A Review on Security of Wireless Sensor Networks using Cryptographic Techniques

DINESH KUMAR GUPTA[1], DR. DEEPIKA PATHAK[2]
[1,2]Department of Computer Application, Dr. A. P. J. Abdul Kalam University, Indore 452016, India
Corresponding Author Email: dineshgupta1111@gmail.com

Abstract*— Wireless Sensor Networks have self-directed sensor nodes close to one or extra base stations. Sensor nodes are linked to all other and transmit the data to the base station. The nodes turn into weak to attacks and require for precious safety techniques as WSN growth. The use of the wireless sensor networks need for the proficient and make safe communication of data. We require the cryptography algorithms which offer high-quality solution for well-organized and safe data transmission. Frequently data confidentiality and key management is applied for giving consistent security techniques. Recognition of appropriate cryptographic technique is a significant confront due to restriction of energy, computation capacity and storage spaces of the sensor nodes. Symmetric cryptography techniques are not appropriate fine when the numeral sensor nodes enhance. Hence asymmetric cryptography based schemes are more used.

***Index Terms*— WSN, Private Key, Public Key, Symmetric and Asymmetric Cryptography.**

I. INTRODUCTION

Wireless Sensor Networks (WSN)

A WSN is a broad network of wireless sensor nodes which sense the information from outside sources. A wireless node keeps machinery like storage space, processing, sensing and message as their major electronic machinery. Normally the power passed by this electronic machinery is low. Electronic devices are the mostly participate the job of contributors for work out. The job of these electronic devices is to gather data in a wireless sensor network and pass the composed information to the network between the further linking nodes. The WSN is relevant for observe human body organs, ecological observe, heat and moisture controlling, motor vehicle travel controlling system etc. [1].

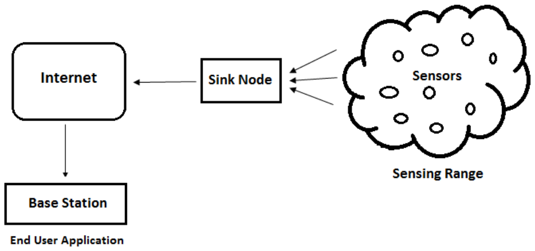

Figure 1: Wireless Sensor Networks

Figure 1: Illustrate the central state of wireless sensor network applications. A simple network is use to watch the type of an application such as human being body organ examine, hotness control or some other uses. During talk throughout the network, a case arises of breakdown which is resolve by using self-configuration and adjustment features of WSN [2].

WSN refers to a mixed system merged with small sensors with common principle computing fundamentals. This network has many self-managing, battery-power and inexpensive wireless nodes arrange to observe and change the environment. WSNs are strictly distinguished by restricted power equipment, short bandwidth, little memory sizes and partial energy. This directs to an extremely challenging atmosphere to offer defense [3].

II. SECURITY NECESSITIES

A WSN is a unique kind of network. It distributes several similarities with a classic computer network. It also demonstrates numerous characteristics which are only one of its kinds. The defense services in a WSN must defend the massage communicated above the network from the resources of attacks and misconduct of nodes [4].

The basic concepts of standard computer network are used for functioning of WSN. The Security necessities in WSN contain:

A. Confidentiality

Confidentiality means the defense procedure which makes sure the information distribute between sender and receiver is not spoken by anybody in the network. Data confidentiality is achieved in WSN with the assist of the following statements.

1) Information must be constrained inside the network.
2) Safe correlation for key organization.
3) Keys must be adaptable with respect to the covered attacks.

An illegal user in a network is not permitted to access data in a network.

B. Authenticity

Authenticity allows the receiver to maintain the originality of data which involves more than one proof of identity. It may be a in the form of password or a key known only the user.

C. Integrity

Integrity means faith the data resources. Data integrity means that the data is not changed by a mistake or any hateful action. Source integrity means information is only initiated form the reliable source. An unofficial user in a network is not permitted to alter the message being conveyed in a network.

D. Availability

Availability means to ensure that the data resource is available for legitimate user. It says data should be available always to the legal users throughout the network even if there are internal or external failures, faults, errors or attacks.

E. Non-repudiation

Non-repudiation means to make sure that the information convey has been sent and received by the persons declare to have sent and received the information.

F. Freshness

Data freshness promises that the data received throughout swap over is raw without any map out of recycle data. In WSN, the information cannot be conveying inside the particular time period, hence we should promise that it is fresh. To accomplish this, time squash are used. It includes two types like

- Weak freshness offers a small organize for the data therefore delay cannot be considered.
- Strong freshness offers a common organize and permits the computation of delays [5].

III. CRYPTOGRAPHIC TECHNIQUES

To keep away from attacks and to accomplish security of information in WSNs, generally cryptographic methods are used as an essential fraction of the WSNs protection design. Cryptographic techniques are mainly encryption methods used to encrypt our crucial data packets into some protected data packets of coded data terms that are being convey over the network in its place of straight original data packets broadcast shows in Fig. 2.

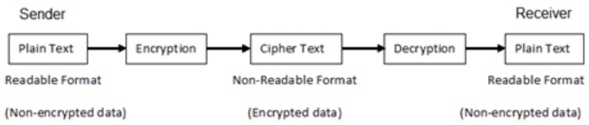

Figure 2: Cryptographic Technique

During communication encrypted data is mostly a set of some additional bits along with the data bits for protected the original data.

After examine the restriction and limits of sensor networks, it is obvious that these types of situations require trivial cryptography to get high level of protection. For a realistic safety solution, every sensor should have stability between costs, performance and safety level however it is extremely hard to get all three design objective at the identical time. It is obvious that in such situation, developers not give up the safety level by using commercial key solutions without any proper method for key distributions. Hence WSN needs additional flexible techniques for key distribution in the network, which is parallel to the methods used in usual preset networks.

Cryptographic methods are offered to gather the basic defense needs of confidentiality and integrity in networks. Mainly there are two cryptographic algorithms Symmetric Cryptography and Asymmetric Cryptography.

A. Symmetric Cryptography

This cryptography uses a single secret key for together encryption and decryption of the data packets in a converse network which is reserved as top secret in a network as given away in Fig. 3.

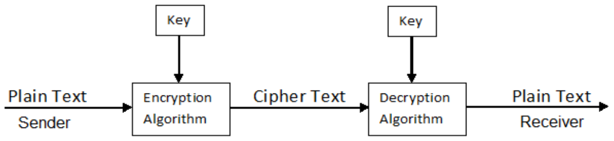

Figure 3: Symmetric Key Cryptography

In this, a single key is used for together functions encryption and decryption. For this secrete key encryption to job, two nodes contribute to same secret key which has to be confined from entrance by others. But the procedure for setting up of key in the network system is a significant matter to resolve by using simply symmetric key. The major challenge is in the case of broad dispersed area in WSN. The Common alteration of key is necessary in insecure area where possibility of attacker knowledge the key is high.

Think a small sensor network that has pair-wise and pre-loaded secret keys in the memory before the development stage. Every sensor node has a catalog of n keys, one for self and (n-1) for others in an n-node sensor network. After deployment stage, nodes can swap the secret keys used for encryption. The network manager can also physically update the keys at any time it is required. But the difficulty arises when new node is added and a new key is needed. Such method can be used for small network but are not useful for large networks.

Let's think KDC (Key Distribution Center) which distributes keys to the couple of nodes every time message has to be recognized. Each node would have to contribute to a single symmetric key through the KDC for the intention of key distribution and authentication. This can direct to amplify in the number of packets flow between nodes and KDC must be well confined and it furthermore requires preset infrastructure with reliable server. But this technique is not common for numerous sensor network deployments.

The above process shows how restricted is KDC in case of WSN. The WSN needs additional flexible techniques for key distribution. Subsequently, other technique is used.

Keeping the key secreted in the network is not easy task in the network.

B. Asymmetric Cryptography

This cryptography uses two keys as public and private keys for data encryption and decryption given away in Fig. 4.

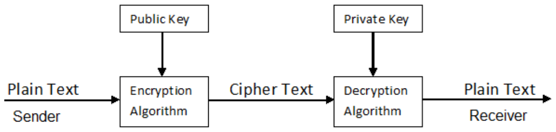

Figure 4: Asymmetric Key Cryptography

The keys are used as two behavior defense providers. Public key encrypt the information and private key decrypt the encrypted information. Private Key is simply given to the official users for accessing the information. A user can decrypt the information at the destination by match up to its public and private key with the sender's public and private key.

Public key methods are the substitute procedure used in put of symmetric keys. It makes simpler the key management and offers extra functionality that is not available in symmetric key methods. Public key cryptography is a broadly used method that safe the message together in private networks and crossways the public network similar to Internet.

Public key cryptography uses a couple of keys named as undisclosed private key and available public key. At this point, the key used for encryption is not identical as the key for decryption. This type of secure method is called asymmetric cryptography.

IV. RSA

The RSA is a technique to apply a public key cryptography whose safety based on the complexity of factoring big prime numbers. RSA means for Ron-Rivest, Adi-Shamir and Leonard-Adleman who are authors invented this technique. They firstly explained this algorithm in 1977 publicly. In this method, it is feasible to encrypt data and generate digital signatures. It is consequently successful. Frequently RSA public key algorithm is generally used in the world [6].

V. ECC

This technique is mostly depending on the algebraic construction of elliptic curves. The complexity in this method is the size of the elliptic curve. ECC stands for Elliptic Curve Cryptography. The main advantage of ECC is a minor key size, reducing storage space and transmission necessities. ECC could offer the same level of protection afforded by an RSA based system. In ECC, The elliptic curve is a plane curve which includes of the points satisfying the equation y2=x3+ax+b [7].

ECC is a verified tool that is used in a lot of different profitable products such as mobile phones, financial transactions, e-mails and several others. Cryptographic safety of systems is depends upon numerical complication. As protection increases, processor's effort at the similar time and act of the system also get better. If we match up to the safety level of ECC then it is lesser than of RSA.

The drawback of ECC is that the whole system is a much more complicated than the RSA scheme. The mathematics behind ECC are rather complex and a broad range of different parameters makes the implementation more difficult. However, small key sizes, relatively low computational requirements and high flexibility justify the choice of ECC as a public key cryptography technique.

A. TinyECC

TinyECC offers easier, configurable, flexible and ready-made software for increasing WSN based organizations with ECC at its center. All the ECC processes with point addition, point replication and point multiplications are maintained by TinyECC [8].

Match up to RSA, ECC has tiny key size, short memory usages etc. Thus it has concerned thought as a safety resolution for wireless sensor networks [9].

VI. DESIGN OF ASYMMETRICAL KEY CRYPTOGRAPHY

The public key cryptography is mostly used as design method as a safety and additional proficiently than symmetrical cryptography. As the fundamental rule of public key says that it includes of a couple of related and dissimilar keys:

- Public Key: Supply to any one publically
- Private Key: Given to valid user confidentially

These keys are correlated to each other but computationally dissimilar.

Asymmetric encryption utilizes two correlated keys (public key and private key) for information encryption and decryption. It takes away the safety risk of key distribution. The private key is never uncovered. An information that is encrypted by with the public key, can only be decrypted by using same method and corresponding private key as shown in Fig. 5. Examples are RSA, ECC etc.

Consequently, it is generally relevant in the network for message communication. Public key cryptography such as RSA or ECC methods is frequently working in WSN.

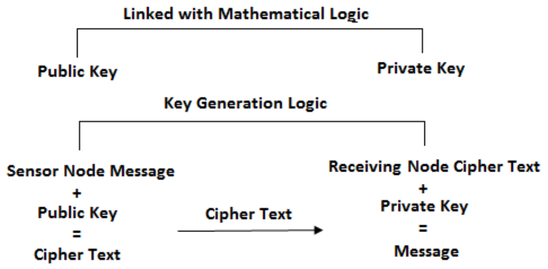

Figure 5: Design of Asymmetric key cryptography

A. General Rule

A simple rule of asymmetric key cryptography can be given by following.

1) Any recipient uses a method to calculate an encryption key and a decryption key.

2) Then the recipient publicizes encryption key to anyone, but the recipient keeps top secret the decryption key.

3) Sender sends a message to Recipient by encrypting the message using the publicized key (Encryption Key) for that receiver.

4) Since only Recipient knows how to decrypt the message by decryption key, therefore it's safe.

The Public Key Cryptography (PKC) is used currently for solving safety issues of WSN. Typically ECC, RSA, PKC are used along with key making methods either using fixed key creation or by using grouping key creation given that number of WSN applications doing well implementations.

The asymmetric cryptography is further capable in safety goals accomplishment as compared to symmetric cryptography. Public key cryptographic methods are initiated to eliminate the weakness of symmetric cryptographic methods.

VII. HYBRID CRYPTOGRAPHY

Symmetric key cryptography has a drawback of key distribution and asymmetric key cryptography needs a lot computation, therefore the power of the sensor is exhausted in it. It is not practicable to use as power is exhausted then sensor will be have no utilize. Hence the hybrid cryptography combines both the methods symmetric and asymmetric cryptography, therefore the benefits of both the methods can be operate in it.

Hybrid cryptography is a technique using various ciphers of dissimilar types collectively, each to its finest benefit. One ordinary method is to produce a arbitrary secret key for a symmetric cipher and then encrypt this key through an asymmetric cipher with the recipient's public key. Next the information itself is encrypted using the symmetric cipher and the secret key. Both the encrypted secret key and the encrypted information are then sent to the recipient. The recipient decrypts the secret key first using own private key and after that uses that key to decrypt the message. This is mostly used in some applications [3].

VII. CONCLUSION

The WSNs persist to raise and turn into broadly used in several applications. So the require for defense becomes dynamic. Conversely, the WSN suffers from a number of constraints such as restricted energy, processing capability and storage space ability. The Cryptography is one of the types for providing safety. Choose the proper cryptography technique for sensor nodes is essential to give safety services in WSNs. The hybrid cryptography is excellent appropriate for WSNs as compared to symmetric or asymmetric cryptography. This method is relatively well appropriate for small and medium WSNs because of its short energy consumptions.

REFERENCES

1. H. Dogra and J. Kohli, "Secure Data Transmission using Cryptography Techniques in Wireless Sensor Networks: A Survey", Indian Journal of Science and Technology, vol. 9, no. 47, pp. 1-5, 2016.
2. E. Shi and A. Perrig, "Designing secure sensor networks", Wireless communication magazine, vol. 11, no. 6, pp. 37-43, 2004.
3. M. Panda, "Security in Wireless Sensor Networks using Cryptographic Techniques", American Journal of Engineering Research (AJER), vol. 03, no. 01, pp. 50-56, 2014.
4. Y. Wang, G. Attebeery and B. Ramamurthy, "A Survey of security issues in Wireless Sensor Networks", IEEE Commynication Surveys and Tutorials, vol. 8, no. 2, pp. 02-23, 2006.
5. A. Faquih and K. Kadam, "Cryptographic Techniques for Wireless Sensor Network Security – A Survey", International Journal of Advanced Computational Engineering and Networking, vol. 3, no. 6, pp. 106-110, 2015.
6. R. L., Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.
7. K. Lauter, "The advantages of Elliptic Curve Cryptography for Wireless Security", IEEE Wireless Communications, vol. 3, pp. 22-25, 2004.
8. N. Saqib, and S. S. Shekhawat, "Securing Wireless Sensor Networks using Elliptical Curve Cryptography", International Journal of Engineering Trends and Technology (IJETT), vol. 56, no. 1, pp. 07-11, 2018.
9. Lokendra Singh, Deepika Pathak, "Optimization & Advancement of Application Specific Clustering Protocols in Wireless Sensor Networks (WSNs)," Journal of Innovative Engineering and Research, vol. 2, no. 1, pp. 24-25, 2019.