Volume 3, Issue 3, March-2016, pp. 92-97 ISSN (O): 2349-7084
International Journal of Computer Engineering In Research Trends
Available online at: www.ijcert.org

Hybrid Protocol for Security Peril Black Hole Attack in MANET

Priya Manwani, Deepty Dubey

Abstract:-MANETs (Mobile Ad hoc Network) is a self-governing system in which different mobile nodes are connected by wireless links. MANETs comprise of mobile nodes that are independent for moving in and out over the network. Nodes are the devices or systems that is laptops, mobile phone etc. those are participating in the network. These nodes can operate as router/host or both simultaneously. These nodes can form uninformed topologies as per their connectivity among nodes over the network. Security in MANETs is the prime anxiety for the fundamental working of network. MANETs frequently will be ill with security threats because of it having features like altering its topology dynamically, open medium, lack of central management & monitoring, cooperative algorithms and no apparent security mechanism. These factors draw an attention for the MANETs against the security intimidation. In this paper we have studied about security attack in MANET and its consequences, proposed technique for black hole detection is hybrid in nature which combines the benefit of proactive and reactive protocol and proposed technique is compared with AODV.

Keywords – MANET, AODV, ZRP

1. INTRODUCTION

MANET (Mobile Ad Hoc Network) is a congregation of mobile nodes that randomly forms the transitory network and it is a network without infrastructure. The security issue is more intricate in MANET when compared with common network which the intruder may get physical access to the wired link or pass over security holes at firewalls and routers. Mobile ad hoc network does not have a clear line of protection due to its infrastructures-less and each node shall be equipped for any threat. As MANET having dynamic characteristics hence it is reachable to all the users it may be a genuine user or the malevolent node which replicate the data or attack in the network. Some of the characteristics of MANET are as follows:

1. No Centralized Administration – Each node in the MNAET has its own communication capabilities for forwarding the data traffic over the network and adjusts according the topology.
2. Flexibility – MANET enables fast organization of the ad hoc network. When a node is to be associated with the network it should have the limited wireless communication range i.e. such node which can be available nearby.
3. Peer to Peer Connectivity of the Nodes – In MANET the nodes neighbor to each other forms a set for communication to which request response messages are flooded.
4. Resource Constraints – The node may have limited energy so this may limit the functionality of the network.
5. Dynamic Network Topology – A node discovers the service of a nearby node using the service discovery protocol.
6. Heterogeneous Nodes – In the MANET architecture any node can participate in forwarding the data packets, the node can be PCs, Smart Phones, Smart Tablets, Embedded Systems.

With the intention of the smooth progress of communication within the network, a routing protocol is used to determine routes between nodes. The most important objective of such an ad hoc network routing protocol is accurate and well organized route enterprise between a pair of nodes so that communication may be delivered in a timely conduct. Route creation should be done with a bare minimum of overhead and bandwidth utilization. Routing protocols may generally be categorized as:

© 2016, IJCERT All Rights Reserved

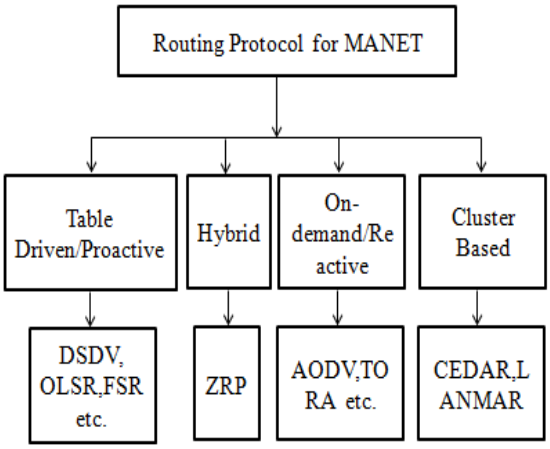


Fig 1. Routing Protocols in MANET

Reactive Protocols:

- Don't find route until demanded.
- When tries to find the destination "on demand", it uses flooding technique to propagate the query.
- Do not consume bandwidth for sending information.
- They consume bandwidth only, when the node start transmitting the data to the destination node.

Proactive routing protocols: Proactive routing protocols work as the other way around as compared to reactive routing protocols. These protocols constantly maintain the updated topology of the network. Every node in the network knows about the other node in advance, in other words the whole network is known to all the nodes making that network.

Hybrid Protocols: Hybrid protocols exploit the strengths of both reactive and proactive protocols, and combine them together to get better results. The network is divided into zones, and use different protocols in two different zones.

In this paper we have gone through various literatures and discussed about security issue in MANET. Basically we have focused on black hole attack in MANET. In section II of this paper we discussed different literature. In section III, IV we have provided comparison of literature and details about types of attack. In section V we have briefed about black hole attack. In section VI we have discussed about some bottle neck i.e. security issue in MANET. In last section we have concluded our survey.

2. LITERATURE SURVEY

Praveen Joshi [Elsevier 2011] presented security issues and their Countermeasures that are adopted on the Network Layer. Network security extends computer security, thus all the things in computer security are still valid, but there are other things to consider as well. Computer security is defined as follows: -Broadly speaking, security is keeping anyone from doing things you do not want them to do to, with, or from your computers or any peripherals In MANET, the nodes also function as routers that discover and maintain routes to other nodes in the network. Establishing an optimal and efficient route between the communicating parties is the primary concern of the routing protocols of MANET. Any attack in routing phase may disrupt the overall communication and the entire network can be paralyzed. Thus, security in network layer plays an important role in the security of the whole network. A number of attacks in network layer have been identified and studied in security research. An attacker can absorb network traffic, inject themselves into the path between the source and destination and thus control the network traffic flow.

Amin Mohebi et. al. [IJII 2013] focused on the numerous researches done in term of black hole attack on AODV-based MANETs. There are several proposals for detection and mitigation of black hole attacks in MANETs. However, most of solutions are not properly working against single black hole attacks and they suffer of detection of cooperative black hole attacks. The author has made a comparison between the existing solutions, but there is no reliable procedure since most of the solutions are having more time delay, much network overhead because of newly introduced packets and some mathematical calculations. In conclusion, the author recommends that using the hybrid techniques could be a proper way to detect cooperative black hole attacks. For future work, to find an effective solution to the black hole attack on AODV protocol which can be proposed.

Harsh Pratap Singh et. al. [IJCA 2013] said that Mobile ad hoc network is an assembly of mobile nodes that haphazardly forms the temporary network and it is an infra-structure-less network. Due to its self-motivator mobility in nature the nodes are more vulnerable to security threats which stimulate the performance of the network. In this paper, a review on a various types of coordinated attack is deliberated such as blackhole / grayhole attack which are most serious threats in mobile ad hoc network. In cooperative blackhole attack more than one node collude to each other hence this attack is more challenging to identify. This paper presents a review of different security mechanism to

© 2016, IJCERT All Rights Reserved

eliminate the blackhole / grayhole attack from the network.

Bhoomika Patel et. al. [Bhoomika Patel 2013] concluded that Blackhole attack is a main security threat. Its detection is the main matter of concern. Many researchers have conducted many techniques to propose different types of prevention mechanisms for blackhole problem. There are different security mechanisms are introduced to prevent blackhole attack. In proposed method not only blackhole nodes are prevented but also they are detected. Also the information of detected nodes are broadcasted to all other nodes to delete the entries of detected blackhole nodes from their routing table. The nodes who receives a broadcast message of detected blackhole nodes, are adding these blackhole nodes in the detected blackhole list so that all future communications can be avoided. Packet Delivery Ratio and Through put is increased with the help of the blackhole prevention and Detection method. By using Blackhole Prevention and Detection method improved security requirement in AODV.

Shahram Behzad, Shahram Jamali [IJCSNS 2015] said that in a wireless mobile ad hoc network (MANET),Similar to other systems, there is a risk of external agent infiltration. These networks are basically no-infrastructure, meaning no routing such as router or switch is used. So, they are highly posed to the risk of damage or exhausting all their common behavior energy. Hence, there is a growing interest towards the methods which can warn the network against the black hole attacks and external agent infiltration. black hole attacks which are among the most dangerous network attacks one of such security issue in MANET, These attacks are induced through each nodes existing in the network, where the node sends confirmation RREP to RREQ, no matter what its routing table is or whether a route exists towards the node. By doing this, the black hole node can deprive the traffic from the source node. So as to get all data packets and drops it.

3. TYPES OF ATTACK IN MANET

Because of their meticulous architecture, MANET's are more effortlessly attacked than wired network. We can classify two types of attack: the active attacks and the passive attacks. A passive attack does not interrupt the operation of the protocol, but tries to determine important information by listening to traffic. In its place, an active attack injects random packets and tries to interrupt the operation of the protocol so as to limit accessibility, gain authentication, or attract packets destined to other nodes. The routing protocols in MANET are quite anxious because attackers can effortlessly attain information about network topology.

A. Attacks Using Modification: One of the simplest ways for a malicious node to disturb the good operation of an ad-hoc network is to announce better routes (to reach other nodes or just a specific one) than the other nodes. This kind of attack is based on the modification of the metric value for a route or by altering control message fields.

B. Attacks using impersonation: These attacks are called spoofing since the malicious node hides its real IP address or MAC addresses and uses another one. As current ad-hoc routing protocols like AODV and DSR do not authenticate source IP address, a malicious node can launch many attacks by using spoofing. For example, a hacker can create loops in the network to isolate a node from the remainder of the network. To do this, the hacker just has to take IP address of other node in the network and then use them to announce new route (with smallest metric) to the others nodes. By doing this, he can easily modify the network topology as he wants.

C. Attacks using fabrication. [Praveen Joshi Elsevier 2011]

A number of attacks in network layer have been identified and studied in security research. An attacker can absorb network traffic, inject themselves into the path between the source and destination and thus control the network traffic flow.

Attacks at different stages are as:

- Attacks at the routing discovery phase
- Attacks at the routing maintenance phase.
- Attacks at data forwarding phase.
- Attacks on particular routing protocols.

Attacks by Names are as:

- Wormhole attack.
- Black hole attack.
- Byzantine attack.
- Rushing attack.
- Resource consumption attack.
- Location disclosure attack.

4. COMPARISON

© 2016, IJCERT All Rights Reserved

Sr. No.	Author	Description
1.	Jian-Ming Chang et. al. Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach IEEE 2015	This paper attempts to resolve this issue by designing a dynamic source routing (DSR)-based routing mechanism, which is referred to as the cooperative bait detection scheme (CBDS), that integrates the advantages of both proactive and reactive defense architectures.
2.	Praveen Joshi Security issues in routing protocols in MANETs at network layer Elsevier 2011	Author focused on the potential countermeasures currently used and designed specifically for MANET. In addition, we can say that security must be ensured for the entire system since a single weak point may give the attacker the opportunity to gain the access of the system and perform malicious tasks. Every day, the attackers are trying to find out the new vulnerability in MANET.
3.	Amin Mohebi et. al. A Survey on Detecting Black-hole Methods in Mobile Ad Hoc Networks IJII 2013	Author focused on the numerous researches done in term of black hole attack on AODV-based MANETs. The AODV is vulnerable against black hole attacks due to having network centric property, where all the nodes have to share their routing tables for each other. In this paper, author presented the survey of existing mitigation methods that have been proposed to secure AODV.
4.	Deepali Virmani et. al. Reliability Analysis to overcome Black Hole Attack In Wireless Sensor Network IJCSIT 2014	Author proposed reliability analysis scheme overcomes the shortcomings of existing cooperative black hole attack using AODV routing protocol. As soon as there is a path available for routing, its reliability is checked using the proposed scheme. The proposed reliability analysis scheme helps in achieving maximum reliability by minimizing the complexity of the system. The final path available after the reliability analysis using the proposed scheme will make the path secure enough to minimize the packet loss, end-to-end delay and the energy utilization of the network as well as maximize the network lifetime in return.
5.	Kanika Bawa and Shashi B. Rana Prevention of Black Hole Attack in MANET using Addition of Genetic Algorithm to Bacterial Foraging Optimization IJCET 2015	Author said that in MANET, routing attacks are peculiarly serious. So, this proposed work tries to design and implement Mobile Ad-hoc Networks using GA and BFO algorithm with Black hole attack and prevent the system from threat using these optimization algorithms.

5. PROPOSED METHODOLOGY

Until now very less attention has been given to Hybrid routing protocol which integrates the advantage of Proactive and Reactive routing protocol. In our proposed approach we have used ZRP (Zone Routing Protocol) which is Hybrid protocol. Zone routing protocol (ZRP) divides the topology into zones and search for nodes to make use of diverse routing protocols inside and between the zones depending on The strengths and weaknesses of these protocols. ZRP is completely modular, sense that any routing protocol can be utilized within and between zones. The size of the zones is definite by a parameter r describing the radius in hops.

© 2016, IJCERT All Rights Reserved

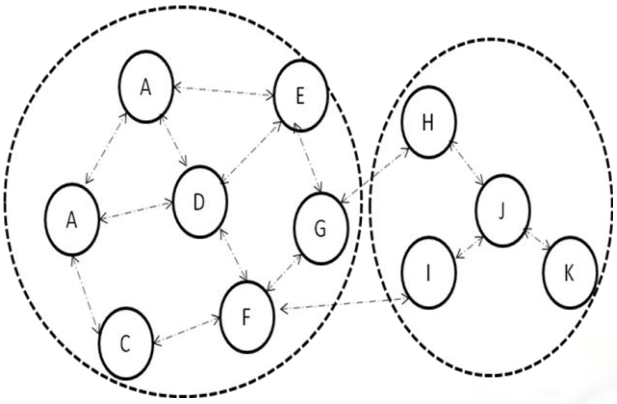
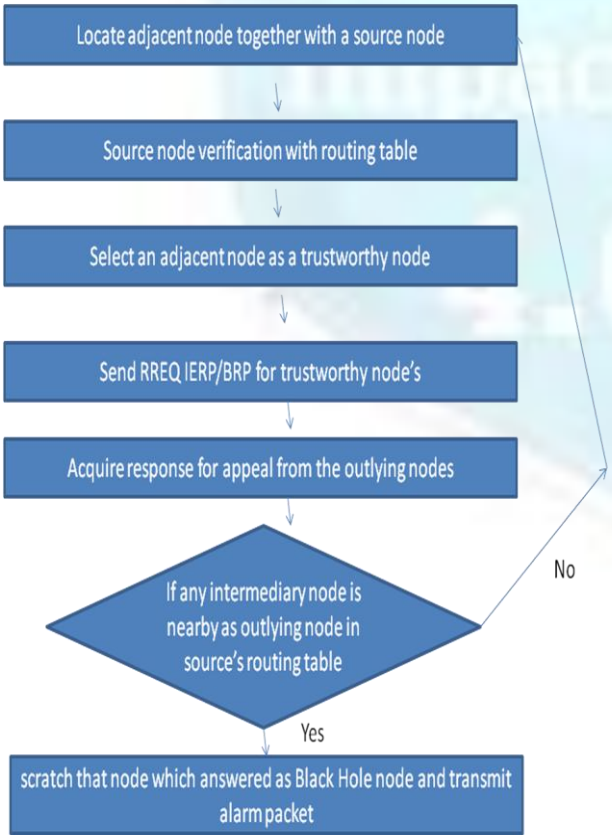


Fig 2. ZRP scenario showing the zones of node A and J using a r value of 2. Within the zones a proactive routing protocol is used while a reactive routing protocol is used between zones.

Intra-zone routing is completed by a proactive protocol because these protocols maintain a state-of-the-art view of the zone topology, which outcome in there is no preliminary delay when communicating with nodes within the zone. Inter-zone routing is completed by a reactive protocol. This removes the necessitate for nodes to keep a proactive unmarked state of the intact network.

5.1. ALGORITHM (PROPOSED SCHEME)



Some important points of ZRP are as follows:

- In the ZRP, proactive procedure scope confines only to the node's local neighborhood.
- Then again, the traversing all over the network, although global in nature, is done by proficiently querying elected nodes in the network, as divergent to querying all the network nodes.
- For a routing protocol to be well-organized, alteration in the network topology should have only a local consequence. In other terms, formation of a new link at one end of the network is a vital local event but, most possibly, not a important part of information at the other end of the network.
- Proactive protocols globally lean to share out such topological changes extensively in the network, incurring huge costs.

6. RESULT & DISCUSSION

MANETs (Mobile Ad hoc Network) is a self-governing system in which different mobile nodes are connected by wireless links. MANETs comprise of mobile nodes that are independent for moving in and out over the network. Nodes are the devices or systems i.e. laptops, mobile phone etc. those are participating in the network. We have used NS2 in ubuntu platform for simulation of our proposed work.

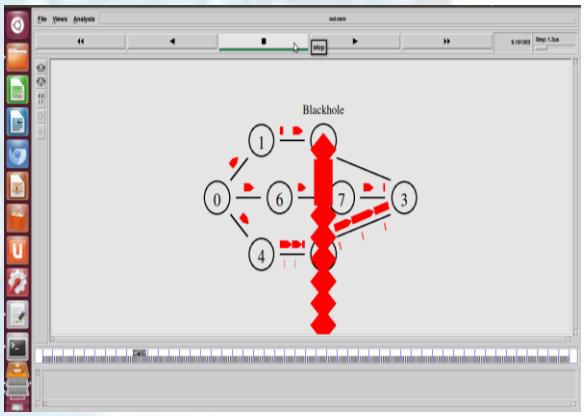
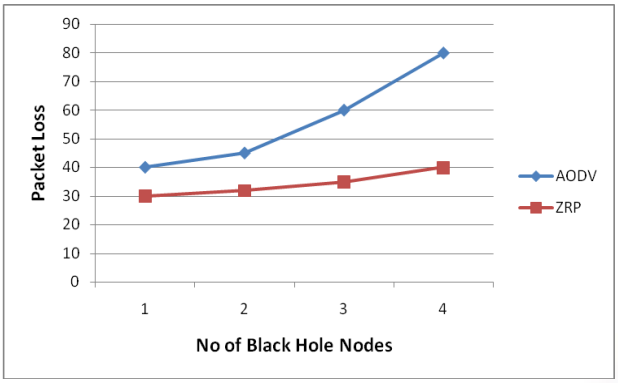


Fig 3.Packet drop due to Black hole node in ZRP and Data Transmission.

After going through our implementation in NS-2 we found find some facts upon which we are providing comparison between AODV and ZRP.

© 2016, IJCERT All Rights Reserved



6. CONCLUSION

MANET (Mobile ad hoc network) is a congregation of mobile nodes that randomly forms the transitory network and it is a network without infrastructure. The security issue is more intricate in MANET when compared with common network which the intruder may get physical access to the wired link or pass over security holes at firewalls and routers.

Security in MANETs is the prime anxiety for the fundamental working of network. MANETs frequently be ill with security threats because of it having features like altering its topology dynamically, open medium, lack of central management & monitoring, cooperative algorithms and no apparent security mechanism. These factors draw an attention for the MANETs against the security intimidation. In this paper we have studied about security attack in MANET and its consequences, how MANETs routing protocol detects black hole attack.

REFERENCES

[1] Praveen Joshi "Security issues in routing protocols in MANETs at network layer", Elsevier, doi:10.1016/j.procs.2010.12.156,pp 954-960, 2011.

[2] Amin Mohebi, Simon Scott "A Survey on Detecting Black-hole Methods in Mobile Ad Hoc Networks", Int. J. Innovative Ideas (IJII), vol. 13, no. 2, April - June 2013

[3] Harsh Pratap Singh, Virendra Pal Singh, Rashmi Singh "Cooperative Blackhole/ Grayhole Attack Detection and Prevention in Mobile Ad hoc Network: A Review", International Journal of Computer Applications (0975 – 8887), vol. 64, no.3, February 2013.

[4] Bhoomika Patel, Khushboo Trivedi "Improving AODV Routing Protocol against Black Hole Attack based on MANET ", International journal of Computer Science and Information Technology, vol. 5(3),pp 3586-3589, 2014.

[5] Rajib Das, Dr. Bipul Syam Purkayastha, Dr. Prodipto Das "Security Measures for Black Hole Attack in MANET: An Approach", HCIS 2014

[6] Deepali Virmani, Ankita Soni, Nikhil Batra "Reliability Analysis to overcome Black Hole Attack in Wireless Sensor Network", IJCSIT 2014.

[7] Shahram Behzad, Shahram Jamali "A Survey over Black hole Attack Detection in Mobile Ad hoc Network", IJCNS, vol.15, no.3, pp 44-51, March 2015.

[8] Priyanka Malhotra, Amit Chaudhary "Impact of Black Hole Attack on AODV Routing Protocol", IJEDR,vol.2, no.3, pp 3143-3148, 2014.

[9] Kanika Bawa and Shashi B. Rana "Prevention of Black Hole Attack in MANET using Addition of Genetic Algorithm to Bacterial Foraging Optimization", IJCET,vol.5, no.4,pp 2406-2411, 2015.

© 2016, IJCERT All Rights Reserved