# Detection and Prevention Methodology for DoS Attack in Mobile ad-hoc Networks

**Shilpa Paul[1], Arpit Chitodiya[2], Deepak Vishwakarma[3]**

*[1]PG Scholar & SKSITS Indore*
*[2]Asst. Professor & SKSITS Indore*
*[3]Asst. Professor & IIST Indore*

---

**Abstract -** *a mobile ad-hoc network (MANET) is an impermanent infrastructure fewer networks in which node communicate with each other lacking of any centralized controlling mechanism. Thus these active behaviors of such network have potential applications in conference, disaster relief and battlefield scenario, and have received important attention in current years. In MANET mobile nodes are open to move from one location to another location such that position of mobile nodes is repeatedly changed. Due to the mobility (rate of position change of mobile node with respect to time) of nodes and constantly changing network topologies pose a number of challenges. Due to this preeminent route may no longer remain at same time instant. There is some security concern which increases fear of attacks on the Mobile ad-hoc network. One of the major concerns in mobile ad-hoc network is a traffic DoS attack in which the traffic is choked by the malicious node which denied network services for the user. Malicious nodes introduce itself as a node which come into the shortest path from source to destination and when it receive data it will interrupt communication in such ways. Mobile ad-hoc network must have a secure way for transmission and communication which is quite a challenging and vital issue. In order to provide secure communication and transmission, the researcher worked specifically on the security issues in mobile ad-hoc network, and many secure routing protocols and security measures within the networks were proposed. The motive of the work is to study about DoS attack and how it can detected in the network. Existing approaches for finding a malicious node which cause traffic jamming is based on nodes retains value and any node whose retains count goes to zero, then every node of that network got message about that malicious node. The proposed approach finds a malicious node using reliability value which determined by the broadcast reliability packet (RL Packet). In this approach at the initial level every node has zero reliability value, specific time slice (TS) and transmission start with a packet termed as reliability packet, node who responded properly in specific time, increases its reliability value and those nodes who does not responded in a specific time, decreases their reliability value and if it goes to less than zero then announced that it's a malicious node. Reliability approach make service availability and retransmission time.*

***Key Words***: MANET, Attacks, DoS, TS, RL.

## 1. INTRODUCTION

A MANET (mobile ad hoc network) is a set of devices or nodes that transmit data across a wireless communication medium mostly based on radio frequency without any existing fixed infrastructure or centralized control. There will be no middle control or infrastructure of network for a MANET to be set up, therefore making its deployment immediate and inexpensive. The nodes capability to move freely ensures a flexible and adaptable dynamic network topology which is an additional important feature of a mobile ad-hoc network. Few of the MANET applications includes emergency disaster relief, wilderness expeditions (transient networks), and community networking through health monitoring using MSN (medical sensor network) and military operations over a battlefield (vulnerable infrastructure).

There are a number of issues in Mobile ad-hoc network which addresses the areas such as IP addressing, protocols, radio interference, security, mobility management, routing, power Constraints, bandwidth constraints, Quality of service(QoS) etc.. Mobile ad-hoc network consists of a set of mobile nodes that carry out basic networking functions like packet forwarding, routing, and service discovery without the help of an established infrastructure. Nodes of a network relay on one another in forwarding a packet to its destination, due to the limited range of each mobile host's wireless transmission [1]. This confirms that the network will not cease operative just because one of the mobile nodes travels out of the range of the others. Nodes should be able to enter and leave the network as they want. Because of the fixed limited transmitter range of the nodes, multiple hops or nodes are generally needed to reach other hops or nodes.
Mobile ad-hoc network has several loop-false due to infrastructure-less environment. These loop-false makes opportunity for attackers to influence the smoothness of network operations. Attacker or unauthorized person can put different attacks by identifying loop-false in the network, which is violating security policies of the network. One of them is a DOS attack to infer such below policies.

- Availability
- Confidentiality
- Authenticity

Additionally, attacks influence different network resources also those are precious for running network process. Some of them defined below.

- Battery Power
- Lifetime
- Throughput
- Packets delay
- Routing overhead

Several mechanisms and protocol advised on individual black hole attack, but required to more work on the DoS attack on which few work approached by researches. In already existing advised approach, certain problem found. Firstly node sent data packet to determine the value of reliability levels of nodes in the network. When nodes play role as a black hole in a group then it do not acknowledgement of data packet because these watch data packets only, in this scenario data packet of the sender read by black hole node. Secondly, is too difficult to detect node as black hole when its reliability level value zero initially when the network is deployed. Thus we required approach to prevent data packet, and perfect detection of DoS attack nodes in the network.

## 2. RELATED WORK

This part of paper presents a small number of newly proposed mechanisms for Management of Node location update based problem in MANET.

In the trade-model, proposed in [6], each and every device has a tamper- resistant security module, public key infrastructure (PKI) to guarantee validation, so it is used for account management. There are two billing mechanisms were introduced that charge nodes as a function of number of hops messages have travelled.

An APE (ad-hoc participation economy) that uses a committed banker node to manage accounts was proposed in [7]. Unlike the tamper-resistant method, the APE uses dedicated banker nodes for account management and it also has services for converting virtual currency into real monetary units. Enhanced mechanisms that use a node as a transaction manager are not reasonable in dynamic ad-hoc networks while location tracking incurs extra overhead.

An associated reputation-based mechanism such as a RPG (reputation participatory guarantee) was proposed [8]. This method provides network layer solutions that indentify selfish nodes lacking of propagating reputation ratings in the wireless network.

A trade-based scheme that based on the accessibility of banker nodes was presented in [9]. This model does not use any tamper- resistant hardware but as a substitute uses credit-clearance services in a non-wired overlay network.

In [10], a reputation-based scheme that discovers the effect of misbehavior on network performance was introduced. It uses a watchdog mechanism for rectify improper nodes and a path rater for selecting routes that do not choose misbehaving nodes.

In [11], CONFIDANT, a reputation-based model that ejects misbehaving nodes by propagating bad Reputation through the network was used.

In [12], a reputation based scheme that only propagates positive reputations between the nodes was proposed. Reputation computation scheme includes the aggregation of three different types of information, based on dissimilar levels of services and observations. This method (reputation computation) incurs larger overhead than other introduced methods. Proposed incentive schemes for enforcing co-operation can be divided into trade-based and reputation-based. Even as extensive work has been carried out on integrity, privacy and confidentiality attacks, the threat to network availability has received fewer attentions. Availability is a significant prerequisite for improving the performance of network. Available studies on Denial of Service attacks (DoS) focus on the analysis of various attack scenarios projecting a particular layer, or propose a probing scheme to detect misbehaving nodes that project a specific network layer function. While using a probing scheme can help in detecting DoS (Denial of Service) attacks, probing packets may introduce communication overhead in the larger network. Reputation rating tied with localized probing schemes can alleviate this issue.

Xiapu Luo et al [13] introduced the major problem of detecting pulsing denial of service (PDoS) attacks which send a series of attack pulses to decrease Transmission control protocol throughput.

Wei-Shen Lai et al [14] have presented a mechanism to observe the traffic pattern in order to alleviate DDoS.

Xiaoxin Wu et al [16] have presented Denial of Service (DoS) elimination technique which uses digital signatures to authenticate legitimate data and plunge packets that do not pass the validation.

Ping Yi et al [17] have proposed a new Denial of Service attack and its defence methods in ad-hoc networks. The new DoS attack, known as Ad-hoc Flooding Attack (AHFA), can result in denial of service (DoS) when used against on-demand routing protocols for MANET.

## 3. PROBLEM DEFINITION

Security Issues in Mobile Ad-hoc Network
Mobile ad-hoc networks are generally more prone to physical security threats than fixed-cable nets. Mobility or

dynamic nature characteristics sometimes become a vulnerable point for attacker to disturb network system or degrade network performance and lifetime. Due to dynamic nature property of ad-hoc network several kinds of attack possible on networks which break security goals.

**Black hole attack**: A Black hole is possible because of the week routing infrastructure. When a malicious node joins the network this difficulty arises. This node falsely replies for route requests without having an active route to the destination and exploits the Routing Protocol to advertise itself as having a good and valid path to a destination node. Actually, in AODV routing for finding the path between source and sink RREQ packets are flooded and all the path replies with RREP packets if malicious node RREP is arrive first, then the requester node suppose the provided information is correct and reply with the data packets.

Wormhole attack: In a wormhole attack more than one malicious node secretly joins the network and according to the nodes they are connected from side to side to high speed data buses by which they assure to send data from source to sink, the creation of attack is driven as a malicious node can record packets at one location in the network and through a channel or secrete path tunnel them to another location which is a confidential network shared with other malicious nodes. Wormhole attack can be done with one node or two nodes, but generally two or more attackers connect by way of a link called wormhole link. There are possibly three types of wormhole attack Closed Wormhole, Half Open Wormhole, and Open Wormhole.

**DoS and Flooding**: DOS and flooding attacks are the most common attacks in MANET. Flooding attacks are of two types RREQ packet flooding and DATA flooding attacks. Flooding means a huge amount of RREQ packets or DATA packets are sent for the purpose of wastage of resources or consume more resources. In Denial-of-Service (DoS) attack, an attacker attempts that legitimate users are not able to accessing information or services. These packets increase unnecessary traffic in the network so that the congestion problem arises. The attacker is act as malicious which send packets flooding to discharge battery power of the genuine node. The most common and noticeable type of DoS attack occurs when an attacker floods a network with information as shown in Fig 1.3., the server can only process a certain number of requests at a time, so if an attacker puts burden of RREQ packets to the server it cannot process the legitimate request.

**Gray-hole attack**: A Gray-hole attack is related to the two attack black hole and worm-hole attack. In this attack nodes forward all packets to some nodes, but may drop packets coming from or ordained to specific nodes. This type of attack is more complicated compared to black hole attack.

Problem Definition- Multi-Hop wireless network has several loop-false due to infrastructure-less environment. These loop-false makes opportunity for attackers to influence the smoothness of network operations. Attacker or unauthorized person can put different attacks by identifying loop-false in the network, which is violating security policies of the network. One of them is a DoS attack to infer such below policies.

- Availability
- Confidentiality
- Authenticity

Additionally, attacks influence different network resources also those are precious for running network process. Some of them defined below.

- Battery Power
- Lifetime
- Throughput
- Packets delay
- Routing overhead

Several mechanisms and protocol advised on individual black hole attack, but required more work on DoS attack on which few work approached by researches. In already existing advised approach, certain problem found. Firstly node sent data packet to determine the value of reliability levels of nodes in the network. When nodes play role as malicious then it do not acknowledgement of data packet because these watch data packets only, in this scenario data packet of the sender read by malicious node. Secondly, is too difficult to detect node as malicious when its reliability level value zero initially when the network is deployed. Thus we required approach to prevent data packet, and perfect detection of malicious nodes in the network.

## 4. PROPOSED MECHANISM

Mobile ad-hoc networks has several drawbacks due to infrastructure-less environment. These loop-false make chance for attackers to influence the smoothness of network operations. Attacker can put different attacks by identifying drawbacks in the network, which is violating security policies of the network. Additionally, attacks influence different network resources also those are precious for running network process such as Throughput, Battery Power, routing overhead and End to End packet delay. Several mechanisms and protocol advised on detection of DoS attack but their also required some work. To provides a solution for identified problem, a mechanism is proposed to prevent data packet loss occurs during the determining TTL value of nodes and detection of malicious attack in the network. The mechanism proposed which use additional packet named as reliability packet (RL packet) before of data packet to determine the TTL value of nodes. The RL value of node is incremented when it receives acknowledgement in specific time slice otherwise it decremented when it does not receive acknowledgement in specific time slice. Each node has a route table which contains path for every node. The node checks the RL value of nodes, if it is abnormal, then node declared as malicious or compromised by DoS.

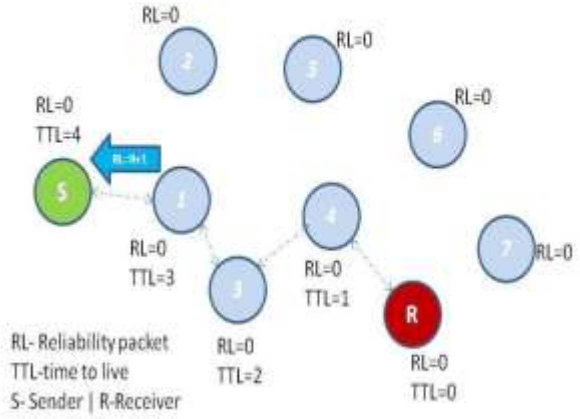

*Figure 4.1 Data Transmission*

### 4.1 Proposed Algorithm

### A. Algorithm

```
Algorithm RL_Mechanism(node,n)
{
                    // Initialize RL value of nodes of the network
 Set RL v: =0;
 Set TS: =0;                        //Timer (Time Slice)
 For i: =1 to n step i: =i+1 do

 node[i]:= RLV;

//Node sends RREQ packet to discover the route

Send (node[i], node[j], RREQ);

node[i] wait for acknowledgement from node(j);

// Start Time Counter

For TS: =0 to 2 step TS: =TS+1 do

//Checking acknowledgement

If (node[i]:Receive(node[j], RREP))

RLv=RLv + 1;                        //incremented by one
Else
                    RLv=RLv - 1;       //decremented by one

End if

Exit

// Checking Reliability packet value

If (node[i]==RLv>0)

Send (node[i], node[j], DATA);
Else

          Declared (node [i+1], Malicious Node);

End if

Exit
}
```

### 4.2 Operation

- Initially all nodes in the network have reliability packet and Time Slice (TS) zero.
- Source Node Send RREQ to its neighbours and Start Time Slice Timer. If the source node got a response in Specific Time Slice (in 3sec.) from neighbour node, then the responded node Reliability packet incremented by one (RLv=0+1) else decremented by one (RLv=0-1).
- And the process continues until the TTL value will become zero.
- Response include: RREP and RERR.

## 5. CONCLUSION

Customary network needs a static infrastructure to establish, but MANET has a different approach. Mobile ad-hoc network does not need fix infrastructure or static infrastructure. It provides facility to node that they can join or leave network any time. Mobile ad-hoc network is a very wide area for research due to its wide collection of concepts. Security of the network is one of the essential features for its deployment. The offered method tried to detect the malicious node in the network. Nodes in the networks which disturbs packet transmission and try to capture transmitted data. In this work we have concentrated on detection of DoS attack. Previous research concentrates on identify a malicious node by calculation there response value if retains count goes to zero then they announce node as the malicious node but there was one problem that initially all nodes have zero value so in this situation it's very difficult to identify malicious node and it is the basic motivation to define new approach so new approach follow a different way to identify DoS attack by introduced a RL packet send at the beginning of communication when all nodes have RL value zero. Approach work in the way by tracking response of nodes means those nodes who answer to sender of packet in time slice (TS) than increase its RL value by 1 (ONE) but it also might be possible in case suspicious node that may not answer to sender so if any sender does not get a answer from the receiver node in time slice than the sender decrement RL value of that node by 1(ONE) and when a node reaches less than 0 (ZERO) value it announce as a malicious node. This methodology reduces the packet drop ratio and re-transmission time.

**Future Work**

Wireless Ad-Hoc networks are widely used networks due to their flexible infrastructure, i.e. it does not depend upon geographic constraints which make it easily deployable. These networks are exposed to both external and internal attacks as there is not centralized security mechanism. A lot of research work is still needed in this area. By this work, try to detect DOS attack in MANET but still there are many more possibilities to find such malicious node in the network and provide a proper valid mechanism to reduce the possibility of interruptions from those suspicious nodes and feel free to transmit data over the network. It always observed that there is also certain area available in where researchers have to find the impact of the DoS attack in other mobile ad-hoc network routing protocols such as DSR, TORA and GRP along with AODV and OLSR protocols. Other types of attacks like Wormhole, Sybil and Jellyfish attacks are needed to be studied along with the DoS attack. They can be classified on the basis of how much they affect the performance of the network. The detection of this behaviour of a Denial of Service attack as well as the elimination tactic for such behaviour has to be carried out for additional research. We will also present a method for malicious node recovery dynamically.

## REFERENCES

[1] Morteza Macki, Karthik Demty, Massoud pedrem: “Power aware Source Routing  Protocols for Ad-hoc Networks”, ISLPED 02, August 12-14, 2002 ACMT 58113-475-4/02/0008.

[2] Liana Khamis Qabajeh, Miss Laiha Mat Kiah, Mohammad Moustafa Qabajeh, Secure Unicast Position-based Routing Protocols for Ad-Hoc Networks, Acta Polytechnica Hungarica Vol. 8, No. 6, 2011

[3] Richa Jain, Samidha Dwivedi Sharma, Study of Location based Energy Efficient AODV Routing Protocols in MANET, IJCTA | Jan-Feb 2013

[4] Young-Bae Ko and Nitin H. Vaidya, Location-Aided Routing (LAR) in mobile ad hoc networks, Wireless Networks 6 (2000) 307–321

[5] Emre Safak, Location Management for Geographic Routing in Wireless Mobile Ad Hoc Networks, Northeastern University Boston, Massachusetts December 2002

[6] Koushik Majumder, Sudhabindu Ray, Subir Kumar Sarkar, “Design and Analysis of a Multi-level Location Information Based Routing Scheme for Mobile Ad hoc Networks”, Mobile Ad-Hoc Networks: Applications

[7] Jie Wu, Senior Member, Shuhui Yang, Fei Dai, “Logarithmic Store-Carry-Forward Routing in Mobile Ad Hoc Networks”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 18, NO. 6, JUNE 2007

[8] Karim El Defrawy, Gene Tsudik, “Privacy-Preserving Location-Based On-Demand Routing in MANETs”, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 29, NO. 10, DECEMBER 2011

[9] Pragati N. Patil, Novel Protocol for Location Tracking of Sensor Nodes in Ad hoc Network, International Conference on Emerging Frontiers in Technology for Rural Area (EFITRA) 2012 Proceedings published in International Journal of Computer Applications® (IJCA)

[10] Silvia Giordano, Ivan Stojmenovic, Ljubica Blazevic, “POSITION BASED ROUTING ALGORITHMS FOR AD HOC NETWORKS: A TAXONOMY”, ICA-DSC-EPFL CH-1015 Lausanne (Switzerland)

[11] Joo-Han Song, Vincent W.S. Wong, and Victor C.M. Leung, A Framework of Secure Location Service for Position-based Ad hoc Routing, PE-WASUN’04, October 7, 2004, Venezia, Italy. Copyright 2004 ACM 1-58113-959-4/04/0010

[12] Dragos Niculescu, Badri Nath “Position and orientation in ad hoc networks”, 2003 Published by Elsevier B.V.

[13] Fazli Erbas, Kyandoghere Kyamakya, Klaus Jobmann, “On the Use of Position Information of Nodes in Mobile Ad hoc Networks”, PROCEEDINGS OF THE 1st WORKSHOP ON POSITIONING, NAVIGATION AND COMMUNICATION (WPNC’04)

[14] Marc Heissenbuttel, “A Novel Position-based and Beacon-less Routing Algorithm for Mobile Ad-Hoc Networks”, Institute of Computer Science and Applied Mathematics University of Bern, Switzerland

[15] Yuan Xue, Baochun Li, “A Location-aided Power-aware Routing Protocol in Mobile Ad Hoc Networks”

[16] S.Mangai, A.Tamilarasi, “Evaluation of the Performance Metrics in Improved Location Aided Cluster based Routing Protocol for GPS Enabled MANETs ”, European Journal of Scientific Research ISSN 1450-216X Vol.46 No.2 (2010), pp.296-308

[17] R. Plestys, R. Zakarevicius, “The Distribution of Route Search Packet Flows in Ad Hoc Networks”, ELECTRONICS AND ELECTRICAL ENGINEERING, ISSN 1392 – 1215 2011. No. 9(115)

[18] Nurhayati, Sung Hee Choi, and Kyung Oh Lee, “A Cluster Based Energy Efficient Location Routing Protocol in Wireless Sensor Networks”, INTERNATIONAL JOURNAL OF COMPUTERS AND COMMUNICATIONS Issue 2, Volume 5, 2011

[19] Deepak Vishwakarma, Anil Khandekar, Nitin Rathore and Ranjeet Osari. Article: Detection and Prevention Mechanism for TTL Field Tampering Form of DDoS Attack in MANET's. International Journal of Computer Applications (IJCA) 117(15):5-10, May 2015.