ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

A Secure Key Exchange Scheme in Wireless Sensor Networks Using Diffie Hellman

K.Hima Bindu[1], Ch.Lavanya Aishani[2], M.Kamalakar[3]

M.Tech Scholar, Department of Computer Science Engineering, Pydah, Visakhapatnam, A.P, India[1]

B.Tech Student, Department of Electronics and Communication Engineering, Lovely Professional University, Jalandhar, Punjab, India[2]

Associate Professor, Department of Computer Science & Engineering, Pydah, Visakhapatnam, A.P, India[3]

ABSTRACT: Authentication is one of the very effective ways to forestall unauthorized and corrupted communications from being forwarded in wireless sensor networks (WSNs). Because of this, many message authentication schemes have been developed, based upon either symmetric-key cryptosystems or public-key cryptosystems. Many of them, yet , have the limitations of high computational and communication expense in addition to absence of scalability and strength to node compromise problems. To address these issues, a polynomial-based scheme was recently introduced. However, this scheme and its extension cables, all have weakness of a built-in threshold decided by the degree of the polynomial: when the number of messages sent is larger than this threshold, the adversary can fully recover the polynomial. In this paper, we propose a scalable authentication plan depending on hybrid key exchange algorithm. While enabling more advanced nodes authentication, our recommended scheme allows any client to transmit an unrestricted number of messages without suffering the threshold problem. In addition, our structure can also provide meaning source privacy using Diffie Hellman key exchange protocol and behave as resistance to sender and receivers.

KEYWORDS: Public-key cryptosystem, Wireless sensor networks (WSNs), Encryption, Decryption, Diffie Hellman key exchange algorithm, ElGamal Signature scheme.

I. INTRODUCTION

The system which allows the sender to send a message to the receiver in such a way that if the improved message will almost discovered by Receiver that is called as message authentication. All of us can also declare communication authentication is data origins authenticity. Protecting the honesty of a message is performed by message authentication. Every user while using concept authentication expects that each and every message should be passing just as same condition that it was sent without adding any modified bits or extra characters.

Wireless sensor networks have special characteristics because of total absence of system or administrative support that they have limited bandwidth, energy constraints, and low computational functions. Instead of all constraint WSN is useful where communication is done without infrastructure support. Security is the main restriction in WSN, as sensor node may be stationed by attacker and the private information may get hacked. In many instances it is sufficient to obtain data transfer between the sensor nodes and the base station. Especially, the base station must have the ability to ensure that the received message was sent by specific sensor node rather than modified while transferring. A large number of WSN applications such as health-care monitoring systems or military domains needs strong and lightweight authentication plans to obtain data from unprivileged users that is absolutely unconfident. To overcome all such security issues many different schemes were discovered. Some schemes works with finding the compromised node, or detecting the injected bogus message in the networking or giving special documentation to the sender or receiver, Encryption and decryption is the famous way of providing the security.

In wireless sensor networks the unofficial and corrupted message can be effectively prevented by concept authentication. We can say message authentication is a short item of information used to authenticate a message to provide integrity and authenticity assurances on the message. Accidental and deliberate message changes, provides an integrity of message even though the message's origin affirms reliability. Until now various authentication schemes have been offered to provide message genuineness and integrity verification for wireless sensor networks (WSNs). Symme-

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

tric-key cryptosystems or public-key cryptosystems are the basic strategies. Most of them, have various limitations like high computational and communication cost to do business, lack of scalability, client compromise attacks. Diffie-Hellman establishes a shared top secret that can be used for secret communications while exchanging data on the community network. Diffie Hellman key exchange is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This Key can then be used to encrypt subsequent communications using a symmetric key cipher. The scheme was first published by Whitfield Diffie and Martin Hellman in 1976.

II. LITERATURE SURVEY

Many 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. However, these schemes require initial time synchronization, 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.

A secret polynomial based message authentication scheme was introduced; this scheme offers information-theoretic security with ideas similar to a threshold secret sharing, where the threshold is determined by the degree of the polynomial. For the public-key based approach, 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.

Attacking cryptographic scheme show attacks that have recently been proposed for achieving various security goals in sensor networks. 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.Rivest, A. Shamir, and L. Adleman 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, 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 do work to provide insights in integrating and designing public-key based security protocols for sensor networks. The signature scheme introduced by author David Pointcheval and Jacques Stern. Here they address the question of providing security proofs for signature schemes in the so-called random oracle model. They establish the generality of this technique against adaptively chosen message attacks. Our main application achieves such a security proof for a slight variant of the Elgamal signature scheme where committed values are hashed together with the message. Ashwini M.Rathod and Archana.C introduces a Secure Network Discovery by Message Authentication in Wireless Sensor Network. They propose a scalable authentication scheme based on elliptic curve cryptography (ECC). While enabling intermediate nodes authentication, that scheme allows any node to transmit an unlimited number of messages without suffering the threshold problem. The system also proposed a source privacy Dining cryptographer scheme which works on preserving security for message authentication over the destination keeping data confidential, that who sends message to whom in a world where any transmission can be traced to its origin. This problem solved by author is unconditionally or cryptographically secure based on one time used key or public keys .Here author actually encrypt the message with intended recipient public keys to ensure the secrecy. The sender keeps the identity of the recipient secret. Also arrange the prefix to each message that the recipient only decrypt the message with recognized prefixed. A different prefix is used each time. New prefix could be agreed in advance, generated cryptographically as needed. A public key distribute system can be used to construct a computationally secure sender untraceably channel. A Statistical En-route Filtering (SEF) mechanism that can detect and drop such false reports. We know that a sensor network composed of a large number of small sensors. These sensor nodes are not equipped with temporary resistsent network. Here the major issue of security compromises in large scale sensor network. In Large scale sensor

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

network detecting and purging bogus reports injected by compromised node is a greater challenge .When a node is compromised that node become accessible. These nodes successfully provide bogus reports to its neighbors which results in manipulated solution. Such problems can be solved by asymmetric cryptography is infeasible. So a new technique of statistical enroute filtering where SEF exploits dense deployment of sensor network. For preventing a node to break down SEF carefully limits amount of information assigned to any node, and releases on the collective decision of multiple sensor for false report. When any sensor report is forwarded to any node, each sending node verifies the correctness of the MAC, carried with certain probability of the report is dropped in correct MAC. Here a key assignment method is designed for enroute detection of false report. They devise a mechanism for collective data report generation, enroll report, filtering and sink verification .Here the author proves that SEF is efficient at detecting and dropping such false report injected by compromised node. It can filter out 80% to 90 % false data by a compromised node. ElGamal Public key cryptography is applied for digital signature. Elgamal also have security on the discrete logarithm problem .Here improved Elgamal algorithm makes more extensive application in the field of authentication. Here we included a new improved Elgamal algorithm over a old Elgamal algorithm which is more efficient. They also tried to show the difference between them mainly in adding the random number to make original more complicated and more difficult to decipher. In case if Elgamal the hackers apparently need to solve logarithm for three times then test each solution and need to go through an inverse element and exponential. This makes the new Elgamal more complex . Here we concentrate on enhancing security of random number. Also provide more complex link between the random number and private key. So that hackers cannot use random number to attack the private key indirectly. An interleaved hop-by-hop authentication scheme is implemented for perfect authentication. In militating application we always need to monitor the opponents activity .These can be achieved by clustering a certain group of nodes for interested area and we can also create a base station in a secure location to control the sensor and to collect the data. A hacker the main culprit may compromise sensor node and then use the same node to inject the false or wrong data to network. Here we focus our work towards the false injection attacks. As per this scheme base station is responsible for enabling the authenticity of report. This scheme filter out the false injected packet into the network by compromised node before reaching towards the base station. In this paper we are using a hybrid key exchange algorithm to enhance the security of the users it is named as Diffie Hellmann key exchange algorithm. By using this algorithm nodes can communicate by exchanging a secret key. By this we can provide security not only to the message but also to the users who communicate.

III. EXISTING SYSTEM

In existing system, a scalable authentication scheme based on elliptic curve cryptography (ECC) was proposed. While enabling intermediate nodes authentication, this scheme allows any node to transmit an unlimited number of messages without suffering the threshold problem. We develop a source anonymous message authentication code (SAMAC) on elliptic curves that can provide unconditional source anonymity through hop by hop message authentication process. In order to evaluate the existing message authentication, SAMAC act as resilience to active and passive attack.

Disadvantages of existing system

1. Increase in routing overhead.
2. Key computation cost is high.
3. Only provides security to the message and doesn't concentrate on security issues of users.

IV. PROPOSED SYSTEM

The proposed system concentrates on providing high privacy to the message authentication. In addition to hop by hop message authentication, key exchange mechanism is enhanced through Diffie-Hellman key exchange algorithm. The source node encrypts the data using the public key of receiver node, and then transmits the data. After receiver receiving the data, it needs a private key for decrypting data. So the receiver request key server to produce a private key, the key server authenticates the receiver, access through key authentication. It is very hard for the malicious node to get a key from key server.

Advantages of proposed system

1. Low routing overhead.
2. Security to message as well as users.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

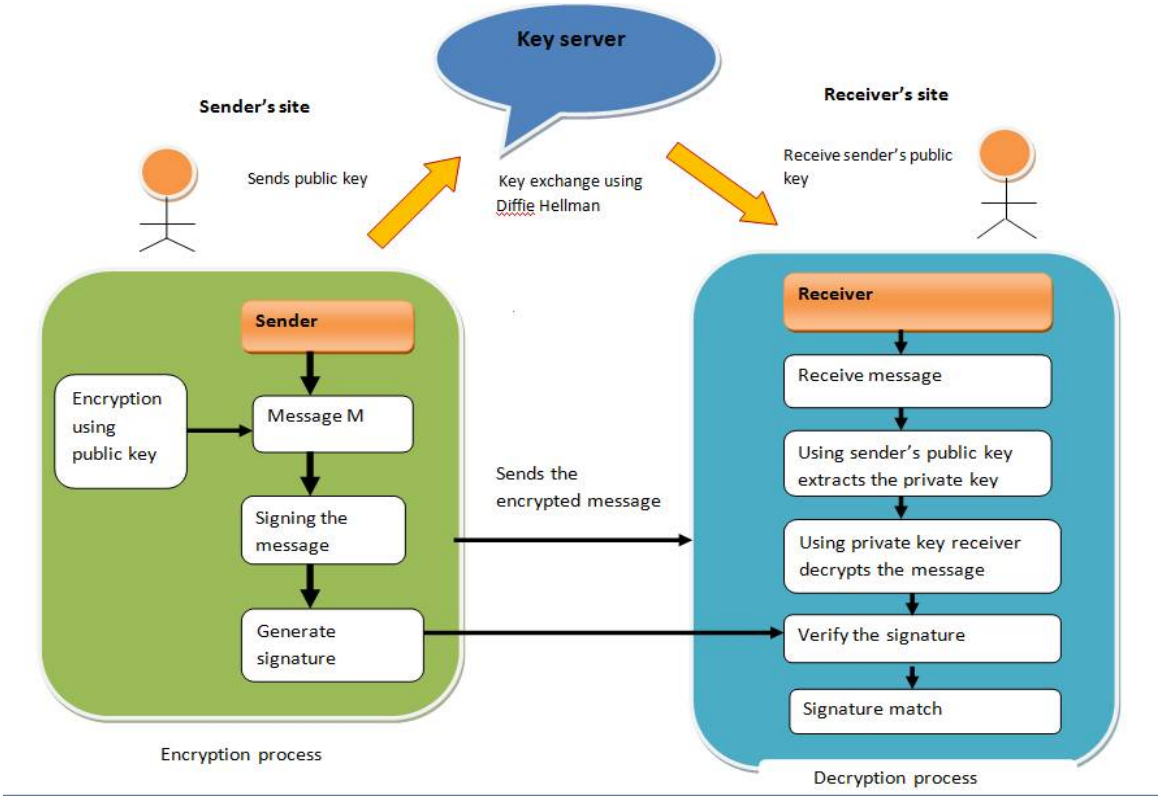
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

3. Increase in security and low security risks.
4. Key authentication time is more efficient.

V. PROPOSED ARCHITECTURE



VI. PROPOSED ALGORITHM

Diffie Hellman key exchange algorithm:

The first published public key algorithm is proposed by Diffie and Hellman and generally referred as "DIF-FIE-HELLMAN KEY EXCHANGE ALGORITHM".
The purpose of the algorithm is to enable two users to securely exchange a key that is used for subsequent encryption of the messages. This algorithm uses modulus arithmetic for its calculation.
Suppose user A and user B wish to communicate by exchanging a key.

1. For this there are two publicly known numbers a prime number 'q' and an integer 'p' that is primitive root of 'q'.
2. Now user A selects a random integer xa<q and computes ya=(p to the power xa)modq.
3. Similarly user B selects a random integer xb<q and computes yb=(p to the power xb)modq.
4. Now user A computes the secret key k=(yb to the power xa)modq.
5. Similarly user B computes the secret key k=(ya to the power xb)mod q.
6. Finally they produce identical results.The result is that the users A and B exchanged a secret value.
7. Here xa and xb are private.

If an intruder wants to stop communication between A and B he will have the values p,q,ya and yb.
With this he cannot calculate the secret key as xa and xb are unknown.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Thus he is forced to take discrete logarithm to determine the key.
For example to determine the private key of user B, the intruder must compute xb=(dlog to the base p,q)yb.
Intruder calculates the key in the same manner as user B calculates it. Here the fact is that it is relatively easy to calculate exponentials modulo a prime,where as it is difficult to calculate discrete logarithms.
For large primes the task is considered infeasible.

Elgamal digital signature scheme:

It is defined by a famous mathematician named "ELGAMAL".It is defined in five steps.

1. Firstly consider a large prime number and let it be 'q'. Then 'p' be primitive root of 'q'.
2. **User A(senders) public/private key generation.**
3. Here user A generates a random integer 'Xa' such that 1<Xa<q-1 where 'q' is prime number and 'Xa' is private key.
4. Then with 'Xa' compute 'Ya' i.e. Ya=(p to the power Xa)modq.
5. Therefore User A's private key is 'Xa' and public key is {q,p,Xa}.
6. **Signing of a message "M".**
7. In order to form digital signature, hash value for the message must be calculated i.e. compute the hash of the message 'M' m=H(M) where 'm' is an integer 0<m<q-1.
8. Choose a random integer 'K' such that 1<k<q-1 and gcd(k,q-1)=1 i.e. 'k' is relative prime to q-1.
9. Now compute S1=(p to the power k)modq.
10. ComputeS2=kinverse(m-XaS1) mod(q-1).
11. Finally signature=(S1,S2).
12. **Verification of signature at user B**
13. At user B compute V1=(p to the power m)mod q and
    V2=((Ya to the power S1)(S1 to the power S2))mod q.
14. If V1=V2 signature is valid.

This is how Elgamal signature scheme is used to perform secure communication between sender and receiver.

VII. CONCLUSION

In order to secure communication message authentication is very important. Through proper message authentication only, one can achieve great security. Security is the only seed that plant the proper tree of authenticity. This paper investigates the different techniques available in message authentication. As per the further proceeding my plan is to develop a new efficient authentication scheme using the elliptic curve cryptography. In this scheme any node can transmit a large number of messages without threshold problem. This service is usually provided through the deployment of a secure message authentication code (MAC). Further we used a hybrid key exchange mechanism for secure communication. Here the communicating parties exchange keys for secure communication. In this paper we not only just exchange keys but also generate signatures for securely exchanging keys. After generating signatures a verification process is performed in order to check whether the communicating parties are authenticated or not. This is how Diffie Hellman key exchange algorithm is used for secure communication in wireless sensor networks.

REFERENCES

1. F. Ye, H. Lou, S. Lu, and L. Zhang, "Statistical En-Route Filtering of Injected False Data in Sensor Networks," Proc. IEEE INFO COM, Mar. 2004.
2. S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-ByHop Authentication Scheme for Filtering False Data in Sensor Networks," Proc. IEEE Symp.Security and Privacy, 2004.
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 Networks," Proc. IEEE INFOCOM, Apr. 2008.
5. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," Proc. IEEE Symp. Security and Privacy, May 2000.
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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

7. 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.
8. T.A. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. Information Theory, vol. IT-31, no. 4, pp. 469-472, July 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," Proc. IEEE 28th Int'l Conf. Distributed Computing Systems (ICDCS), pp. 11-18, 2008.
10. D. Pointcheval and J. Stern, "Security Proofs for Signature Schemes," Proc. Advances in Cryptology (EUROCRYPT), pp. 387398, 1996.
11. Efficient Key Establishment for Wireless Sensor Networks Using Elliptic Curve Diffie-Hellman. Tony Chung and Utz Roedig. 2007
12. A New Approach for Establishing Pairwise Keys for Securing Wireless Sensor Networks. Wacker, Knoll, Heiber and Rothermel. 2005.