Improved Routing Security using Intrusion Detection System in Mobile Ad Hoc Network

Hemlata Kaurav
Computer Science Engineering
Maharana Pratap College of technology, India
hkaurav07@gmail.com

Krishna Kumar Joshi (Asst. prof.)
Computer Science Engineering
Maharana Pratap College of technology, India
krishnakjoshi@gmail.com

***Abstract*—Ad-hoc networks have lots of difficulties than conventional networks. It has challenges like foundation less and self-organizing networks. They don't have any settled base. In MANETs there will be no incorporated power to manage the network. Nodes need to depend on different nodes to keep the network connected. As the ad-hoc network is dynamic and each transmission in these networks get to be powerless against numerous number of attacks and security turns into a major issue.**

Keywords— Mobile Ad Hoc Network, Attacks, Routing Protocol, AODV, Intrusion Detection System, Security.

I. INTRODUCTION

A mobile ad hoc network (MANET) is a technique of wirelessly mobility nodes that dynamically self-prepare in temporary and arbitrary network topologies. In this n network, central nodes perform and cooperate like a router and transmit messages from unique node to another. It is enough helpful in circumstances where we have shortage of fixed grid infrastructure, such as an emergency situations or rescue operation, medical assistance. For scholar it has been rapid an interesting research region in create a routing protocol discovering the best probable route in a dynamic atmosphere of MANET's [1].

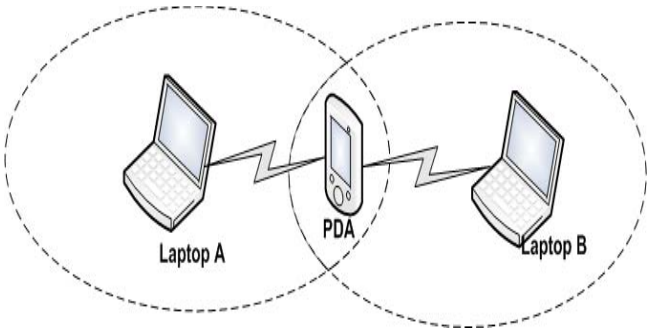

Fig.1 MANET

The nodes are referred to various mobility devices like mobiles, laptops, MP3 players, PDAs etc. Thus we can define a MANET as a self-organized collection of nodes which kind a temporal net without the help of any central base station. An important issue in such networks is the security reason thru the continuous dynamic disposition of the network. Nodes in as networks communicate with every one when they're within a certain transmission range but they need the cooperation from the middle nodes for forwarding packets when they're multi hop far from every one [2].

II. ATTACKS ON MANET

MANETs are therefore found to be the subject to various attacks for instance Wormhole, Black hole, Flooding, Link Spoofing, DoS, Replay, Rushing, Byzantine, gray hole etc.

A. Black Hole Attack

Black hole attacks are the most generic attacks in the DOS attack category. In Black hole attack the malicious node try to stupid the dispatcher node that it's the legitimate destination node thru transfer incorrect reply messages to the dispatcher. The malicious node may reply with the very high sequence number so the sender node would think that the malicious node is a target node or it has a novel node to the target.

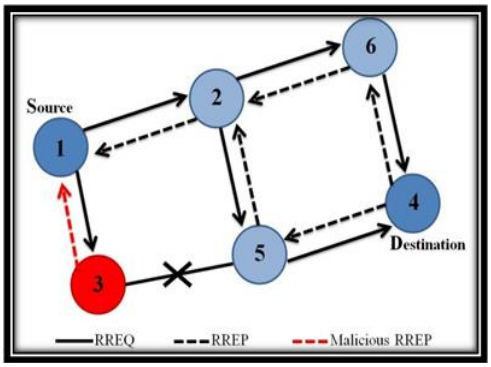

Fig.2 Black Hole Attack

Suppose Source S wants to communicate to the Target D. As shown in Figure 2. S broadcasts the RREQ packet to the network. Nodes M and 1 receive the RREQ. Node 1 will check its routing table. If node 1 finds in the routing table a route to the receiver it will generate the RREP packet and send to source otherwise it will forward the RREQ packet further. On the another way, malicious node M after receiving the RREQ packet from S does not forwards the packet and immediately sends a false RREP to S. As node M doesn't necessity to check its routing table, S will accept the first reply

from M. Thus S gets a wrong belief that M has a legal path to the receiver and then forwards the data packets through M. The malicious node M then intercepts the data packets and start to drop them moreover the malicious node intercepts the manage packets too. This can cause risky problems. A malicious node intercepts the RREQ packets and prevents the establishment of route and also saves its battery for forwarding its own packets. Black hole attacks are divided into two segments for instance Sole black hole attack and Collaborative attack [3].

B. Gray hole attack

Gray hole attack is a form of the attack on the MANET. In gray hole Attack a malicious node inhibit to forward few packets and merely drops them. The attacker choicely drops the packets originating from a sole IP address or a range of IP addresses and forwards the outstanding packets. All nodes conserves a routing table that save the subsequent hop node info for a route a packet to a target node, when a sender node needs to route a packet to the target node, it uses a specific route if such a path is accessible in its routing table. Otherwise, node begins a route detection procedure thru broadcasting the Route Request (RREQ) message to its near. On receiving the RREQ message, the middle nodes update their routing tables for an opposite route to sender node. A Route Reply (RREP) message is transfer again to the dispatcher node when the RREQ query arrive either the target node own self or any other node which has a existing route to a destination. The gray hole attack has two significant phases, in first levels, a malicious node utilizes the AODV protocol to encourage own self like having a legal path to the target node, with the interrupting intension, even though the route is false. In the next phase, nodes drop the interrupted packets with a creation probability. Finding of gray hole is a difficult process [4].

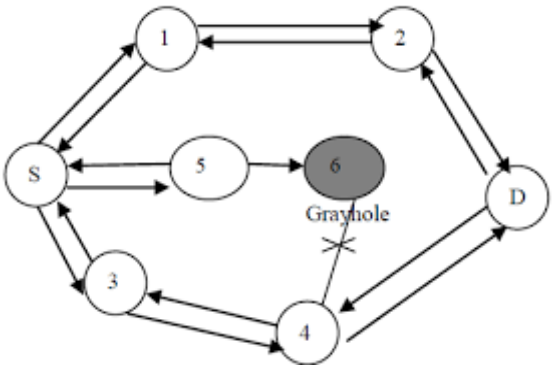

Fig.3 Gray hole attack

C) Wormhole attack

The wormhole attack, where two colluding nodes that are far apart are linked thru a tunnel giving an illusion which they are neighbors. Every of these nodes accept route request and topology control messages from the grid and transmit it to the other colluding node thru tunnel that will then repetition it into the grid from there. Thru exploiting this additional tunnel, these nodes are able to advertise which they have the shortest path thru them. Once this link is established, the attackers may elect each other as multipoint relays (MPRs) that then lead to aswap of few topology controls (TC) data packets and c messages thru the wormhole tunnel. Since these MPRs forward flawed topology info, it outcomes in spreading of incorrect topology info throughout the grid. On acceptance this wrong info, another nodes may transfer their messages thru them for rapid delivery. Thus, it stops honest intermediate nodes from establishing links amid sender to receiver. Infrequently, due to this, even a wormhole attacker may fall victim to its own success. Several kinds of Wormhole attacks are recognized. , a specific form of wormhole attack called as “in-band wormhole attack” is identified. A game theoretic process has been followed to detect intrusion in the grid. Presence of a crucial authority is supposed for monitoring the network. This is a limitation in wireless scenario such as military or emergency rescue [5].

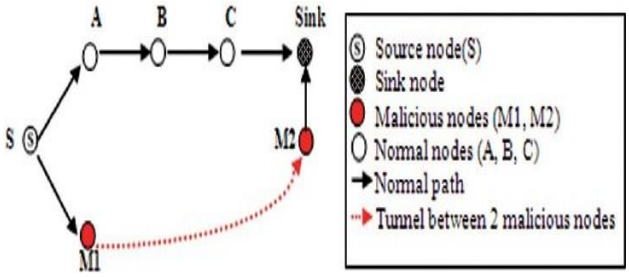

Fig. 4 Wormhole attack

III. IDS

An IDS stand for Intrusion Detection System that is a software system exploited to examine malicious activities and policy violations in a network and generates reports. These basically fall into three classes namely, Anomaly based and Specification based and Signature Based, IDS. The signature based IDS is used to match the data against known characteristics and used to limit known attacks. The Anomaly based IDS includes taking the profiles of usualdemean or of systems by automated training and flagging the unknown activity to be suspicious while under operation. This detects unknown attacks but triggers false alarm on high probability. The specification based system, abstracts the expected behaviors of vital objects and crafts security objectives, which are then compared with required object characteristics. The main merit of this is previous knowledge of the attack is not required and hence extensively used in the applications of many stringent programs and many other protocols. Precisely, AODV routing protocol has been accepted and exactly monitors the vulnerabilities in the n/w layer. A result is defined depend on the GA IDS method for the discovery of weaknesses in AODV [6].

IV. LITERATURE SURVEY

Nitika Gupta (2016) et al presented that these attacks and also about how by using hardware rather than software we can solve the wormhole attacks by using cryptography and the digital signature method [7].

Vaishali Gaikwad (Mohite) (2015) et al presented that a unique way which uses Cooperative Cluster Agents. In the define method they pass SRT-RRT and DRI table like an input to Cooperative Security Agents. Based on these inputs the CSAs use cross checking and detection flow mechanisms for identifying cooperative black hole attack, once it is detected that can be avert thru passing alert notification in the MANET. For implementation of the proposed scheme we will use network simulator - *ns-2.35*. Evaluate define the solution and equate it with standard AODV protocol in words of packet delivery ratio and end-to-end delay and throughput,[8].

S.V. VASANTHA (2015) et al presented that Bulwark-AODV which prevents single or accessory Black hole attacks thru identifying malicious route replies at source and intermediate nodes and finds a shortest valid path. It also works in case of single adjacent node to the sender and when there are many Black holes in the grid. It detects Gray holes thru snooping the data packets ACKs. ACK Forgery if any is recognized thru the source thru checking the ACK return time. Simulation results indicate better performance even though special cases are considered [9].

Dipamala Nemade (2015) et al presented that the extensive distribution and open medium of node creates MANET permeable to malicious attacks. It request for more secure IDS. The EAACK IDS resolves the limitations of accept confined transmission power, collision, and incorrect misbehavior report in past system. EAACK makes use of DSR routing protocol for network of small scale. However, as the grid size enhancement and due to dynamic environment, performance of DSR protocol affects [10].

Nisha Soms (2015) et al presented that an improved detection tool in a Zone depend IDS. A comprehensive simulation is executed to reading the presentation of ZBIDS below several routing attacks as wormhole and impersonation and black hole and grayhole. The simulation outcomes are depends on the define architecture and demonstrations which the enhanced ZBIDS has achieved desirable presentation to meet the security necessity of MANETs [11].

Sara chadli (2014) et al presented that novel IDS architecture for MANETs, this architecture is a mixture replica hierarchical depend on cooperation and clusters replica depend on a SMA (multi-agent system). In this architecture, agents use knowledge related to global security ontology, it can be exploited to infer new detection rules [12].

Santosh kumar Sabat (2014) et al presented that an Energy efficient leader choice in MANET for IDS. As MANET don't have any central controller, the leader choice in every cluster becomes very significant. The objective of the chosen leader is to serve the IDS for the whole cluster. Our leader election is depending on energy and Reputation value level of each node. NS2 atmosphere and presented the evaluation of energy Residual or consumption energy of nodes having fixed transmission range with define adaptive energy pattern. Adaptive energy pattern adjusts the range of transmission of every node depend on the maximum distance amid nodes in every cluster. Energy of each node is conserved as compared to node having fixed transmission range [13].

Hizbullah Khattak (2013) et al presented that hybrid method for stopping black/gray hole attacks thru electing second shortest route for secure route selection and hash timestamp and function base result for containing data transmission [14].

Mohammad Rafiqul Alam(2010) et al presented that a novel detection mechanism known as RTT-TC, that is depend on round trip time (RTT) topological comparisons (TC) and measurements. MANET running on AODV routing protocol which define method that can reach both high detection rate and precision of alarms [15].

V. PROBLEM STATMENT

In this work when network area enhance and number of node increase collusion will occur so that number of packet drop increase in this condition secure path maintain is going to be tough or on the basis of secure routing not possible to find out malicious node.

VI. PROPOSED WORK

In our proposed work we use directional antenna for built highly connected environment for forwarding packet in Mac layer we used direct RTS or CTC for making highly connective graph and after that we use secure routing for forwarding packet for secure routing we enhance the working of AODV protocol. The work will be conducted using NS-2 tool.

Proposed Algorithm:

Step:1 initialize network
Step:2 use directional antenna
Step:3 built network fully connected
Step:4 for packet forwarding, RTS/CTC used directly
Step:5 now secure routing use for forwarding the packet
Step:6 we get enhanced working of AODV protocol
Step:7 exit

VII. RESULT ANALYSIS

The performance of the network is described in terms of throughput, packet delivery ratio and routing overhead. The

implementation of the proposed work is performed in NS2. The simulation is done on the nodes and AODV protocol is used for the communication.

1. Throughput
   Throughput of the network is calculated by the total number of packets sent over a particular period of time. In this graph, it is shown that the throughput increase as compared to existing works.

Fig. 5 Throughput Graph

2. Packet delivery Ratio
   Packet delivery ratio is the number of packets received over the number of packets sent which should be more for the network performance. In our graph, it is shown that our proposed technique is much better than the existing techniques.

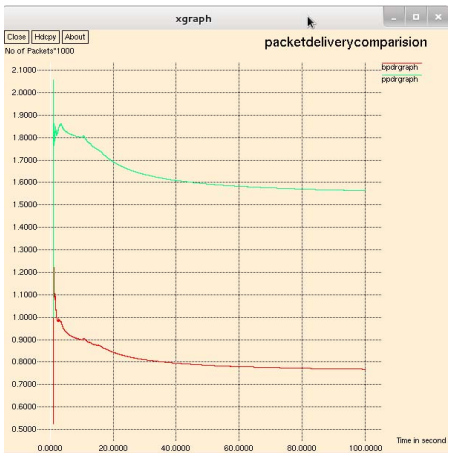

Fig. 6 PDR Graph

3. Routing overhead
   It is the total number of control packets in the network which reduce the performance. In our graph, it shows that the routing overhead is less which is good for the network.

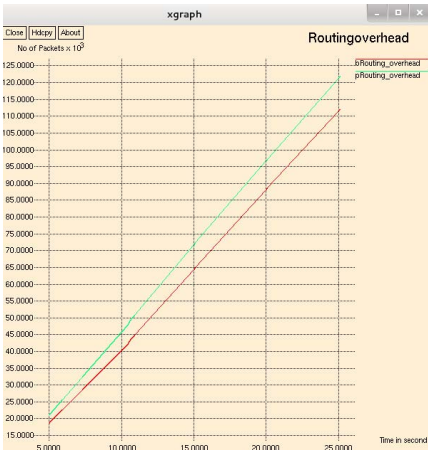

Fig. 7 Routing Overhead Graph

Conclusion

Packet-dropping attack has dependably been a noteworthy risk to the security in MANET. In this paper we have introduced an overview of the best in class on securing MANETs against packet dropping attack. A large portion of the current methodologies are utilized to identify just the bad conduct interfaces as opposed to the malicious nodes. Besides, they neglect to identify halfway dropping of packets in MANET. The detection of packet droppers in MANETs is a test despite the fact that numerous methodologies have been proposed against packet dropping attack. Some methodologies that depend on cryptography and key management are too expensive.

REFERENCES

1. Hizbullah Khattak, Nizamuddin. "A Hybrid Approach for Preventing Black and Gray Hole Attacks in MANET", 978-1-4799-0615-4/13/$31.00 ©2013 IEEE.

2. Rakesh Ranjan, Nirnemesh Kumar Singh, Mr. Ajay Singh, "Security Issues of Black Hole Attacks in MANET", ISBN:978-1-4799-8890-7/15/$31.00 ©2015 IEEE.

3. Mr. Ankit D. Patel, Mr. KartikChawda, "*Blackhole and Grayhole Attacks in MANET"* ISBN No.978-1-4799-3834-6/14/$31.00©2014 IEEE.

4. Parineet D. Shukla, Ashok M. Kanthe, Dina Simunic, "An Analytical Approach for Detection of Gray Hole Attack in Mobile Ad-hoc Network", 978-1-4799-3975-6/14/$31.00 ©2014 IEEE.

5. ReshmiMaulik, NabenduChaki, "A Comprehensive Review on Wormhole Attacks in MANET", 978-1-4244-7818-7/10/$26.00_c 2010 IEEE.

6. K.S.Sujatha, VydekiDharmar, R.S.Bhuvaneswaran, "Design of Genetic Algorithm based IDS for MANET", ISBN: 978-1-4673-1601-9/12/$31.00 ©2012 IEEE.

7. Nitika Gupta, Shailendra Narayan Singh, "WORMHOLE ATTACKS IN MANET", 978-1-4673-8203-8/16/$31.00_c 2016 IEEE.

8. VaishaliGaikwad(Mohite), LataRagha, "Security Agents for Detecting and Avoiding Cooperative Blackhole Attacks in MANET", 978-1-4673-9223-5/15/$31.00_c 2015 IEEE.

9. S.V. VASANTHA, DR. A. DAMODARAM, "Bulwark AODV against Black hole and Gray hole attacks in MANET", 978-1-4799-7849-6/15/$31.00 ©2015 IEEE.

10. Dipamala Nemade, Ashish T. Bhole, "Performance Evaluation of EAACK IDS using AODV and DSR Routing Protocols in MANET", 978-1-4673-9563-2/15/$31.00 ©2015 IEEE.

11. NishaSoms, R.SajiPriya, A.SukkiriyaBanu, Dr.P.Malathi, "AComprehensive Performance Analysis of Zone Based Intrusion Detection System in MobileAd hoc Networks", 978-1-4673-6823-0/15/$31.00©2015 IEEE.

12. Sara chadli,Mohamed Emharraf, Mohammed Sabar, Abdelhak Ziyyat, "the design of an architecture for MANET based on multi-agent", 978-1-4799-5979-2/14/$31.00 ©2014 IEEE.

13. SantoshkumarSabat, SujataKadam, "Adaptive Energy Aware Reputation Based Leader election for IDS in MANET", 978-1-4799-3358-7114/$31.00 ©2014 IEEE.

14. HizbullahKhattak, Nizamuddin, "A Hybrid Approach for Preventing Black and Gray Hole Attacks in MANET", 978-1-4799-0615-4/13/$31.00 ©2013 IEEE.

15. Mohammad RafiqulAlam, King Sun Chan, "RTT-TC: A Topological Comparison Based Method to Detect Wormhole Attacks in MANET", 978-1-4244-6871-3/10/$26.00 ©2010 IEEE.