Securing Resource-Constrained Wireless Ad Hoc Networks
(Invited Paper)

Yuguang Fang* and Yanchao Zhang†
* University of Florida, Gainesville, FL 32611. Email: fang@ece.ufl.edu
†New Jersey Institute of Technology, Newark, NJ 07102. Email: yczhang@njit.edu

Abstract— **Huge interest and demand on information superhighway have pressed various telecommunications research fronts and lead to a new form of future Internet consisting of wired and wireless segments where resource-constrained devices such as palm pilots and 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-constrained segments. In this paper, we present a novel approach to addressing security issues and demonstrate why and how the ID-based cryptography can be effectively applied to the resource-constrained wireless networks for various network security problems.**

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 mobile ad hoc networks and wireless sensor networks. 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 disaster rescue (such as Hurricane Katrina), military operations, homeland security and public safety, where fixed infrastructures are often not available or 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 categories, namely, mobile ad hoc networks (MANETs) and wireless sensor networks (WSNs). The former comprises mobile nodes that are free to move around randomly 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, that is, fixed at where they were deployed. 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].

In this paper, we present a recently developed novel approach to addressing a number of challenging issues in securing wireless ad hoc networks (WANETs) ([6]–[10]). We articulate that the new emerging ID-based cryptography can be effectively utilized to address such difficult security issues.

II. Wireless Security Challenges

Wireless has penetrated into our life in every corner nowadays. Wireless indeed offers us many advantages. Unfortunately, wireless also poses many design challenges. Wireless channel condition is usually very poor (e.g., due to fading) and time-varying (due to mobility or power depletion or unpredictable interference), leading to constant transmission failure. We also face many resource limitation in terms of bandwidth, power, and computing resources (memory and CPU). The channel environment is open, and hence potential interception or eavesdropping causes security problems. Finally, for many WANETs, there are no trusted infrastructure in place to implement the well-developed secure architec-

This work was partially supported in part by the National Science Foundation under grant CNS-0626881 and under grant ANI-0093241 (CAREER Award).

ture 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. In the current literature, there are mainly two major approaches: symmetric approach approach and asymmetric key approach (PKI). Symmetric key approach does offer many advantages: 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 mandated by this approach, tends to demand much higher communication overhead, and does not support digital signature. On the other hand, asymmetric key approach is scalable with easier key establishment, has better authentication technique, and owns embedded digital signature. However, it is indeed computationally intensive with larger key size, has difficult public key management and more overheads due to certificate management. It is not an easy task to choose between symmetric key approach and asymmetric approach in WANETs, and an appropriate decision should rely on the salient feature of the WANETs we are interested in.

Inspired by the recently resurging Identity-based Public Key Cryptography (ID-PKC), we recently have developed a novel approach to addressing security issues in WANETs. We present the basic idea in this paper.

III. Why Identity-Based Cryptography?

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 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 relies on reliable trustworthy infrastructure. 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].

In 1984, Shamir proposed the idea of the ID-PKC [12], where an entity's public key can be derived directly from certain aspects of its identity, for example, an IP address 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 [13], 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 ([14] and the references thereof) due to the novel application of a cryptographic technique called *pairing*, which is outlined as follows [15].

Let p, q be two large primes and $\mathsf{E}/\mathbb{F}_p$ denote an elliptic curve $y^2 = x^3 + ax + b$ 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 $\mathsf{E}/\mathbb{F}_p$, and by $\mathbb{G}_2$ a q-order subgroup of the multiplicative group of the finite field $\mathbb{F}^*_{p^2}$. When $a \in \mathbb{Z}_q$ 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[1] in both $\mathbb{G}_1$ and $\mathbb{G}_2$. From a cryptographic point of view, a pairing is a map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ with the following properties:

- $\hat{e}$ is *bilinear*: $\forall\ P, Q, R \in \mathbb{G}_1$,
$$\begin{aligned} \hat{e}(P+Q,R) &= \hat{e}(P,R)\cdot\hat{e}(Q,R) \\ \hat{e}(P,Q+R) &= \hat{e}(P,Q)\cdot\hat{e}(P,R). \qquad (1) \end{aligned}$$
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*, i.e., $\hat{e}(P, Q) = \hat{e}(Q, P)$ for $\forall\ P, Q \in \mathbb{G}_1$, which follows immediately from the bilinearity and the fact that $\mathbb{G}_1$ is a cyclic group. Typically, the map $\hat{e}$ will be derived from either the (modified) Weil [15] or Tate [16] pairing on a super-singular elliptic curve over a finite field.

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

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

$S_x = sH_1(ID_x)$, 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. Many efficient cryptographic primitives have been proposed recently on how to leverage identity-based public/private key pairs to realize essential public-key operations. 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.

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 to be suitable for WANETs, which led to a burst of interesting results based on pure symmetric-key cryptography, such as [17]–[22]. However, the inherent limitations of symmetric-key cryptography render these proposals suffer from the lack of authentication, scalability and resilience to node compromise [23].

Although ID-PKC has comparable computational efficiency to that of the conventional PKC [24], 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. We observe that, 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

$$\begin{aligned} & K_{xy} = \hat{e}(S_x, H_1(ID_y)) = \hat{e}(sH_1(ID_x), H_1(ID_y)) \\ = \;& \hat{e}(H_1(ID_x), H_1(ID_y))^s = \hat{e}(H_1(ID_x), sH_1(ID_y)) \\ = \;& \hat{e}(H_1(ID_x), S_y) = \hat{e}(S_y, H_1(ID_x)) = K_{yx}. \qquad (2) \end{aligned}$$

This method of *identity-based, non-interactive* shared-key establishment is reported in [25] and obviously can further reduce both communication and computation overheads. 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. 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 [15], [26].

IV. An Exemplar Application: Sensor Network Security

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 that senses an intrusion event, 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 be able to 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 [7].

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 share key without exchanging any secret materials. 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

$$V_B = H_2(\hat{e}(K_B, H_1(ID_A@L_A)) \parallel n_A \parallel n_B \parallel 0), \tag{3}$$

where H_2 is another hash function. Once receiving B's reply, node A can determine that 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

$$V'_B = H_2(\hat{e}(K_A, H_1(ID_B@L_B)) \parallel n_A \parallel n_B \parallel 0). \tag{4}$$

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

$$\begin{aligned} &\hat{e}(K_B, H_1(ID_A@L_A)) = \hat{e}(K_A, H_1(ID_B@L_B)) \\ &= \hat{e}(H_1(ID_B@L_B)), H_1(ID_A@L_A))^s \in \mathbb{G}_2. \end{aligned} \tag{5}$$

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

$$V_A = H_2(\hat{e}(K_A, H_1(ID_B@L_B)) \parallel n_A \parallel n_B \parallel 1). \tag{6}$$

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 [27], [28]. 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) [28]. 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 far away nodes think they are neighbors [27]. 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 [7]. In conclusion, our location-based security approach indeed provides a unifying and effective security scheme.

V. Conclusions

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.

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, "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.

[7] 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.

[8] ——, "MASK: anonymous on-demand routing in mobile ad hoc networks," *IEEE Transactions on Wireless Communications*, vol. 5, no. 9, pp. 2376–2385, September 2006.

[9] ——, "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.

[10] Y. Zhang and Y. Fang, "A secure authentication and billing architecture for wireless mesh networks," *ACM Wireless Networks*, 2006, accepted.

[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. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[14] R. Dutta, R. Barua, and P. Sarkar, "Pairing-based cryptography : A survey," Cryptology ePrint Archive Report 2004/064, 2004.

[15] 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.

[16] 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.

[17] L. Eschenauer and V. Gligor, "A key-management scheme for distributed sensor networks," in *ACM CCS*, Washington, DC, Nov. 2002.

[18] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *IEEE Symposium on Security & Privacy*, Oakland, CA, May 2003.

[19] 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.

[20] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in *ACM CCS*, Washington, DC, Oct. 2003.

[21] ——, "Location-based pairwise key establishments for static sensor networks," in *ACM SASN*, Fairfax, VA, Oct. 2003.

[22] R. Anderson, H. Chan, and A. Perrig, "Key infection: Smart trust for smart dust," in *IEEE ICNP'04*, Berlin, Germany, Oct. 2004.

[23] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53–57, June 2004.

[24] W. Mao, "An identity-based non-interactive authentication framework for computational grids," Hewlett-Packard Laboratories, Technical Report HPL-2004-96, June 2004.

[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] M. C. Mont and P. Bramhall, "IBE applied to privacy and identity management," Hewlett-Packard Laboratories, Technical Report HPL-2003-101, May 2003.

[27] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2, 2003.

[28] 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.