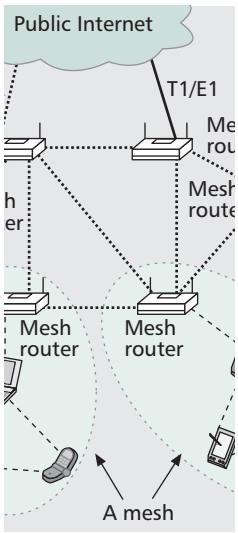
ACCEPTED FROM OPEN CALL

SECURITY, PRIVACY, AND ACCOUNTABILITY IN WIRELESS ACCESS NETWORKS

WENJING LOU, WORCESTER POLYTECHNIC INSTITUTE
KUI REN, ILLINOIS INSTITUTE OF TECHNOLOGY



The presence of ubiquitous connectivity provided by wireless communications and mobile computing has changed the way humans interact with information. At the same time, it has made communication security and privacy a hot-button issue.

ABSTRACT

The presence of ubiquitous connectivity provided by wireless communications and mobile computing has changed the way humans interact with information. At the same time, it has made communication security and privacy a hot-button issue. In this article we address the security and privacy concerns in wireless access networks. We first discuss the general cryptographic means to design privacy-preserving security protocols, where the dilemma of attaining both security and privacy goals, especially user accountability vs. user privacy, is highlighted. We then present a novel authentication framework that integrates a new key management scheme based on the principle of separation of powers and an adapted construction of Boneh and Shacham's group signature scheme, as an enhanced resort to simultaneously achieve security, privacy, and accountability in wireless access networks.

INTRODUCTION

The technology advances in wireless communications and mobile computing have led to the prevalent network accesses through mobile devices communicating wirelessly. From workplace Wi-Fi infrastructure to home high-speed wireless mesh network access, from Web browsers in cellular phones to public hot spots, it seems that wireless access networks are everywhere. Entertainment, e-banking, e-commerce, and medicine; exciting new applications are developed to work in mobile devices that are extending the reach of today's network even further. At the same time, the threats posed by such technology advances to personal security and privacy are unprecedented, from both the unintended disclosure of sensitive information by inexperienced or non-vigilant users as well as the ease of wireless signal interception and rapidly evolving sophistication of surveillance gadgetry.

Security and privacy have been essential problems since the arrival of the information era. Security is essential in any network and has been relatively well studied. There is a well defined security architecture, which consists of security attacks, security mechanisms, and security services/requirements, to define, study, and evaluate security needs in a systematic way. In the context of wireless access networks, the main security goals include:

- *Authentication*: Ensures that the origin and destination of a conversation are correctly identified, with an assurance that the identities between two communicating parties are not falsified.
- *Confidentiality*: Prevents unauthorized disclosure of transmitted information from passive attacks, such as eavesdropping.
- *Integrity*: Ensures that the transmitted information is not illegally modified. Modification includes changing, deleting, creating, delaying, or replaying transmitted messages.
- *Non-repudiation*: Guarantees that neither the sender nor the receiver of a message is able to deny the transmission.
- *Access control*: The ability to limit and control access to devices and applications via communication links.
- *Availability*: Requires the network services to be available to authorized parties whenever needed.

It is known that in different applications, the importance of those security requirements may differ in degree but not in kind.

Recently privacy has also become a critical issue, especially in contexts such as banking, commerce, diplomacy, and medicine. But if you ask what exactly the privacy concerns are, you may have a variety of answers from different perspectives. Some may worry about personal conversations eavesdropped on by a third party due to the easy interception of wireless signals; some may be concerned with insurance companies digging through personal medical records to deny coverage to certain people; some may be angry about how corporations collect private data to target their advertisements; or, even worse, the data may be used to sort everyone into some category. There has not been a well established standard for privacy. The definition of privacy also varies with the application scenario. In the context of wireless access networks, we deem the following privacy services/requirements indispensable:

1536-1284/09/$25.00 © 2009 IEEE

- *Anonymity*: The identity of the origin and/or the destination of a conversation is hidden from adversaries unless it is intentionally disclosed by the user.
- *Non-linkability*: Different communication sessions associated with the same user should not be linkable. An adversary cannot link the communication activities of a particular user together and thus establish the user's profile, which contains much private information.
- *Context privacy*: An adversary should not be able to learn the exact access context information (location, duration, type of service request, etc.) of a user unless the user decides to divulge such information.
- *Confidentiality and integrity*: The interactions between a user and a service should have both confidentiality and integrity protections whenever such protections are required. This requirement can be achieved by security mechanisms for the same purpose.

Furthermore, it should be noted that, depending on the roles and the resources available, adversaries can be outsiders (e.g., eavesdroppers, other legitimate users), insiders (e.g., service providers), or even the communicating party on the other side of the conversation. Privacy services may be provided at different levels against adversaries with various levels of knowledge and capability [1].

In reality, privacy is a conundrum because its quest often contradicts the requirements of security. Perfect privacy protection, such as true anonymity that hides a user's identity from eavesdroppers, service providers, and even the other communicating party, not only in itself is a difficult technical challenge, but also raises a serious security concern: how can we hold a malicious user accountable if he/she is able to launch attacks anonymously? Conscious tradeoffs must be made to realize both security and privacy protections.

Authentication is the first line of access security that ensures only legal users gain access to the network. Essentially, and also as done in the current Wi-Fi, WiMAX, and cellular systems, authentication is done through a challenge-response process, based on the simple idea that the user being authenticated proves knowledge of some secret only known to him/herself. Figure 1 outlines the typical authentication procedures based on either secret-key or public-key cryptography. It is clear that the user has to reveal his/her identity so that the access point can verify the user's credential in order to authenticate the user. It achieves the security objective — user authentication. However, user privacy is not protected. In fact, current wireless systems provide very limited user privacy protection. In cellular systems, GSM provides a low level of anonymity. The subscriber's identity is protected from eavesdroppers on the wireless interface through the use of a short-term temporary mobile subscriber identity (TMSI) instead of the user's long-term international mobile subscriber identity (IMSI). TMSI only prevents an eavesdropper from identifying a subscriber. The service (the base station) has full knowledge of the user and can easily identify a user and trace his/her activities. The Wi-Fi system only provides data confidentiality; no privacy protection is provided so far. Privacy protection for wireless communications is far from satisfactory.

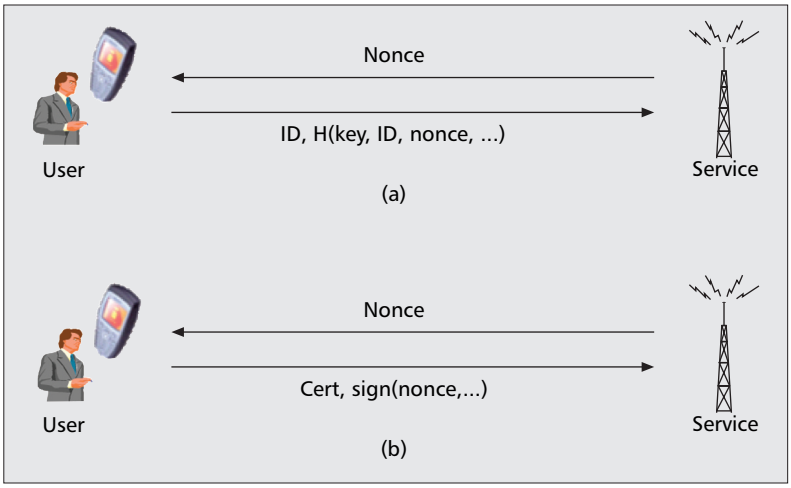
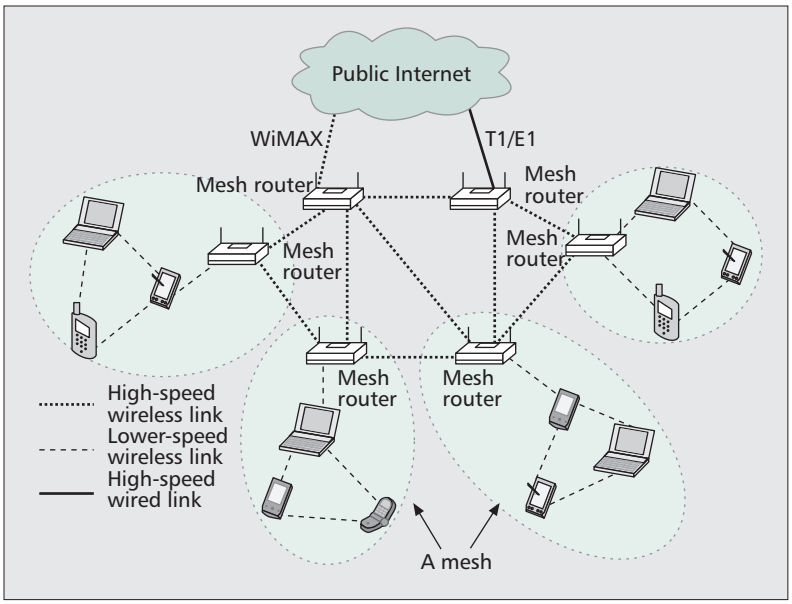


Figure 1. *Typical challenge-response authentication: a) secret key cryptography-based; b) public key cryptography-based.*

Approaches to Privacy-Preserving Security Protocols

Security and privacy are two seemingly contradictive objectives in the case of access authentication. On one hand, a user has to reveal his/her identity in order to be verified for authentication purposes. On the other hand, the identity of the user serves as a unique identifier that an attacker can make use of to filter out a particular user's online transactions, and trace his/her whereabouts and activities, which may leak sensitive user privacy information. The linkability among a user's online transactions may also enable an unauthorized user profiling without the user's consent. Much research work has been focused on anonymous user authentication that enhances user privacy while maintaining access security. The basic idea for anonymous authentication is that through some cryptographic means, a legitimate user's legitimacy of using the service can be verified, while at the same time the particular identity of the user is somehow concealed. Toward this end, techniques such as blind signature, ring signature, and group signature have been used to provide both user authentication and k-anonymity (i.e., hiding a particular user's identity in a group of k other users). We review these cryptographic tools briefly and discuss their effects on privacy preserving as follows.

Blind signature [2] is a variation of a digital signature scheme in which the content of a message is disguised from its signer. Blind signature schemes can be implemented based on a number of well-known digital signature schemes, such as Rivest Shamir Adleman (RSA). To produce a signature on a message, a user first blinds the message with a blinding function f, typically by combining it with a random blinding factor, and then forwards the blinded message to the signer. The signer signs the blinded message using a



■ **Figure 2.** *WMN network architecture [8].*

standard signing algorithm, say $S_A(m)$, which denotes the signature of A on m, and sends the result back to the user, who then unblinds it with an unblinding function g to obtain the signer's signature on the original message. The algorithm is designed such that $g(S_A(f(m))) = S_A(m)$.

While used in anonymous access authentication, a legitimate user typically obtains blind signatures from the service provider, and unblinds them and uses them as the authentication tokens. Besides hiding the user's true identity, blind signatures can also provide non-linkability, which prevents the signer from linking a blinded message it signed to the unblinded version it may be called upon to verify. In this case the signed, blinded value is unblinded prior to verification in such a way that the signature remains valid for the unblinded message. This can be useful to hide not only the user's true identity, but also the linkage among the signatures of the same unknown user. Blind signature schemes find a great deal of use in applications where sender privacy is important. This includes various digital cash schemes and voting protocols. Reference [3] described a privacy-preserving authentication protocol based on blind signature, in which a one-way hash chain is also incorporated to improve the authentication efficiency.

Ring signature [4] is a signer-ambiguous signature scheme first introduced by Cramer *et al.* in 1994. With ring signature, a set of possible users (signers) should be specified, and each user should be associated with the public key of some standard signature scheme such as RSA. To generate a ring signature, the actual signer declares an arbitrary set of possible signers that must include him/herself, and computes the signature of any message by him/herself using only his/her secret key and the others' public keys. Ring signatures can be verified by the intended recipient as a valid signature from one of the declared signers, without revealing exactly which signer actually produced the signature. Ring signatures provide an elegant way to leak authoritative secrets in an anonymous way and can be used to solve multiparty computation problems. In the case of anonymous access authentication, ring signatures allow a legitimate user to hide his/her true identity among an arbitrarily selected set of other users. The non-linkability of multiple transactions of the same user is also well protected.

However, although both blind signature based schemes and ring signature based schemes provide user anonymity protection, they suffer from degraded security protection due to the lack of user accountability. Both schemes provide irrevocable anonymity. Technically there is no way to revoke the anonymity of the user unless he/she decides to expose him/herself. Bad user behaviors and insider attacks cannot be traced, even by the service provider.

Group signature is another signer-ambiguous signature scheme that is suitable for user privacy protection due to the k-anonymity it provides. Group signature is a relatively recent cryptographic concept introduced by Chaum and van Heyst in 1991 [5]. Similar to a ring signature, a group signature scheme allows a member of a group to sign a message on behalf of the group, without revealing which actual member produced the signature. A verifier can only tell that a member of the group signed the message, but not exactly which member. However, different from a ring signature, in exceptional cases such as a legal dispute, a group signature can be opened by a designated group controller to reveal unambiguously the identity of the signature's originator. Some group signature schemes support revocation, where group membership can be disabled. One of the most recent group signature schemes is the one proposed by Boneh and Shacham [6], which has a very short signature size comparable to that of an RSA-1024 signature [7].

The capability of revoking the anonymity of a user when necessary makes group signature a compelling cryptographic primitive to privacy-preserving applications. Nevertheless, the revocation capability of group signature schemes, on one hand, provides enhanced security as bad users will be held accountable for their malicious behaviors, but on the other hand represents degraded user privacy protection because when directly applied to user authentication, the network operator, who usually serves as the group controller, will always be able to track the user. As we show in the next section, this is not desirable, especially in a network where the operators are not highly trustworthy.

Separation of Powers: A Privacy-Preserving yet Accountable Authentication Framework

Providing security, privacy, and accountability seems to be a dilemma, and has been an unique challenge in wireless access networks. In this section we present a novel privacy-preserving yet accountable authentication architecture. We present the framework in the case of a metropolitan wireless mesh network. However, we believe the general idea of achieving security, privacy, and

accountability simultaneously based on the principle of separation of powers applies to other networks too.

Wireless mesh networks (WMNs) have been posed as the competitive rival to the future wireless cellular technologies and a promising technology for ubiquitous high-speed network access, secure facility surveillance, disaster relief, public safety, and homeland security. In a metro-scale community mesh network, people access WMNs from everywhere within the community such as offices, homes, restaurants, hospitals, hotels, shopping malls, and even vehicles. Through WMNs they access the public Internet in different roles and contexts for services like emails, e-banking, e-commerce, and Web surfing, and also interact with their local peers for file sharing, teleconferencing, online gaming, instant chatting, and so on. All these communications contain various kinds of sensitive user information like personal identities, activities, location information, financial information, transaction profiles, and social/business connections. Figure 2 [8] shows the topological structure of a multihop layered WMN. The first layer consists of access points, which are high-speed wired Internet entry points. The second layer comprises stationary mesh routers that form a multihop backbone via long-range high-speed wireless techniques such as WiMAX. The wireless backbone connects to wired access points at some mesh routers through high-speed wireless links. The third layer consists of a large number of mobile network users. These network users access the network either by a direct wireless link or through a chain of other peer users to a nearby mesh router.

Due to the intrinsically open and distributed nature of WMNs, it is essential to enforce network access control to cope with both free riders and malicious attackers. Dynamic access to WMNs should be subject to successful user authentication based on properly pre-established trust between users and the network operator; otherwise, network access should be denied. On the other hand, it is also critical to provide adequate provisioning for user privacy as WMN communications usually contain a vast amount of sensitive user information. The wireless medium, open network architecture, and lack of physical protection over mesh routers render WMNs highly vulnerable to various privacy-oriented attacks. These attacks range from passive eavesdropping to active message phishing, interception, and alteration, which could easily lead to the leakage of user information. The wide deployment of WMNs can succeed only after users are assured of their ability to manage privacy risks and maintain their desired level of privacy.

As discussed in the previous section, it is not a difficult job to provide satisfactory user access control. However, in terms of privacy protection and user accountability, existing solutions either fail to provide user accountability (e.g., blind signature and ring signature) or fall short on user privacy protection (e.g., group signature). The state-of-the-art solutions cannot deal with the breach of user privacy as users can always be tracked (at least) by the network operator. In what follows we present a sophisticated privacy-enhanced yet accountable security framework for metropolitan WMNs, termed PEACE, which aims to provide:

- Adequate user access control: Only a legitimate user can gain network access.
- *k*-anonymity and non-linkability: The true identity of the user is hidden among a group of *k* other users, even to the network operator. The transactions from the same user cannot be linked together.
- User accountability: A user's true identity can be revealed when legally demanded and in an appropriate manner (i.e., with at least the collaboration of two network entities).

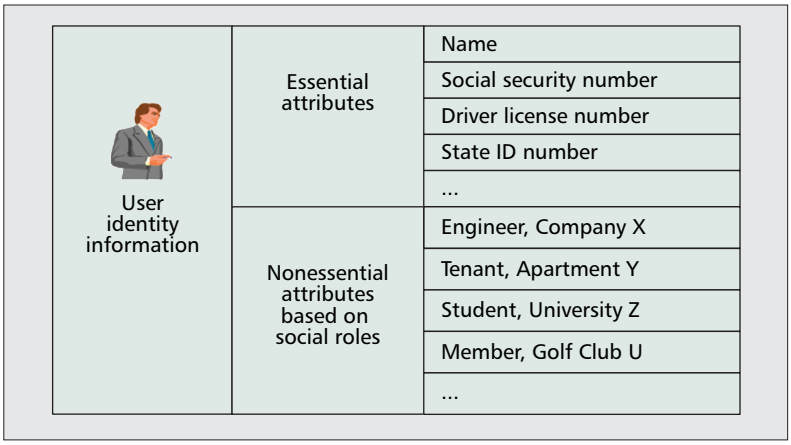


Figure 3. *The format of user identity information.*

In practice, we observe that a user typically belongs to some naturally formed social groups and usually accesses the WMN in different roles and different contexts. For example, a user as an engineer may access the WMN in his/her office as an employee of a company. The same user may also access the WMN from a university campus as a student, from a rented apartment as a tenant, from a golf club as a paid member, and so on. Based on this observation, we establish a practical user trust model that provides sophisticated user privacy credential management and addresses user accountability simultaneously. In our trust model, we hence refer to the user identity as a user's collective attribute information according to his/her different roles in society. In the above example, the *user identity* may include {*name, SSN, engineer of company X, tenant of apartment Y, student of university Z, member of golf club V*, …}.

Formally, we can divide the user identity information into two different categories, *essential attributes* and *nonessential attributes*, as shown in Fig. 3. The essential attributes include all the information that can be used to uniquely identify a specific user such as the user's name, social security number, driver license number, and passport number. On the other hand, the nonessential attributes of a user may include the different social roles as indicated in the above example. We note that if an essential attribute of a user is disclosed, this user can be uniquely identified. On the other hand, disclosing a nonessential attribute does not lead to full exposure of the user's identity. A user can still main-

Upon registration from a group manager, the network operator allocates a set of group secret keys to this user group. The network operator divides each group secret key into two parts, one part sent to the requesting group manager and the other part to the TTP.

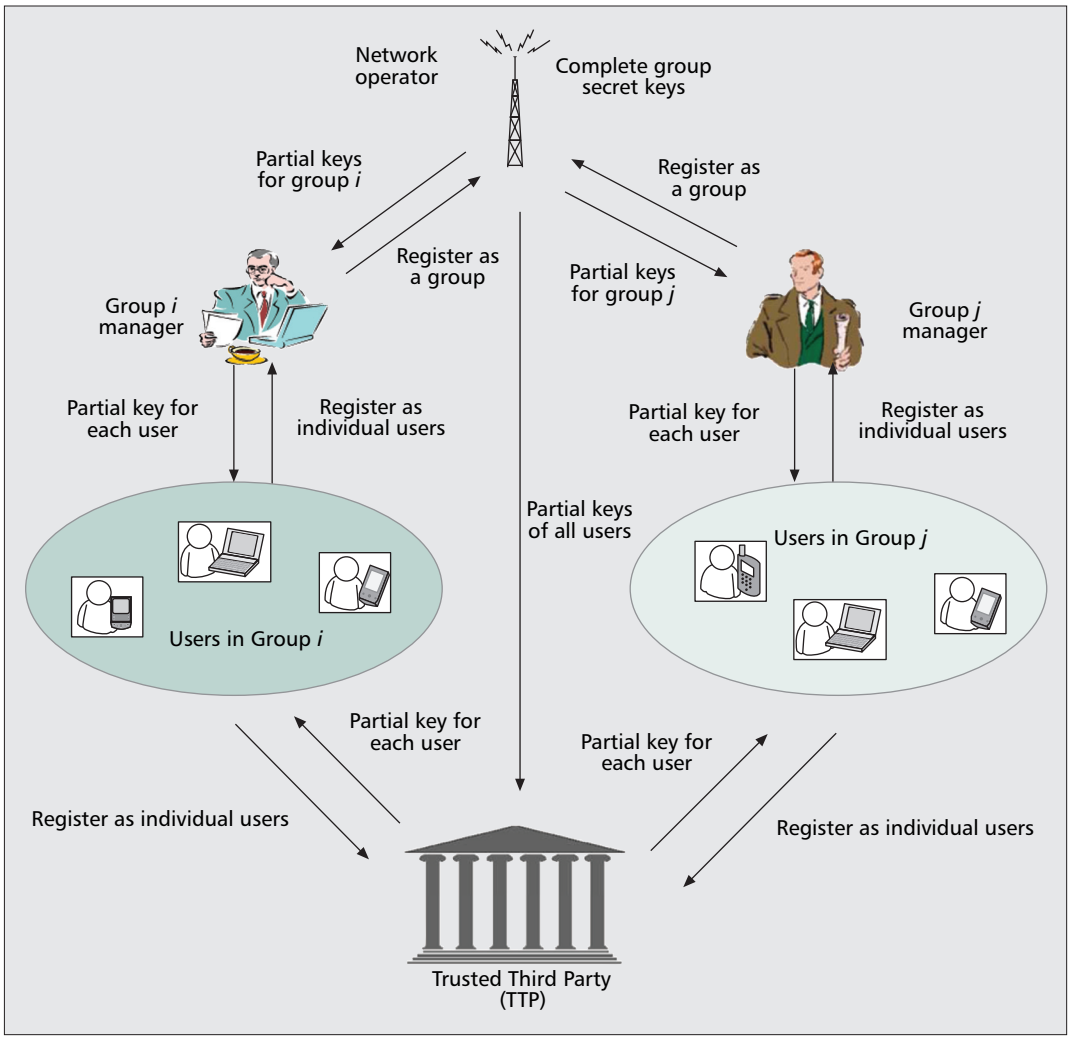


Figure 4. *PEACE trust model.*

tain a certain level of anonymity. It is further observed that nonessential attributes of users are still sufficient for accountability purposes from the network operator's perspective. This is because the network operator, when performing network access control, only cares if the requester is a legitimate user or not; it does not care who the requester is, unless there is a dispute arising from that particular access.

Figure 4 depicts a high-level illustration of the PEACE trust model, which consists of four kinds of network entities: the network operator, user group managers, users organized in groups, and a trusted third party (TTP). Each user group is a collection of users according to certain aspects of their nonessential attributes. For instance, a company is a user group consisting of all its employees, and all the tenants of an apartment building are another user group maintained by the corresponding apartment management office. Each user group has one group manager responsible for adding and removing users. Before accessing the WMN, each user has to enroll in at least one user group whose manager thus knows both the essential and nonessential attributes of the user. In PEACE, users no longer directly register with the network operator; instead, each group manager subscribes to the network operator on behalf of its group members. Upon registration from a group manager, the network operator allocates a set of group secret keys to this user group. The network operator divides each group secret key into two parts, one part sent to the requesting group manager and the other part to the TTP. To access the WMN, each user requests one part of the group secret key from the group manager and the other part from the TTP to recover the complete group secret key. The user also needs to return signed acknowledgments to both the group manager and the TTP to ensure non-repudiation of the subsequent network accesses.

The above key management scheme is based on the principle of separation of powers and possesses a number of salient features. First, from the network access control point of view, every legitimate user with a valid group secret key can generate a valid access credential (i.e., the signature of the authentication challenge, typically a nonce) upon request. The validity of this access credential can be verified by the network operator. Therefore, access security is guaranteed. Second, PEACE divides user identity information and corresponding secret key information among three autonomous entities:

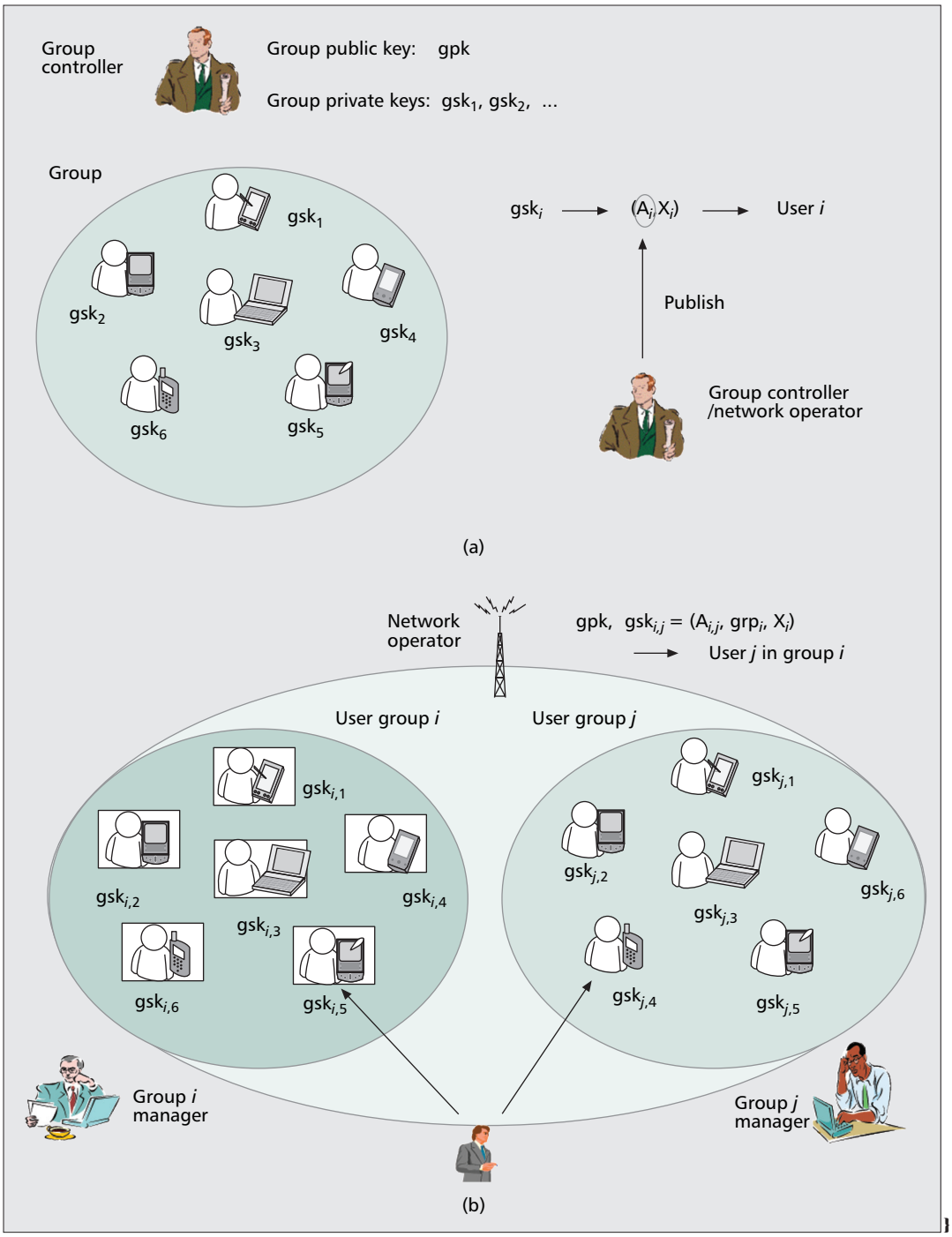


Figure 5. *Construction of access credential: a) based on Boneh's group signature scheme; b) based on our modified group signature construction.*

The system is designed in such a way that given an access credential submitted by a user, neither the the network operator, the group manager, nor the TTP can determine the user's essential attribute or compromise his privacy unless any two of them collude.

the network operator, the group manager, and the TTP. In particular, the network operator knows the complete user secret key information, but not the mapping of the keys to the essential attributes of the users; the group manager or the TTP knows the essential attributes of the users, but not the complete secret key information. The system is designed in such a way that given an access credential submitted by a user, neither the network operator, the group manager, nor the TTP can determine the user's essential attribute or compromise his/her privacy unless any two of them collude. User privacy is enhanced in this way. Last, in case of service disputes or frauds, an authorized entity such as a law enforcement authority can collect information from the network operator, the user group manager, and the TTP to precisely identify the responsible user and hold him/her accountable. Therefore, user accountability can be attained as well.

Group signature schemes lie at the heart of this design. However, the proposed framework cannot be fully realized by the direct application of the existing construction of group signature. As shown in Fig. 5a, with Boneh and Shacham's

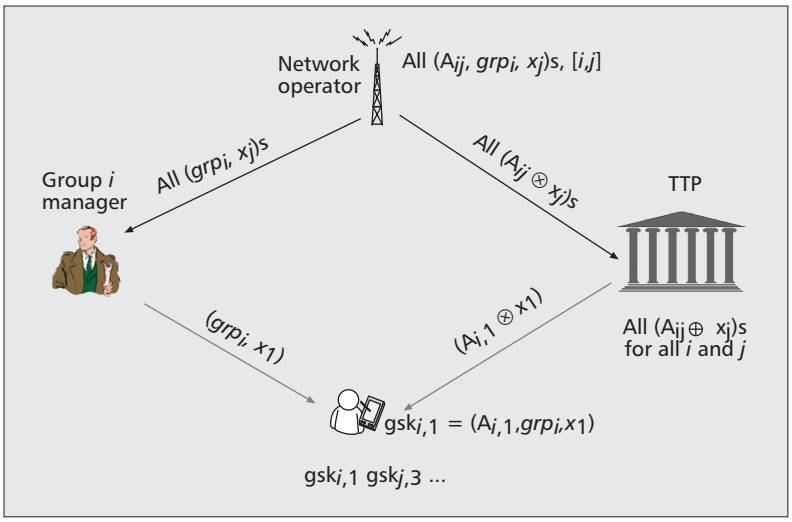


Figure 6. *Illustration of key distribution.*

scheme, the group controller keeps the mapping between each individual user i and his/her corresponding group secret key $gsk_i = (\mathbf{A}_i, \mathbf{x}_i)$, where $\mathbf{A}_i$ is computed from $\mathbf{x}_i$,a number randomly picked for each user, and the system master secret. When the group controller wants to revoke a user, he/she publishes the user's $\mathbf{A}_i$ so that every signature signed using this gsk_i can be detected and rejected. This also means that the group controller can always track the user communications by checking the related signatures. Hence, user privacy is not protected against the group controller, which is the network operator in the case of WMNs.

To deal with this problem, we propose a new construction of group signature that adapts Boneh and Shacham's group signature construction to the proposed separation of powers key management scheme. As shown in Fig. 5b, there are multiple user groups in a metropolitan WMN. Note that the same user may belong to multiple groups according to his non-essential social attributes. Each group naturally has a group manager. But from the perspective of the network operator, there is only one big lump sum group for the ease of management. The network operator prepares a group public key *gpk* that is common to all the users and also generates a large number of group secret keys for each network user with the following format, $gsk[i, j] = (\mathbf{A}_{i,j}, \mathbf{grp}_i, \mathbf{x}_j)$, where $\mathbf{grp}_i$ indicates the ID of the group which the user belongs to, and $\mathbf{A}_{i,j}$ and $\mathbf{x}_j$ have similar meaning as in the original group signature construction. Our new construction embeds user group information into their respective *gsk*. However, signing and verification algorithms are kept same when we substitute the original $\mathbf{A}_i$ with $\mathbf{A}_{i,j} + \mathbf{grp}_i$.

The new group signature construction then incarnates the separation of powers key distribution scheme as follows (Fig. 6). The network operator generates group public key *gpk*, $\mathbf{grp}_i$'s for all user groups, and $(\mathbf{A}_{i,j}, \mathbf{x}_j)$'s for all users in each group. The group secret key for an individual user j in group i thus has the format $gsk[i, j] = (\mathbf{A}_{i,j}, \mathbf{grp}_i, \mathbf{x}_j)$. The network operator further splits *gsk* into two parts. All $(\mathbf{grp}_i, \mathbf{x}_j)$s are sent to group i's manager GM_i, while all information about $\mathbf{A}_{i,j}$s is sent to TTP in the form of $(\mathbf{A}_{i,j} \oplus \mathbf{x}_j)$'s. GM_i is responsible for assigning each $(\mathbf{grp}_i, \mathbf{x}_j)$ to a particular group member j in his/her group, and keeps the mapping of the user and the corresponding partial key assigned to that user. The user needs to obtain the other part of the *gsk*, $\mathbf{A}_{i,j}$, from TTP by requesting $(\mathbf{A}_{i,j} \oplus \mathbf{x}_j)$.

It should be pointed out that in order to trace a user, one has to know the corresponding $\mathbf{A}_{i,j} + \mathbf{grp}_i$ value of the user's *gsk*. Only with such knowledge can one connect an access credential (i.e., signature generated by the user's group secret key) to the user and thus trace the user. With the proposed adaption on group signature construction, the network operator knows all three parts of a *gsk*, but does not know to whom the *gsk* is assigned, only to which group the *gsk* is assigned. So when the network operator opens a signature, it can only link the signature to the corresponding user group. Tracing to a user group is, in many cases, sufficient for user accountability purposes from the network operation perspective. So a user is hidden among all the group members to the network operator, which gives a reasonable level of anonymity, k-anonymity, from the user's perspective. However, linkability of signatures generated from the same group secret key cannot be kept from the network operator. Group manager GM_i keeps the mapping between the user and the user's corresponding $(\mathbf{grp}_i, \mathbf{x}_j)$, but has no knowledge of the corresponding $\mathbf{A}_{i,j}$, which is essential to open a signature and thus trace a user. Therefore, anonymity is achieved against the group manager as he/she has no capability to link an access credential to an essential attribute of a user. Nor can he/she link together multiple access credentials generated by the same group secret key. Therefore, non-linkability is also achieved against group managers. TTP knows a user's essential attribute, and the mapping between the user and the user's $(\mathbf{A}_{i,j} \oplus \mathbf{x}_j, \mathbf{grp}_i)$. But without knowing $\mathbf{x}_j$, TTP cannot recover $\mathbf{A}_{i,j}$, which essentially disables it from tracing a particular user by the signature he/she generated. Anonymity and non-linkability are thus achieved against the TTP as well.

In summary, in the proposed framework, with the adapted group signature scheme and the designed key distribution scheme, the link between each *gsk* and its corresponding user is not held by any network entity, be it network operator, group manager, or TTP. Anonymity is achieved against all the network entities, and linkability is only possible by the network operator, not any other network entities. However, the user identity can be revealed when disputes arise, and at least two network entities collaborate and combine their knowledge (e.g., when requested by law enforcement). Therefore, the proposed framework strikes a better balance between user accountability and privacy than the state-of-the-art solutions to privacy-preserving authentication protocols.

The proposed framework can be further developed to implement a suite of security services, including key agreement and mutual authentication with mesh routers, preventing

rogue mesh routers and phishing attacks, user revocation by the network operator publishing $(\mathbf{A}_{i,j} + \mathbf{grp}_i)$s of revoked users, and so on. Please refer to [9] for more detail.

Conclusion

Although there are plenty of good reasons to provide user privacy, numerous network-based attacks and terrorism have shifted the boundaries between public interest and the right to be left alone. In this article we address security and privacy issues in wireless access networks. Particularly, we focus on user accountability, an important aspect opposed to privacy but often overlooked in the current privacy protection research. We discuss general approaches to achieving security and privacy and their effects on user accountability. We propose a novel authentication framework that achieves enhanced user privacy protection with appropriate user accountability.

Acknowledgment

This work was supported in part by the U.S. National Science Foundation under grants CNS-0626601, CNS-0716306, CNS-0831628, and CNS-0831963.

References

[1] R. Lu *et al.*, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," *IEEE INFOCOM*, Phoenix, AZ, Apr. 2008.
[2] D. Chaum, "Blind Signatures for Untraceable Payments," *Advances in Cryptology — Crypto '82*, 1983.
[3] K. Ren *et al.*, "A Novel Privacy Preserving Authentication and Access Control Scheme for Pervasive Computing Environment," *IEEE Trans. Vehic. Tech.*, July 2006, pp. 1373–84.
[4] R. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," *ASIACRYPT*, 2001.
[5] D. Chaum and E. van Heyst, "Group Signatures," *Proc. Eurocrypt, LNCS*, vol. 547, 1991, pp. 257–65.
[6] D. Boneh and H. Shacham, "Group Signatures with Verifier-Local Revocation," *ACM CCS*, 2004, pp. 168–77.
[7] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Commun. ACM*, vol. 21, no. 2, 1978, pp. 120–26.
[8] Y. Zhang and Y. Fang, "ARSA: An Attack-Resilient Security Architecture for Multi-Hop Wireless Mesh Networks," *IEEE JSAC*, vol. 24, no. 10, Oct. 2006, pp. 1916–28.
[9] K. Ren and W. Lou, "A Sophisticated Privacy-Enhanced yet Accountable Security Framework for Wireless Mesh Networks," *28th ICDCS '08*, Beijing, China, June 2008.

Biographies

Wenjing Lou (wjlou@ece.wpi.edu) earned a Ph.D. in electrical and computer engineering from the University of Florida. She joined the Electrical and Computer Engineering Department at Worcester Polytechnic Institute as an assistant professor in 2003, where she is now an associate professor. Her current research interests are in the areas of ad hoc, sensor, and mesh networks, with emphases on network security and routing issues. She is a recipient of the U.S. National Science Foundation Faculty Early Career Development (CAREER) award in 2008.

Kui Ren (kren@ece.iit.edu) is an assistant professor in the Department of ECE, Illinois Institute of Technology. He received his Ph.D. degree from Worcester Polytechnic Institute. His current research interests include security and privacy issues in cloud computing and wireless ad hoc, sensor, and mesh network security. His research is supported by the U.S. National Science Foundation.

Although there are plenty of good reasons to provide user privacy, numerous network-based attacks and terrorism have shifted the boundaries between public interest and the right to be left alone.