Wireless Sensor Network and Security Mechanism by Encryption

Shafiqul Abidin

Abstract—Due to rapid increase in wireless sensor network applications in today's time, WSN has become quite vulnerable. The node capture attack is the most crucial attack. In this attack, the attacker captures one or more node and tries to extract all the confidential information present in that node. The attacker is able to compromise an essential part of the WSN network. Presence of huge number of nodes and minimal hardware support creates complication in managing keys in WSN. The other issues present in the key management are energy constraints and limited memory. Therefore, there is a requirement of an optimal key management scheme which will be able to reduce node capture attack and uses energy efficiently. By simulating the previously recorded results we are able to see the techniques which effectively increases packet delivery ratio and uses less energy. The information that is to be transferred between two sensor nodes is extremely confidential and it needs to be secured. This can be achieved by cryptography. In cryptography, the data is encoded so that no external agency is able to interpret the message. There are lot of issues concerned with the security WSNs. The first one is Confidentiality. It ensures that the information should be transferred only between the sender and the receiver and no unauthorized entities could be able to access any information. The other issue is Integrity. It restricts any alteration of the message either accidently or maliciously while transmission. The next issue to be dealt with is Authentication. It means the key will be there only in the trusted nodes. When first node has delivered a message to the second node, the second node will give a confirmation reply if it has received the message. All the present nodes get the same key in the network.

Index Terms—Sensor Network, WSN, Cryptography, Authentication, Network Protocols, Quality-of-Service , QoS.

I. Introduction

There are four layers of WSN. The first one is *Physical layer*. This layer allows the interface to transmit stream of bits. Physical layer looks after signal detection, carrier frequency generation and frequency selection. Data link layer is the next layer. This layer is used for multiplexing data stream and also controls errors. It makes sure of reliability of point to point connection and can even be multipoint connection. Another layer is the Network Layer. This is the most important of all the layers of WSN [1]. This major function of this layer is routing. This layer faces a number of challenges depending on the applications. The foremost challenges are power saving and limited memories. The basic idea of the routing protocol is to determine reliable path and even the redundant paths according to a scale called metric.

It changes from protocol to protocol [2].Transport Layer is the next layer of WSN. This layer is used to provide reliability and congestion avoidance. The major function of this layer is to organize the system and control the other networks. Majority of the security protocols for WSN believe that the attacker is capable to achieve entire control over the node by direct physical access. Besides having lot of advantages , it is quite vulnerable to adversary. The foremost reason for the vulnerability of WSN is limited amount of energy present in sensors and the adverse environment in which they are deployed. The reason for blockage of the nodes in sensor can be due to depletion of the energy, communication link errors and physical damage. Due to distributed Wireless Technology, WSNs are being implemented in numerous applications. The Quality Of Service (QOS) of WSN has been reduced because of not providing proper security protocols [3]. Attack can be defined as the unauthorized access to another system without the permission. Wireless sensor network attacks can be divided into two broad categories as Active and Passive. Active attack majorly alters or modifies the data, therefore interrupting the functioning of the established network. Passive attack makes the adversary to discover information, eavesdrops on the traffic flowing across the network without altering the data. There are a variety of attacking techniques present in WSN which are namely, the Denial of service (Dos) attack on routing protocol, node takeovers. These are the attacks which tends to compromise the physical security of the node. The process of encrypting the data at the sender and decrypting it at the receiver is cryptography. Using cryptography, we can restrict the access of data by any external agency. Various techniques used in cryptography are Symmetric cryptography and Asymmetric Cryptography. In symmetric cryptography, the encryption as well as the decryption is performed by a single key. All the sensor nodes share a common key. This key should be kept secret in the environment which is a difficult task. It requires less energy and has high effectiveness. In Asymmetric Cryptography, two keys are used for data encryption and decryption. One key is public and the other key is private. The private key is always kept secretive. The message that has been encrypted

Manuscript revised June 5, 2019 and published on July 10, 2019
***Shafiqul Abidin**, HMR Institute of Technology & Management, Delhi, India,*

doi: 10.32622/ijrat.76201924

by the public key can be decrypted only by applying the same cryptographic technique with the help of matching private key. Hybrid cryptography is the combination of both symmetric and asymmetric cryptography[4]. It is used to overcome the disadvantages of symmetric and asymmetric cryptography. In symmetric key, there is a problem in the process of key distribution and in asymmetric algorithm, lot of energy is wasted. Hybrid cryptography uses multiple ciphers of different kinds. The best characteristics of each cipher is considered [5] . A random key is generated for the symmetric cipher to carry out the process of decryption and then this key is encrypted using asymmetric cipher.

II. Network Security

WSN comprised number of nodes. These nodes have limited functionalities and capabilities. Further, these nodes have low storage capacities and lack in communication y Of nodes are limited as they have very low storage capacities and controlled communication. Limitations in WSNs are also because of limited available energy to the nodes. In addition to this nodes are of small sized. Due to the limitations and constraints in WSNs, it is more complicated to optimize security mechanisms directly. There are various constraints of WSN. The first one is Energy constraint: This is the most crucial constraint present in the WSN as the bits in WSN require large amount of energy during the transmission of bits. The study[6] basically tells that energy consumed to transmit the bit during transmission is equivalent to 700-1000 instructions. Due to this, the cost of communication becomes more than the cost of computation. The energy constraints have been divided into three categories namely : energy for sensor transducer, energy for communication between sensors, energy for microprocessor computation. Next is Memory Limitations. Due to the extremely small size of the sensor, the memory present in the sensor is too less. The memories present in the nodes are the flash and the RAM [7].

Downloaded applications' codes are stored in flash memory equipped with the nodes. Whereas Random Access Memory (RAM) is used for storing application data. High Latency is another constraint [9]. In WSN, due to the presence of the multi hop routing, high processing time of node and network congestion leads to high latency. Hence due to this, sometimes it becomes difficult to achieve the synchronization. The next constraint is Unattended Operation. In majority of the cases, when the nodes are deployed in the remote area, they are left unattended. This makes them vulnerable to physical attacks in particular environment. Detection of physical tampering is quite difficult by managing remote WSN. Unreliable communication is another constraint to be dealt with. This constraint is a major threat to the sensor security. This constraint damages the packets by channel errors or by channel dropping. In this, routing is based on connectionless protocol which makes it unreliable[8]. Due to the presence of the broadcasting nature of the transmission medium wireless network becomes vulnerable to the attacks. The other reason for the vulnerability of the WSN is that nodes are not physically safe as due to their placement in hostile environment. The attacks on the WSN can be categorized into two parts: Attack against security mechanism and Attack against the basic mechanism. Dos: The other attacks on the WSN are Denial of service. In this particular type of attack, there is an unintentional failure of nodes. The simplest dos attacks majorly tries to overload the node by sending the useless packets and thus diminishing the node energy. The dos attacks can be further classified as the Sybil attack: In the Sybil attack, a single node presents multiple identities to the other nodes in the network. By using this attack, the attacker can be present at more than one location[9].The Sybil attack tries to degrade the data security and data integrity. This attack also targets the defect tolerant schemes namely multipath routing. The counter measures for the Sybil attack are Encryption of data and data Authentication. These techniques can help in eliminating the Sybil attack. Public key cryptography is also useful in removing this attack but its quite an expensive solution. Tampering: In this attack, again the physical layer is targeted. In this attack, the node is being captured and the sensitive information from the node is extracted such as the public and private keys of the nodes. Collision: This type of the attack is seen on the data link layer. In this, two nodes attempt to transmit on the same frequency simultaneously and due to which collision occurs. An attacker also try to cause the collision in specific packets. The countermeasure to avoid the collision is the error correcting codes. Hello flood attack: This attack can be called as the noval attack against the WSN. The attack uses the hello packets as their foremost weapon to get control of the WSN sensors. In this attack, the attacker tries to waste the node's energy to a large extent by the laptop class attacks and is able to create a routing delay. Jamming: In this type of the dos attack, the physical layer of the WSN is targeted. The jamming interferes with the radio frequencies and results into the interruption of the established connection[10].It can disrupt signal in two forms first if the source is powerful then it can interrupt the entire network or if the portion is small then it can only disrupt the part of the total established network.

Layer presents in the network connection in WSN is physical layer. The physical layer is the layer which is responsible for the frequency selection and is also known as the frequency generation, data encryption, modulation of information. The attacks which thus disturb the physical layer are the jamming. Network layer: The network layer is the layer which deals with the routing protocols. The threats seen in the network layer are Sybil , wormhole and selective forwarding. Counter measure of the Attacks in the network security are Selective forwarding. The counter measure taken to counter the attack is regular monitoring of the data using the source routing. This measure can be used by key management to secure the routing. Wormhole attack: The counter measure of the wormhole attack can be achieved by physical monitoring of the field devices and regular monitoring of the network. Using the source routing, monitoring system may use the leach packet technique. Sybil attack: The counter measure of this attack is that the device is

doi: 10.32622/ijrat.76201924

needed to be reset and the present session keys are to be changed. The measure can be taken by the help of cryptography as in that the nodes are been provided a globally shared key [11]. The Sybil attack thus can also be countered by using symmetric key with the trusted base station. Sink hole: This type of the attack is quite difficult to counter as in this attack the use of the advertised information is there as remaining energy[12]. The counter measure tends to work with the help of key management and secure routing.

A. *Cryptography in WSNs*

Selection of appropriate cryptography technique is essential and most basic step in order to overcome the security issues arising in WSN. Cryptography methods should be selected in such a way that they are able to overcome various constraints of sensor nodes such as processing time, power consumption and size of the data. In this section, public key cryptography and symmetric key cryptography have been discussed.

III. Public Key Cryptography

In Public Key Cryptography, all the nodes share the same key. Public key faces various security issues such as authentication and Robustness. In Robustness, if the secret of one node is compromised then the security of entire network is broken. To overcome this, we use Private Key cryptography [13]. The operation performed by the public key can be very fast. Public Key Cryptography can be applied in sensor nodes with the usage of correct parameters. The external agent and the base station comprises of adequate computational resources such as battery, CPU, memory, etc. Various applications of Public Key are RSA, ElGamal and Elliptic Curve. RSA is the most popular practical application of public key. It is used for secure transmission of data between the nodes. It is a type of an asymmetric cryptography algorithm. In asymmetric cryptography, there are two separate keys, one is public and the other one is private. The public key is shared by all the nodes and the private key is kept secret. Public key can be decrypted very easily so in RSA algorithm, the public key was made very large and it consisted of several prime numbers. Therefore, the one who has a good knowledge of prime numbers can only be able to decrypt the key. RSA is comparatively a slow algorithm. In most of the cases, the RSA passes the encrypted key for symmetric key cryptography which is able to perform complex encryption and decryption at a very high speed. In symmetric key cryptography, there is only one key for both encryption and decryption. RSA has the capability to perform both encryption and decryption within seconds. RSA provides vulnerability to Dos attacks. In Doss attack, extra packets are transferred and it prevents users from accessing various services. There are different types of Dos attack in different layers. Public key cryptography encounters higher chances of attack. One such attack is Sink Hole attack. In Sink Hole Attack, attacker will try to compromise the secret of any one node and make this node more attractive in the environment. Attacker gets all the traffic from a particular area through a compromised node creating a sink hole. The other important algorithm that is used in Public Key Cryptography is ECC. ECC algorithm reduces the communication and processing overhead by offering equal security using a smaller sized key. RSA comprising of 1024-bit keys provides same security as compared to ECC having 160 bit-keys[14]. WSN is administered using central point of every sensor possessing a certificate which is signed by the central point of private key using ECC or RSA signature. The results have proved that the ECC signatures are comparatively cheaper as compared to RSA signatures. The key exchange protocol based on ECC displays better results in comparison to key exchange protocol based on RSA at the server side whereas at the client side, there is not much difference in energy consumption. As there is an increase in the key size, the relative performance of ECC also increases over RSA. ECC and RSA cryptography implementation on Mica2 nodes gave a proof that protocols based on public key are very efficient. Further, one more scheme named TinyECC has also been implemented on Mica2. Malan et al also conducted various useful work on ECC cryptography using Mica2. In this, he distributed a symmetric key, for encryption of the link layer using TinySec module. Public key is preferred over private key in terms of the expense. The speed at which the public key performs operations can be increased by selecting small value of the integer such as e=2^16 + 1 whereas the operation speed of the private key cannot be increased[15].

IV. Symmetric key Cryptography in WSNs

In Symmetric Key Cryptography, a single key is used to perform the encryption and decryption. In this, a common key is shared by the two sensor nodes. The algorithms based on the symmetric key can be classified into two: Block Ciphers and Stream Ciphers. Block Ciphers are used to perform fixed number of transformations on the plain text. Stream Ciphers are used for performing the time varying transformations. The major security challenge that symmetric key faces is reliable exchange of symmetric key between the two sensor nodes. Symmetric key cryptography has higher operation speed in comparison to the Asymmetric key cryptography[12]. Symmetric key algorithms are also given more preference over public key methods because the security algorithms of symmetric key consume low power. It also provides better security services. Various Symmetric Key algorithms that are used in WSN are: CAST, AES, RC4, RC5, MD5, IDEA, SHA-1. The memory size and the execution time of each algorithm was recorded. Every architecture class and the encryption class had uniform cryptographic cost. The decision for selecting the suitable algorithm depends upon the communicational and computational capability of the nodes. There are certain disadvantages of symmetric key as well. The key distribution schemes used might not be perfect. There is a need to design effective distribution schemes. With the advancement in technology, more powerful nodes might be required to carry operations in the sensor nodes.

doi: 10.32622/ijrat.76201924

V. KEY MANAGEMENT PROTOCOLS

The key management is one of the keen areas of research in WSN and security. This is the core mechanism for providing secure, reliable services and applications of WSN. The aim of the key management is to ascertain keys among the nodes of sensor in reliable and secured manner. As the nodes of WSN have power constraints, so because of this the key management protocol for the network must be quite light weight[12]. Key management protocols in WSN are largely based on symmetric key cryptography. Generally, the public key cryptography techniques are computationally intensive.

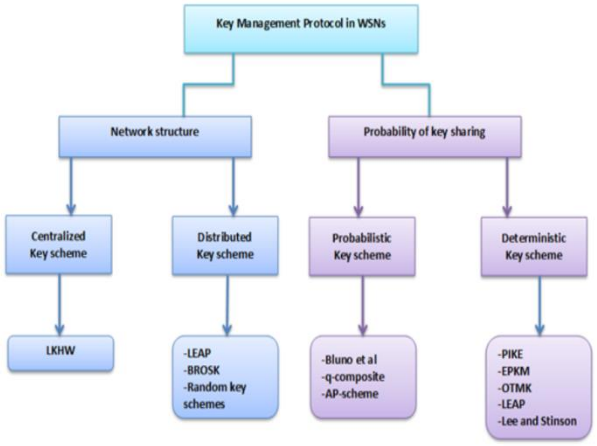

Fig.1.Key Management Protocols in WSNs.

Key Management based on Network Structure

A. Key Management Based on Network Structure

The key management protocol can be distributed or centralized depending upon the network structure thus been present in front. In the centralized key management there is only single entity which controls the distribution and generation of the keys. The particular entity is known as the key distribution center (KDC).[7] The LKHW is the only existing protocol that is based on the centralized key distribution. The foremost drawback of this scheme is that it's a single point failure scheme. If the central controller fails the entire security is compromised. The other issues related to this scheme is lack of scalability and it does not provide the data authentication. In contrast to the centralized key management, in the distributed key management protocol different controller manages different key related activities. The key management used in the literature are mostly distributed in nature.

B. Key Managementon Probability of Key Sharing

Another form of key management is the key probability. Depending on this probability the key management is further divided into two categories namely deterministic and probabilistic.

C. Deterministic Key Distribution Schemes

The authentication protocol proposed by Zhu et al[6] is a type of key management protocol for WSN based on symmetric key algorithm. The algorithm uses different key mechanism for individual packets depending upon the security need. There has been four types of keys established to determine for nodes which are: individual key shared with base station, group of key shared by all nodes present in the network, pair wise key shared with next neighbor node, cluster key shared with multiple neighbor nodes. The cluster key is been used for local broadcast and all the other are used for merely peer to peer communication. There's been an assumption that the time required to attack a node is greater than the network establishment time. In the above security measure all the nodes are equipped with an initial common key before the deployment. With the help of the common key been provided the nodes derive the master key. Thus after this, the nodes tend to exchange information as they have been authenticated by receiver. After the exchange of the information the common key are deleted and is been assumed that no node is been compromised.

A large number of key management protocols concerned with WSN are relied on distributed and probabilistic schemes. A random key pre-distribution scheme for the WSN are carried out by Eschaenauer and Gligor. The proposed mechanism contains three steps: key pre-distribution, shared key discovery and the path key establishment. In the key pre-distribution step, every sensor is been equipped with a ring key which is been stored in memory.

VI. CONCLUSION

The general use of the WSN is to gather the records from the insecure environment. The WSN represents a promising domain as they can be used in variety of applications, such as battle fields surveillance , patient health monitoring. The WSN has been able to enhance the productivity through increased accessibility. With the increase in the sensor techniques now a days, inexpensive WSN have been put in the applications. There has been a rapid increase in the applications of the WSN. The given example of these application are Area monitoring. It is the common application of the WSN. In this, the WSN is been deployed over a area where there is a certain phenomena to be checked. Physical life example of this is geo-fencing. Health Care Monitoring is another application. The medical applications of the WSN can be of the two types namely wearable and implanted. The wearable devices are the devices which are been used on the outer surface of the human body. The implanted devices are been used inside the human body. The another application is Air pollution monitoring. WSN have been used in several cities to monitor the amount of toxic gases present in the atmosphere. The cities which have deployed the WSN in this field are namely London, Brisbane. Data Logging is an important application of WSN. Wireless networks are also being used for the collection of the data to monitor the environmental information. The statistical information can then be used to see how the systems have been working. Environmental Sector is another technology based on WSN. WSN has several environmental applications. The WSN are being customized to monitor environmental parameters and the agricultural area. The major activities are designing and development of energy efficient wireless gateways. The development of remote monitoring system to check the status of the nodes and the sensor parameters. Intelligent Buildings(Bridges) is another application. Now a days as due

doi: 10.32622/ijrat.76201924

to the rapid increase of the WSN in our life we are thus able to build up the smart buildings. The WSN used in these buildings make them quite optimum for the environment as with the help of sensors we are able to reduce energy wastage by proper ventilation, air conditioning (HVAC) control [3].These types of the buildings are also capable of monitoring mechanical stress generated after earthquakes.

REFERENCES

[1] Shafiqul Abidin, Manu Ahuja and Mohd Izhar "Minimizing Risks in Wireless Sensor Network", IEEE International Conference on Electrical, Electronics, Computers, Communication, Mechanical and Computing – EECCMC- 18, November, 2018.

[2] R Muraleedharan and L. A. Osadciw, "Balancing the performance of a sensor network using an ant system," 2013.

[3] J. P. Walters, et al., "Wireless sensor network security: A survey," Security in distributed, grid, mobile, and pervasive computing, p. 367, 2007

[4] Antoine Bagula bagula@cs.uct.ac.za http://isat.cs.uct.ac.za

[5] Wood,A . D., & Stankovic, J. A.(2002). Denial of Service in sensor networks.IEEE Computer,35(10),54-62

[6] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D.E. Culler, and K. Pister, "System architecture directions for networked sensors", In Proceedings of the 9th International Conference on Architectural Support for Programming Languages and Operating Systems, New York, ACM Press, 2000, pp. 93-104.

[7] 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 Communications Security, pp. 62-72, New York, NY, USA, 2003, ACM Press.

[8] R. Di Pietro, L.V. Mancini, Y.W. Law, S. Etalle, and P. Havinga, "LKHW: A directed diffusion-based secure multi-cast scheme for wireless sensor networks", In Proceedings of the 32nd International Conference on Parallel Processing Workshops (ICPPW'03), IEEE Computer Society Press, 2003, pp. 397- 406.

[9] Shafiqul Abidin and Mohd Izhar "Attacks on Wireless and its Limitations" International Journal of Computer Science and Engineering, Vol 5, Issue 11, pp 157-160, November 2017.

[10] Perrig, A., Szewczyk,R., Wen, V., Culler,D., & Tygar,J. D.(2002).SPINS:Security Protocols for sensor networks.Wireless Networks,8(5),521-534.

[11] *Shish Ahmad, Mohd. Rizwan beg, Qaman Abhas, "Energy Efficient* Sensor Network Security Using Stream Cipher Mode of Operation.", International Conf. on ICCCT'10.

[12] Vrugunti Chandra Sekhar, Mrudula Sarvabhatla,"Security In Wireless Sensor Networks With Public Key Techniques",ICCCI-2012.

[13] Soufiene Ben Othman, Abdelbasset Trad, Habib Youssef,"Performance Evaluation Of Encryption Algorithm For Wireless Sensor Networks",International Conference on Information Technology ande-services,2012.

[14] Jaydip Sen,"A Survey on Wireless Sensor Network Security", IJCNIS, August 2009.

[15] Madhumita Panda,"Security in Wireless Sensor Networks using Cryptographic Techniques",American Journal of Engineering Research,2016.

AUTHOR PROFILE

Dr. Shafiqul Abidin has accomplished M Tech (IT) and Ph D (IT) and presently associated as Professor & Head – Department of Information Technology, HMR Institute of Technology & Management (Affiliated with Guru Gobind Singh Indraprastha University), Delhi, India. He has published many research papers in national / international journals of repute and conferences. Dr. Abidin has visited various countries for teaching and research purpose in their institutions for a period of more than five years.

doi: 10.32622/ijrat.76201924