Sinkhole attack detection based on redundancy mechanism in wireless sensor network

Mamta patel[1], Prof. Mohammed Bakhtawar Ahmed

[1]Research Scholar, [2]Assistant Professor
Department of computer science and engineering,
kalinga University, Raipur, India

***Abstract*— Wireless sensor networks has a bright future because of its low-cost, save-power, and easy implementation .etc. However, its security problems have become hot research topics in many applications. Sinkhole attack is just one of frequently encountered security problems, which is easily combined with other attacks to cause more damage. In order to prevent sinkhole attack, we do some research on it, and one way to detect the sinkhole attack based on the redundancy mechanism is proposed in this paper. For the suspicious nodes, messages are sent to them through multi-paths. By evaluating the replied comprehensively, the attacked nodes are finally confirmed. Lastly, a simulation is performed to test the effectiveness of the method. And the simulation shows that the approach could work to some extent.**

***Keywords*— Sinkhole attack; detection; redundancy; wireless sensor networks**

I. INTRODUCTION

Wireless sensor network(WSN's) is a combination of variable number sensor nodes which are equipped with tiny processor, memory ,transmitter and/or receiver node. A node in a wireless network may vary in size from a grain of dust to huge antenna as well as these sensor node is a self-governing independent node capable to communicate with any other node in a network. A popularity of wireless sensor network increases day by day as well as wireless network emerging in various field because it increases the efficiency of the network by simplifying the accessibility of information resources easier and faster as well as it is less expensive than wired network, easily implemented and easy maintenance.

Due to changing infrastructure and decentralised administration of wireless sensor network (WSN's) are vulnerable to various kinds of attack such as selective forwarding, HELLO flooding, Sybil, Blackhole, Wormhole, Sinkhole etc [6]. Sinkhole attack often a frequent attack that encounter in a wireless network. It is one of the big security thread in a wireless network that disrupt the working of routing protocol. In this attack, an attacker node (sinknode) propagates a forge or bogus routing information in surrounding node and tell their neighbour that it exist in the shortest route. When the surrounding node receives this forge routing information they believes that a sinknode exist in the shortest path to send the information to the destination node and they starts forwarding the data to the sinknode rather than genuine destination node. Therefore in wireless sensor network sinkhole attack has massive negative impact even there is only one sinknode . It increases the load on a particular network therefore chance of network fall on that area will also increases Wireless Sensor Network (WSN's) composed of variable number of distributed autonomous sensors. A wireless sensor consist a few to thousand's number of autonomous sensor node in which each node composed with tiny size of processor, small memory, limited power as well as transmitter and/or receiver. This self-directed node independently able to communicate with any other node in a wireless sensor node. In the wireless sensor networks size of sensor node vary in size from grain of dust to huge satellite dish. In the same way, the price of sensors vary from few hundreds to thousands rupees that depends on the complexity and functionality of the individual sensor nodes. In the below figure 1.1 shown the overview of simple wireless sensor networks.

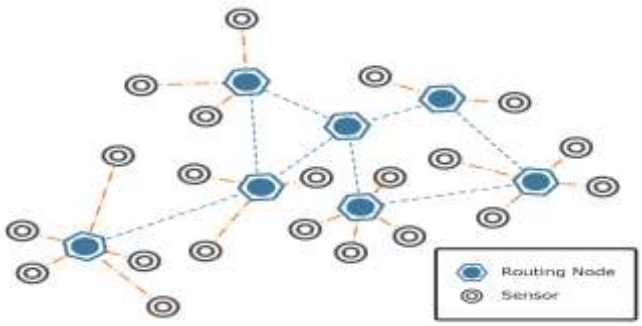


Figure 1.1: overview of simple WSN's

II. RELATED WORK

Sinkhole attack detection based on redundancy mechanism in wireless sensor network" Procedia Computer Science, Information Technology and Quantitative Management, this paper proposed a methodology of detection of sinkhole attack based on redundancy mechanism. In the proposed methodology we have set of suspicious and trusted nodes. For detection of sinknode set of trusted nodes send the data to suspicious node by using multi- path When the trusted nodes receives reply message from various nodes then by evaluating these message it confirms which suspicious node is a malicious node. "Detection and isolation of sinkhole attack from AODV routing protocol in MANET", IEEE computer society, Sixth International Conference on Computational Intelligence and Communication Network,

this paper suggested a method for detection and isolation of sinkhole attack and provide substitution AODV from multipath AODV . (Shashi Pratap Singh Tomer, Brijesh Kumar Chaurasia, 2014)

"Hop-count monitoring: Detecting sinkhole attack in wireless sensor network", IEEE, this paper proposed a novel algorithm for detecting sinkhole attack which is based on the hop-count monitoring. The value of hop-count is easily available from routing table and implements a ADS (Anomaly Detection System) that dynamically maintain a hop-count parameter such as distance between source node and target node. In the proposed strategy a by using a single ADS we achieve detection rate of 96% with no false alarm and with small number of ADS we can get 100% detection rate [10]. (Daniel Dallas, Christopher Leckie, Kotagiri Ramamohanarao 2007)

There are various technological progress made and concepts developed in the past decades for the detection of sinkhole attack in WSN's summarized as follows:

- Detection of sinkhole attack using source sequence number of current and previous request.
- Sinkhole detection based on received signal strength indicator (RSSI) of message that requires the collaboration of some Extra Monitor(EM) nodes.
- Using link quality indicator (LQI).
- Using the mutual understanding among the mobile nodes.
- Detection of sinkhole based on redundancy mechanism.

A sinkhole attack is a big security threat in wireless sensor network that disrupt the working of routing protocol. In this attack a attacker node is looks like a normal other nodes therefore it is difficult to identify it. In this attack, the target of sinknode (attacker node) is that it attract the network traffic to itself, for this a sinknode propagates the forge or bogus routing information and misguide the surrounding nodes that it exist in a shortest route to send the information to the destination node. When the surrounding node receives this forge or bogus routing message from sinknode they believes that sinknode is exist in a shortest path to send the information to destination node. Once a sinknode get success in getting network traffic then it may perform: selective forwarding, alter or drop packet. As well as it increases the overhead on a particular link, congestion, energy consumption therefore a network will goes down.

III. PROPOSED METHOD

In the proposed methodology to detect the sinkhole attack in the wireless sensor networks the detection process is divided into three phase which are as follows:

Phase- I

Topology Generation & Data transmission

Step 1: Invoke random topology generation.

Step 2: Invocation of route discovery phase.

Step 3: Data transmission.

Phase- II

Sinkhole Implementation

Step 1: Source sends RREQ to the neighbourhood.

Step 2: If- neighbour node is a intruder it will send RREP with high sequence number and less hop count value.

Step 3: Else- neighbour node is destination, reply RREP to source.

Step 4: If- neighbour is not intruder and not destination, node forward RREQ until it reaches to destination node or reaches end of the count node.

Step 5: On receiving various RREQ by malicious, it picks the reverse route path and forwards the forge RREQ with high sequence number & less hop count.

Step 6: On receiving forge RREQ by neighbour node, it believes sinknode is exist in the shortest path to send the data to destination node and starts forwarding the data to sinknode rather than genuine destination.

Phase- III

Detection Phase

Step 1: Appointing highly connected node as a monitor node.

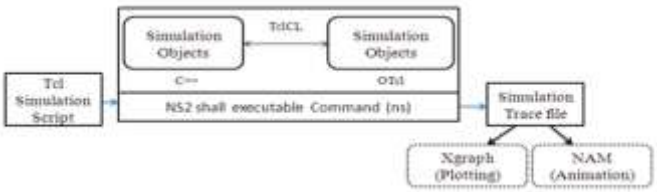
Step 2: Monitor node will keep track of routing RREQ and RREP

Step 3: Separating the forward route and reverse route from source to destination.

Step 4: If-node present in the reverse path but not in the forward path then assign node as a malicious or sinknode.

Step 5: Else-nodes present in both reverse and forward path, none of the intruder node

In a AODV routing protocol, whenever a sinkhole attack is encounters then a sinknode (attacker node) starts modifying the sequence number of route request (RREQ) message in a network. When a intermediate node receives the same route request from several path then sequence number of route request is used to avoid multiple transmission of some route request as well as to prevent loop formation. First of all a sinknode selects a source and destination node and starts monitoring the sequence number of route request (RREQ) packet generated by source node. Thereafter a sinknode generates forge or bogus route request (RREQ) message with high sequence number (to tell it is a fresh route) and less hop count value (to tell it is a shortest route to send the information to the destination) [4,9] and broadcast to surrounding nodes. When the surrounding node receives this forge route request (RREQ) packet it believes that it is a fresh and shortest route to send the data to the destination node and starts forwarding the data to the sinknode rather than genuine destination. As already discussed once the sinknode gets the access on the data it may perform selective forwarding, alter or drop packet. In the below figure 3.1 and 3.2 illustrates the sinkhole attack in a AODV routing protocol and how it disrupt the working the AODV.



Basic Architecture of Network Simulator 2

Network Simulator is a network simulatoe software that represents the behaviour of real life computer network. Network simulator is a event driven simulation software which is helpful in designing communication network having dynamic nature.

It work at the packet level and to support the simulation sprovides the number of protocol such as TCP, UDP, FTP, DSR, HTTP etc.Network simulator can simulate the both wired network and wireless network and it is a unix based system.

This appliction is used for variety of application. This is especialy designed for saving time and cost. Network simulator saves our time and cost by establishing virtual network for test containing routers, switches, computer etc.

Network simulator -2 runs on GNU/Linus, Solaris, Mac OS X systems .Different kinds of wide area network tevhnologies like TCP, ATM, IP etc ansd local area network technology such as token ring, ethhernet etc can be easily simulated and easily tested by user. A user can easily costomised the network in order to fulfill their specific needs.

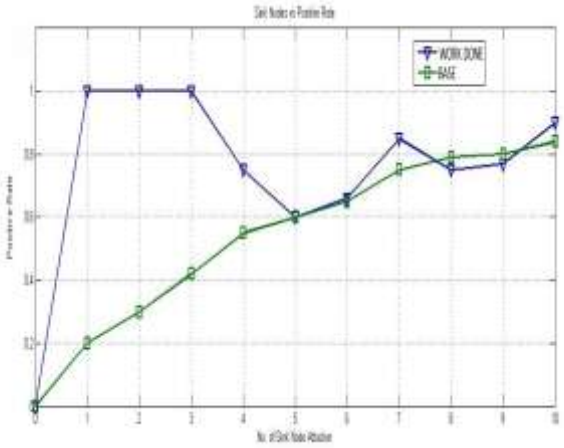
Network simulator composed by the two programming language which are C++ and Object oriented tool command language (OTcl) :

- Natwork Simulator a uses a TCL programming language replaced by Object OTcl (object oriented TCl)
- The core or internal structure of network simulator -2 is written in C++ programming language but the simulation object of C++ language are linked to the shadow objet in OTcl.
- Object oriented Tcl language which is a extention of Tcl script language is used to write the network simulation script.

IV. RESULTS AND ANALYSIS

This section concerned with the simulation result and elevated performance of the suggested technique. The suggested technique shows the elevation based on the detection rate of sinkhole attack in a wireless sensor network. Here, first of all we will talk about the simulation parameter which are shown in below table :

S.No.	Simulation Parameter	Values
1	Simulation Software	Network Simulator All In One (2.35)
2	Number Of Nodes For Experiment	20-120
3	Channel Type	Channel/Wireless Channel
4	Radio Propagation Model	Propagation/Two ray ground waves
5	Traffic Type	CBR
6	Area (M*M)	1000*1000
7	Routing Protocol	Ad Hoc On-Demand Routing
8	Antenna	Omni Antenna
9	MAC Type	Mac /802.11
10	Network interface type	Phy/WirelessPhy
11	Simulation Time	600 sec



Comparison Of Detection Rate

V. CONCLUSION

Our present work is relevant to the detection of sinkhole attack based on the analysis of routing behaviour in a wireless sensor networks (WSNs). Our suggested algorithm consist a three phase: topology generation & data transmission, sinkhole implementation and detection phase. In this scheme to we detect the sinknode by analysing the forward and reverse routes. This is a simple method to detect the sinkhole attack, which elevates the detection of the malicious node in terms of detection rate and the feasibility of proposed methodology is proved by the simulation. However, Sinkhole attack detection rate 100% is not realistic because there are various causes of failure of detection of attack therefore we can only try to elevate the detection rate.

VI.REFERENCES

[1] Ahmad Salehi S., M.A. Razzaque, Parisa Naraei, Ali Farrokhtala, “Detection of Sinkhole Attack in Wireless Sensor Networks”, IEEE International Conference on Space Science and Communication (IconSpace), 1-3 July 2013.

[2] Asad Amir Pirzada and Chris McDonald “Circumventing Sinkholes and Wormholes in Wireless Sensor Networks”.(http://www.ctr.kcl.ac.uk/IWWAN2005/papers/58.pdf)

[3] Benjamin J. Culpepper and H. Chris Tseng, “Sinkhole Intrusion Indicators in DSR MANETs”, First International Conference on Broadband Networks (BROADNETS’04) IEEE.

[4] Byung Goo Choi, Eung Jun Cho, Jin Ho Kim, Choong Seon Hong and Jin Hyoung Kim," A Sinkhole Attack Detection Mechanism for LQI based Mesh Routing in WSN", IEEE International Conference on Information Networking, 2009.

[5] Chanatip Tumrongwittayapak* and Ruttikorn Varakulsiripunth Chanatip Tumrongwittayapak and Ruttikorn Varakulsiripunth," Detecting Sinkhole Attacks In Wireless Sensor Networks" ICROS-SICE International Joint Conference 2009

[6] Chanatip Tumrongwittayapak and Ruttikorn Varakulsiripunth," Detecting Sinkhole Attack And Selective Forwarding Attack In Wireless Sensor Networks", IEEE 2009.

[7] Changlong Chen, Min Song, and George Hsieh," Intrusion Detection of Sinkhole Attacks In Large-scale Wireless Sensor Networks", IEEE 2010.

[8] D. B. Jagannadha Rao , Karnam Sreenu, Parsi Kalpana3 "A Study on Dynamic Source Routing Protocol for Wireless Ad Hoc Networks", International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 8, October 2012

[9] D.Sheela , Naveen kumar. C and Dr. G.Mahadevan, "A non cryptographic method of sink hole attack detection in wireless sensor networks", IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011.

[10] Daniel Dallas, Christopher Leckie, Kotagiri Ramamohanarao," Hop-Count Monitoring: Detecting Sinkhole Attacks in Wireless Sensor Networks" IEEE 2007.

[11] Devi. P, Kannammal. A "A Pragmatic Approach To Secure DSR Protocol From Sinkhole Attack In AD HOC Environment", Journal of Theoretical and Applied Information Technology 31st August 2014. Vol. 66 No.3

[12] Dr. Umadevi Chezhiyan " Measurement Based Analysis of Reactive Protocols in MANET", International Journal of Wired and Wireless Communications Vol.1, Issue 2, April, 2013.

[13] D. Sheela, Nirmala. S, Sangita Nath and Dr. G Mahadevan " A Recent Technique to Detect Sink Hole Attacks in WSN". (http://psrcentre.org/images/extraimages/27.%20158 .pdf)