ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

Message Authentication and Source Privacy in Wireless Sensor Networks

Prof. P. A. Khodke[1], Mansi S. Nanwani[2]

Head of Computer Science & Engineering Dept., Prof. Ram Meghe College of Engineering And Management, Badnera, Maharashtra, India[1]

Computer Engineering, Prof. Ram Meghe College of Engineering & Management, Badnera, Maharashtra, India[2]

Abstract: Message authentication is one of the most effective ways to thwart unauthorized and corrupted messages from being forwarded in wireless networks. For this reason, many message authentication schemes have been developed, based on either symmetric-key cryptosystems or public-key cryptosystems. Most of them, however, have the limitations of high computational and communication overhead in addition to lack of scalability and resilience to node compromise attacks. To address these issues, a polynomial-based scheme was recently introduced. However, this scheme and its extensions all have the weakness of a built-in threshold determined by the degree of the polynomial when the number of messages transmitted is larger than this threshold, the adversary can fully recover the polynomial.

Keywords: Authentication, Elliptic Curve, Symmetric Key Cryptography, Public Key Cryptography.

I. INTRODUCTION

Message authentication plays a key role in thwarting unauthorized and corrupted messages from being forwarded in networks to save the precious sensor energy. For this reason, many authentication schemes have been proposed in literature to provide message authenticity and integrity verification for wireless sensor networks (WSNs) [1]–[5]. These schemes can largely be divided into two categories: public-key based approaches and symmetric-key based approaches. The symmetric-key based approach requires complex key management, lacks of scalability, and is not resilient to large numbers of node compromise attacks since the message sender and the receiver have to share a secret key. The shared key is used by the sender to generate a message authentication code (MAC) for each transmitted message. However, for this method, the authenticity and integrity of the message can only be verified by the node with the shared secret key, which is generally shared by a group of sensor nodes. An intruder can compromise the key by capturing a single sensor node. In addition, this method does not work in multicast networks.

To solve the scalability problem, a secret polynomial based message authentication scheme was introduced in [3]. The idea of this scheme is like a threshold secret sharing, where the threshold is calculated by the degree of the polynomial. This approach offers information-theoretic security of the shared secret key when the number of messages transmitted is less than the threshold. The intermediate nodes verify the authenticity of the message through a polynomial evaluation. However, when the number of messages transmitted is larger than the threshold, the polynomial can be fully recovered and the system is completely broken. Key distribution is a central problem in cryptographic systems, and is a major component of the security subsystem of distributed systems, communication systems, and data networks.

The increase in bandwidth, size, usage, and applications of such systems is likely to pose new challenges and to require novel ideas. A growing application area in networking is “conferencing” a group of entities (or network locations) collaborate privately in an interactive procedure (such as: board meeting, scientific discussion, a task-force, a classroom, or a bulletin-board). In this work we consider perfectly-secure key distribution for conferences. (Note that key distribution for two-party communication (session keys) is a special case of Conferences of size two). If users of a group (a conference) wish to communicate in a network using symmetric encryption, they must share a common key. A key distribution scheme (denoted KDS for short) is a method to distribute initial private pieces of information among a set of users, such that each group of a given size (or up to a given size) can compute a common key for secure conference. This information is generated and distributed by a trusted server which is active only at the distribution phase.

II. LITERATURE REVIEW

Wireless sensor networks (WSNs) consist of hundreds or even thousands of small devices each with sensing, processing, and communication capabilities to monitor the real-world environment and are used in a variety of applications such as military sensing and tracking, environmental monitoring, disaster management, etc. But when WSN is deployed in open, unmonitored, hostile environment, or operated on unattended mode sensor nodes will be exposed to the risk of being captured by an active attacker

Types of attacks that happen in wireless sensor networks are:

Passive attacks: Through passive attacks, the adversaries could eavesdrop on messages transmitted in the network

DOI 10.17148/IJARCCE.2015.49113

and perform traffic analysis.

Active attacks: Active attacks can only be launched from the compromised sensor nodes. Once the sensor nodes are compromised, the adversaries will obtain all the information stored in the compromised nodes, including the security parameters of the compromised nodes. The adversaries can modify the contents of the messages, and inject their own messages.

III. PROPOSED METHOD

Message authentication: The message receiver should be able to verify whether a received message is sent by the node that is claimed.

Message integrity: The message receiver should be able to verify whether the message has been en-route by the adversaries. In other words, the adversaries cannot modify the message content without being detected.

Identity and location privacy: The receiver cannot determine the message sender's ID and location by analyzing the message contents or the local traffic.

Node compromise resilience: The scheme should be resilient to node compromise attacks. No matter how many nodes are registered, the remaining nodes can still be secure.

Efficiency: The scheme should be efficient in terms of both computational and communication overhead.

IV. TERMINOLOGY

Privacy is sometimes referred to as anonymity. Communication anonymity in information management has been discussed in a number of previous works [11], [12], [13], [14], [15], [16]. It generally refers to the state of being unidentifiable within a set of subjects. This set is called the AS. Sender anonymity means that a particular message is not linkable to any sender, and no message is linkable to a particular sender.

We will start with the definition of the unconditionally secure SAMA.

Definition 1 (SAMA). A SAMA consists of the following two algorithms:

- Generate (m; Q1; Q2; . . .;Qn). Given a message m and the public keys Q1;Q2; . . .;Qn of the AS S ={A1;A2; . . .;An}, the actual message sender At; 1<=t<=n, produces an anonymous message S(m) using its own private key dt.
- Verify S(m). Given a message m and an anonymous message S(m), which includes the public keys of all members in the AS, a verifier can determine whether S(m) is generated by a member in the AS.

The security requirements for SAMA include:

- Sender ambiguity. The probability that a verifier successfully determines the real sender of the anonymous message is exactly 1/n, where n is the total number of members in the AS.
- Unforgeability. An anonymous message scheme is unforgettable if no adversary, given the public keys of all members of the AS and the anonymous messages m1;m2; . . .;mn adaptively chosen by the adversary, can produce in polynomial time a new valid anonymous message with non-negligible probability.

In this paper, the user ID and the user public key will be used interchangeably without making any distinctions.

V. MODIFIED ELGAMAL SIGNATURE SCHEME

Definition (MES): The modified ElGamal signature scheme [17] consists of the following three algorithms:
Key generation algorithm. Let p be a large prime and g be a generator of Zp. Both p and g are made public. For a random private key x € Z_p, the public key y is computed from y = g^x mod p.

Signature algorithm: The MES can also have many variants [18], [19]. For the purpose of efficiency, we will describe the variant, called optimal scheme. To sign a message m, one chooses a random k € Z_{p-1}, then computes the exponentiation r= g^k mod p and solves s from:

$$S= rxh(m, r) + k \bmod (p - 1); (1)$$

where h is a one-way hash function. The signature of message m is defined as the pair (r, s).

Verification algorithm: The verifier checks whether the signature equation gs=$ry^{rh(m,r)}$ mod p: If the equality holds true, then the verifier Accepts the signature, and Rejects otherwise.

VI. RELATED WORK

Message authentication is one of the most effective ways to prevent the corrupted and unauthorized message from being affected in wireless sensor network. To overcome this, based on their various key cryptosystems many message authentication scheme has been developed. Some of them have the limitations in addition to lack of scalability and resilience to node compromise attacks. The authors have introduced a polynomial-based scheme to address these issues. This scheme and its extension also have the weakness of a built-in threshold determined by the degree of the polynomial. The author's scheme is more efficient than the polynomial-based approach on basis of both theoretical analysis and simulation results demonstrate. The authors provide hop-by-hop message authentication without the weakness of the built in threshold of the polynomial-based scheme. The authors have also discussed the possible techniques for compromised node identification [1]. Sensor networks are used for security compromises on a large scale. A compromised node if transferred in large quantities of false sensing reports which, if detected, would be passed on to the main target. Attack by such sensors can cause false alarms and the depletion of the finite amount of energy in a battery powered network. So the authors have introduced a Statistical En-route Filtering (SEF) mechanism that can detect and drop such false reports. It requires each sensing report be verified by multiple keyed message authentication codes (MACs), each generated by a node that detects the same event. SEF's detection and filtering power increases with the deployment density and the sensor field size. The author's analysis and simulation

DOI 10.17148/IJARCCE.2015.49113

results show that SEF can detect false reports even when the attacker has obtained the security keys from a number of compromised nodes, as long as those keys belong to a small number of the key pool partitions. It can filter out 80-90% false data by a compromised node within 10 forwarding hops [2]. Sensor networks are deployed in unattended environments, leaving these networks to false data injection attacks. In this attack an adversary injects false data into the network with the goal of attacking the base station or depleting the resources of the relaying nodes. These attacks cannot be prevented by the Standard authentication mechanisms. In this paper, the authors have presented an authentication scheme to prevent these false data injection attack on sensor network. This scheme guarantees the detection of false data by the base station which works in the best case [3]. The authors have introduced a key distribution scheme for dynamic conferences in which an offline trusted server distributes the information to a set of users. Any group of users can compute a common security key. The authors have studied the application of such perfectly secure systems. In this setting, any group of some users can compute a common key by each user computing using only his private piece of information and the identities of the other group users. These keys would be secure against the coalition of the other users. If these users pool together their pieces then they cannot compute anything about a key of the previous users. The authors have introduced a non-interactive model where users compute the common key without any interaction. The authors have also shown some various applications and useful modification of their basic scheme [4].

ACKNOWLEDGMENT

Success is the manifestation of diligence, inspiration, motivation and innovation. I attribute my success in this venture to my guide **Prof. P. A. Khodke** who showed the guiding light at every stage of my paper preparation. I indebted to **Prof. N. V. Thakur**, Dean, Department of Computer Engineering, who has provided facilities and the infrastructure to work at an extended ends. Last but not the least I am also thankful to all the faculty members for helping directly or indirectly to accomplish the paper work.

REFERENCES

[1] Jian Li Yun Li Jian Ren Jie Wu "Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks" 1045-9219/13/$31.00 © 2013 IEEE.

[2] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering false data in sensor networks," in *IEEE Symposium on Security and Privacy*, 2004.

[3] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," in *Advances in Cryptology - Crypto'92*, ser. Lecture Notes in Computer Science Volume 740, 1992, pp. 471–486.

[4] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and compromiseresilient message authentication in sensor networks," in *IEEE INFOCOM*, Phoenix, AZ., April 15-17 2008.

[5] A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in *IEEE Symposium on Security and Privacy*, May 2000.

[6] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking cryptographic schemes based on "perturbation polynomials"," Cryptology ePrint Archive, Report 2009/098, 2009, http://eprint.iacr.org/.

[7] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications. of the Assoc. of Comp. Mach.*, vol. 21, no. 2, pp. 120–126, 1978.

[8] T. A. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[9] H. Wang, S. Sheng, C. Tan, and Q. Li, "Comparing symmetric-key and public-key based security schemes in sensor networks: A case study of user access control," in *IEEE ICDCS*, Beijing, China, 2008, pp. 11–18.

[10] D. Pointcheval and J. Stern, "Security proofs for signature schemes," in *Advances in Cryptology - EUROCRYPT*, ser. Lecture Notes in Computer Science Volume 1070, 1996, pp. 387–398.

[11] D. Pointcheval and J. Stern, "Security Proofs for Signature Schemes," Proc. Advances in Cryptology (EUROCRYPT), pp. 387-398, 1996.

[12] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Comm. ACM, vol. 24, no. 2, pp. 84-88, Feb. 1981.

[13] D. Chaum, "The Dinning Cryptographer Problem: Unconditional Sender and Recipient Untraceability," J. Cryptology, vol. 1, no. 1, pp. 65-75, 1988.

[14] A. Pfitzmann and M. Hansen, "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management a Proposal for Terminology," http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf, Feb. 2008.

[15] A. Pfitzmann and M. Waidner, "Networks without User Observability— Design Options.," Proc. Advances in Cryptology (EUROCRYPT), vol. 219, pp. 245-253, 1985.

[16] M. Reiter and A. Rubin, "Crowds: Anonymity for Web Transaction," ACM Trans. Information and System Security, vol. 1, no. 1, pp. 66-92, 1998.

[17] M. Waidner, "Unconditional Sender and Recipient Untraceability in Spite of Active Attacks," Proc. Advances in Cryptology (EUROCRYPT), pp. 302-319, 1989.

[18] D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," J. Cryptology, vol. 13, no. 3, pp. 361- 396, 2000.

[19] L. Harn and Y. Xu, "Design of Generalized ElGamal Type Digital Signature Schemes Based on Discrete Logarithm," Electronics Letters, vol. 30, no. 24, pp. 2025-2026, 1994.

[20] K. Nyberg and R.A. Rueppel, "Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem," Proc. Advances in Cryptology (EUROCRYPT), vol. 950, pp. 182-193, 1995.

[21] R. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," Proc. Advances in Cryptology (ASIACRYPT), 2001.

[22] M. Bellare and P. Rogaway, "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols," Proc. ACM First Conf. Computer and Comm. Security (CCS '93), pp. 62-73, 1993.

[23] "Cryptographic Key Length Recommendation," http://www.keylength.com/en/3/, 2013.

[24] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and compromise resilient message authentication in sensor networks," in IEEE INFOCOM, Phoenix, AZ., April 15-17 2008.

[25] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications. of the Assoc. of Comp. Mach., vol. 21, no. 2, pp. 120–126,

[26] H. Wang, S. Sheng, C. Tan, and Q. Li, "Comparing symmetric-key and public-key based security schemes in sensor networks: A case study of user access control," in IEEE ICDCS, Beijing, China, 2008, pp. 11–18.

[27] L. Harn and Y. Xu, "Design of generalized El-Gamal type digital signature schemes based on discrete logarithm," Electronics Letters, vol. 30

[28] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking crypto10 graphic schemes based on "perturbation polynomials"," Cryptology ePrint Archive, Report 2009/098, 2009.

[29] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications. of the Assoc. of Comp. Mach., vol. 21.

[30] Elliptic Curve Cryptography and Digital Rights Management Lecture Notes on "Computer and Network Security" by Avi Kak February 26, 2013.