Volume 5, Issue 7, July 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Providing Message Authentication and Integrity Based on Elliptic Curves in Wireless Sensor Networks

Azmath Pasha M A* Dept. of CSE, DBIT, Bangalore, India
Pushpavathi T P Dept. of CSE, DBIT, Bangalore, India
Goutham Nadig Mphasis, Bangalore, India

Abstract— Today, when communicating over the network, to send a message from one location to another the security is of utmost importance, because every user is concerned that the message reaches the desired destination without being modified enroute. To provide authentication, a scheme was developed which was based on polynomials. However, this scheme had problems i.e., the messages transferred to a particular node or to a node in a group suffered from threshold limit, only a limited number of messages can be transferred. Once the messages transferred are greater than the threshold the system can be easily corrupted by calculating the coefficients. To overcome this limitation and to provide better security, authenticity and integrity, in this scheme we transfer an anonymous message based on hash function and encrypting the message using elliptic curve cryptography. The use of hash function provides message integrity by using secure hashing algorithm and the recent progress in ECC provides a secure way to transfer the message. In this scheme each and every node verifies the authenticity and integrity of the message. It protects the location of the source; in addition to that it overcomes the limitation of polynomial scheme. The analysis of both the systems shows that the proposed scheme is more efficient.

Keywords— Hop by Hop authentication, signature, secret key, public key cryptography, sender anonymity, discrete logarithms, wireless sensor networks, hashing technique

I. INTRODUCTION

The significance of authenticating the message and protecting the identity of the source has become one of the most important aspects in wireless sensors networks to prevent the consumption of sensor power from the adversaries. To achieve this, many schemes proposed in the literature to provide authenticity and the integrity of the message. Symmetric key, public key and hash functions are the three approaches upon which these schemes are based on.

The hash function such as MD5, secure hash function algorithm can be used to provide message integrity. In the symmetric key approach, a secret single key is shared between two end users or group of users in a network. By using this key the information is shared by generating a code for each message transmitted, this code is called message authentication code or simply MAC. But this approach had the scalability problem. However, because a single key is shared among group of nodes any attacker can compromise a node and can gain access to corrupt the system. To resolve this problem, a polynomial scheme [1] was introduced. This authentication scheme suffered with the problem of threshold limit. To avoid this, a perturbation factor [2] i.e., a random noise was added to complicate the adversary from calculating the coefficients of the polynomial. The recent progress in error correcting code techniques [3] shows that this noise can be completely removed.

As for the public key approach, it digitally signs a message where the sender uses the receiver's public key which is shared among the group of nodes to encrypt its message which is thus can only be decrypted using the receivers public key and vice versa. This approach proved to be more efficient compared to symmetric key. However, this approach had the limitation of high computation overhead. The development of elliptic curve cryptography (ECC) based on public key can be used to overcome this limitation of high computational overhead.

In this paper we use a combination of hash and public key to propose an anonymous message based on ECC. This scheme provides both the authenticity and integrity to transfer the message to the intended user securely. The analysis shows that this scheme is more efficient than the polynomial authentication scheme.

1. The contributions made in this paper are the following:
2. Initialize the nodes with the hash value generated for the message content using SHA1 algorithm.
3. Send an anonymous message based on the elliptic curves through which the location of the source is protected.
4. Overcome the threshold limit of the existing system.
5. Resilient to node compromise attack.
6. The scheme is more efficient than the existing system.

The rest of the paper is organized as follows: Section II presents the literature survey which discusses about different schemes proposed to provide better security to the messages transferred. Section III provides a brief description of the

existing system and its limitations. Section IV discusses about the proposed methodology to overcome these limitations based on elliptic curve cryptography. Finally we conclude in section V.

II. LITERATURE SURVEY

Following implementations of the existing system are discussed below which led to secure transmission of message.

Adrian Perrig, Ran Canetti, J. D. Tyga, Dawn Song proposed Efficient Authentication over lossy channel [4], in this paper the author discusses about two efficient schemes, TESLA and EMSS. TESLA stands for Timed Efficient Stream Loss-tolerant Authentication and EMSS stands for Efficient Multi-chained Stream Signature. TESLA scheme is highly robust and scalable providing sender authentication in addition to less overhead. However, it had the limitation of slight delay in authentication. EMSS scheme provides no repudiation of origin, high loss resistance and low overhead at the cost of slightly delayed verification.

R. Rivest, A Shamir, and L. Adleman [5] proposed "A method for Obtaining Digital Signatures and Public-Key Cryptosystems". In this paper, the 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 number p and q. Decryption is similar. The security of the system rests in part on the difficulty of factoring the published divisor, n.

Fan Ye, Haiyun Luo, Songwu, Lixia Zhang introduced "Statistical En-route Filtering Mechanism (SEF) [6]. In this paper, they propose a scheme that prevents the adversary from breaking down the entire system. To detect any false report generated, this scheme relies on collective decisions of multiple nodes. Each intermediate node verifies the report generated by the previous node over the network. If an incorrect is detected, the report is dropped and the message is resend. However, the sink will further verify the correctness of each report generated by each node.

III. EXISTING SYSTEM

The symmetric-key based approach requires complex key management [7], 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) [7] for each transmitted message. However, for 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. An intruder can compromise the key by capturing a single sensor node. In addition, this method does not work in multicast networks.

To solve the scalability problem, a secret polynomial based message authentication scheme was introduced [1]. 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. However, 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 [2] 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 [3]. For the public-key based approach [5], [8], 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.

The issues identified in existing system are as follows:

a. When the number of messages transmitted is larger than that of the threshold specified, the system can be corrupted by compromising a weak node and gaining access to all sensitive information.
b. Slightly delayed authentication.
c. The use of symmetric key approach makes it complicated to manage the keys since a single secret key is shared is used between the end users to communicate in a network.

The following proposed method overcomes all these limitations and in addition to that it also provides sender anonymity.

IV. PROPOSED SYSTEM

The methodology used in the proposed system to achieve the following goals is to use SHA1 algorithm to generate a unique hash value for the message and ECC algorithm to provide both authenticity and integrity to the message.

A. Goals to be achieved

- Authenticating the message: The messages send to any node in the network or in the particular group, it should be able to verify that the information is sent from the intended source. Any intruder cannot compromise a node without being detected and inject false data.
- Message Integrity: The node in the network should be able to verify that the message is not modified during transmission. If any adversary changes the message contents, it must be detected and action should be taken to remove the false data.

- Resilience: If a node is compromised by the adversary, this scheme ensures that the remaining nodes can still be secure and trusted to transmit the message to the intended receiver.
- Protecting identity and location: The location or the identity of the source is protected. The attacker cannot identify the source location by analyzing the traffic.
- Hop by Hop Transfer: The message should be transmitted in a path that is secure and no node in the path is compromised. The scheme must be able to hop the data to a different path if any node is attacked by the adversary in the path that the data is being sent.
- Efficiency: This scheme is efficient in terms of faster authentication, providing integrity compared to the previous existing system.

To achieve these goals some of the assumptions have to be made described in the following subsection.

B. System model and Assumptions

Each node in the sensor group is able to communicate with its neighbouring node using some geographic protocol. There is an Intrusion Detection System manager which detects the type of attack that the adversary is trying to compromise the system. In this paper, it considers two types of attacks:

- Passive attack: The aim of this type of attack is only to listen to the messages being exchanged between two or more parties and perform traffic analysis.
- Active attack: The active attacker tries to compromise a weak node to gain access to the system. Once a node is compromised the attacker has the ability to change the contents of the message or inject its own false messages.

C. Implementation

Based on the above assumptions the system is implemented to achieve the goals specified and to send the message in a secure manner. The methodology proposed in this paper is as follows.

Consider a group of nodes connected in a multi hop communication system. These nodes are capable of communicating with the other nodes through geographic protocol to transfer the message from one hop to next as shown in figure below. The figure1.1 shows how the message is transferred from one party to the other in the network. If a node is compromised by the adversary it discards the node and hops to the next least energy path node. The architecture in figure 1.2 shows that the IDS manager is responsible to detect the type of attacker and to acknowledge the router to take action to prevent the adversary from corrupting the system.

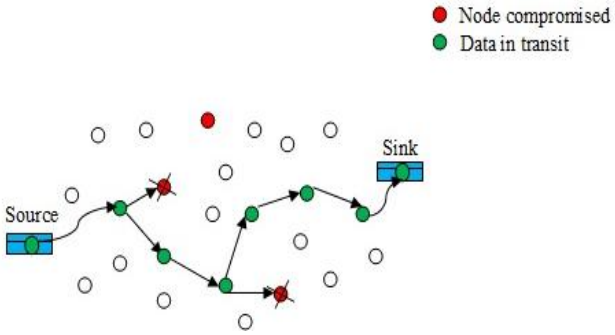


Figure 1.1: A simple hop to hop message transfer

The compromised node is discarded and the message hops to next path to transfer the data to the intended destination. First, the nodes in the cluster are initialized to a particular hash value of the message content generated using SHA1 algorithm. This provides enough diversity to the adversary that once the node is initialized to a unique hash value, the attacker cannot compromise a node and inject its own data without being detected since this hash value is unique to that message content. Even a slight change in the message will result in a different hash value which is unacceptable by other nodes forwarding the data. Because of this unique hash value the integrity of the message can be verified by each intermediate node. When the hash value is initialized for all nodes, the message is encrypted using ECC encryption technique to provide both authenticity and integrity of the message. The message is encrypted based on the elliptic curves. ECC is more advantageous in providing more security to the message since it uses small key compared to other cryptosystem techniques such as RSA.

The service provider or the source node initializes the nodes in the cluster to a unique hash value using hashing technique such as SHA1. It generates a MAC code for all the nodes. The message is then encrypted using elliptic curve cryptography. The generation of the MAC is one-way meaning that it cannot be easily decrypted since every message has its unique hash value and a small change in the message would result in a different MAC key as all the nodes are initialized to that particular hash value of the message content by the source in the beginning of the transmission. By applying brute force technique the adversary cannot compute or decrypt the message since the elliptic curve cryptography uses small keys that are complicated to be calculated compared to other previous public key cryptosystems. In the implementation of this scheme, the router routes the data from one node to another by choosing a least energy path. During transmission if any of the nodes is compromised by an adversary, the router detects it and acknowledges the intrusion detection system manager to determine the type of attacker attacking the node.

The following is a depiction of the system architecture.

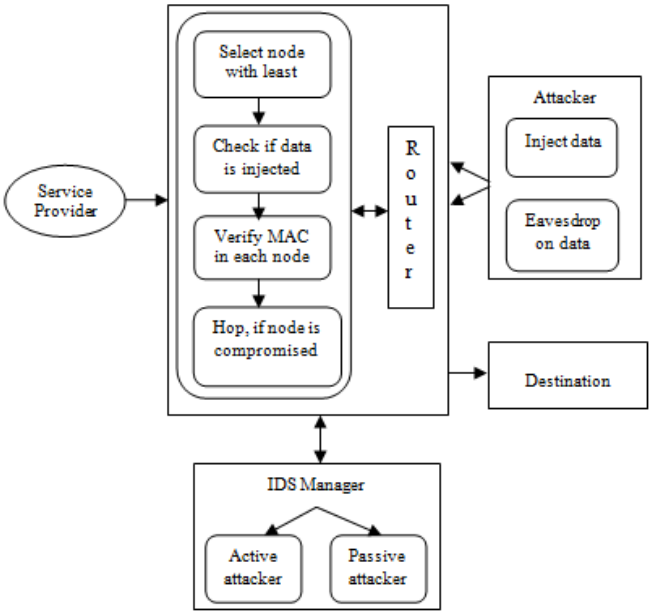


Figure 1.2: System Architecture

D. Algorithms

The following algorithms are used to implement the proposed system which provides message authentication and integrity.

Algorithm 1: Selecting the least energy path

```
while (nodes)
{
        Initialize MAC for all nodes
        if (energy of node==0)
                Send data;
        else {
                if (energy of node>0){
                        Select least energy node;
                }
            }
}
```

Algorithm 2: Localizing the node

```
while (nodes)
{
        if (node== injected){
                IDS manager determines the attacker; send the details to router,
                if (attack==active) {
                        Router localizes the node with malicious data and hops to next least energy path;
                If (attack==passive) {
                        Router rectifies the IP address to its original IP;
        }
        else
                Send data normally;
}
```

Algorithm 3: Secure Hashing Algorithm (SHA1)

It produces a 160 bit block message digest. The description of this algorithm[10] is as follows:

Step1: Padding

Pad the message with a single one followed by zeroes until the final block has 448 bits.

Append the size of the original message as an unsigned 64 bit integer.

Step 2: Initialize the 5 hash blocks (h0, h1, h2, h3, h4) to the specific constants defined in the SHA1 standard.

Step 3: Hash (for each 512bit Block)

Allocate an 80 word array for the message schedule

Set the first 16 words to be the 512bit block split into 16 words.

The rest of the words are generated using the following:

word [i3] XOR word [i8] XOR word [i14] XOR word[i16] then rotated 1 bit to the left.

Step 4: Loop 80 times using the following function

Calculate SHAfunction() and the constant K (these are based on the current round number.

- e=d
- d=c
- c=b (rotated left 30)
- b=a
- a = a (rotated left 5) + SHAfunction () + e + k + word [i]

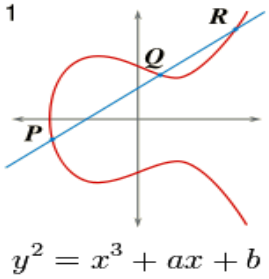
Step 5: Add a, b, c, d and e to the hash output.

Algorithm 4: Elliptic Curve Cryptography (ECC)

The ECC algorithm[11] provides better security than compared to previous encryption algorithms since it uses a small key size.

The equation of elliptic curve can be given by,

$$y2 = x3 + ax + b$$



The scalar multiplication is significantly important operation of ECC. The scalar multiplication calculates,

$$Q = kP$$

Where, P – point on the curve

k – private key and

Q – public key (point on the curve)

Using this equation encrypts the message by public key and decrypts the message by private key and the process is repeated by point addition and point doubling methods.

- In point addition, two points are added to obtain another point say, M= L+K.
- In point doubling, point L adds itself i.e. M=2L.

The following table describes why ECC is more advantageous than the conventional encryption techniques [12]:

Table IComparing key sizes for three different approaches of encryption

Comparison of different approaches		
Symmetric encryption Key size in bits	**RSA key size in bits**	**ECC key size In bits**
80	1024	132
112	2048	160
128	3072	210
192	7680	283
256	15360	409

The selection of path depends on DSR protocol which selects a least energy path to transfer the data while the message is being encrypted by ECC algorithm and the message content is initialized by a hash value. Thus the scheme can detect if any adversary is trying to attack a node to prevent the system from being corrupted and to transfer the information in most secure and authentic way.

When the node is compromised by an adversary, the localization technique is applied so that the message reaches its destination without being modified to the intended receiver. The localization technique discards the node that contains malicious data and hops to different least energy path to send the information. The proposed system prevents any intruder from breaking down the system and provides better security to the message in transit.

V. CONCLUSION

The proposed system overcomes the threshold problem where we can send any number of messages from one party to another. A message can reach its destination without being modified and during transmission if any intruder compromises a node, it cannot inject its own message without being detected. It provides both authentication and integrity of the message ensuring that the message is received from the acclaimed and is not been modified by any adversary meaning that it is not injected by false data. It also protects the identity of the sender in a network so that the adversary would not able to calculate by performing traffic analysis. The proposed system is more advantageous in terms of communication overhead and computation overhead than compared to polynomial scheme.

REFERENCES

[1] 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.

[2] 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..

[3] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking cryptographic schemes based on "perturbution factors","Cryptology ePrint Archive, Report2009/098, 2009, http://eprint.iacr.org/

[4] A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient authentication andsigning of multicast streams over lossy channels," in IEEE Symposium on Security and Privacy, May 2000.

[5] 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.

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

[7] Jian Li, Yun Li, Jian Ren, and Jie Wu,"Hop by hop message authentication and source privacy in wiireless sensor networks", in IEEE Transactions on Parallel and Distributed Systems, Volume:25, Issue:5, Issue Date : May 2014.

[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] http://www.cs.rit.edu/~bcw5910/482/TeamFlux.pdf

[11] Professor Rahila Bilal, Anna University and Dr.M.Rajaram, Anna University, "High Speed and Low Space Complexity FPGA Based ECC Processor", in International Journal of Computer Applications (0975 – 8887) Volume 8– No.3, October 2010

[12] Swadeep Singh , Anupriya Garg , AnshulSachdeva, "Comparison of Cryptographic Algorithms: ECC & RSA", in International Journal of Computer Science and Communication Engineering IJCSCE Special issue on "Recent Advances in Engineering & Technology" NCRAET-2013

[13] 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.

[14] 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.

[15] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Communications of the ACM, vol. 24, no. 2, pp. 84–88,

[16] M. Waidner, "Unconditional sender and recipient untraceability in spite of active attacks," in Advances in Cryptology - EUROCRYPT, ser. Lecture Notes in Computer Science Volume 434, 1989, pp. 302–319.

[17] R. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in Advances in Cryptology–ASIACRYPT, ser. Lecture Notes in Computer Science, vol 2248/2001. Springer Berlin / Heidelberg, 2001.

[18] BlueKrypt, "Cryptographic key length recommendation," http://www. keylength.com/en/3/

