ISSN No:-2456 – 2165

A Survey on the Mechanisms used for the Detection and the Prevention of the Selective Forwarding and Black-Hole Attacks in the Wsns

Shwetha S S
Information Science & Engineering Department
Acharya Institute of Technology
Bangalore, Karnataka, India
shwetha.gowda.04@gmail.com

Abstract— Wireless Sensor Networks (WSN) is a leading technology these days and has a broad variety of application such as battleground supervision, traffic surveillance, flood finding, forest fire discovery etc. But wireless sensor networks are vulnerable to a multiplicity of possible attacks which hamper the normal process of the system. Selective forwarding and Black hole attack are most harsh security hazards that have an effect on the network from its regular functioning by unkindly advertising itself surrounded by shortest path to the targeted node and then drops all in receipt of packets. There be a lot of methods have been projected to preserve network from selective forwarding and black hole attack, but not any of the methods looks most capable to defend alongside these attacks. So in this paper, we have examined the existing justification for selective forwarding and black hole attacks using different protocol.

Keywords—WSNs; Security; Selective Forwarding Attack; Blackhole Attack; Attacks;

I. INTRODUCTION TO WSN

Technological developments in wireless communication knowledge have lead to the expansion of reasonably priced sensor nodes. The accessibility of these nodes has completed Wireless Sensor Networks (WSN) single of the most talented knowledge of the precedent decade. A wireless sensor network is fashioned by a large amount of disseminated sensor nodes in meticulous surroundings for monitoring and sensing. In a large amount cases, these minute sensors nodes are operational with a processor, transmitter, radio transceiver, memory furthermore a battery [3]. The purpose of these autonomous nodes is sensing, monitoring and gathering data within a précised area and distributing this information support to base location for examine. The base position acts like a gateway intended for connecting by means of end user position. Wireless communication is utilized to broadcast data among base station and sensor nodes using a position of predefined regulations described as routing protocols. In current years, protection of wireless sensor networks have be made the major issue. Wireless sensor network are susceptible to many kinds of threats. The most and major serious hazards are selective forwarding and black hole attack [4]. By the nodes which are malicious in the network which suffers from the black hole attack which make use of the routing some set of rules nothing but the protocol to broadcast itself as containing the shortest pathway toward the node whose information it wants to hamper[2]. The black hole attack cause severe intimidation to the wireless sensor network security, in view of the fact that it drops packets constantly. Selective forwarding attacks, sensitive packets dropped due to the malicious nodes in the network, for example, a packet exposure to the adversary reservoir movements [5].

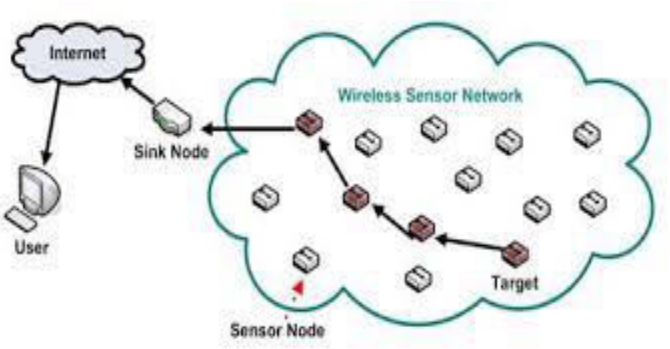

Figure 1.1: Wireless Sensor Network Architecture.

II. SECURITY ATTACKS IN WIRELESS SENSOR NETWORK

In earlier period various kinds of WSN routing protocols been designed with no considering a security, an adversary be capable of set awake various of attack scheduled the network such like wormhole attack, sinkhole attack, hello flood attack, black hole attack, selective forwarding attacks etc.

A. Wormhole attack.

An attacker reports packets at single location through the tunnels in the network to a further location. Routing know how to be interrupt when routing manage messages which are forwarded through the channel. This channel between get together of two attackers is referred like a wormhole [6].

B. Jamming attacks.

Jamming attacks be individuals which try en route for interfere through the broadcast and response of wireless indication by releasing the RF signals. There are dissimilar category of jammers that aim to intentionally infuse false information during the announcement between the nodes which influence the data broadcast and also the concert of WSN condensed as it basis the over usage of scarce property like memory , battery power etc. [10].

C. Selective forwarding attack.

During a selective forwarding attack the malicious nodes performs like black hole as well as may reject to forward assured messages and just drop them, guarantee that they not broadcast any further. Conversely, such an invader runs the danger neighboring nodes resolve conclude to failed and settle on to seek a different route[11].

D. Hello flood attack.

In Hello Flood attack the malicious nodes transmit HELLO packets towards its adjacent nodes and influence them to set up routes transient them. The purpose of HELLO flooding is to build the network addicted to a confusion state, preventing legal data packets from accomplish their destinations. To accomplish this, the opponent only wants to transmit HELLO messages by means of large an adequate amount of power[9].

E. Black hole attack.

Black hole attacks take place while an intruder confine and reprograms the location of nodes inside the network to obstruct the packets they take delivery of instead of promote them towards base location. Since, resulted any in sequence that come into the black hole section is captured. Black hole attacks be an easy to compose and which they are competent of discouragement network efficiency by dividing wall the network, those are the significant event in sequence do not attain the base location [12].

F. Sybil attack.

In Sybil attacks, a malevolent node performs like many endorsed nodes by counterfeit multiple authorized node IDs. It can be able to then change, selectively remove or falsify packets. It can as well eavesdrop on transitory data flow. Here, there can be two types attacks of Sybil, in the initial type the nasty node falsify several authorized IDs in single location, although in the subsequent type the malevolent node falsify numerous IDs at various locations[9].

III. TECHNIQUES USED FOR DETECTION AND PREVENTION OF BLACK HOLE ATTACKS

Black hole attacks happens when an trespasser confine and reprograms a locate of nodes inside the network in the direction of obstruct the packets that they take delivery of in its place of forwarding them to the base location [2]. The network routine parameters i.e. end- to- end delay and throughput, energy are exaggerated in the occurrence of black hole nodes; throughput turn out to be very fewer and end- to- end hurdle increases [2]. When the foundation choose the pathway including the invader node, the passage starts passing from side to side the adversary node in addition to this nodes establish reducing the packets selectively or else in whole. At this time, re-programmed nodes be phrased the same as black hole nodes as well as the region surrounded by the black-hole nodes be in the black hole constituency. Black hole region is the entrance point to a huge number of injurious attacks[1].

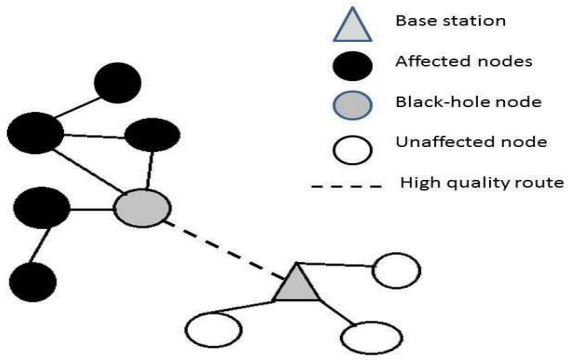

Figure 3.1: Black hole attack.

In the Exponential trust based mechanism [4], a Streak counter is used to store up the consecutive amount of packets dropped along with a trust factor is sustained for every node. The trust factor plunges exponentially by means of every successive packet are dropped which assist in noticing the malicious node. In this method, they maintain a counter in the reminiscence which supplies trust factor of every node. This utilize streak counter in which continue a record of count up of successive packets dropped. This technique prove a reduce in the amount of packets plunged ahead of the node being identified as a malevolent node. Responsibility of the network is extremely less. The method employ a streak counter which continues the count of successive packets dropped.

The REWARD [13] which meant for receives, watch, redirect which be link among replication. The algorithm intended for finding away the particular black holes or else group of malevolent nodes. The routing method is used to design for network nodes along with their broadcast power provide. REWARD ahead packets by means of geographic position of router. The records base stay records for apprehensive node. The algorithm has two kinds of messages they are MISS and SAMBA. REWARD permits to security characteristic and existence routine. REWARD is additional suitable by means

of dense networks wherever is easier to discover neighboring nodes extent the distance.

In "Checking Agents & multiple Base stations" technique[1] which identify black hole attacker in whole network in with the intention of towering detection rate like shown in simulation effect. Their projected trust model and trust computation describe trust height of association connecting nodes within network. This procedure uses routing from side to side numerous base position only when present is a possibility of incidence of black holes inside the network. if not routing from side to side adjacent base position is completed to reduce additional use of communication in the sensor network. Therefore, it decreases the utilization of power in the network through the node which be a major issue which is imperfect in addition to is to exist considered cautiously in the networks.

A novel acknowledgement based [14] detection method which assist to make simpler the elimination of black holes with assurance flourishing deliverance of packets in the direction of destination. Every sensor nodes be unspecified to have similar message ranges. The direction-finding algorithm is organized on untrustworthy MAC protocol with present may be packet drops or ACK in the sensor network. Their algorithm be able to successfully recognize and eliminate 100% black hole nodes along with make sure additional than 99% packet release. They contain simulated merely in conditions of the packet release portion but not on top of the end to end delay, power efficiency etc.

In the single hop and multi hop leach approach[16] the objective of the black hole assault is to gather as a great deal information probable by the malevolent nodes with afterward go down them. In this document we be as long as simulation consequences for information transmitted, numeral of living nodes and remaining energy through contrast single hop LEACH and multi hop LEACH that the result of Blackhole attack on top of them. The information transmitted is smallest amount in multi hop LEACH network exaggerated through Blackhole attack in addition to maximum within the network of the single hop LEACH with no attack. The nodes be alive for a greatest duration inside single hop LEACH by means of attack. The remaining energy is maximum in single hop LEACH by means of attack. Therefore, the collision of Blackhole attack is additional on the multi hop in the LEACH network than in single hop LEACH sensor network.

IV. TECHNIQUES USED FOR DETECTION AND PREVENTION OF SELECTIVE FORWARDING ATTACKS

Multi-hop form of announcement is usually favored in wireless sensor network information gathering procedure. Though, a malicious node might decline to forward convinced messages as well as just drop them, make certain to they are not broadcast any additional[8]. This type attack be able to detected but packet order numbers are check properly and continuously in a combination free network. Accumulation of information packet order number in packet identification can reduce this attack. Figure 4.1 and 4.2 shows situation of selective forward attack. In figure 4.1, foundation node "S" ahead's its information packet D1, D2, D3, D4 to node "A" as well as node "A" onwards these established packets towards node "B". During other furnish an opponent node "AD" selectively forwards the packets D1, D3 even as reducing packet D2 in addition to D4[8]. Inside another situations exposed in figure 4.2, an opponent might selectively go down packets initiate from single source in addition to onward that of others.

According to the research by authors Narendra Kumar Patel, Gaurav Singal [16] routine of the LEACH protocol is appraise with the selective forwarding attack by Network Simulator. It been experimental that how the delivered packets are affected, what time numerals of malevolent nodes enlarge. Once the detection moreover removal of malevolent nodes once more delivery ratio of the packet is calculated.

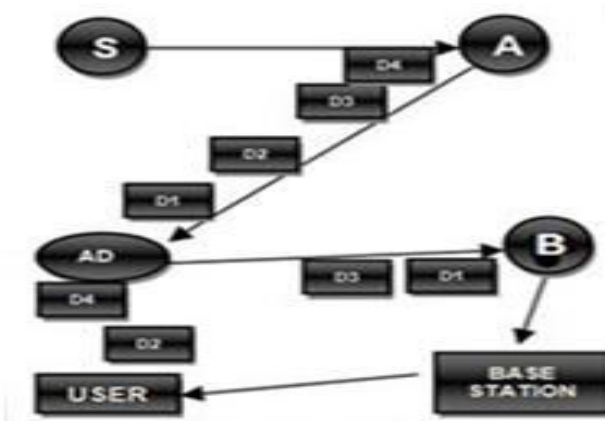

Figure 4.1: Adversary Drop Selected Packet of Node

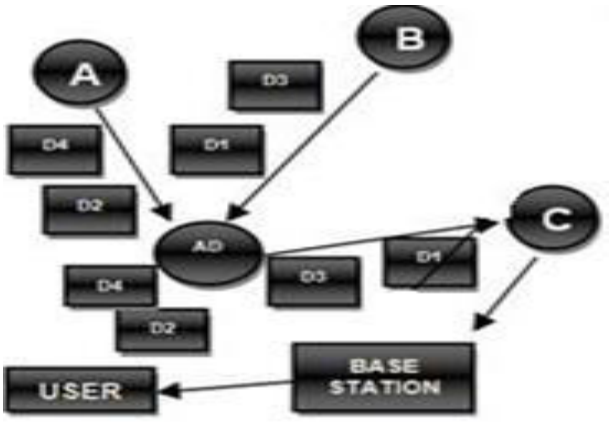

Figure 4.2: Adversary Drop All From Selected Node

They experimental that as projected quantity of cluster heads altered from 5 near 10, packet release is reduce for together 100 sensor nodes in the network along with 200 sensor nodes in the network. Which is also experimental that for far above the ground power networks packet launched be more than small energy networks in every case.

According to the technique K. Sophia et al[17] have projected a federal intrusion detection method supported on Support Vector Machines (SVMs) also have worn sliding porthole used for selective forwarding and black hole attacks. In this exacting scheme they simply notice the attacks. They as well claimed to, this is the primary attempt to be relevant SVMs as a explanation in WSN security. This method elevate alarm based on top of the 2D characteristic vector like bandwidth, hop count by means of routing in sequence restricted to the base position of network. Their method can notice black hole attacks by means of 100% accurateness and selective forwarding attacks by means of 85% accurateness. In this plan intrusion detection be achieve in the base position and therefore the nodes make use of no power to support this by additional security feature. Method detects the malicious node with the exception of identify it.

In the paper "Detecting sink hole and selective forwarding attack in wireless sensor networks" [18], authors presented an efficient method for recognize selective forwarding attacks inside a wireless sensor network through initiating the lightweight proposal described as Traffic Monitor Based Selective Forwarding Attack Detection Scheme. This procedure uses EM nodes to observe every traffic of the sensor network. EM node which eavesdrops every traffic within the sensor network, along with if the evaluation is BS after that EM node produce the information are Node ID, Source ID, Next Hop ID towards the TMBSFD described as Traffic Monitor Based Selective Forwarding Attacks Detector. The simulation consequences show the resourceful detection of selective forwarding attacks in the WSNs. We realize detection through 100% entirety and fewer percentages of forged positive rates.

In the paper "Hop-by-Hop Cooperative Detection of Selective Forwarding Attacks in Energy Harvesting Wireless Sensor Networks"[19], authors have examine a countermeasure toward selective forwarding attack within power harvesting WSNs. They first examine four adversarial situation based on top of an implied acknowledgment eavesdropping and after that projected a Hop-by-hop Cooperative Detection (HCD) method to competently sense promote misbehaviors. To perceive the full possible of the projected techniques. On behalf of that an example, extra than two malevolent nodes are successively located all along a onward pathway to go under the surface, or else surround a further. They arranged to think about six adversarial situations and recognize their susceptible cases, examine any onward misbehavior, as well as expand the projected HCD scheme.

In the paper" Detecting selective forwarding attacks in wireless sensor networks "[5], authors have intended a simple and proficient security method for sense selective forwarding attacks. Different common move toward in which discovery is realize in the base position otherwise in a innermost organizer, Their method get together the base position with the foundation nodes encompass the ability to notice selective forwarding attacks. Accordingly, even after the base location is for the time being deafened through adversaries, attacks preserve still exist detected. Within the future effort, they planned to put together the jamming discovery techniques with their scheme, therefore the original source of the abnormal packet defeat be able to find out.

V. CONCLUSION

Wireless Sensor Networks are susceptible to numerous kinds of attacks suitable to operation of sensor nodes in unattended surroundings. These kinds of networks are undergo beginning the misbehavior nodes kinds of attacks like selective forwarding and black hole attack as present is no federal security administration. In this survey, firstly it contains the introduction to the WSN. Next, presented some of the security attacks in WSNs. This survey which furthermore gives the different presented techniques used for the detection and the prevention of the selective forwarding and the black hole attacks. It is to be believed that this survey will help prospect researches in developing a superior knowledge regarding the attacks and their contradict measures.

REFERENCES

[1]. Nitesh Gondwal, Chander Diwaker, " Detecting B lack hole attacks in WSN by check agent using multiple base stations" American International Journal of Research in Science, Technology, Engineering & Mathematics, 3(2), June-August, 2013, pp. 149-152.
[2]. Chunnu Lal, Akash Shrivastava, " An energy preserving detection mechanism for black hole attack in wireless sensor network" International Journal of Computer Applications (0975 – 8887) Volume 115 – No. 16, April 2015.
[3]. Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal and Kashif Naseer Qureshi "A Survey of Wireless Sensor Network Security and Routing Techniques " Research Journal of Applied Sciences, Engineering and Technology 9(11): 1016-1026, 2015 ISSN: 2040-7459; e-ISSN: 2040-7467.
[4]. Dr. Deepali Virmani 1, Manas Hemrajani 2, Shringarica Chandel3 " Exponential trust based mechanism to detect black hole attack in wireless sensor network" Bhagwan Parshuram Institute of Technology 2012.
[5]. Bo Yu, Bin Xiao " Detecting selective forwarding attacks in wireless sensor networks" IEEE,1-4244-0054-6/06/$20.00 ©2006.
[6]. Teodor-grigore lupu "Main Types of attacks in wireless sensor networks" Recent Advances in Signals and Systems, ISSN: 1790-5109, 2010.
[7]. Kai Xing , Shyaam Sundhar Rajamadam Srinivasan , Manny Rivera , Jiang Li , Xiuzhen Cheng "Attacks and countermeasures in sensor networks: A survey" NETWORK SECURITY Scott Huang, David MacCallum, and Ding Zhu Du(Eds.) pp.2005 Springer.
[8]. Usham Robinchandra Singh, Sudipta Roy, Herojit Mutum " A survey on wireless sensor network security and its countermeasures: an overview" International Journal of Engineering Science Invention ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726, 2013.

[9]. Weiping Wang1, Shigeng Zhang, Guihua Duan, and Hong Song, “security in wireless sensor networks." Wireless Network Security© Higher Education Press, Beijing and Springer-Verlag Berlin Heidelberg 2013.
[10]. Mehreen Shaikh, Abid. H Syed, " A survey on jamming attacks, detection and defending strategies in wieless sensor networks" International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308,Mar 2014.
[11]. Leela Krishna Bysani, Ashok Kumar Turuk, "A survey on selective forwarding attack in wireless sensor networks"978-1-4244-9190-2/11,IEEE,2011.
[12]. Gaurav Gulhane, Nikita Mahajan, " Performance evaluation of wireless sensor network under black hole attack" IJCAT International Journal of Computing and Technology, Volume 1, Issue 3, April 2014.
[13]. Zdravko Karakehayov " Using REWARD to detect team black hole attacks in wireless sensor network" University of Southern Denmark Mads Clausen Institute Grundtvigs Alle 150, DK-6400 Sønderborg, Denmark,2010.
[14]. R. Tanuja, M. K. Rekha, S. H. Manjula, K. R. Venugopal, S. S. Iyengar and L. M. Patnaik " Elimination of black hole and false data injection attacks in wireless sensor networks" Proceedings of the Third International Conference on Trends in Information, Telecommunication and Computing, Lecture Notes in Electrical Engineering 150, DOI: 10.1007/978-1-4614-3363-7_55, Springer Science+Business Media New York 2013.
[15]. Siddiq Iqbal, Aravind Srinivas S P, Sudarshan G, Sagar S Kashyap " Effect of black hole attack on single hop and multihop leach protocol"Aravind Srinivas S P et al Int. Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 4, Issue 5(Version 7), May 2014, pp.75-78.
[16]. Narendra Kumar Patel , Gaurav Singal , " Selective forwarding attack in leach in wsn"International Journal of Electronics, Electrical and Computational System IJEECS ,2014,Volume 1, Issue 1.
[17]. Sophia Kaplantzis , Alistair Shilton , Nallasamy Mani , Y. Ahmet S¸ekercioglu, "Detecting selective forwarding attacks in wireless sensor networks using support vector machines" IEEE,2007.
[18]. Umashri Karkikatti, Nalini N" Detecting sink hole and selective forwarding attack in wireless sensor networks" International Journal of Science and Research (IJSR),Volume 3 Issue 6, June 2014.
[19]. Sunho Lim, Lauren Huie, " Hop-by-Hop Cooperative Detection of Selective Forwarding Attacks in Energy Harvesting Wireless Sensor Networks" IEEE, 2015.