Providing Sender Anonymity with Message Authentication in Sensor Networks using Elliptic Curve Digital Signature Algorithm

Priya T V[1], Sreerag B M[2]

[1, 2]Department of IT, Nehru College of Engineering, Thiruvilwamala, Thrissur, India

Abstract: ***Message authentication is one of the important parameter used to avoid unauthorized accesses in Wireless Sensor Networks (WSN). Because of its importance many authentication schemes were developed based on symmetric key cryptosystems and public key cryptosystems. But they all faced the challenge of high communication and computational overhead. To solve this problems authentication based on ECC was introduced. This authentication scheme is advantageous in terms of computational overhead, memory space utilization and security resilience. Our main aim is to minimize the total power consumption of the nodes in WSN and thereby to save the precious sensor energy. Hence an authentication scheme based on ECDSA was proposed in this paper which is a variant of ElGamal signature scheme recently proposed. This can be used to provide source anonymity along with message authentication. The simulation results show that the proposed scheme is faster and generates smaller signature which adds to the advantage of the system.***

Keywords: wireless sensor networks, ECC, source anonymity

1. Introduction

The rapid growth of computer networks allowed large files, such as digital images, to be easily transmitted over the internet [1]. Data encryption and authentication are widely used to ensure security. Message authentication prevents unauthorised and corrupted messages in the network to save precious sensor energy. Hence the need of message authentication is widely increasing. For this reason many authentication scheme have been proposed to provide message authenticity and integrity verification for wireless sensor networks (WSNs). It can be broadly classified in to two categories: public key based approach and symmetric key based approach.

Wireless Sensor Networks consist of large number of sensor nodes capable of communicating with its neighbour nodes directly using routing protocols. The open nature of the network makes the attacker to inject malicious packets thereby compromises the nodes. Privacy in sensor network usually includes both content privacy and contextual privacy. Threats towards content privacy can be countered by using encryption and authentication.

The symmetric key approach uses a single key for both signing and verification of the message. Hence they require complex key management and lacks scalability. Since the message sender and the receiver share a secret key, when a single node is compromised the key may be known to the attacker. This may compromise the security of the entire network.

To solve the scalability problem of the symmetric key based authentication scheme, a polynomial based authentication scheme was introduced in [3]. It is a threshold secret sharing scheme where the threshold is the degree of the polynomial used. This approach offers the security of the shared secret key when the number of messages transmitted is less than the threshold. But when the number of messages transmitted is greater than the threshold, the polynomial can be fully recovered and therefore the network can be completely broken. An alternative solution to this problem was proposed in [4] where the main idea is to use an perturbation factor or a random noise to the polynomial so that the attacker cannot solve the coefficients of the polynomial and thus security of the system can be preserved.

Another approach for message authenticity is the public key based authentication scheme where the signing of the message is done by the sender's public key and the verification of the signature is done at every intermediate node and at the receiver using the sender's public key.

High computational overhead is one the limitation of public key approach. But the recent progress in Elliptic Curve Cryptography (ECC) shows that public key schemes can be more advantageous in terms of computational complexity, memory usage and security resilience, since public key approach has a simple and clean key management [5]. Hence an authentication scheme for WSNs based on ElGamal signature scheme based on elliptic curve was proposed in [6] which allows all the intermediate nodes to verify the authenticity of the message thereby reduces the number of unauthorised messages being forwarded through the network.

This paper proposes a secure and efficient message authentication scheme based on ECDSA (Elliptic Curve DSA) which provides message authentication along with message source anonymity. This scheme allows intermediate nodes to authenticate the message so that any corrupted message can be detected and dropped by intermediate node and hence the precious sensor energy can be saved. The simulation results shows that the proposed scheme is more efficient than the previous scheme in terms of security and computational overhead.

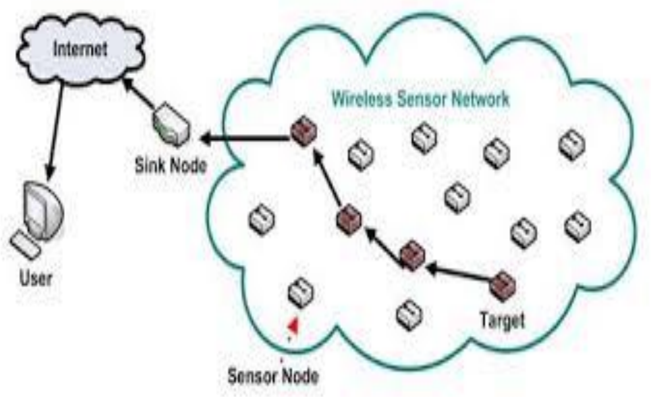

Figure 1: Wireless Sensor Network

The remainder of this paper is organised as follows: Section 2 discusses the recent works with a focus on Hop by Hop authentication based on ElGamal signature scheme. Section 3 describes the proposed Source Anonymous message authentication scheme based on ECDSA. Section 4 describes the performance analysis and simulation results of the proposed scheme and finally we conclude in section 5.

2. Related Work

Authentication is the process of verifying the identity of the sender of the message to impart security and confidentiality to the network. With the huge growth of computer networks and the latest advances in digital technologies, the need for message authentication is increasing. As a result, different authentication techniques have been used to provide the required protection. In [7], a symmetric and hash based authentication scheme for WSNs were proposed. In this scheme a secret key is shared among a group of sensor nodes in the network. Here key generation and maintenance is easy but if one node is compromised by the attacker then the secret key may be known. This may break the security of the entire network.

In [3] a secret polynomial based authentication scheme was introduced. This scheme offers information security and is and is similar to a threshold secret sharing scheme. Here there will a threshold value which is determined by the degree of the polynomial. When the number of messages transmitted is lower than the threshold, the scheme works well. But if the number of messages transmitted is greater than the threshold, the polynomial can be fully recovered thereby breaks the authenticity and security of the system. To solve this problem, a random noise or a perturbation factor can be used. The added perturbation factor can be completely removed using error correcting code techniques.

In the public key based approach for message authentication, the sender signs the message using sender's private which can be only to that node. All the intermediate nodes and the receiver can verify the signature using sender's public key which can be known to all nodes in the network. However the use of public key – private key pair for authentication imparts additional complexity to the network. This adds to the computational and communicational overhead of the system. But due to the emergence of Elliptic Curve Cryptography (ECC), the public key approach proves to be advantageous in terms of memory usage, computational complexity and security resilience since they have simple and clean key management [8]. A 160 bit ECC can provide as much security as that of a 1024 bit RSA scheme.

Providing anonymity to the sender is one the important challenge in WSN. Various anonymous communication protocols include Mixnet [9] and DC-net [2]. By providing anonymity to a node, the attacker cannot trace the geographical location of the node and hence adds to the security of the node. Mixnet provides anonymity by packet re-shuffling. Here there will be a group of mix servers. Sender encrypts the message along with the ID of the receiver using public key of the mix. Mix accumulates all this messages and decrypts them and sends to the receiver. But tis protocols rely on statistical property of the network traffic and hence they cannot provide perfect anonymity. DC-net on the other hand is a multi-party communication scheme where a group of nodes share a secret key. This protocol provides anonymity but here only one node can send at a time and hence additional bandwidth utilization is required.

Recently a message authentication scheme based on ElGamal signature was introduced [6]. This scheme is based on the concept of ECC. It allows the intermediate nodes to authenticate the message thereby blocking untrusted messages from being forwarded through the network. For wireless sensor network (WSN), conserving sensor energy is one among the greatest challenge. This scheme by providing node by node authentication can save the precious sensor energy. Also the computational and communication overhead of this scheme is considerably low as ElGamal signature scheme based on elliptic curves was used for authentication.

In this scheme the message sender generates a source anonymous message authenticator based on ElGamal signature scheme on elliptic curves. Here there is a security server (SS) that is responsible for generation, storage and distribution of security parameters among all the nodes in the network. If a single node is captured by the attacker, then all sensitive information will be known to the attacker. In such cases, the compromised node will not be able to create new public keys that will be accepted by SS and other nodes in the network. For a source node to send a message, it first selects the destination and then selects some intermediate nodes between the sender and the destination. This set with the sender node, destination node and the intermediate nodes is referred to as the Ambiguity Set (AS). The AS selected will be the subset of the public key list SS. It is as shown in fig 2. The advantage of selecting AS is that, when an attacker receives some message, he can find the previous hop of the message. But he will be unable to determine whether the previous hop is the actual message originator or not.

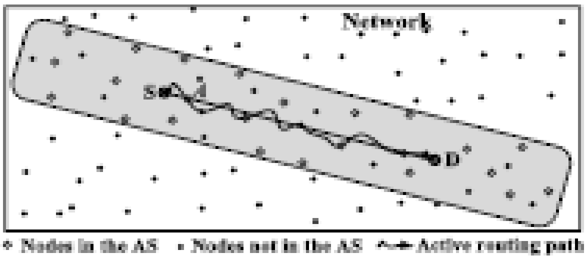

Figure 2: Ambiguity Set

While selecting the AS the nodes in all direction of the source node need to be included. The nodes selected should add sufficient ambiguity to the original sender. For greater efficiency nodes within a predefined routing range need to be selected.

3. Sender anonymous message authentication based on ECDSA

Message authentication while providing sender anonymity can be achieved using two algorithms:

- Generate $(m,Q_1,Q_2,..,Q_n)$: for a message m and the public keys $Q_1,Q_2,..,Q_n$, the message sender say A_t produces a anonymous message S(m) using its private key d_t.
- Verify S(m): by knowing the message m and S(m), the receiver can determine whether S(m) is generated by a member in AS.

With the huge growth of computer networks and the latest advances in digital technologies, a huge amount of digital data is being exchanged over various types of networks. In such cases security of the data need to be ensured and hence the need of message authentication is highly increasing.

Suppose a node (say Alice) needs to transmit a message to another node (say Bob) anonymously through the network. First, the sender node need to select an AS which includes itself, destination and some intermediate nodes. Let AS includes n members, say, AS, S={A1,A2,..,An}. Here let the actual message sender be A_t where $1 \leq t \leq N$. Suppose the original message be m. to make it secure, it is signed using the private key of A_t ,say, d_t where $1\leq t \leq N$. The authentication generation algorithm performs the following steps:

1. Select a random and pairwise key K_i for $1\leq i \leq n-1$ and computes r_i such that $(r_i,y_i)=K_iG$. If r_i is 0 then repeat the step again.
2. Then computes k_i^{-1} mod n.
3. Now calculate h(m) and converts it to an integer e.
4. Computes $s = k_i^{-1}(e+d_i*r_i)$ mod n. If s=0, then go to step 1.

Thus the anonymous message S(m) is defined as:

$S(m) = (m, S, r_1, y_1,….., r_n, y_n, s)$.

For the receiver to verify the anonymous message S(m), he must have a copy of the public keys Q_1, Q_2, …., Q_n. Then he:

1. Checks that $Q_i \neq O$, i = 1, …, n, otherwise invalid.
2. Checks that Q_i, i = 1,…,n lies on the elliptic curve.
3. Checks that $nQ_i = O$, i = 1,..,n.

Then to verify the authenticity, he follows these steps:

1. Verify that r_i i = 1,.., n and s are integers within the range [1, N-1]. If not, then the signature will be treated as invalid.
2. Computes the hash value h_i such that $h_i = h(m, r_i)$ where h is the hash function to compute the message digest and converts it to integer e.
3. Now computes $w= s^{-1}$ mod n and calculates u1=e×w mod n.
4. Similarly calculates u2 and X as $u2=r_i\times w$ mod n and $X=u1\times G + u2 \times G$
5. Accepts the signature only if $X=r_i$.
6. Also calculates $(x_0, y_0) = sG – \Sigma\, r_ih_iQ_i$.
7. If the first coordinate of $\Sigma_i\, (r_i, y_i)$ equals $x_{0,}$ then signature is valid and verifier accepts the signature.

4. Performance Analysis and Simulation Results

Intermediate node authentication helps each node in the routing path to verify the authenticity of the message being transmitted. In case of sensor nodes, power consumption is an important parameter which needs to be addressed. In order to reduce the total power consumed for signing and verification of message, the authentication based on ElGamal signature scheme recently proposed is replaced by ECDSA. Theoretical and experimental analysis shows that the proposed scheme works well in terms of energy consumption, packet delivery ratio and throughput. This is as shown in fig 4(a), 4(b), 4(c) and 4(d).

Fig. 4(a) shows that the throughput of the proposed scheme is high when compared to the existing scheme.

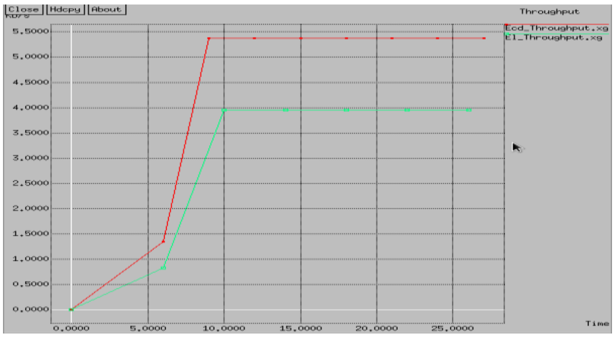

Figure 4(a): Throughput

Fig. 4(c) shows that the proposed scheme works well in terms of packet delivery ratio. The proposed scheme reduces the packet dropping rate and hence the efficiency of the system can be increased.

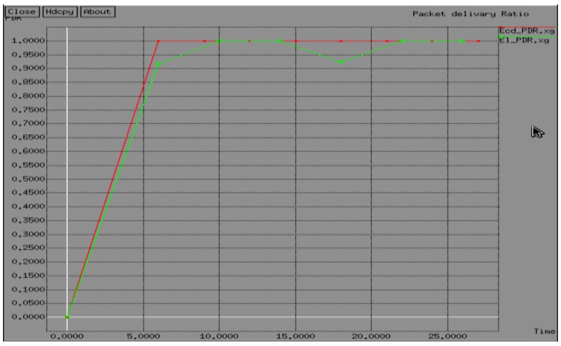

Figure 4(c): packet delivery ratio

Fig 4(b) shows that the energy consumption of the proposed ECDSA based authentication is constant when compared to the existing ElGamal based message authentication.

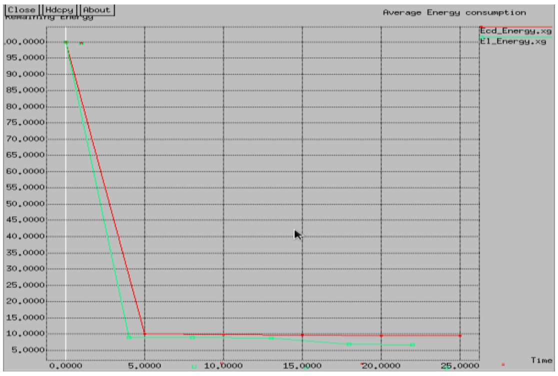

Figure 4(b): Average Energy Consumption

Fig. 4(d) indicates that the packet drop rate of the proposed scheme is less and remains constantly low when compared to the existing scheme.

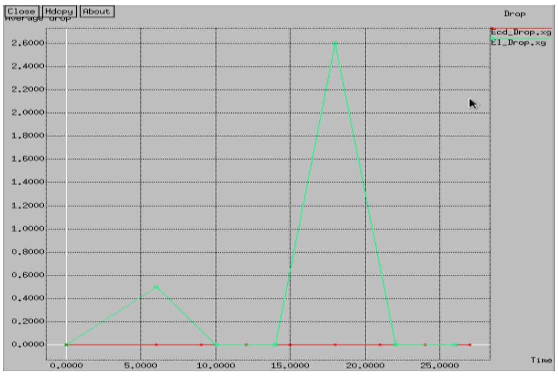

Figure 4(d): Packet Drop Ratio

5. Conclusion

In this paper, a simple and strong method has been proposed for message authentication with sender anonymity for WSN using Elliptic Curve Digital Signature Algorithm. When compared to the existing source anonymous message authentication for WSN which uses ElGamal signature scheme, the method proposed in this paper produces signature of smaller sizes and hence computational complexity and time consumption of sensor nodes can be reduced. Comparison is done through simulation using ns-2. Both theoretical and experimental results show that the power consumption of the sensor nodes was decreased when the proposed method was used for node by node message authentication. Thus the proposed scheme by reducing the total power consumption in WSN ensures efficiency and authenticity of the message being transmitted. Hence we could say that the proposed scheme is efficient in terms of computational overhead, memory usage, energy consumption and message delay. The experimental results showed that our proposed scheme improved the computational time largely. While there is some potential insecure point in our proposed scheme, we need further improvement and analysis in the future. The proposed method provides perfect authenticity of the message but it fails to provide message content security. An attacker can easily modify the message content. The future work includes extending the proposed mechanism to provide message content security by first encrypting the message and then signing the encrypted message. But this may create some additional overhead in terms of energy consumption which needs to be addressed.

References

[1] A. Hertzmann, C. Jacobs, N. Oliver, B. Curless, and D. Salesin, “Image Analogies,” Proc. ACM Siggraph, 2001.

[2] D. Chaum, “The Dinning Cryptographer Problem: Unconditional Sender and Recipient Untraceability,” J. Cryptology, vol. 1, no. 1, pp. 65- 75, 1988.

[3] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, “Perfectly Secure Key Distribution for Dynamic Conferences,” Proc. *Advances in cryptology (crypto’92)*, pp. 471-486, Apr 1992.

[4] W. Zhang, N. Subramanian, and G. Wang, “Lightweight and Compromise-Resilient Message Authentication in Sensor Neworks,” *Proc. IEEE INFOCOM*, Apr. 2008.

[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. Distributed Computing Systems (ICDCS), pp. 11-18, 2008.

[6] Jian Li, Yun Li and Jian Ren, “Hop By Hop Message Authentication And Source Privacy In Wireless Sensor Networks,” IEEE Trans. On parallel and Distributed Systems, vol. 25, no. 5, pp. 1223-1232, May 2014.

[7] 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.

[8] Don Johnson, Alfred Menezes and Scott Vanstone, “the Elliptic Curve Digital Signature Algorithm (ECDSA)”.

[9] D. Chaum, “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms,” Comm. ACM, vol. 24, no. 2, pp. 84-88, Feb. 1981.