Pairing-Based Cryptography for Sensor Networks

Leonardo B. Oliveira*
UNICAMP, Brazil
leob@ic.unicamp.br

Ricardo Dahab
UNICAMP, Brazil
rdahab@ic.unicamp.br

Abstract

Pairing-based Cryptography has enabled a wide range of cryptographic schemes. This work discusses these schemes in the context of wireless sensor networks. To our knowledge, ours is the first work to address this subject.

1 Introduction

Wireless sensor networks (WSNs) [7] are ad hoc networks comprised mainly of small sensor nodes with limited resources and one or more base stations (BSs). They are used for monitoring purposes, providing information about the area being monitored to the rest of the system. When embedded in critical applications, WSNs are likely to be attacked [18] and it is thus crucial to devise security solutions particularly tailored to their needs.

Until recently, security solutions for WSNs relied on symmetric encryption algorithms (e.g., RC5 [15] and SkipJack [10]) to provide properties such as authentication and confidentiality since, due to their resource constraints, nodes cannot afford to use conventional algorithms of Public Key Cryptography (PKC) (e.g. RSA/DSA).

Although more efficient, symmetric cryptosystems have some drawbacks. Firstly, nodes face the *key agreement* problem, i.e., they must decide on a shared key to communicate securely. This problem is even worse in WSNs due to the open and unattended environments where nodes are commonly deployed [18]. Further, the ideal level of security in these cryptosystems is achieved by using pairwise keys. However, this scheme is not scalable and thus is inadequate for WSNs which may comprise thousands of nodes. Finally, symmetric cryptosystems do not provide nonrepudiation.

To address some of theses drawbacks, a number of key predistribution schemes have been proposed (e.g., [6, 13, 19]). Although effective in trying to achieve a good tradeoff between resource consumption and resiliency, these proposals eventually incur some degree of overhead.

LEAP [19], perhaps the most efficient proposal, allows a pairwise key agreement protocol between neighboring nodes using only symmetric primitives. However, LEAP has also drawbacks. Firstly, LEAP assumes that a predistributed key shared among all nodes will not be disclosed during the t initial time units of the network operation. Secondly, LEAP assumes that once this key is erased, it cannot be recovered from memory. According to Anderson and Kuhn's work [1], however, this is not always the case. Lastly, LEAP does not provide digital authentication and repudiation of messages is still possible.

Today, motivated by this vulnerabilities, the cryptography community in WSNs has been investigating more efficient techniques of PKC. By using Elliptic Curve Cryptography (ECC [14, 12]), for example, it has been shown (e.g., [8]) that PKC is indeed feasible in WSNs since ECC consumes considerably less resources than conventional PKC, for a given security level.

However, in order to use effectively ECC in WSNs, it is first necessary to enable authentication of public keys. Otherwise, the network shall be vulnerable to *man-in-the-middle* attacks. Public key authentication is usually achieved by means of a Public Key Infra-structure (PKI), which issues certificates and requires users to store, exchange, and verify them. These operations, in turn, incur high overheads of storage, communication, and computation and, as a result, are inadequate for WSNs [5].

Identity-Based Cryptography (IBC) [17] is an exception where an information that uniquely identifies users (e.g. IP or email addresses) can be used to both exchange keys and encrypt data, and thus PKI is unnecessary. Although the notion of IBC dates from Shamir's original work [17], it only has become truly practical with the advent on Pairing-Based Cryptography (PBC) [16, 9, 3]. Next Section, we briefly describe the benefits of PBC in the context of WSNs.

2 Applying PBC to WSNs

With the advent of more powerful classes of nodes (e.g., *Imotes* [11]) it has become possible to use PBC in the context of WSNs. In addition, because PBC has become more and more efficient (e.g., [2]), we believe that it will be soon enabled in a wide range of nodes platforms. In the follow-

*Supported by FAPESP under grant 2005/00557-9

ing, we list some PBC applications and argue why they are interesting in the context of WSNs.

- *Identity-Based Non-Interactive Key Distribution:* in WSNs, nodes often become unavailable, leave, or enter the network. An identity-based non-interactive key distribution scheme (e.g., [16]), where parties can "noninteractively" decide on a shared key without using a PKI, would be very useful if applied to WSNs.

- *Multi-Party Key Agreement:* hierarchical WSNs are organized into clusters and often nodes have to (securely) exchange information among the other members of the cluster. Multi-party key agreement protocols (e.g. [9]) establish a shared key among multiple participants with less rounds than traditional key agreement protocols and would make this procedure faster and more efficient in WSNs.

- *Identity-Based Encryption (IBE):* today, IBE schemes from PBC (e.g. [3]) seem to be the only truly practical mean of providing public-key encryption in WSNs since they do not require a PKI. Instead, they employ users' identification (e.g., node *id*) as public keys.

- *Short Signatures:* WSNs have strong bandwidth constraints and thus require short signatures. Short signature schemes from PBC (e.g. [4]) offer signatures on the order of 160 bits for a level of security similar to that of 320-bit DSA signatures.

Having said this, we argue that PBC is not only ideal for WSNs, but vice-versa as well. For example, IBC schemes require an unconditionally trusted entity to issue users' private keys. WSNs, however, posses intrinsically such an entity, i.e., the BS. An additional requirement is that the keys must be delivered over confidential and authentic channels to users, which in turn imposes a communication overhead. In most of the WSN applications, however, node's private keys would be distributed *offline*, i.e., they would be generated and loaded directly into nodes. And finally, even *static* keys generated with Sakai et al's pioneering work on PBC [16] – inadequate for the vast majority of applications – can be used to derive encryption keys in WSNs. Due to the short lifetime of the network, a single key is enough for most of the WSN applications.

References

[1] R. J. Anderson and M. Kuhn. Tamper resistance – a cautionary note. In *2nd* USENIX *Workshop on Electronic Commerce*, pages 1–11. The USENIX Association, Nov 1996.

[2] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott. Efficient algorithms for pairing-based cryptosystems. In *CRYPTO '02: the 22nd Annual International Cryptology Conference on Advances in Cryptology*, pages 354–368, London, UK, 2002. Springer-Verlag.

[3] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In *CRYPTO 2001*, number 2139 in LNCS, pages 213–229, Berlin Heidelberg, 2001. Springer-Verlag.

[4] D. Boneh, B. Lynn, and H. Schacham. Short signatures from the Weil pairing. *Journal of Cryptology*, 17(4):297–319, 2004.

[5] W. Du, R. Wang, and P. Ning. An efficient scheme for authenticating public keys in sensor networks. In *6th ACM international symposium on Mobile ad hoc networking and computing (MobiHoc '05)*, pages 58–67, New York, 2005.

[6] L. Eschenauer and V. D. Gligor. A key management scheme for distributed sensor networks. In *9th ACM conf. on Computer and communications security*, pages 41–47, 2002.

[7] D. Estrin, R. Govindan, J. S. Heidemann, and S. Kumar. Next century challenges: Scalable coordination in sensor networks. In *Mobile Computing and Networking (MobiCom'99)*, pages 263–270, Seattle, WA USA, 1999.

[8] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz. Comparing elliptic curve cryptography and rsa on 8-bit cpus. In *Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, pages 119–132, 2004.

[9] A. Joux. A one round protocol for tripartite diffie-hellman. In *ANTS-IV: the 4th Int'l Symposium on Algorithmic Number Theory*, pages 385–394, London, 2000. Springer-Verlag.

[10] C. Karlof, N. Sastry, and D. Wagner. Tinysec: A link layer security architecture for wireless sensor networks. In *2nd ACM SensSys*, pages 162–175, Nov 2004.

[11] R. M. Kling. Intel mote: An enhanced sensor network node. In *Int'l Workshop on Advanced Sensors, Structural Health Monitoring, and Smart Structures*, pages 12–17, Nov 2003.

[12] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, 48:203–209, 1987.

[13] D. Liu, P. Ning, and R. Li. Establishing pairwise keys in distributed sensor networks. *ACM Transactions on Information and System Security (TISSEC)*, 8(1):41–77, 2005. Also appeared in 10th ACM CCS '03.

[14] V. Miller. Uses of elliptic curves in cryptography, advances in cryptology. In *Crypto'85, Lecture Notes in Computer Science*, volume 218, pages 417–426. Springer-Verlag, 1986.

[15] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar. SPINS: Security protocols for sensor networks. *Wireless Networks*, 8(5):521–534, Sept. 2002. Also appeared in MobiCom'01.

[16] R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairing. In *Symposium on Cryptography and Information Security (SCIS2000)*, pages 26–28, Jan 2000.

[17] A. Shamir. Identity-based cryptosystems and signature schemes. In *CRYPTO'84: on Advances in cryptology*, pages 47–53. Springer-Verlag, 1984.

[18] A. D. Wood and J. A. Stankovic. Denial of service in sensor networks. *IEEE Computer*, 35(10):54–62, Oct. 2002.

[19] S. Zhu, S. Setia, and S. Jajodia. LEAP: efficient security mechanisms for large-scale distributed sensor networks. In *10th ACM conference on Computer and communication security*, pages 62–72. ACM Press, 2003.