International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 11
July 2016

A Study on Sink Hole attacks in a Wireless Sensor Network

Jaidev Dhanoa
Research Scholar
Sri Guru Granth Sahib World University

Mrs. Sukhpreet Kaur
Assistant Professor
Sri Guru Granth Sahib World University

Abstract- *Wireless sensor network is a branch of networking that deals with sensing of information from deployed area. Sensor nodes collect the information by sensing and transmit using sink nodes. Sink nodes collects the information from sensor nodes and transmit this information to base station. Transmission of data from sources to destination using various routing and off-demand routing techniques. A sink hole attack is performed on sink nodes, attacking node replaces the actual sink node by advertising its availability and resumes all the data from the sensor node. The actual data is not received at the base station, which results in the loss of the information from the network.*

Keywords-Wireless sensor network, Sinkhole attack, Rule based, Hybrid based intrusion detection.

1. INTRODUCTION

1.1 Wireless sensor network

A wireless sensor network is a gathering of specific transducers with a correspondences foundation for observing and recording conditions at diverse areas. Generally checked parameters are temperature, humidity, weight, wind direction and velocity, enlightenment force, vibration power, sound force, force line voltage, substance focuses, pollutant and basic body capacities. A sensor system comprises of various detection stations called sensor nodes, each of which is little, lightweight and versatile. Each sensor node is outfitted with a transducer, microcomputer, handset and force source. The transducer produces electrical signs focused around sensed physical impacts and phenomena. The microcomputer courses of action and stores the sensor yield. The handset gets charges from a focal PC and transmits information to that PC. The power for every sensor node is gotten from a battery [2].

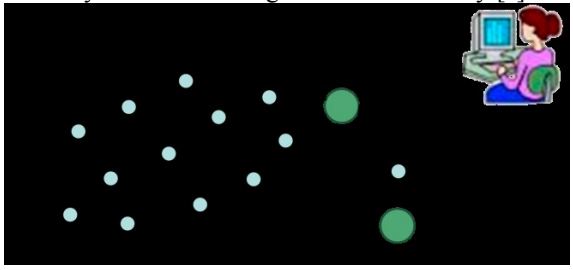

Figure 1: Wireless Sensor Network [11]

A Wireless Sensor Network Mobile communications and wireless networking technology has seen a third time advancement. In technological advancements and also in application demands various classes of communication networks have combined like Cellular networks, Ad hoc Networks, Sensor Networks and Mesh Networks. Cellular network depend upon infrastructure. Ad hoc networks are comes in the category of wireless networks that organize multi hop radio relaying when the nodes are dynamically and arbitrarily located. Ad-hoc network are does not depend upon network. Nodes measure the ambient conditions in the environment surrounding them. These measurements include signal transformation that can be processed to show some characteristics about the phenomenon. The data collected is routed to sink node which is very special node .Then by using internet or satellite the sink node send data to user, through a gateway [5].

1.2 Routing Protocols in WSN

1.2.1 Location-based Protocols: In this protocol the sensor nodes tends to use location information to guide routing discovery as well as data forwarding, transmissions of the information and avoiding information loss in the entire network. Area data is needed for the sensor nodes to sense organizes but the greater part of the steering conventions to compute the separation between two specific nodes so that vitality utilization can be evaluated. In this segment, we display a specimen of area mind full routing protocols proposed for WSNs [6].

1.2.2 Data Centric Protocols: Data-centric protocols contrast from traditional address-centric protocols in a way that the information is sent from source sensors to the sink. In address-centric protocol each of the source sensors that have the proper information reacts by sending its information to the sink free of all different sensors. In data-centric protocols, when the source sensors send their information to the sink, halfway sensors can perform some manifestation of collection on the information starting from different source sensors and send the totaled information around the sink. This procedure can bring about

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 11
July 2016

vitality funds due to less transmission needed to send the information from the sources to the sink.

1.2.3 Mobility-based Protocols: Mobility brings new difficulties to routing protocols in WSNs. Sink versatility requires energy efficient protocols to ensure information conveyance started from source sensors to portable sinks [7].

1.2.4 Multipath-based Protocols: Considering information transmission between source sensors and the sink, there are two routing paradigms: single-way routing and multipath routing. In single-way routing, each one source sensor sends its information to the sink by means of the briefest way. In multipath routing, each one source sensor finds to start with k-shortest ways to the sink and partitions its heap evenly among these ways.

1.3 Attacks in WSN

There are various kinds of attack that can affect the entire system or can degrade the performance of system. The attacks can be categorized into following types:

1.3.1 Black hole Attack

When some malicious user enter into the network and stop forwarding messages to next nodes by dropping messages are called as black node.

1.3.2 Grey hole Attack

This attack occurs if some node dropping 50% of the packets and rest 50% is sending by altering the message. In this way wrong information is broadcast.

1.3.3 Sink hole Attack

In a sinkhole attack, the enemy's point is to bait about all the activity from a specific range through a traded off node, making an allegorical sinkhole with the enemy at the middle. Sinkhole assaults commonly work by making a traded off node look particularly appealing to encompassing nodes concerning the directing calculation. Sinkhole attacks are hard to counter on the grounds that directing data supplied by a node is hard to confirm. As an example, a laptop class foe has a solid force radio transmitter that permits it to give a transmitting so as to amaze course with enough power to achieve a wide region of the network [1].

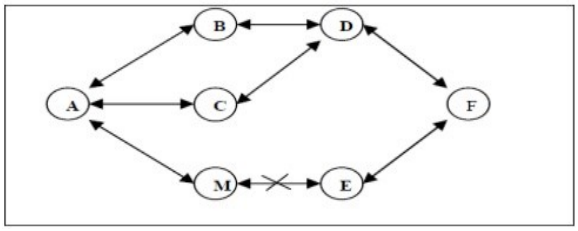

Figure 1.3: Sink Hole Attack [11]

This is another clarification of sinkhole attack in wireless sensor network and this time the attack is propelled under TinyAODV (Ad-hoc On Demand Vector) protocol. TinyAODV protocol is the same as AODV in MANET however this one is lighter contrasted with AODV and it was altered deliberately for wireless sensor network. The quantity of hops to base station is the steering metric that utilized as a part of this protocol. For the most part the course from source to destination is made when one of the nodes send a solicitation, the source node sends a RREQ (Route ask for) parcel to his neighbors when needs to send packets. Next one of the neighbors near destination is answer by sending back RREP (Route Reply) parcel, [3] if not the packet is sent to different nodes near that destination. At long last, the source gets RREP parcel from neighbor then select one node with less number of jumps to destination. The sinkhole node or traded off node dispatches an assault by send back RREP packet. In RREP packet it gives little number of hops which shows close vicinity to the base station. At that point the source node chooses to forward packet to sinkhole node. The bargained node then performs the same system to its whole neighbors and tries to pull in however much activity as could reasonably be expected.

Case in point, Fig 1.2 shows node M dispatches sinkhole attack in Tiny AODV. Node A sends RREQ to node BCM. However node M rather than telecast to node E like nodes B and C does to node D, he answers back RREP to node A. At that point node A will dismiss node B and C, then forward packets to M since node A and B are extremely far to F contrast with node M.[4].

2. APPROACHES USED

2.1 Rule based

The rules are designed based on the behaviour or technique used to launch sinkhole attack. Then those rules are imbedding in intrusion detection system which runs on each sensor nodes. Those rules were then applied to the packet transmitted through the network nodes. If any node violates the rules is considered as adversary and isolated from the network. In it used rule based approach to detect sinkhole attack. They create two rules and implanted in Intrusion detection system (IDS). When one of the rules is violated by one of the nodes, the intrusion detection system triggered an alarm but it does not provide node ID of compromised node. The first rule "for each overhead route update packet the ID of the sender must be different your node ID". The second rule "for each overhead route update packet the ID of

the sender must be one of the node ID in your neighbours". There are two rules, the first rule "rule for each overhead route update packet the ID of the sender must be one of node ID in your neighbours". The second rule "for each pair of parent and child node their link quality they advertise for the link between them, the difference cannot exceed 50.

2.2 Anomaly-based detection

In anomaly based detection the normal user behaviour is defined and intrusion detection is searching for anything that is anomalous in the network. In this method intrusion is considered as anomalous activity because it looks abnormal compare to normal behaviour. The rule based and statistical approaches are also included under anomaly based detection approach. The RSSI (Received Signal Strength Indicator) is value with the help of EM (Extra Monitor) nodes to detect sinkhole attack. The EM had high communication range and one of their functions is to calculate RSSI of node and send to base station with ID of source and next hop. This process happens instantly when node are deployed. Base station uses that RSSI value to calculate VGM (visual geographical map). That VGM shows the position of each node, then later when EM send updated RSSI value and base station identify there is change in packet flow from previous data this indicate there is sinkhole attack. The compromised node is identified and isolated from the network by base station using VGM value. However, if attack is launched immediately after network deployment, the system will not be able to detect that attack. Also the numbers of EM nodes were not specified for specific number of sensor nodes and the proposed method is focused only on static network. [2]

2.3 Hybrid based intrusion detection

The combination of both anomaly and signature based or misused based is used in this approach. The false positive rate which produced by anomaly based is reduced in this approach due to the use of both method. Also the advantage of this approach is to be able to catch any suspicious nodes which their signature is not included in detection database. Coppolino and Spagnuolo proposed hybrid Intrusion detection system to detect sinkhole attack and other attacks. They used detection agent which was responsible for identifying sinkhole attack. The hybrid intrusion detection was attached to sensor node and share resource of that node. The suspicious nodes were inserted to the blacklist based on anomalous behaviour after analyzed the collected data from neighbours. Then that list is sent to central agent to make final decision based on feature of attack pattern (misused based). It was designed for static wireless sensor network. [6]

2.4 Message Digest Algorithm

Detection of sinkhole attack in wireless sensor networks using message digest algorithms. The main goal of the protocol is to detect the exact sink hole using the one-way hash chains. In the proposed method destination detects the attack only when the digest obtained from the trustable forward path and the digest obtained through the trustable node to the destination are different. It also ensures the data integrity of the messages transferred using the trustable path. The algorithm is also robust to deal with cooperative malicious nodes that attempt to hide the real intruder. [3]

S.No.	Method	Advantages	Disadvantages	Related Papers
1	**Rule based**	Highly flexible middleware architecture able to provide support for a wide range of different applications. uses only single-hop communication, thus permitting very simple node failure detection and message reliability assurance mechanisms	Only response to received events so doesn't work on its own.	
2	**Anomaly-based detection**	Benefits it generates like increasing the rule set helps in less false positive alarms.	Main drawback is defining its rule set. The efficiency of the system depends on how well it is implemented and tested on all protocols	2
3	**Hybrid based intrusion detection**	The technique has random forest classification algorithm is used to achieve high speed.	The performance level of anomaly detection tends to be reduced, due	6

		Accuracy of technique is also high.	to a large number of connections.	
4	**Using Message Digest Algorithm**	Ensures the data integrity of the messages transferred using the trustable path.	Detects the attack only when the digest obtained from the trustable forward path and the digest obtained through the trustable node to the destination are different	3

3. REVIEW OF LITERATURE

Ahmad Salehi S. et.al.[1] "Detection of Sinkhole Attack in Wireless Sensor Networks" In this paper Author proposed a communication approach for data gathering. This approach is very risky to sinkhole attack, where an burglar attacker attack surrounding nodes with fake routing information. For finding the attacker in an sinkhole attack author used an algorithm which is firstly find the group of doubted nodes on the basis of consistency of data then the attacker is find efficiently in that group by checking the network flow. Therefore, accuracy and efficiency of algorithm would be verified.

A. Balakrishnan et. al [2] "A Novel Anomaly Detection Algorithm for WSN" Now these days energy consumption become a big issue in wireless sensor network. WSN is easily affected by various types of attacks and nodes compromises. There are many systems intrusion detection system (IDS) is one of them for this type of problem. There are lot of works on signature based anomaly based IDS. There is need of new upgraded versions of IDS algorithm as related to the malicious activities. The anomaly based detection is used for the safe cluster formation, re-clustering periodically and cluster monitoring efficiently from the detection of the attacks in the system. In this simulation anomaly detection algorithms performance is shown and detecting instructions using rule based AD scheme.

S. Sharmila et. al [3] "Detection of Sinkhole Attack in Wireless Sensor Networks Using Message Digest Algorithms" Wireless sensor networks (WSN) is on risk of routing attacks. By the use of one-way hash chains the sink hole is detected by the protocol. When the digest obtained from the safe forward path and trustable node to the destination only then the method proposed destination detects the attack. By use of safe path it makes sure the data integrity and the transferring of the messages. The algorithm used here is strong to deal with the malicious nodes that hide the errors or data. By MATLAB the algorithm used here is tested. Through the simulations the performance of proposed algorithm is seen. And the accuracy of the algorithm is confirmed. It is done in the terms of success rate, false positive rate and false negative rate.

Mohamed Guerroumi.et.al. [4] "Intrusion detection system against Sink Hole attack in wireless sensor networks with mobile sink" In the proposed work of wireless sensor network author has used Intrusion Detection System (IDS) on the sinkhole attack with mobile sink. In this model, to differentiate between real and fake sink nodes in it network area is divided into a flat grid of cells, and author used the signature-based technique. These cells are represented by the detection rate of a cell. Here in the IDS there is shown two types of sink mobility: periodic and random. Adding up the cell leader doesn't get activated simultaneously so the energy consumption incurred by the IDS is low. The efficiency of the proposed IDS is evaluated by the simulation. Where the terms like detection rate, efficiency, and energy consumption are used.

Van dana B. Salve,et.al.[5] "AODV Based Secure Routing Algorithm against Sinkhole Attack in Wirelesses Sensor Networks" Wireless sensor networks consisting of nodes with sensing, computation and wireless communication. Applications used in the fields like military, ecological, and health-related areas include the monitoring of sensitive information where security is must. Sinkhole is one of the destructing routing attacks that try to attract data by sending fake routing information to its neighbors. This paper presents AODV secure routing algorithm based on mobile routing that is used to detect sinkhole nodes by finding difference of sequence numbers using threshold value. It shows performance evaluation of ADOV which gives the safe routing algorithm. And the simulations are performed. It shows the efficiency and accuracy of the algorithm by the meter like Throughput, PDR and Packet loss. The simulations here are carried on NS2.

4. CONCLUSION

In the WSN sensor nodes collect the information by sensing the information and transmit using sink nodes. Sink nodes collect the information from sensor nodes and transmit this information to base station. In the transmission of data from source to destination various routing and off-demand routing

are used. In wireless sensor network various malicious nodes has been introduced to perform various types of attacks on the network to degrade or collect same information. The new attack that has been used for acquiring information by performing sink hole attack. Sink hole attack is performed on sink node attacking node replaces the actual sink node by advertising its availability and resumes all the data from the sensor node. Actual data doesn't receive at base station that loss the information of the network. To overcome the issue of sink hole attack detection scheme has to be implement that detect attacking node and provide reliable information. In this paper we have presented a brief study of how does a sink hole attack works on a wireles sensor network. It also discribes the varios types of routing protocals and attacks that occuer on awireles sensor network.

REFRENCES

[1] Ahmad Salehi S. "Detection of Sinkhole Attack in Wireless Sensor Networks", IEEE International Conference on Space Science and Communication, 2013, pp. 361-365.

[2] A. Balakrishnan "A Novel Anomaly Detection Algorithm for WSN" IEEE Conf. on Advances in Computing and Communications (ICACC), 2015,pp. 118 – 121.

[3] S. Sharmila "Detection of Sinkhole Attack in Wireless Sensor Networks Using Message Digest Algorithms" IEEE Conf. on Process Automation, Control and Computing (PACC), 2011,pp. 1 – 6.

[4] Mohamed Guerroumi "Intrusion detection system against SinkHole attack in wireless sensor networks with mobile sink" IEEE International Conference on Information Technology, 2015, pp. 307- 313.

[5] Van dana B. Salve, "AODV Based Secure Routing Algorithm against Sinkhole Attack in Wirelesses Sensor Networks", IEEE International Conference on Electrical, Computer and Communication Technologies, 2015, pp. 1 – 7.

[6] Guerroumi, M., "Intrusion Detection System against Sink Hole Attack in Wireless Sensor Networks with Mobile Sink" IEEE International Conference on Information Technology - New Generations, 2015, pp. 307 – 313.

[7] Varshney, K.K. "Performance analysis of malicious nodes in IEEE 802.15.4 based wireless sensor network" IEEE International Conference on Information Communication and Embedded Systems, 2014, pp. 1 – 5.

[8] Yong-Sik Choi, "A study on sensor nodes attestation protocol in a Wireless Sensor Network", IEEE Conf. on Advanced Communication Technology (ICACT), 2010, pp. 1738-9445.

[9] Yuling Lei "The Research of Coverage Problems in Wireless Sensor Network", IEEE Conf. on Wireless Networks and Information Systems, 2009, pp 31 – 34.

[10] Mittal, R. "Wireless sensor networks for monitoring the environmental activities" IEEE Conf on Computational Intelligence and Computing Research (ICCIC), 2010, pp. 1 – 5.

[11] www.Google.com/photo/wireless+sensor+network.