ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 13, March 2016

IMPROVING SECURITY WITH WATCHDOG SECURITY ASSOCIATION IN WSN

Maharaj C.B[1], student, Ruban Arul Raj M[2], student,

BalaPravin Singh[3],student,Kailasam S[4], student

[1, 2, 3,4]PSN College of Engineering and Technology,Tirunelveli, TN

***Abstract*—Message authentication is the important concept in the Wireless Sensor Network's. Most of the authentication schemes are using either the symmetric-key cryptosystems or the public-key cryptosystems. Each of them having their own advantages over other. By enabling the intermediate node authentication we can improve the source privacy in the WSN. In this paper we discuss about the SAMA based message authentication in the WSN. SAMA based scheme is more efficient than the polynomial-based approach. It is also used to reduce the file query delay based on the replication. It is efficient to enhance the file availability using replication protocols.**

***Index Terms*—cryptosystem, message authentication, polynomial-based scheme, SAMA, source privacy,trustedvalue,file availability.**

1. INTRODUCTION

BY enabling the message authentication we can consume a lot of energy in the wireless sensor networks. For the message authentication most of the network admins using either symmetric-key cryptosystems or the public-key cryptosystems or using both.

The symmetric-key based cryptosystems it requires a complex key management. In this method the message authenticity is verified by the shared key and that key is generated by the message authentication code (MAC).The symmetric-key based approach is well suitable for the single cast networks but it's not suitable for the multicast network. Because for each of the single message transmitted sender and the receiver have to use the shared key. It is more complicated one in the multicast networks.

In the public-key cryptosystems digital signature is used for transmitting the message which is generated by the message sender. This is more advantageous than the symmetric-key systems in terms of the memory usage, security, computational complexity.

In this paper, we propose a secure and efficient source anonymous message authentication (SAMA) scheme based on the optimal modified ElGamal signature (MES) scheme on elliptic curves. This MES technique is secure against adaptive chosen-message attacks. As we said before by enabling the intermediate nodes to authenticate the message so that all corrupted message can be detected and dropped to conserve the sensor power. In the SAMA based message authentication we doesn't face the threshold problem.

This paper is organized as follows:

Section 2 presents the existing system inthe message authentication and the Section 3 is about proposed system for the message authentication Section 4 describes performance analysisand in Section 5 output of this paper we conclude this paper in section 6.

2. *EXISTING SYSTEM IN THE MESSAGE AUTHENTICATION*

Most of the WSN'S using symmetric-key and hash based authentication for sharing the message in the sensor node. By using these schemes we have to share the authentication key among the sensor nodes. If an intruder can compromise the single node the whole network becomes the vulnerable one. Another type of the symmetric-key approach requires synchronization among the nodes in the entire network. This is suitable for the small scale networks. Because it requires the initial time synchronization and delay is increased in significant manner when the network is scales up.

A secret polynomial based message authentication scheme is also used for the message authentication. This scheme offers threshold secret sharing between the nodes, here the threshold is predetermined 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. However, when the number of messages transmitted is larger than the threshold, the polynomial can be fully recovered and the system is completely broken. To increase the threshold and the complexity for the intruder to reconstruct the secret polynomial, a random noise, also called a perturbation factor, was added to the polynomial in 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.

In the public-key based approach messages are transmitted along with the digital signature of the message which is generated by the sender's private key. By this key all the nodes in the network can authenticate the message. Public-key approaches have a simple key management.

In the existing systems mix net or the DC-net protocols are widely used. A mix net provides source privacy by using the packet re-shuffling through the mix net servers. In a mixnet, message sender encrypts the transmitted message, and the ID of the recipient, using the public key of the mix. Since the mix net protocols have some advantages they are unable to provide provable source privacy.DC-net is an anonymous multi-party computation scheme. Some pairs of the participants are required to share secret keys. DC-net provides perfect sender anonymity without requiring trusted servers. But, in DC-net, only one user can send the message at a time, so it takes extra bandwidth to handle collision.

To achieve the privacy in the nodes we use group signature instead of using the ring signature. In the ring signature it doesn't have any group managers. But by using the group signature we can prevent, that any user can sign the message by using his secret key and by using the others public key.

3. PROPOSED SYSTEM FOR THE MESSAGE AUTHENTIACTION

In this paper, 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.

3.1. SECURITYY ANALYSIS

In this section we discuss about that the SAMA based scheme is best for the source privacy

3.1.1. Anonymity

The proof of the

I. The process of generating the SAMA can be chosen by any members in the AS with equal probability.

II. Anybody from the message sender position can generate the SAMA in the straightforward.

3.1.2. Unforgeability

In this section we prove that the SAMA is secure against the adaptive-chosen message attacks.

We will introduce the two Lemmas. Lemma 1 is the splitting Lemma also known as the probabilistic Lemma. Lemma 2 is the slight modification of the Forking Lemma.

3.2.Source Privacy

The source privacy is directly related to the selection of the AS.Before a message is transmitted, the message source node selects an AS from the public key list. Why this is because 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, therefore the selection of the AS should create sufficient diversity.Sothe privacy of the message should be well protected in the network.

To balance the source privacy and the efficiency, we should select the nodes in the predefined range from the routing path and the AS does not have to include all nodes in that range.

3.3. Key management and the Compromised Node Detection

For improving security in the wireless network we have to continuously monitor the nodes in the network. Because once the node is compromised by the trackers or crackers the information stored in the node is completely accessible by the intruders.

For that the key management for the network should be selected properly.

3.3.1. Compromised Node Detection

In this we will discuss how the compromised node is detected. We know that the node information is delivered to the sink node.When a message is received by the sink node, the message source is hidden in an AS. We know that the SAMA scheme guarantees that the message integrity is untampered, when aunwanted message is received by the sink node, the source node is viewed as compromised. If the compromised source nodetransmits one message, it would be very difficult for the sink node to be identified which is compromised node and it's easy when it's transmitted more number of messages.

When the node has been detected as a compromised node the source sender can remove its public key from the list. Once the public-key is removed from the list any message transmitted from the node will immediately dropped from the node to save the power in the sensor node.

4. PERFORMANCE AND ANALYSIS

In this sectionwe discuss about the theoretical analysis. Also we will compare our proposed scheme with the bivariate polynomial-based symmetric-key scheme.

4.1. Theoretical Analysis

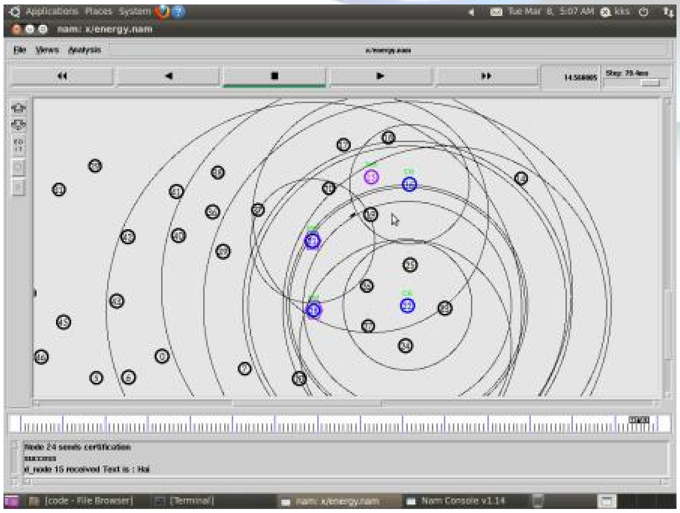
Key management is one of the major issues for the authentication in the sensor nodes. Before using the hop-by-hop message authentication sensor nodes are utilizes the end-to-end node authentication scheme. This scheme doesn't enables the intermediate node authentication and also this schemes consume more energy power. The message authentication is checked at the recipient end of the node. So that that the protocol that provide hop-by-hop message authentication is a important concept in the message authentication.

Hop-by-hop message authentication is achieved by the public-key encryption.

In the bivariate polynomial-based scheme only one node will act as a base station and the remaining will act as intermediate or the receiver section. Sink node concept doesn't applicable to this scheme and the only one base station is easy to hack. For that we are move to the polynomial based approach or the SAMA based technique for the message authentication. While we using the SAMA based scheme the modified EIGamal signature (MES) should also include in the protocol.

The recent process in the elliptic curve cryptography shows that he polynomial based scheme is the best in terms of the memory usage, computational overhead.

5.OUTPUT



```
Node 24 sends certification
success
d_node 15 received Text is : Hai
```

Output is obtained by network simulator 2(ns2.34). The program is written by tool command language(tcl). The output is shown from nam window.In this output we assign source as 22 and destination is 15.

6. CONCLUSION

In this paper we discuss about the SAMA based ECC and the hop-by-hop message authentication scheme based on the SAMA. We also discussed the possibilities of finding the compromised nodes. Based on the theoretical analysis we can conclude that SAMA based scheme is advantageous than the polynomial based scheme. In our scheme there is no threshold problem and the distribution nature of our algorithm makes more suitable for the decentralized networks. This paper is only focused about when the intruder try to compromise the node it will only prevent that action only. We didn't discuss anything about how to trace out the intruder. In the network preventing the node from the intruder isn't enough for the security. We also use Ambassador and Coordinator node used to allot the nodes based by the Mobile adhoc networks used faster way communication.Ambassador node which capable to collect the neighbor foreign group information.The node which can connect the different groups to share the file coordinator node which is stable in the group, and contacting to the group node frequently.The node which is capable to collect the information of file availability in own group. There is a method for replication to allocate the file. It is based by the Optimal File Replication Rule. It is used to enhance the file availability and reduce the time delay for file transformation. P2P communication is used in this method. In this method each node acts to be a both server/client. In this method bandwidth is calculated by the each node.We also enhance the security we include find out the trusted value for each node. It is used to find out which node is act to be attacker node and which nodes are healthy nodes. The main advantage is it is used reduce the communication overhead.

ACKNOWLEDGEMENTS

This research paper is organized by Department of ECE, PSN College of Engineering &Technology, TN. This project is guided by Ms, Lumi Rosin L Assistant professor of ECE,PSN College of Engineering and Technology. She is well known for her Networking Knowledge.

REFERENCES

[1] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.

[2] 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.

[3] A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient Authentica-tion and Signing of Multicast Streams over Lossy Channels," Proc.IEEE Symp. Security and Privacy, May 2000

[4] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-By-Hop

Authentication Scheme for Filtering False Data in Sensor Networks," Proc. IEEE Symp. Security and Privacy, 2004.

[5] 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," Proc. IEEE 28th Int'l Conf. Dis-tributed Computing Systems (ICDCS), pp. 11-18, 2008.

[6] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking Cryptographic Schemes Based on 'Perturbation Polynomials'," Report 2009/098, http://eprint.iacr.org/, 2009.

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

Maharaj C.B[1]currently pursuing his BE in Electronics and Communication Engineering in PSN College of Engineering and Technology. His current research interests network security, ethical hacking, cyber security, cloud computing.

Ruban Arul Raj M[2]currently pursuing his BE in Electronics and Communication Engineering in PSN College of Engineering and Technology. His interested areas are DSP, DIP.

Bala Pravin Singh[3] currently pursuing his BE in Electronics and Communication Engineering in PSN College of Engineering and Technology. His interested areas are image processing, cryptography, network security.

Kailasam S[4]currently pursuing his BE in Electronics and Communication Engineering in PSN College of Engineering and Technology. His area of interests arecryptography, network security, network coding.