International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.06, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

DETECTION OF SINKHOLE ATTAC*K IN WIRLESS SENSOR NETWORK USING TIMESTAMP STRATEGY*

Kuldeep Kaur[1], Gurbinder Singh Brar[2]

[1]*Research Scholar, AIET, Faridkot*

[2]*Associate Professor,CSE, AIET, Faridkot*

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 the information and transmit using sink nodes. Sink nodes collects the information from sensor nodes and transmit this information to base station. WSN has been used for sensing information from different environment using energy for sensing and transmission. 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. In the previous research sinkhole attack has been detected on the basis of attacked area detection and intruder detection in the attacked area.

Keywords: WSN, Attacks, Challenges, Sink Hole Attack.

I INTRODUCTION

1.1Wireless Sensor Network

A wireless sensor network is a group of specialized transducers with a communications infrastructure for monitoring and recording conditions at diverse locations. Commonly monitored parameters are temperature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels and vital body functions. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications.

1.2 Attacks in WSN

1.2.1 Denial of Service attack: This strike happens when the aggressor increments control of a vehicle's benefits or jams the channel of correspondence utilized by the Vehicular Network, so it makes tangle to send separating information to its end of the line.

1.2.2 Message Suppression Attack: An assailant specifically dropping packets from the system, these bundles may hold discriminating data for the beneficiary, the aggressor stifle these parcels and can utilize them again as a part of other time.

1.2.3 Fabrication Attack: An aggressor can make this assault by sending wrong information into the system, the information could be wrong or the transmitter could assert that it is another person. This assault incorporates create messages, warnings, declarations, personalities.

1.2.4 Alteration Attack: This assault happens when aggressor modifies current information, it incorporates deferring the transmission of the data, replaying prior transmission, or changing the genuine section of the information transmitted

1.2.5 Replay Attack: This assault happens when an aggressor replay the transmission of a prior data to exploit the circumstances of the message at time of sending.

1.2.6 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.

1.2.7 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.

1.2.8 Sybil Attack: In this attack, attacker generates multiple identities to simulate multiple nodes. Each node send messages with multiple identities, in this way other nodes realize that there are many nodes in the network at the same time. This attack is very dangerous because one node can give its various locations at the same time and this creating security risk.

1.2.9 Sink Hole Attack: In Sink Hole attack malicious node acts as a black hole bto attract all the traffic in the sensor network. Attacker listens to requests for routes then replies to the target nodes. It inserts itself between the communicating nodes; it is able to do anything with the packets passing between them.

1.2.10 Cloning attack: A node replication attack involves an attacker inserting a new node into a network which has been cloned from an existing node, such cloning being relatively simple task with current sensor node hardware. This new node can act exactly like the old node or it can have some extra behavior.

1.3 Sinkhole Attacks:

In a sinkhole attack an intruder compromises a node or introduces a counterfeit node inside the network and uses it to launch an attack. The compromised node tries to attract all the traffic from neighbor nodes based on the routing metric used in the routing protocol. When the compromised node manages to achieve that, it will launch an attack. Sinkhole attacks are a type of network layer attack where the compromised node sends fake routing information to its neighbors to attract network traffic to itself [7]. Due to the ad hoc network and many to one communication pattern of wireless sensor networks where many nodes send data to a single base station, WSNs are particularly vulnerable to sinkhole attacks. Based on the communication flow in the WSN the sinkhole does not need to target all the nodes in the network but only those close to the base station. We consider two scenarios of sinkhole attacks. In the first the intruder has more power than other nodes. In the second the intruder and other nodes have the same power. In both cases the intruder claims to have the shortest path to base station so that it can attract network traffic. In a wireless sensor network the best path to the base station is the basic metric for routing data.

1.4 Challenges in Detection of Sinkhole Attack In WSNs

1.4.1 Communication Pattern in WSN: Sinkhole attacks normally occur when compromised node send fake routing information to other nodes in the network with aim of attracting as many traffic as possible. Based on that communication pattern the intruder will only compromised the nodes which are close to base station instead of targeting all nodes in the network. This is considered as challenges because the communication pattern itself provides opportunity for attack.

1.4.2 Sinkhole attack is unpredictable: The compromised node used its routing metric that used by routing protocol to lie to his neighbors in order to launch sinkhole attack. Then all the data from his neighbors to base station will pass through compromised node.

1.4.3 Insider Attack: Insider attack and outsider attack are two categories of attack in wireless sensor network. Outside attack is when intruder is not part of network. In inside attack the intruder compromises one of the legitimate node through node tempering or through weakness in its system software then compromised node inject false information in network after listen to secret information. Inside attack can disrupt the network by modifying routing packet.

1.4.4 Resource Constraints: The limited power supply, low communication range, low memory capacity and low computational power are the main constrained in wireless sensor network that hinder implementation of strong security mechanism.

1.4.5 Physical attack: A wireless sensor network normally deployed in hostile environment and left unattended. This provides a opportunity for an intruder to attack a node physically and get access to all necessary information.

II REVIEW OF LITERATURE

A.Vijayalakshmi. et al [1] "Mobile Agent Middleware Security for Wireless Sensor Networks" Wireless Sensor Networks have gained much attention in recent applications. However, they are very much subjected to the security threats. To provide security arrangements in sensor nodes, the energy required to carry out the operation may reduce the life time of the sensor nodes. In order to optimize the energy usage in sensor nodes, Middleware concept is introduced. The Middleware to provide security for the Wireless Sensor Networks is arranged in the Mobile agent with the capability of optimizing the power usage with the sensor nodes. An energy efficient Mobile agent based algorithm is simulated. It will be established that the Mobile agents provide the security arrangements to the Wireless sensor networks for the reduction of sinkhole and cloning attacks.

Ahmad Salehi S. et.al.[2] "Detection of Sinkhole Attack in Wireless Sensor Networks" Generally wireless sensor networks rely of many to one communication approach for data gathering. This approach is extremely susceptible to sinkhole attack, where an intruder attracts surrounding nodes with unfaithful routing information, and subsequently presents selective forwarding or change the data that carry through it. A sinkhole attack causes an important threat to sensor networks and it should be considered that the sensor nodes are mostly spread out in open areas and of weak computation and battery power. In order to detect the intruder in a sinkhole attack this paper suggests an algorithm which firstly finds a group of suspected nodes by analyzing the consistency of data. Then, the intruder is recognized efficiently in the group by checking the network flow information. The proposed algorithm's performance has been evaluated by using numerical analysis and simulations. Therefore, accuracy and efficiency of algorithm would be verified.

Ching-Tsung Hsueh et. al. [3] "A Secure Scheme against Power Exhausting Attacks in Hierarchical Wireless Sensor Networks" Security and energy efficiency are critical concerns in wireless sensor network (WSN) design. This paper aims to develop an energy-efficient secure scheme against power exhausting attacks, especially the denial-of-sleep attacks, which can shorten the lifetime of WSNs rapidly. Although various media

access control (MAC) protocols have been proposed to save the power and extend the lifetime of WSNs, the existing designs of MAC protocol are insufficient to protect the WSNs from denial-of-sleep attacks in MAC layer. This is attributed to the fact that the well-known security mechanisms usually awake the sensor nodes before these nodes are allowed to execute the security processes.. This paper proposes a cross-layer design of secure scheme integrating the MAC protocol. The analyses show that the proposed scheme can counter the replay attack and forge attack in an energy-efficient way. The detailed analysis of energy distribution shows a reasonable decision rule of coordination between energy conservation and security requirements for WSNs.

Deshpande, P. et al [4] "Techniques improving throughput of wireless sensor network: A survey" In wireless sensor networks, maintaining the higher throughput is the main concern. Wireless senor networks are basically formed with a few powerful base stations and a large number of resource-constrained sensor nodes.The wireless sensor network composed of n number of sensors or nodes, where each and every node is connected to one or several nodes or sensors. Wireless sensor nodes of zig bee system basically build on two aspects of protocol stack that are IEEE 802.15.4 standard and zigbee protocol.

Guerroumi, M. et.al.[5] "Intrusion Detection System against Sink Hole Attack in Wireless Sensor Networks with Mobile Sink" In this paper, we propose an Intrusion Detection System (IDS) against Sinkhole attack in wireless sensor networks with mobile sink. In the detection model, the network area is divided into a flat grid of cells, and we use the signature-based technique, which is represented by the detection rate of a cell, to distinguish between real and fake sink nodes. The proposed IDS consider two types of sink mobility: periodic and random. In addition, as the cell leaders do not activate their IDS agent simultaneously, the additional energy consumption incurred by the IDS is low. Simulation results show the efficiency of the proposed IDS in terms of detection rate, efficiency, and energy consumption

III METHDOLOGY

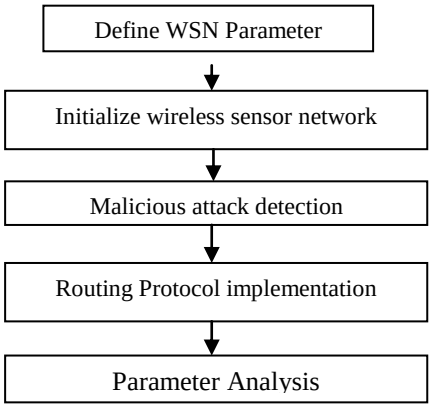

Fig 3.1 Flow of purposed work

Figure 3.1 represents the flow of the purposed work that represents various steps that must be carried out for evaluation of desired objectives. In the purposed work malicious node detection has been done in wireless sensor network. In the purposed work wireless sensor network has been initialized by defining various

parameters in the purposed work. These parameters have been defined in table 5.1. After initialization of sensor nodes sensor node collect information from sensing environment and transmits sensor information to base station with help of sink nodes. In WSN sink nodes have been utilized for transmission of information from sensor to base station or to other sink nodes. Attackers encounter sinkhole attack in WSN for degrading network performance. In the purposed work sink nodes have been provided a timestamp for broadcasting message for collection of data. Sink nodes available in the network broadcast message to all sensor nodes for collection of data. Nodes will transmit request within timestamp that has been defined by the trusting authority. In the purposed work AODV routing protocol has been used for transmission of data. Malicious node changes the route table strategy of AODV that transmit request to all nodes that comprised node contain a shortest path for data transmission to base station. To detect sink hole attacking node available in the network destination sequence number has been utilized. On the basis of DSN sink hole attacking nodes has been detected in the purposed work. After detection message various parameters have been analyzed for performance evaluation of purposed work.

IV RESULTS

In the purposed work WSN has been initialized for sensing information from environment. The sensor nodes have been deployed in the environment for capturing information. These nodes capture information from particular environment and transmit this information to base station. Various parameters have been used in WSN for sensing information. These nodes consume energy while sensing, receiving and transmitting information.

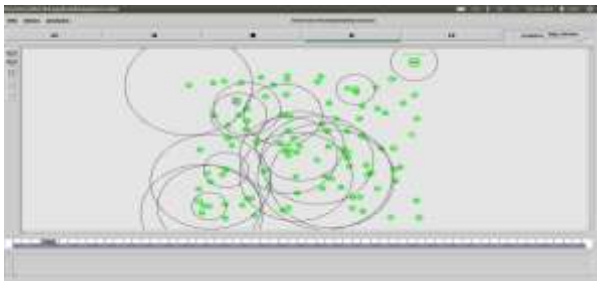

Fig 4.1 Attack occurred in the Network

This figure is use to represent the Sinkhole attack occurred in the network. 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.

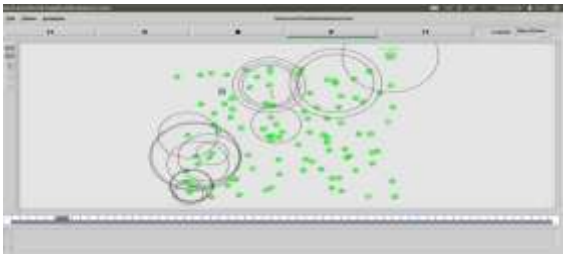

Fig 4.2 Detection of Sinkhole Attack

In wireless sensor network the packet are transmitted based on routing metric that used by different routing protocols. The compromised node used its routing metric that used by routing protocol to lie to his neighbors in order to launch sinkhole attack. Then all the data from his neighbors to base station will pass through compromised node. In this actual data doesn't receive at base station that loss the information of the network. Here, the sink hole attack detection scheme has to be implement that detect attacking node and provide reliable information.

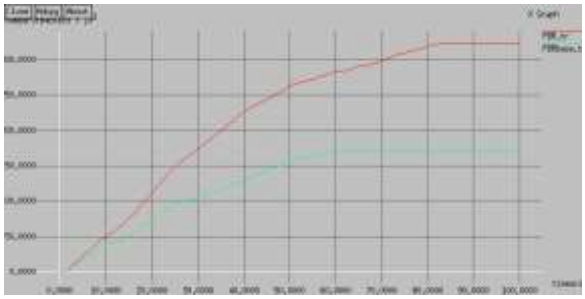

Fig 4.3 Packet Delivery Ratio

In this X-axis represent the Time and Y-axis represent the Bytes send over the network. This figure is use to represent the Packet Delivery Ratio. Packet Delivery Ratio is defined as the number of packet deliver with respect to time. This graphical representation represents two different lines by red and green color. Packet delivery ratio by purposed DSN approach is much higher than that of previous approach that is secure AODV routing protocol.

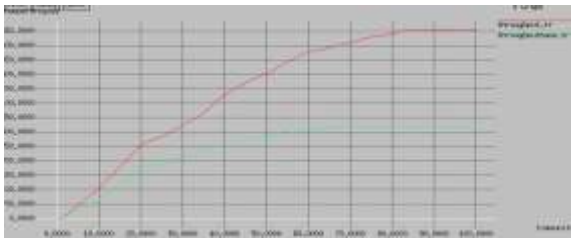

Fig 4.4 Throughput

This figure is use to represent the Throughput. Throughput is defined as the number of packet delivered successfully over the network. Throughput represents bytes transmitted per unit time. This graph represents comparison between purposed and AODV routing protocol. By analyzing graph plotting one can say that purposed approach provides much higher throughput than that of AODV based detection approach.

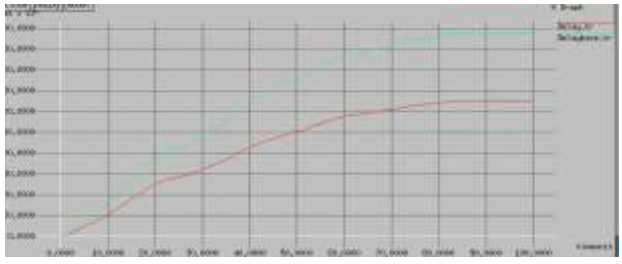

Fig 4.5 Packet Delay

This figure is use to represent the Packet Delay. Packet Delay is defined as the Delay between packets during transmission. In this graph delay has been measure for purposed and previous approach. Delay has been measured in terms of time units. Purposed approach has higher delay than that of previous approach due to transmission of enquiry packets over the network for detection of sinkhole attack.

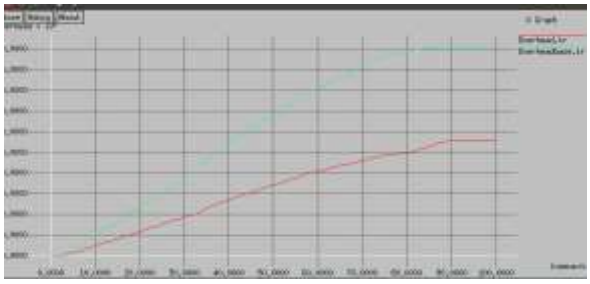

Fig 4.6 Overhead

This figure is use to represent the network overhead. Overhead has been caused due to routing packets that has been transmitted over the network. Overhead cause various problems over the network.

V CONCLUSION& FUTURE SCOPE

Conclusion: Wireless sensor network has been used for sensing various types of information from sensing environment. In the work sinkhole attack detection has been done that has been attacked by any attacker by developing a compromised node in WSN. The attackers introduce the node in the network that advertises for data collection from sensor nodes and transmit data to wrong destination. In the purposed work sinkhole detection has been done on the basis detection algorithm that utilized timestamp strategy. In this strategy genuine nodes has been provided a timestamp so that all the sink nodes available in the network broadcast message for data collection within particular time stamp. This approach has been hybrid with destination sequence number matching approach, that checks all the path DSN if any path has higher difference in DSN that node has been detected as malicious node available in the network. The path accumulated by malicious node has been denied for data transmission so that data loss must be reduced. In the purposed work various parameters have been analyzed for performance evaluation of purposed work so that validation can be done. On the basis of these parameters that are throughput, packet delivery ratio, jitter and delay one can conclude that purposed work provides much better results than previous approaches.

VI FUTURE WORK

In the future reference purposed approach can be utilized for real world application so that sinkhole attack can be detected. In future reference a study can be done for malicious node detection and network lifetime improvement for large scale wireless sensor network. In recent researches mobile wireless sensor network attracts individuals for utilization in sensing information that can be an area of research for malicious node detection.

REFRENCES

[1] A. Vijayalakshmi., "Mobile Agent Middleware Security for Wireless Sensor Networks" IEEE International Conference on Communication and Signal Processing, 2014, pp. 1669- 1673.

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

[3] ching-Tsung Hsueh"A Secure Scheme Against Power Exhausting Attacks in Hierarchical Wireless Sensor Networks" IEEE international Conference on Sensors Journal ,pp- 3590 – 3602, Volume: 15, Issue: 6, June 2015.

[4] Debiao He "A secure temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks" IEEE international Conference on Wireless and Pervasive Computing, pp-453-459, 2014.

[5] 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.

[6] Geetha, R. "Fuzzy logic based compromised node detection and revocation in clustered wireless sensor networks" IEEE Conf. on Information Communication and Embedded Systems (ICICES),2014,pp- 1 – 6.

[7] Guanglai Chen "Notice of Retraction the design of wireless wave height sensor network node based on Zigbee technology", IEEE Conf. on Electric Information and Control Engineering (ICEICE), 2011, pp. 3683 – 3686.

[8] hongsong chen "Quantitative Trustworthy Evaluation Scheme for Trust Routing Scheme in Wireless Sensor Networks" IEEE international Conference on Trustcom/BigDataSE,pp-345-350,2015.

[9] imran Makhdoom"A novel code attestation scheme against Sybil Attack in Wireless Sensor Networks" IEEE international Conference on Software Engineering ,pp-456-460,2014.

[10] Krithiga, J "Efficient Code Guard mechanism against pollution attacks in interflow Network coding" IEEE Conf. on Communications and Signal Processing (ICCSP), 2014,pp- 1384 – 1388.

[11] 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.

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