IJCRT.ORG ISSN : 2320-2882
INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

PREVENTION OF BLACK HOLE ATTACKS IN MANETs USING ZONE BASED ROUTING

[1]Ms. Nikita, [2]Ms. Akanksha Bana

[1]M.tech (Scholar), School of Engineering and Technology, Noida International University,

Plot no-1, Sector- 17 A, Yamuna Expressway, Gautam Budh Nagar, U.P.-201310

[2]Asst. Professor, School of Engineering and Technology, Noida International University

Plot no-1, Sector- 17 A, Yamuna Expressway, Gautam Budh Nagar, U.P.-201310

Abstract

A MANET is a type of ad-hoc network that can change locations and configure itself on the fly. Because MANETs are mobile, they use wireless connections to connect to various networks. This can be standard Wi- Fi connections, or another medium, such as a cellular or satellite transmission. A Mobile Sensor Network (MSN) is a collection of mobilize attached sensor nodes. The relation between WSN and MSN is that when WSN is that when WSN nodes are moving they are known as MSN. Routing is a basic step for data exchange in MSN. It becomes essential to design a secure network as it finds applications in different fields where data and communication are important like that in defense areas and disaster rescue operations. The black hole attack is one of the security risks. In this attack, a malicious node falsely advertise or impersonates itself as a valid route for destination and once source selects it as a route, it starts dropping the data packets instead of forwarding. In this work, Zone Based Energy Efficient Routing Protocol (ZEEP) is one of the protocols which are the modification form of one of the most prominent routing algorithm, ad- hoc on demand distance vector (AODV) routing, for the MANETs.

In this black hole attack in AODV and ZEEP protocols using network simulator and have tried to find that the effect of Black Hole Attack is less effect in ZEEP protocol. Simulations are carried out in the MATLAB and the efficiency of the network in terms of throughput and Packet Delivery Ratio (PDR), End- to- End and Energy Consumption are measured.

In this research, I will identify or survey related work done by the various authors in past regarding prevention of the black hole attack in the network.

Index Terms- AODV, Black hole attack, MANET, ZEEP

1. INTRODUCTION

The increasing use of mobile devices brings new dimensions in wireless communication area. The proliferation of new, powerful efficient and compact communication devices life personnel digital assistants (PDA's), pagers, laptops and cellular phones, having extraordinary processing power paved the way for advance mobile connectivity. We are moving from the personal computer age to the omnipresent computing age in which a user utilizes at the same time, several electronic platforms through which he can access all the required information whenever and whenever needed. The nature of omnipresent devices makes wireless networks the easiest solution for their interconnection and as a consequences.

Now, most of the connections among the wireless devices are achieved via fixed Infra- Structure based service provider, or private networks. Whereas infrastructure based networks provide a great way for mobile devices to provide network service, it takes time and potentially high cost to set up the necessary infrastructure. There are many conditions where a person required necessary networking connections are not available in a given geographic area, and providing the needed connectivity and network services in these situations becomes a real challenge. For all these reasons, combined with advanced processing speed and memory capacity, new alternative ways to deliver mobile connectivity have been merged.

1.1 Wireless Sensor Network (WSN):-

When a person required necessary networking connections are not available in a given geographic area, and providing the needed connectivity and network services in these situations becomes a real challenge.

Wireless Sensor Networks (WSNs) enable new applications and require non- conventional paradigms for protocol design due to several constraints. Owing to the requirement for low device complexity together with low energy consumption (i.e. long network lifetime), a proper balance between communication and signal/ data processing capabilities must be found [1].

WSN is a collection of relatively inexpensive computational nodes that measure local environmental conditions like temperature, sound, pressure etc. forward such information to a base station for appropriate processing. WSN's nodes can sense the environment, can communicate with neighboring nodes, and can, in many cases, perform basic computations on the data being collected.

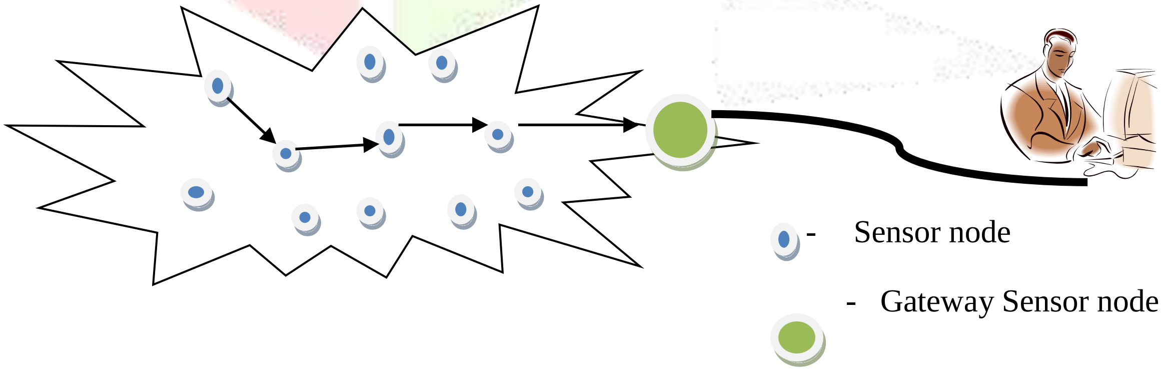

Figure: - 1 Wireless Sensor Network

Figure 1 describes the structure of a wireless sensor network. The application scenario for WSN includes environmental monitoring, from perimeter security to inventory management and from habitat monitoring to battlefield management with WSNs one can monitor and control factories, offices, homes, vehicles, cities, the environment etc. application like volcanic eruption, earthquake detection, and tsunami alerting that generally require wireless nodes deployed in remote, even difficult- to- reach locations.

1.2 Mobile Wireless Sensor Network (MSN):-

MSN can be defined as a wireless sensor network (WSN) in which sensor nodes are mobile. MSN is a smaller, emerging field of research in contrast to their well- established predecessor. Many of their applications are similar, such as environment monitoring or surveillance.

Here are some advantages of MSN-

a) Mobile nodes in MSN can be use to re- organize the network.
b) Mobility can reduce energy consumption during communication.
c) MSN can achieve better targeting.
d) By reducing no. of hops, the probability of error decreases and data fidelity can be achieved by MSN.

Not only advantages there are also many disadvantages,

a) Mobility in WSN is a very challenging task due to path breakage and node failure.
b) Frequent location changes can lead to drain of energy and increase of collisions.

Most of its application scenario requires efficient and reliable routing protocols other than flooding based data sending procedures. [2]

Routing is the most challenging issue and direct concern to energy in MSN comparable with adhoc and cellular networks [3]. Clustering techniques for routing in MSN is considered most suited based on its characteristics such as energy- efficient, scalable, lower latency etc.

1.3 Energy Efficient Routing Protocol:-

Energy efficient routing protocols are kind of routing techniques where sensor nodes save their energy level by using different technique to increase node and network lifetime.

The main goal of MSN is not only to transmit data from a source node to destination node, but also increase the lifetime of the network [4]. This can be achieved by employing energy efficient routing protocols.

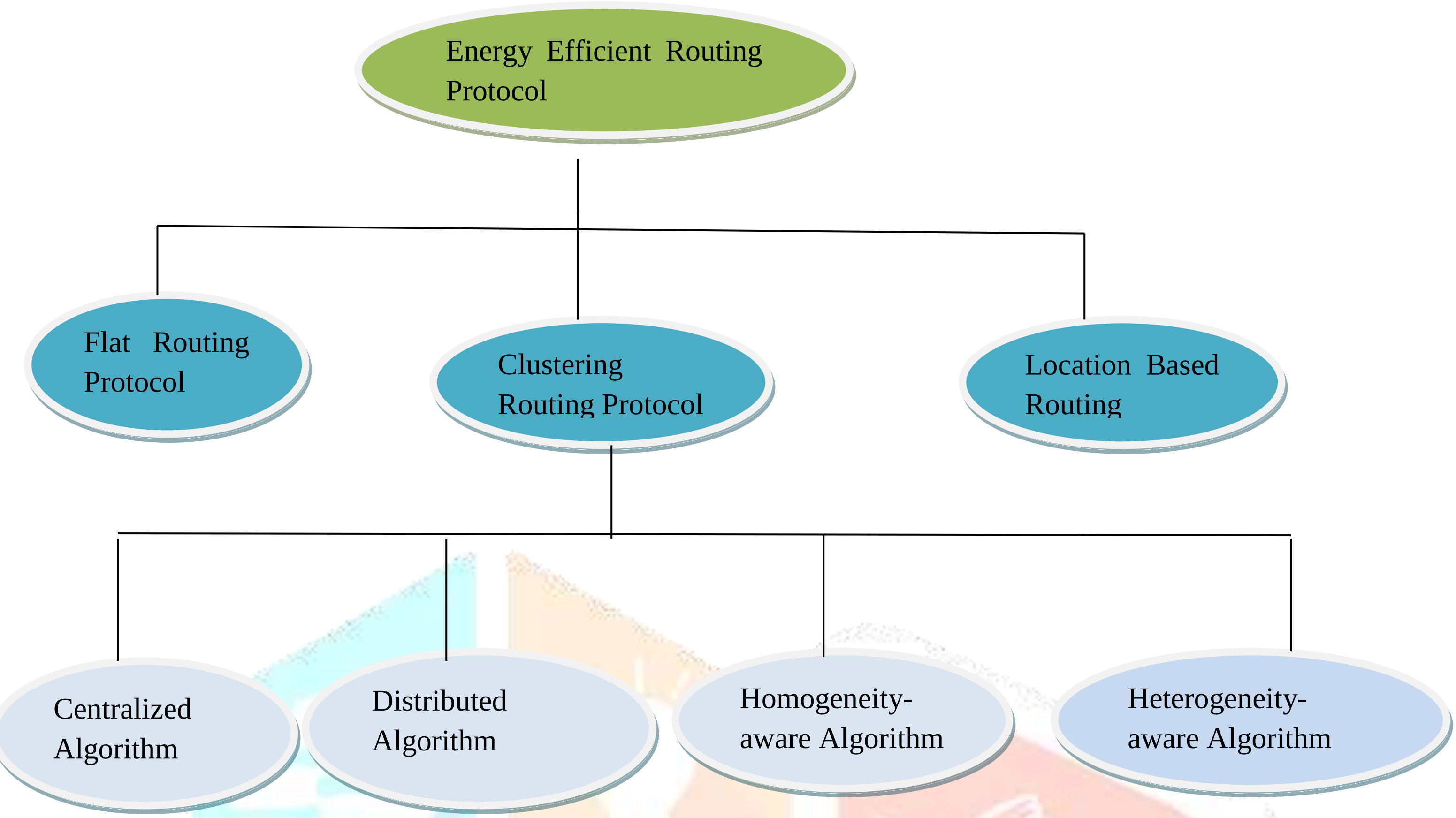
Energy Efficient Routing Protocol
Flat Routing Protocol
Clustering Routing Protocol
Location Based Routing
Centralized Algorithm
Distributed Algorithm
Homogeneity-aware Algorithm
Heterogeneity-aware Algorithm

Figure 2- Energy Efficient Routing Protocol

The on- going research in MSN is mostly concentrated on designing protocols that use the less possible energy during the communication of the nodes.

i. The potential task of the protocols is not only to find the lowest energy path from a source to a destination, but also to find the most efficient way to extend the networks lifetime.
ii. Routing algorithms, which are closely associated with dynamic programming, can be based on different network analysis communication system including maximal flow, shortest- route, and minimum span problems.
iii. The shortest path routing schemes figure out the shortest path from any given node to the destination node. If the cost, instead of the link length, is associated with each link, these algorithms can also compute the minimum cost routes.
iv. These algorithms can be centralized or decentralized. The usual way of routing in MSN is to route packets on the minimum- cost path from the source the destination (sink or base station).
v. In case that the nodes generate data constantly and the bandwidth is constrained, then routing data on the minimum- cost paths can overload wireless links- close to the base station.
vi. The efficient Dijkstra algorithm, which has polynomial complexity, and the Bellman- Ford Algorithm, which finds the path with the least no. of hops are the two very well known and well- defined algorithm for shortest path routing.

2. BLACK HOLE ATTACK

In black hole attack, a malicious node uses its routing protocol in order to publicize itself for having the shortest route to the destination node. This aggressive node publicizes its availability of fresh routes regardless of checking its routing table [5].

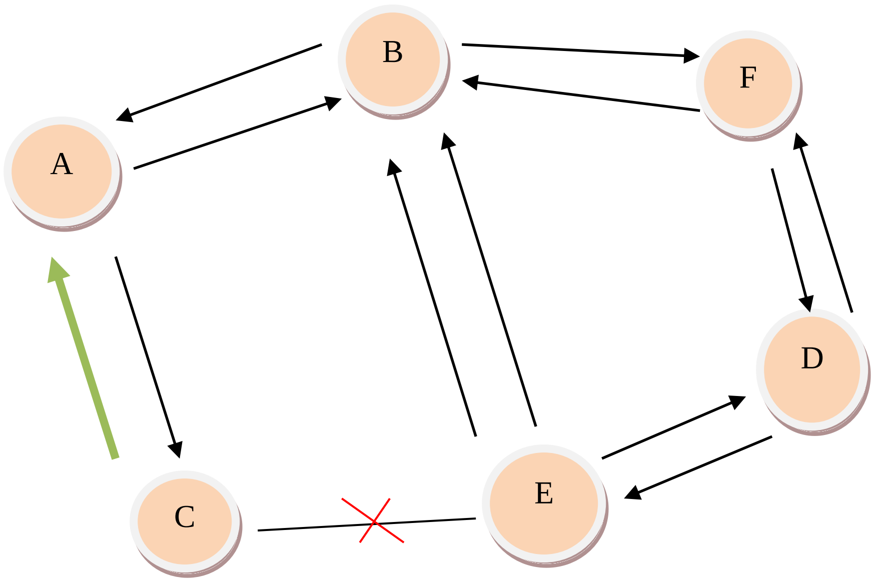

Figure- 3 Black Hole Attack

3. LITERATURE SURVEY

Dinesh Mishra et al. analyzed the effects of black hole attack in mobile ad hoc network using AODV and DSR routing protocols. The authors considered the throughput as the main performance measure. Simulation results, by NS-2 simulator, showed that a higher data packet loss when using DSR as compared to AODV. The observation and results showed that DSR data loss is around 55-60% in the presence of black hole attack, while 45-60% in the AODV routing. AODV protocol provides better performance than the DSR in the presence of black holes with minimal additional delay and overhead [6].

Deng et al. proposed a method to solve the black hole problem. This method is to disable the ability of an intermediate node to reply in a RREP message, so all reply messages should be sent out only by the destination node. This method increases the routing delay, especially for a large network. Besides, a malicious node can take advantage by fabricating a reply message claiming it was sent from the destination node. Another solution was proposed in this paper that depends on using one more route to the intermediate node that replays the RREQ message to check whether the route from the intermediate node to the destination node exists or not. If it does not exist, the reply message from the intermediate node is discarded and an alarm message to the network is sent out. Using this method, the black hole problem was avoided, and further malicious behavior was also prevented. This method cannot prevent multiple black hole attacks [7].

Patcha et al [8] proposed a proper way of prevention of black hole attack. To handle collision among nodes they introduced the watchdog method. In this algorithm, nodes are divided into three parts in network i.e. trusted, watchdog and ordinary nodes. Every watchdog node that is chosen should watch carefully its normal node neighbors a notice whether they can be behaved as trusted or malicious node.

Geo et al [9] presented aggregate signature algorithm to trace packet dropping nodes. They bind up into three algorithm (1) Creating proof algorithm, (2) The checkup algorithm, (3) The diagnosis algorithm. The advantages of this presented work are (1) the bandwidth overhead is low. (2) The security issues are fulfilled. (3) No need of bidirectional communication link. (4) There is broad scope of applications.

Golok et al. (2012) presents an approach which leads to prevent the black hole node [10]. Nobody will pay attention to malicious node's Hello message packet. The various authors have given various proposals for detection and prevention of black hole attack in MANET but every suggestion has some limitations and their respected solutions.

It is clear that malicious node is the main security threat that affects the performance of the AODV routing protocol. Every parameter has shown incredible improvement except avg. jitter and avg. end- to- end delay due to the overhead of key mechanism. It will be expensive such that the value of these parameters can be enhanced.

Modi et al. [11] in this paper an algorithm is proposed that used the trust value which is used to identify the malicious node, after identifying the malicious node it will be removed from the neighboring table and the source node would select the another path. This proposed algorithm offers a secure way transmission between any nodes in network topology. Researchers propose modification to the AODV protocol and justify the solution with implementation and simulation using NS-2.33. This simulation analysis shows the important improvement in end-to- end delay, throughput, and packet delivery ratio of AODV in presence of Black hole attack.

K. Selvavinayaki, DR. E. Karthikeyan et al. [12] to reduce the effect of black hole attack, a New Enhanced Proactive Secret Sharing Scheme (NEPSS) to detect the black hole nodes and to ensure the data confidentiality, data integrity and authenticity has been proposed. In first phase of the proposed algorithm, the detection of black hole attack is achieved using trust active and recommendation of the nodes. In second phase of the work, Enhanced Proactive secret sharing scheme is used to provide the data authentication and integrity. The simulation results shows the proposed algorithm achieves the better packet delivery ratio, misbehavior detection efficiency, fewer packets overhead and low end to end delay than the existing schemes.

Prachee N. Patil et al. [13] The Dynamic Source Routing (DSR) algorithm makes use of caching concepts to store all newly constructed routing paths in mobile ad hoc networks. Route caching is aggressively used by DSR. By virtue of source routing, it is possible to cache every overhead route without causing loops. Basically the forwarding nodes are caching source route from the packet and forwards it for future use. Also, the destination replies to all requests. Thus the source learns many alternate routes to the destination that are cached. Here authors of this proposed a new approach for black hole prevention in DSR based on route caching. In this approach, once the black hole node is detected in MANET during the path construction, they pass the black hole node id to path function of DSR. In this function, paths are ready to be added in route cache; however priory to add each path in route cache is decided by parsing these paths for presence of black hole node id. This process makes use of normal time of caching process only. In this paper, we propose the cache based black hole prevention algorithm for DSR routing protocols in MANETs.

4. EVALUATION RESULT

The proposed work aims at prevention of the black hole nodes in the network to reduce energy consumption in the network. It is based on two important things that black hole node modifies the sequence number with a huge value and secondly it always replies positively to every incoming RREQ.

Due to dynamic infrastructure- less nature and lack of centralized monitoring points, the ad hoc networks are vulnerable to Black hole attack. The network performance and reliability is broken by the attacks on ad hoc routing protocols. Many mechanisms have been proposed to overcome the Black hole Attack.

Overhearing the node's behavior

```
Watchdog ()
Begin
    If sender/ forwarder overhears a data packet
    Begin
        If expected packets
        Begin
            Recorded as a forwarded packet
            Status (next hop) =good
            And
            If sent packets time-out
            Begin
                If count (non-forwarded packet)> threshold
                Begin
                    If status (next hop)! = good
                    Begin
                        Send alarm packet to source
                        Status (next hop) = malicious
                    End
                End
            End
        End
    End
End
```

A malicious node or black hole node send Route Response (RREP) incorrectly of having route to destination with minimum hop count and when sender sends the data packet to this malicious node, it drops the entire packet in the network. The propose watchdog mechanism detect this black hole nodes in a MANET. This method first detects a black hole node in the network and then provides a new route to source node. In this, the performance of original-AODV and modified AODV called as watchdog-AODV (or W-AODV) in the presence of multiple black hole nodes is find out on the basis of throughput and packet delivery ratio and routing and control load.

Researchers propose modification to the AODV protocol and justify the solution with implementation and simulation using NS-2.33. This simulation analysis shows the important improvement in end-to-end delay, throughput, and packet delivery ratio of AODV in presence of Black hole attack.

5. CONCLUSION

The proposed scheme, Security is the important feature in wireless network. In these papers, to analyzed the effects of black hole attack in MANET using AODV and DSR routing protocols. The observation and result showed that DSR data loss is around 55-60% in the presence of black hole attack, while 45-60% in the AODV routing. The dynamic Source Routing (DSR) algorithm makes use of caching concepts to store all newly constructed routing paths in MANETs. Basically the forwarding nodes are caching source route from the packets and forwards it to the future use. In this method, if the black hole node is detected in MANET during the path construction, they pass the black hole node id to path function of DSR.

6. FUTURE WORK/ RECOMMENDATION

As a future work, the proposed scheme may be analyzed against various other schemes related to prevention of such attacks to check the efficiency of the proposed scheme. In future we will come with some wonderful ideas about how to solve this kind of attack in case of energy efficient routing protocol.

ACKNOWLEGMENT

I am very thankful to my supervisor and co- author Ms. Akanksha Bana, Assistant professor, department of CSE & IT, Noida International University for her continuous guidance, support and motivation towards my research.

REFERENCES

[1] K Sohraby, D Minoli, T Znati ‘Wireless Sensor Networks Technology, Protocols and Applications’. ISBN: 978-0-471-74300-2, 2007.

[2] Getsy S Sara and D. Sridharam, ‘Routing in mobile wireless sensor network: a survey’, Springer, Aug. 2013. Telecommunication System 57, 51- 79, 2014.

[3] Q. Cao, T. Abdelzaher, T. He and R. Kravets ‘Cluster- based Forwarding for reliable End- to- End delivery in wireless sensor networks’ IEEE Infocom 07, May 2007.

[4] Nikaos A. Pantazis, Stefanos A. Nikolidakis and Dimitrios D. Vergados, ‘Energy- Efficient Routing protocols in wireless sensor networks: A Survey’, IEEE Communications Surveys and Tutorials, Vol. 15 No. 2, Second Quarter 2013.

[5] Elahe Fazeldehkordi, Oluwatobi Ayodeji Akanbi, in a Study of Black Hole Attack Solutions, ISBN: 978-0-12-805367-6, 2016.

[6] Mishra D, Jain KY Agarwal S. “Behavior analysis of malicious node in the different routing algorithms in mobile ad hoc network (MANET)”, Proceeding form ACT’09: IEEE advances in computing. Control and Telecommunication Technologies, Trivandrum. December 2009; 28-29: 621-623.

[7] Deng H, Li W Agrawal DP. Routing security in wireless Ad Hoc networks. Cincinnati, OH, USA; IEEE Communications Magazine. ISSN: 0163-6804, Vol. 40, Oct. 2002. Pp. 70-75.

[8] A. Patcha, A. Mishra, “ Collaborative Security architecture of black hole attack prevention in mobile ad hoc networks [C]”, Radio and Wireless Conference, 2003, pp.75-78.

[9] X.P. Geo, W. Chen," A Novel Grey hole Attack Detection Scheme for Mobile Adhoc Networks [C]", IFIP International Conference On Network and Parallel Computing Workshop, 2007, pp. 209-214.

[10] Mr. Golok Panda, Mr. Gouri Shankar Mishra & Mr. Ashok Kumar Sahoo, "Prevention of Black Hole Attack in AODV protocols for Mobile Ad Hoc Network by Key Authentication." IRACST- International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 2, No.3, June 2012.

[11] Nirali Modi & Vinit Kumar Gupta, " Prevention of Black hole Attack using AODV Routing Protocol in MANET", International Journal of Computer Science and Information Technologies, Vol. 5(3), 3254-3258, 2014.

[12] K. Selvavinayaki, Dr. E. Karthikeyan, "A secured data transmission method using enhanced proactive secret sharing scheme to prevent black hole attacks in MANETs", International Journal of Theoretical and Applied Information Technology, Vol. 67 No. 3, 2014.

[13] P. N. Patil and A. T. Bhole, "Black hole attack prevention in mobile Ad Hoc networks using route caching," 2013 Tenth International Conference on Wireless and Optical Communications Networks (WOCN), Bhopal, 2013, pp. 1-6.