INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Message Authentication between the Nodes using modified El-Gamal Signature on Elliptic Curve

Chinnaswamy C.N[1], Natesha B V[2]

[1]Associate Professor Department of IS & Engineering,
National institute of engineering, Mysore-570 008
[2]II[nd] year M-Tech, Computer Network Engineering,
National institute of engineering, Mysore-570 008

Abstract : *Message authentication is one of the most effective way to thwart an intruder who can compromise with the nodes and can access to the data and corrupt the data in wireless sensor network, many conventional methods have been developed to solve the problem that message being corrupted such as symmetric key cryptography and public key cryptography ,but they have their own problems such as threshold overhead and key management and computation overhead and scalability .In order to overcome these problem developed a new authentication scheme using the elliptic curve cryptography while enabling the intermediate node Authentication .*

Index terms: *Authentication, Elliptic Curve, Symmetric Key Cryptography, Public Key Cryptography.*

1. 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]. These schemes can largely be divided into two categories: public-key based approaches and symmetric-key based approaches. The symmetric-key based approach [2]-[3] 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. In symmetric key approach message authenticity and integrity can only provided only between the nodes with shared key, so an intruder can compromise with the nodes and access to the key.

The second approach is polynomial based approach which is developed to provide the scalability which is based on the information, security is provided by sharing the threshold where threshold means the degree of the polynomial, if the number of the message transmitted is less than the threshold authenticity can be provided if the number of messages greater than the threshold the authentication will not be provided. An alternative solution was proposed in to thwart the intruder from recovering the polynomial by computing the coefficients of the polynomial. The idea is to add a random noise, also called a perturbation factor, to the polynomial so that the coefficients of the polynomial cannot be easily solved. However, a recent study shows that the random noise can be completely removed from the polynomial using error-correcting code techniques.

For 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. The recent progress on elliptic curve cryptography (ECC) shows that the public-key schemes can be more advantageous in terms of computational complexity, memory usage, and security resilience, since public-key based approaches have a simple and better key computation.

Here we propose an unconditionally secure and efficient source anonymous message authentication (SAMA) scheme based on the optimal modified El-Gamal signature (MES) [4]-[6] scheme on elliptic curves. This MES scheme is secure against adaptive chosen-message attacks which provide the source privacy and corrupted message can be identified and minimize the node processing power. The recent progress on elliptic curve cryptography (ECC) shows that the public-key schemes can be more advantageous in terms of computational complexity, memory usage, and security resilience, since public-key based approaches have a simple and clean key management Which also helps in achieving compromise-resiliency, flexible-time authentication and source identity protection, our scheme does not have the threshold problem.

2. LITERATURE SURVEY

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

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

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 happens in wireless sensor networks are:

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

3. PROPOSED METHOD

a. Proposed Method achieves the Following

- **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
- **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.
- **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.

b. Source Anonymous Message Authentication Scheme on Elliptic Curve

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.

c. Why elliptic curve cryptography

The computational overhead of the RSA-based approach to public-key cryptography increases with the size of the keys. Elliptic curve cryptography (ECC) [7] can provide the same level and type of security as RSA but with much shorter keys. Table 1 shows comparison of the key size used in the different kind of cryptographic, it shows that the elliptic curve cryptographic algorithms which requires the shorter key size and which increase the speed of the computation and expand the application of the cryptographic algorithm usage in many real time application such as e-commerce and mobile mobility.

Table 1: Compares the key sizes for three different approaches to encryption for comparable levels of security against brute-force attacks.

Symmetric encryption Key size in bits	RSA and Diffie – Hellman key size in bits	ECC key size In bits
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

d. Definition of the Algorithms

1. A SAMA (Source Anonymous Message Authentication) consists of the following two algorithms:

- **Generate** (m,Q1,Q2,.,.,.,Qn): Given a message m and the public keys Q_1,Q_2,Q_3. . . . . , Q_n of the AS S ={A1,A2,.,.,.,An}, the actual message sender At, $1< t \leq n$, produces an anonymous message S(m) using its own private key d
- **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.

2. Modified El-Gamal signature scheme consists of the following three algorithms:

- **Key generation algorithm:** Let p be a large prime and g be a generator of Z_p*. Both p and g are made public. For a random private key $x \in Z_p$*, the public key y is computed from y = gx mod 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 ∈ Zp^*−1, then computes the exponentiation r = gk mod p and , Solves s from: s = rxh (m, r) + k mod (p − 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.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Key management is one of the major issues for secret-key based authentication schemes. This is especially true for large scale WSNs. While many of these schemes are designed to provide node authentication, they can only provide end-to-end node authentication using the secret key shared between the two nodes, which implies that only the receiver can verify the authenticity of the messages en-route. This means that no intermediate node can authenticate the message in general. The intermediate nodes may have to forward a manipulated message for many hops before the message can finally be authenticated and dropped by the receiving node. This not only consumes extra sensor power, but also increases the network collision and decreases the message delivery ratio. In addition to performance improvement, enabling intermediate node authentication will thwart adversaries from performing denial-of service attacks through message manipulation to deplete the energy and communication resources of the wireless network. Therefore, developing a protocol that can provide hop by hop intermediate node authentication is an important research task. Most of the authentication schemes are based on symmetric key schemes, including the polynomial evaluation based threshold authentication scheme. The secret bi-variate polynomial is defined as

$$f(x, y)= \sum_{i=0}^{dx} \sum_{j=0}^{dy} A_{i,j} x^i y^j \qquad (i)$$

where each coefficient Ax,y is an element of a finite field Fp, and d_x and dy are the degrees of this polynomial. dx and d_y are also related to the message length and the computational complexity of this scheme. From the performance aspect, d_x and d_y should be as short as possible.

On the other hand, it is easy to see that when either more than $d_y + 1$ messages transmitted from the base station are received and recorded by the intruders, or more than $d_x + 1$ sensor nodes have been compromised, the intruders can recover the polynomial f(x, y) via Lagrange interpolation. In this case, the security of the system is totally broken and the system cannot be used anymore. This property requires that both d_x and d_y be very large for the scheme to be resilient to node compromise attacks.

An alternative approach based on perturbation of the polynomial was also explored. The main idea is to add a small amount of random noise to the polynomial in the original scheme so that the adversaries will no longer be able to solve the coefficients using Lagrange interpolation. However, this technique is proved to be vulnerable to security attacks, since the random noise can be removed from the polynomial using error-correcting techniques.

While hop-by-hop authentication can be achieved through a public-key encryption system, the public-key based schemes were generally considered as not preferred, mainly due to their high computational overhead. However, our research demonstrates that it is not always true, especially for elliptic curve public-key cryptosystems. In our scheme, each SAMA contains an AS of n randomly selected nodes that dynamically changes for each message. For n = 1, our scheme can provide at least the same security as the bi-variate polynomial-based scheme. For n > 1, we can provide extra source privacy benefits. Even if one message is corrupted, other messages transmitted in the network can still be secure. Therefore, n can be much smaller than the parameters d_x and d_y. In fact, even a small n may provide adequate source privacy, while ensuring high system performance. In addition, in the bi-variate polynomial-based scheme, there is only one base station that can send messages. All the other nodes can only act as intermediate nodes or receivers. This property makes the base station easy to attack, and severely narrows the applicability of this scheme. In fact, the major traffic in WSNs is packet delivery from the sensor nodes to the sink node. In this case, our scheme enables every node to transmit the message to the sink node as a message initiator. The recent progress on elliptic curve cryptography (ECC) has demonstrated that the public-key based schemes have more advantages in terms of memory usage, message complexity, and security resilience, since public-key based approaches have a simple and clean key management.

e. Applications of elliptic curve cryptography

Because of much smaller key sizes in ECC algorithms can be implemented on smart cards without much mathematical co processors, ECC can be used in the proliferation of the mobile devices and E-commerce, such as online transactions where user has to provide some private credentials and digital signature generation for the authentication purpose, secure browser sessions and it can be used where security is needed but lacks the power storage and computational power that is necessary for our present day applications.

4. CONCLUSION

Proposed source anonymous message authentication scheme using the modified El-Gamal signature on elliptic curve in order to provide the message authentication between nodes in a wireless sensor network. Elliptic curve cryptography which is similar to the public key cryptography methods such as RSA and other but it requires less computation and it is very useful in the proliferation of the mobile devices due to the use of shorter key.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

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

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

[6] 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.

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

AUTHORS

1) CHINNASWAMY C N

Associate Professor, Department Of Information Science & Engineering at National Institute Of Engineering Mysore.
Email-id: **chinnaswamynie@gmail.com**

2) NATESHA B V

M-tech in Computer Network Engineering, Department of Information Science & Engineering, at National Institute Of Engineering, Mysore.
Email-id: **nateshbv18@gmail.com**