera.com

Abstract. The goal of this work is the specification of the type of identifiers needed in a wireless mesh network scenario that supports the provisioning of both network security and privacy at the same time. A business model and business cases for a privacy-friendly identity management system are also presented.

1 Introduction

The extension of the radio range of access points using wireless relays is usually called wireless mesh networks. Mesh networking is an elegant and affordable technical solution for extending the range and the provisioning of services that are deployed in an infrastructured network behind an access point, such as a private network or even the Internet. Mesh networks may be combined with mobile ad hoc routing and have its radio range extended even more using mobile client devices as intermediary nodes to forward packets from users that are located beyond the radio range of a wireless access point or a wireless relay. In Figure 1, we illustrate a wireless mesh network scenario.

There are many research problems included in the scenario shown in Figure 1. These problems are divided into three large groups: one on performance aspects, regarding hybrid ad hoc routing, QoS, transport layers and roaming between relays for instance[1]; the second group deals with the economic and business problems involved, especially regarding how to stimulate and reward the cooperation among mobile nodes; and finally the third group encompasses the security and privacy aspects in such scenarios. This proposal focuses on the security and privacy issues, more specifically on the problem of identity management and user untraceability against other network participants. Untraceability is the property of being untraceable and, in the scope of this work, not traceable against attackers trying to track, stalk, impersonate or profile other users. The Pfitzmann and Hansen terminology [13] is followed in this paper.

On the other hand, the provisioning of non-revocable anonymous access to the network is undesirable for several reasons, especially because anonymous

[1] The IEEE 802.11 task group S is currently working on the standardization for mesh network based on the IEEE 802.11 standard [2]

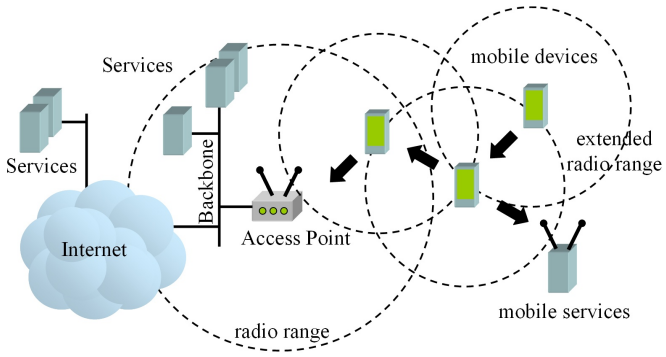

Fig. 1. A mesh network with one gateway connected to the backbone of the telecommunication / service provider and also to the Internet, and one wireless relay connecting 3 nodes through a mobile ad hoc network. Services are provided directly from the provider's backbone, from the Internet and also from the mobile network.

access makes the identification of malicious insiders, i.e., subscribed users misbehaving in the network into an impossible problem. Anonymous access also makes it difficult to reward subscribers forwarding packets from other users in the mobile ad hoc network; and, it turns billing into a difficult task. Therefore, the telecommunication service provider (TP) must be able to identify any subscriber for the purposes of billing and security.

The first step for the provisioning of anonymity towards other network users is to provide untraceable identifiers to the network subscribers. Although anonymity and identifiers seems two opposite concepts, identification is a basic requirement for the provisioning of reliable anonymity, as stated in the identity-anonymity paradox [12]. Unique identifiers are especially required to prevent the Sybil attack[2] [9]. Therefore, the TP has to distribute network identifiers that will be used for the provisioning of anonymity / pseudonymity. Data link and IP addresses must change accordingly to the rate of changes of the network identifier to prevent stalking using information obtained from those layers.

The goal of this work is the specification of the identifiers needed in a wireless mesh network scenario that can support the provisioning of network security and privacy simultaneously. We describe the system requirements, suggest an adequate solution and evaluate its advantages and disadvantages.

The organization of the paper is as follows. In Section 2 we present the security threats in a wireless mesh network scenario, the trivial solution and the implications to users' privacy. Section 3 presents the basic structure of an identity management system, the privacy rights of each entity and the requirements for the deployment of digital identifiers in a wireless mesh scenario. Section 4 discusses the available techniques to issue anonymous identifiers, while Section 5 presents the business model of the system. Section 6 concludes the paper.

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

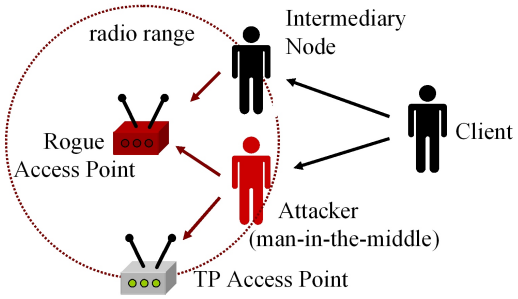

Fig. 2. Possible threats related to impersonation and man-in-the-middle attacks in wireless mesh networks. In the figure, a client has her data being forwarded either by a honest intermediary node to a rogue access point or by an attacker towards a rogue access point or to an authentic access point that belongs to the TP.

2 Security Threats, the Trivial Solution and Privacy

The threats involved in this scenario include privacy and network security threats. Network security threats include impersonation and man-in-the-middle attacks, as depicted in Figure 2. In an ad hoc network, the total absence of identification may lead to a Sybil attack [9], since honest users are not able to detect the relationship between logical identifiers (e. g., IP addresses) and physical devices is actually one to one. In the absence of trustable identification, network security cannot be guaranteed, and those security threats may affect also the network sanity and performance, and even denying the usage of the network by honest users [12].

Preventing the security threats described could be trivially achieved with the deployment of a Certification Authority (CA) and authentication servers (AS) on the TP side (using two-way authentication), distribution of X.509 public key certificates [1], mutual authentication and end-to-end secure channels between network entities. Users and servers would then be able to univocally identify other network entities and verify the authenticity of their communication partners. There are many details involved even within this trivial solution, such as: decisions regarding the end-to-end secure communication protocol suite between users and servers, and users and users; the authentication protocols and data link security between wireless relays and access points; the use of on upper layer encryption, such as VPN connections, for users' transactions; and the security properties of the ad hoc routing algorithms (to be used in the extended radio range).

However, the presented solution does not address the privacy threats. Privacy threats include profiling, monitoring and stalking of devices using the provided identifiers as source of information[3]. X.509 public key digital certifi-

[3] Some threats related to physical and routing layer attacks are not going to be considered in the scope of this paper. Such threats include network jamming and radio device tracking using radio fingerprints and signal to noise (S/N) ratio techniques.

cates are not privacy-friendly since it is possible to track users using the serial number information of those certificates. Data link and network layer information (i. e., $\{MAC, IP\}$ pairs) could be used as privacy-friendly identifiers because they can be changed regularly [10], but this information cannot provide trustable identification [12] and makes the system vulnerable to Sybil attacks. Thus, the usage of privacy-friendly certificate-like identification, issued by a Trusted Third Party (TTP), is a solution for both privacy and security threats in a wireless mesh network scenario.

3 Identities and Identity Management System

The identity management (IdM) system in the wireless mesh network scenario follows the general three type categorization for IdM [11]: *account management*, *profiling* and *management of own identities*. The account management – for authentication, authorization and accounting (AAA) purposes – is done by the TP. The management of own identities is performed by each network user, who is able control her partial identities using an IdM tool. Profiling is done by the service providers (SP), especially for the purpose of service customization and / or customer relationship management. Therefore, identifiers are used in different ways in a wireless mesh network. A privacy-friendly wireless mesh network has the following basic rights for users and other parties:

a) users have the right to remain anonymous towards other users.
b) users have the right to choose to be anonymous or to have a pseudonym towards a SP. Pseudonyms may be used to obtain personalized services and are usually associated to the disclosure of a user's partial identity.
c) TP have the right to identify users and eventually revoke their identifiers. Identification of pseudonyms and disclosure of anonymous users must be supported to allow identification of malicious nodes in the network or even for authentication, authorization and accounting (AAA) purposes, for instance[4]. A TP must respect the privacy of users and therefore handle their personal data according to the legislation regarding data protection[5].
d) SP have the right to retain and process (anonymized) users' related information according to the applicable legislation.

Thus, a user has many identifiers: a single identifier towards the TP, one or more pseudonyms towards different SP, and one-time identifiers (on transaction pseudonyms) towards other users. Figure 3 provides an illustration of the multiple identifiers described in this paragraph. The security and privacy requirements for digital identifiers in a wireless mesh network scenario are:

[4] Assuming that the TP is trusted and fair regarding the disclosure of identifiers.
[5] In Europe, this includes the EU Data Protection Directives 95/46/EC, the EU Directive 2002/58/EC on privacy electronic communications and the EC Data Retention Directive 2006/24/EC.

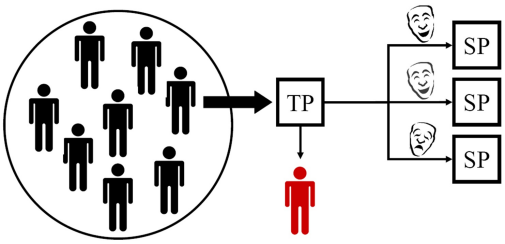

Fig. 3. Users are anonymous among their peers and at the same time are uniquely identified by the TP and may have different identities towards different SP.

i) Identifiers must be unique. This is needed to guarantee the the 1-to-1 relationship between logical identifiers and physical devices, especially in the extended radio range of the wireless mesh network. Uniqueness is needed for preventing Sybil attacks [9] in the wireless mesh network.
ii) Identifiers must be anonymous towards all other entities, except the TP. This is required for the provisioning of user untraceability against other network entities (e. g., other mobile users, SP).
iii) Re-identification of anonymous identifiers must be supported. The TP shall be able to identify users and eventually revoke their identifiers. Anonymity revocation is needed to identify malicious nodes, such as clones, or eventually for AAA purposes, for instance[6].
iv) It must be possible to authenticate peer devices without the interference of the AS. This is needed for supporting mobile ad hoc services or P2P applications that can be provided without the support of the TP's telecommunication infrastructure.

A simplified network topology depicting the basic infrastructure and services supported or connected to the TP is shown in Figure 4.

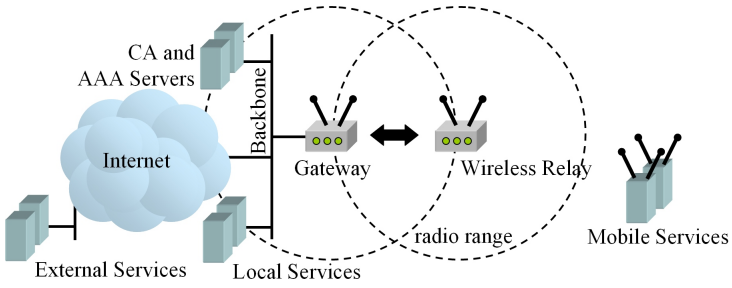

Fig. 4. The basic infrastructure provided by the TP includes the wireless mesh network, CA and AAA servers and other internal and external services.

[6] We assume that the TP is trusted and fair regarding the disclosure of identifiers.

4 Anonymous Credentials in a Wireless Mesh Network

The usage of either anonymous attribute certificates (ATC) [3] or anonymous credentials [6, 7, 5] is recommended since they might provide untraceability to the user if used correctly. Untraceability is provided by preventing unauthorized identification of network clients by distinguishing multiple appearances of a given node into the mesh network. Thus, each appearance of a user in the network must be unlikable to a previous appearance. The set of potential attackers include other (colluding) nodes in the mobile ad hoc network or a service provider (SP). ATC are based on zero-knowledge (ZK) proofs of knowledge[7] and are structured as a composition of a group certificate and an X.509 attribute certificate [1]. There are mechanisms associated with ATC that allow users' identities to be disclosed, traced or revoked by an identity escrow [3]. ATC do not offer guarantees to the 1-1 relationship between identifiers and devices (item "*i*" – Section 3) since there are no means to prevent or detect ATC sharing. Anonymous credentials can be constructed using either blind signatures or ZK proofs. Anonymous credentials based on ZK proofs can, beyond providing anonymity, be used multiple times (multiple show) [7], be revocable [4] and detect sharing of credentials [5]. Therefore, anonymous credentials have the potential to fulfill all the basic security and privacy requirements for identifiers in a wireless mesh scenario presented in Section 3.

5 Business Model for a Privacy-Friendly IdM

To discuss a business model for a privacy-friendly IdM we have to clarify the general conditions in which such a model need to exist. The TP's key assets are the following three: (*i*) its customers, (*ii*) its technical infrastructure, and (*iii*) its technical competence. For the further discussion the first two are of significance.

The customer is a utterly important asset for the TP. To maintain customers' loyalty and trust significant resources are required from the TP (i. e., customer relationship management). The TP aims to protect and strengthen its customer relationships and is reluctant to put it at risk. A third party (SP) must not receive enough "identifying" information that allows it to deal with the TP's customers directly. Customer satisfaction decreases with inappropriate handling of personal information. The TP is interested to act in a privacy-friendly way, so that the customer is satisfied and do not consider churn.

The second important factor is the network infrastructure (i. e., networking hardware). The TP has to invest heavily into infrastructure to provide a broader range of services to more customers. Mesh networks is a way to reach more customers without infrastructure investments. A drawback is that mesh networks imply that the TP loses the control over part of the network. From a

[7] ZK proofs of knowledge are interactive proofs in which the verifier learns nothing besides the fact that the statement that is proven is true [14, 8].

security point of view, this loss of control requires that the operator (a) do its uttermost to maintain security by investing into security mechanisms and (b) informing the customer about the risk.

A customer's identity can be divided in partial identities that enable the customer and the TP to use only a subset of the personal information for the purpose at hand. Partial identities can be far better tailored to the purpose of the SP and the TP does not risk to lose control of its customer's identities. By offering support to an IdM service the TP allows its customers to control their partial identities. Moreover, an IdM is an value-added service that increases the market attractiveness of the TP to keep and attract more customers, and also offers new business opportunities (e. g., the customer pays for the service, third parties pay for obtained information), which allow the creation of new income sources. We discuss some of them as business cases next.

Business Case - IdM for mesh networks: mesh networking allows more customer to use the TP network. This creates revenue from more subscriptions (i. e., more customers are in range for using the service) and service usage (i. e., traffic). It is crucial that the parties are identifiable to guarantee network sanity and allow for billing / compensation payments. The use of persistent identifiers would affect the privacy and risk the customers' privacy. Therefore, an IdM must be able to provide anonymous identifiers which fulfill the rights presented in Section 3.

Business Case - Provide an IdM infrastructure for third parties: identities are used in different scenarios. A single IdM system implies that different services do not need to manage identities. Costs and risks involved can be forwarded using a third party IdM. The TP role is to provide an IdM infrastructure.

6 Summary and Future Work

In this paper we introduced the problem of security and privacy-friendly identification in wireless mesh networks. We presented four security and privacy requirements for digital identifiers in these environments. We compared two solutions for anonymous identifiers, anonymous attribute certificates and anonymous credentials, and concluded that anonymous credentials fulfill all requirements: the provisioning of anonymity, uniqueness, revocability and independence of a central authentication server.

We also presented a business model that justifies the economic need of anonymous identifiers and wireless mesh network from a telecommunication provider viewpoint. We support our business model with two business cases.

A multiple-show, revocable, anonymous credential system, with credential sharing detection, derived from the periodic n-times spendable e-token scheme [5] is a work-in-progress initiated within the EU Fidis Project[8]. As a future work, we plan the development of a prototype which will provide a proof-of-concept implementation of the selected scheme.

[8] See http://www.fidis.net

References

1. ITU-T Recommendation X.509, The Directory: public-key and attribute certificate frameworks. Recommendation X.509 - International Telecommunications Union, The International Telegraph and Telephone Consultative Committee, Data Communication Networks: Open Systems Interconnection (OSI); Security, Structure and Applications, Aug 2005.
2. IEEE P802.11 TGs. Status of Project IEEE 802.11s, Mar 2007. See `http://www.ieee802.org/11/Reports/tgs_update.htm`.
3. V. Benjumea, J. Lopez, and J. M. Troya. Anonymous Attribute Certificates based on Traceable Signatures. *Internet Research: Electronic Networking Applications and Policy. Special Issue on Privacy and Anonymity in the Digital Era: Theory, Technologies and Practice*, 16(2):120–139, 2006.
4. J. Camenisch. Efficient Private Credential Systems and Applications: Cryptography for Privacy – Credential$^+$ Systems. 3^{rd} Fidis Doctoral Consortium Event, Stockholm, Sweden, 9–13 Aug 2006.
5. J. Camenisch, S. Hohenberger, M. Kohlweiss, A. Lysyanskaya, and M. Meyerovich. How to Win the Clone Wars: Efficient Periodic n-Times Anonymous Authentication. In *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS 2006)*, 30 Oct – 3 Nov 2006.
6. J. Camenisch and A. 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.
7. J. Camenisch and A. Lysyanskaya. A Signature Scheme with Efficient Protocols. In *Security in Communication Networks: Third International Conference (SCN 2002)*, volume 2576/2003 of *Lecture Notes in Computer Science*, pages 268–289, Amalfi, Italy, 12–13 Sep 2002. Springer Berlin/Heidelberg, LNCS 2576.
8. J. Camenisch and M. Stadler. Proof systems for general statements about discrete logarithms. Technical Report TR 260, Institute for Theoretical Computer Science, ETH Zürich, Mar 1997.
9. J. R. Douceur. The Sybil Attack. In P. Druschel, F. Kaashoek, and A. Rowstron, editors, *Peer-to-Peer Systems: Proceedings of the 1^{st} International Peer-to-Peer Systems Workshop (IPTPS)*, volume 2429, pages 251–260. Springer-Verlag, 7–8 Mar 2002.
10. M. Gruteser and D. Grunwald. Enhancing Location Privacy in Wireless LAN Through Disposable Interface Identifiers: A Quantitative Analysis. In P. Kermani, editor, *Proceedings of the 1^{st} ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots (WMASH 2003)*, 19 Sep 2003.
11. M. Hansen. Identity Management in Civil Registration. 2^{nd} Conference on eServices in European Civil Registration, 8 Sep 2006.
12. L. A. 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, September 2006.
13. A. Pfitzmann and M. 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/`.
14. C. P. Schnorr. Efficient signature generation for smart cards. *Journal of Cryptology*, 4(3):239–252, 1991.