Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Survey on Different Packet Drop Detection Techniques in Mobile Ad-Hoc Network

Brijesh V. Patel
Computer Science& Engineering, Parul Institute of Engineering
Limda,Waghodia,Vadodara,Gujarat

Abstract— Mobile means to move any direction and ad-hoc means temporary infrastructure less network. In mobile ad-hoc network packet sending and receiving is most important things. When packets send to one node to another node this sending node reach to destination at this time if packets are drop so because of this reason security is not maintained. Packets drop using malicious node or not and also find the detection of packet drop. In this paper various security techniques in packet dropping attack for the security purpose.

Keywords-Mobile ad-hoc network (MANET), malicious node, Packet drop Attack, Homomorphic linear authenticator (HLA), voting mechanism, selfish

I. INTRODUCTION

Mobile ad-hoc network is infrastructure less network. It is internet protocol based network of mobile wireless mechanism nodes connected with each other. The node of MANET have not have centralized mechanism. Each device move to in any direction and will therefore change its link to other device frequently.

Types of mobile Ad-hoc network:

A. **Vehicular ad-hoc network(VANETs)**
VANETS are used for communication among vehicles and road side equipment.

B. **Intelligent Vehicular Ad Hoc Networks (inVANETs)**
It is kind of artificial intelligence that helps vehicles to behave in intelligent manners during the vehicles to vehicles collision, accident, drunken driver etc.

C. **Internet Based Mobile Ad Hoc network(iMANETs)**
Ad-hoc networks that link mobile node to fixed internet gateway node. In such a type of networks normal ad-hoc algorithm is not apply.

In mobile ad-hoc network packet may be dropped using many ways:

A. **Unsteadiness of the medium**
- When link is broken packet may be dropped
- When heavy traffic in medium packet may be dropped.
- When confusion in medium packet may be dropped.

B. **Genuine of node**
- When over flow of transmission queue.
- When lack of energy resources due to packet is dropped.

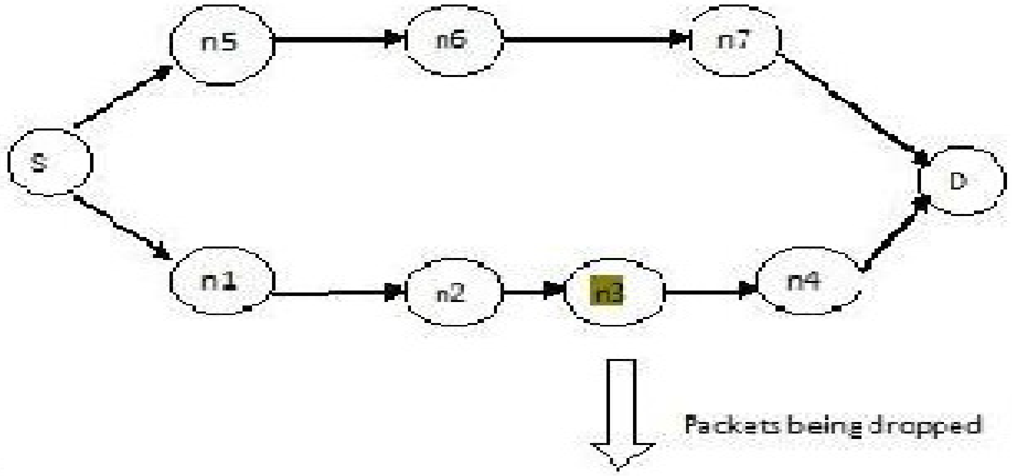
C. **Selfishness of the node**
- Packet dropped due to selfishness of node to save the resources.

D. Malicious of the node

- When malignant node acts of malicious node so packets are dropped.

II RELATED WORK

When packet send to one node to another node. First node (sender node) checks initially which node forwards the packet. This node information is known to another node [1]. Credit system provides intensive cooperation. its credit send to its own packet. Malicious node continue to drop the packets so its credit decrease the as a results will not able sends its own traffic [4]. Different kind of certification revocation method like voting mechanism and nonvoting mechanism in this method selfish node voting its neighbor node [2]. Cryptographic method in this bloom filter is used to construct the proofs of the forwarding of packet at each node [2].



S-Source node
D-Destination node
N-Intermediate node

Fig1. Packet Drop in Mobile Ad-hoc Network [1]

III DIFFERENT METHOD OF PACKET DROPPING AND ITS DETECTION

A. Voting based Method

Voting based method is defined as malicious attacker's certificate through vote from valid neighbor node [3]. The certificate of newly joining node is created by its neighbor node. Attacker contain certificate revoked from its neighbor node.

B. Reliability based classification

As node behavior there are three types of node like attacker node, legitimate node and malicious node. In legitimate node communication is secure as deemed with any other node. It is able to truly detection of packet from malicious node and positively in order to guarantee of network security. A malicious node does not execute protocol to detecting misbehavior, revoke malicious attacker. Attacker node is defined as selfish node which can attack on neighbor node and disturbed the communication.

C. Homomorphic linear authenticator based public auditing

In this HLA detector to verify the truthfulness of packet loss data to be reported by node. This structure is collusion proof, privacy, low storage and communication overhead [5].

IV COMPARISON ABOVE MENTION METHOD

Comparison above mention method is presented in given table.

Table1. Comparison between method
FPR-False Packet Ratio
PDLR- Packet Delivery Ratio

Scenario	Node	Malicious packet	Throughput (kbps)	FPR	PDLR
A	10	0	76.77	0.112	1
B	10	1	67.82	0.115	0.8452
C	10	2	60.81	0.2145	0.7864

V CONCLUSION

In this paper various packet dropping and its detection are explained. The entire algorithm based upon its application. There are many research on mobile ad-hoc network packet dropping and its detection is highly challenging in real environment. There are many challenges mobile ad-hoc network such as network life time, network etc.

ACKNOWLEDGEMENT

With the cooperation of my guide, I am highly indebted to Asst. Prof. TANVI VARMA, for her valuable guidance and supervision regarding my topic as well as for providing necessary information regarding review paper.

REFERENCES

[1] P.seweth, vinod bhupati,unmasking packet drop attack in MANET,International general of emerging trends and Technolgy in computer science,Nov-Dec 2013.

[2] Wei liu,student menber,IEEE,hiroki nishiyan,member,IEEE,Nirwan ansari,fellow,IEEE jieyang and nei kato,senio member IEEE,Cluster based certificate reevocation with vindication capability of mobile ad-hoc networkIEEE,vol-24,Feb-2013.

[3] Haunyu zhao,xin yang and xiaolinLi,c trust: trust management in cyclic mobile ad-hoc network,IEEE,No-6 vol-62,july 2013.

[4] Tao shu, Marwan krunz,detection of malicious packet dropping in wireless ad-hoc networkbased on privancy preserving public auditing,wisec ACM 987-1-4503-1265-3/12/04,2012.

[5] Tao shu, marwan krunz, privancy preserving truthful detection of packet dropping attack in wireless ad-hoc network,IEEE,1536-1233,10.1109/TMC 2014.2330818.2014