SECURING RESOURCE-CONSTRAINED WIRELESS AD HOC NETWORKS

YUGUANG FANG, UNIVERSITY OF FLORIDA AND XIDIAN UNIVERSITY
XIAOYAN ZHU, XIDIAN UNIVERSITY
YANCHAO ZHANG, NEW JERSEY INSTITUTE OF TECHNOLOGY

The authors discuss a novel approach to addressing security issues and articulate why and how the ID- based cryptography can be effectively applied to address various security problems in the resource-constrained wireless networks.

ABSTRACT

Huge interest in and demand for services over the information superhighway have pressed various telecommunications research fronts and led to a new form of future Internet consisting of wired and wireless segments where resource-constrained devices such as mobile devices, smart phones, palm pilots, and wireless sensors may become integral parts of the Internet rather than access-only platforms. One of the key design problems is the security in such heterogeneous networks, particularly over wireless networks with resource constraints. In this tutorial article we discuss a novel approach to addressing security issues, and articulate why and how ID-based cryptography can be effectively applied to address various security problems in resource-constrained wireless networks.

INTRODUCTION

In the last few years we have witnessed a surge of research and development activities for wireless ad hoc networks (WANETs) such as wireless local area networks (WLANs), mobile ad hoc networks (MANETs), and wireless sensor networks (WSNs). Unlike conventional infrastructure-based wireless networks such as wireless cellular networks, WANETs feature rapidly deployable self-organizing and self-maintaining capabilities, and can be formed on the fly as needed. Due to such salient features, WANETs have naturally been deployed in emergency rescue, disaster relief, military operations, homeland security, and public safety, where fixed infrastructures are often either destroyed, unavailable, or unreliable, while fast network establishment and self-maintenance are a must. In such a network each node functions not only as an end host but also as a router, forwarding packets for other nodes to enable otherwise impossible multihop communications. WANETs can generally be classified into two main categories, mobile ad hoc networks and wireless sensor networks. The former comprises mobile nodes that are free to move and organize themselves arbitrarily, while the latter consists of a large number of sensor nodes that are more limited in power, computational capacities, and memory than nodes in MANETs [1]. Moreover, WSNs also differ from MANETs in that most sensor nodes are stationary after deployment. Recently, we have witnessed the marriage of infrastructured wireless networks and infrastructureless ad hoc networks, leading to a new flexible network architecture called wireless mesh networks (WMNs) that find many interesting applications such as high-speed Internet access, surveillance, and public safety [2]. Thus, the future Internet architecture will consist of wireless ad hoc networking segments with resource-constrained mobile nodes or sensors, and the security issues over such weakest wireless links must be addressed. However, many salient characteristics of WANETs not only pose diverse security challenges but also offer many opportunities one needs to take into account when designing security mechanisms for them [3–5]. So it is of vital importance to seek efficient and effective security mechanisms to advance the realistic deployment of WANETs.

Although wireless indeed offers us many advantages, it also poses many design challenges. Wireless channel condition is usually very poor and time-varying due to mobility, power depletion, or unpredictable interference, leading to constant transmission failures. We also face many resource limitations in terms of bandwidth, power, and computing resources. The channel environment is open, and hence potential interception or eavesdropping causes security concerns. For many WANETs, there is no trusted infrastructure in place to implement a well devel-

This work was partially supported by the National Science Foundation under grants CNS-0716450, CNS-0716302, and CNS0626881. The works of Fang and Zhu were also partially supported by the 111 Project under Grant B08038. A preliminary version of this article was presented at the IEEE Sarnoff Symposium held in Princeton, New Jersey on April 30–May 2, 2007.

1536-1284/09/$25.00 © 2009 IEEE

oped secure architecture such as public key infrastructure (PKI), which may rely on the trusted certificate authority (CA) to handle the certificate management.

Due to these various constraints, security design becomes very challenging. Security schemes for wired networks may not be feasible for WANETs; computationally intensive schemes will not work well, and power hungry operations in either computation or communications should be avoided. We have to re-evaluate the trust model, predict or investigate unconventional attacks due to the salient features of the WANETs, and come up with more appropriate strategies. In the current literature there are mainly two major approaches: symmetric and asymmetric (PKI). The former uses the same key in encryption and decryption, while the latter uses different keys. The symmetric key approach offers many advantages such as low computational overhead and no need for certificates. This is why it was favored in addressing security issues in WANETs in the past. Unfortunately, it is not scalable, and it is not easy to establish the secret key required by this approach; it tends to demand much higher communication overhead in order to make it work properly and efficiently, and it does not support the digital signature required for authentication. Moreover, it may not fare well when taking both computational and communication complexity into consideration in practical situations. On the other hand, the asymmetric key approach is scalable with easier key establishment, has a better authentication technique, and owns an embedded digital signature. Unfortunately, it is indeed computationally intensive with larger key size, and has difficult public key management and more overhead due to certificate management,which may rely on some commonly trusted infrastructure or entities in the network to be secured. Moreover, it opens new possible denial of service (DoS) attacks due to authentication and power depletion. It is not easy to decide between symmetric and asymmetric approaches in WANETs.

Inspired by the recently resurging identity-based public key cryptography (ID-PKC), we have recently developed a novel approach to addressing a number of challenging security issues in WANETs [6–10] and demonstrate why ID-PKC is a perfect fit for WANETs, and how to apply this new approach effectively. In this tutorial article we intend to present the fundamental ideas behind this approach. We articulate that the new emerging ID-based cryptography (or noninteractive cryptography) can be effectively utilized, together with the salient features of WANETs, to address such difficult security issues. As an example application, we demonstrate that the proposed approach can effectively address a few notorious attacks in WSNs with a unifying solution. It is our hope that this article can serve as a stepping stone to develop more comprehensive and viable schemes to secure our future cyberspace with wireless components. The preliminary version of this article was presented at the IEEE Sarnoff Symposium in 2007.

Why Identity-Based Cryptography?

Since our proposed schemes heavily rely on the ID-PKC, we first want to justify why this technique is a perfect fit for WANETs, specifically for MANETs and WSNs.

Identity-Based Public Key Cryptography

In traditional public key cryptosystems, a user's public key is a string not related to his/her identity; thus, there is a need to provide an assurance (or binding) about the relationship between a public key and the identity of the holder of the corresponding private key. This assurance is delivered in the form of a certificate in the traditional PKI. The PKI has to deal with the issues associated with certificate management, including revocation, storage, and distribution, and the computational costs of certificate verification, which often rely on reliable trustworthy infrastructure (certificate agency, CA). These issues are particularly acute in low-power and low-bandwidth situations (e.g., in WANETs), where the need to transmit and check certificates has been identified as a significant limitation [11]. Moreover, it is challenging to select the set of nodes in such networks to assume the duty of the CAs to efficiently manage the certificates.

PKI has to deal with the issues associated with certificate management, including revocation, storage and distribution and the computational costs of certificate verification, which often rely on reliable trustworthy infrastructure.

In 1984 Shamir proposed the idea of the ID-PKC [12], where an entity's public key can be derived directly from a certain aspect of its identity, for example, an IP address, a telephone number, or an email address associated with a user. Private keys are generated for entities by a trusted authority (TA), sometimes also called a private key generator (PKG). In contrast to conventional PKC such as RSA, the ID-PKC completely eliminates the need for public key certificates and hence for complicated certificate management. Despite its attractive features, the ID-PKC has undergone rapid development only recently [13] due to the novel application of a cryptographic technique called *pairing*, which is outlined as follows [14].

Let p, q be two large primes and $\mathsf{E}/\mathbb{F}_p$ denote an elliptic curve over the finite field $\mathbb{F}_p$ appropriately chosen for security purposes. We denote by $\mathbb{G}_1$ a q-order subgroup of the additive group of points of $\mathsf{E}/\mathbb{F}_p$, and by $\mathbb{G}_2$ a q-order subgroup of the multiplicative group of the finite field $\mathbb{F}^*_{p^2}$. When $a \in Z_q$ and $P \in \mathbb{G}_1$, we write mP for P added to itself m times, also called scalar multiplication of P by an integer m. Assume that the discrete logarithm problem (DLP) is hard[1] in both $\mathbb{G}_1$ and $\mathbb{G}_2$. From a cryptographic point of view, a pairing is a map $\hat{e}$: $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ with the following properties:

- $\hat{e}$ is *bilinear*: $\forall\ P, Q, R \in \mathbb{G}_1$.
  $\hat{e}(P + Q, R) = \hat{e}(P, R) \cdot \hat{e}(Q, R)$.
  $\hat{e}(P, Q + \mathrm{R}) = \hat{e}(P, Q) \cdot \hat{e}(P, R)$.

Consequently, for $\forall\ a, b \in Z_q$, we have $\hat{e}(aP, bQ)= \hat{e}(aP, Q)b = \hat{e}(P, bQ)a = \hat{e}(P, Q)ab$.

- $\hat{e}$ is *non-degenerate*: if P is a generator of $\mathbb{G}_1$, then $\hat{e}(P, P)$ is a generator of $\mathbb{G}_2$ In other words, $\hat{e}(P, P) \neq 1$.
- $\hat{e}$ is efficiently computable.

It is also worth pointing out that $\hat{e}$ is *symmetric*. Typically, the map $\hat{e}$ will be derived from either the (modified) Weil [14] or Tate [15] pairing on a super-singular elliptic curve over a finite

[1] *It is computationally infeasible to extract the integer* $\mathrm{x} \in \mathrm{Z}^*_{\mathrm{q}} = \{\mathrm{i} | 1 \leq \mathrm{i} \leq \mathrm{q} - 1\}$, *given* P, Q $\in \mathbb{G}_1$ *(respectively,* P, Q $\in \mathbb{G}_2$*), such that* Q = xP *(respectively,* Q = Px*).*

Due to the constraints of WANETs, in the past, it is believed that PKC is too complex, slow and power hungry to be suitable for WANETs. This opinion has led to a burst of interesting research results based on pure symmetric-key cryptography.

field. The finite field containing $\mathbb{G}_2$ as a subgroup typically uses a security parameter k, which is the same for most popular public key cryptographic systems, such as RSA or discrete-logarithm-based systems, sto obtain a degree of security protection similar to that in those popular public key cryptographic systems. Therefore, the cost of computing a bilinear pairing is similar to that of computing a public key cryptographic operation in those popular cryptographic systems [16].

Fast hardware implementations of the pairing have been reported recently [17, 18]. For example, it is reported in [18] that the Tate pairing can be calculated in about 6 ms on a field programmable gate array (FPGA). We refer readers to [14, 15, 19] for a more comprehensive description of how these groups, pairings, and other parameters should be selected in practice for efficiency and security.

To bootstrap a pairing-based ID-PKC cryptosystem, a TA runs some initialization function on an input, the security parameter k, to generate a prime q, two suitable groups $\mathbb{G}_1$, $\mathbb{G}_2$ of order q, a bilinear map $\hat{e}$, and an arbitrary generator $P \in \mathbb{G}_1$. The TA then selects a random key $s \in Z_q$ as its *master secret* and sets $P_{\text{pub}} = sP$. Upon a key registration request from an entity x whose identity we denote ID_x, the TA issues a private key $S_x = sH_1(ID_x)$, where H_1 is a cryptographic hash function deterministically mapping strings in $\{0, 1\}^*$ onto $\mathbb{G}_1$ Under the hardness assumption of the discrete logarithm in $\mathbb{G}_1$, it is hard to find the master key s of the TA from the public/private key pair (ID_x,S_x). In addition, parameters $\langle \mathbb{G}_1, \mathbb{G}_2, H_1, P, P_{\text{pub}} \rangle$ are publicly known, while the TA should well safeguard and prevent unauthorized access to its master secret s. In MANETs and WSNs, the TA can be the system administrator or network planner who usually does not appear in the resulting network operations; that is, a TA is used only before the network deployment.

Many efficient cryptographic primitives have been proposed recently on how to leverage identity-based public/private key pairs to realize essential public key operations such as encryption/decryption and signature generation/verification [13, references therein]. The security of most existing ID-PKC schemes depends on the difficulty of solving the bilinear Diffie-Hellman problem (BDHP): given $\langle P, xP, yP, zP \rangle$ with random $x, y, z \in Z_q^*$ and $P \in \mathbb{G}_1$, there is no q algorithm running in expected polynomial time, which can compute $\hat{e}(P, P)xyz$ with non-negligible probability [13].

Suitability of ID-PKC to Wireless Ad Hoc Networks

How to establish a shared secret key between any two or more communicating nodes for subsequent cryptographic use is a fundamental problem of the security study in WANETs. Due to the constraints of WANETs, in the past it was believed that PKC was too complex, slow, and power hungry to be suitable for WANETs. This opinion has led to a burst of interesting research results based on pure symmetric key cryptography [20–24]. However, the inherent limitations of symmetric key cryptography mean these proposals suffer from the lack of authentication, scalability, and resilience to node compromise discussed earlier.

Although ID-PKC has comparable computational efficiency to that of conventional PKC [16], there are at least *three significant advantages* of ID-PKC over conventional PKC. First, ID-PKC removes the need for certificates, and hence certificate distribution and verification. Considering the resource- constrained nature of WANETs, this often represents nontrivial savings in both communication and computation overheads, especially in large-scale WANETs. Second, ID-PKC facilitates noninteractive key agreement. Computationally expensive public key techniques are often used to establish a shared key between two communication entities, based on which subsequent communications can be secured with computationally more efficient symmetric key techniques. Traditional shared key establishment based on conventional PKC requires message exchange between two parties. By contrast, any two parties, if both have an authentic public/private pair from the same TA based on ID-PKC, have already shared a secret key without exchanging any message. For example, suppose nodes x with identity ID_x and y with identity ID_y have obtained their respective private keys $S_x = sH_1(ID_x)$ and $S_y = sH_1(ID_y)$ from the same TA during network initialization. They can calculate the shared key between them as

$$\begin{aligned} K_{xy} &= \hat{e}(S_x, H_1(ID_y)) \\ &= \hat{e}(sH_1(ID_x), H_1(ID_y)) \\ &= \hat{e}(H_1(ID_x), H_1(ID_y))^s \\ &= \hat{e}(H_1(ID_x), sH_1(ID_y)) \\ &= \hat{e}(H_1(ID_x), S_y) = \hat{e}(S_y, sH_1(ID_x)) \\ &= K_{yx} \end{aligned}$$

Due to the difficulty of solving the BDHP, K_{xy} is exclusively available to nodes x and y without counting on the TA, which usually does not appear in the network. This method of *identity-based noninteractive* shared key establishment is reported in [25] and obviously can further reduce both communication and computation overheads, which is obviously desirable in resource-constrained WANETs. This is particularly important when we realize that the proposed ID-based schemes do not rely on any trustworthy entities or interactions with trusted entities in order to exchange shared key materials during network operation (certificate management); hence, ID-PKC is a perfect fit for WANETs in which there is generally a lack of commonly trustworthy entities. Finally, the fact that any type of string can be a public key in ID-PKC provides many useful properties that do not exist with conventional PKC. For instance, if one wants to talk to Gator at the University of Florida, Gator's public key can be in the form "*GatorID* || University of Florida" where || denotes the concatenation of messages. In so doing, when we send a message to *Gator*, only *Gator* at the University of Florida can decrypt the message. This is difficult, if not impossible, to achieve in a conventional public key cryptosystem, in which a source has to obtain the destination's authenticated public key before actually sending encrypted messages. This idea can be further extended by including even more information in the public key, such as some confidentiality specification, to realize many other interesting applications [14].

Despite its attractive features, ID-PKC has not received the attention it deserves as a powerful tool to secure WANETs until recently. Khalili *et al*. [26] suggested the possible application of ID-PKC combined with the secret sharing technique [27]. Deng *et al*. [28] proposed an identity-based key management scheme for MANETs. Moreover, Bohio and Miri [29] proposed to use identity-based keys for securing MANET broadcast communications. As an addition, Saxena *et al*. [30] applied ID-PKC to realize access control for ad hoc network groups such as peer-to-peer (P2P) systems and MANETs, and demonstrated with experimental results the superiority of ID-PKC over conventional certificate-based PKC in MANETs. Recently, we have developed several security schemes based on ID-PKC and demonstrated their effectiveness in addressing security issues in WANETs [7–10, 31].

In summary, although ID-PKC cannot completely replace conventional certificate-based PKC under all circumstances, it does provide more efficient, lightweight, and flexible solutions in many application scenarios such as resource-constrained WANETs.

Securing Wireless Sensor Networks

To demonstrate the effective use of ID-PKC, we take WSNs as an example application. One kind of WSN is area monitoring for potential enemy intrusion. Sensors are deployed in the area of interest. Whenever there is any intrusion detected, a warning message is used to report the event via possibly multihop communications to the remote monitoring center or a base station so that appropriate actions can be taken.

In this setting, in order to securely send a report from a node sensing an intrusion, the following issues have to be carefully addressed. Nodes have to be able to authenticate each other to make sure that the report is not from the intruder; when the report is transmitted, it should not be detected by the intruder; it should be guaranteed that the report was not tampered with during delivery; and the designed security scheme should resist various serious attacks such as Sybil, node duplication, random walk, wormhole, and bogus message injection attacks. There are many separate solutions to addressing the aforementioned issues; however, it is difficult to combine them due to different or even conflicting underlying assumptions. Even if it is possible to combine some of them, it is far too complex to implement for WSNs. Moreover, most prior solutions do not work well even when a small number of nodes are compromised by attackers. More important, many solutions address one problem while inducing others. Finally, most schemes apply the symmetric key approach and reduce computational cost; unfortunately, they tend to dramatically increase the communications cost, which is often ignored by many in their performance evaluation.

In order to come up with a unifying and effective solution to the aforementioned security issues, we have to utilize the salient feature of WSNs. We observe that almost all WSN applications are location-dependent and require a sensor node to know its own location, as in military sensing and tracking. Most sensor nodes are stationary once deployed and can be identified by their IDs plus their locations. Moreover, most sensor nodes have a limited communication range and can only directly communicate with others inside their communication range. Based on these features, we propose a novel location-based security solution, demonstrated next [8].

The authors propose a novel location-based security solution. The basic idea of their location-based approach is as follows. Name a node with both an ID and its location and thus bind the ID and location together.

The basic idea of our location-based approach is as follows. Name a node with both an ID and its location, and thus bind the ID and location together. We do this because of the observation that "*Michael@UF*" will be more specific than "*Michael*." If we let ID_A and L_A indicate the ID and location of sensor node A, respectively, we can assign the public-private key pair as $(ID_A@L_A, K_A)$ where $K_A = sH_1(ID_A@L_A)$, the location-based key (LBK) corresponding to the ID-location pair $ID_A@L_A$, and s is the sensor network master secret key known only to the TA (i.e., the sensor network owner), which is never exposed to the sensor network field. According to ID-based cryptography, each sensor node can only know its own private key, but not the master secret key, and any two sensors could establish a shared key without exchanging any secret material. Next, we want to demonstrate how we can address a few other security issues with this unifying approach.

To mutually authenticate each other, node A transmits to B an authentication request with its location L_A and a random nonce n_A. Upon receiving this request, node B with location L_B first checks whether the claimed location L_A is indeed in its transmission range (i.e., the distance check). If the check fails, node B simply discards the request and determines that node A is not an authentic neighbor. Otherwise, B replies with its own location L_B, a random nonce n_B, and an authenticator V_B calculated as

$$V_B = H_2(\hat{e}(K_B, H_1(ID_A@L_A)) \parallel n_A \parallel n_B \parallel 0),$$

where H_2 is another hash function. Once it has received B's reply, node A can determine whether B is in its transmission range based on the provided L_B If not, the authentication fails. Otherwise, A proceeds to compute a verifier V'_B as

$$V'_B = H_2(\hat{e}(K_A, H_1(ID_B@L_B)) \parallel n_A \parallel n_B \parallel 0).$$

According to the bilinearity of the pairing $\hat{e}$, if and only if both A and B have the authentic LBKs corresponding to their claimed locations can they have

$$\hat{e}(K_B, H_1(ID_A@L_A)) = \hat{e}(K_A, H_1(ID_B@L_B)) = \hat{e}(H_1(ID_B@L_B)),H_1(ID_A@L_A))^s \in \mathbb{G}_2.$$

After verifying the equality of V'_B and V_B, A can ascertain that B is an authentic neighbor with the claimed location L_B. Node A then sends to B its own authenticator V_A computed as

$$V_A = H_2(\hat{e}(K_A, H_1(ID_B@L_B)) \parallel n_A \parallel n_B \parallel 1).$$

Many resource-constrained networks such as wireless ad hoc networks rely on cooperation. How to take advantage of the cooperative nature in the ID-based security approach is under research.

By a simple calculation, node *B* can determine whether *A* is an authentic neighbor with the claimed location L_A using a similar approach as demonstrated for node *B*. Based on this three-way handshaking, nodes *A* and *B* can achieve mutual authentication and establish a secure link between them.

With this location-based ID-PKC approach, our scheme can defend effectively against the aforementioned security attacks. When an adversary launches a Sybil attack, the only possible way is to compromise one legitimate node to recover the private key first, then substitute the ID with its own [32, 33]. However, when other nodes receive the authentication request from the adversary, the ID-location pair will not match that used to generate the private key; hence, the authentication will fail, and the Sybil attack will not be effective. In a node duplication attack or random walk attack, an adversary, when compromising a node, will either duplicate the compromised node in other places or move around in the sensor network to gain communication with other nodes using the compromised secret material (the private key) [33]. Our location-based key approach will localize the damage of such attacks within the neighborhood of the compromised node because whenever the adversary moves out of that neighborhood, the authentication will fail because the distance check fails. In a wormhole attack adversaries could relay an authentication request to make two faraway nodes think they are neighbors [32]. Our approach can also easily defeat this attack because the authentication will fail due to either the failure of the distance check or the mismatch of the ID-location pair provided with those used to generate the private LBKs. To guard against bogus message injection, the whole sensor network is divided into different areas covering multiple sensor nodes. Each area is equipped with a private area LBK for report signature, and each sensor node in this area is given a partial share of the area LBK based on the secret sharing scheme in such a way that only when a preset number, say *t*, shares are obtained can the area LBK be recovered. Thus, if we require all event reports to be signed by at least *t* sensors in the area for validity, the adversary has to compromise at least *t* sensor nodes in an area in order to recover the area key to sign its injected messages. Without the area signature, the injected message will be filtered out en route to the BS. The detail can be found in [8]. In conclusion, our location-based security approach indeed provides a unifying and effective security scheme.

Conclusions and Future Research Directions

ID-PKC has indeed found many interesting applications in which a traditional approach may not be effective. In this article we attempt to demonstrate the advantages of ID-PKC in resource-constrained wireless ad hoc networks and hope to inspire more research on this approach. There are many challenging research problems ahead. One of the obstacles is the computational complexity of the pairing operations, which is still under intensive research. In most research we have carried out, we assume that the network in consideration is homogeneous, yet there are many networks that are inheritably heterogeneous, and how to tackle the security issues using ID-PKC is still open. Finally, many resource-constrained networks such as wireless ad hoc networks rely on cooperation. How to take advantage of this cooperative nature in the ID-based security approach is under research.

References

[1] I. Akyildiz *et al*., "A Survey on Sensor Networks," *IEEE Commun. Mag*., vol. 40, no. 8, Aug. 2002, pp. 102–16.

[2] Akyildiz, X. Wang, and W. Wang, "Wireless Mesh Networks: A Survey," *Comp. Net.*, Mar. 2005.

[3] Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," *IEEE Sec. & Privacy*, vol. 2, no. 3, May–June 2004, pp. 28–39.

[4] W. Lou and Y. Fang, "A Survey on Wireless Security in Mobile Ad Hoc Networks: Challenges and Possible Solutions," in *Ad Hoc Wireless Networking* (Springer Network Theory and Applications Series), vol. 14, X. Chen, X. Huang, and D.-Z. Du, Eds., Kluwer/Springer, 2004.

[5] H. Yang *et al*., "Security in Mobile Ad Hoc Networks: Challenges and Solutions," *IEEE Wireless Commun*., vol. 11, no. 1, Feb. 2004, pp. 38–47.

[6] Y. Zhang and Y. Fang, "A Secure Authentication and Billing Architecture for Wireless Mesh Networks," *ACM Wireless Net*., vol. 13, no. 5, Oct. 2007, pp. 569–82.

[7] 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.

[8] Y. Zhang *et al*., "Location-based Security Mechanisms in Wireless Sensor Networks," *IEEE JSAC*, vol. 24, no. 2, Feb. 2006, pp. 247–60.

[9] Y. Zhang *et al*., "MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks," *IEEE Trans. Wireless Commun*., vol. 5, no. 9, Sept. 2006, pp. 2376–85.

[10] Y. Zhang *et al*., "Securing Mobile Ad Hoc Networks with Certificateless Public Keys," *IEEE Trans. Dependable Secure Comp*., vol. 3, no. 4, Oct.–Dec. 2006, pp. 386–99.

[11] S. Al-Riyami and K. Paterson, "Certificateless Public Key Cryptography," *Proc. AsiaCrypt '03*, LNCS 2894, Springer-Verlag, 2003, pp. 452–73.

[12] A. Shamir, "Identity Based Cryptosystems and Signature Schemes," *Proc. CRYPTO '84*, LNCS 196, Springer-Verlag, 1984, pp. 47–53.

[13] R. Dutta, R. Barua, and P. Sarkar, "Pairing-based Cryptography: A Survey," *Cryptology ePrint Archive*, rep. 2004/064, 2004.

[14] D. Boneh and M. Franklin, "Identify-based Encryption from the Weil Pairing," *Proc. CRYPTO '01*, LNCS 2139, Springer-Verlag, 2001, pp. 213–29.

[15] P. Barreto, H. Kim, B. Bynn, and M. Scott, "Efficient Algorithms for Pairing-Based Cryptosystems," *Proc. CRYPTO '02*, LNCS 2442. Springer-Verlag, 2002, pp. 354–68.

[16] W. Mao, "An Identity-Based Non-Interactive Authentication Framework for Computational Grids," Hewlett-Packard Labs. tech. rep. HPL-2004-96, June 2004.

[17] T. Kerins *et al*., "Efficient Hardware for the Tate Pairing Calculation in Characteristic Three," *Cryptology ePrint* archive, rep. 2005/065, 2005; http://eprint.iacr.org/2005/065

[18] T. Kerins *et al*., "A Hardware Accelerator For Pairing Based Cryptosystems," submitted preprint, 2005; http://paginas.terra.com.br/informatica/paulobarreto

[19] P. Barreto, B. Lynn, and M. Scott, "On the Selection of Pairing-Friendly Groups," *Sel. Areas Cryptography 2003*, LNCS 3006, Springer-Verlag, 2004, pp. 17–25.

[20] L. Eschenauer and V. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," *Proc. ACM CCS*, Washington, DC, Nov. 2002.

[21] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," *IEEE Symp. Sec. & Privacy*, Oakland, CA, May 2003.

[22] W. Du *et al*., "A Pairwise Key Pre-Distribution Scheme for Wireless Sensor Networks," *Proc. ACM CCS*, Washington, DC, Oct. 2003.

[23] D. Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks," *Proc. ACM CCS*, Washington, DC, Oct. 2003.

[24] D. Liu and P. Ning, "Location-based Pairwise Key Establishments for Static Sensor Networks," *Proc. ACM SASN*, Fairfax, VA, Oct. 2003.

[25] R. Sakai, K. Ohgishi, and M. Kasahara, "Cryptosystems

Based on Pairing," *Proc. 2000 Symp. Cryptography Info. Sec.*, Okinawa, Japan, Jan. 2000.

[26] A. Khalili, J. Katz, and W. Arbaugh, "Toward Secure Key Distribution in Truly Ad-Hoc Networks," *IEEE Wksp. Secu. Assurance Ad Hoc Net.*, Orlando, FL, Jan. 2003.

[27] A. Shamir, "How to Share a Secret," *Commun. ACM*, vol. 22, no. 11, 1979, pp. 612–13.

[28] H. Deng, A. Mukherjee, and D. Agrawal, "Threshold and Identity-Based Key Management and Authentication for Wireless Ad Hoc Networks," *Int'l. Conf. Info. Tech.: Coding Comp. '04*, Las Vegas, NV, Apr. 2004.

[29] M. Bohio and A. Miri, "Efficient Identity-Based Security Schemes for Ad Hoc Network Routing Protocols," *Elsevier Ad Hoc Net. J.*, vol. 2, no. 3, 2004, pp. 309–17.

[30] N. Saxena, G. Tsudik, and J. H. Yi, "Identity-Based Access Control for Ad Hoc Groups," *Proc. Int'l. Conf. Info. Sec. Cryptology*, Seoul, Korea, Dec. 2004.

[31] J. Sun, C. Zhang, and Y. Fang, "A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks," *Proc. 27th IEEE INFOCOM '08*, Phoenix, AZ, Apr. 13–18 2008.

[32] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *Ad Hoc Net.*, vol. 1, no. 2, 2003.

[33] J. Newsome *et al.*, "The Sybil Attack in Sensor Networks: Analysis & Defenses," *Proc. 3rd IPSN '04*, Berkeley, CA, Apr. 2004.

Biographies

YUGUANG FANG [F'08] (fang@ece.ufl.edu) received a Ph.D. degree in systems engineering from Case Western Reserve University in January 1994 and a Ph.D. degree in electrical engineering from Boston University in May 1997. He was an assistant professor in the Department of Electrical and Computer Engineering at New Jersey Institute of Technology from July 1998 to May 2000. He then joined the Department of Electrical and Computer Engineering at the University of Florida in May 2000 as an assistant professor, got an early promotion to associate professor with tenure in August 2003, and became a full professor in August 2005. He holds a University of Florida Research Foundation (UFRF) Professorship from 2006 to 2009 and a Changjiang Scholar Chair Professorship from 2008 to 2011 with Xidian University, Xi'an, China. He has published over 250 papers in refereed professional journals and conferences, and won the Best Paper Award at the 2006 International Conference on Network Protocols and at IEEE GLOBECOM 2002. He received the National Science Foundation Faculty Early Career Award in 2001 and the Office of Naval Research Young Investigator Award in 2002. He is currently serving as the Editor-in-Chief of *EEE Wireless Communications* and has served on several editorial boards of technical journals including *IEEE Transactions on Communications*, *IEEE Transactions on Wireless Communications*, *IEEE Transactions on Mobile Computing*, *IEEE Wireless Communications*, and *ACM Wireless Networks*. He has also actively participiatied in professional conference organizations such as serving as Technical Program Vice-Chair for IEEE INFOCOM 2005, Technical Program Symposium Co-Chair for IEEE GLOBECOM 2004, and a member of the Technical Program Committee for IEEE INFOCOM (1998, 2000, 2003–2007) and ACM Mobihoc (2008–2009).

XIAOYAN ZHU (xyzhu@mail.xidian.edu.cn) received her B.E. degree in information engineering in July 2000 and her M.E. degree in information and communications engineering in March 2004, both from Xidian University. She is now working toward her Ph.D. degree at Xidian University. Her research interests include wireless security and network coding.

YANCHAO ZHANG [M'06] (yczhang@njit.edu) received his B.E. degree in computer communications from Nanjing University of Posts and Telecommunications, China, in July 1999, an M.E. degree in computer applications from Beijing University of Posts and Telecommunications in April 2002, and a Ph.D. degree in electrical and computer engineering from the University of Florida, Gainesville, in August 2006. He is currently an assistant professor in the Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark. His research interests include network and distributed system security, wireless networking, and mobile computing.