NETWORK LAYER ATTACKS -A REVIEW

Mayur Srivastava[1], Amit Dixit[2]
[1]Assistant Professor, Quantum School of Technology, Roorkee, India
[2]Dean & Prof. Dept. of ECE, Quantum School of Technology, Roorkee, India

Abstract

A wireless sensor network is an encapsulated form of different tiny sensor motes, which can perform a different operation such as sensing, processing and transmitting information among each other. WSN is commonly used in research area, commercial application and defense projects. WSN generate new opportunity for the people to search out there threats easily and also useful for monitoring any environmental process. In this paper we are going to discuss different attacks on network layer and there detection and prevention techniques.

Keywords: Wireless sensor networks, Networks layer, Security, Attacks.

I. INTRODUCTION

WSN is commonly used in research area, commercial application and defense projects. WSN generate new opportunity for the people to search out there threats easily and also useful for monitoring any environmental process [1]. Low-Energy Adaptive Cluster Head (LEACH) is one of the most popular routing protocols which disperse the energy load among the various sensor nodes. The effect of attack is more if the attacker becomes the cluster head. In that case it can affect the data of the whole cluster attached to it [2].This paper is basically divided into 4 sections In first section we provide the introduction about wireless sensor network and in second section we covered all the different types of attacks occurred in network layer. Section 3 contains literature review on network layer and in section 4 we conclude our paper.

II. NETWORK LAYER ATTACKS

Network layer is one of the layers of OSI Model we emphasize our talk on this layer due to our research field and still there is many scope remain in this area. There are different types of attacks occurred in network layer some of them are Spoofed routing information, Selective packet forwarding, Sinkhole attack, Sybil attack, Wormhole attack, Blackhole and Grayhole attack, Hello Flood, Information Disclosure, Acknowledgement Spoofing.

Table1: Attacks & Defenses of network layer

Layer	Attacks	Defense
Network	Spoofed & Selective forwarding	Authentication, Monitoring, Filtering
	Sinkhole	Redundancy Probing
	Sybil	Authentication, Monitoring, redundancy
	Wormhole	Authentication, Probing
	Grayhole & Blackhole	Monitoring, authentication
	Hello Flood	Authentication, Packet curbs by using geographic & temporal info.

Selective Packet Forwarding attack: In selective forwarding attack, most of the time malicious nodes behave like normal nodes but drop some sensitivepackets selectively and such selective dropping is very tough to detect [3]. In a multihop networks, each node rely on other for sending messages faithfully to the base station. But intruder insert a malicious node between the path of message flow and this malicious node refuse to forward any message. Such type of attack comes under selective forwarding attack and is accomplished when the adversary drops packets coming from specific sources in the network [4].

Sinkhole Attack: In a sinkhole attack malicious nodes or compromised node give attractive information to the entire neighboring node that he has extremely high quality route to base station. Some protocols might actually try to verify the quality of route with end-to-end acknowledgements containing reliability or latency information [5]. WSN is generally consists of many sensor nodes were sensors are scattered in a much unattended manner so such networks are very prone to comes under attacker think area. Here intruder attracts surrounding nodes by transmitting a common message to all his surroundings that he has high quality routes to the base station and then alter the data passing through it. Some secure or geographic based routing protocols resist to the sinkhole attacks in certain level, many current routing protocols in sensor networks are susceptible to the sinkhole attack [6].

Sybil Attack: In this type of attack, a malicious node behaves as if it were a large number of nodes, for example impersonating other nodes or simply by claiming false identities. By using only one physical device an intruder may create an arbitrary number of additional node identities [7]. In [8] Sybil attack was introduced to denote an attack where the malicious node called Sybil node tries to forge multiple identification in a certain area. In wireless sensor network Sybil attack is easy to perform because a same frequency is shared among all the nodes. Due to message broadcasting with different identifications, Sybil node furnishes the group based decisions and disorder network middleware services severally [9].

Wormhole attack: In this attack two nodes are connected with each other via a medium which is not available to normal nodes, with this out of band channel the nodes are able to communicate with one another over a range in which normal nodes cannot [10]. In this attack a wormhole tunnel is manufactured by combination of any two compromising nodes (generally located at different location) which collaborate together to generate an illusion that they are just one hop away and there by routing the packets to them as neighbor nodes. As soon as wormhole entities generate the tunnel successfully, they can drop the packets, replay, tampers the packet or forward them selectively [11].

Blackhole Attack: Blackhole attack comes under network layer of OSI Model it is the part of Denial of service in which an adversary may create a compromise node which block the packet transmission instead of transferring packets towards the destination node. Or in other words, all the information was captured by malicious node instead of delivering it to the destination node [12]. This attack is also known as packet drop attacks. In wireless sensor network mostly two protocols are in use and they are Dynamic Source Routing (DSR) and Ad-hoc On-Demand Distance Vector (AODV). Here DSR uses Route request packet (RREQ) and Route response packet (RREP) for finding the best routes. An RREQ has the address of the destination node and it goes to all the nodes attached to that network. When it receives the destination address, it creates an RREP in response and sends it back to the original sender [14].

Hello Flood: In this type of attack an adversary plays a game to make fool to the entire neighbor by transmitting a message that they are within its neighborhood, here attacker use a high-powered transmitter [13].

Spoofed routing information: Spoofed routing means that the intruder may alter or spoof direct routing information.

III. LITERATURE REVIEW

A considerable amount of work has been done for the detection technique used in different attacks in a network layer. We review some previous year paper to know about different types of attacks comes under network layer and also there detection techniques.

Table 2: Different detection techniques used in previous year

First Author	**Network Layer Attacks**	**Detection Technique Used**
Edith C.H. Ngai, 2007 [15]	Sink Hole Attack	**Light weight algorithm** The algorithm consists of two steps: It first locates a list of suspected nodes by checking data consistency, and then identifies the intruder in the list through analyzing the network flow information.
Sina Hamedheidari, 2013 [16]	Sink Hole Attack	**Mobile Agent based approach** We use mobile agents to inform nodes of their valid neighbors so they will not listen to the traffics generated by malicious ones. Our proposed algorithm to detect and prevent sinkhole attacks is formed of two phases: network deployment phase tells how the network is configured and, network maintenance phase which indicates how to keep the network safe
Ioannis Krontiris, 2014 [17]	Sink Hole Attack	**Two Steps for Detection:** **1.** For each overheard route update packet, check the sender field, which must belong to one of your neighbors. **2.** For each [parent, child] pair of your neighbors, compare the link quality estimate they advertise for the link between them. Their difference cannot exceed 50
Dhara Buch, 2011 [18]	Wormhole Attack	This approach is mainly in two Phase: **Key Generation Phase** that derives key for data protection. Second phase is executed for **Wormhole detection Phase**
Zubair Ahmed Khan, 2012 [10]	Wormhole Attack	Algorithm: Three steps are used in this algorithm. Step 1: Suspected paths are identified. Step 2: When a node receives such a processing request, it will check its own table and if the same pattern exists, it will reply as true to the requesting node. Step 3: in this step the nodes at the two ends of wormhole send some encrypted messages to one another

Yin, J, 2006 June [19]	Blackhole Attack	Randomized data acknowledgement scheme
Karakehayov, 2007 Sep [20]	Blackhole Attack	REWARD (Receive, Watch & Redirect Algorithm)
M.Tiwari, 2009 Nov [21]	Blackhole Attack	Specification based Intrusion
Taylor, 2014 April [22]	Blackhole Attack	Advanced Detection of Intrusion on Sensor Network (ADIOS)
Motamedi, 2015 May [23]	Blackhole Attack	Unmanned Aerial Vehicle Technique (UAV)
Salehi, 2016 [24]	Blackhole Attack	Discrete Time Markov Chain (DTMC) Model

IV. CONCLUSION

As we reviewed many previous paper and learn different detection techniques used for detecting denial of service or DoS Attack on network layer. With the help of this paper we would like to emphasize our study only on network layer attacks and try to get best detection technique with energy efficient. In wireless sensor network there is many scope still remain for searching an energy efficient detection techniques.

References:

[1] Datema, S. (2005). A case study of wireless sensor network attacks. Delft University of Technology, Delft University of Technology.

[2] Gaur, M. T. M., & Laxmi, V. (2013). Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN. In The 8th International Symposium on Intelligent Systems Techniques for AdHoc and Wireless Sensor Networks (Procedia Computer Science 19 (2013) 1101--1107. DOI= 10.1016/j. procs. 2013.06. 155

[3] Yu, B., & Xiao, B. (2006, April). Detecting selective forwarding attacks in wireless sensor networks. In Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International (pp. 8-pp). IEEE.

[4] Kaplantzis, S., Shilton, A., Mani, N., & Sekercioglu, Y. A. (2007, December). Detecting selective forwarding attacks in wireless sensor networks using support vector machines. In Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on (pp. 335-340). IEEE.

[5] Tumrongwittayapak, C., & Varakulsiripunth, R. (2009, December). Detecting sinkhole attack and selective forwarding attack in wireless sensor networks. In Information, Communications and Signal Processing, 2009. ICICS 2009. 7th International Conference on (pp. 1-5). IEEE.

[6] Ngai, E. C., Liu, J., & Lyu, M. R. (2006, June). On the intruder detection for sinkhole attack in wireless sensor networks. In Communications, 2006. ICC'06. IEEE International Conference on (Vol. 8, pp. 3383-3389). IEEE.

[7] Newsome, J., Shi, E., Song, D., & Perrig, A. (2004, April). The Sybil attack in sensor networks: analysis & defenses. In Proceedings of the 3rd international symposium on Information processing in sensor networks (pp. 259-268). ACM.

[8] J. R. Douceur. The Sybil attack. In IPTPS ’01: Revised Papers from the First International Workshop on Peer-to-Peer Systems, pages 251–260, 2002

[9] Demirbas, M., & Song, Y. (2006, June). An RSSI-based scheme for Sybil attack detection in wireless sensor networks. In Proceedings of the 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks (pp. 564-570). IEEE Computer Society.

[10] Khan, Z. A., & Islam, M. H. (2012, October). Wormhole attack: A new detection technique. In Emerging Technologies (ICET), 2012 International Conference on (pp. 1-6). IEEE.

[11] Maidamwar, P., & Chavhan, N. (2013). Impact of wormhole attack on performance of LEACH in wireless sensor networks.

International Journal of Computer Networking, Wireless and Mobile Communications, 3(3), 21-32.

[12] Sheela, D., Srividhya, V. R., Asma, B. A., & Chidanand, G. M. (2012). Detecting Black Hole Attacks in Wireless Sensor Networks Using Mobile Agent. In International Conference on Artificial Intelligence and Embedded Systems (ICAIES (pp. 15-16).

[13] Srivastava, M., & Dixit, A. BLACKHOLE DETECTION TECHNIQUE IN WSN-A REVIEW.

[14] Taylor, V. F., & Fokum, D. T. (2014, April). Mitigating black hole attacks in wireless sensor networks using node-resident expert systems. In Wireless Telecommunications Symposium (WTS), 2014 (pp. 1-7). IEEE.

[15] Ngai, E. C., Liu, J., & Lyu, M. R. (2007). An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks. Computer Communications, 30(11), 2353-2364.

[16] Hamedheidari, S., & Rafeh, R. (2013). A novel agent-based approach to detect sinkhole attacks in wireless sensor networks. Computers & Security, 37, 1-14.

[17] Krontiris, I., Giannetsos, T., & Dimitriou, T. (2008, October). Launching a sinkhole attack in wireless sensor networks; the intruder side. In Networking and Communications, 2008. WIMOB'08. IEEE International Conference on Wireless and Mobile Computing, (pp. 526-531). IEEE.

[18] Buch, D., & Jinwala, D. (2011). Detection of wormhole attacks in wireless sensor network.

[19] Yin, J., & Madria, S. K. (2006, June). A hierarchical secure routing protocol against black hole attacks in sensor networks. In Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference on (Vol. 1, pp. 8-pp). IEEE.

[20] Karakehayov, Z. (2007, September). Security-lifetime tradeoffs for wireless sensor networks. In Emerging Technologies and Factory Automation, 2007. ETFA. IEEE Conference on (pp. 646-650). IEEE.

[21] Tiwari, M., Arya, K. V., Choudhari, R., & Choudhary, K. S. (2009, November). Designing intrusion detection to detect black hole and selective forwarding attack in WSN based on local information. In Computer Sciences and Convergence Information Technology, 2009. ICCIT'09. Fourth International Conference on (pp. 824-828). IEEE.

[22] Taylor, V. F., & Fokum, D. T. (2014, April). Mitigating black hole attacks in wireless sensor networks using node-resident expert systems. In Wireless Telecommunications Symposium (WTS), 2014 (pp. 1-7). IEEE.

[23] Motamedi, M., & Yazdani, N. (2015, May). Detection of black hole attack in wireless sensor network using UAV. In Information and Knowledge Technology (IKT), 2015 7th Conference on (pp. 1-5). IEEE.

[24] Salehi, M., Boukerche, A., & Darehshoorzadeh, A. (2016). Modeling and performance evaluation of security attacks on opportunistic routing protocols for multihop wireless networks. Ad Hoc Networks, 50, 88-101.Chicago.