International Journal of Computational Science, Mathematics and Engineering
IJCSME-Volume-3-Issue-1-January-2016
E-ISSN-2349-8439

PAILLIER HOMOMORPHISM: A Technique for Secure Data Transmission in Sensor Network

Mr. Nithin Kumar[1], Mr. SachinAcharya T[2], Mrs. Nagarathna[3]

ABSTRACT: Wireless sensor network is a special type of ad-hoc network. It is mainly used in critical systems whose failure may result in serious economic and business losses and threats to human life and surveillance, medical applications, intrusion detection systems and many more. As the outcomes of these systems are critical, the security of wireless sensor networks which senses the events or gives an input for computation is very essential. The lack of required level of security may be because of the human intervention, restriction of resources to cut short the budget of the system or due to system failures or errors. In this paper, we present a holistic view of security issues and malicious attacks in wireless sensor networks and an acceptable secure data transmission technique where the communication between the wireless sensor nodes is secured.

Keywords: Wireless sensor networks, Security goals, Security attacks, Security techniques, Data security, Cryptography, Homomorphism

I. INTRODUCTION

The advancement in technology has a very determined need for networking. The networks may be wired or wireless. The wired networking may follow specific patterns such as LAN, WAN, PAN and MAN. The wireless networks use sensors for communication between the nodes and hence they are popular as *Wireless sensor networks (WSN). The* wireless sensor networks are preferable than wired networks because there is no need for communication monitoring between the nodes and is efficient with respect to energy and cost [19]. The sensor nodes in a wireless sensor network may be densely deployed and even the topology of the nodes within the network may change due to failures or mobility. This sensor does not have a global identification but can be multifunctional. Considering these elegant properties of wireless sensor networks, it is used in several business and mission critical systems. The sensors in the wireless sensor networks even consume less power and are widely preferred and acceptable in several applications

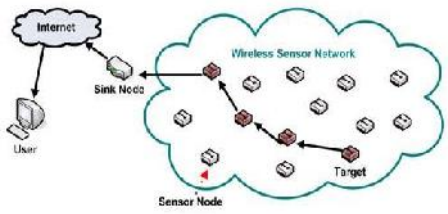

Figure 1: Wireless Sensor Network

[1]M.Tech scholar/Department of CS&E/P.E.S College of Engineering, Mandya, 571401, India
[2]M.Tech scholar/Department of CS&E/P.E.S College of Engineering, Mandya, 571401, India
[3]Associate Professor/Department of CS&E/P.E.S College of Engineering, Mandya, 571401, India

As these sensors play a prominent role in the network, securing them is also a major issue. Even while securing them the energy consumption with respect to computation, memory and transmission range are considered. The main motive of security services is to secure the resources and information from attacks and misbehavior. Some of the expected security goals are [20]:

- *Availability*, the services from the wireless sensor networks should be available at all instances even in the situations of denial of service attacks.
- *Authorization*, only the authorized users must be given access to the network and its components.
- *Confidentiality*, only the desired recipients should share and use the messages and other resources within the network.
- *Integrity*, the message exchange between the nodes in a network should not reach the hands malicious intermediary nodes.
- *Non repudiation*, the node should not deny about sending a message that it has previously sent.

Apart from the above mentioned goals, data freshness, self-organization, time synchronization and secure localization should also be considered while planning to secure the wireless sensor networks. Wireless sensor networks are frequently prone to attacks because of their broadcast nature of the transmission medium. Sometimes even the nodes may be placed in certain physical danger zones where there are not secured and even can be accessed by an intruder. Several commonly occurring attacks which are frequently observed are eavesdropping, packet dropping, packet replay attacks, spoofing of packets and denial of service [21]. The organization of the paper is: section II deals with different types of attacks on WSN, section III deals with different security techniques for handling attacks in WSN, section IV

DOI: 10.18645/IJCSME.31.001

deals with homomorphic encryption to provide data security in WSN, section V provides conclusion and finally paper ends with few references.

II. SECURITY ATTACKS

WSN are vulnerable to several security attacks because of their broadcast nature of data transmission, and wireless sensor networks may also sufferfrom additional threats because sensor nodes are deployed in unpractical environments where they are not protected. The attacks in wireless sensor networks may occur from inside the network or from outside the network or intruder. According to the interruption of communication act, the attacks in WSN can be classified as being active or passive. It may be passive where the attack may be of the sort of eavesdropping or it may be active where the complete or a part of data may be altered or a false stream of data may be produced.

Some of the passive attacks frequently observed are:

A. TRAFFIC ANALYSIS

It involves the process of interrupting and examining messages in order to deduce information from patterns in a network. Keep *monitoring* of network traffic can help in reducing these kinds of attacks.

B. EAVESDROPPING

It is limited to just listening and analysis of the network traffic. It can be easily realized but very difficult to detect. It affects the confidentiality of the network system. Certain encryption techniques can be used to avoid eavesdropping.

Some of the active attacks commonly seen in WSNs are:

C. JAMMING

It's a type of attack which interfaces with the radio frequencies that a network's nodes are using. It may be powerful to affect the whole network or disrupt a smaller portion of it. The authenticity of the WSN may be affected. *Code spreading* can be used to avoid jamming.

D. TAMPERING

Here the attacker tries to access the sensitive information from the network such as cryptographic keys. The integrity of the network may be effected. *Tamper proofing* technique can be used as a defense against tampering.

E. COLLISION

When two nodes try to transmit on a same frequency simultaneously, then collision occurs. The checksum mismatch at the receiving end may occur when packets collide. It effects both integrity and confidentiality of the WSN. *Error correcting codes* are a typical defense system for collisions in WSN.

F. SINKHOLE ATTACK

In this attack the attacker makes a compromised node look more attractive in its environment. In this way, the attacker makes the surrounding nodes feel that it's a genuine node.

G. SYBIL ATTACK

In this attack a node can show more than one identity to the network. This may mainly leads to confusions and may result in miscommunications.

In the further sections, we discuss certain techniques to avoid these kinds of security attacks.

III. SECURITY TECHNIQUES IN WSNs

In this section, we present different types of defense mechanisms for various types of attacks in wireless sensor networks. Firstly, we present different types of cryptographic mechanisms, a number of key management protocols for wireless sensor networks are discussed next, defending against DOS attacks, various source routing mechanisms.

Cryptographic mechanisms selection is a difficult task in Wireless sensor networks because cryptographic mechanisms used in WSN should meet the constraints of WSNs such as battery power, size of data and code, time. Basically there are two types of cryptographic mechanisms, such as *Public key cryptography* and *Symmetric key cryptography*[1] [3]. Public key algorithms such as RSA arecomputationally complex in nature and usually require thousands of instructions to execute a security operation. Since most of public key cryptography is computationally complex in nature, WSN will make use of symmetric key cryptography in which a single key is shared between two communicating sides which is used for both encryption and decryption[2] [4].

Key management is an area that has received maximum attention of researchers in WSN. Key management is an important part of security mechanism in WSNs [9]. The use of key management is to establish the keys between the nodes in WSNs in a secure and efficient manner. In addition to that key management also provides facilities to secure node addition and relocation. The key management protocols that are used in WSNs have constraints on energy consumption and time so the most of key management protocols are based on symmetric key cryptography because public key cryptography is computationally complex in nature.

The key management can be classified into two main classes. They are

DOI: 10.18645/IJCSME.31.001

- Key management based on network structure.
- Key management on probability of key sharing.

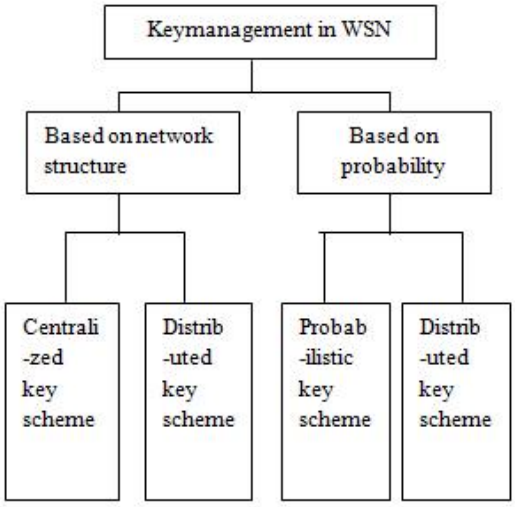

Figure 2: Classification of Key management in WSN

As shown in Figure 2, the key management can be classified into two types such as, *Key management based on network infrastructure* is a key management scheme depending on underlying network infrastructure [5] [6]. In centralized key management, there will be one entity (KDC) that will be responsible for key generation, key regeneration and distribution of keys. But in distributed key management different key management and different controllers are used to handle different set of operations such as generation, regeneration and distribution. *Key management on probability of key sharing* in which the key management protocol in WSNs can be classified based on probability of key sharing between a pair of sensor nodes in WSN [7]. Based on these probabilities the key management can be further classified into *deterministic* or *probabilistic*.

DOS attacks in WSN can be defended in physical layer, network layer and link layer. *Defense in physical layer* in which jamming attack is defended by adopting variations of communication such as frequency hopping and code spreading [12]. Frequency hopping spread spectrum (FHSS) is a method of transmitting signals from source to destination by rapidly switching frequency in random fashion known to both source and destination. *Defense in link layer* in which collision attack is defended by using error correcting codes [12] These error correcting codes works good at lower level collision such as environmental errors but these codes cause additional processing and transmission overhead in WSNs. *Defense in network layer* may be applied against spoofing attacks in WSNs by attaching Message authentication code (MAC) after the message [10] [11]. By attaching MAC to the message, the receiver can verify whether the message have been spoofed or altered.

WSN consists of several routing protocols. Based on network structure the routing protocols are classified into three categories. *Flat based routing*, in which all the nodes are treated as same with equal roles and functionality. *Hierarchical based routing*, in which nodes play important role in the network [16]. *Location based routing*, in which sensor nodes positions are taken into account to route data in the network [11]. The goal of secure routing protocols in WSNs is to provide Integrity, Authentication and Availability of messages. The existing secure routing algorithms for WSNs are based on symmetric key cryptography. µTESLA (the micro version of Timed, Efficient, Streaming, Loss tolerant, Authentication protocol) is an extension of [13, 14] has been proposed for authentication purpose in WSNs. µTESLA protocol requires timely unicast of initial parameters from base station to sensor node and this causes long delay in large scale sensor networks. Lia and Ning have proposed a multilevel key chain authentication to overcome the deficiency of µTESLA.

IV. HOMOMORPHIC ENCRYPTION IN WSNs

Homomorphic encryption is an encryption method which makes use of homomorphism and allows us to carry out arithmetic operations on cipher text. A *multiplicative homomorphic* method is a homomorphic encryption in which decryption of the two cipher texts yields the multiplication of the two corresponding plaintexts. Homomorphic encryption methods are useful whenever communicating parties are not having the decryption key(s) to perform arithmetic operations on a set of cipher texts [17][18]. In this paper we are introducing ahomomorphic encryption for wireless sensor networks to provide data security based on cipher based homomorphic encryption called as *paillier cryptosystem.* A paillier cryptosystem is a homomorphic encryption technique that is proposed by pasacalpaillier in 1999. The paillier cryptosystem is an *additive homomorphic* cryptosystem and makes use of asymmetric key algorithms, where the key used to encrypt a message is not the same as the key used to decrypt it. Each user has a pair of cryptographic keys, a *public* key and a *private* key. The private key is a secret key for every individual, and the public key may be widely distributed. Messages are encrypted using public key and can only be

DOI: 10.18645/IJCSME.31.001

decrypted with the corresponding private key. A standard notations used to describehomomorphic encryptions method is as follows, Enc() and dec() denotes the encryption and decryption techniques and s_1 and s_2 denotessensor$_1$ and sensor$_2$ data readings, Cindicates cipher text, and K indicates the key used for encryption and decryption respectively. If sensor data is grouped under addition operation, then we say that Enc() is an *additive homomorphic* encryption method.

A. PAILLIER CRYPTOSYSTEM

Paillier cryptosystem is anhomomorphic encryption algorithm that consists of following three main phases as shown below

1. Key generation (K)

The key generation steps executed by all the nodes in the network to generate public key is as following.

Step 1: select any two large prime numbers *p* and *q*randomly and independent of oneanother such that GCD(pq,(p-1)(q-1))=1..

Step 2: calculate the value of n=p*qand λ(n)=LCM(p-1,q-1)

Step 3: Choose a random variable g such that$g \in \mathbb{Z}^*_{n2}$, where $\mathbb{Z}^*_{n2}$is a set of n^{th} residues in a multiplicative subgroup.

Step 4: Ensure n divides the order of g by calculating the presence of the following modular multiplicative inverse:

$\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n$, where functionL is given by $L(u) = \frac{u-1}{n}$

Step 5: The public key is (n,g) for encryption.

Step 6: The private key is (μ,λ) for decryption.

2. Encryption (Enc)

Encryption at each node with the public key is as following.

Step 1: Let Sbe a sensor data to be encrypted where $S \in \mathbb{Z}_n$

Step 2: Select random variable r such that $r \in \mathbb{Z}_n^*$

Step 3: Generate cipher text using: $C = g^m.r^n \bmod n^2$

$C1 = EncK1\ (S1)$ (1)

$C2 = EncK2\ (S2)$ (2)

In equation (1) and (2), C1 and C2 indicates the cipher text of sensor data of sensor S1 and S2, and Enc( ) is an encryption function with public keys K1 and K2 respectively.

There is an efficient algorithm that can calculate a valid cipher text C3 from C1 and C2, cipher text C3 ∈ C using key K3 as shown below:

$C3 = EncK3\ (S1 \oplus S2)$

The decryption of cipher text C3 using a key K3 generates sensor data S1⊕ S2.

3. Decryption (Dec)

Decryption at the special intermediate node or the sink node is as following.

Step 1: Let C be the cipher text to be decrypted, where $C \in \mathbb{Z}^*_{n2}$

Step 2: Generate plain text using: $m = L(C^{\lambda} \bmod n^2) \cdot \mu \bmod n$

B. WORKED EXAMPLE

The following example illustrates paillier cryptosystem in WSN. Consider two sensor nodes named S1and S2 that are used to sense same physical phenomena. Let the data to beencrypted is 1010. Since they represent the same physical phenomena S1 = S2 = m = 1010.

- **Key generation**

Choose any two large prime numbers

P=293 and q=433

And calculate public key n = p*q = 126869 and

$n^2 = 16095743161$.

Compute λ(n) = LCM (p-1,q-1) = 31536.

Select random variable g such that, it is co-prime to n (GCD (L (g^{λ} (n) mod n^2), n) =1) i.e.

g = 6497955158.

Then public key is (126869, 6497955158) .

- **Encryption**at each sensor node.

n = 126869 g= 6497955158 $n^2 = 16095743161$

Select random variable r such that$r \in \mathbb{Z}_n^*$. For S1 r = 34, and for S2 r = 1312.

Using the formula $C = g^m.r^n \bmod n^2$, sensor data readings will be encrypted to respective cipher text as shown below

DOI: 10.18645/IJCSME.31.001

C_1 = 4821154392 and C_2 = 5720727730.

- **Decryption** at intermediate special node or sink node.

λ (n) = 31536 g= 6497955158 n^2 = 16095743161

L ($g^{\lambda} \bmod n^2$) = L ($6497955158^{31536} \bmod 16095743161$) = L (3967320500) = 31271.

$\mu = L(g^{\lambda} \bmod n^2)^{-1} \bmod n = 53022$.

The private key (μ,λ) generated is (31536, 53022).

L ($C_1^{\lambda} \bmod n^2$) = L (15249400063) = 120198.

L ($C_2^{\lambda} \bmod n^2$) = L (15249400063) = 120198

Generate sensor data readings using:

Sensor data = L ($C^{\lambda} \bmod n^2$) . μ mod n

Sensor data = 120198.53022 mod 126869

=1010.

C. ADVANTAGES OF PAILLIER CRYPTOSYSTEM IN WSNs

1) Paillier cryptosystem makes user to perform some operation on encrypted data without decryption keys.
2) Secret sensor data is transmitted over several sensor nodes in such a way that no one can retrieve the secret sensor data.
Finally, by applying this homomorphism function on encrypted data in WSNs provides a data security, data confidentiality, and data integrity to the data that's being transmitted through different nodes in a wireless sensor network.

IV.CONCLUSION

In this paper, we explain the encryption of sensor data using paillier homomorphism which is a concept on security that provides secure data transmission in WSN. Paillierhomomorphic encryption deals with the production of same cipher data by preserving the uniqueness of homomorphism that makes it different from other security techniques and methodologies. This method mainly focuses on maintaining the data integrity and data confidentiality of the transmitted data over several sensor nodes in a sensor network. Adoption of this technique overcomes certain drawbacks of other network security techniques and helps in maintaining the security goals in a sensor network.

REFERENCES

[1] A.J. Menezes, S.A. Vanstone, and P.C.V. Oorschot, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL, 1996.
[2] R.L. Rivest, "The RC5 encryption algorithm", In Fast Software Encryption, B. Preneel, Ed. Springer, 1995, pp. 86-96.
[3] D. Eastlake and P. Jones, U.S. Secure Hash algorithm 1 (SHA1), RFC 3174 (Informational), September 2001.
[4] R.L. Rivest, "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.
[5] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanism for large –scale distributed sensor networks", In *Proceedings of the 10th ACM Conference on Computer and*
[6] B. Lai, S. Kim, and I. Verbauwhede, "Scalable session key construction protocols for wireless sensor networks", In *IEEEWorkshop on Large Scale Real Time and Embedded Systems*, 2002.*Communications Security*, pp. 62-72, New York, NY, USA, 2003, ACM Press.
[7] S.A. Camtepe and B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks", In *Proceedings of the 9th European Symposium on Research ComputerSecurity*, 2004.
[8] J. Lee and D.R. Stinson, "Deterministic key pre-distribution schemes for distributed sensor networks", In *Proceedings ofSelected Areas in Cryptography*, 2004, pp. 294-307.
[9] J. Lee and D.R. Stinson, "A combinatorial approach to key predistribution for distributed sensor networks", In *Proceedings of theIEEE Wireless Communications and Networking Conference*, 2005.
[10] A. Perrig, R. Szewczyk, V. Wen, D.E. Culler, and J.D. Tygar, "SPINS: Security protocols for sensor networks", *WirelessNetworks*, Vol.8 , No. 5, pp. 521-534, September 2002.
[11] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", In *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols andApplications*, May 2003, pp. 113-127.
[12] A.D. Wood and J.A. Stankovic, "Denial of service in sensor networks", *IEEE Computer*, Vol. 35, No. 10, pp. 54-62, 2002.
[13] D. Liu and P. Ning, "Multilevel μTESLA: Broadcast authentication for distributed sensor networks", *Transactions on EmbeddedComputing Systems*, Vol. 3, No. 4, pp. 800-836, 2004.
[14] D. Liu and P. Ning, "Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks", In *Proceedings of the 10th Annual*

Network and Distributed System Security Symposium, San Diego, CA, February 2003, pp. 263-276.
[15] B. Karp and H.T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks", In *Proceedings of the 6th AnnualInternational Conference on Mobile Computing and Networking*, pp. 243-254, ACM Press, 2000.
[16] J.N. Al-Karaki and A.E. Kamal, "Routing techniques in wireless sensor networks: A survey, *IEEE Wireless Communications*, Vol. 11, No. 6, pp. 6-28, December 2004.
[17] Juan Wei, ShanqingGuo, QiuliangXu, "Secure Homomorphic Aggregation Algorithm of Mixed Operations in Wireless Sensor Networks", IEEE © 2011.
[18] NehaChhabra, ParikshitSingla "A Security Enhancing Homomorphic Encryption" Volume 2 Issue 7,July 2013
[19] D.Estin et al., "Intstrumenting the world with WSN", Proc. Intl conf. Acoustics, Speech and Signal Processing, Salt lake city,UT, May 2001
[20] Dr. G.Padmavathi, Mrs. D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks" IJCSIS
[21] E.Shi and A.Perrig, "Designing Secure sensor networks", Wireless comm. Mag., vol 11, no. 6, Dec 2004 pp. 38-43]