Volume 5, Issue II, Feb. 2017
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

An efficient key management in Wireless Sensor Networks using ECDH Digital Signature algorithm

Neha Kapoor [1], Er. Sushil Lekhi [2]
[1]Research Scholar, [2]Assistant Professor
Computer Science Engineering Department, Punjab Technical University
Rayat Institute of Engineering & Information Technology, Ropar, India
[1] erkapoor.neha@gmail.com, [2] lekhi.engg@gmail.com

Abstract: *Wireless sensor networks (WSNs) consist of immense number of small sensor nodes that pass the collected information using the wireless channels. Most sensor networks comprises of thousands of low power, less- cost nodes expand to monitor and affect the environment. When the sensor nodes are installed in any environment, the problem of secure sharing of keys between sensor nodes becomes an issue of attention as sensor nodes are susceptible to various types of undesirable e attacks. In the proposed research work, Elliptic Curve Diffie Hellman (ECDH) Cryptography algorithm has been implemented. Elliptic Curve Diffie Hellman (ECDH) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECDH generate keys through the properties of the elliptic curve equation instead of earlier method of generation as the product of very large prime numbers. Our primary objective is to study about symmetric and asymmetric security algorithms for wireless sensor networks. Further study is about various key management techniques in wireless sensor networks. The entire scenario has been implemented in Network simulator version 3. Digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party. The use of Digital Signature in the proposed work ensures security and authentication. It has been observed that the implementation of ECDH algorithm is showing better results as compared to simple ECC algorithm being implemented in the previous work. The comparison has been shown using parameters such as execution time of the algorithm with sink and without sink.*

Keywords: *Wireless Sensor Network, ECDH, ECC, Network security, Encryption and Decryption.*

1. INTRODUCTION

Wireless sensor networks (WSNs) consist of large number of tiny sensor nodes that send the gathered information using the wireless link. This sensor network is a amalgamate system combining insignificant sensors and actuate with figure out elements. Most of the sensor networks consist of thousands of low power, less- cost nodes expand to check and affect the environment. WSNs have number of applications like traffic control, health monitoring and environment monitoring etc. Most of the applications of WSNs need secure communication of information at both ends. Therefore security in WSNs is an important issue because sensor nodes have minimum storage and energy for processing [1, 2]. When these sensor nodes are used in any environment, the issue of secured sharing of keys between sensor nodes becomes an issue of attention as sensor nodes are prone to many types of undesirable attacks. Wireless nodes can communicate with each other using wireless channels. Wireless networking is a method by which homes, telecommunications networks and business installations ignore the costly process of introducing cables into a home, office etc. Wireless telecommunications networks are installed using radio communication. Wireless network gives facility of movement and also provide capability to extend applications to various parts of a building, city, or nearly anywhere in the world.[3]

2. SECURITY REQUIREMENTS FOR WSN

a) Message authentication: The message receiver should be able to verify whether a received message is sent by the node that is claimed or by a node in a particular group. In other words, the receiver cannot pretend to be an innocent node and inject fake messages into the network without being detected.[4,5]

b) Message integrity: The message receiver should be able to identify whether the message has been modified en-route by the adversaries. In other words, the adversaries cannot modify the message content without being detected.

c) Identity and location privacy: The adversaries cannot determine the message sender's ID and location by analyzing the message contents or the local traffic.

d) Node compromise resilience. The scheme should be active to node compromise attacks. No matter how many nodes are compromised, the remaining nodes can still be secure.

e) Efficiency: The Security scheme should be efficient in terms of both computational and communication overhead.

3. TYPES OF WIRELESS SENSOR NETWORK

Depending on the environment, the types of networks are decided so that those can be deployed underwater, underground, on land, and so on.

a) Terrestrial WSNs: Terrestrial WSNs are reliable of communicating base stations efficiently, and consist of hundreds to thousands of wireless sensor nodes deployed

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

either in disorganized (ad hoc) or structured (Preplanned) manner. In a disorganized mode, the sensor nodes are randomly spread within the target area that is discarded from a fixed plane. The preplanned or structured mode considers optimal placement, grid placement, and 2D, 3D placement models. In this WSN, the battery power is limited; however, battery is equipped with solar cells as an alternative power source.[6]

b) **Underground WSNs:** The underground wireless sensor networks are more costly than the terrestrial WSNs in terms of deployment and demand, maintenance, and equipment cost attentions and careful planning. The WSNs networks consist of a couple of sensor nodes that are not visible in the ground to monitor underground conditions. To broadcast information from the sensor nodes to the base station, extra sink nodes are located above the ground. The underground wireless sensor networks deployed divided into the ground are difficult to reactivate. The sensor battery nodes equipped with a limited battery power are difficult to recharge. In addition to this, the underground environment makes wireless communication a objection due to high level of attenuation and signal drop.

c) **Under Water WSNs**: More than 70% of the earth is occupied with water. These networks consist of a number of sensor nodes and vehicles deployed under water. Self-governing underwater vehicles are used for gathering data from these sensor nodes. A challenge of underwater communication is a large propagation delay, and bandwidth and sensor failures. Under water WSNs are attached with a limited battery that cannot be recharged or replaced. The issue of energy reservation for under water WSNs involves the development of underwater communication and networking technologies.

d) **Multimedia WSNs:** Multimedia wireless sensor networks have been proposed to enable tracking and observation of events in the form of multimedia, such as imaging, video, and audio. These networks consist of low-cost sensor nodes equipped with microphones and cameras. These nodes are linked with each other over a wireless connection for data compression, data retrieval and cooperation. The challenges with the multimedia WSN include high energy consumption, high bandwidth needed, data processing and compressing techniques. In addition to this, multimedia contents require high bandwidth for the contents to be delivered properly and easily.

e) **Mobile WSNs:** These networks consist of a collection of sensor nodes that can be moved on their own and can be interacted with the physical environment. The mobile nodes have the ability to compute sense and communicate. The mobile wireless sensor networks are much more versatile than the static sensor networks. The advantages of MWSN over the static wireless sensor networks include better and improved coverage, better energy efficiency.[4]

4. EXISTING WORK

In previous work several secure WSN protocols for revocations and renewal of cryptographic keys in the network based on symmetric encryption and elliptic curve cryptography (ECC) have been proposed. For all their solutions, they gave a formal analysis of the security of the protocols using Scyther, a self verification tool for cryptographic protocols. All the proposed protocols were proven safe but have different security levels by using different types of keys. They present the results without the execution time of the sink, since in many applications the base station is a special node with extra resources. [7]

4.1. Key Revocation protocol

It guarantees an authenticated allocation of new keys that are efficient in terms of storage, communication and calculation overhead. The protocol minimizes the number and the size of re-keying messages. It achieves the required level of confidentiality and authenticity of re-keying messages by only using symmetric ciphers and one-way functions. Hence, the protocol is scalable, and particularly attractive for large and/or highly dynamic groups. [8,9]

4.2. Renewing and Revoking of Keys

A certificate indicates a time period during which it is valid. Attempts to utilize a certificate for authentication after or before its validity period will fail. Therefore, mechanisms for managing certificate renewal are essential for any certificate management strategy. For example, an administrator may want to be notified automatically when a certificate is about to die, so that an appropriate renewal process can be finished in plenty of time without causing the certificate's subject any problem. The renewal process may involve reusing the similar public-private key pair or allocating a new one.

5. PROPOSED SOLUTION

In the proposed research work, ECDH algorithm with Digital Signature has been implemented. Computations needed for the ECDH authentication are: key pair generation (private key, public key), the signature computation, and the signature verification.

A. KEY PAIR GENERATION

Before an ECDSA authenticator can run, it needs to identify its private key. The public key is calculated from the private key and the domain parameters. The key pair must be in the authenticator's memory. As the name implies, the private key is not visible to the outside world. The public key, in contrast, must be openly accessible.

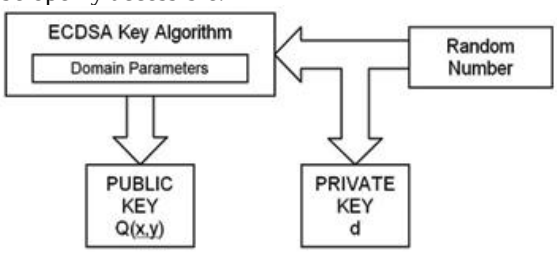

Figure 1: Key pair generation process

Volume 5, Issue II, Feb. 2017
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

A random number generator is initiated and, when its operation is finished, delivers the numeric value that becomes the private key d (a scalar). The public key Q(x,y) is calculated in equation (1) as:

$$Q(x, y) = d \times G(x, y)$$

B. DIGITAL SIGNATURE COMPUTATION

A digital signature allows the recipient of a message to verify the message's authenticity using the authenticator's public key. First, the variable-length message is converted to a fixed-length message digest h(m) using a secure hash algorithm. After the message digest is computed, a random number generator is activated to provide a value k for the elliptic curve computations.

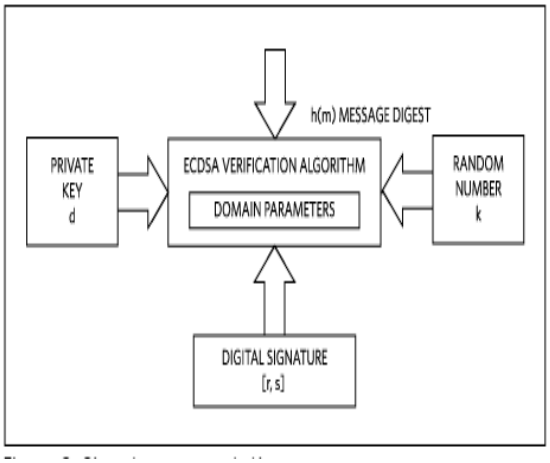

Figure 2: Signature Computation

C. SIGNATURE VERFIFICATION

The signature verification is the counterpart of the signature computation. Its purpose is to verify the message's authenticity using the authenticator's public key. Using the same secure hash algorithm as in the signature step, the message digest signed by the authenticator is computed which, together with the public key Q(x,y) and the digital signature components r and s, leads to the result.

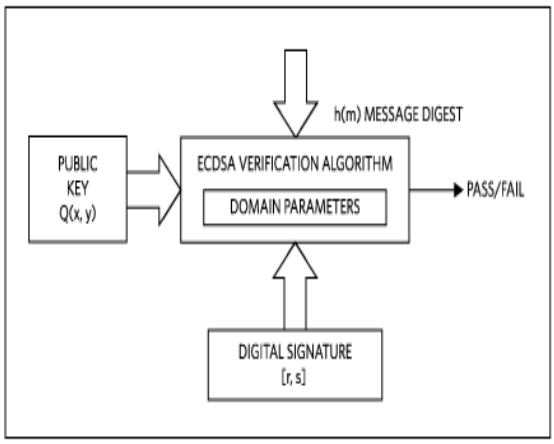

Figure 3: Signature Verification

6. OBJECTIVES

The major objectives of the proposed research work are:

1. To study about symmetric and asymmetric security algorithms for wireless sensor networks.
2. To implement entire work in Network Simulator version 3.
3. To implement the concept of Diffie Hellman algorithm and Digital Signature in Simple ECC algorithm and compare the results on the basis of various parameters such execution time.

7. RESULTS

The use of Digital Signature in the proposed work ensures security and authentication. It has been observed that the implementation of ECDH algorithm is showing better results as compared to simple ECC algorithm being implemented in the previous work. The comparison has been shown using parameters such as execution time of the algorithm with sink and without sink.

Execution Time: It is the time during which a program is running (executing), in contrast to other program lifecycle phases such as compile time, link time and load time.

Table 1: Execution Time

Sr. NO.	PROTOCOL	TIME WITH S(ms)	TIME WITHOUT S(ms)
1	Revocation	155.37	87.58
2	Renewing SymKey	10042.32	10042.32
3	Renewing AsymKey	6797.75	3436.24
4	Renewing Network Key	221.09	121.4
5	Improved ECDH	90.7491	49.5849

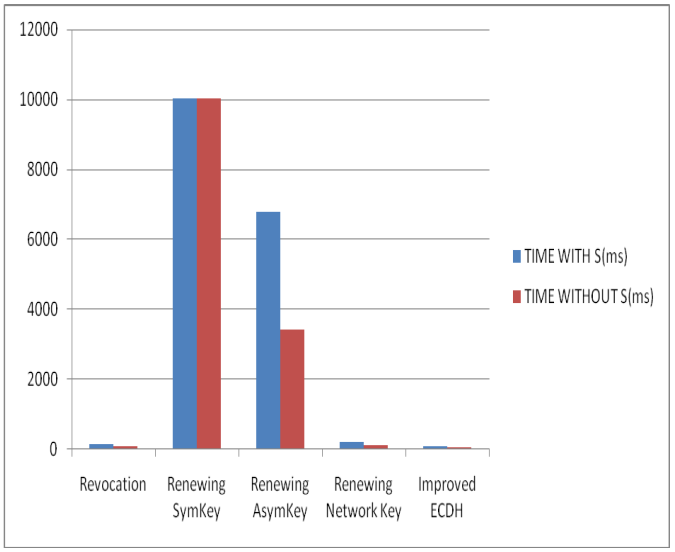

Figure 4: Execution time

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

8. CONCLUSION AND FUTURE SCOPE

It is concluded that ECC algorithm with Digital Signature is performing better as compared to ECC algorithm. Simulation results are obtained using Network Simulator version 3. Parameter used for comparison is Execution time. ECDH algorithm with Digital Signature is secured as compared to ECC algorithm in the sense it provides Authenticity and Confidentiality as well. It also resolves the existing problems of Replay attack, Man in Middle attack and Mutual Authentication. ECDH with Digital Signature has been proved as the best cryptographic technique for secure data transmission in a resource constrained environment.

In future, new security mechanism can be implemented with better security and privacy. The implemented work can be tested on real time systems. Further security parameters should be considered for a better and improved security. These security algorithms may be implemented on Health care systems where medical data security is very crucial. Also in future they can be tested on Universities and Colleges information management system where they can provide required security to the confidential data.

REFERENCES

[1] **Al-Sakib Khan Pathan, Hyung-Woo Lee and Choong Seon Hong (2006), "*Security in Wireless Sensor Networks: Issues and Challenges*" ICACT2006, ISBN 89-5519-129-4, pp 20-22.**

[2] **Mona Sharifnejad, Mohsen Sharifi, Mansoureh Ghiasabadi and Sareh Beheshti (2007), "*A Survey on Wireless Sensor Networks Security*", 4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications", March 25-29, 2007.**

[3] **Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz (2008), "*Security Issues in Wireless Sensor Networks*", International Journal of Communications, Issue 1, Volume 2, 2008.**

[4] **Hemanta Kumar Kalita1 and Avijit Kar (2009), "*Wireless Sensor Network Security Analysis*", International Journal of Next-Generation Networks (IJNGN), Vol.1, No.1, December 2009**

[5] **Gaurav Sharma, Suman Bala, A. K. Verma and Tej Singh (2010), "*Security in Wireless Sensor Networks using Frequency Hopping*", International Journal of Computer Applications (0975 – 8887), Volume 12– No.6, December 2010.**

[6] **Hemanta Kumar Kalita and Avijit Kar (2011), "*Key Management and Security Planning in Wireless Ad-Hoc Networks*", 2nd International Conference and workshop on Emerging Trends in Technology (ICWET) 2011.**

[7] **T. Lalitha and R. Umarani (2012), "*Cluster based Efficient Key Management and Authentication Technique for Wireless Sensor Networks*", International Journal of Computer Applications (0975 – 8887), Volume 39– No.16, February 2012.**

[8] **Jyoti Shukla and Babli Kumari (2013), "*Security Threats and Defense Approaches in Wireless Sensor Networks: An Overview*", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 3, March 2013.**

[9] **P.Uthaya Bhanu1 and J. Saravanan (2014), "*Data Security in Wireless Sensor Network*", International Journal of Innovative Research in Computer and Communication Engineering, ISSN (Online): 2320-9801, Vol. 2, Issue 2, February 2014.**

[10] **Jian Li, Yun Li, Jian Ren and Jie Wu (2014), "*Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks*", IEEE transactions on parallel and distributed systems, vol. 25, no. 5, may 2014.**

[11] **Ismail Mansour, G´erard Chalhoub, Pascal Lafourcade, and Franc¸ois Delobel "*Secure Key Renewal and Revocation for Wireless Sensor Networks*", 39th Annual IEEE Conference on Local Computer Networks LCN 2014, Edmonton, Canada.**

[12] **Wenliang Du, Jing Deng. Yunghsidng S. Hant. Shigang ChenT. and Prainod K. Varshney(2004), "*A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge*", IEEE 2004, 07803-8355-9/0.**

[13] **A Price, "*A Key Pre-Distribution Scheme for Wireless Sensor Networks*," IEEE TRANSACTIONS, pp 253–260, 2005.**

[14] **X. Huang and M. Yang, "*Secure Key Management Protocol for Wireless Sensor Network Based on Dynamic Cluster*," *IEEE TRANSACTIONS*, no. 90304015, 2006.**

[15] **Y. Xiao, V. Krishna, B. Sun, X. Du, and F. Hu, "*A survey of key management schemes in wireless sensor networks*," *IEEE TRANSACTIONS*, vol. 30, pp. 2314–2341, 2007.**