Detection of sink Hole Attack in Wireless Sensor Network using Advanced Secure AODV Routing Protocol

Deepa Gupta
Research Scholar at department of Computer Science &Engg.
Sachdeva Engg. College for Girls, Gharuan

Harinder Kaur
Assistant Professor at department of Computer Science &Engg.
Sachdeva Engg. College for Girls, Gharuan

Rakesh Kumar
Assistant Professor at department of Computer Science &Engg.
Sachdeva Engg. College for Girls, Gharuan

ABSTRACT

wireless sensor network has been used for data sensing and collection at a single point for decision making process. Attack comprising in WSN produced various issues in data transmission and data management. Sinkhole attack is a compromised attack in WSN that compromised nodes that advertises a shortest path for data transmission. In this paper a new approach has been purposed for detection of sinkhole compromised nodes available in the network. On the basis of simulation results we can see that purposed approach provides better results.

Keywords

WSN, Sinkhole, DSN, TDMA and PDR

1. INTRODUCTION

1.1 Structure of wireless sensor network

The wireless sensor network is contains of autonomous mobile nodes organized by wireless multi hop communication paths. In their any node communicate and move at the same time. In the wireless sensor networks contains no fixed network transportation or executive support dissimilar other conventional network that requires fixed network transportation. The topology of ad hoc network can change because nodes may not be fixed example of Changes as dynamically as mobile node join leave the network. The Ad hoc networks can also be defined as self-creating, self-organizing, and self-administering [1].in there no routers or additional base stations to the route packets from the source of destination. The wireless ad hoc network is self-configuring network of the mobile nodes connected by wireless links the union of which forms a random topology. The active nodes proceed as a router free to move randomly arbitrarily and manage them arbitrarily; such a network may operate in a standalone fashion or may be connected to the larger Internet [1, 2].following the figure 1 the interconnection between three nodes. Showing all nodes is creating communication between A and C must discover the route through B. The circle in the figure represents the supposed range of each node's radio transceiver. A wireless ad hoc network is much more flexible than wired network. It does not necessary complex wired organization and other network equipment's.

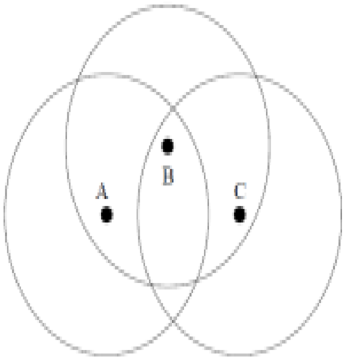

Fig.1 Simple Wireless ad hoc networks with three participating nodes

1.2 Security in Wireless Ad hoc Network

In the safety point of view, the lots of issues for security purpose in wireless sensor network. These links essential amid nodes in wireless networks are highly risk to link attacks or routing attacks. in this attack more leads to Route trouble, Interfering, Loss of clandestine Information, Message distortion, Denial of Service (DoS) [6], Data Tempering etc. in the wireless ad hoc networks are also disposed to the tribulations connected to the compromised nodes, this node act like the way is correct but the same time they make use of the flaws and inconsistencies in the routing protocols (DSR, AODV). The compromised node can be turn into malicious node and thus create the new routing massages or advertise itself in an accessible links and start creating incorrect link state information that outcome in network delay energy utilization and finally makes the network disabled. Some Reactive [7] (On-Demand) and proactive [7] (Periodic) routing protocols are susceptible to these attacks.

1.3 Sinkhole Attack

The sinkhole attack is one of the server attacks in the wireless ad hoc network. In the wireless ad hoc network using through the sinkhole attack compromised node or malicious node advertises the wrong routing information to rise as an exact node or receives the whole network jam. Following receiving whole network jam it is modifies the secret information, changes through the data packets and drop them to create the whole network is very complex. The malicious node perform to attract the secrete data from the neighboring nodes. Sinkhole attacks affects the performance of Ad hoc networks protocols such as AODV [3] by using flaws as maximizing the sequence number or minimizing the hop count [4]. This way to perform the malicious node behaves like to be the best path for the nodes communication. In the DSR protocol; sinkhole attack modifies order no in RREQ.

1.4 Effect of Sinkhole Attack on routing protocols

The Routing protocols are required whenever a data packet needs to be transmitted from source node to the destination node by communicating with number of intermediate nodes. Various routing protocols have been proposed for such kind of ad hoc networks. These protocols help to find a specific route for packet delivery and deliver the packet to the correct destination. The studies on various aspects of routing protocols have been an active area of research for many years. This paper analyzes the "Sinkhole Attack" that can be easily employed against various routing protocols. Routing protocols used in wireless Ad hoc networks can be classified in two major types.

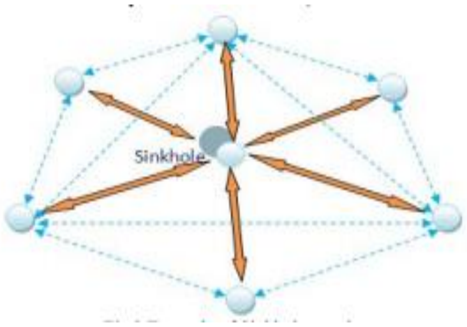

Fig.2 Example of Sinkhole attack

- Table-driven routing protocols (Pro-Active)
- On-demand routing protocols (Reactive)

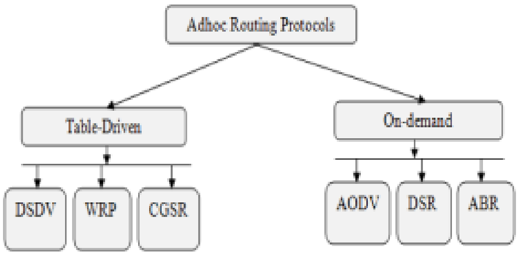

Fig.3 Ad hoc Routing Protocols

Table-driven routing protocols are enhancements of the wired network routing protocols. They maintain a table structure in order to store the routing information of each router. Table is consistently updated to maintain the correct information of network status [5, 7]. On the other hand, on-demand routing protocols executes the path finding process when a path is required by a node.

2. REVIEW OF LITERATURE

Varshney, K.K. [7] "Performance analysis of malicious nodes in IEEE 802.15.4 based wireless sensor network "this paper represented to the wireless sensor network (WSN) it has different field of applications, and the wireless sensor network is very much horizontal to the many security threats. In the wireless sensor network there are many number of attacks like black hole attack, selective forwarding attacks and sinkhole attack Sybil attack etc. This paper mainly concentrates on the performance of wireless sensor network in the presence of black hole attackers using Ad-hoc on Demand Distance Vector Routing Protocol (AODV). The black hole type of attacker nodes absorbs all messages passing through it. Therefore the affected node attacks the whole traffic in the network and more performance sensor network using the AODV with black hole and without black hole attack is also analyzed. The simulation is done by using NS-2.3

Ritwik Banerjee [8] "Energy efficient routing and bypassing energy-hole through mobile sink in WSN" in this paper author present application areas of the wireless sensor network frequently suffered from the peril of partial energy resources. In this paper defined potentiality of the application is directly dependent on the no of active nodes are accessible within the sensor network. The lifetime of the sensor nodes is the eventual way to improve the lifetime of the entire sensor network. Allowing for the mobile sink node raises a new aspect to the WSN applications in the large scale networking. In the case of improving the performance using target detection. In this paper we introduce a novel cluster based routing protocol which is aimed to optimize the nodes energy usage with considering the mobility for the sink node to pretend the common energy-hole problem.

Babar Nazir [9] "Mobile Sink based Routing Protocol (MSRP) for Prolonging Network Lifetime in Clustered Wireless Sensor Network "this paper represent the WSN(wireless sensor network), in these type sensors near the sink hold to transmit the data of the nodes away from the sink hole. As well as result they consume their energy very quickly. The network partitioning or we can significantly limit the network lifetime. This type of problem is hotspot trouble. Newly in the WSN very critical issue for using hotspot or energy hole near the sink. In this paper author mainly focus on hotspot problem and purposed Mobile Sink based Routing Protocol (MSRP) for using Prolonging Network Lifetime in Clustered Wireless Sensor Network. In the MSRP all mobile sink moves in the clustered WSN to collect sensed data from the CHs within its vicinity. Through the data gathering mobile sink also maintains in sequence about the remaining energy of the CHs. to access the performance of the proposed strategy intensive simulation are out using OMNet-4.0. In this paper author compare with the purposed approach to the static sink and multiple sinks strategies, using metrics such as energy per packet, The simulation results demonstrate that MSRP is effective in prolonging the network lifetime as well as in improving throughput than static sink and multiple sink strategies

Pushpendu Karet [10] "Reliable and Efficient Data Acquisition in Wireless Sensor Networks in the Presence of Trans faulty Nodes" in this paper author introduced to the collection of spatially distributed sensor nodes in the wireless sensor network in which

Collaboratively to sense the physical phenomena around them then send the sensed information to the sink node through single-hop or multi-hop paths.in this paper author purposed scheme named REDAST, for reliable or efficient data acquisition in stationary WSN in the presence of Trans-faulty nodes. During the Trans faulty acts like sensor node gets temporarily isolated from the network. The temporary node separation leads to the arrangement of dynamic communication holes in the network, which form and disappear dynamically. In their increase the size and the decrease the size as well as dynamically these affects the result in loss of information in the radiation-affected area. The data fusion performed to get real information from the unnecessary information received from the radiation-affected area REDAST, achieves better energy efficiency and reduced average end-to-end delay than sensor nodes having only acoustic mode of communication.

3. METHODOLOGY

WSN is used for capturing information from non-approachable areas so that sensor can be deployed in the particular region and these sensors can be used for information sensing and collection at a single point. In the process of data collection from sensor nodes sink nodes available in the network collect all sensed information. This captured information can be used for decision making process.

In the proposed work sinkhole attack detection in wireless sensor network has been done. In this process data has been transmitted from different from different sensor nodes to base station by using the time stamp allocated to each node. In this research a reactive protocol has been used for data transmission from source to destination. This routing protocol has been used for path selection for data transmission from source to destination.

In the process of data transmission from source to destination a node transmit a route request that contain information about source, destination id, hop count and destination sequence number. In this process all the neighbor nodes receive request and create a path to destination for data transmission. In this process source node receives route reply (RREP) from all the neighboring nodes and selects a shortest path that contain minimum number of hops for data transmission.

Sinkhole attack affected node in the network transmit RREP with minimum number of hops and source node start transmitting message via shortest path transmitted by malicious node. Sinkhole attacking node has property that compromised a node for having a shortest path from source to destination. But due to advertising of malicious node this gathers information from source node but does not forward information to base station.

- **Detection of Sinkhole node**

In the process of detection of sinkhole attack in wireless sensor network different approaches have been purposed to detect a malicious node. In the purposed work sinkhole node has been detected using hybrid detection mechanism that use Time stamp, Destination sequence number and packet delivery ratio of a single node. In this process source node start transmitting information to destination that causes selection of intermediate nodes available in the network to select a best route for data transmission.

In this process nodes have allocated a slot of time stamp to forward information from source to destination that utilizes this particular timestamp for forwarding information. Nodes available in the network utilizes TDMA scheduling for data transmission at given time slot. In this process any node that broadcast RREQ packet before or after a particular time stamp has been detected and undergoes process of sinkhole detection process. In this process mechanism nodes DSN and packet delivery ratio of all the nodes have been analyzed. To detect malicious node following described approach has been followed.

In the process of WSN N, number of sensor nodes has been deployed and t (i) is time slot given to all the nodes for data transmission then.

Pseudo code for sinkhole detection

```
For I=1 to N
If I (t)! = t (I)
Detect a node I as malicious node,
Else
Check DSN for following path selected for data transmission.
If DSN > Neighbor nodes DSN
And packet delivery ratio is less than a particular threshold,
Detect node as malicious node and broadcast message to all the nodes from base station.
End if
End if
End for
```

On the basis of above defined algorithm detection of sinkhole node has been detected.

4. RESULTS AND DISCUSSIONS

In order to verify our purposed approach for sinkhole detection in WSN, we have simulated our purposed work using 1000 X 1000 m area by deploying 50 nodes in the network and for sensing information from the area and this information have been transmitted from nodes to base station. In these process nodes location has been fixed and network has been deployed in the particular area. This node that has been deployed in the network has been used for sensing information by losing some energy in data sensing, aggregation, receiving and transmitting information. Malicious nodes % has been defined in the network that changes their hop count at each interval of time to attract source node to forward information.

In the process of sinkhole detection in WSN various parameters have been analyzed for performance evaluation of purposed work. These parameters are packet delivery ratio, end to end delay, network overhead and throughput of the system.

a. Packet delivery ratio

Packet delivery ratio in WSN has been measured for computing efficiency of the purposed system. Packet delivery ratio has been measured as the ratio between total numbers of packet properly delivered to destination to the total number of packet transmitted.

PDR=Total number of packets delivered/ Total number of packets send

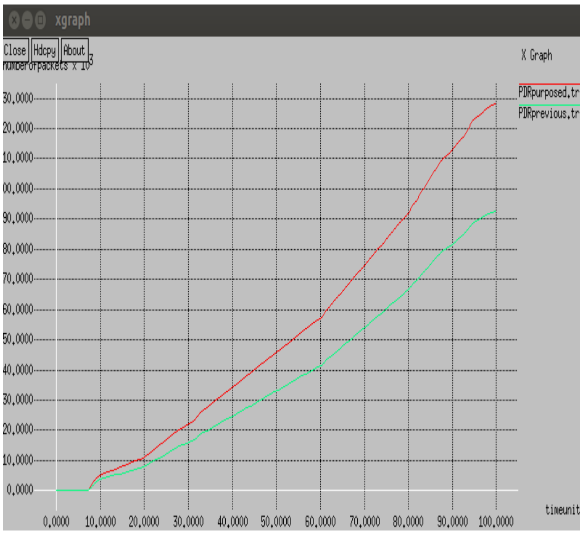

Fig 4 Packet delivery ratio

b. End to End Delay

In WSN end to end delay refers to delay occurred in the delivery of messages from source to destination due to network load and congestion occurred in the network. This has been measured by the total time taken in transmitting time from source to destination. It has been measured in milliseconds.

EED=D/Number of packet

Where D denoted sum of time duration taken in delivering all message from source to destination.

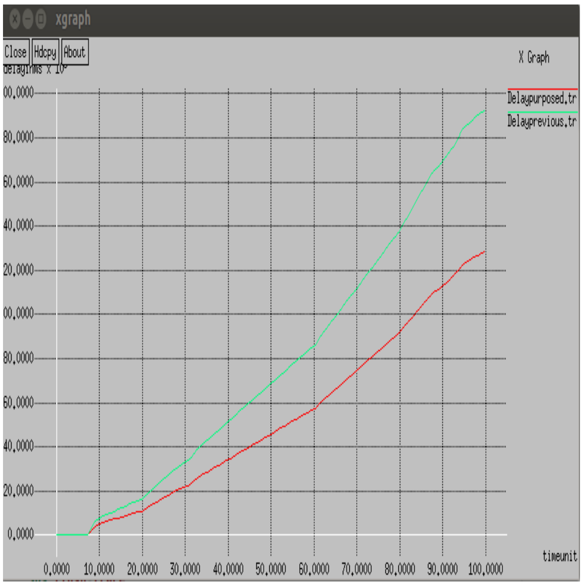

Fig 5 End to End delay

c. Throughput

In WSN throughput has been measured for prediction of bits that have been successfully transmitted in particular unit of time. Throughput is measured by total number of bytes transmitted over the network in particular unit of time.

Throughput= Total number of bits transmitted/ Simulation time

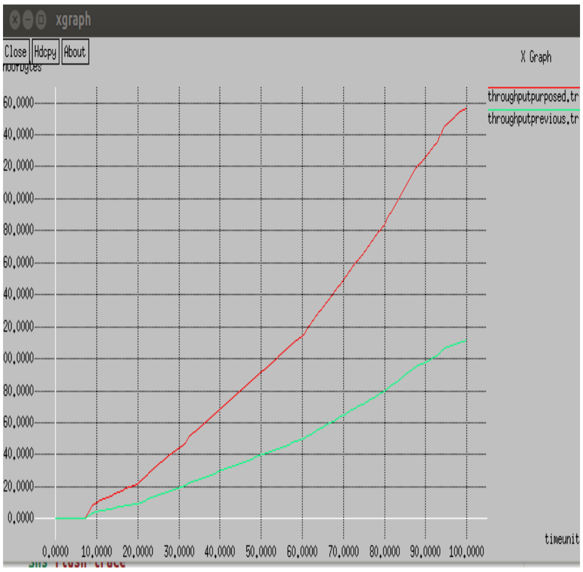

Fig 6 Throughput

d. Routing Overhead

Routing over is another parameter that has been analyzed for performance evaluation of purposed work. In the network data transmitting various routing packets have to be transmitted for checking of neighbor nodes are active or not. These routing packets do not contain any application content as data packets do. These packets utilize same bandwidth that data packets have been utilized. These routing packers are overhead in the network.

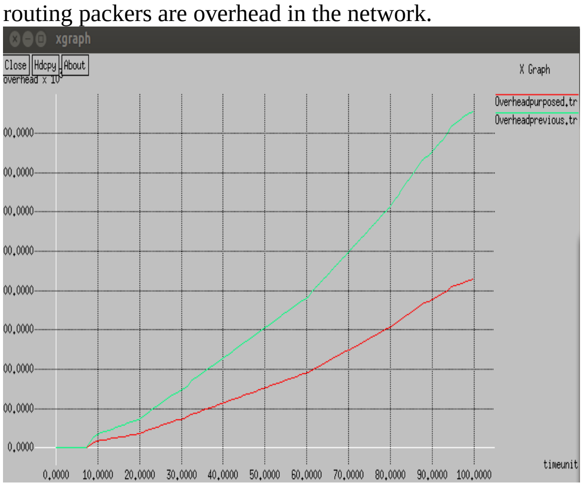

Fig 7 Routing Overhead

5. CONCLUSION

WSN is a type of networking that has been used for sensing information from non-approachable areas. In WSN energy and malicious nodes are two main concerned issues. Sinkhole attack performed by attackers degrades performance of the network. In this paper a hybrid approach has been purposed from detection of sinkhole attack in the network that causes degradation of the network performance. Purposed approach used destination sequence number and one hop neighbor mechanism to detect sinkhole occurred in the network. Purposed approach provides better efficiency for detection of malicious nodes occurred in the network and provide better throughput and packet delivery ratio.

6. REFERENCES

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

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

[3] 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.

[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] Sheela, D. “A non-cryptographic method of sink hole attack detection in wireless sensor networks” IEEE International Conference on Information Technology, 2011, pp. 527–532.

[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] Ritwik Banerjee “Energy efficient routing and bypassing energy-hole through mobile sink in WSN” IEEE Conf. on Computer Communication and Informatics (ICCCI), 2014, pp. 1 – 6.

[9] Babar Nazir “Mobile Sink based Routing Protocol (MSRP) for Prolonging Network Lifetime in Clustered Wireless Sensor Network” IEEE Conf. on Computer Applications and Industrial Electronics (ICCAIE), 2010, pp. 624–629.

[10] Pushpendu Karet “Reliable and Efficient Data Acquisition in Wireless Sensor Networks in the Presence of Trans faulty Nodes” IEEE Conf. on IEEE Transactions on Network and Service Management, 2016, pp. 99 – 112.