

# Securing Resource-Constrained Wireless Ad Hoc Networks

Yuguang Fang, *Fellow, IEEE*, Xiaoyan Zhu, and Yanchao Zhang, *Member, IEEE*

**Abstract**—Huge interest and demand on services over 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 paper, we 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.

**Index Terms**—Wireless ad hoc networks, wireless security, ID-based cryptography, pairing.

## I. 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

This work was partially supported by the National Science Foundation under grants CNS-0716450, CNS-0716302 and CNS-0626881. The works of Fang and Zhu were also partially supported by the 111 Project under Grant B08038. A preliminary version of this paper was presented at the IEEE Sarnoff Symposium held in Princeton, New Jersey on April 30-May 2, 2007.

Y. Fang is with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611, USA, and also with the National Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China (e-mail: fang@ece.ufl.edu).

X. Zhu is with the National Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China (e-mail: xyzhu@mail.xidian.edu.cn).

Y. Zhang is with the Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark, NJ 07102, USA (e-mail: yczhang@njit.edu).

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, not available or not reliable, 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 multi-hop communications. WANETs can be generally classified into two main categories, namely, 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 as compared to 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 wireless ad hoc networks.

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 or power depletion or unpredictable interference, leading to constant transmission failures. We also face many resource limitation 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 are no trusted infrastructure in place to implement the well-developed 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 wireless ad hoc networks, 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 non-conventional 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 approach and asymmetric key approach (PKI). The former uses the same key in encryption and decryption while the latter uses different keys. Symmetric key approach does offer many advantages such as low computational overhead and no need for certificate. This is why this approach was favored in addressing security issues in WANETs in the past. Unfortunately, it is not scalable and not easy to establish the secret key required by this approach, tends to demand much higher communication overhead in order to make it work properly and efficiently, and does not support 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, asymmetric key approach is scalable with easier key establishment, has better authentication technique, and owns embedded digital signature. Unfortunately, it is indeed computationally intensive with larger key size, has difficult public key management and more overheads 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 attack. It is not an easy decision to make between symmetric key approach and asymmetric approach 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 paper, we intend to present the fundamental ideas behind this approach. We articulate that the new emerging ID-based cryptography (or the non-interactive cryptography) can be effectively utilized, together with the salient features of the WANETs, to address such difficult security issues. As an exemplar application, we demonstrate that the proposed approach can effectively address a few notorious attacks in the WSNs with a unifying solution. It is our high hope that this paper 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 paper was presented at the IEEE Sarnoff Symposium in 2007.

## II. WHY IDENTITY-BASED CRYPTOGRAPHY?

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

### A. Identity-Based Public-Key Cryptography

In the traditional public-key cryptosystems, a user's public key is a string not related to his/her identity and 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 certificate in the traditional Public Key Infrastructure (PKI). 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 or CA). These issues are particularly acute in low-power and low-bandwidth situations, for example, 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.

In 1984, Shamir proposed the idea of the ID-PKC [12], where an entity's public key can be derived directly from 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 the complicated certificate management. Despite its attractive features, the ID-PKC has undergone a 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  $E/\mathbb{F}_p$  denote an elliptic curve over the finite field  $\mathbb{F}_p$  appropriately chosen for security purpose. We denote by  $\mathbb{G}_1$  a  $q$ -order subgroup of the additive group of points of  $E/\mathbb{F}_p$ , and by  $\mathbb{G}_2$  a  $q$ -order subgroup of the multiplicative group of the finite field  $\mathbb{F}_{p^2}^*$ . When  $a \in \mathbb{Z}_q$  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<sup>1</sup> 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*:  $\forall P, Q, R \in \mathbb{G}_1$ ,

$$\hat{e}(P + Q, R) = \hat{e}(P, R) \cdot \hat{e}(Q, R)$$

$$\hat{e}(P, Q + R) = \hat{e}(P, Q) \cdot \hat{e}(P, R).$$

Consequently, for  $\forall a, b \in \mathbb{Z}_q$ , 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 supersingular elliptic curve over a finite field. The finite field containing  $\mathbb{G}_2$  as a subgroup typically uses a security parameter  $k$  which is the same as that for most popular public-key cryptographic systems, such as RSA or discrete-logarithm based systems, so as to 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 FPGA. We refer the 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.

<sup>1</sup>It is computationally infeasible to extract the integer  $x \in \mathbb{Z}_q^* = \{i | 1 \leq i \leq q - 1\}$ , given  $P, Q \in \mathbb{G}_1$  (respectively,  $P, Q \in \mathbb{G}_2$ ) such that  $Q = xP$  (respectively,  $Q = P^x$ ).

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  $s \in \mathbb{Z}_q$  as its *master secret* and sets  $P_{pub} = sP$ . Upon a key registration request from an entity  $x$  whose identity we denote by  $ID_x$ , 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  $\langle \mathbb{G}_1, \mathbb{G}_2, H_1, P, P_{pub} \rangle$  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 the network planner who usually does not appear in the resulting network operations, i.e., 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 (see [13] and the 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  $x, y, z \in \mathbb{Z}_q^*$  and  $P \in \mathbb{G}_1$ , there is no algorithm running in expected polynomial time, which can compute  $\hat{e}(P, P)^{xyz}$  with non-negligible probability [13].

## B. 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 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, such as [20]–[24]. However, the inherent limitations of symmetric-key cryptography render these proposals suffer from the lack of authentication, scalability and resilience to node compromise as we also discussed before.

Although ID-PKC has comparable computational efficiency to that of the conventional PKC [16], there are at least **three significant advantages** of ID-PKC

over the conventional PKC. First, ID-PKC removes the need for certificates and hence the certificate distribution and verification. Considering the resource-constrained nature of WANETs, this often represents non-trivial savings in both communication and computation overheads, especially in large-scale WANETs. Second, ID-PKC facilitates non-interactive key agreement. It is a common practice that 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 the 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 the 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 from the same TA their respective private key  $S_x = sH_1(ID_x)$  and  $S_y = sH_1(ID_y)$  during the network initialization. They can calculate the shared key between them as

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

Due to the difficulty of solving the BDHP,  $K_{xy}$  is exclusively available to nodes  $x$  and  $y$  without counting on the TA that usually does not appear in the network. This method of *identity-based, non-interactive* 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 the network operation (certificate management), hence ID-PKC is a perfect fit for WANETs in which there is generally 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 the conventional PKC. For instance, if one wants to talk to Gator at the University of Florida, then 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*, then only *Gator* at the University of Florida can decrypt the message. This is difficult, if not impossible, to achieve in the 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 deserved attention 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 the conventional certificate-based PKC in MANETs. Recently, we have developed several security schemes based on the ID-PKC and demonstrated their effectiveness in addressing security issues in WANETs [7]–[10], [31].

In summary, although the 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 the resource-constrained WANETs.

### III. SECURING WIRELESS SENSOR NETWORKS

To demonstrate the effective use of the ID-PKC, we take the wireless sensor networks as an exemplar application. One kind of WSNs is the area monitoring for potential enemy intrusion. Sensors are deployed in the area of interest. Whenever there is any intrusion detected, a warning message will be used to report the event via possibly multiple-hop 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 few 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; the report should

be guaranteed that it was not tampered with during the delivery; and the designed security scheme should resist various serious attacks such as Sybil attack, node duplication attack, random walk attack, wormhole attack and bogus message injection attack. 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 be implemented for WSNs. Moreover, most prior solutions do not work well even when a small number of nodes are compromised by attackers. More importantly, many solutions address one problem while inducing other problems. Finally, most schemes apply the symmetric key approach and do reduce the 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. As 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 as we demonstrate next [8].

The basic idea of our location-based approach is as follows: name a node with both ID and its location and thus bind both the ID and the location together. The reason 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 the location of sensor node  $A$ , respectively, then 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 Trusted Authority (TA) (i.e., the sensor network owner), which is never exposed to the sensor network field. According to the 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 check 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 determine 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 receiving  $B$ '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

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

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

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

By a simple calculation, node  $B$  can determine whether  $A$  is an authentic neighbor with the claimed location  $L_A$  using a similar approach we demonstrated for node  $B$ . Based on this three-way handshaking, nodes  $A$  and  $B$  can achieve mutual authentication and establish an 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 hence the Sybil attack will not be effective. In the 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 that neighborhood, the authentication will fail because the distance check fails. In the wormhole attack, adversaries could relay 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 the way that only when a preset number, say  $t$ , shares are obtained, can the area LBK be recovered. Thus, if we require all event report be signed by at least  $t$  sensors in the area for its 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.

#### IV. CONCLUSIONS AND FUTURE RESEARCH DIRECTIONS

ID-based Public Key Cryptography (ID-PKC) indeed has found many interesting applications in which traditional approach may not be effective. In this paper, we attempt to demonstrate the advantages of the 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 the ID-PKC is still open. Finally, 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.

#### REFERENCES

- [1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–116, Aug. 2002.
- [2] I. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: A survey," *Computer Networks*, Mar. 2005.
- [3] Hu and A. Perrig, "A survey of secure wireless ad hoc routing," *IEEE Security & Privacy*, vol. 2, no. 3, pp. 28–39, May-June 2004.
- [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)*, edited by X. Chen, X. Huang and D.-Z. Du, Kluwer Academic Publishers/Springer, 2004.
- [5] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: Challenges and solutions," *IEEE Wireless Commun. Mag.*, vol. 11, no. 1, pp. 38–47, Feb. 2004.
- [6] Y. Zhang and Y. Fang, "A secure authentication and billing architecture for wireless mesh networks," *ACM Wireless Networks*, vol. 13, no. 5, pp. 569–582, October 2007.
- [7] —, "ARSA: an attack-resilient security architecture for multi-hop wireless mesh networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 10, pp. 1916–1928, October 2006.
- [8] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-based security mechanisms in wireless sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 247–260, February 2006.
- [9] —, "MASK: anonymous on-demand routing in mobile ad hoc networks," *IEEE Transactions on Wireless Communications*, vol. 5, no. 9, pp. 2376–2385, September 2006.
- [10] —, "Securing mobile ad hoc networks with certificateless public keys," *IEEE Transactions on Dependable and Secure Computing*, vol. 3, no. 4, pp. 386–399, October-December 2006.
- [11] S. Al-Riyami and K. Paterson, "Certificateless public key cryptography," in *Proc. AsiaCrypt'03*, ser. LNCS, vol. 2894. Springer-Verlag, 2003, pp. 452–473.
- [12] A. Shamir, "Identity based cryptosystems and signature schemes," in *Proc. CRYPTO'84*, ser. LNCS, vol. 196. Springer-Verlag, 1984, pp. 47–53.
- [13] R. Dutta, R. Barua, and P. Sarkar, "Pairing-based cryptography : A survey," *Cryptology ePrint Archive Report 2004/064*, 2004.
- [14] D. Boneh and M. Franklin, "Identify-based encryption from the weil pairing," in *Proc. CRYPTO'01*, ser. LNCS, vol. 2139. Springer-Verlag, 2001, pp. 213–229.
- [15] P. Barreto, H. Kim, B. Bynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," in *Proc. CRYPTO'02*, ser. LNCS, vol. 2442. Springer-Verlag, 2002, pp. 354–368.
- [16] W. Mao, "An identity-based non-interactive authentication framework for computational grids," *Hewlett-Packard Laboratories, Technical Report HPL-2004-96*, June 2004.
- [17] T. Kerins, W. Marnane, E. Popovici, and P. Barreto, "Efficient hardware for the Tate pairing calculation in characteristic three," *Cryptology ePrint Archive, Report 2005/065*, 2005. [Online]. Available: <http://eprint.iacr.org/2005/065>

- [18] —, “A hardware accelerator for pairing based cryptosystems,” submitted preprint, 2005. [Online]. Available: <http://paginas.terra.com.br/informatica/paulobarreto>
- [19] P. Barreto, B. Lynn, and M. Scott, “On the selection of pairing-friendly groups,” in *Selected Areas in Cryptography – SAC’2003*, ser. LNCS, vol. 3006. Springer-Verlag, 2004, pp. 17–25.
- [20] L. Eschenauer and V. Gligor, “A key-management scheme for distributed sensor networks,” in *ACM CCS*, Washington, DC, Nov. 2002.
- [21] H. Chan, A. Perrig, and D. Song, “Random key predistribution schemes for sensor networks,” in *IEEE Symposium on Security & Privacy*, Oakland, CA, May 2003.
- [22] W. Du, J. Deng, Y. Han, and P. Varshney, “A pairwise key pre-distribution scheme for wireless sensor networks,” in *ACM CCS*, Washington, DC, Oct. 2003.
- [23] D. Liu and P. Ning, “Establishing pairwise keys in distributed sensor networks,” in *ACM CCS*, Washington, DC, Oct. 2003.
- [24] —, “Location-based pairwise key establishments for static sensor networks,” in *ACM SASN*, Fairfax, VA, Oct. 2003.
- [25] R. Sakai, K. Ohgishi, and M. Kasahara, “Cryptosystems based on pairing,” in *Proc. 2000 Symposium on Cryptography and Information Security (SCIS2000)*, Okinawa, Japan, Jan. 2000.
- [26] A. Khalili, J. Katz, and W. Arbaugh, “Toward secure key distribution in truly ad-hoc networks,” in *IEEE Workshop on Security and Assurance in Ad Hoc Networks*, Orlando, FL, Jan. 2003.
- [27] A. Shamir, “How to share a secret,” *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.
- [28] H. Deng, A. Mukherjee, and D. Agrawal, “Threshold and identity-based key management and authentication for wireless ad hoc networks,” in *International Conference on Information Technology: Coding and Computing (ITCC’04)*, Las Vegas, Nevada, April 2004.
- [29] M. Bohio and A. Miri, “Efficient identity-based security schemes for ad hoc network routing protocols,” *Elsevier Ad Hoc Networks Journal*, vol. 2, no. 3, pp. 309–317, 2004.
- [30] N. Saxena, G. Tsudik, and J. H. Yi, “Identity-based access control for ad hoc groups,” in *Proc. Int. Conf. Inform. Security Cryptology*, Seoul, Korea, Dec. 2004.
- [31] J. Sun, C. Zhang, and Y. Fang, “A security architecture achieving anonymity and traceability in wireless meshnetworks,” in *The 27th IEEE International Conference on Computer Communications (INFOCOM’08)*, Phoenix, AZ, April 13-18 2008.
- [32] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures,” *Ad Hoc Networks*, vol. 1, no. 2, 2003.
- [33] J. Newsome, E. Shi, D. Song, and A. Perrig, “The sybil attack in sensor networks: Analysis & defenses,” in *Proc. of the Third International Symposium on Information Processing in Sensor Networks (IPSN 2004)*, Berkeley, CA, April 2004.

PLACE  
PHOTO  
HERE

**Yuguang Fang** (F’08) 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 University of Florida in May 2000 as an assistant professor, got an early promotion to associate professor with tenure in August 2003 and to 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. He received the National Science Foundation Faculty Early Career Award in 2001 and the Office of Naval Research Young Investigator Award in 2002. He 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 have also been actively participating in professional conference organizations such as serving as the Technical Program Vice-Chair for IEEE INFOCOM 2005, Technical Program Symposium Co-Chair for IEEE Globecom 2004, and a member of Technical Program Committee for IEEE INFOCOM (1998, 2000, 2003-2007).

PLACE  
PHOTO  
HERE

**Xiaoyan Zhu** received her BE degree in Information Engineering from Xidian University, Xian, China, in July 2000, and her ME degree in Information and Communications Engineering from Xidian University, Xian, China, in March 2004. She is now working towards her Ph.D. degree at Xidian University. Her research interests include wireless security and network coding.

PLACE  
PHOTO  
HERE

**Yanchao Zhang** (M’06) received the BE degree in computer communications from the Nanjing University of Posts and Telecommunications, Nanjing, China, in July 1999, the ME degree in computer applications from the Beijing University of Posts and Telecommunications, Beijing, in April 2002, and the PhD 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.