A Novel Privacy Protocol for Message Authentication in Hop-by-Hop Wireless Sensor Networks

Sumala Hemababu [#1], Majji Venkata Appala Naidu [*2]

M.tech Scholar [#1], Associate Professor [*2]
Department of Computer Science & Engineering,
Sri Sivani College Of Engineering,
Etcherla, Srikakulam Dist (INDIA).

Abstract

In wireless sensor networks message authentication plays a very effective way to identify unauthorized and corrupted messages from being forwarded. To avoid these attacks many message authentication schemes have been developed till to date, based on either symmetric key cryptosystems or public key cryptosystems. Most of them, however, have the limitations of high computational and communication overhead. To address these problems, a new polynomial-based scheme was recently introduced based on threshold function. In this paper, we propose a scalable authentication scheme based on new elliptic curve cryptography (NECC),While enabling several 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. By conducting various theoretical analysis and simulation results, we finally demonstrate that our proposed scheme is more efficient than the polynomial-based approach in terms of computational and communication overhead under comparable security levels while providing message source privacy.

Keywords

Hop-by-hop authentication, crypto system, public-key cryptosystem, decentralized control

1. Introduction

In wireless sensor networks message authentication plays a very effective way to identify unauthorized and corrupted messages from being forwarded in networks to save the precious sensor energy. To solve these problems, many authentication schemes have been proposed in literature till today to provide message authenticity [1]–[5] and integrity verification for wireless sensor networks (WSNs)**.** These schemes can mainly be divided into two categories: public-key based approaches and private-key based approaches.

The shared key which is generated between sender and receiver is used by the sender to generate a message authentication code (MAC) for each transmitted message. However, for this proposed method, the authentication 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 who enters internally can compromise the key by capturing a single sensor node. In addition, this method does not work in multicast networks.

For the public-key based encryption method, each and every message is transmitted along with the digital signature of the message generated using the sender's private key. For authentication of that message, every intermediate

user and the final receiver use the sender's public key [7], [8]. One of the major limitations of the public key based encryption method is the high computational and communication overhead. There have been a recent progress on new elliptic curve cryptography (NECC) which 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 [9].

The major contributions of this paper are the following:

1) I have developed a novel source anonymous message authentication code (NSAMAC) on elliptic curves that can provide always unconditional source anonymity.
2) I have developed an efficient hop-by-hop message authentication mechanism for WSNs without the threshold limitation.
3) I have monitored network implementation criteria on source node privacy protection in WSNs.
4) I have proposed an efficient key management framework to ensure isolation of the compromised nodes.
5) I have provided extensive simulation results under ns-2 and TelosB on multiple security levels.

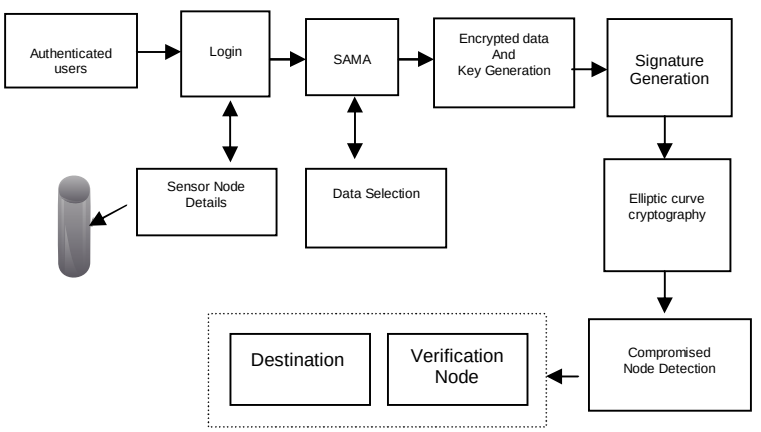


Figure 1. System Architecture

2. Related Work and Assumptions

In this section, we mainly discuss the literature which is clearly related with our proposed implementation method in wireless sensor networks.

2.1 Attacking Cryptographic Schemes Based on Perturbation Polynomials

We show attacks on several cryptographic schemes that have recently been proposed for achieving various security goals in sensor networks. Roughly speaking, these schemes all use "Perturbation polynomials" to add "noise" to polynomial based systems that offer information-theoretic security, in an attempt to increase the resilience threshold while maintaining efficiency. We show that the heuristic security arguments given for these modified schemes do not hold, and that they can be completely broken once we allow even a slight extension of the parameters beyond those achieved by the underlying information-theoretic schemes. Our attacks apply to the key redistribution scheme .the access-control schemes and the authentication schemes of our results cast doubt on the viability of using "perturbation polynomials" for designing secure cryptographic schemes[10].

2.2 Interleaved Hop-by-Hop Authentication against False Data Injection Attacks in Sensor Networks

Sensor networks are often deployed in unattended environments, thus leaving these networks vulnerable to false data injection attacks in which an adversary injects false data into the network with the goal of deceiving the base station or depleting the resources of the relaying nodes. Standard authentication mechanisms cannot prevent this attack if the adversary has compromised one or a small number of sensor nodes.

We present three interleaved hop-by-hop authentication Schemes that guarantee that the base station can detect injected false data immediately when no more than t nodes are compromised [11], where t is a system design parameter. Moreover, these Schemes enable an intermediate forwarding node to detect and discard false data packets as early as possible. Our performance analysis shows that our scheme is efficient with respect to the Security it provides, and it also allows a tradeoff between security and performance. A prototype Implementation of our scheme indicates that our scheme is practical and can be deployed on the Current generation of sensor nodes.

3. Proposed New Source Anonymous Message Authentication (NSAMA) On Elliptic Curves

In this section, we propose an unconditionally secure and efficient source anonymous message authentication scheme (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.

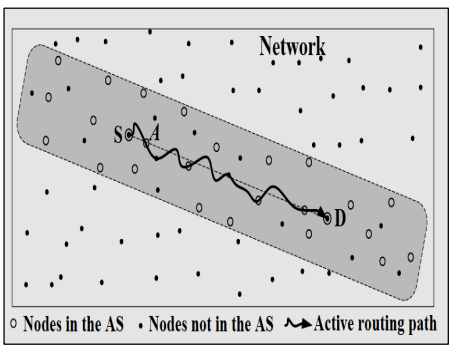


Figure 2. Anonymous set selection in active routing

A. Proposed MES Scheme on Elliptic Curves

Let $p > 3$ be an odd prime. An elliptic curve E is defined by an equation of the form:

$$E: \; y^2 = x^3 + ax + b \bmod p,$$

where $a, b \in \mathbb{F}_p$, and $4a^3 + 27b^2 \not\equiv 0 \bmod p$. The set $E(\mathbb{F}_p)$ consists of all points $(x, y) \in \mathbb{F}_p$ on the curve, together with a special point $\mathcal{O}$, called the point at infinity.

Let $G = (x_G, y_G)$ be a base point on $E(\mathbb{F}_p)$ whose order is a very large value N. User A selects a random integer $d_A \in [1, N-1]$ as his private key. Then, he can compute his public key Q_A from $Q_A = d_A \times G$.

Signature generation algorithm: For Alice to sign a message m, she follows these steps:

1) Select a random integer k_A, $1 \le k_A \le N-1$.
2) Calculate $r = x_A \bmod N$, where $(x_A, y_A) = k_A G$. If $r = 0$, go back to step 1.
3) Calculate $h_A \xleftarrow{l} h(m, r)$, where h is a cryptographic hash function, such as SHA-1, and $\xleftarrow{l}$ denotes the l leftmost bits of the hash.
4) Calculate $s = r d_A h_A + k_A \bmod N$. If $s = 0$, go back to step 2.
5) The signature is the pair (r, s).

Signature verification algorithm: For Bob to authenticate Alice's signature, he must have a copy of her public key Q_A, then he:

1) Checks that $Q_A \neq \mathcal{O}$, otherwise invalid
2) Checks that Q_A lies on the curve
3) Checks that $nQ_A = \mathcal{O}$

After that, Bob follows these steps to verify the signature:

1) Verify that r and s are integers in $[1, N-1]$. If not, the signature is invalid.
2) Calculate $h_A \xleftarrow{l} h(m, r)$, where h is the same function used in the signature generation.
3) Calculate $(x_1, x_2) = sG - rh_A Q_A \bmod N$.
4) The signature is valid if $r = x_1 \bmod N$, invalid otherwise.

In fact, if the signature is correctly generated, then:

$$\begin{aligned}(x_1, x_2) &= sG - rh_A Q_A \\ &= (rd_A h_A + k_A)G - rh_A Q_A \\ &= k_A G + rh_A Q_A - rh_A Q_A \\ &= k_A G.\end{aligned}$$

Therefore, we have $x1 = r$, and the verifier should Accept the signature.

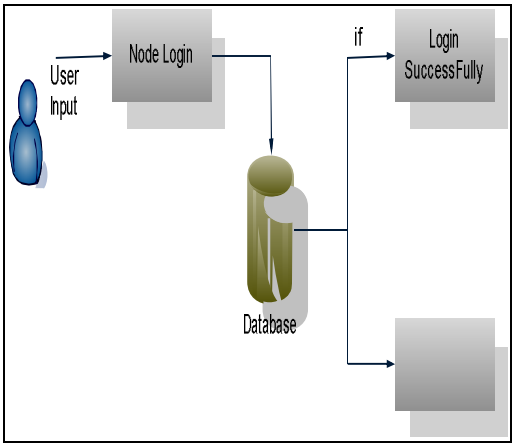
4. Implementation Modules

Implementation is a stage where the theoretical design is automatically converted into practical form. This is mainly divided into following five modules.

1. Sensor Node deployment Module
2. Authenticate the Source Node and Message
3. Key Generation and Signature Generation
4. Compromised node detection
5. Node isolation.

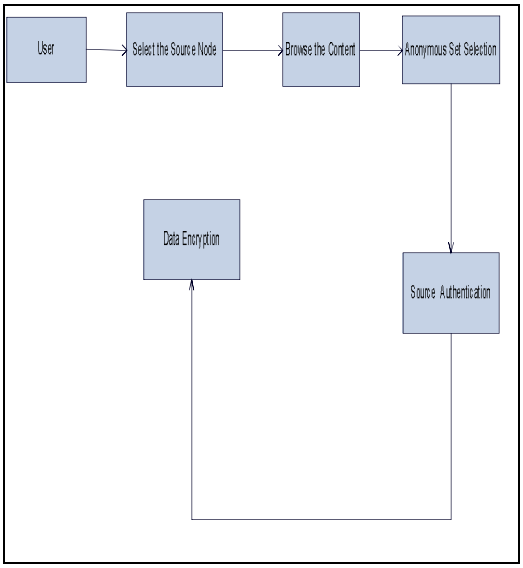
1. Sensor Node Deployment Module

In this module, we create Nodes and form a Network. Users enter the Node Name, IpAddress, port number, of the node to register in the Database. While entering the next node the user must check the database for that node exists or new one.



2. Authenticate the Source Node and Message

The users to select the source node then browse the content to provide the source node authentication. A security solution should scale for large group of receivers and long multi-hop paths. Thus, a solution that is based on a distinct authentication key for every receiver will introduce prohibitive overhead to the message and consume significant portion of the available bandwidth. Moreover, the solution should scale for large number of senders by requiring reasonable memory resources at the individual receivers for storing authentication keys. Finally, it is desired to enable the validation of every packet without excessive delay and independent of the other packets.

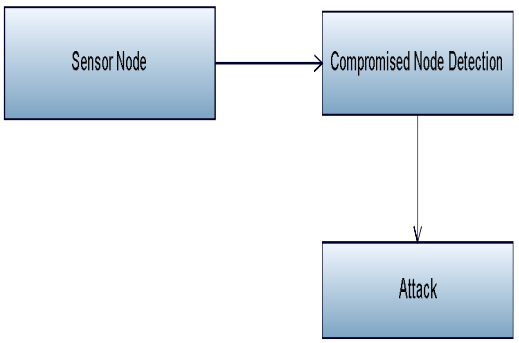


3. Key Generation and Signature Generation

The source generates the keys at the time of establishing session. The keys will be securely transmitted to the head of every packet that hosts one or multiple receivers. The multicast message is then transmitted to the authenticate the source and then deliver the message to the intended receivers.
After data encryption the key generation and signature generation are generated then send the data to the destination node via intermediate node. Finally, verify the content.

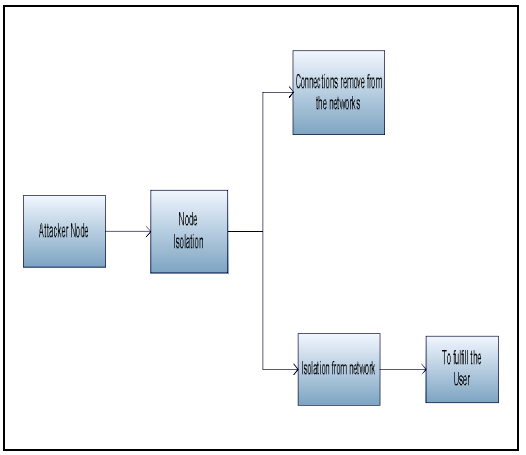
4. Compromised Node Detection

The compromise node detection are detected in this way find the misbehave node in the network. The misbehave node are find using security server in the network.



5. Node Isolation

After finding the attacker node it can isolate from the network or connections remove from the network. In this node cannot communicate other node. It can inform to all node in the network. Node Isolation may be the most intuitive way to prevent further attacks from being launched by malicious nodes in network.



5. Conclusion

The first proposed a novel and efficient new source anonymous message authentication scheme (NSAMA) based on elliptic curve cryptography (ECC). While ensuring message sender privacy, NSAMA 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 propose a hop-by-hop message authentication scheme based on the NSAMA. 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.

6. References

[1] F. Ye, H. Lou, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," in *IEEE INFOCOM*, March 2004.

[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. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *ComCommunications of the ACM*, vol. 24, no. 2, pp. 84–88, February 1981.

7. About the Authors

Sumala Hemababu is currently pursuing his 2 Years M.Tech (CSE) in Computer Science and Engineering at Sri Sivani College Of Engineering, Etcherla, Srikakulam District. His area of interests includes Networks Security.

Majji Venkata Appala Naidu is currently working as an Associate Professor in Computer Science and Engineering at Sri Sivani College Of Engineering, Etcherla, Srikakulam District. His research interests include Networks Security and Data Mining.