R.Kalpana *et al*, International Journal of Computer Science and Mobile Applications,
Vol.3 Issue. 11, November- 2015, pg. 25-30 **ISSN: 2321-8363**

SEMANTICALLY SECURED MESSAGE AUTHENTICATION FOR WIRELESS SENSOR NETWORKS

K.Noel Binny M.sc., M.Phil.,PGDCA[1]

R.Kalpana[2]

Abstract:

Message authentication is one of the best impressive ways to thwart unauthorized and corrupted messages from vitality delivered in wireless sensor networks (WSNs). For this reason, many message authentication schemes have been flourished, based on each of two, symmetric-key cryptosystems public-key cryptosystems. Most of them, however, have the constraints of high computational and communication over bearer in addition to lack of scalability and resilience to node compromise attacks. To overcome these problems, a scalable authentication scheme based on elliptic curve cryptography (ECC) has been used. But it is not semantically secure, means it is still possible to extract a message. And ECC is Complicated and tricky to implement securely, particularly the standard curves. So to provide a semantic security, a semantically secured message authentication approach is proposed. An authentication is provided by an ElGamal encryption algorithm. By this, it not possible to extract a plaintext message by knowing any information from cipher text message. Both theoretical analysis and simulation outcome determined that our proposed scheme is more efficient than the polynomial-based access in terms of computational and communication processing overhead under comparable security levels while providing message source privacy.

Key words: Message Authentication, wireless sensor network, elliptic curve cryptography, ElGamal Encryption.

1. Introduction

MESSAGE authentication has a major role in securing from unauthorized and infected messages from being transmitted in networks to save the valuable sensor resources. For this, lots of authentication schemes have been N developed for message authentication and integrity verification for wireless sensor networks(WSNs) .This approach is broadly classified into two types public-key approach and symmetric-key approach. The symmetric-key approach needs a complex key management, needs of scalability, and is not resilient to more prominent number of nodes to compromise assaults since the a secret key is shared between the sender and receiver. The sender uses a shared key to generate a message authentication code (MAC) for message transmission. Node having shared secret key performs the authenticity and integrity of message. This key is shared by a group of sensor nodes. By capturing a single sensor node, an intruder can compromise the key. And this methodology will not work in multicast networks. A secret polynomial based message authentication scheme is used to solve the scalability problem. This is similar to a threshold secret sharing, where the degree of polynomial is used to determine the threshold. When the number of messages transmitted is less than the threshold, then this mechanism provides information-theoretic security of the shared secret key. The intermediate nodes verify the message authentication by polynomial evaluation. The system is fully broken which means the polynomial is fully recovered. This situation happens when the number of messages transmitted is larger than the threshold value.

To prevent the intruder from retrieving the polynomial alternative solution is proposed. Intruder computes the polynomial value by calculating the coefficients of the polynomial. As a solution random noise is added this is called as perturbation factor. Because of these coefficients of the polynomial is not easily solved. By using error-correcting code technique random noise is completely removed.

In public key mechanism, message is transmitted along with the digital signature which is spawn using senders' private key. By using the sender's public key an in-between node which forwards a message and the final receiver can authenticate the message. Computational overhead is more which is the drawback of public key based scheme. For this elliptic curve cryptography (ECC) is used along with the public key mechanism. This approach provides many advantages compared to that of public key mechanism.

2. Related Work

Efficient Authentication over lossy channel[1] paper introduced efficient schemes, TESLA and EMSS, for secure lossy multicast streams. TESLA, short for Timed Efficient Stream Loss-tolerant Authentication, offers sender authentication, strong loss robustness, high scalability, and minimal overhead, at the cost of loose initial time synchronization and slightly delayed authentication. EMSS, short for Efficient Multi-chained Stream Signature, provides no repudiation of origin, high loss resistance, and low overhead, at the cost of slightly delayed verification. Attacking cryptographic scheme[2] show attacks on several cryptographic that have recently been proposed for achieving various security goals in sensor networks. They also told that 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. They 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 R.L. Rivets, A. Shamir, and L. Adelman[3] proposed a Method for Obtaining Digital Signatures and Public-Key Cryptosystems. They also show that a message is encrypted by representing it as a number M, raising M to a publicly specified power e, and then taking the remainder when the result is divided by the publicly specified product, n, of two large secret prime numbers p and q. Decryption is similar. The security of the system rests in part on the difficulty of factoring the published divisor, n Comparing Symmetric-Key and Public-Key Based Security Schemes[4] proposed a system that builds the user access control on commercial off-the-shelf sensor devices as a case study to show that the public-key scheme can be more advantageous in terms of the memory usage, message complexity, and security resilience. They also does work to provides insights in integrating and designing public-key based security protocols for sensor networks.

3. Network Model Construction

The WSNs are counterfeit to subsist 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 interacting with its neighbouring nodes directly using geographic routing. The entire network is fully linked through multi-hop communications. We assume there is a security server (SS) that is responsible for formation, storage and dissemination of the security parameters among the network.

4. SSAMA with ElGamal Encryption

Privacy is sometimes referred to as anonymity. It generally refers to unidentifiable within a collection of subjects. This collection is termed as AS. Sender namelessness means that a particular message is not linkable to any sender, and no message is linkable to a particular sender. To effectively handle the anonymity SAMA (source anonymous message authentication) is used.

Semantically secured source anonymous message authentication (SSAMA) mechanism is used to secure the message semantically. If the message is semantically insured, it is absurd for a computationally bounded adversary to derive significant knowledge of the a message (plaintext) when given only its cipher text and the corresponding public encryption key.

To achieve such semantic security for a message an ElGamal encryption algorithm is used. ElGamal encryption is chosen because it is probabilistic. Probabilistic means that a single plaintext can be encrypted to many possible cipher texts.

Authentication is achieved by signature generated by ElGamal encryption mechanism. The generated signature and message content is encrypted with key value of an ElGamal algorithm.

Key & signature generation process involves the following steps.

1. Let p be a large prime and g be a generator of p i.e. a set of numbers generated by giving p as input to a random generator.
2. Both p and g are made public
3. Choose a private key x randomly from g i.e. x€g. and compute public key y by formula
   $y = g^x \bmod p$.

4. To sign a message m, The signature of message m is defined as the pair (r,s).
   $r = g^k \bmod p$ where k is a random number chosen from g.
   $s = rxh(m,r) + k \bmod(p-1)$ where h is one way hash function.

5. The verifier checks whether the signature equation $g^s = ry^{rh(m,r)} \bmod p$ holds.
   If the equality holds true, then the verifier Accepts the signature, else Rejects it.

   The accepted signature is encrypted using the public key y and send it to the destination.

5. AS Selection and Source Privacy

The appropriate selection of an Ambiguity Set (AS) plays a main part in message source aloofness, since the actual message source node will be hidden in the AS. Before a message is transmitted, the message originnode chooses an AS from the public key list in SS (Security Server) as its choice. To afford message source privacy, the message origin needs to select the AS which include nodes from all directions of the source node. It also includes nodes from the opposite direction of the successor node. So, even the immediate follower node will not be able to differentiate the message source node from the forwarder based on the message that it receives.

Security Analysis

Using ElGamal Encryption scheme the signature is generated and the key value is used to encrypt the message and message content. Since the sensor node collects the data and places in a sink node, there is need to hide the details of source node. Else the intruder will grasp the information about the source node and use this to compromise the security. Here, the identity of the source node is also hidden from all the other nodes, so there is no way for an intruder to identify who is the sender.

If the nodes repeatedly use the same AS it will be termed as compromised node. The sink node keeps tracking message from the compromised node to confirm it is compromised node. So it can be confined from the AS set. When a node is diagnosed as compromised, the SS can remove its public key from its public key list. Once the public key of a node is removed from the public key list, any message with the AS containing the compromised node will be dropped without any process to save the precious sensor power. Thus the security feature provided by this approach is more feasible and it enhances the existing security feature.

Performance Evaluation

ElGamal encryption provides an enhanced security feature than the existing security feature providing algorithms. Since the message is authenticated and source node information is hidden from its neighbour node, the possibility for the intruder to identify source information is minimized. The memory usage, message complexity, and security resilience feature are achieved in a better measurable way.

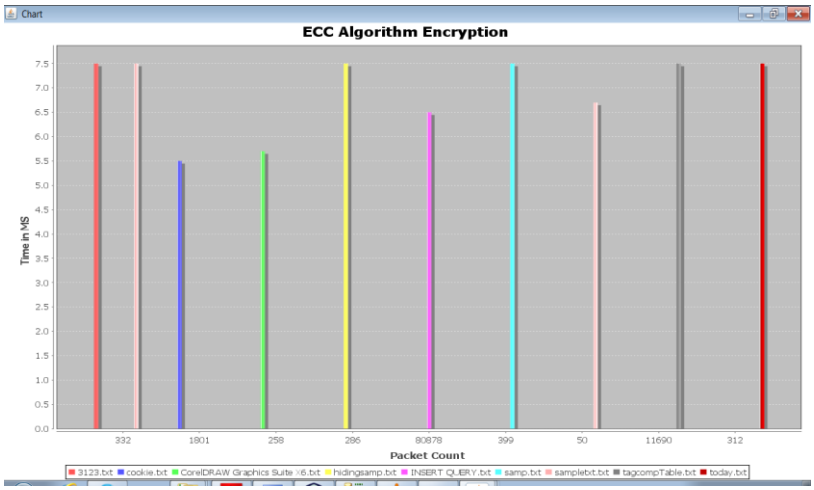

Fig 5.1 Packet Transmission Rate by ECC Algorithm

Fig 5.1 shows the number of packets transmitted in specified time by ECC algorithm. Time is deliberated in micro seconds.

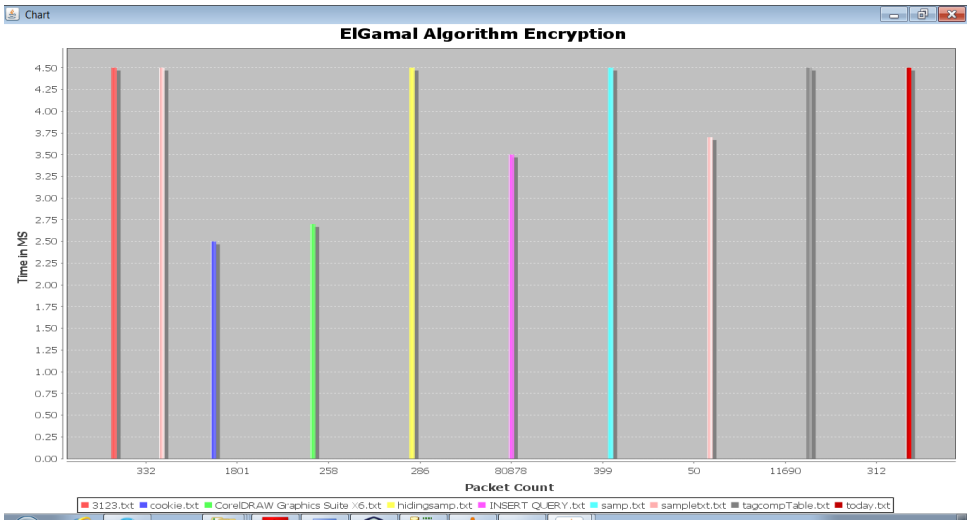

Fig 5.2 Packet Transmission Rate by ElGamal Algorithm

Fig 5.2 shows the number of packets transmitted in specified time by ElGamal algorithm. Time is measured in micro seconds. From figure 5.1 and 5.2 it is clear that the ElGamal Encryption algorithm achieves a better transmission rate than the Elliptical Curve Cryptography algorithm. The transmission rate is doubled by ElGamal encryption. By including security feature and transmitting a packet at this time rate gives a better performance for a network.

Results | Messages

	filename	filesize	delaytime
1	3123.txt	332	7.5
2	cookie.txt	1801	5.5
3	CorelDRAW Graphics Suite X6.txt	258	5.7
4	hidingsamp.txt	286	6.7
5	hidingsamp.txt	286	7.5
6	INSERT QUERY.txt	80878	6.5
7	samp.txt	399	7.5
8	sampletxt.txt	50	6.7
9	sampletxt.txt	332	7.5
10	tagcompTable.txt	11690	6.7
11	tagcompTable.txt	11690	7.5
12	today.txt	312	7.5

Fig 5.3 Packet Transmission Delay by ECC Algorithm

Fig 5.3 shows the delay time taken by ECC algorithm for transmitting files of varied sizes.

Results | Messages

	filename	filesize	delaytime
1	3123.txt	332	4.5
2	cookie.txt	1801	2.5
3	CorelDRAW Graphics Suite X6.txt	258	2.7
4	hidingsamp.txt	286	3.7
5	hidingsamp.txt	286	4.5
6	INSERT QUERY.txt	80878	3.5
7	samp.txt	399	4.5
8	sampletxt.txt	50	3.7
9	sampletxt.txt	332	4.5
10	tagcompTable.txt	11690	3.7
11	tagcompTable.txt	11690	4.5
12	today.txt	312	4.5

Fig 5.4 Packet Transmission Delay by ElGamal Algorithm

Fig 5.4 shows the delay time taken by ElGamal algorithm for transmitting files of varied sizes. From fig 5.3 and 5.4 it is clear that ECC algorithm is dabbling in transmitting a packet than the ElGamal Algorithm. By having more delay time it provides a way for security anxious for a packet waiting in network. As though it is encrypted it is waiting time makes it prone to security threads. From the performance evaluation, it is identified that ElGamal algorithm provides a better security along with faster transmission with low delay.

Conclusion

Message authentication plays an important part in thwarting unauthorized and corrupted messages from being forwarded in networks to save the precious sensor energy. For this many authentication scheme is proposed. The entire encryption scheme provides the security and authenticity to the message. But it fails to provide the semantic security to the message. The authentication scheme proposed by the Elliptic curve encryption scheme is inspected and prepared. Its and native security encryption algorithm‘s pullbacks give an rise to ElGamal

encryption scheme to provide the message a semantic authenticity. In this scheme, the key value is randomly generated and it is used to generate the signature. This signature provides the authenticity to the message. To enhance the security feature the signature value is encrypted and the message content is encrypted with the selected key value. The further enhanced feature is, the identity of the source is hidden by AS node. So the intruder's opportunity of compromising security is minimized. It has an efficient mechanism of identifying and isolating the compromised node. The memory usage, message complexity, and security resilience feature are achieved in a better measurable way compared to all existing encryption algorithm. Thus the semantic security feature for a message is implemented successfully with ElGamal encryption.

References

1. *S.Aakasham , S.R.Mugunthan,"A Secure QOS Distributed Routing Protocol for Hybrid Wireless Networks," IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 2, Ver. II (Mar – Apr. 2015), PP 50-58.*
2. *Amira Y. Haikal, M. Badawy, and Hesham A. Ali,"Towards Internet QoS Provisioning Based on Generic Distributed QoS Adaptive Routing Engine,".The Scientific World Journal Volume 2014 (2014), Article ID 694847, 29 pageshttp://dx.doi.org/10.1155/2014/694847.*
3. *A. Cheng, Real-Time Systems: Scheduling Analysis, and Verification, first ed. Wiley-Interscience, 2002.*
4. *DhanyaDileepkumar, Asha, " An Enhanced Qos Oriented Distributed Routing Protocol With Traffic Awareness For Hybrid Wireless Networks", T.S Proceedings of 32nd IRF International Conference.*
5. *Golestani, S.J. , Morristown, " A self-clocked fair queueing scheme for broadband applications," INFOCOM '94. Networking for Global Communications, 13th Proceedings IEEE*
6. *P. Gupta and P.R. Kumar, "The Capacity of Wireless Networks," IEEE Trans. Information Theory, vol. 46, no. 2, pp. 388 - 404, Mar. 2000.*
7. *D.B. Johnson and D.A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, vol. 353, pp. 153-181, 1996.*
8. *J. Kurose and K. Ross, Computer Networking: A Top-Down Approach Featuring the Internet. Addison Wesley, 2004.*
9. *D. Lin and R. Morris, "Dynamics of Random Early Detection," Proc. ACM Special Interest Group Data Comm.*
10. *P.K. Mckinley, H. Xu, A. Esfahan an, and L.M. Ni, "Unicast-Based Multicast Communication in Wormhole-Routed Direct Networks," IEEE Trans. Parallel Data and Distributed Systems, vol. 5, no. 12, pp. 1252-1265, Dec. 1992.*
11. *NavidNikaein and Christian Bonnet ,"A Glance at Quality of Service Models for Mobile Ad Hoc Networks," http://www.eurecom.fr/en/publication/1084/detail/a-glance-at-quality-of-service-models-for-mobile-ad-hoc networks.*
12. *Priyananci.S, Suriya.M , Anandakumar.H ,Anuradha.B," Efficient Estimation of Hybrid Wireless Networks Using Qos-Oriented Distributed Routingprotocol," in International Journal of Engineering Sciences &Researchtechnology*
13. *Ronal Benitto D , Ruby.D , "A QOS Based Routing in Mobile Ad-Hoc Networks," International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 5, May 2015.*
14. *C. Shen and S. Rajagopalan, "Protocol-Independent Multicast Packet Delivery Improvement Service for Mobile Ad Hoc Networks," Ad Hoc Networks, vol. 5, pp. 210-227, 2007*
15. *XenofonFafoutis, Lyngby,Vasilios A. Siris,"Handover incentives for self-interested WLANs with overlapping Coverage," IEEE Transactions on Mobile Computing.*

