Security Coercion in Mobile Ad-Hoc Network: A Survey

Dr. Siddhartha Choubey
Shri Shankaracharya Technical Campus Junwani, Bhilai (C.G)

Sandeep Agrawal
Shri Shankaracharya Technical Campus Junwani, Bhilai (C.G)

Abstract

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 in MANET is more intricate when comparison is done with common network for which the intrusion can be done by getting physical way in to the wired link or pass over sanctuary holes at routers and firewalls. MANETs are defenseless to plentiful attacks. This is a self-governing arrangement in which different mobile nodes are associated by wireless links. MANETs cover of mobile nodes those are self-governing for moving in and out over the network. Nodes in MANET can operate as router/host or reciprocally concurrently. MANET often be unwell with security coercion because of it have features like lack of central management, varying topology dynamically, cooperative algorithms, open medium & monitoring, and no noticeable security mechanism. These made this issue as attentive focus by researcher for the MANETs against the sanctuary threats. In this paper we have elaborated about sanctuary distress in MANET and their penalty.
Keywords: MANET; AODV; ZRP

I. INTRODUCTION

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. Due to this MANET's posses different issues which are as follows:

- Wireless means: - Wireless medium is free to admittance by everybody and it is lying face down to bit errors or interfacing problem.
- Lack of Centralized System: - There is lack of central authority to observe the traffic in a extremely dynamic and outsized scale ad-hoc network therefore it makes the revealing of attacks complex.
- Resource accessibility: - An intruder can simply become an imperative routing agent and interrupt the network process by disobeying the protocol specifications as a MANET is based on cooperative environments.
- Infrastructure Less: - There are no definite infrastructures for certificates, key distribution, addressing, etc.
- Scalability: - The protocols and services that are applied to the adhoc network should be well-matched to the endlessly altering scale of the adhoc network.
- Dynamic topology: - Dynamic topology may contravene the conviction relationship among the nodes.
- Constrained power supply: - Node in mobile ad-hoc network can act in a selfish manner when there is use of battery to sustain some functions in the network.
- Bandwidth constraint: - Collaboration based security solutions must consider the bandwidth limitation related with links.
- Multi hop Routing: - As the nodes are reliant on each other for routing, adversaries can produce fabricated routes to create routing loops, false routes etc.

Safety measures in Mobile Ad-Hoc Network (MANET) are the principal distress for the basic functionality of network. Accessibility of network services, privacy and reliability of the data can be achieved by assuring that security issues have been met. MANET frequently endure from sanctuary attacks because of its features like open medium, altering its topology dynamically, lack of central monitoring and management, cooperative algorithms and there is no clear protection mechanism. These factors have tainted the battle field situation for the MANET adjacent to the security threats.

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

According to Harsh Pratap Singh et. al. [IJCA 2013] 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.

According to Bhoomika Patel et. al. [IJCSIT 2014] 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 black hole attack. In proposed method not only blackhole nodes are prevented but also they are detected. Also the information of detected nodes is 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 Throughput is increased with the help of the blackhole prevention and Detection method. By using Blackhole Prevention and Detection method improved security requirement in AODV.

According to Ms.Apurva Kulkarni et. al. [IJSRM 2015] 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.

According to Priyanka Malhotraet. al. [IJEDR 2014] 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.

According to Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai [IEEE 2015] 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).

III. SECURITY ATTACKS IN MANET

Due to their fastidious engineering, MANET's are more easily assaulted than wired system. We can characterize two sorts of assault: the dynamic assaults and the aloof assaults. A uninvolved assault does not intrude on the operation of the convention, but rather tries to decide imperative data by listening to activity. In its place, a dynamic assault infuses arbitrary parcels and tries to interfere with the operation of the convention in order to breaking point availability, pick up confirmation, or draw in bundles bound to different hubs. The steering conventions in MANET are entirely on edge since assailants can easily achieve data about system topology.

1) 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.
2) 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.

A. *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. BLACK HOLE ATTACK

Number of security assaults has been recognized in system layer by various examination thinks about. An attacker can drench up system activity, get themselves into the way between the source and destination and hence control the system movement stream. Among various assaults we are concentrating upon Black opening assault.

FIG. shows how black hole problem arises, here node "S" want to send data packets to node "D" and initiate the route discovery process. So if node "M" 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 "S" before any other node. In this way node "S" will think that this is the active route and thus active route discovery is complete. Node "S" will ignore all other replies and will start seeding data packets to node "D". In this way all the data packet will be lost consumed or lost.

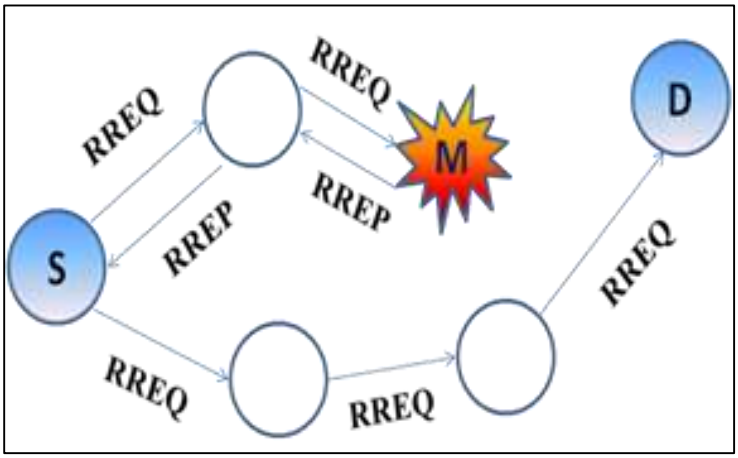

Fig. 1: Black Hole Attack

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. CONCLUSION

Security in Mobile Ad-Hoc Network (MANET) is the most imperative sympathy toward the fundamental usefulness of system. Accessibility of system administrations, privacy and uprightness of the information can be accomplished by guaranteeing that security issues have been met. MANET frequently experience the ill effects of security assaults due to its elements like open medium, changing its topology progressively, absence of focal checking and administration, helpful calculations and no reasonable barrier system. These components have changed the war zone circumstance for the MANET against the security dangers.

REFERENCES

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