IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 55-60
www.iosrjournals.org

Packet Dropping in Wireless Ad Hoc Networks

Shanida T K, Smitha Karunan

M Tech Scholar Department of Computer Science Engineering Govt Engineering college, Mananthavady, Wayanad Kerala, India- 670644

Assistant Professor Department of Computer Science Engineering Govt Engineering College, Mananthavady, Wayanad Kerala, India- 670644

Abstract: *Wireless ad hoc networks have gained much im-portance due to its simplicity and low cost of deployment. The decentralized management of this network makes it susceptible to various attacks. Packet dropping is one of the major security issue. Moblie ad hoc networks is a kind of ad hoc wireless networks in which nodes are mobile. This paper presents a survey on packet dropping, packet dropping attack detection techniques, MANET and packet dropping in MANET. The paper concludes with the necessity of motivating a malicious node in case of malicious packet dropping in wireless ad hoc networks.*

I. Introduction

Wireless ad hoc networks is one of the category of wireless networks which operates without the support of any fixed infrastructure. In this network nodes not only acts as hosts but also as routers which forwards data packets. Due to its self-organizing behavior ad hoc networks are mainly used in military applications, emergency operations and disaster recoveries.

Packet loss is a serious issue in wireless ad hoc networks. There are several classifications for packet dropping and packet dropping detection techniques[1]. The major classifi-cations for packet dropping includes legitimate packet drop-ping, stealthy packet dropping and malicious packet dropping. Packet dropping detection techniques are mainly classified into watch dog technique, side channel monitoring, monitoring agent techniques, TwoAck and PathRater. In case of mobile nodes, mobility is also a reason for packet loss.

II. Packet Dropping

A. Legitimate Packet Dropping

Legitimate packet dropping in which no compromised nodes are there may occur due to network congestion, channel conditions and resource constraints.

1) Network Congestion: Congestion is one of the crucial factor which leads to packet loss. Scalability is possible in ad hoc wireless networks due to the movement of nodes which is also a cause for congestion.
2) Channel Conditions: Interference, free path loss, pres-ence of noise on the channel are certain channel conditions. These factors leads to packet dropping or bit error in the signal which is transmitted.
3) Resource Constraints: Energy is one of the resource constraints that have to be considered with great importance. The nodes having limited energy saves their energy by not forwarding packets. This selfish behavior of the nodes leads to packet drop.

B. Stealthy Packet Dropping

Stealthy packet dropping launch attacks that are harmful as brute force attacks. It minimizes the cost and the visibility of the attacker[2]. Stealthy packet dropping attack types are [3]:

- **Power Control**

The next hop is excluded by controlling the transmission. In the route there will be a compromised node with the capability to control power.

- **Misrouting**

Packets are forwarded to the next hop which is wrong. In the route there will be a compromised node in misrouting.

- **Colluding collision**

Collision occurs at the next hop by the transmission of packets simultaneously. There will be a compromised node and an external attacker near to this compromised node(next hop) in the route.

- **Identity Delegation**

The colluding partner near to the sender is given the responsibility for relay. There will be a compromised node and an external attacker near to the compromised node in the route.

These attacks cannot be detected by Baseline Local Monitoring(BLM), instead stealthy packet dropping at-tacks can be mitigated by a protocol called SADEC. In
SADEC a local monitoring will be done in the nodes by maintaining an additional routing path information and the responsibility to check each neighbor[3].

C. Malicious Packet Dropping

Packet dropping due to malicious nodes which takes part in the route during data transmission is termed as malicious packet dropping. These nodes behave as trusted nodes and exploits the vulnerabilities of the routing protocols which leads to high damage in the network. An intermediate node which is malicious can even suspend the communication or generate wrong information between the source and the destination

1) Malicious Packet Dropping in AODV: In Ad hoc On Demand Distance Vector (AODV) Routing Protocol the source broadcasts the RREQ(Route Request) message and the desti-nation on receiving the message sends a RREP(Route Reply) message back to its neighbor after updating the sequence number of the source. An intermediate node can even send back a RREP without relaying to the destination if there exists a route to the destination through this intermediate node. A node which is malicious can cause packet drop by not rebroadcasting RREQ and sends RREP by claiming it has the shortest path to the destination. Then the source sends the packet to this malicious node itself which in turn leads to packet dropping[1].

2) Malicious Packet Dropping in OLSR: Multipoint Re-lays(MPR) are used in Optimized Link State Routing Pro-tocol(OLSR). For network optimization MPR known as set of neighboring nodes are used to spread the link state informa-tion. Topology Control messages(TC) are used to broadcast link state periodically. In one hop neighbors each node selects its MPR for minimizing the retransmissions by reaching all its neighbors in two hop. Broadcasting of TC messages lead to the construction of the network with partial topology in which non neighbors are also included in the route. A malicious node causes packet drop in the network by claiming it as the MPR even though it is not. It sends TC messages and leads to packet dropping since routing services are dependent on MPR in OLSR.

III. Packet Dropping Attack Detection Techniques

A. Watch Dog Technique

Each node can act as a watch dog detection agent which saves the copy of packets into the buffer before forwarding which leads to the monitoring of packet relay from one node to another.

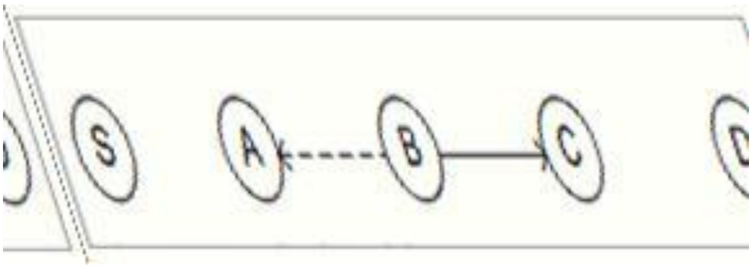

Fig. 1. An Illustarion of Watch Dog Technique[1]

In Fig.1 S is the source node and D is the destination node. S sends packet to node A. When A sends packet to node B, A saves the copy of packets in the watch dog buffer for monitoring. When B sends packet to node C, A can also get the copy of packets since it is in the transmission range of node B. Thus A can check whether B has forwarded all the packets to C with the copy of packets it has recieved and those in the watch dog buffer. This technique is applicable in environments which has knowledge about neighbors in two hop metric.

B. Side Channel Monitoring

Sub-set of neighbors for each node which lies in the route between the source and the destination are selected inorder to monitor the behaviors during message forwarding. The information about the misbehaving nodes are obtained by the source through an alarm channel . Alarm channel is formed of both primary channel which consists of nodes and secondary channel which consists of sub- set of neighbors for monitoring.

C. Monitoring Agent Technique

The packets sent by neighboring nodes are captured within a transmission range. The information about the neighbors in one hop is collected by all the nodes. Average packet dropping rate, average number of packets transmitted, total number of packets transmitted and packet drop rate at a node which is particular are the information collected by the nodes.

D. TwoAck

In this technique nodes sends acknowledgment two hop backwards. If a node does not receive TWOACK packet then the link to next node is considered as misbehaving and it will be eliminated from the next route onwards.

E. Sequence Number Model

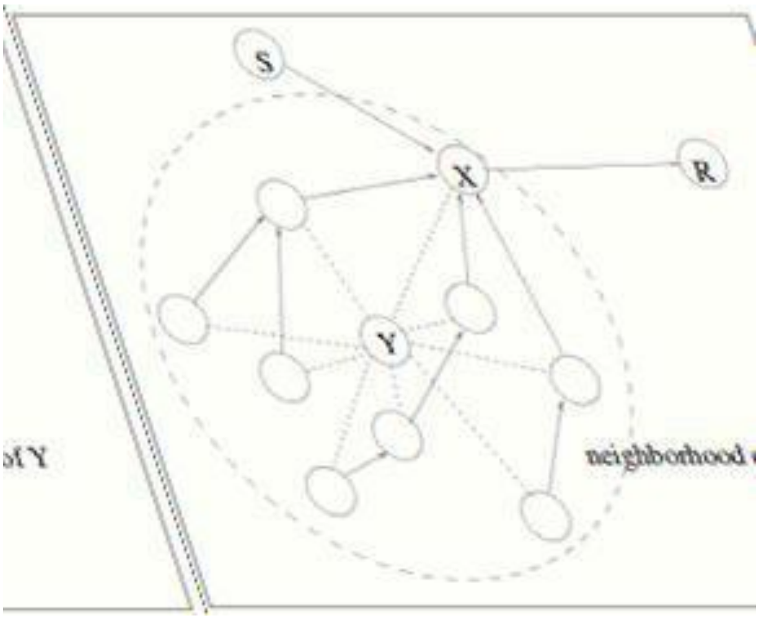

Fig. 2. An Illustarion of Sequence Number Model[1]

In Fig.2 S is the source node and R is the destination node. R is not in the communication range of S. An intermediate node X is used for communication. Packet loss rate can be determined by the destination R by checking whether there is an exceed in the sequence number of the packets which came through the intermediate node X with a specific thresh-old value. In such a situation R begins investigation being suspicious. R sends a special message to X to broadcast to its all neighbors. The special message conveys to communicate to node R. To avoid false neighbors to communicate to node R an authentication mechanism on the basis of a private symmetric session key is there. When node R gets the response through information it can determine whether malicious behavior of nodes are leading to packet loss or not.

F. PathRater

Each node maintains ratings on the basis of the information about the misbehavior of the nodes and the link reliability for every other nodes in the network for the purpose of opting an appropriate path. The metric used here is obtained by taking the average value of ratings of nodes in the path. If multiple path exists then those with the highest value for metric is chosen as the path. The metric value will be updated after a particular time interval. If malicious nodes are present in the path then the metric value will be negative.

Watch dog detection is susceptible to cooperate attacks and partial attacks.The communication overhead and computa-tional overhead is also less. Computational and communication overheads are average in case of Single Channel Monitoring.

TwoAck attack detection technique has low computation over-head and high communication overhead. In Sequence Number Model communication overhead is high and computation overhead is average. It is susceptible to partial attacks and this detection technique is not applicable to mobile environment. Communication overhead is low and computation overhead is high in the case of PathRater. Monitoring Agent is not advisable in the case of mobile environment and it also leads to high overheads during attack detection. Thus it is essential to design packet dropping attack detection techniques in wireless ad hoc networks which operates in both static and mobile environment with low computation and communication overhead.

IV. MANET

Mobile Ad hoc Network(MANET) ia a self-configuring network and a kind of Wireless ad hoc network in which nodes are mobile and autonomous in nature. It is an infras-tructure less network in which nodes can move anywhere in the network which in turn leads to tremendous changes in the topology. Distributed operation occurs since there is no central authority. It supports multi-hop routing and packets are forwarded through intermediate nodes. It is less expensive and fast deployment can be done. Nodes in MANET usually has low power storage, small memory and less CPU capability[5]. There are several drawbacks for MANET even though it is scalable.

It has limited bandwidth. Due to frequent topology changes frequent path break occurs which in turn leads to frequent route changes. Hidden terminal problem is another challenge faced by MANET in which collision occurs at the receiver node due to the simultaneous transmission of nodes which are not in the sender's transmission range but in the receiver's transmission range[6]. Power source has restrictions since the nodes are small in size, light weight and portable. It is also susceptible to various security attacks like eavesdropping.

MANET is mainly used in commercial sector, military battlefield, rescue operations, collaborative networks, sensor networks and for free internet connection sharing[5][6].

A. Packet Dropping in MANET

Packet dropping attack is similar to denial of service in which nodes drops the packet in MANET without forwarding. It is difficult to detect packet dropping attacks in MANET. Packet dropping mainly occurs due to malicious nodes. A node can be malicious due to several reasons. Some of them are[7]:

- Packet drop which results due to denial of packet for-warding action.
- Wastage of battery due to operations which is unneces-sarily done.
- Buffer over ow due to filling of fake updates in the buffer.
- Creates confusion by inserting stale packets.
- Delaying the packet forwarding intentionally.
- Consuming the bandwidth so that legitimate nodes cannot operate.
- By tampering the contents of the packets.
- Breaking the link so that legitimate nodes cannot com-municate.
- Sending fake routes to interrupt the communication.
- Capturing session during the communication between the legitimate nodes.
- Isolating legitimate nodes to create delay purposefully and to route the packets in another path.
- A node entering in the network without authentication.

The attacks due to malicious nodes can be specifically categorized as following:

- Black hole attack in which all packets are dropped intentionally.
- Selectively drops the packets to and from certain nodes due to the dislike of malicious nodes.
- Grey hole attack in which some portion of packets are retained.

There are several packet dropping attacks in MANET. They can be generally classified as following[8]:

- Flooding attack

In this attack a node which is malicious broadcasts Route Request(RREQ) which is fake to a destination which does not even exist in the network. This RREQ will not receive any reply since there is no destination. This results ooding in the network. It also leads to exhaustion of resources in the network. It is also known as resource consumption attack.

This attack can be prevented by neighbor suppression technique. In this method each node determines the rate of RREQ of the neighbors and if this value is greater than the threshold which is already defined then neighbors ID is added into the black list. Thus the requests coming from the nodes in the black list is dropped. This technique is not applicable in the case where threshold value is greater than the ooding rate.

- Black hole attack

In this attack in response to RREQ sent by the the source a fabricated Route Reply(RRP) will be sent by the attacker claiming that it has the shortest route to the destination. Thus packet dropping occurs since all the packets are sent through this malicious node itself. This attack can be prevented by introducing control packets such as Route Confirmation Request(CREQ) and Route Confirmation Reply(CRP). Intermediate nodes sends CREQ to the node which is in the next hop towards the destination along with the RREP[8]. This mechanism has limitations. This is not applicable when the malicious nodes are placed consecutively.

Wormhole attack

This attack is also known as tunneling attack in which no compromised nodes exists. In every communication confidentiality and authenticity has to be satisfied. It is one of the severe attacks in MANET. Pair of malicious nodes will be connected in this attack. When the ma-licious node receives RREQ it forwards it to its partner which is malicious through the tunnel. Then the colluding partner sends the RREQ to its neighbors.

This attack can be prevented by two approaches. They are known as temporal leashes and geographical leashes. Temporal leash is on the basis of expiration time and the other one is on the basis of synchronized clocks. Selective forwarding attack

This attack is also known as grey hole attack in which only selected packets are dropped and others are for-warded. Thus it is difficult to detect the node which is malicious. This can be done in two ways. A particular source or destination can be selected and denies the packet relay to that nodes or to drop the packets which is selected randomly.

Selfish node attack

This attack is caused due to the selfish behavior of the nodes. To save the resources like power, bandwidth etc the node stops forwarding the packets which in turn leads to the degradation of the network.

Link spoofing attack

In this attack the node which is malicious provides the false information about the link with the non-neighbors which leads to packet dropping and results in network degradation.

This attack can be prevented by location information based detection method. Detection is done by using GPS and timestamp. This method has limitation such as every node must have a GPS supported device.

Sybil attack

In this attack there exists a single malicious node which acts as different nodes to other nodes. It can be done in several ways. This attack can be done by impersonation. Another approach for attack launch is by using false identities. The node which launch sybil attack can com-municate directly or indirectly with the other legitimate nodes in the network and routing is disrupted. Blackmail attack

In this attack a malicious node misrepresents a legitimate node as attacker by adding it into the black list. Thus the attacker node blackmails the legitimate node. It is used against protocols which uses attack detection techniques like watch dog and pathrater. A node which is good is considered bad by other legitimate nodes due to the misconception that the node is malicious.

. Location disclosure attack

In this attack confidential information like location of the node is obtained by the attacker through monitoring, probing or through traffic analysis.

Packet dropping is an unavoidable issue in MANET. There are approaches for detection of packet dropping attacks in MANET, but they are on the basis of the assumption that most of the nodes are misbehaving which is not usual in the case of MANET[9].

B. Mobility

In MANET, mobility is also a factor which contributes to packet loss. Packet loss due to mobility occurs due to various reasons. If the route to destination is not available then the packets may drop at the source node itself. If the next hop is not available then packet loss occurs at intermediate nodes.

In wireless ad hoc networks malicious packet dropping can be detected and verified by ensuring the truthfulness of the packet loss information by an auditor on the basis of a public auditing architecture[4]. An independent auditor which is not the part of the route between the source and the destination identifies the node which is malicious. Auditor needs to collect information from each node between the source and destina-tion to facilitate the investigation. High detection accuracy is achieved through this mechanism. Auditor will not be able to gain the contents of the packet during auditing phase. Thus privacy preserving feature is also supported in this mechanism. Low communication and storage overheads are maintained at intermediate nodes. This mechanism fails to consider the feature mobility in attack detection even though mobility plays a vital role in case of packet loss in mobile ad hoc networks.

Malicious packet dropping due to malicious nodes is a major category of packet dropping attacks in wireless ad hoc networks. These malicious nodes after detection are commonly isolated from the network. But isolating this nodes will effect the performance of the network. So some techniques to make these malicious nodes active in the network by motivating them inorder to increase the efficiency of the network is essential.

V. Conclusion

Packet dropping is the major factor for loss of packets in wireless ad hoc networks. Malicious packet dropping due to the intentional attack of malicious nodes is one of the important packet dropping attacks. Packet dropping attack detection techniques have several limitations. Mobility feature must be considered during detection of malicious nodes in MANET. Isolating malicious nodes after detection will effect the performance of the network. Thus there is a need to motivate the malicious nodes detected inorder to make them active again in wireless ad hoc networks.

References

[1]. Kennedy Edermacu, Matin Euku and Richard Ssekibuule, ”Packet Drop Attack Detection Techniques in Wireless Ad Hoc Networks: A Review”, International Journal of Network Security and Its Applications(IJNSA), Vol.6, No.5, September 2015.

[2]. E.S Phalguna Krishna, M.Ganesh Karthik, I.D. Krishna Chandra, ”A Survey Report on Stealthy Packet Dropping”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012.

[3]. Issa Khalil and Saurabh Bagchi, ”Stealthy Attacks in Wireless Ad Hoc Networks: Detection and Countermeasure”, IEEE Transactions on Mobile Computing, Vol 10, No.8, August 2011.

[4]. Tao Shu and Marwan Krunz, ”Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks”, IEEE Transactions on Mobile Computing, Vol.14, No.4, April 2015.

[5]. Mohit Kumar and Reshmi Mishra, ”An Overview of MANET: History, Challenges and Applications”, Indian Journal Of Computer Science and Rngineering(IJCSE).

[6]. Arti, Dr S.S Tyagi, ”Study of MANET: Characteristics, Challenges, Application and Security Attacks”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

[7]. Manju Khari, Radhika Saini,”Defining Malicious Behavior of a Node and its Defensive Methods in Ad Hoc Network”, International Journal of Computer Applications, Vol 20, N0.4, April 2011.

[8]. Dinesh Goyall, Kshitij Bhargava,”Packet Dropping Attacks in MANET: A Survey”, Journal of Advanced Computing and Communication Tech-nologies, Vol 2, N0.3, June 2014.

[9]. Soufiene Djahel, Farid Nait-abdesselam, and Zonghua Zhang, ”Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges”, IEEE Communications Surveys and Tutorials, Vol 13, N0.4, Fourth Quarter 2011.