ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 6, June 2016

An Approach For Revealing Of Attack In MANET ZRP

Himanshi Sahu
School of Engineering and IT, MATS University
Raipur C.G.

Deepak Xaxa
School of Engineering and IT, MATS University
Raipur C.G.

***Abstract*— MANETs (Mobile Ad hoc Network) are vulnerable to numerous attacks. MANET is a autonomous system in which diverse mobile nodes are linked by wireless links. MANETs encompass of mobile nodes those are self-regulating for stirring in and out over the network. Nodes are the devices or systems i.e. laptops, mobile phone etc. those are contributing in the network. These nodes can function as host/router or mutually concurrently. As per their connectivity these nodes can form uninformed topologies among nodes over the network. Sanctuary in MANETs is the leading apprehension for the elementary working of network. MANET often be laid up with security intimidation because of it have features like varying topology dynamically, lack of central management, open medium & monitoring, cooperative algorithms and no perceptible security mechanism. These factors draw an attention for the MANETs against the security threats. In this paper we have deliberated about security concern in MANET and its consequences, how different MANETs routing protocol handles black hole attack and we have proposed technique which reveals black hole in MANET, protocol used is hybrid in scenery which makes amalgam of proactive and reactive protocol and proposed method is compared with AODV.**

Keywords—MANET; AODV; ZRP

I. Introduction

MANET is a network of mobile and wireless machine nodes allied with radio which are arranged IP based without infrastructure. There is no any centralized administration mechanism. It is well-known for its routeable network properties where every node acts as a “router” to frontward the traffic to other particular node in the network. There are diverse types of MANETs

- InVANETs – Intelligent vehicular ad hoc networks make use of artificial intelligence to tackle unexpected situations like vehicle collision and accidents.
- Vehicular ad hoc networks (VANETs) – Enables effective communication with another vehicle or helps to communicate with roadside equipments.
- Internet Based Mobile Ad hoc Networks (iMANET) – helps to link fixed as well as mobile nodes.

Characteristics of MANET

- All nodes in MANET, works like both host and router. i.e. it is self-governing in behavior.
- The MANETs are competent of multi-hop routing when a source node and destination node for a message is beyond the radio range.
- The nodes can join or abscond the network any instant of time, making the network topology dynamic in nature.
- Mobile nodes are characterized with less memory, light weight features and less power.
- The consistency, efficiency, constancy and capability of wireless links are often substandard when compared with wired links. This figure out the unpredictable link bandwidth of wireless links.
- Mobile and impulsive performance which demands minimum human involvement to organize the network.
- Distributed nature of operation for security, routing and host configuration. A centralized firewall is absent here.
- All nodes have indistinguishable features with similar errands and capabilities and hence it forms a wholly symmetric environment.
- High user density and huge level of user mobility.
- Nodal connectivity is discontinuous.

With the intention of smooth the 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:

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.

II. Literature Survey

Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai [IEEE 2015] said that in mobile ad hoc networks (MANETs), a primary requirement for the establishment of communication among nodes is that nodes should cooperate with each other. In the presence of malevolent nodes, this requirement may lead to serious security concerns; for instance, such nodes may disrupt the routing process. In this context, preventing or detecting malicious nodes launching grayhole or collaborative blackhole attacks is a challenge. 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. Our CBDS method implements a reverse tracing technique to help in achieving the stated goal. Simulation results are provided, showing that in the presence of malicious-node attacks, the CBDS outperforms the DSR, 2ACK, and best-effort fault-tolerant routing (BFTR) protocols (chosen as benchmarks) in terms of packet delivery ratio and routing overhead (chosen as performance metrics).

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 infrastureless network. Due to its self-motivatedor 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 eliminate the blackhole / grayhole attack from the network.

Bhoomika Patel et. al. [IJCSIT 2014] said 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 mechanisums 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 Throghput is increased with the help of the blackhole prevention and Detection method. By using Blackhole Prevention and Detection method improved security requirement in AODV.

Ms.Apurva Kulkarni et. al. [IJSRM 2015] said that These MANET Stands for Mobile Ad-hoc network is an autonomous system of mobile routers and its associated hosts connected by wireless links. Because MANETS are mobile, they use wireless connections to connect to various networks Mobile Ad-hoc Network are formed dynamically by an Autonomous system of mobile nodes that are connected via wireless links. Nodes in MANET Communicate directly with each other when they are in same communication range otherwise they rely on their neighbors to send messages.MANET is a unique application. MANET is prone to various types of attacks due to its increased use. So Todays urgent need is to develop efficient intrusion-detection system to protect MANET from malicious attacks.This paper focuses on Enhanced Adaptive Acknowledgment (EAACK) which is an IDS Specially designed for MANET which will detect malicious nodes very efficiently and in addition to that EAACK can be extended further by adopting hybrid encryption as a preventive measure which will enhance security of messages in MANET.

Priyanka Malhotraet. al. [IJEDR 2014] said that The future of ad- hoc networks is really appealing, giving the vision of ―anytime, anywhere and cheap communications. Before those imagined scenarios come true, huge amount of work is to be done in both research and implementation. We tried to discover and analyze the impact of Black Hole attack in MANETs using AODV routing protocol by generating the traffic using the CBR, the same needs to be tested for the other ways of generating traffic i.e. exponential or the Poisson. There is a need to analyze Black Hole attack in other MANETs routing protocols such as DSR, TORA and GRP. Other types of attacks such as Wormhole, Jellyfish and Sybil attacks are needed to be studied in comparison with Black

Hole attack. They can be categorized on the basis of how much they affect the performance of the network.

III. Attacks 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:

1. Attacks at the routing discovery phase
2. Attacks at the routing maintenance phase.
3. Attacks at data forwarding phase.
4. Attacks on particular routing protocols.

Attacks by Names are as:

1. Wormhole attack.
2. Black hole attack.
3. Byzantine attack.
4. Rushing attack.
5. Resource consumption attack.
6. Location disclosure attack.

IV. Comparison

Sr. No.	Author	Protocol Used	Description
1.	Jian-Ming Chang et. al. IEEE 2015	Dynamic Source Routing (DSR)	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.	Harsh Pratap Singh et. Al. IJCA 2013	Ad hoc On Demand Distance Vector (AODV)	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.
3.	Bhoomika Patel et. al. IJCSIT 2014	Ad hoc On Demand Distance Vector (AODV)	Packet Delivery Ratio and Throghput is increased with the help of the blackhole prevention and Detection method. By using Blackhole Prevention and Detection method improved security requirement in AODV.

4.	Ms.Apurva Kulkarni et. al. IJSRM 2015	Enhanced Adaptive Acknowledgment (EAACK	This paper focuses on Enhanced Adaptive Acknowledgment (EAACK) which is an IDS Specially designed for MANET which will detect malicious nodes very efficiently and in addition to that EAACK can be extended further by adopting hybrid encryption as a preventive measure which will enhance security of messages in MANET.
5.	Priyanka Malhotra et. al. IJEDR 2014	Ad hoc On Demand Distance Vector (AODV)	In particular, black hole attacks can be easily deployed into the MANETs by the adversary. Our objective is to thoroughly capture and analyze the impact of Black Hole attacks on MANET performance using reactive (AODV) routing protocol with varying number of Black Hole nodes in the MANET.

V. Blackhole Attack

Number of security attacks has been identified in network layer by different research studies. An assailant can soak up network traffic, bring in themselves into the path between the source and destination and thus control the network traffic flow. Among different attacks we are concentrating upon Black hole attack.

FIG. shows how black hole problem arises, here node “A” want to send data packets to node “D” and initiate the route discovery process. So if node “C” is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node “A” before any other node. In this way node “A” will think that this is the active route and thus active route discovery is complete. Node “A” will ignore all other replies and will start seeding data packets to node “C”. In this way all the data packet will be lost consumed or lost.

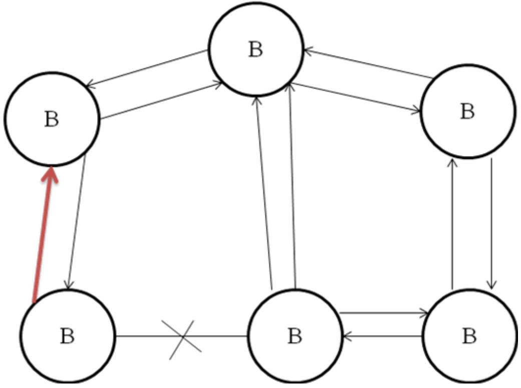

Fig. Black Hole Attack

VI. Problem Identification

After going through different literature we have identified some problem in security over MANET’s are as follows.

- Earlier the works done on security issues i.e. attack (Black Hole attack) involved in MANET were based on reactive routing protocol like Ad-Hoc on Demand Distance Vector (AODV).
- Black Hole attack is deliberated under the AODV routing protocol and its belongings are elaborated by stating how this attack disturb the performance of MANET.
- Very less consideration has been given to the fact to study the impact of Black Hole attack in MANET using both Reactive and Proactive protocols and to compare the susceptibility of both these protocols against the attack.
- There is requirement to address both these types of protocols as well as the impacts of the attacks on the MANETs.

VII. Proposed Methdology

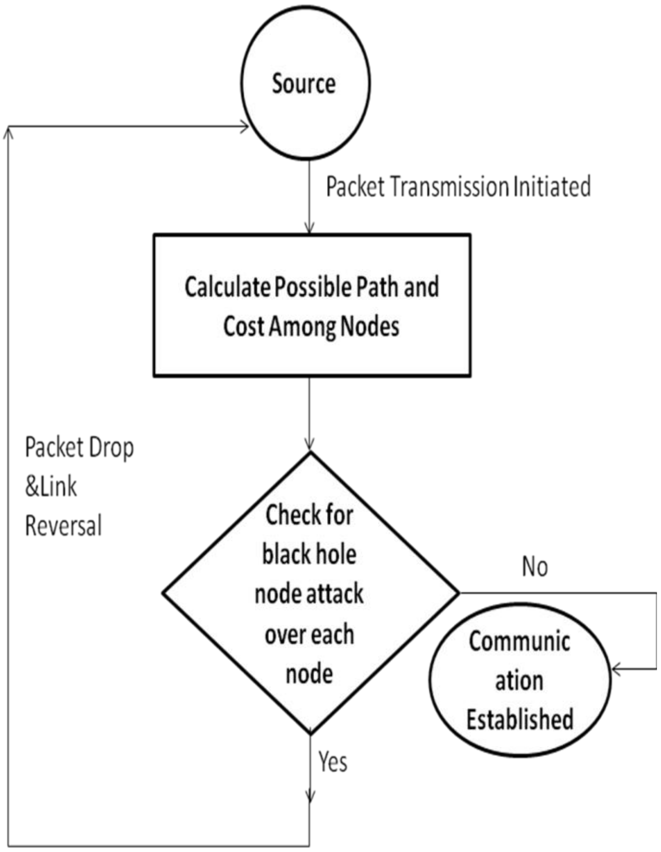
Source
Packet Transmission Initiated
Calculate Possible Path and Cost Among Nodes
Packet Drop &Link Reversal
Check for black hole node attack over each node
No
Communic ation Established
Yes

Fig. Proposed Layout

VIII. Result and Discussion

Performance Constraints	AODV	ZRP
Category	On-Demand	Hybrid
Protocol Type	Distance Vector	Link Reversal
Multicast	Yes	No
Message Overhead	High	Medium
Feature	Only keeps track of next hop in route	Routing range defined in hops
Network Throughput against black hole	Low	High

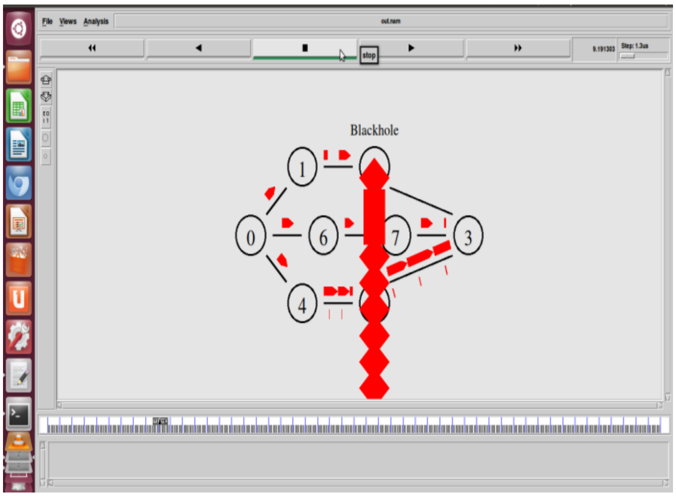

Fig. Packet drop due to Black hole node in ZRP

We have simulated our proposed approach in NS-2 and found facts accordingly below graph shows comparison between AODV and proposed hybrid ZRO protocol.

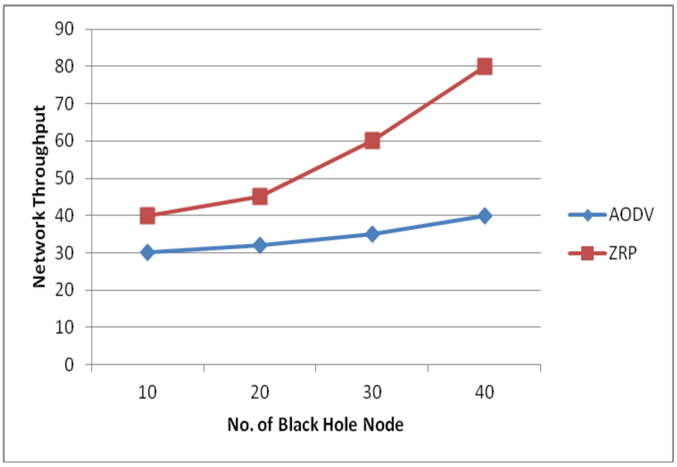

Fig. Performance Comaprsion ADOV vs ZRP

IX. Conclusion

Security in Mobile Ad-Hoc Network (MANET) is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats.

References

[1] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach IEEE 2015.

[2] Kanika Bawa, and Shashi B. Rana Prevention of Black Hole Attack in MANET using Addition of Genetic Algorithm to Bacterial Foraging Optimization IJCET 2015.

[3] Meenakshi, Kapil Kumar Kaswan Simulation Of Black Hole Attack In Adhoc Network Using Ns2 IJTR 2014.

[4] Swati Jain, Naveen Hemrajani Detection and Mitigation Techniques of Black Hole Attack in MANET: An Overview IJSR 2013.

[5] Shahram Behzad, Shahram Jamali A Survey over Black hole Attack Detection in Mobile Ad hoc Network IJCSNS 2015.

[6] Priyanka Malhotra, Amit Chaudhary Impact of Black Hole Attack on AODV Routing Protocol IJEDR 2014.

[7] M.Kayalvizhi, Mr.G.Arul Kumaran, A.Nithyasri Detection and Prevention of Sinkhole Attack on Zone Routing Protocol (ZRP) in MANET IJMTER-2014.

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

[9] Ms.Apurva Kulkarni, Mr.Prashant Rewagad, Mr. Mayur Agrawal Prevention and Detection of Attacks in MANET Using Hybrid Approach IJSRM 2015.

[10] Bhoomika Patel, Khushboo Trivedi Improving AODV Routing Protocol against Black Hole Attack based on MANET IJCSIT 2014.

[11] Harsh Pratap Singh Cooperative Blackhole/ Grayhole Attack Detection and Prevention in Mobile Ad hoc Network: A Review IJCA 2013.

[12] Amin Mohebi, Simon Scott A Survey on Detecting Black-hole Methods in Mobile Ad Hoc Networks IJII April - June 2013.