IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-4, April 2019 E-ISSN: 2347-2693

A Review Paper on Various Attacks on Wireless Sensor Networks

M. Dahiya[1*], A.Sangwan[2]

[1,2]Department of ECE, University Institute of Engineering and Technology (U.I.E.T), MDU, Rohtak, India

[*]*Corresponding Author: mansidahiya121295@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v7i4.2935 | Available online at: www.ijcseonline.org

Accepted: 07/Apr/2019, Published: 30/Apr/2019

Abstract –As we know wireless sensor network have many advantages such as its high speed and high quality which increase its use in modern time. As so the security in wireless sensor network became the most important factor. There are many security issues but the most important is "eavesdropping". Eavesdropping is a type of attack in which the information being transmitted is attained or captured by some other devices. It is not possible to tell if a system had faced some kind of eavesdropping or not. In this paper various advantages and disadvantages will be discussed. There will be some application of WSNS and some introduction of eavesdropping issue with some techniques to detect this issue. We will also see various other attacks which leads to effect the security of wireless sensor networks. This paper will help in improving security in wireless sensor networks. This paper will further help in improving accuracy of wireless sensor networks. This paper will also light up various advantages and disadvantage of the technique which is being used for improving the security of wireless sensor networks.

***Keywords*:-** Wireless sensor networks (WSNS), eavesdropping and security enhancement.

I. INTRODUCTION

1.1 WIRELESS NETWORK

A network which contains nodes is connected through a wireless connection is termed as wireless network. No cables or wires are required for any kind of connection. some of the examples of wireless network are Wi-Fi networks or WLAN, satellite communication network, terrestrial microwave network and wireless sensor network. WSNS are arranged in large scale sensing environment which sense the signal at regular intervals and transfer the data into digital signal and pass on to the base node.

1.2 TYPES OF WIRELESS NETWORKS

- Wireless Local Area Etwork (WLAN):

a network which connects minimum two devices having wireless techniques to access internet using PDA.PROTABLE PC AND WLAN in some restricted hotspots. It provides high speed in small areas because of radio waves being used.

- Wireless Matropolitan Area Network (WMAN):

a network which allow to use internet services using WLAN. It provides high data rate with brad range

- Wirless Wide Area Network (WWAN):

in this internet service is accessed by sing WWAN access card or laptop. It provides high data rate and range is additionally boarded.

- Wireless Personal Area Network (WPAN):

a network which allow limited capacity of users. It provides high speed with respect to range restricted.

1.3 WIRELSS SENSOR NETWORK

As discussed above WSN are those network which have sensor nodes which sense the signal present in nearby environment and transform it into digital form and pass it to base node.

TYPES OF WSN:-

a) **Homogeneous network:-**

in this single network topology is used. In other terms we can say WSN which have same hardware complexity and battery energy are termed homogeneous network. It is not complex network.

b) **Heterogeneous network:-**

it is complex network as it required various topologies. in other words we can say that different functions and battery energy are being used by two or more nodes.

1.4 ADVANTAGES OF WIRELESS SENSOR NETWORKS

There are some advantages of wireless sensor networks such as :-

1) **FLEXIBILITY**:-

WSNs can be accessible from anywhere. It also enables to connect remotely after being away from a building. It also provide flexibility in case of ad hoc environment

2) **LESS EXPENSIVE:-**

The WSNs is less expensive as it do not require any wires or cables for connection and it also requires less maintenance.

3) **VOIP FACILITY:-**

It provides VOICE OVER INTERNET PROTOCOL service.

4) **SCALABILITY:-**

Any new user connection is easy to make.

5) **EASY SETUP:-**

Network could be setup without fixed infrasturure.

1.5 DISADVANTAGES OF WIRELESS SENSOR NETWORKS

- **Security issues:-**

WSNs has less security. It includes the risk of eavesdropping and so use encryption techniques.

- **RELIABILITY:-**

WSNs can be easily affected by environment and so, the signal interference is high.

- **LESS SPEED:-**

WSNs is slow in nature and so it provides less speed in busy networks.

II. TYPES OF ATTACKS

- **SYBIL ATTACKS**:-

It is a vulnerable attack.in this attack a node is connected to another node with different identical legal nodes. So, multi identities can be represent by a single node. Integration of data security of data and resource utilizationare the main terms which are disturbed. There are some mechanisms such as authentication and encryption which can help from Sybil attacks.

- **WORMHOLE ATTACKS**:-

in such kind of attack an attacker used to store some packets on to some location and then transfer them to some another place.this type of attack have significant risk on wsn because these attacks do not require any kind of compromising with respect to sensor or any other network.

- **DENIAL OF SERVICE ATTACK(DOS)**:-

this type of attacks mainly disrupt wireless transmission and at the receiver side these types of attacks re identified as noise or collision. network infrastructure, server application and network access are some targets where the attackers used to reach. This attack not only disturbed or destroy the network but it also diminishes the capacity of network. DOS attacks occurs in various layers.

- **HELLO FLOODING ATTACK:-**

In such kind of attack a hello packet which Is in the form of a weapon is released for accessing the network sensors. In this the attacker who is having the high radio transmission divides the transferred power of hello packet into numerous sensor nodes and these are then separated into large area of a wireless sensor network. There are many agreements which requires adjacent node to node broadcasting. Data will be send to the nodes which also have the hello messages send by some malicious node. This malicious node will have a strong powerful connection.

- **SINKHOLE ATTACK:-**

This attack is the dangerous attack among all other attacks as this attack forbid the base station to achieve the accurate as well as correct sensing data. The goal in sinkhole attack is that an metaphorical sinkhole having adversary at the center is generated. The sinkhole attacks works by establishing nodes by attracting the neighboring nodes using some routing algorithm.

- **CONCLUSION:-**

As we know that for using as well as to accept the wireless sensor network the main focus is in the secured transmission of data. So, this paper reviewed some of the algorithm and routing protocols that can be used to enhance the security of wireless sensor network. This paper also discussed about the eavesdropping issue. This paper will contribute for further research in the field of enhancing the security of wireless sensor network. By considering this paper a new technique could be possibly attain which will use some relay communication and relay algorithm in enhancing the security of wireless sensor network with multiple eavesdropping.

III. LITERETURE REVIEW

- **2007 contietal.[2007]**

In 2007 contiental proposed a channel protocol for securing each pair of communication in wireless sensor network. In this a secured channel is established between the pairs of sensor of a wireless sensor network. After studying and analyzing it was cleared that a specified mechanism is required for setting up the channel security.

- **2014 Di pietro, et al.[2014]**

In this various types of wireless ad hoc networks such as unattended wireless sensor network(UWSN), wireless mesh network(WMNs),delay tolerant networks(DTNs) and vehicular ad-hoc network(VANETS). These all networks were discussed in very depth with their problems and security features. So, the researcher stated that there are few issues which should be further researched in future for better secured system.

- **2015 chen ,et al.[2015]**

In 2015 a technique named as *Wireless Information and Power Transfer(WIPT)* but the problem with this technique leads to less utilization of this technique. Problems such as shorter distance for transferring power, path loss was high and channel fading occurs frequently. So , to overcome all such problems new techniques were introduced which were named as multi-antenna based WIPT techniques which were based on multi-antenna technique such as limited feedback multi-antenna technique for shorter transmitting distance and large scale multiple input multiple output (known as MASSIVE MIMO) for longer transmitting distance. The result thus shows that this new scheme using multi-antenna is more effective than earlier WIPT technique.

- **2016 Xu,et al.[2016]**

In this research paper the main focus was on to secure the relay communication in the IOT(internet of things) networks. This design technique was exposed to the eavesdrooper with some unknown number and location which leads to less secure connection or communication. Use of single antenna as well as multi antenna scenario was considered in this study which leads to obtain the allocated optical power, secrecy outage probability and code word rates. The result obtained clearly showed that use of multi-antenna was more beneficial then single antenna as it is more secured.

- **Li & Lee** et al. [2012]

suggested a novel user authentication scheme with smart cards for the wireless communication environments. The report described that the various existing schemes for authentication in the wireless networks like anonymous user authentication scheme introduced by He are prone to eavesdropping attack and is not practical for real-life implementation. The result concluded by the study clearly showed that the technique proposed in the paper is more secure, immune to a variety of attacks and a good scheme that can be implemented in the mobile wireless networking.

- **He et al. [2011]**

explained the existing smart card-based secure authentication schemes along with their weaknesses and proposed a secure and light-weight authentication scheme in which user anonymity is presented. The scheme suggested by the study is simple to implement for the mobile users because of the reason that it only performs encryption and decryption operations. Due to the simplicity of the scheme, the technique enjoys computation and communication efficiency. The result obtained shows that provided scheme is better, simple and secure as compared to earlier card based authentication schemes.

- **Xenakis&Merakos [2004]**

discussed the security framework of 3G mobile networks including security requirements, a security architecture that is used for the Universal Mobile Telecommunication Systems (UMTSs) network. The study points out that use of the existing security schemes like VPN (Virtual Private Networks), firewalls for the UMTS network resulted in the vulnerability of the network and thus specified a proposal for enhancement of security in 3G networks. The result showed that suggested proposal couldbe easily combined with the existing network architecture for ensuring the safe functionality of the UMTS networks [4].

- **Plößl&Federrath[2008]**

specified an efficient security infrastructure for the vehicular ad hoc networks (VANET) along with giving the security requirements like confidentiality, integrity, and availability, etc. The scheme is proposed for the VANET networks because of the fact of the increase in traffic on roads and thus having requirement of the safety of people. VANETs have the ability to enhance the road safety for the people. Thus result obtained showed that VANET is useful networks for people to maintain road safety [5].

- **Karlof&Wagner [2003]**

discussed the attacks that occur in the process of routing in the wireless sensor networks. The study presented the various attacks that occur against wireless sensor networks like HELLO flood attacks, acknowledgment spoofing, wormholes and sinkholes attacks, etc. and also suggested a variety of measures for handling these various types of attacks. Although the various types of routing protocols have been designed for the wireless sensor networks, none of these are designed with the goal of security in mind. Thus it is concluded from the research that currently available protocols are not secure and there is a need to develop secure protocols for wireless sensor networks so that these networks can be utilized in various applications [10].

- **Roman, et al. [2013]**

explored the features and challenges of security and privacy In distributed internet of things. In the distributed architectures, entities exchange information and communicate with each other in a dynamic way. The study provided a deep detail on distributed internet of things and concluded that although distributed architectures have various features, still there are numerous challenges that need to be solved, like assuring interoperability, reaching a business model, and managing the authentication and authorization of entities [14].

- **Stavrou&Pitsillides[2010]**

examined the various secure multipath routing protocols used in the wireless sensor networks (WSNs). The study described the various multipath routing protocols along with their security aspects, objectives, and implementation approach. The paper also lists the reasons that demand the security in multipath routing protocols, and for this reason, thestudy suggested the thread model that can be used for secure routing in the WSN networks and also specified a basic set of criteria that need to be considered while choosing the routing protocol [15].

- **Bao, et al. [2013]**

proposed the relay selection schemes for dual hop networks with the security constraints, in which a number of eavesdropper nodes may listen to the source message. To reduce the message hacking of source message by the eavesdropper nodes, system model and three relay selection techniques are discussed in the paper that area minimum selection, conventional selection and optimal selection and the system performance for the three schemes based on the various factors like non-zero achievable secrecy rate, secrecy outage probability and achievable secrecy rate is analyzed. The analysis clearly shows the correctness of the approaches [16].

- **Han et al. [2009]**

introduce the Physical Layer Security Game so that the malicious nodes are not able to obtain the information.The study suggested that security capacity can be improved using friendly jammers interfere with the eavesdroppers. Findings from study showed that the game outcomes are able to achieve effectiveness.

- **Arbaugh, et al. [2002]**

discussed that security mechanisms used by the various majority of access points supporting the IEEE 802.11 wireless standard have various security flaws. Thus most of the deployed 802.11 wireless networks are at risk of compromise. The research revealed that the combination of these mechanisms couldprovide a robust interim solution until hardware supporting the new standards is deployed, and suggested novel solution does not require any changes or additions to any deployed wireless equipment, and is easily deployed [18].

- **Yang, et al. [2015]**

examined the security, a major issue in the 5G network where wireless transmissions are inherently vulnerable to security breaches. To maintain the security study focused on the physical layer security, which safeguards data confidentiality. The study describes three technologies for security that are heterogeneous networks, massive multiple-input Multiple-Output, and millimeter wave. The novel solutions developed by the research can take data confidentiality to a whole new level, thus creating a new security paradigm for the 5G networks [19].

- **Dantu, et al. [2006]**

examined the EAP (Extensible Authentication Protocol) methods for wireless networks. The study examined the variety of widely used EAP methods are examined and evaluated for their advantages and susceptibility to types of attacks and proposed suitable EAP methods for wireless technologies beyond LANs, including RFID and WiMAX. The Findings of the research clearly showed that a new lightweight and secure EAP method is warranted for fixed mobile convergence interoperability [20].

REFERENCES

[1]. .Xu, Q., Ren, P., Song, H., & Du, Q. (2016). Security Enhancement for IoT Communications Exposed to Eavesdroppers with Uncertain Locations. *IEEE Access*, *4*, 2840-2853.

[2]. 2) Di Pietro, R., Guarino, S., Verde, N., & Domingo-Ferrer, J. (2014). Security in wireless ad-hoc networks –A survey. *Computer Communications*, *51*, 1-20. [12] Di Pietro, R., & Viejo, A. (2011).Location privacy and resilience in wireless sensor networks querying.*Computer Communications*, *34*(3), 515-523.

[3]. 3) Chen, X., Zhang, Z., Chen, H., & Zhang, H. (2015). Enhancing wireless information and power transfer by exploiting multi-antenna techniques.*IEEE Communications Magazine*, *53*(4), 133-141.

[4]. 4) Li, C., & Lee, C. (2012). A novel user authentication and privacy-preserving scheme with smart cards for wireless communications.*Mathematical and Computer Modelling*, *55*(1-2), 35-44.

[5]. He, D., Ma, M., Zhang, Y., Chen, C., & Bu, J. (2011). A strong user authentication scheme with smart cards for wireless communications.*Computer Communications*, *34*(3), 367-374. doi: 10.1016/j.comcom.2010.02.031

[6]. .6)Demakis, C., &Merinos, L. (2004). Security in third-generation mobile systems.*IEE Colloquium on Security in Networks*, *27*, 638-650. doi: 10.1016/j.comcom.2003.12.004. Plößl, K., &Federrath, H. (2008). A privacy-aware and efficient security infrastructure for vehicular ad hoc networks.*Computer Standards & Interfaces*, *30*(6), 390-397.

[7]. Raj, A. B., Ramesh, M. V., Kulkarni, R. V., & T., H. (2012). Security Enhancement in Wireless Sensor Networks Using Machine Learning.*2012 IEEE 14th International Conference on High-Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems*, 1264-1269. 1196 *Dr. Charanjit Singh and Dr. RajbirKaur, MitthatmeerKaur*

[8]. Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks*, *1*(2-3), 293-315

[9]. A.H. Farooqi and F.A. Khan, Intrusion Detection Systems for Wireless Sensor Networks: A Survey, in FGCN/ACN 2009, CCIS, vol. 56, pp. 234-241.

[10]. Y. Zhang, N. Meratnia, and P. Havinga, "Outlier Detection Techniques for Wireless Sensor Networks: A Survey", IEEE Commun. Surveys Tutorials, vol. 12, no. 2, 2010.

[11]. T. Bhattasali, and R. Chaki, A Survey of Recent Intrusion Detection Systems for Wireless Sensor Network, in 4th International Conference on Network Security and Applications (CNSA-2011), Springer, 2011, pp. 268- 280.

[12]. Nabil Ali Alrajeh, S. Khan, and Bilal Shams, Intrusion Detection Systems in Wireless Sensor Networks: A Review, International Journal of Distributed Sensor Networks Volume 2013 (2013), Article ID 167575

[13]. S. Khan, N. Mast, and J. Loo, "Denial of service attacks and mitigation techniques in IEEE 802.11 Wireless mesh networks," , vol. 12, pp. 1–8, 2009.

[14]. M. Ngadi, A.H. Abdullah, and S. Mandala, "A survey on MANET intrusion detection", International J.Computer Science and Security, volume 2, number 1, pages 1-11, 2008.

[15]. Y. Zhang, W. Lee, and Y.A. Huang, "Intrusion detection techniques for mobile wireless networks", J. Wireless Networks, vol. 9, num. 5, pp. 545-556, 2003.

[16]. S. Khan, K. K. Loo, and Z. U. Din, "Framework for intrusion detection in IEEE 802.11 wireless mesh networks," , vol. 7, no. 4, pp. 435–440, 2010.

[17]. N. Noury, T. Herve, V. Rialle, G. Virone, E. Mercier, G. Morey, A. Moro, T. Porcheron,"Monitoring behavior in home using a smart fall sensor", IEEE-EMBS Special Topic Conference on Micro-technologies in Medicine and Biology, October 2000, pp. 607–610.

[18]. K. Nagarathna, Kiran Y. B, J D. Mallapur, S. Hiremath (2012) worked on "Trust Based Secured Routing in Wireless Multimedia Sensor Networks", 2012 Fourth International Conference on Computational Intelligence, Communication Systems and Networks.

[19]. Theodore Zahariadis, Helen Leligou, Panagiotis Karkazis, Panagiotis Trakadas, Ioannis Papaefstathiou, Charalambos Vangelatos, Lionel Besson, "Design And Implementation Of A Trust-Aware Routing Protocol For Large Wsns",

International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3, July 2010.

[20]. Idris M.Atakli ,Hongking Hu, Yu Chan, " Malicious Node Detection in Wireless Sensor Networks using Weighted Trust Evalution ," The Symposis on Simulation of systems Security(SSSS 08),Ottawa,Canada, April 14 17,2008.

[21]. Janani.C and Mrs. P.Chitra, "*Trust Evaluation Based Security In Wireless Sensor Network*", (IJITR) International Journal Of Innovative Technology And Research, Volume No. 1, Issue No. 1, December-January 2013, 054-060.