ELLIPTIC CURVE CRYPTOGRAPHY FOR MESSAGE AUTHENTICATION IN WSN

***Manjula M, ** Dr.T. Senthil Prakash , *** Ms.Ramya Raveendran**

**M.E Student, Shree Venkateshwara Hi-Tech Eng College, Erode-Gobi,India*
***Professor & HOD,Shree Venkateshwara Hi-Tech Eng College*
Erode-Gobi,India
****M.E Student, Shree Venkateshwara Hi-Tech Eng College*
Erode-Gobi,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). Message authentication schemes have been developed, based on either symmetric-key cryptosystems or public-key cryptosystems which, 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. While enabling intermediate Nodes authentication, proposed scheme allows any node to transmit an unlimited number of messages without suffering the threshold problem. In addition, this scheme can also provide message source privacy. Both theoretical analysis and simulation results demonstrate that 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; symmetric key cryptosystem; public-key cryptosystem; source privacy; Modified Elgamal Signature (MES); Elliptic Curve Cryptography (ECC)

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).These schemes can largely be divided in to 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.To solve the scalability problem, a secret polynomial based message authentication scheme was introduced.The idea of this scheme is similar to a threshold secret sharing, where the threshold is determined 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. When the number of messages transmitted is larger than the threshold, the polynomial can be fully recovered and the system is completely broken. An alternative solution was proposed in to thwart the intruder from recovering the polynomial. The random noise can be completely removed from the polynomial using error correcting code techniques.

RELATED WORK

In symmetric key and hash based authentication schemes were proposed for WSNs. In these schemes, each symmetric authentication key is shared by a group of sensor nodes. An intruder can compromise the key by capturing a single sensor node. Therefore, these schemes are not resilient to node compromise attacks. Another type of symmetric-key scheme requires synchronization among nodes. These schemes, including TESLA and its variants, can also provide message sender authentication. However, this scheme requires initial time synchro-nization, which is not easy to be implemented in large scale WSNs. In addition, they also introduce delay in message authentication, and the delay increases as the network scales up.

Message authentication are used in different applications and security is one of the key characteristic of all the applications for that, many authors proposed different kinds of security algorit hms like symmetric key algorithm and public key algorithm. Both passive and active attacks are discussed in that algorithms and also recovery mechanisms are shown in simulation. The advantages and disadvantages of such algorithms are discussed below.

A. Statistical Enroute Filtering

Statistical En-route Filtering (SEF) mechanism detects and drops false reports. SEF requires each sensing report must be validated by multiple keyed message authentication codes (MACs), each generated message by a node that detects the same event. As the report is forwarded, each node verifies the correctness of the MACs probabilistically and drops those invalid MACs at earliest points. The sink filters out remaining false reports that escape the enroute filtering. SEF exploits to determine the truthfulness of each report through collective decision-making by multiple detecting nodes and collective false-report-detection by multiple forwarding.

For the public-key based approach, each message is transmitted along with the digital signature of the mes-sage generated using the sender's private key. Every intermediate forwarder and the final receiver can authen-ticate the message using the sender's public key. The recent progress on 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 a simple and clean key management.

B. *Secret Polynomial Message Authentication*

A secret polynomial based message authentication scheme was introduced to prevent message form adversaries. This scheme offers security with ideas similar to a threshold secret sharing, where the threshold is determined by the degree of the polynomial. If the number of messages transmitted is below the threshold, then the intermediate node to verify the authenticity of the message through polynomial evaluation. When the number of messages transmitted is larger than the threshold, the polynomial be fully recovered by adversary and the system is broken completely.

SELECTION AND SOURCE PRIVACY

The appropriate selection of an AS plays a key role in mes-sage source privacy, since the actual message source node will be hidden in the AS. In this section, we will discuss techniques that can prevent the adversaries from tracking the message source through the AS analysis in combination with local traffic analysis. Before a message is transmitted, the message source node selects an AS from the public key list in the SS as its choice. This set should include itself, together with some other nodes. When an adversary receives a message, he can possi-bly find the direction of the previous hop, or even the real node of the previous hop. However, the adversary is unable to distinguish whether the previous node is the actual source node or simply a forwarder node if the adversary is unable to monitor the traffic of the previous hop.

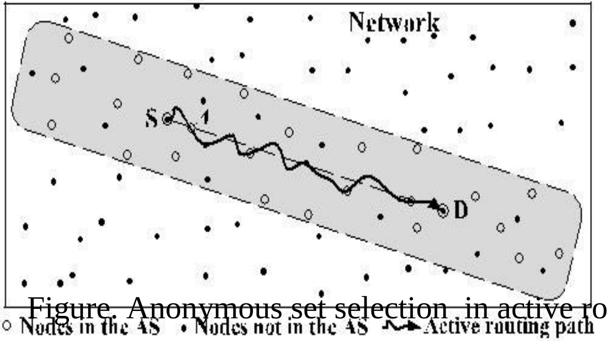

Figure. Anonymous set selection in active routing.

PROBLEM STATEMENT

Message authentication is one of the most effective ways to thwart unauthorized and corrupted messages from being forwarded in wireless sensor networks (WSNs). Most of them have the limitations of high computational and communication overhead in addition to lack of scalability and resilience to node compromise attacks. An intruder can compromise the key by capturing a single sensor node. In addition, symmetric key based method does not work in multicast networks. The intermediate node can verify the authenticity of message through polynomial evaluation. In polynomial based scheme, when the number of messages transmitted is larger than the threshold the adversary can fully recover the polynomial.

SYMMETRIC-KEY BASED APPROACH

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. In 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.

A. Secret Polynomial based message authentication

To solve the scalability problem, a secret polynomial based message authentication scheme was introduced. The idea of this scheme is similar to a threshold secret sharing, where the threshold is determined 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.

B. Perturbation Factor

An alternative solution was proposed 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. The random noise can be completely removed from the polynomial using error-correcting code techniques.

PUBLIC KEY BASED APPROACH

In the public-key based approach, each message is transmitted Along with the digital signature of the message generated using the sender’s p intermediate forwarder and the final receiver can authenticate the message using the sender’ publickey. 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.

A. Message Sender Anonymity

Message sender anonymity based on ring signatures was introduced. This approach enables the message sender to generate a source anonymous message signature with content authenticity assurance. To generate a ring signature, a ring member randomly selects an AS and forges a message signature for all other members. Then adversaries can trap-door information to glue the ring together. The original scheme has very limited flexibility and very high complexity

PERFORMANCE EVALUATION

A. Simulation Model And Parameters

To evaluate the performance of proposed system, compare it with some existing techniques using NS-2 Simulator. The bivariate polynomial based scheme is a symmetric key based implementation, while proposed scheme is based on ECC. Assume that the key size to be l for symmetric key cryptosystem, the key size for proposed should be 2l which is much shorter than the traditional public key cryptosystem. Thesimulation parameters are helpful in simulating the proposed system. Table 1 shows the process time for existing scheme and Table 2 shows the process time for proposed scheme.

B. Performance Metrics

The ECC scheme is compared against polynomial based and it has provided the positive results. Packet delivery ratio (PDR): PDR defines the ratio of the number of packets received by the destinationnode to the number of packets sent by the source node.

Routing overhead (RO): RO defines the ratio of the amount of routing-related transmissions [RouteREQuest (RREQ), Route REPly (RREP), Route ERRor (RERR), ACK, S-ACK, and MRA].

Delay: Delay is the interarrival time of 1stand 2ndpacket to that of total data packets delivered.

C.Results

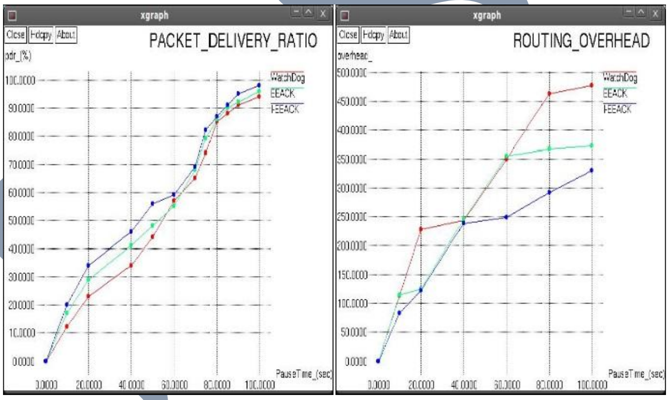

Figure C.Packet delivery Ratio and Routing overhead

Enhanced message authentication scheme is evaluated by comparing it with other existing algorithms using the NS-2 Simulator. Fig 4.1 shows Packet Delivery Ratio of the proposed method over other existing methods

CONCLUSION

The system is aimed to provide 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 message to provide message content authenticity. It also provides a hop-by-hop message authentication scheme based on the SAMA.

The implementation of the system provides more efficient than the bivariate polynomial based scheme in terms of computational overhead, energy consumption, delivery ratio, message delay, and memory consumption.

ACKNOWLEDGMENT

I thank Professor & HOD Dr. T. Senthil Prakash for valuable discussions during the early stages of this paper and thanks toMs. Ramya Raveendran for her helpful suggestion regarding the work and collecting the fabulous study materials .Last but not the least I want to say thanks to the anonymous reviewers for their valuable comments , suggestions and corrections.

REFERENCES

[1] "Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks ",Jian Li, Yun Li, Jian Ren, Senior Member, IEEE, and Jie Wu, Fellow, IEEE",2015.

[2] "Cryptographic Key Length Recommendation," http://www. keylength.com/en/3/, 2013. M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking Crypto-graphic Schemes Based on 'Perturbation Polynomials'," Report 2009/098, http://eprint.iacr.org/, 2009.

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

[4] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "Tinypk: Securing sensor networks with public key technology," ACM SASN'04,October 2004.

[5] F. Ye, H. Lou, Statistical.Lu,en-routeandfilteringLof.injectedZhang,falsedata in "sensor networks," IEEEinINFOCOM, March 2004.

[6] S. Zhu, S. Setia,As interleaved.Jajodia ,hop-by-hopauthentication and schemeP. For Ning, filteringfalse" data in sensor networks,"IEEE inSymposium on Security and Privacy, 2004.

[7] Blundo, A. De Santis, A. Herzberg,Perfectly-secureSkey. distributionKutten,for U dynamic conferences," Advancesin in Cryptology - Crypto'92,ser.Lecture Notes in Computer Science Volume 740, 1992, pp. 471–486.

[8] W. Zhang, N. Subramanian,Lightweight And compromise and Resilient G.Wang, messageauthentication in sensor networks," IEEEin INFOCOM, Phoenix, AZ., April 15-17 2008.

[9] M. Albrecht, C. Gentry,AttackingS.cryptographic Halevi,schemesand Jbased.Katz,on polynomials"," Cryptology ePrint Archive, Report 2009.