© 2016 IJSRSET | Volume 2 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Review on Implementation of Message Authentication Scheme for Elliptic Curve Cryptography in Wireless Sensor Networks

Mangesh M. Ghonge*, Minal S. Kale

Department of Computer Science, Jagadambha College of Engineering & Technology, Yavatmal, Maharashtra, India

ABSTRACT

Message authentication is one of the most effective ways to thwart unauthorized and corrupted messages from being forwarded in wireless sensor networks (WSNs). 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. In this paper, we propose a scalable authentication scheme based on elliptic curve cryptography (ECC). While enabling intermediate nodes authentication, our proposed scheme allows any node to transmit an unlimited number of messages without suffering the threshold problem. In addition, our scheme can also provide message source privacy.

Keywords: Hop-by-hop authentication, symmetric-key cryptosystem, public-key cryptosystem, source privacy, simulation, wireless sensor networks (WSNs), distributed algorithm, decentralized control

I. INTRODUCTION

Message authentication plays a key role in thwarting unauthorized and corrupted packets from being circulated in networks to save precious sensor energy. For this reason, many schemes have been proposed in literature to provide message authenticity and integrity in network communications [1], [2]. These schemes can largely be divided into public-key-based and symmetric-key-based approaches. A secret polynomial-based message authentication scheme was introduced in [1]. To thwart the intruder from recovering the polynomial by computing the coefficients of the polynomial, the idea of adding random noise, called a perturbation factor, to the polynomial was proposed [2]. However, a recent study shows that the random noise can be completely removed from the polynomial using error-correcting code techniques [3]. In this paper, we propose an unconditionally secure and efficient source anonymous message authentication (SAMA) scheme, based on the optimal modified ElGamal signature (MES) scheme on elliptic curves. This MES scheme is secure against no-message attacks and adaptive chosen-message attacks in the random oracle model

[4]. our scheme enables the intermediate nodes to authenticate the message so that all corrupted packets can be dropped to conserve sensor power. While achieving compromise-resiliency, flexible-time authentication and source identity protection, our scheme does not have the threshold problem. Both theoretical analysis and simulation results demonstrate that our proposed scheme is more efficient than the polynomial-based algorithms under comparable security levels.

II. METHODS AND MATERIAL

A. Literature Review

A secret polynomial-based message authentication scheme was introduced in [1]. This scheme offers information theoretic security with ideas similar to a threshold secret sharing scheme, where the threshold is determined by the degree of the polynomial. When the number of messages transmitted is below the threshold, the scheme enables the intermediate node to verify the authenticity of the message through polynomial evaluation. However, when the number of messages transmitted is larger than the threshold, the polynomial can be fully recovered and the system becomes completely broken. To increase the threshold and the complexity for the intruder to break the secret polynomial, random noise, also called a perturbation factor, was added to the polynomial in [2]. The main idea is to thwart the adversary from computing the coefficient of the polynomial. However, the added perturbation factor can be completely removed using error-correcting code techniques [3]. The recent progress on elliptic curve cryptography (ECC) shows that the public-key schemes can be more advantageous in terms of memory usage, message complexity, and security resilience since public-key-based approaches have simple and clean key management [7]. The existing anonymous communication protocols are largely stemmed from mix net [8]. A mix net provides anonymity via packet re-shuffling through a set of mix servers (with at least one being trusted). Recently, message sender anonymity based on ring signatures was introduced [9]. This approach enables the message sender to generate a source-anonymous message signature with content authenticity assurance. The original scheme has very limited flexibility and very high complexity. Moreover, the original paper only focuses on the cryptographic algorithm, and the relevant network issues were left unaddressed.

B. Terminology and Preliminary

In this section, we will briefly describe the terminology and the cryptographic tools that will be used in this paper.

i. Threat Model and Assumptions

The WSNs are assumed to consist of a large number of sensor nodes. We assume that each sensor node knows its relative location in the sensor domain and is capable of communicating with its neighboring nodes directly using geographic routing. The whole network is fully connected through multi-hop communications. We assume there is a security server (SS) that is responsible for generation, storage and distribution of the security parameters among the network. This server will never be compromised. However, after deployment, the sensor nodes may be captured and compromised by attackers. Once compromised, all information stored in the sensor nodes can be accessed by the attackers. The compromised nodes can be reprogrammed and fully controlled by the attackers. However, the compromised nodes will not be able to create new public keys that can be accepted by the SS and other nodes.

ii. Design Goals

Our proposed authentication scheme aims at achieving the following goals:

Message authentication- The message receiver should be able to verify whether a received message is sent by the node that is claimed or by a node in a particular group. In other words, the adversaries cannot pretend to be an innocent node and inject fake messages into the network without being detected.

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

Hop-by-hop message authentication- Every forwarder on the routing path should be able to verify the authenticity and integrity of the messages upon reception.

Identity and location privacy-The adversaries 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 compromised, the remaining nodes can still be secure.

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

iii. Terminology

Privacy is sometimes referred to as anonymity. Communication anonymity in information management has been discussed in a number of previous works. 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 ¼ fA1; A2; . . .;Ang, the actual message sender. At; 1 _ t _ n, produces an anonymous message S (m) using its own private key d_t.
- **Verify S (m).** Given a message m and an anonymous message SðmÞ, 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 unforgeable 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.

iv. Modified Elgamal Signature Scheme

Definition 2 (MES) - The modified ElGamal signature scheme consists of the following three algorithms:

- **Key generation algorithm**. Let p be a large prime and g be a generator: Both p and g are made public. For a random private key x, the public key y is computed from $y = g^x \bmod p$.
- **Signature algorithm**. The MES can also have many variants. For the purpose of efficiency, we will describe the variant, called optimal scheme. To sign a message m, one chooses a random k , then computes the exponentiation $r = g^k \bmod p$ and solves s from:

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

  where h is a one-way hash function. signature of message m is defined as the pair(r, s).
- **Verification algorithm**. The verifier checks whether the signature equation $g^s = ry^{rh(m, r)} \bmod p$: If the equality holds true, then the verifier. Accepts the signature, and rejects otherwise.

C. Proposed Source Anonymous Message Authentication On Elliptic Curves

In this section, we propose an unconditionally secure and efficient SAMA. The main idea is that for each message m to be released, the message sender, or the sending node, generates a source anonymous message authenticator for the message m. The generation is based on the MES scheme on elliptic curves. For a ring signature, each ring member is required to compute a forgery signature for all other members in the AS. In our scheme, the entire SAMA generation requires only three steps, which link all non-senders and the message sender to the SAMA alike. In addition, our design enables the SAMA to be verified through a single equation without individually verifying the signatures.

D. Analysis of Problem

The public-key based approach, each message is transmitted along with the digital signature of the message generated using the sender's private key. Every intermediate forwarder and the final receiver can authenticate the message using the sender's public key. One of the limitations of the public-key based scheme is the high computational overhead. Computational complexity, memory usage, and security resilience, since public-key based approaches have a simple and clean key management.

Disadvantage of Existing System

- High computational and communication overhead.
- Lack of scalability and resilience to node compromise attacks.
- Polynomial-based scheme have the weakness of a built-in threshold determined by the degree of the polynomial.

III. RESULTS AND DISCUSSION

A. Proposed Work & Objectives

- We propose an unconditionally secure and efficient SAMA. The main idea is that for each message m to be released, the message sender, or the sending node, generates a source anonymous message authenticator for the message m.
- The generation is based on the MES scheme on elliptic curves. For a ring signature, each ring member is required to compute a forgery signature for all other members in the AS.
- In our scheme, the entire SAMA generation requires only three steps, which link all non-senders and the message sender to the SAMA alike. In addition, our design enables the SAMA to be verified through a single equation without individually verifying the signatures.
- After generates a source anonymous message authenticator for the message m, sender will use shortest path among multiple possible path from sender to receiver.

Advantages of Proposed System

- A novel and efficient SAMA based on ECC. While ensuring message sender privacy, SAMA can be applied to any message to provide message content authenticity.
- To provide hop by hop message authentication without the weakness of the built- in threshold of the polynomial-based scheme, we then proposed a hop-by-hop message authentication scheme based on the SAMA.
- When applied to WSNs with fixed sink nodes, we also discussed possible techniques for compromised node identification.

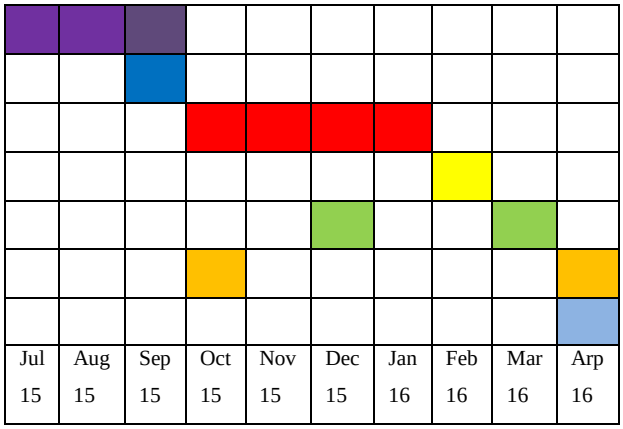
B. Expected Outcome

In this project, we first proposed a novel and efficient source anonymous message authentication scheme (SAMA) based on elliptic curve cryptography (ECC). While ensuring message sender privacy, SAMA can be applied to any messages to provide hop-by-hop message content authenticity through shortest path without the weakness of the built-in threshold of the polynomial-based scheme.

C. Plan Of Research

Below table show the step wise plans to complete my project within this academic year 2015-16.

RESEARCH PLANNING



	Literature Survey
	Analysis & Detailed Study
	Implementation

	Verification of Design
	Intermediate Result & Final Result Analysis
	Thesis Writing & Submission
	Paper Publications

IV. CONCLUSION

In this paper, we first implement the message authentication scheme elliptic curve cryptography in wireless sensor networks and efficient SAMA based on ECC. While ensuring message sender privacy, SAMA can be applied to any message to provide message content authenticity. To provide hop by hop message authentication without the weakness of the built in threshold of the polynomial based scheme, we then proposed a hop by hop message authentication scheme based on a SAMA. When applied to WSNs with fixed sink nodes, we also discussed possible techniques for compromised node identification. We compared our proposed scheme with the bivariate polynomial-based

scheme through simulations using ns-2 and TelosB. Both theoretical and simulation results show that in comparable scenarios, our proposed scheme is more efficient than the bivariate polynomial-based scheme in terms of computational overhead, energy consumption, delivery ratio, message delay, and memory consumption.

V. REFERENCES

[1] 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, Lecture Notes in Computer Science Volume 740, pp. 471–486, 1992.

[2] 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.

[3] 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/.

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

[5] L. Harn and Y. Xu, "Design of generalized ElGamal type digital signature schemes based on discret logarithm," Electronics Letters, vol. 30, no. 24, pp. 2025–2026, 1994.

[6] K. Nyberg and R. A. Rueppel, "Message recovery for signature schemes based on the discrete logarithm problem," in Advances in Cryptology - EUROCRYPT, Lecture Notes in Computer Science Volume 950, pp. 182– 193, 1995.

[7] 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), pp. 11–18, 2008.

[8] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Communications of the ACM, vol. 24, pp. 84–88, February 1981.

[9] R. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in Advances in Cryptology–ASIACRYPT, Lecture Notes in Computer Science, vol 2248/2001, Springer Berlin / Heidelberg, 2001.