

Securing Wireless Sensor Networks with Location Based Keys

Wenjing Lou
ECE Department, WPI

1 Introduction

Recent advancement in microprocessor, memory, and wireless networking and communication technologies have made the deployment of wireless sensor networks possible. A wireless sensor network typically is composed of a large number of low-cost sensor nodes which work collectively to carry out some real-time sensing and monitoring tasks within a designated area. This emerging technology has drawn growing attention recently since it provides a promising solution to some challenging tasks, such as the military sensing and tracking in the hostile ground, the remote sensing in nuclear plants, mines, and other hazardous industrial venues, real-time traffic monitoring, realtime weather monitoring, wild animal monitoring and tracking, etc.

Security has become a primary concern recently in sensor networks, especially when they are deployed in military applications or in safety-critical applications such as the nuclear plant safety monitoring. Key management is possibly the most critical and complex issue when talking about security in wireless sensor networks. An effective and efficient key management system is the foundation of many other security services, such as authentication, confidentiality, and integrity, etc. It is well-known that public key cryptography (PKC) makes the key management simpler, more scalable, and more efficient. However, it is argued that the computational overhead involved in the public key operations limits its application in the stringent resource constrained sensor networks. In addition, the management and transmission of the public key certificate¹ itself introduce non-negligible storage and communication overheads in sensor networks where the node storage capacity is small (a few KBytes data memory as in Berkeley's Mica Mote) and the packets are relatively short (a typical size of 30 bytes with header). On the other hand, secret key cryptography is computationally efficient compared to public key cryptography. However, the key management based on secret keys is not scalable and requires extra communication and protocol overheads. In addition, the security of the schemes is severely threatened when the number of compromised nodes increases. Moreover, purely secret key cryptography based schemes have very limited capability to support other security services, such as node-to-node authentication, since keys can be issued to multiple nodes. One way hash chains have also been investigated as another cryptographic tool to establish the trust relationship among nodes, particularly for the authentication of the broadcast traffic from the base station. However, protocols based on this approach like μ TESLA require a complicated delayed key disclosure scheme which requires constant key updates, the nodes have to store keys, and be time synchronized.

In this project we aim to develop novel approaches to solve the difficult trust establishment and key management problem in wireless sensor networks. The security mechanisms we intend to develop would feature *lightweight*, *resilient*, *scalable*, and be specifically designed to fit into the characteristics of sensor networks and their application specific tasks and communication patterns.

2 Our Approach - Location-Based Key Management

Our approach to tackle the challenging key management problem is the proposal of location-based keys where the location information of sensors are used as the identifiers in an identity-based public key crypto-

¹A public key certificate could be lengthy. At minimum it should include a node's identity, its public key, and a digital signature which alone is usually more than 16 bytes long.

graphic system. Due to the inbred properties of identity-based cryptography, other security services, such as node-to-node authentication, pairwise key establishment, etc., are expected to be made efficient and reliable. Our proposal is based on the following observations and cryptographic foundations.

ID-PKC and pairing concept

Identity-based public-key cryptography (ID-PKC) arises as a promising candidate during our search for an efficient security solution for sensor networks. First introduced by Shamir in 1984, ID-PKC simplifies public-key management by allowing public keys to be directly derived from publicly available information that uniquely and undeniably identifies users, e.g., telephone numbers, email addresses, and social security numbers. It thus eliminates the need for public-key certificates and the need to maintain a huge database containing a list of public keys and their respective owners. This inbred feature makes ID-PKC attractive for the wireless arena where communication bandwidth, memory storage, and battery life are more constrained.

The rapid development of ID-PKC has only taken place recently due to the application of *pairing*. Pairing technique forms the cryptographic foundation of our approach. We outline its basic concept as follows.

Let $\mathbb{G}_1, \mathbb{G}_2$ be two groups of the same prime order q . We view \mathbb{G}_1 as an additive group and \mathbb{G}_2 as a multiplicative group. A pairing is a computable *bilinear map* $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ satisfying the following properties:

1. *Bilinearity*: $\forall P, Q, R, S \in \mathbb{G}_1$, we have

$$\hat{e}(P + Q, R + S) = \hat{e}(P, R)\hat{e}(P, S)\hat{e}(Q, R)\hat{e}(Q, S).^2 \quad (1)$$

2. *Non-degeneracy*: If $\hat{e}(P, Q) = 1$ for all $Q \in \mathbb{G}_1$, then P must be the identity element in \mathbb{G}_1 .
3. *Computability*: There exists an efficient algorithm to compute $\hat{e}(P, Q)$ for all $P, Q \in \mathbb{G}_1$.

Modified Weil and Tate pairings on supersingular elliptic curves are examples of such bilinear maps, for which the *Bilinear Diffie-Hellman Problem* (BDHP) is believed to be hard, i.e., it is believed that, given $\langle P, xP, yP, zP \rangle$ for random $x, y, z \in \mathbb{Z}_q^{*3}$ and $P \in \mathbb{G}_1$, there is no algorithm running in expected polynomial time, which can compute $\hat{e}(P, P)^{xyz} \in \mathbb{G}_2$ with non-negligible probability.

Location-based keys

It is observed that most sensor networks have an intrinsic property that sensor nodes are stationary, that is, fixed at where they were deployed. Almost all applications of sensor networks require sensors to be aware of their physical locations. For example, the detection of a target or an event in surveillance or monitoring sensor networks is always associated with location information. Many sensor self-positioning algorithms have been proposed. The location information has been widely used to facilitate network functions such as target tracking, geographic routing, location directory service, and collaborative signal processing, etc. Sensor location can also serve as ID, as it may be unnecessary or impossible for each sensor to have a unique ID before its deployment.

The potential of using location information to secure sensor networks has so far drawn little attention. We propose to use the location information to identify a sensor node in a ID-PKC as the solution to the complex key management problem. The basic cryptographic definition for the proposed location-based key management is outlined as follows.

Assume that a sensor, say A , has a unique geographic location pos_A . It then can be initialized with an location-based key, or LBK for short, which is calculated as $LK_A = \kappa H_1(pos_A)$, where $H_1 : \{0, 1\}^* \rightarrow \mathbb{G}_1$ is a collision-resistant cryptographic hash function mapping arbitrary strings to points in \mathbb{G}_1 , and κ is the system master-key which does not present in the sensor field except at the network initialization phase. Since the Discrete Log Problem (DLP) is believed to be hard in \mathbb{G}_1 , given a $\langle pos_A, LK_A \rangle$ pair, adversaries

²In particular, $\forall P, Q \in \mathbb{G}_1, \forall a, b \in \mathbb{Z}_q^*, \hat{e}(aP, bQ) = \hat{e}(aP, Q)^b = \hat{e}(P, bQ)^a = \hat{e}(P, Q)^{ab}$ etc.

³ \mathbb{Z}_q^* is the *multiplicative group* of integers modulo q . In particular, if q is a prime, $\mathbb{Z}_q^* = \{a \mid 1 \leq a \leq q - 1\}$.

cannot deduce the system master-key κ with non-negligible probability. As a result, even if compromising an arbitrary number of nodes and their LBKs, adversaries are unable to exploit the acquired knowledge to calculate the LBKs of the remaining non-compromised nodes.

The proposed location-based key management system is a novel solution to the difficult key management in sensor networks. The potential of using location information and the application of the newly developed pairing concept are unexplored problems and have strong impact on security research in sensor networks. The properties inherited from ID-based key management system are anticipated to greatly simplify the key management schemes and many other security services whose security highly depends on the security and availability of the keys. For example, the proposed scheme removes the need of public key certificates and all necessary operations to verify the certificates; it is scalable since each node only needs to know its own location based key; it is resilient since the compromise of one node does not affect the security of other nodes, etc. In addition, since the location of sensor nodes can be verified, they would also have broad impact on securing other network functions such as securing routing protocols and securing traffic delivery. It is anticipated that the efficiency and robustness of public key cryptography in key management will help to build lightweight⁴ and resilient security mechanisms that depend on the effective key management.

Public key cryptography used to be considered impossible in sensor networks due to its computationally intensive operations. However, recent state of the art in ultra-low power public key cryptography for wireless sensor networks indicates that this intuition of infeasibility comes from the emulation of the cryptographic primitives in software on general purpose micro-controllers. By implementing PKC in a custom-designed low-power coprocessor that can be imbedded in the sensor nodes to handle all the computation intensive tasks can greatly alleviate this infeasibility. In addition, pairing is a relatively new cryptographic concept in contrast to RSA public key cryptography. We anticipate that the evaluation cost of the pairing will be much reduced with the rapid advance in the realm of cryptography. For example, according to the recent result, the Tate pairing can be evaluated up to 10 times better than previously reported implementations.

3 Project Outcomes

In this project, we proposed to design a location-based key management system, based on which, we designed a set of security mechanisms and evaluated their performance in terms of overhead and security. Extensive design and simulation studies have been carried out by the PI and her two Ph.D students, Kui Ren and Kai Zeng. The students have received training in cryptography, security, and networking.

The results from this project have helped in four grant proposals the PI submitted to NSF, ONR, and a company during the academic year 2005-06. As a result, the PI received two grants, one from NSF and one from a company.

1. COLLABORATIVE RESEARCH: UPASS An Attack-Resilient Security Architecture for Wireless Mesh Networks, Sponsored by National Science Foundation. PI, \$250,000, 9/15/2006-8/31/2009. In collaboration with Prof. Yuguang Fang, University of Florida.
2. Power-aware / Energy-efficient Routing and Security in Wireless Sensor Networks, Sponsored by AirSprite Technologies, Inc. PI, \$100,000, 1/1/2006-12/31/2006

There are also a number of publications that came out from this project.

1. Kui Ren, Wenjing Lou, Kai Zeng, and Patrick J. Moran, "On broadcast authentication in wireless sensor networks", accepted by *IEEE Transactions on Wireless Communications*

⁴in terms of communication overhead

2. Kui Ren and Wenjing Lou, Privacy-enhanced, attack-resilient access control in pervasive computing environments with optional context authentication capability, to appear in *ACM Mobile Networks and Applications (MONET)* (special issue on Wireless Broadband Access)
3. Kui Ren, Wenjing Lou, Kai Zeng, Feng Bao, Jianying Zhou, and Robert H. Deng, Routing optimization security in mobile IPv6, *Computer Networks*, vol. 50, issue 13, pp.2401-2419, 2006.
4. Wenjing Lou, Younggoo Kwon, H-SPREAD: A hybrid multipath scheme for secure and reliable data collection in wireless sensor networks, *IEEE Transactions on Vehicular Technology*, vol. 55, no. 4, July 2006.
5. Kui Ren, Wenjing Lou, Kwangjo Kim, Robert Deng, A novel privacy preserving authentication and access control scheme for pervasive computing environment, *IEEE Transactions on Vehicular Technology*, vol. 55, no. 4, July 2006.
6. Kui Ren, Kai Zeng, Wenjing Lou, A new approach for random key pre-distribution in large-scale wireless sensor networks, *Journal of Wireless Communication and Mobile Computing* (Special Issue on Wireless Networks Security), vol. 6, issue 3, pp. 307-318, 2006.
7. Kui Ren, Kai Zeng, Wenjing Lou, "Fault-tolerant event boundary detection in wireless sensor networks", *IEEE Global Telecommunications Conference (GLOBECOM 2006)*, November 27-December 1, 2006, San Francisco, CA, USA
8. Kui Ren, Wenjing Lou, and Patrick J. Moran, A proactive data security framework for mission-critical sensor networks, *IEEE Military Communication Conference (MILCOM 2006)*, Washington, DC, October 23-25, 2006.
9. Kai Zeng, Wenjing Lou, Kui Ren, and Patrick J. Moran, Energy-efficient geographic routing in environmentally powered wireless sensor networks, *IEEE Military Communication Conference (MILCOM 2006)*, Washington, DC, October 23-25, 2006.
10. Kui Ren, Kai Zeng, Wenjing Lou, and Patrick J. Moran, "On broadcast authentication in wireless sensor networks", *International Conference on Wireless Algorithms, Systems, and Applications (WASA 2006)*, Xi'an, China, August 15-18, 2006. **Best Paper Award**
11. Kai Zeng, Kui Ren, Wenjing Lou, and Patrick J. Moran, "Energy aware efficient geographical routing in lossy wireless sensor networks with environmental energy supply", *The Third International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks (QShine 2006)*, Waterloo, Ontario, Canada, August 7-9, 2006
12. Kui Ren, Wenjing Lou, and Yanchao Zhang, LEDS: Providing location-aware end-to-end data security in wireless sensor networks, *IEEE INFOCOM 2006*, Barcelona, Spain, April 2006. (Acceptance ratio 18%).