ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Investigating the Impact of Sinkhole Attack for Flat Based Multi Hop Routing Protocols in Wireless Mobile Sensor Networks

Akhila Polina
M.Tech Student,
Department of Computer Science & Engineering,
Raghu Engineering College,
Visakhapatnam.

Tatarao Vana, M.Tech
Assistant Professor,
Department of Computer Science & Engineering,
Raghu Engineering College,
Visakhapatnam.

Abstract:

Due to the enormous changes in the wireless technology within a short span of time, researchers are concentrated on micro electro mechanical systems as well as wireless mobile sensor networks due to enormous opportunities for doing their research. Wmsn networks are more vulnerable due to wireless environment. Due to the vulnerable nature of wmsn, so many types of attacks are attacked for network. Out of all threats sink hole attack is more severe type of attack, it will attack on all layers of a wmsn network, hence it is more dangerous type of attack. It consumes the all resources of a network by pretending as it has a shortest route to reach the sink node. In this paper, we proposed a method for detection and avoidance of sinkhole attack and we investigate the impact of sinkhole attack for flat based routing protocols in wmsn by considering the Qos metrics of network like throughput and average end to end delay from our simulation results using ns2. Hence we concluded that sinkhole effect is more on flat based routing protocols, due to the predefined routing paths available in the routing table. So that, malicious node presented in a route then there is no chance for transmission of a data in the network.

Keywords:

Wmsn, Protocol, Sinkhole Attack , QoS, Proactive , Reactive.

Introduction :

Due to the enormous change in the wireless technology from last decade, researchers are more concentrated on wmsn. Wireless mobile sensor networks are collection of distributed collection of distributed autonomous sensor networks for monitoring the environmental conditions.

Due to the self-configurable nature of wmsn, makes the researchers for applying the wmsn for central administrative applications. wmsn is used in military applications, industrial applications, home automation and surveillance applications. Hence wmsn is used for creating the dynamic networking for temporary communication. Due to the small size of sensor node in wmsn, have limited resources like low battery power, low computation capability, low communication capability and low processing power of the collected data.

Hence sensor nodes in the sensor network will consumes the resources, when they needed. Sensor nodes in wmsn are randomly deployed in monitoring area through wireless technology in topology form for providing the reliability and robustness of network and transmitted the collected data in a multi-hop routing manner from the sensor node to the sink node in a continuous manner in wireless environment. Due to the wireless nature of a network makes the environment more vulnerable.

Due to the vulnerable nature of wireless environment, security plays a crucial role for providing the confidentiality and integrity for transmitting collected data in the network. Hence, security in wireless mobile sensor networks placed in higher position of a research in many more applications.

Detection of a malicious attack in wireless mobile sensor network is a challenging issue and it is helpful for reducing the wastage of resources of a network to prolong the network lifetime autonomously and. In wmsn, different types of attacks are presented. They are black hole attack, wormhole attack, flooding attack, Sybil attack and sinkhole attack….etc.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

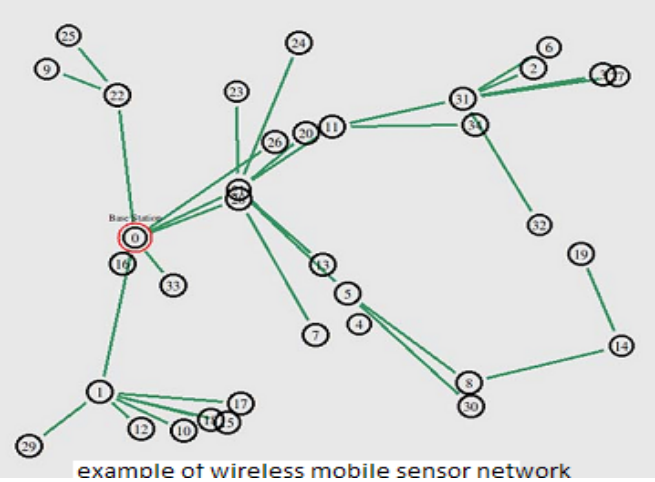

Fig 1: example of wireless mobile sensor network

Out of all types of security attacks in wmsn, sinkhole attack is more dangerous attack, because in this attack, malicious node attacks on each and every layer presented in the wmsn layer architecture. Sinkhole attack in network layer consumes almost all resources of a network by misleading almost all nodes in wmsn by pretending it has a shortest route to reach the sink node and drops the all packets. Hence, detection of sinkhole attack is a challenging issue for the new researchers in wireless environment nature of wmsn. In present work, we focused on detection of sinkhole attack for flat based routing protocols in wireless mobile sensor networks. Since sink hole attack, intruder attracts the traffic of a network for collected data transmission either using reactive routing protocols and proactive routing protocols. We simulated the wmsn in ns2 with proactive routing protocols and reactive routing protocols presented in flat based model and validate the simulation results using QoS metrics of a network. The rest of this paper organized as follows section II for flat based reactive routing protocols and proactive routing protocols presented in the wmsn ; section III for detection technique of sink hole attack for wmsn ; section IV for simulation environment of wmsn, with and without sinkhole attack in network layer and section V for results and analysis; section VI for conclusion based on analysis of results.

Flat based multi hop routing protocols:

Out of all layers in the wmsn architecture, network layer is having its own importance than all other layers, finding the route in the network layer for collected data transmission from sensor node to the sink node is consuming more resources of a network.

If we select the unnecessary path for data transmission causes to wastage of resources in the network. So that selection of a route in the network is very important for wmsn. Routing protocols in wmsn are divided into different ways based on the geographical structure of a network environment.Sensor nodes collect the data by using multi-hop routing based techniques. Sink node collects the data using query based approach in wmsn. Sink node sends the query for getting data within the network region; sensor node sends the data through already defined route or forming a route instantaneously. Based on selection of routing path, routing protocols once again divided into three types

1. Proactive routing protocols
2. Reactive routing protocols
3. Hybrid routing protocols

In proactive routing protocol, multi hop routing path is already predefined and stored in routing table. When the data was observed by sensor node, identify the available paths from the observed sensor node to the sink node in the network. According to that, the data is transmitted in the shortest path. However the constraint in the proactive routing protocol is overhead is more and follows the same route which is already defined. Because the path is maintained in a routing table of sensor node.It consumes the more energy of a sensor node. Example of proactive routing protocol is available in below figure.

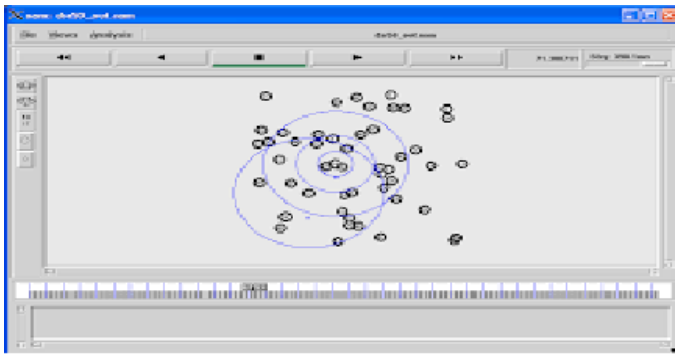

Fig 2: dsdv proactive routing protocol

In reactive multi hop routing protocol, route is established when the node in the network is required on demanded in adhoc fashion. For creating the routing path from sensor node to the sink node sensor node broadcast the route request to find the path to sink node. After reaching the route request to the sink node,

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

sink node send the route reply in the same path to the sensor node. Hence after establishing the adhoc route path between the sensor nodes to the sink node, collected data is transmitted. if any link failed in the routing path then route error message is broadcasted for finding the error where the link is broken. Reactive routing protocols are minimizing the overhead and bandwidth utilization due to the forming of a network instantaneously and maintained the records of routing paths in a tabular form. But to due to the reactive routing protocols delay is increased.

Working functionality of a reactive routing protocol in wmsn is as shown in below figure.

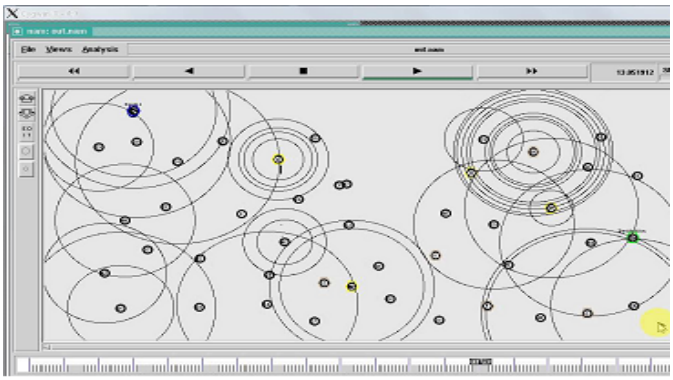

fig: example of reactive routing protocol for wmsn

Fig 3: aodv reactive routing protocol for wmsn

In hybrid routing protocol, route is established based on reactive and proactive multi hop protocols features.

Out of these three types of multi hop data centric routing protocols, we implemented proactive routing protocols and reactive routing protocols and compared the performance of these routing protocols when sinkhole attack is presented in the network by considering the QoS metric values of wireless mobile sensor network. And detection of a sinkhole attack by considering the transmission delay and average transmission energy of a sensor node to the sink node by considering the threshold values of transmission energy and transmission delay.

Sinkhole attack:

Due to the usage of wireless technology in wmsn, it is more vulnerable and there is a chance for more types of attacks for misleading the network goals. Hence, there are major challenging issues are presented for designing the wireless mobile sensor network.

Due to the limited resources of a sensor network, when an attack was happened in the sensor network, consumes resources of a network unnecessarily and reduces the network lifetime. Hence we need to detect the security attack and avoid the attack autonomously for increasing the network and providing the data confidentiality and integrity of a transmitted data of sensor node.

Based on the operation performed by the intruder, attacks are divided in to two types
1. Active attacks
2. Passive attacks

Attacker may find out the original content of a transmitted data and modify the transmitted data by using goal oriented active attacks or drops the transmitted packets by placed in the middle of the route.
Goal oriented active attacks presented in wmsn are

1.Black hole attack.2.Wormhole attack. 3. Sinkhole attack.4. DoS... etc.
Out of all goal oriented attacks presented in the wireless mobile sensor network, sinkhole attack is more dangerous type of attack. Sinkhole attack affects all layers presented in the wmsn architecture. In sinkhole attack, intruder captures the single node for holding the entire network. Sinkhole attack tries to attract all the traffic presented in the network towards the compromised node of an attacker by changing the original path presented in the network. Hence detection of sinkhole attack is very important for reducing the wastage of resources of a network.Hence, detection of sinkhole attack is very important to minimize the resource wastage present inside the network. Here in this paper, investigate the impact of sinkhole attack for flat based routing protocols with multi hop nature based on the availability of data at sensor node in the network. Sinkhole attack is of two types

1) Inside node acts as malicious node
2) Outside node of the network acts as malicious network

In the first type of sinkhole attack, malicious node attracts one of the nodes inside the network and makes that node for attracting all traffic present inside the network,so that network resources consumed unnecessarily and reduces the network lifetime. Where as in the second type of sinkhole attack, outside resourcefull node connected to the network and consumes the network resources unnecessarily by forming the tunneling with network.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

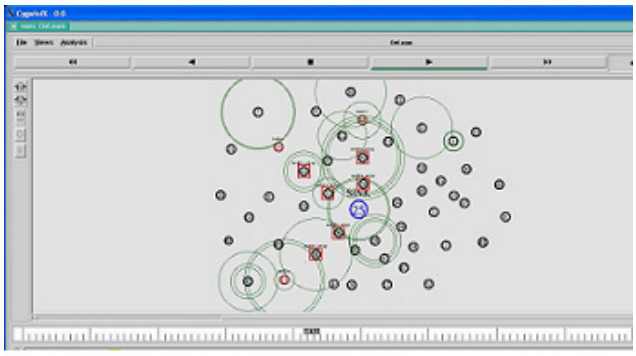

fig: wireless sensor network

In the network layer, finding the shortest path between sensor nodes to the sink node is the key issue presented in wireless mobile sensor network. This process consumes the resources of a network for finding the route in the network between the sensor nodes to the sink node for wireless mobile sensor networks. By considering the threshold transmission energy, time delay based on number of iterations and packet delivery ratio of the sensor nodes, find out the whether there is a sinkhole attack present or not in the network and if malicious node presented in the network, avoid the routes contained the malicious node for reducing the wastage of resources in the network. Here, we explained the detection and avoidance of a sinkhole attack in a step by step process by consider the network parameters. From this, we can easily judge whether an attacker is presented or not

Begin

Sa is the sensor network area Sn is no of senor nodes in the network

Sp is the total no of paths available for data transmission to the sink node

Sm is the total no of suspicious nodes presented in the sensor network

En is average transmission energy of a data for sensor node

Et threshold energy for transmission of data (Et= 0.0475J)

Pt is the total no of packets transmitted to the sink node

Pr is the total no of packets received by the sink node

Time delay(180) #for transmission of a data (threshold value)

After time delay calculate Pr= Pt/ Pr

If Pr is tends to ∞ and time delay>threshold time delay for 5 iterations and transmission energy is more than threshold energy then sinkhole attack is presented

Remove the suspicious node Sm from the route and find alternate paths to reach the sink node.

Hence remove the paths presented in the routing table and transmit data in other paths

Else

Continue for data transmission in the mobile sensor network

Simulation scenario of wmsn with and without sinkhole attack for multi hop routing protocol

Experimental setup:

We conducted simulation scenario, with 978x 524 simulation area with 12 sensor nodes inside the network for monitoring the network area. Sensor nodes are placed in a network by using random deployment model with uniform distribution in the simulation area by connecting in mesh topology structure. Each sensor node in the network with uniform speed 5m/s along with base station and makes any one of the sensor node as malicious node in the network. Consider the flat based routing protocols of wmsn. One is from proactive routing protocols list and another from reactive routing protocol. And the simulation time of the each experiment is 10 seconds with default mac properties.

Simulation pictures of dsdv and aodv routing protocols:

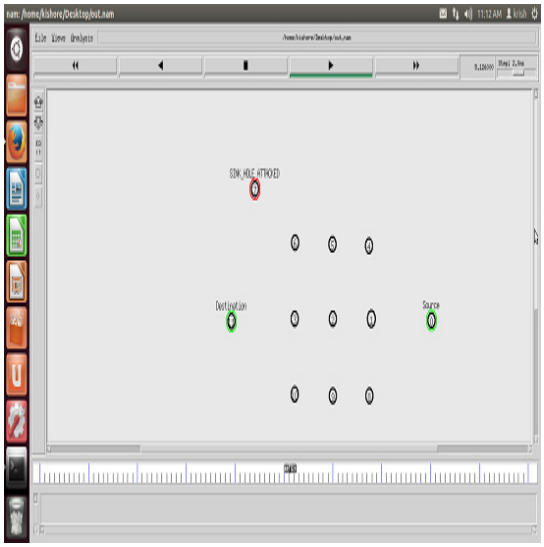

Fig :dsdv protocol with sinkhole attack

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

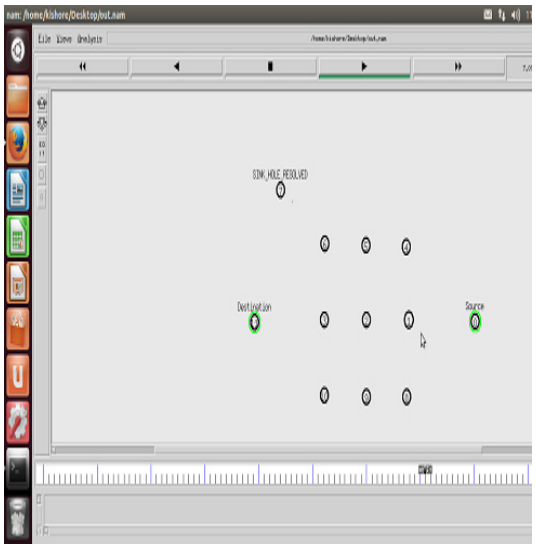

Fig: dsdv protocol without sinkhole attack

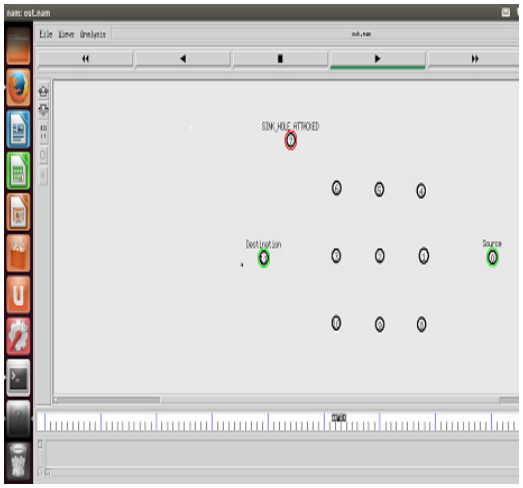

Fig: aodv protocol with sinkhole attack

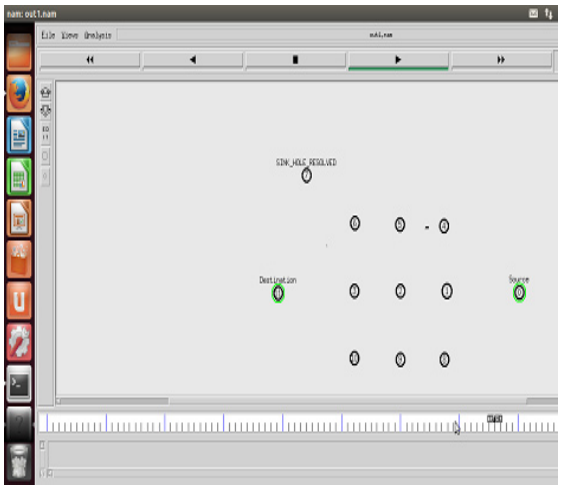

Fig:aodv protocol without sinkhole attack

Results and analysis:

From the experimental setup, simulate the scenarios of dsdv routing protocol with sinkhole attack and aodv routing protocol with and without sinkhole attack in different conditions under same conditions. The QoS metric values of a network will take for measuring the performance of a network in these different scenarios. Throughput and end to end delay are measure parameters which influence the network performance. Hence, we took those parameter values in all scenarios.

Results from the scenarios:

Routing protocol	Throughput(in kbps)	Avg End to End Delay(in ms)
Dsdv without sinkhole attack	1114.59	9948.1
Dsdv with sinkhole attack	1092.55	9961.63
Aodv without sinkhole attack	1202.2	9490.77
Aodv with sinkhole attack	1194.39	9495.73

Table: experimental results of Dsdv and Aodv with and without sinkhole attack

The above results, told that sinkhole attack affects on the Dsdv protocol for throughput parameter is 2% more where as in Avge end to end delay the gap is very low. In the case of Aodv routing protocol, affect of sinkhole

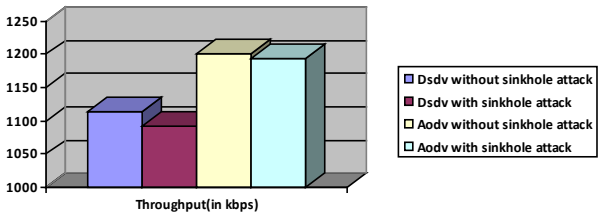

Fig: throughput of all scenarios in a graph

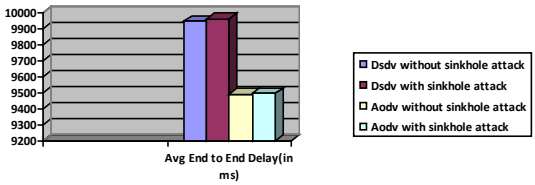

Fig: Avg End to End delay of all scenarios in a graph.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Conclusion:

The obtained results explain that dsdv routing is more vulnerable for sinkhole attack than compared with aodv routing protocol in wmsn environment. Hence proactive routing protocols not suitable for wireless mobile sensor network environments in flat based routing protocols even we detect and avoid the sinkhole attack. In future we can apply sinkhole attack for heirarichal multi hop routing protocols and analyze their performance for wireless mobile sensor networks.

References:

[1] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS '00), January 2000.

[2] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," IEEE Transactions on Wireless Communications, vol. 1, no. 4, pp. 660–670, 2002.

[3] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, Volume: 40 Issue: 8, pp.102-114, August 2002.

[4] C.Perkins, C.; Belding-Royer, E.; Das, S. (July 2003). Ad hoc On-Demand Distance Vector (AODV) Routing. IETF. RFC 3561. Retrieved 2010-06-18.[3]https://www.ietf.org/rfc/rfc3561.txt

[5] C.Perkins, Charles E. and Bhagwat, Pravin (1994). "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers" (pdf). Retrieved2006-10-20.

[6] J. A. Chaudhry, U. Tariq, M. A. Amin, and R. G. Rittenhouse, "Dealing with sinkhole attacks in wireless mobile sensor networks," Advanced Science and Technology Letters, vol. 29, pp. 7–12, 2013.

[7] I. Krontiris, T. Dimitriou, T. Giannetsos, and M. Mpasoukos, "Intrusion detection of sinkhole attacks in wireless mobile sensor network," in Proceedings of the 3rd International Workshop on Algorithmic Aspects of Wireless mobile sensor Networks (AlgoSensors '07), vol. 4837, pp. 150–161, Wrocław, Poland, 2007.

[8] Ioannis Krontiris, Tassos Dimitriou, Thanassis Giannetsos, and Marios Mpasoukos," Intrusion Detection of Sinkhole Attacks in Wireless mobile sensor Networks" in Third International Workshop, ALGOSENSORS 2007, Wroclaw, Poland, July 14, 2007. Pp 150-161

[9] H. Shafiei, A. Khonsari, H. Derakhshi, and P. Mousavi, "Detection and mitigation of sinkhole attacks in wireless mobile sensor networks," Journal of Computer and System Sciences, vol. 80, no. 3, pp. 644–653, 2014.

[10] Anita Kanavalli, Dennis Sserubiri, P Deepa Shenoy, Venugopal K R and L M Patnaik "A Flat Routing Protocol for Sensor Networks, " in International Conference on Methods and Models in Computer Science, 2009.

[11].www.google.co.in

.

[12]. https://www.ietf.org