IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol. 9, Issue.3, March 2021 E-ISSN: 2347-2693

# A Review on Network Layer Attacks in Wireless Sensor Networks

**Parvathy K.[1*], S. Rajalakshmi[2]**

[1,2]Department of Computer Science and Engineering, Sri Ramakrishna Institute of Technology, Coimbatore, India

[*]*Corresponding Author: parvathy.cse@srit.org*

DOI: https://doi.org/10.26438/ijcse/v9i3.4548 | Available online at: www.ijcseonline.org

Received: 20/Mar/2021, Accepted: 23/Mar/2021, Published: 31/Mar/2021

***Abstract***— The wireless sensor networks (WSN) are said to be one of the popular networks in using all-inclusive applications like lots of applications in environment monitoring, military applications, health care monitoring, habitat monitoring, etc. .These networks are structured in many or more number of sensor nodes. The Deployment of nodes in these networks are not secure which may cause to security attacks. In this paper, different types of attacks and network layer attacks are discussed in wireless sensor networks and how to enhance and detect the attacks from the WSN by using some of the methods to resolve the problem.

***Keywords*—** Wireless Sensor Networks,Attacks,Network Layer.

## I. INTRODUCTION

Wireless sensor networks are new-fangled wireless networks which are distributed, low-power, low-cost and small in size[2].[9] Wireless sensor networks are used in many all-inclusive applications like Health-care, Habitat monitoring, civilian application, military application, traffic control and environment monitoring. [2,3]In Environment, the WSN are used to measure the environmental conditions like temperature, pressure, sound and humidity etc.

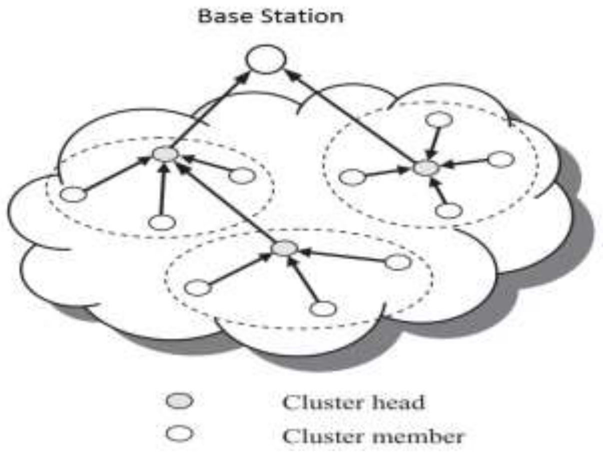

Fig.1.1 Wireless Sensor Networks

The [7,9]WSN are constructed to many number of nodes in which each number of nodes are connected to one or more sensors. A sensor node is typically made up of a radio transmitter, an interfacing circuit, a microcontroller and a battery. The radio transmitter is connected along with an antenna. There are the constraints in sensor node such as limited storage, low power, low latency, low bandwidth, low physical size and limited energy. These sensor node constraints are very obstacles to sensor security. There are different types of attacks has been happened while communication take place between among the node, whether it is within communication range or out of range (i.e.) insider attack or outsider attack, so the security issues on routing such as data aggregation, route discovery, data dissemination etc.Wireless Sensor Networks [2,4] is also an another form of adhoc network, these security goals shrouds both traditional network and unique constraint of adhoc network. [7,10] The security goals are divides into two ways: Primary and Secondary. The primary goals can also be called as standard security goals as Confidentiality, Integrity, Authentication and availability. The secondary goals are data freshness, self-organization [3]. Confidentiality refers to the capability to obscure message from the eavesdroppers. Integrity means that message which was received cannot able to modify by the attacker. Authentication which means it verifies the identity of sender and receiver for blocking the modification of the packets and injecting the bogus packets. Availability which means the resource is available for the message to communicate during the data communication. Data Freshness is When the data is recent, and it assures that old message cannot be replayed.

## II. RELATED WORK

[3] Discussed about the wireless sensor networks and its types.[5] given briefly about the types of attacks as active attack and passive attack. It also given the types in active and passive attacks. [6,8,9] illustrates about the layers in Wireless sensor networks. In this paper which discuss about network layer and its attacks .[10] mentions about wormhole attacks and its types as open, half open and close wormhole attacks.[12] discuss about blackhole attack and its types.[15] discuss about Sybil attack, how it cause in wireless sensor networks.[16] discuss about Sybil

attacks.[15,16,17,18,19,20,21,23,25] discuss and explains about the detection mechanism of attacks in wireless sensor networks

## III. ATTACKS ON WIRELESS SENSOR NETWORKS

During the communication between sender and receiver, [5,7] the wireless sensor networks are endangered which may cause to security attacks. In this case, the network is unprotected.[14] In WSN, the security attacks are divided into two types: Active Attacks and Passive Attacks.

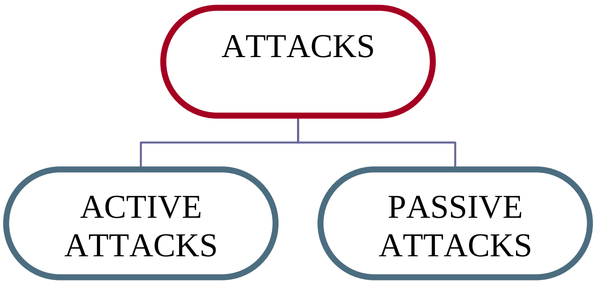

Fig.1.2.Types of Attacks

Active Attack which means the intruder who gets inside the communication between sender and the receiver and changes the network packet and sends a false network packet. Passive Attack which means when the intruder who get inside the communication without knowing to the sender and receiver.

## IV. ATTACKS ON NETWORK LAYER

An Intruder fetches the information by unauthorisation of data in Wireless sensor Network environment.[11]There are different types of network layer security attacks:
1) Wormhole Attack
2) Black hole Attack
3) Sybil Attack
4) Sinkhole Attack

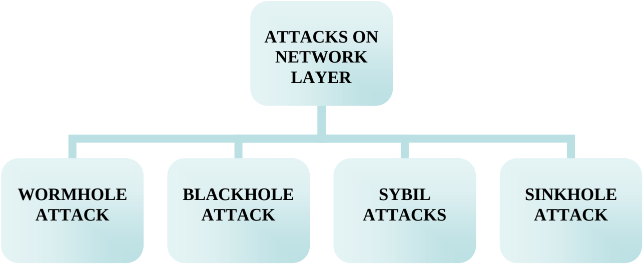

Fig.1.3.Attacks in Network Layer in WSN

*Wormhole Attack*
The Attack[5] where the intruder which make a link to source and destination to communicate among the two node, this make of easily accessible to share the information. Wormhole attack[12] has different types they are:
1) Open Wormhole attack
2) Half Open Wormhole attack
3) Close Wormhole attack

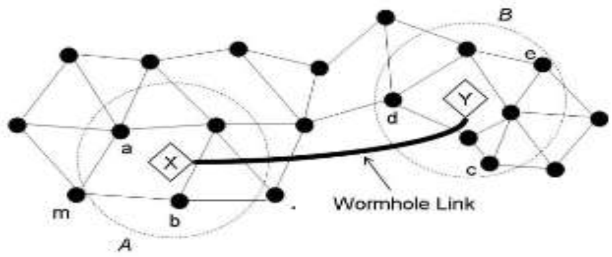

Fig.1.4. Worm Hole Attack

two node, this make of easily accessible to share the information. Wormhole attack[12] has different types they are:
1) Open Wormhole attack
2) Half Open Wormhole attack
3) Close Wormhole attack

In open wormhole attack, the attacker gets inside to the source and destination, it creates false path without the knowledge of the users, the attacker will monitor the information and thus send to destination by attacker itself. Half open which means during the communication the attackers get inside to the source node and create the false path send to receiver.

During the communication among source and destination the intruder who does not sent any packets and creates a false path in hidden node.

*Black hole Attack.*
The Attack is[10] called as Routing layer attack, where the packet transmissions in many number of nodes from the routing layer.

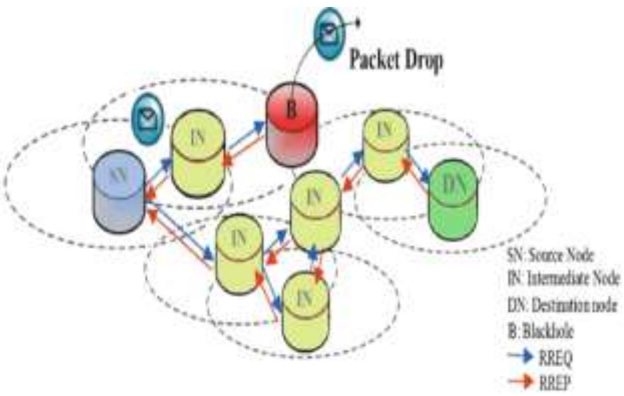

Fig.1.5.Black Hole Attack

In this attack mainly focuses on attack. In this [11] attack it is impossible to prevent and mitigate easily. It may prevent temporarily in the networks. There are two types of
1) Internal Black hole attack
2) External Black hole attack

Internal Black hole Attack is the Attack may come inside the network and the inside node which make a false node and makes a route to sender node and Receiver node. External Black hole Attack is the attack which comes outside the network it can be called as DOS attacks. It may cause the network traffic and make damage to the entire network.

*Sybil Attack*

The Attack which [15] makes the nodes as suspicious and create number of identities so that attacker can able to create many number of identical nodes. They are one of the root causes for geographic Routing Protocols. [13] The attack which mainly focuses on multi-hop Routing, Distributed Storage.

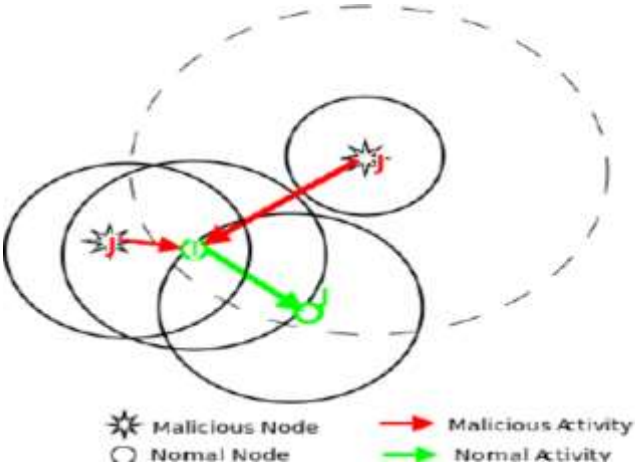

Fig.1.6.Sybil Attack

*Sink Hole Attack*

The Attack is the [3] insider Attack, by which the attacker who get inside through the node to the network and fetch the information from the neighbours nodes which is based on the routing protocol. This [6] makes the communication to one or more node that makes the Wireless Sensor Networks vulnerable. There are [9][21][22] different types of techniques used in sinkhole attack.

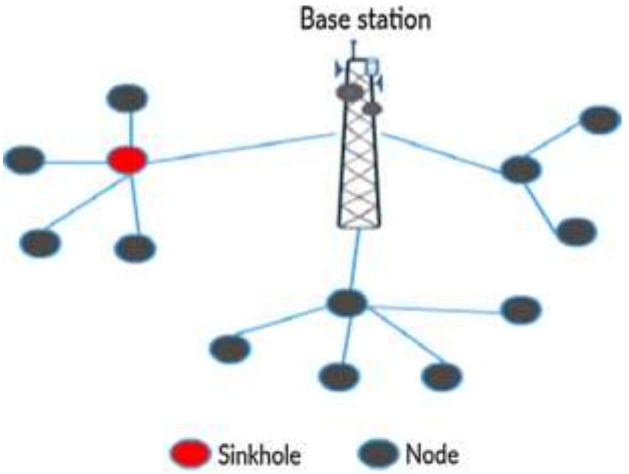

Fig.1.7. Sink Hole Attack

## V. DETECTION MECHANISMS FOR ATTACKS ON NETWORK LAYER

The [16] technique to detect the worm hole attack are Message Travelling time information-based method and Location and Time-based approaches. The technique [17] called packet leashes, which gives limit distance to travel the packet to the network. In the case of time leashes approach [18] it is also called as temporal leashes which node which include the time at which time the packet is send and receive node along with the time and verifies the values of the time, so that it helps to fetch the malicious node very easily.

For the [19] detection of black hole attack the techniques can be as REWARD in Wireless Sensor Networks and Energy Efficient Intrusion Detection System for Black Hole Attacks in WSN. The [20] technique called REWARD (Receive, Watch, Redirect) which easily detect the malicious nodes. It forwards the packet the packets in the form of router called geographic location to keep noticing of malicious nodes. It helps to improve to be more secure and performance. The next technique [20] to detect the hierarchical routing protocol, which use to prevent from black hole attacks. It is a simple technique. it verifies both sensor node and the base station by forwarding the packets.

The techniques to detect the Sybil attack are RSSI Method and K-Mean method.

The technique [24] called K-mean method; it is also called as RSS base detection method. It helps to detect the attack by changing of time and transmission power. This method is mainly for clustering method. This method is used as node which is to be large amount of time and more power, Thus the node is said to cause Sybil attack. if it in the case of short amount of time and less power then it is not detected by Sybil attack. The technique [24] called RSSI Method which helps to checking the level of power at different time. The technique that search for the correct location of malicious node. It is a multiple handle algorithm which helps to find the malicious node.

The detection mechanisms [25] to mitigate sinkhole attack are Mobile Agent Based Approach and Message Digest Algorithm.

The technique called [25] mobile Agent based approach, which use to detect with help of mobile agent. The Mobile Agent which means self control, it helps to move from one node to another not by sending the data. The mobile agent which gather all information from mobile sensor node to entire network so that node which helps to detect the sink hole attack, whether the information gathered to the node is malicious node. The technique called [27] Message Digest Algorithm which helps to detect the sinkhole, it mainly detect the attack using the method called one-way hash chain. It transmits the message from source to destination by trustable path. It helps the malicious node to hide the information from the attacker.

## VI. CONCLUSION

In this paper, we have discussed about wireless sensor networks attacks and its types. We have given a brief explanation about network layer and its attacks. We have classified and explained about attacks in network layer WSN.Moreover we have discussed about detection mechanisms of attacks in WSN.

## REFERENCES

[1] Chelli P, “ Security Issues in Wireless Sensor Networks: Attacks and Countermeasures,” Proceedings of the World Congress on Engineering 2015, **Vol. 1, WCE 2015, July 13 3, 2015**, London, U.K.

[2] Kanchan Kaushal and Taranvir Kaur, “A Survey on Attacks of WSN and their Security Mechanisms,” International Journal of Computer Applications, **Volume 118, No. 18, May 2015.**

[3] Sahabul Alam and Debashis De , “ Analysis of security threats in wireless sensor network,” International Journal of Wireless & Mobile Networks (IJWMN), **Vol. 6, No. 2, April 2014.**

[4] Naser Alajmi , “ Wireless Sensor Networks Attacks and Solutions,” (IJCSIS) International Journal of Computer Science and Information Security, **Vol. 12, No. 7, July 2014.**

[5] J. Steffi Agino Priyanka, S. Tephillah and A . M. Balamurugan, “Attacks and countermeasures in WSN,” International Journal of Electronics & Communication (IIJEC), **Volume 2, Issue 1, January 2014,** ISSN 2321-5984.

[6] Jaydip Sen , A Survey on Wireless Sensor Network Security, **Vol. 1,No. 2, August 2009,** International Journal of Communication Networks and Information Security (IJCNIS)

[7] G.Anand, Dr.H.G.Chandrakanth, Dr.M.N.Giriprasad, SECURITY THREATS & ISSUES IN WIRELESS SENSOR NETWORKS International Journal of Engineering Research and Applications(IJERA) ISSN: 2248-9622 www.ijera.com **Vol. 2, Issue 1,Jan-Feb2012,**

[8] Manju Gupta and C. Ram Gupta, Security Issues In Wireless Sensor Network, **Vol. 2, No. 2, pp. 355-358, July-December 2011,** IJCSC.

[9] Priyanka K. Shah and Kajal V. Shukla Secure Data Aggregation Issues in Wireless Sensor Network: A Survey, Journal of Information and Communication Technologies, ISSN 2047-3168, **Volume 2, Issue 1, January 2012.**

[10] Modares, H, Kuala Lumpur Salleh, R. Moravejosharieh. Overview of Security Issues in Wireless Sensor Networks Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference on **20-22 Sept. 2011.**

[11] Rajeshwar Singh1, Singh D.K and Lalan Kumar, A review on security issues in wireless sensor network, ISSN: 0976-8742 & EISSN:0976-8750, **Vol. 1, Issue 1, PP-01-07, 2010,** JISCE.

[12] T.Kavitha, D.Sridharan Security Vulnerabilities In Wireless Sensor Networks: A Survey, Journal of Information Assurance and Security **5, 031-044, 2010**

[13] M. Gruteser, G. Schelle, A. Jain, R. Han, and D. Grunwald, “Privacy-aware location sensor networks”, In Proceedings of the 9th USENIX Workshop on Hot Topics in Operating Systems, (HotOS IX), **2003.**

[14] A. Perrig, J. Stankovic, and D. Wagner, “Security in wireless sensor networks”, *Communications of ACM* , **Vol 47, No. 6, pp. 53-57, 2004**

[15] E. Shi and A. Perrig, “Designing secure sensor networks”, Wireless Communication Magazine, **Vol. 11, No. 6, pp. 38-43, December 2004.**

[16] Jaspreet Kaur, Tavleen Kaur”A Comparative Study of Techniques Used in Detection and Prevention of Black Hole Attack inWireless Sensor Networks”,ijreset, **Vol. 2 Issue III, March 2014.**

[17] Yunzhou Zhang1,2, Xiaohua Zhang1, Zeyu Wang1, Honglei Liu College of Information Science and Engineering , Shenyang SIASUNG Robot & Automation Northeastern University Company, Ltd. Shenyang, P.R.China “Virtual Edge Based Coverage Hole Detection Algorithm in Wireless Sensor Networks” IEEE **2013.**

[18] Mohammad Wazid, Student Member, IEEE, Avita Katal, Student Member, IEEE and R H Goudar “TBESP Algorithm for Wireless Sensor Network under Black hole Attack” **2013.**

[19] Nishant Sharma1, Upinderpal Singh” Various Approaches to Detect Wormhole Attack in Wireless Sensor Networks” IJCSMC, **Vol. 3, Issue. 2, pg.29 – 33, February 2014.**

[20] Y. C. Hu, A. Perrig and D. B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks", in 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), **pp. 1976-1986, 2003.**

[21] Vinay Soni, Pratik Modi, Vishvash Chaudhri,” Detecting Sinkhole Attack in Wireless Sensor Network”, **Volume 2, Issue 2, February 2013.**

[22] D.Sheela, Naveen kumar. C and Dr. G.Mahadevan; “A Non Cryptographic Method of Sinkhole Attack Detection in Wireless Sensor Networks” IEEE-International Conference on Recent Trends in Information Technology,ICRTIT**, pp. 527-532, 2011.**

[23] S.Sharmila and Dr G Umamaheswari; “Detection of sinkhole Attack in Wireless Sensor Networks using Message Digest Algorithms” International Conference on Process Automation, Control and Computing (PACC)**, pp. 1-6, 2011.**

[24] Abirami.K, Santhi.B,” Sybil attack in Wireless Sensor Network”,IJET.

[25] Yingying chen, “Detecting and localizing identity-based attacks in wireless sensor network”,IEEE Journal, **June 2010.**

## AUTHORS PROFILE

*Ms Parvathy K* is currently working as Assistant Professor in Department of Computer Science and Engineering in Sri Ramakrishna Institute of Technology, Coimbatore. She Completed her Master and Bachelor degree in CSE at Sri Ramakrishna Engineering College Coimbatore.Her main research work focuses on Internet of Things,Cryptography Algorithms,Network Security and wireless sensor networks. She has 2 years of teaching experience and 1 year of Research Experience.

*Ms Rajalakshmi S* is currently working as Assistant Professor in Department of Computer Science and Engineering in Sri Ramakrishna Institute of Technology, Coimbatore. She Completed her Master degree in CSE at Anna University Coimbatore and Bachelor degree in CSE at Maharaja Engineering College Avinashi Coimbatore.Her main research work focuses on Machine learning,Artificial Intelligence and wireless sensor networks. She has 2 years of teaching experience and 1 year of Research Experience.