Volume 7, Issue 4, April 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Blackhole Attack Detection Techniques in WSN: A Review

Er. Mandeep Thakur
M.tech Scholar, Deptt.of CSE, Punjabi University
Regional Centre for Information Technology and Management, Mohali, Punjab, India

Asst. Prof. Amninder Kaur
Deptt.of CSE, Punjabi University
Regional Centre for Information Technology and Management, Mohali, Punjab, India

Abstract: ***The wireless sensor network is the decentralized type of network, the size of the sensor networks is very small due to which battery power of the nodes is limited. Due to self configuring nature of the wireless sensor networks, various type security attacks are possible in the network. The security attacks are broadly classified into active and passive attacks. The blackhole attack is the active type of attack which reduced the network efficiency in terms of various parameters. In this paper, various techniques has been reviewed which detect and isolate malicious nodes from the network***

Keywords: NDFD, AODV, TBESP

I. INTRODUCTION TO WSN

The wireless sensor networks are formed by the collection of nodes which are geographically distributed. These networks are used in applications which involve the monitoring of fields that have environmental pollution, vehicle safety, building safety, warehouse inventories, health of patients, etc. Due to evolutions in technology as well as increase in demand of the wireless sensor networks there is a need to enhance the properties of nodes. The wireless medium is used for communication or data transmission among the nodes [1]. The wireless medium may either of radio frequencies, infrared or any other medium, of course, having no wired connection. These nodes are deployed in a random fashion and they can communicate among themselves to make an ad-hoc network [2]. If the node is not able to communicate with other through direct link, i.e. they are out of coverage area of each other; the data can be sending to the other node by using the nodes in between them. This property is referred as multi-hoping [3]. All sensor nodes work cooperatively to serve the requests. Generally WSNs are not centralized one as there is peer-to-peer communication between the nodes. So there is no requirement of prior established infrastructure to deploy the network.

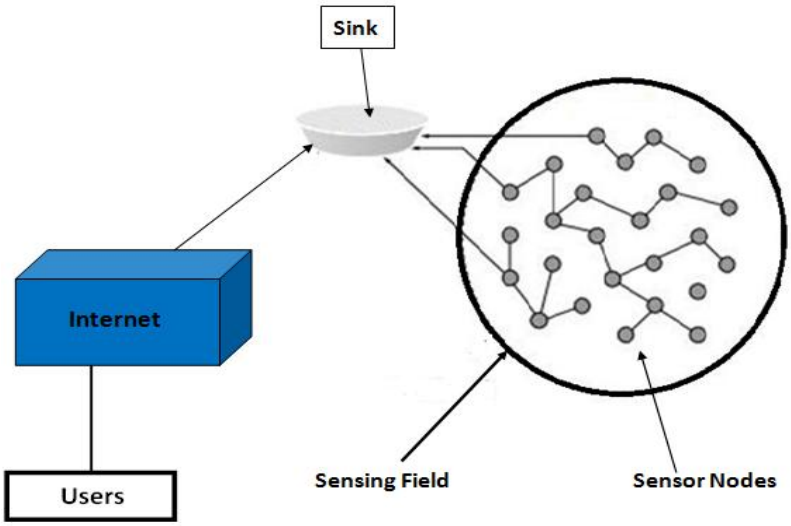

Figure.1.1 Structure of Wireless Sensor Network

Challenges of WSN

- Routing : Routing is the exchange of information from one station of networks to other and Protocol is the set of standard or rules to exchange data between two devices. Such protocols deals with the typical limitations of these networks, which include high power consumption, high error rate, low bandwidth. The routing protocols are classified as:- (a) Table driven (Proactive) (b) On-demand driven (c) Hybrid protocols.
- Qos : The QoS must system be able to manage several simultaneous services with a specific response time limitation for each service

The QoS system must supply service differentiation in the service provider to the consumer –consumer category

- Security : Security concerns arising because both customer data and program are residing at provider Premises. Security is always a major concern in Open System Architectures
- Calibration: Calibration is the process of adjusting the raw sensor readings obtained from the sensors into corrected values by comparing it with some standard values. Manual calibration of sensors in a sensor network is a time consuming anddifficult task due to failure of sensor nodes and random noise which makes manual calibration of sensors too expensive .
- Deployment: Deployment means implementing the wireless sensor network in real world location. It is very laborious and cumbersome activity and depends on the demographic location of the application that how network will be deployed. At locations which are hard to reach, sensors are dropped from helicopter or may be in some locations sensors are placed according to
- some topology. Energy management issues like
- battery recharge and changing are challenges in real
- world scenarios. Deployment of sensor networks
- results in network congestion due to many
- concurrent transmission attempts made by several
- sensor nodes. Low data yield is a problem in real
- world scenario as network delivers insufficient
- amount of information.

II. SECURITY ATTACKS

Any action that compromises the security of information owned by an organization information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems often *threat* & *attack* used to mean same thing have a wide range of attacks.

Generic types of attacks

- passive
- active

A. Passive attack

A passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted.

Two types of passive attacks are:

- Release of message contents
- Traffic analysis

B. Active attack

Active attacks involve some modification of the data stream or the creation of a false stream. Active attacks can be subdivided into four categories:

- Masquerade,
- Replay,
- Modification of Messages
- Denial of Service.

III. BLACK HOLE ATTACK

An attack caused by an external adversary on a subset of sensor nodes in a network is known as a black hole attack. The nodes are captured and re-programmed by the adversary such that they do not transmit the data packets. These involve the packets that are generated by them or the ones from the sensor nodes which are to be forwarded. The nodes that are re-programmed are known as black hole nodes and the region which holds such nodes is known as the black hole region.

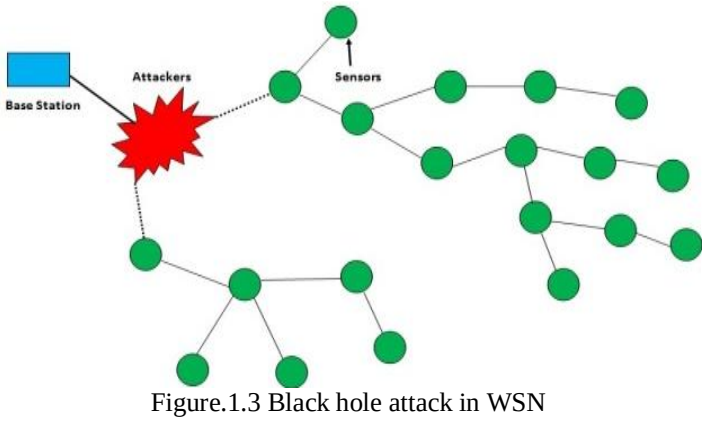

Figure.1.3 Black hole attack in WSN

As seen in the figure, the small circles seen are the sensor nodes and the region holding them is the black hole region. If a path is selected such that the attacker node is involved in it, then as the traffic passes through the adversary node present in it, the nodes start dropping the packets in a selective manner or as a whole. The re-programmed nodes are known as the black hole nodes and the region holding them is called the black hole region. This region is an entrance to a large number of attacks [11]. The activities in the network are affected a lot by the attacks and the packet loss, and delay factors increase however, the throughput of the network decreases.

IV. REVIEW OF LITERATURE

Taylor Vincent F, Fokum Daniel T discussed [1] Wireless sensor networks comprise of autonomous, self-organizing, low-power nodes which cooperatively measure data in an environment and cooperate to route this data to its intended destination. Black hole attacks are potentially devastating attacks on wireless sensor networks in which a malicious node utilizes spurious route updates to attract network movement that it then drops. We propose a robust and flexible attack detection scheme that uses a watchdog mechanism and lightweight expert system on every node to detect anomalies in the behavior of neighboring nodes. Utilizing this scheme, regardless of the possibility that malicious nodes are inserted into the network, great nodes will have the capacity to identify them based on their behavior as inferred from their network activity. We examine the resource-preserving mechanisms of our system utilizing simulations and demonstrate that we can allow groups of nodes to all in all evaluate network activity and identify attacks while regarding the limited hardware resources (handling, memory and capacity) that are typically accessible on wireless sensor network nodes.

Binod Kumar Mishra et.al presented [2] that wireless sensor network comprises of topographically dispersed autonomous sensors to monitor and control over physical or environmental conditions, similar to temperature, sound, pressure and so forth and this information is passed through sensors in the network to a next location. Military applications was required the development of security in wireless sensor networks. Today such networks are utilized as a part of many areas like industrial, health, and commercial applications. Black hole attack is happens, when an intermediary captures and re-programs a set of nodes in the network to block/drop the packets and generates false messages instead of forwarding correct/true information towards the base station in wireless sensor network. Close-by many techniques have been proposed in the literature for detection and prevention of black hole attack in sensor network. There are different solutions proposed in the literature which identifies black hole attack and gives successful delivery of data to the base station.

Yingpei Zeng et.al suggests [7] that Wireless sensor networks (WSNs) deployed in hostile environments are vulnerable to clone attacks. In such attack, an adversary compromises a couple of nodes, replicates them, and inserts subjective number of replicas into the network. Thusly, the adversary can complete many internal attacks. Past solutions on detecting clone attacks have a few drawbacks. Initially, some of them require a central control, which introduces a few inherent limits. Second, some of them are deterministic and vulnerable to simple witness compromising attacks. Third, in a few solutions the adversary can without much of a stretch take in the critical witness nodes to start smart attacks and protect replicas from being detected. In this paper, we first demonstrate that keeping in mind the end goal to abstain from existing drawbacks, replica-detection protocols must be non-deterministic and completely circulated (NDFD), and fulfill three security requirements on witness selection. To our knowledge only one existing protocol, randomized multicast is NDFA and satisfy what we require,even having communication overhead. At that point, based on random walk, we propose two new NDFD protocols, RAndom WaLk (RAWL) and Table-assisted RAndom WaLk (TRAWL), which fulfill the requirements while having just moderate communication and memory overheads. The random walk strategy outperforms past strategies since it distributes a center stride, the witness selection, to each passed node of random walks, and after that the adversary can't without much of a stretch discover the critical witness nodes. We theoretically analyze the required number of walk steps for ensuring detection. Our simulation results demonstrate that our protocols outperform an existing NDFD protocol with the lowest overheads in witness selection, and TRAWL even has lower memory overhead than that protocol. The communication overheads of our protocols are higher yet are affordable considering their security benefits.

Ngai, E.C-H et.al describe [8] that In a wireless sensor network, multiple nodes would send sensor readings to a base station for further handling. It is notable that such a many-to-one communication is highly vulnerable to the sinkhole attack, where an intruder attracts encompassing nodes with unfaithful routing information, and after that performs selective forwarding or modifies the data passing through it. A sinkhole attack forms a serious danger to sensor networks, particularly considering that such networks are regularly deployed in open areas and of frail computation and battery power. In this paper, we introduce a novel algorithm for detecting the intruder in a sinkhole attack. The algorithm first finds a rundown of suspected nodes, and after that viably identifies the intruder in the rundown through a network flow graph. The algorithm is likewise robust to deal with cooperative malicious nodes that attempt to hide the real intruder. We have evaluated the performance of the proposed algorithm through both numerical analysis and simulations, which confirmed the effectiveness and precision of the algorithm. Our results likewise suggest that its communication and computation overheads are reasonably low for wireless sensor networks.

Chun–Hsin Wang and Yang-Tang Li suggests [12], In mobile specially appointed networks (MANET), network security problems emerge in an endless stream. For instance, malicious nodes may get to be distinctly quick nodes of routing paths first by answering satire routing information. At that point data packets may be stolen, modified, and even dropped by malicious nodes. These sorts of behavior interfere or interrupt communication between nodes, squandering superfluous bandwidth resource. In the literature, there exists many works on taking care of malicious nodes problems in

MANET. The majority of proposed solutions need to adjust unique routing protocols or include new protocols. It's difficult to be practicable for real-world deployment. In this paper, we proposed another strategy to detect malicious nodes actively. Without modifying or including routing protocols, just few pairs of detection nodes are required, which can identify and isolate malicious nodes. In our simulation, the results demonstrate that packets delivery rate can be enhanced 17% by one sets of detection nodes and the average additional overhead of every node is just increased by 0.1 KB/s.

Medadian Mehdi et.al describes [13] that, a mobile specially appointed network (MANET) is an autonomous network that comprises of mobile nodes that speak with each other over wireless connections. Without a settled foundation, nodes need to cooperate so as to give the fundamental network functionality. One of the principal routing protocols utilized as a part of Ad hoc networks is AODV (Ad hoc on request Distance Vector) protocol. The security of the AODV protocol is threaded by a particular sort of attack called `Black Hole' attack. In this attack a malicious node advertises itself as having the shortest path to the destination node. To combat with black hole attack, it is proposed to wait and check the replies from all the neighboring nodes to locate a protected route yet this approach suffers from high delay. In this paper, an approach is proposed to combat the Black hole attack by utilizing negotiation with neighbors who claim to have a route to destination. the Simulation's results demonstrate that the proposed protocol gives better security furthermore better performance in terms of parcel delivery than the conventional AODV in the presence of Blackholes with minimal additional delay and Overhead.

Mohammad Wazid et.al suggest [14], Wireless Sensor Network comprises of extensive number of sensor nodes with limited battery power, which are randomly deployed over certain area for a few applications. Wireless Sensor Network (WSN) has an awesome potential to be deployed in extensive variety of applications like consumer, industrial and defense sectors. WSN s are susceptible to different attacks, in which Blackhole a sort of Denial of Service (DoS)attack is exceptionally hard to detect and defend. In blackhole attack, an adversary captures and re-programs a set of nodes in the network to block the packets they receive instead of forwarding them towards the base station. Subsequently any information that enters the blackhole locale is caught and doesn't achieve the destination. Because of this attack, high end-to-end delay is introduced in the network and performance of the network (i.e. throughput) is debased. In this paper a near performance analysis of two WSN's topologies i.e. Tree and Mesh under blackhole attack is finished. On the off chance that there is a WSN inclined to blackhole attack and requires time efficient network service for information exchange then Tree topology is to be chosen. In the event that it requires throughput efficient and consistent service in the network then Mesh topology is recommended. An algorithm named as Topology Based Efficient Service Prediction (TBESP) algorithm has been proposed depending upon the analysis done which will help in choosing the most appropriate topology according to the network service requirement under blackhole attack.

Mukesh Tiwari et.al discussed [15] wireless sensor networks (WSNs) are being deployed every now and again in assortment of environments, for example, military surveillance, forest fire monitoring, chemical leakage monitoring and so forth. Sensor nodes have limited communication capability and low computation resources so every node is powerless entity that can be effectively compromised by adversary by launching malicious software inside the network. Performance evaluation of wireless sensor network requires realistic demonstrating of Intrusion detection system since the vast majority of WSNs are application particular. In WSN, nodes have particular properties, for example, stable neighbors' information that aides in detection of anomalies in network. Nodes monitor their neighborhood and collaborate with cluster head to detect malicious behavior. Despite the fact that nodes don't have worldwide view however they can at present detect an intrusion with certain probability and report to cluster head. This paper introduces a specification based Intrusion Detection System for wireless sensor networks.

Samir Athmani et.al presented [16] because of their particular characteristics, wireless sensor networks (WSN) are extremely vulnerable to malicious attacks. Black hole is a standout amongst the most malicious attacks that target sensors routing protocols. This sort of attacks can have devastating effect on hierarchical routing protocols. A few security solutions have been proposed to secure WSNs from black hole attacks. In any case, a large portion of these solutions are complex and energy inefficient. In this paper they propose a hierarchical energy efficient intrusion detection system, to protect sensor network from black hole attacks. Their approach is simple and based on control packets exchange between sensor node and base station. They have experimentally evaluated our system utilizing the NS simulator to demonstrate its effectiveness in detecting and preventing efficiently the black hole attacks.

V. CONCLUSION

In this paper, it is been concluded that wireless sensor networks is the decentralized type of network in which sensor nodes sense the environmental conditions and pass the information to base station. Due to decentralized nature of the network various type of active and passive attacks are possible which reduce network performance. The blackhole attack is the active type of attack which reduce network performance in terms of various parameters. In this paper, various techniques which are used for detection of malicious nodes are reviewed and discussed in terms of various parameters.

REFERENCES

[1] Taylor Vincent F, Fokum Daniel T "Mitigating Black Hole Attacks in Wireless Sensor Networks Using Node-Resident Expert Systems", Washington, DC,pp.1-7,IEEE,2014.

[2] Mishra Binood Kumar,Nikam Mohan C,Lakkadwala Prashant," Security Against Black Hole attack in wireless Sensor Network –A Review",2014 Fourth International Conference on communication System and Network Technologies, IEEE Computer Society Washington, DC, USA, pp.615-620, IEEE 2014.

[3] Mudasser Iqbal, "An Energy-Aware Dynamic Clustering Algorithm for Load Balancing in Wireless Sensor Networks",Journal of Communications,vol.1,no.3,pp. 10-20, June 2006.

[4] Sharma Amita, Wadhwa Yogita, Aggarwal Ankit,International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 1,pp. 336 January2013.

[5] Corke Peter, Wark Tim, Jurdak Raja, Hu Wen, Valencia Philip, Moore Darren," Environmental Wireless Sensor Networks" Vol. 98, No. 11, pp.1903-1917,November IEEE 2010.

[6] Kaur Avrinderpal,Garg upasna,Enhanced Cluster Based Distributer Fault Tolerance Algorithm for Mobile Node in WSN" (IJECS),Volume 3,Issue 10 , pp.8487-8492,October 2014.

[7] Zeng Yingpei, Cao Jiannong, Zhang Shigeng, Guo Shanqing and Xie Li "Random-walk based approach to detect clone attacks in wireless sensor networks vol.28, no.5, pp.973-691,June 2010, IEEE Journal.

[8] Edith C. H. Ngai, Jiangchuan Liu and Michael R. Lyu; "On the Intruder Detection for Sinkhole attack in Wireless Sensor Networks" IEEE International Conference on Communications, Volume 8, pp. 3383-3389, IEEE 2006.

[9] Shree Raj, Khan R. A." Wormhole Attack in Wireless Sensor Network" International Journal of Computer Networks and Communications Security Vol.2, No.1, pp. 22–26,January 2014.

[10] LV Shaohe,Wang Xiaodong, Zhao Xin, Zhou Xingming, " Detecting the Sybil Attack Cooperatively in Wireless Sensor Networks",Computational Intelligence and Security 2008, CIS '08 International Conference on Volume 1Suzhou,pp.442-446,IEEE 2008.

[11] Baviskar B.R, Patil V.N, "Black hole attacks mitigation and prevention in wireless sensor network" International Journal of Innovative Research in Advanced Engineering (IJIRAE), Volume 1 ,Issue 4, pp.167-169,May 2014.

[12] Wang Chun-Hsin and Li Yang-Tang, "Active Black Holes Detection in Ad-Hoc Wireless Networks", Ubiquitous and Future Networks (ICUFN) 2013 Fifth International Conference on Da Nang, pp.94-99, IEEE, 2013.

[13] Mehdi Medadian, Ahmad Mebadi, Elham Shahri, "Combat with Black Hole Attack in AODV Routing Protocol", Proceedings of the 2009 IEEE 9th Malaysia International Conference on Communications, 15 -17 December 2009, Kuala Lumpur Malaysia, IEEE 2009.

[14] Wazid Mohammad, Katal Avita, Goudar R H,"TBESP Algorithm for Wireless Sensor Network under Blackhole Attack",International conference on Communication and Signal Processing, April 3-5, 2013, India, pp.1086-1091, IEEE 2013.

[15] Tiwari Mukesh, Arya Karm Veer, Choudhari Rahul, Kumar Sidharth Choudhary," Designing Intrusion Detection to Detect Black hole and Selective Forwarding Attack in WSN based on local Information", Fourth International Conference on Computer Sciences and Convergence Information Technology on Seoul, pp.824-828,IEEE 2009.

[16] Samir Athmani, Djallel Eddine Boubiche and Azeddine Bilami,"Hierarchical Energy Efficient Intrusion Detection System for Black Hole Attacks in WSNs",Computer and Information Technology (WCCIT), 2013 World Congress on Sousse,pp.1- 5,IEEE,2013.

[17] Virendra Pal Singh Sweta Jain and Jyoti Singhai,"Hello Flood Attack and its Countermeasures in Wireless Sensor Networks", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 11, pp.227,May 2010.

