International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 04, 2020
ISSN: 1475-7192

SECURITY PERSPECTIVE ON WIRELESS SENSOR NETWORKS- A REVIEW

[1]V. Gowsalya, [2]K. Mahalakshmi, [3]R. Senthil Kumaran

Abstract *Wireless Sensor Network is a scheme contemplated to get intense information to build the information and communication system which leads to a remarkable improvement in the reliability and efficiency of the system. Wireless sensor network includes great benefits for their low cost, smart sensors and small scale factors. It can be found in a variety of both civilian and military applications worldwide. Sensor networks are rising as an attractive technology with great promise for the future. The challenges in wireless sensor networks include energy consumption, bandwidth demand, storage, power, memory, components, lifetime and security. Security is one of the most significant parts in wireless sensor network. The security services involved in WSN should protect the information transferred over the network, it also detects the misbehavior of nodes and protects the node from attacks. Security involves various schemes such as authentication, integrity, overhead and key management. This paper reveals the issues and challenges related to security in wireless sensor networks. The overview of security threats and the security mechanisms for wireless sensor networks are analyzed.*

Index Terms— *Sensors; Network Security; Challenges; Threats and attacks.*

I. INTRODUCTION

Wireless sensor network is a wireless network consists of base stations and nodes. The physical conditions can be detected and monitored. It passes the data through the network to a main location and it organizes the collected data to a central location. WSN can be defined as a network of devices that can view the information which was gathered from a monitored field through wireless link. The data is forwarded through multiple nodes and with a gateway the data is further connected to other networks. The more modern wireless sensor networks are bi-directional and it also enabling the control of sensor activity. The

[1] V. Gowsalya who is pursuing Bachelor degree in Electronics and Communication Engineering at IFET College of engineering, Villupuram. E-mail:gowsalyav9@gmail.com

[2] K. Mahalakshmi who is pursuing Bachelor degree in Electronics and Eommunication Engineering at IFET College of engineering, Villupuram. E-mail:mahabari1999@gmail.com

[3] Dr. R. Senthil Kumaran, Associate professor in Electronics and Communication engineering at IFET College of engineering, Villupuram. E-mail:sen19841@gmail.com

Received: 03 Dec 2019 | Revised: 21 Jan 2020 | Accepted: 18 Feb 2020

basic components of wireless sensor networks are sensors, processors, transceivers and power unit. It also has additional components such as location finding system, power generator and mobilizing unit. Various security schemes are involved in wireless sensor networks. There are different methods such as secure routing mechanisms, secure broadcast mechanisms which were discussed in this paper. It is the process of ensuring the security on wireless sensor networks. Because of the absence of central authority and the random development of nodes in a network, the security threats in wireless sensor network occurs. WSN security is a big concern to detect the intrusion and it should apply the mitigation method. These issues have been overcome by various techniques as such discussed in this paper with the help of security. Due to the deployment nature and the resources limitations of tiny sensor devices used in sensor network, the security is a crucial one. Security is the prevention of unauthorized access in the node. It is significant to prevent the node from the attack, hence the security planning is very much needed in WSN and it needs to focus on the threats which create the greatest risk. There are two major security issues such as privacy preserving and node authentication. The privacy preserving is to maintain the confidentiality of data under security mechanisms and the node authentication which does not allow the unauthorized node to access in a network. The main characteristics of security include authentication, data integrity privacy, non-repudiation, data secrecy.

II. SECURTIY TECHNIQUES IN WSN

A. Symmetric Key Based Scheme

It is a type of encryption scheme. The messages can be encrypted and decrypted by using this scheme and it has a significant scope to provide secret communication. The symmetric key in the sense, it uses the same key for both encrypt and decrypt the data. The major issue in this scheme is the key exchange problem. It is the old and popular technique for encryption. There are various symmetric key based schemes which provide secure and efficient communication. In order to develop the data security in computer systems, the symmetric keys are majorly used. There are two common symmetric encryption based schemes which are block ciphers and stream ciphers. Block ciphers group data into blocks of certain size and each block is encrypted using the corresponding key. Stream ciphers do not encrypt plain text data by block but rather by 1 bit increments.

B. Aggregate Signature Scheme

An aggregate signature scheme is one of the schemes used in security. It is a digital signature which supports aggregation in which all the signatures are aggregated into a single short signature. It is used for data integrity and it gives rise to verifiable encrypted signatures. The scheme is useful for reducing the size of certificate chains and also for reducing the message size. The data aggregation methods provide a secure and efficient data. Identity based aggregation schemes are the advanced method of aggregate signature scheme, it allows the verifiable user to access the data and also it allows the designated user to compress the data.

C. Time Stamp Based Authentication

It is a password authentication schemes which allows the client to log into the server and it identifies the user activity of authentication. It is the process which is done by a correct password of the user to the server. It is the secure and the improved version of protocol. The time stamp based protocols are the secure authentication based protocols, most of the security attacks which can be protected or avoided by using this type of authentication schemes. It is one of the popular validate method involved to provide security in wireless sensor networks.

D. Weighing method, Artificial neural network and Swarm intelligence

In weightings method, every node is highly trusted at initial stage and the weight of the node is assumed as one. The information provided by each sensor nodes can be calculated. In artificial neural network, the trust value based on both present and past history of the node. It involves learning process, interconnection pattern and the activation function. The swarm intelligence is the method which provides the spatial arrangement and the synchronization motion of the individuals. These three methods are the types used in bio-inspiration based security mechanisms.

E. Message Authentication Code

A message authentication code is a short piece of information used to authenticate a code. Message's data integrity as well as authenticity is protected by MAC value. Message authentication code is use for data integrity. This security can break the cipher by attacking. It is used to detect both accidental and intentional modification of data by using a cryptographic checksum. The inputs required are a message and a secret key. The four types of MAC include unconditionally secure, Hash function based, Stream cipher based, Block cipher based. A secret key in conjunction with a cryptography hash function became widely used for security.

III. LITERATURE SURVEY

A. Hybrid Security Mechanism for Intrusion Detection

The intrusion detection is a mechanism to detect the existence of unsuitable or unusual moving attackers. The fundamental issues to characterize WSN parameters are node density and sensing range. In WSN, the detecting and tracking of moving objects are the major classes of application. The symmetric key based scheme [3] which includes different number of protocols for authentication and session key establishment. These protocols require a large number of transmissions. In order to achieve the goals of data secrecy and integrity the symmetric key methods with the public key infrastructure [2] schemes have been proposed. The unbalanced distribution of keys used to open up the existence of sensor nodes with equal level of security and the reduction of consequence of node compromise. The probability that two node share q key is given by,

$$1 - \sum_{i=0}^{q-1} p(i) \qquad (1)$$

To characterize the effects of unbalanced key management system the establishment protocol known as WIGER was implemented. The LION protocol as infrastructure less environment network and TIGER as the scheme relying on presence of KDC. WIGER is the combination of both the protocols .The advantage of WIGER that allows sensor network to operate in a secure and efficient manner of the resources. The emerging work in elliptic curve cryptography [1] includes various key distribution schemes. In this paper, the heterogeneity in sensor network was leveraged to provide mechanism for secure communication. The probability unbalanced key distribution method includes WIGER protocol which is suitable for the dynamic environment and has the benefit of all available security resources.

Received: 03 Dec 2019 | Revised: 21 Jan 2020 | Accepted: 18 Feb 2020

B. Securable Identity based Encryption technique by generating key in Wireless sensor network

In the field of WSN research, the managing of secure and efficient big data aggregation methods are very interesting. The existing method is aggregate signature scheme. It only focuses on data integrity protection. It does not provide a designated verifier for wireless sensor networks. To overcome this drawback, the Identity based aggregate signature scheme was proposed. It not only keep data integrity it also reduces transmission and storage cost for WSN and it generates the key with designated verifier. The privacy preserving scheme [5] is one of the encryption scheme which generates the key to access the node in wireless sensor networks. The ID generation is based on the node details. Nodes are storing the details and the server will check the node details. After checking, server generates the ID for the node. Node login is based on the server which generates the ID. The user authentication will store the node details and generate the ID for the user. The smart grid management [6] includes the tree based authentication schemes. In ID aggregation method if the user wants to download the file, the server will verify the user and provide key to the authenticated user. After receiving the file, it decrypts the file. Data centre store the user sending files and retrieve the user requested file. The data centre is based on user. It also provides the encryption technique for mobile cloud networks [4]. The ID based aggregate signature schemes have been proposed to compress many signatures generated by sensor node into a short one and also generating the key for providing security to the user information. Hence it is proved that our proposed scheme is secure and resists coalition attacks. The signature is valid if every single signature used in the aggregation is valid.

C. Secure and Efficient Data Transmission

In WSN, the secure communication is needed. In wireless sensor networks the secure data transmission is a critical issue. The SET-IBS and SET-DTA protocol involves with respect to the security requirements and security analysis against various attacks. The existing method include various cluster based protocols, these cluster based protocols only have limited scope to provide security against high level security attacks. To overcome this drawback the SET-DTA and SET-IBS schemes were proposed. Most of the security attacks can be protected or avoided by time-based authentication schemes. The proposed security protocol SET-DTA into two processes as the authentication process and session establishment process. It also includes various aggregates for monitoring the sensor networks [7].The data transmission protocols for WSN, including cluster based protocol. It is vulnerable to security attacks. The data transmission and data aggregation depend on the cluster head which causes serious damage to the network, if attacker manage to compromise the cluster head, it cause damage and hence disrupts the network. The SET-DTA is proposed to reduce the computational overhead in SET-IBS with data scheme. SET-DTA scheme in which the secret key for user, the equation is given by,

$$\beta = \alpha^{x} \bmod p \qquad (2)$$

where,

α and p are public keys;

x is the secret key;

$$\alpha^{x} = \beta \bmod p \qquad (3)$$

The proposed scheme is very much focus against high level security attacks like node capture attack and the security issues [8] can be analysed. The paper presents a secure data transmission for cluster based WSN. The similar method includes

the chaotic encryption [9] which provides the security gateway. The proposed SET-IBS and SET-DTA protocols have better performance than existing secure protocols for CWSN which achieves security requirements and to overcome the problem in the existing secure transmission.

D. Novel approach for Security in Wireless sensor network using Bio-inspirations

The Biologically inspired approaches involved in the security of wireless sensor networks which is one of the interesting field to evaluate because of the relation between the security and the survival of human body under pathogenic attacks. The biologically inspired approach in which the taxonomy can be analysed [10]. The weightings method, in which every node is highly trusted at first stage and the weight of each node is unity. The information provided by each sensor nodes can be calculated. The equation for weightings method is given by,

$$E = \sum_{i=1}^{N} W_n * U_n \qquad (4)$$

Where,

U_n is the data from sensor nodes;

E is the aggregation result;

W_n is the weight;

In artificial neural network, based on both present and past history of node the trust value is involved. It includes three aspects such as learning process, interconnection pattern and the activation function. The swarm intelligence is the method provides the spatial arrangement and the synchronization motion of the individuals. These three methods are the types used in bio-inspiration based security mechanisms. The proposed work includes the machine learning. It is based on biologically inspired security model which can be divided into machine learning module and immune module. There is a trust in wireless sensor networks using bio inspired technologies [11]. The detection of fraudulent nodes can be done by Support vector machine and Anomaly detection engine. The removal of fraudulent node can be done by immune model. Machine learning is one of the intrusion detection systems which check the network traffic and the identification of attack. K-means is one of the methods which are the unsupervised machine learning method works on the principle of finding a structure of unlabelled data. Support vector machine method is used to classify the data and make a decision boundary between the fault and good data. The Anomaly detection engine is used for the boundary values between the two regions which is the output of SVM. The equation involved in anomaly detection engine is given by,

$$p(x) = \prod_{j=1}^{n} p(x_j, \mu_{j,\sigma_j^2}) \qquad (5)$$

where,

μ is the mean value;

σ is the standard deviation;

p(x) is the probability distribution;

The Artificial immune systems [12] have intelligent capabilities of detecting antigens. The paper described the human immune system focus on the adaptive immune system consists of T-cells and B-cells. The aim is to derive inspiration from these cells to design a security system for next generation in WSN.

E. Security to Wireless Sensor Network against Malicious attach using Hamming residue method

Wireless Sensor Network consists of small sensor nodes with limited energy and these nodes have the ability to monitor the physical conditions and it's communicating the information among the nodes. WSN are autonomous hence without the requirement of physical medium it communicate the information through the nodes. Wireless Sensor Network is proves to security threads due to the absence of central authority and random deployment of node in the network. The malicious attack is one of well known attach which imitates one modes then misleading other nodes. To overcome these attach, the methods are involved either by cryptographic approaches [13] or by time synchronizing but its fails of the autonomous structure. To mitigate the malicious attacks on efficient approach called Hamming residue methods [13-15] are used. The method used to reduce the complexity and eliminates the key distribution among the nodes. This simple techniques enhances the security of network against malicious attach and it's improve the efficiency of network. By reducing the complexity, the Hamming residue method is proposed and a codeword is generated by use of initial security bits (user choice) and security check bits (hamming bits) are initialized. After this, using IPV6 the HRM information is stored in header and if code matches with code generated intermediate node, then it can access the data. The Hamming code can be used depending on codeword length "n" and number of initial security bit "k", (n, k).

$$W=W_1 \ldots . W_2 \ldots . W_3 \ldots . W_n \quad (6)$$

$$W=S_1 \ldots . S_2 \ldots . S_3 \ldots . S_n \quad SC_1 \ldots . SC_2 \ldots . SC_3 \ldots . SC_p \quad (7)$$

where,

SC-Security checks bits.

$$SC = S \times SP_m \quad (8)$$

The presented approach can reduce the mathematical complexity which in turn increases the PDR by minimizing the delay. PDR (Packet Delivery Ratio)[15] is ratio of number of received packets to the transmitted packets. At each node, the new security code word is generated which enhances confidentially among the nodes and can easily detect the rival node in network. The Hamming residue techniques should improves the security of wireless sensor network and is simple but effective.

F. WSN and GSM based home security system

A remote home security system [16, 19] is designed by combining the advantages of Wireless Sensor Network and GSM [17] technology is presented. It can detect intrusion, fire, etc… and inform the user remotely about the incidence with the development of IT technology, network and automatic control technology. WSN having the advantages of wide covering area, reasonable cost, fast monitoring, etc… While GSM has the advantages of mature technology, wide covering area, long distance communication, etc… By combining the advantages of WSN and GSM the remote home security is presented. Firstly, once some dangerous instance are happens in home such as fire, thief wherever the user are this system can call and sent SMS to use through GSM network. GSM can increase the reliability in term of user being informed about the intrusion immediately. Secondly, the WSN has established the feature without use of cable and it consumes low power. The system structure is composed of base station /gateway, a control panel, a dialer, several sensor node and mobile phones. The sensor node is placed

in different zones of house. These sensors can detect the intrusion or abnormal condition and it can send the information to base station. The GSM [17] modules can send the SMS containing intrusion log to the user otherwise it start calling. By using control, user configures all the user configurable operation. Instead of calling once, our system does the same three times for increasing reliability. Without the knowledge of owner, the secret code cannot be tampered. The system should also include the software design for WSN node, dialer and control panel. It also includes two modules, base station and sensor node. The former is responsible for wirelessly collecting sensor data and send it to the dialer. In dialer, it receives the abnormal data from base station through one of its port. GSM module SIM300 [19] used for calling and number stored in its EEPROM. Along with vice call, it also sends message containing information about intrusion to the owner. Control panel is user interaction part of the system. Its wait for user input and any control character received from dialer. The hardware includes radio transceiver XBEE, SIM300 GSM module, etc… The software is developed in C language on CVAVR. With the advantages of reliability, low cost, low power consumption. The combination of WSN and GSM can be also used in other practical application.

G. Secure data aggregation for wireless sensor network using double cluster head approach

In Wireless Sensor Network, data aggregation [20] is defined as method of acquiring sensed data from neighbouring nodes and merged to send data to base station. Double cluster head based secure aggregation [22] method is proposed which is more suitable for cluster based communication with security. Communication overhead is greatly reduced in the proposed model while deploying more number of nodes. The clustering mechanism is required to minimize the complexity in the communication process and its needed base station to deploy every cluster and is called cell splitting. Reduction of cell size will give more flexibility. To achieve the maximum efficiency of network, a double cluster head based data aggregation method is proposed. Double cluster head aggregation [20-23] approach consider the two nodes as cluster head and co-cluster head by taking various factors into consideration like minimum distance, residual energy and nodes lifetime. The total duration of session of aggregation is identified based on buffer capacity of sensor nodes and reading capability. The residual energy and node degree should be given as,

$$R_e = I_e - (T_e + X_e) \quad (9)$$

where,

I - Initial energy of the node at the starting point

T - Transmission of data

X- Reception of data

$$\text{Node-degree} = N\_Deg/\pi \times \delta \quad (10)$$

where,

δ – Communication range

The proposed system constructed with two cluster heads, main cluster and to co-cluster head and it's provides considerable security. The aggregation techniques can also improve the lifetime of the network.

H. Security and timing analysis of hybrid algorithm for Zigbee in Wireless sensor network

The Wireless sensor interacts with sensitive data and it may operates in against condition, hence security of this network gain higher importance. AES and ECC algorithm [25] from symmetric cryptographic technique are respectively chosen for providing security. By applying ECC and AES algorithm serially, the security of WSN is enhanced. The encryption of ECC and

AES is done by Zigbee [24]. A WSN consists of several of sensor node that gathers data from remote sensor locations, processes data and communicate through data signals. The necessity of security for Wireless Sensor Network includes limited power resources, small memory size and deployed in remote area. Security algorithm are used depends on computational time, key size, power requirement. A Zigbee provides security transmission of data in WSN. It requires low power & low cost. It is built over IEEE 802.15.4 standard. For scanning the channel, it uses Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA) Protocol. Zigbee used Advanced Encryption Standard (AES) [26] algorithm for encryption of plain text before sending over channel. It was using 128 bit key size. The security of Zigbee can be increased by incorporated ECC and AES algorithm. In this system, 8 bit input data from temperature, humidity and smoke is applied to ECC algorithm which encryption it with 16 bit shared key. This cipher text is again encrypted with 128 bit key from AES [26] algorithm of Zigbee and transmitted through wireless channel. The one type of symmetric algorithm used for providing security in Zigbee is AES (Advanced Encryption Standard). The encryption should follows byte substitution, rows shifting, column mixing, add round key. For decryption above operation are performed in reverse order. The one of asymmetric technique used is ECC (Elliptic Curve Cryptography). The discrete logarithm problem for ECC is given as

$$Q = x \times P \tag{11}$$

where,

P- Fixed prime elliptical

x -Number of times P added to it

The encryption and decryption of ECC is given as,

$$PA = nA \times G$$

$$= Pm + nA(nB \times G) - (nA \times G)\, nB$$

$$PA = Pm \tag{12}$$

The security has been enhanced by combining ECC & AES algorithm of Zigbee [24-26] will increase the encryption and decryption time. Also timing requirement for each algorithm is evaluated by mixing AES algorithm with ECC algorithm will increase the security of Zigbee.

IV. CONCLUSION

WSN has the wide range of applications. It is to be considered as one of the most effective solution in remote areas. In this paper, a review is done on WSN technology. WSN is an assurance for technology and is used in huge application. It consists of many futuristic applications for both the public and military. Security in WSN is one of the major research issues. This paper reviews about the various prospects such as key management, authentication and secure routing protocols to improve the security of the network. The research in this part is still large in future and the applications are very broad. This paper gives a clear view of improving the security by enhancing the WSN techniques. A secure communication scheme must restrict the damages caused by the intruders. Hence security is one of the most significant challenges involved in the wireless communication network.

REFERENCES

[1] A. Liu and P. Ning, "TinyECC: Elliptic Curve Cryptography for Sensor Networks'' (Version0.1) 2005.

[2] D. Malan, M. Welsh, and M. Smith, "A Public-Key Infrastructure for Key Distribution in Tiny OS Based on Elliptic Curve Cryptography, *Proc .IEE Int'l Conf. Sensor And Ad Hoc Comm.And Networks*, 2004.

[3] L.Eschenauer and V.Gligor,"A Key Management Scheme for Distributed Sensor Networks," *Proc.ACM Conf. Computer and Comm. Security (CCS'02),* Nov. 2002.

[4] H. Li, D. Liu, Y. Dai, and T. Luan" Engineering Searchable Encryption of Mobile Cloud N/W When QoE Meets QoP," 2015.

[5] H. Li, X. Lin, H. Yang, X. Liang, R. Lu, and X. Shen, "EPPDR: An Efficient Privacy-Preserving Demand Response Scheme with Adaptive Key Evolution in Smart Grid, "2014

[6] H. Li, R. Lu, L. Zhou, B. Yang, X. Shen, "An Efficient Merkle Tree Based Authentication Scheme for Smart Grid," 2014

[7] J. Zhao, R. Govindan, and D. Estrin,"Computing aggregates for monitoring sensor Networks," *in Proc. 2nd Int. Workshop Sensor Network Protocol* Appl., 2003, pp. 139–158.

[8] Modares, Hero; Salleh, Rosli; Moravejosharieh, Amirhossein;, "Overview of Security Issues in WSNs," Computational Intelligence, Modelling and Simulation (CIMSiM), *2011 the International Conference on*, vol., no.,pp.308-311, 20- 22 Sept. 2011.

[9] Wang Hai-Chun; Huang Tao;"Design of Security Gateway Based on Chaotic Encryption,"Internet Technology and Applications (iTAP), *2011 International Conference on* vol. no, pp.1-4,16 , 18 Aug.2011.

[10] Meisel, Michael, Vasileios Pappas, and Lixia Zhang, "A tax of biologically inspired research in computer networking*", Elsevier Computer Networks Journal*, vol. 54, no. 6, pp. 901-916, 2009.

[11] Gomez Marmol, Felix, and Gregorio Martnez Perez "Providing trust in wireless sensor Networks using a bio-inspired technique." *Telecommunication systems*, vol. 46, no. 2, pp. 163-180, 2011.

[12] Julie Green smith, Amanda Whit brook and Uwe Michelin, "Artificial Immune Systems", Book on Handbook of Metahewistic, 2010.

[13] S.J. Ahmad, V.S.K. Reddy, Damodaram, P.Radha Krishna,
"A dynamic priority scheduling Scheme for multimedia streaming over MANETs to improve QoS''*Int Conf Distributed Computer Internet* Tech., 122–126 (2016).

[14] W. Zhang, S. Zhu, G. Cao, " Pre-distribution and local collaboration- based group rekeying for wireless sensor net works''. Ad Hoc Netw. 7 (6), 1229–1242 (2009).

[15] S. Guo, Z. Qian,,"A compromise-resilient pair- wise Re-keying protocol in hierarchical wireless Sensor networks'. *Comput Syst.Sci.Eng.* 25(6),397–405(2010).

[16] Huang, H., Xiao, S. Meng, X., and Xiong, Y. "A Remote Home Security System Based on Wireless Sensor Network

and GSM Technology' *Proceedings of Second International Conference on Networks Security Wireless Communications and Trusted Computing,* 2010.

[17] Qiao Qu, Zhao Guohao, Wei Baohua, "Design of Home Safeguard System Based on GSM Techniques", *Electronic Engineer*, vol.32,No.11, pp.76-78, Nov.2006.

[18] Li Wenzhong, Duan Chauyo, C80517 , "Series MCU and Short Distance Wireless Data Communication'', *Beijing, Beijing University of Aeronautic & Astronautics Press*, 2007, pp.188 -190

[19] Wu Chengdong, Zheng Jugang, Liu Daren,Xi Kun "Study on Smart Home Network Technology Based on Wireless Sensor Network", *Academic Journal of Shenyang Jiahzhu University*, Vol. 21, No. 6, pp.753756, Nov.2005