Survey of effect of packet dropping attack in AODV routing And detection of such nodes in MANET

Neema Soliyal
Department of Computer Science and Engineering
G.B.Pant Engineering College Ghurdauri, Pauri Garhwal
Uttarakhand, India
neemacse@gmail.com

Alok Tomar
Assistant professor,
Excess Computer Education Society, Dehradun
Uttarakhand, India
alokvictory1@gmail.com

Abstract

Mobile Ad-hoc Network (MANET) is an application of wireless network with self-configuring mobile nodes. MANET does not require any fixed infrastructure. Nodes in MANET can communicate with each other nodes if and only if all the nodes are in the same range. This distribution of nodes makes MANET vulnerable to various attacks, packet dropping attack or black hole attack is one of the possible attacks. It is very hard to detect and prevent. To prevent from packet dropping attack, detection of misbehavior links and selfish nodes plays a important role in MANETs. In this paper we will compare all technique how they detect the misbehavior link and malicious node.

Keywords: MANET; Techniques to prevent from various attacks, Packet drop attack;

1. Introduction

Mobile ad-hoc network (MANET) is a collection of autonomous nodes, which have the properties like mobility, wireless [1]. MANETs have dynamic network topology and self-configuring so that nodes in network can move independently in any direction and change their links to other nodes in network frequently. Mobile ad-hoc network (MANET) is a self-configuring network consisting of nodes working cooperatively in ad-hoc manner without a fixed network infrastructure [9], [22]. Each node in a MANET is mobile and is free to move in a random fashion. The salient distinct feature of MANET is the dual behaviour of each node, where it acts as both router and host. MANET nodes include cell phones, laptops etc., have limited computation, communication and energy resources. MANET is much more vulnerable to attacks [1], [2], [5], [13], [25] as compared to a wired network due to the-

Following factors Complex security solutions cannot be used because nodes have limited energy.

- Packet transmission is done in wireless medium.
- Complex security solutions cannot be used because nodes have limited energy.
- There is no central management point, which makes it difficult to ensure that all nodes participating in the network are benign.
- Mobility of nodes makes routing even more challenging as the topology keeps changing regularly. Having mentioned the general issues in MANETs,

These reason behind MANET popularity and benefits are:

- Low expense of organization: Ad-hoc networks can be deployed on the fly, thus requiring no expensive infrastructure such as copper wires, data cables, etc.
- Fast arrangement: Ad-hoc networks are very convenient and easy to deploy when compared to WirelessLANs (WLAN), since it requires less manual intervention.
- Dynamic configuration: Ad-hoc network configuration can change dynamically with time. It is very easy to change the network topology when compared to configurability of LANs.

Attacks can be launched from all layers of the protocol stack [2], [5], [23] but the routing layer attacks are the most damaging. Malicious code and repudiation are done in application layer. Session hijacking and flooding are done in transport layer. Flooding, black hole, grey hole, worm hole, link spoofing, link withholding, location disclosure etc. are done in network layer. Malicious behaviour, selfish behaviour etc., are done in data link/MAC layer. Interference, traffic jamming, eavesdropping etc., are done in physical layer. A routing protocol [13], [24] specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a network. Routing algorithms determine the specific choice of route. Each router has a priori knowledge about the networks attached to it directly.

A routing protocol shares this information among immediate neighbours, and then throughout the network. A routing protocol [13], [24] specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a network. Routing algorithms determine the specific choice of route.

2. AODV Routing in MANET

The routing protocols of MANET can be of two types reactive or proactive. The DSDV routing is an example of proactive routing. It maintains a route table and each node periodically receive route update information and update route table with latest route. If more mobile nodes, more routing traffic is generated due to frequent route updates. So other option is reactive protocol. DSR is an example of reactive routing in MANET. In this protocol, source node search for route when it wants to send data to any destination. Dynamically, then needed route is established and maintained. No route table is maintained on each node. DSR works better with high mobility network but not good for network in which nodes are almost stationary. The solution is the AODV routing. This protocol uses some features of DSDV and some from DSR. The routing protocol is classified into proactive and reactive protocols.

2.1. Proactive Routing protocols

are table driven; all routing decisions are made by the nodes based on their predetermined routes. Every participating node maintains routing information in a routing table. In proactive routing, discovery is easy and route maintenance is hard due to the dynamic topology of the network. Destination Sequenced Distance Vector (DSDV) and Fisheye State Routing (FSR) protocol are some of the most popularly used table-driven protocols. Proactive protocols find the least cost to reach the destination.

2.2 Reactive Routing protocols

are on-demand [7], [8], the routes are discovered when a node desires to send a packet. Two main processes involved are route discovery and route maintenance. Dynamic Source Routing (DSR) and Ad-hoc On-demand Distance Vector (AODV) are some of the most popularly used on-demand driven protocols. Reactive protocols find the minimum hop count to reach the destination. Both of these protocols fail to consider other important QoS parameters like bandwidth, jitter, node energy level, queue length etc.

3. Packet Drop Attack In MANET

A packet dropping attack is a type of denial of service in which a node in the network will drop the packets Instead of forwarding them, this is shown in the fig 1.

The packet dropping attack [3], [6], [11] is very hard to detect and prevent because it occurs when the node becomes compromised due to a number of different Causes.

The packet dropping attack in MANETs can be classified into several categories in terms of the strategy adopted by the malicious node to launch the attack.

Mobile ad-hoc networks are more vulnerable to security attacks due to their special characteristics such as limited battery and memory resources, dynamic topology, multi-hop routing, lack of centralized system, no fixed infrastructure [5]. There are many routing protocols developed for MANETs but no protocol is efficient to secure the network.

- The malicious node can intentionally drop all the forwarded packets going through it (black hole).
- It can selectively drop the packets originated from or destined to certain nodes that it dislikes.
- A special case of black hole attack dubbed gray hole attack is introduced. In this attack, the malicious node retains a portion of packets (one packet out of N received packets or one packet in a certain time window), while the rest is normally relayed.

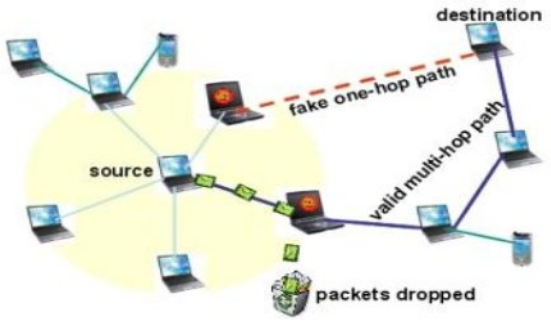

Fig 1. Packet dropping attack

The compromised node will broadcast the message [11], [12] that it has the shortest path towards a destination to initiate packet dropping attack.

Hence, all packet transmissions will be directed through the compromised node, and the node is able to drop the packets. If malicious node attempts to drop all the packets, the attack can be identified through common networking tools. Moreover, when the other routers notice that the compromised router is dropping all the packets, they will generally begin to remove that router from their forwarding table. Hence, there is no packet transmission through the compromised node. However, it is very hard to detect the packet dropping attack, if the malicious router begins dropping packets on a specific

Period of time or over every n packet, because some packet transmission still flows across the network. For the prevention of packet dropping attack, detection of Selfish nodes [6], [11], [12], [17] plays an important role in MANETs.

3.1. Reasons for Dropping Packets

1. A packet may be dropped due to contention in the medium.
2. A packet may be dropped due to congestion and corruption in the medium.
3. A packet may be dropped due to overflow of the transmission queue.
4. A packet may be dropped due to the malignant act of a malicious node.
5. A packet may be dropped due to much bandwidth consumed by a attacker node.
6. A packet may be dropped due to lack of energy resources.
7. A packet may be dropped due to the selfishness of a node to save its resources.
8. A packet may be dropped due to broken link.

4. Selfish Nodes Detection in MANETs

Recently, several approaches were proposed to deal with malicious attacks. In this section some of the existing approaches which are mainly used for detecting routing misbehavior are discussed.

4.1. Neighbourhood-Based Method

Neighbourhood-based method is used to detect the black hole attack and a recovery of routing protocol that establish a correct path from source to destination [2].
In neighbourhood-based method we can able to identify the malicious nodes in network and in route recovery protocol the source node sends a modified route entry control packet to destination node so that source will send packets to the destination by re-routing. In this method, we achieved higher throughput and lower detection time but this method fails when the attackers sends the fake reply packets. In Multiple Route Replies (MRR) method [2], source node waits for more than two RREP packets from modes in network. After receiving multiple RREP packets the source node verifies whether there is a common hop in the path or not. If there is a common hop then source confirms as the route is safe and it starts sending packets along this path. But drawback of this method is time delay because source node needs to wait for multiple RREPs.

4.2. Watchdog Approach

In Watchdog Mechanism mechanism every node will listen to the next node in order to identify the Misbehaving node in network. If any node in active path is dropping packets more than threshold value then source node is notified. But this method fails in identifying misbehaving node in some conditions [3]. Let us consider one example, suppose x-y-z is path in network. The node 'x' may fail in identifying misbehaving node in the following conditions.

1. When node 'x' is listening to node 'y', if a collision occurs in node 'x' then node 'x' cannot find whether this collision is due to forwarding packets by node 'y'(well behaving) or any other node in the network transmitting packets to node 'x' while node 'y'(misbehaving) is not forwarding the packets.
2. If node 'y' transmission is weak so that node 'z' does not received the packets from node 'y', but
3. Node 'x' detects that node 'y' forwarded the packets.
4. If node 'z' does not received packets because of collision at node 'z', but node 'y' is not re-transmitted the packets.
5. If both nodes 'y' and 'z' are misbehaving, node 'y' forwarded packets to node 'z' but node 'z' dropping the packets and node 'y' not informing to node 'x'.
6. If node 'y' is dropping packets but less than the threshold value then node 'x' can find that node is misbehaving.

Watchdog approach fails to detect a misbehaving node because of the presence of:

- Ambiguous collisions - It prevents X from overhearing Y's transmission if other neighbour sends packets to X at the same time.
- Receiver collisions - In this problem, node X checks whether Y sends the packet to Z, but not the reception at Z.
- Limited transmission power - The intermediate nodes may not send the reports if it has limited Transmission power.
- False misbehavior - It occurs when nodes report falsely about other nodes.
- Collusion - If collusion occurs in multiple nodes then it may affect the packet transmission.
- Partial dropping – It occurs if a node drops fewer packets.

In Pathrater Mechanism, it maintains rate for every node in network such as a node is decreased with rate when a node is identified as misbehaving node [4]. These node rates are used to find the most reliable route to destination node. But this method also having the same drawbacks as watchdog mechanism such as receiver collisions, limited transmission power.
Step 1: Apply the monitoring nodes in the network that will cover the entire network topology.

Step 2: Monitoring nodes will monitors all the incoming packets and outgoing packets of the active nodes.
Step 3: If the incoming packets and outgoing packets are not same i.e. attack is present. Then the monitoring node will intimate it to sender to resend the message by re-routing.
Step 4: If step 3 executed successfully then it can be concluded that message is reached to the destination.

4.3. Collaborative security architecture

This approach is extension to the watchdog approach. In this approach, the nodes in the network are classified into two categories, one is trusted and another is ordinary nodes. The nodes which are involved in initial network formation of the network are called as trusted nodes. These nodes which are joining later on the network are called as ordinary nodes. The ordinary node can be promoted as trusted node if the node demonstrates its reliability. Another supposition in this approach is that all the trusted nodes in the network should not be a malicious or selfish node. The nodes which are involve in watchdog nodes are selected from the set of trusted nodes for a given period of time based on the node energy, available node storage capacity and node computing power. The watchdog node has the additional duty to monitor other nodes in the network for a fixed period of time to detect the malicious behavior.
Watchdog node maintains threshold values of two types SUSPECT_THRESHOLD and ACCEPTANCE_THRESHOLD to measure the reliability of the node which is comes under non trusted nodes. If any node in network crosses the SUSPECT_THRESHOLD, it will be declared as malicious node by the watchdog approach. If a node crosses the ACCEPTANCE_THRESHOLD, it will be pronounced as trusted node. The existing AODV protocol was extended with some additional packet types send data, nodes neighbors, trusted_enc_request, trusted_enc_reply, watchdog and malicious to implement the security. However, the extra packet types increases the network overhead.

4.4. Collaborative watchdog approach

Collaborative watchdog approach to reduce the detection time of malicious nodes in the network, based on contact dissemination. In this approach, initially the collaborative node does not have any information about the malicious nodes. The collaborative node gets the information about the malicious node when a contact occurs based on either as a malicious contact or as a collaborative Contact. When the watchdog node receives packets from a new node it is assumed as a new contact. Then, the node transmits a message specifying all known malicious nodes to this new node.
The main overhead of this approach is the number of messages needed for this transmission. Moreover, the effects of false positives and false negatives are not measured.

4.5. TWOACK approach

TWOACK and Selective TWOACK (S-TWOACK) approaches [15]. TWOACK approach detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from source to destination. Each node in the path is required to send an acknowledgment packet. It is neither an enhancement nor a watchdog based approach. It is required to work on routing protocols such as DSR [10].

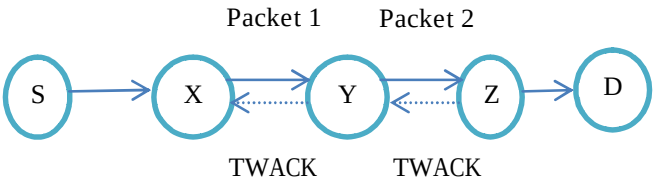

Fig 3. TWOACK Approach

TWOACK approach requires an explicit acknowledgment to be sent by Z to notify X about the successful reception of the data packet. When node Z receives the data packet successfully, it sends a 2ACK packet to X with the id of the corresponding data packet. The TWOACK transmission takes place for every set of triplets along the route, as shown in the fig 3. This approach is mainly used to resolve the receiver collision and limited transmission power problems of watchdog approach. Cost is the main overhead of this approach since it requires a two-hop ack for every data packet. In S-TWOACK scheme, each TWOACK packet acknowledges the receipt of all the data packets over the period of time.

4.6. Cross layer approach

Cross-layer approach for packet drop used to identify data packet droppers. In this approach, the two types of the monitoring protocol are used in network layer and the MAC layer. Each node maintains a record of the forwarding of each packet and it transmits, like watchdog approach. To overcome with the network overhead, for each received packet the node transmits two-hop ACK coordinated with MAC ACK. To prevent an intermediate node from destroying two-hop ACK, public key distribution is used in this methodology. To reduce the cost of this approach, random two-hop ACK is used. In this approach, a arbitrary ACK is transmitted in every three consecutive nodes instead of transmitting ACK for every data packet. A node will choose an even number if it needs an ACK, otherwise it will choose an odd number.

This approach increases the network overhead because of public key distribution.

4.7. Adaptive ACKnowledgment scheme (AACK)

Adaptive acknowledgment scheme [20], a network layer acknowledgment based scheme in which the TwoAck and end-to-end schemes are combined. In this approach, if a sender has more than one destination in the network, it will operate in two different modes, Adaptive ACK mode and TwoACK mode.

A switching system is used to enable a node to work in two different modes. The default mode of the switching system is AACK mode. The source node will inform the intermediate node about the flow mode, so that the intermediate node will forward the packets in AACK mode, or it will send TWOACK packet to the previous two hop node in TACK mode.

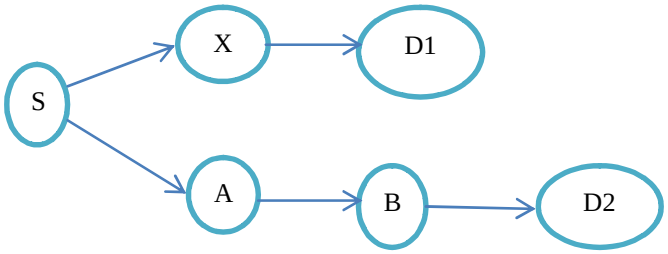

Fig .4 AACK Approach

In the fig 4, a source node S has two flows, S-X-D1 and S-A-B-D2. The switching system will enable the Source node to operate in AACK mode for the path S-A-B-D2 since it has more than two hops, and in TACK mode for the path S-X-D1

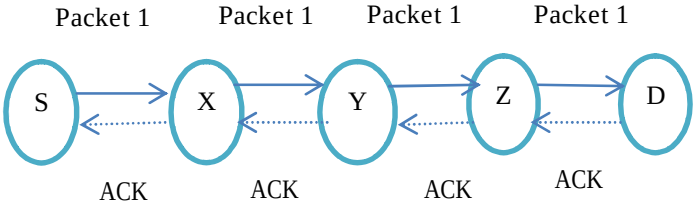

Fig 5. Packet transmission in AACK mode

In AACK mode, the destination node sends only one ACK packet to the source node instead of sending ACK packet for every three consecutive nodes. When the destination node D receives the data packet1 from the source node S through intermediate nodes X, Y and Z, it is required to send an ACK packet to the source node, as shown in the fig 5. Hence, it reduces the network overhead. But, both TWOACK and AACK fail to detect the malicious node with the presence of false misbehavior report and forged acknowledgment packets. This scheme is used to Overcome collisions and limited transmission power problem of watchdog approach. Moreover it improves the TWOACK scheme. However, in AACK mode, the long path causes packet dropping attack due to significant delay.

4.8. 2ACK

2ACK approach to detect the adverse effects of selfish nodes [15]. It is based on a simple 2-hop acknowledgment packet. The receiver node in the 2-ACK scheme sends 2-ACK packets only for a fraction of received data packets. It has an authentication mechanism to make sure that the 2-ACK packets are genuine. This reduces the network overhead by minimizing the number of ACK packets and also it is cost effective. However, it focuses only on link behavior rather than a single node.

5. Conclusion

Packet-dropping attack has always been a major threat to the security in MANET. In this paper we have presented a survey of the securing MANETs against packet dropping attack. Most of the existing approaches are used to detect only the misbehavior links rather than the malicious nodes. Moreover, they fail to detect partial dropping of packets in MANET. The detection of packet droppers in MANET is a challenge even though many approaches have been proposed against packet dropping attack. Some approaches that rely on cryptography and key management are too expensive. Each approach can work only with specific attack. The approaches that work well in the presence of one malicious node are not suitable for multiple colluding attackers. The focus on all possible types of attack for more secure and reliable MANET with minimizing the cost can still improve the effectiveness and efficiency of the security schemes.

References

[1] R. Akbani, T. Korkmaz, and G. V. S. Raju, “Mobile Ad-hoc Network Security,” in *Lecture Notes in Electrical Engineering*, New York: Springer-Verlag,.

[2] R. H. Akbani, S. Patel, and D. C. Jinwala, “DoS attacks in mobile ad-hoc networks: A survey,” in *Proc. 2nd Int. Meeting ACCT*, Rohtak, Haryana, India, 2012, .

[3] S. Djahel, F.N. Abdesselam, Zonghua Zhang, Mitigating Packet Dropping Problem in Mobile Ad-hoc Networks : Proposals and Challenges, IEEE Communications Surveys & Tutorials, Fourth Quarter 2011.

[4] D. Djenouri, N.Badache, Cross-Layer Approach to Detect Data Packet Droppers in Mobile Ad-Hoc Networks, IWSOS , 2006.

[5] P.Goyal, S.Batra, Ajit Singh, A Literature Review of Security Attack in Mobile Ad-hoc Networks,

International Journal of Computer Applications, Vol.9, No.12, November 2010.
[6] E. Hernandez, M.D. Serrat, Improving Selfish Node Detection in MANETs Using a Collaborative Watchdog, IEEE Communications Letters, May 2012.
[7] Y.Hu, D.Johnson and A.Perrig, " SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in proc. 4th IEEE Workshop Mobile Comput. Syst. Appl., 2002,.
[8] Y.Hu, A.Perrig, and D.Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in proc. 8th ACM Int.Conf.MobileCom, Atlanda, GA, 2002,.
[9] G. Jayakumar and G. Gopinath, "*Ad-hoc* mobile wireless networks routing protocol—A review," *J. Comput. Sci.*„2007.
[10] D.Johnson and D.Maltz, "Dynamic Source Routing in ad hoc wireless networks," in mobile computing. Norwell, MA: Kluwer, 1996,
[11] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in *Proc. 12th Int. Conf. iiWAS*, Paris, France, Nov. 8–10, 2010,
[12] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in *Proc. IEEE 25th Int. Conf. AINA*, Biopolis, Singapore, Mar. 22–25, 2011
[13] B.Kannhavong, H. Nakayama, Y.Nemoto, Nei Kato, A Survey of Routing Attacks in Mobile Ad-Hoc Networks, IEEE Wireless Communication, October 2007.
[14] J.S.Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," IEEE Trans.Ind.Electron.„ Apr. 2008.
[15] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, An Acknowledgment-Based Approach for the Detection of Routing Misbehaviour in MANETs. In the IEEE Transactions on Mobile Computing2007.
[16] S. Marti, T.J. Giuli, K. Lai, and M. Baker, Mitigating Routing Misbehaviour in Mobile Ad-hoc Networks. In the Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, ACM, pp. 255-265, Boston, Massachusetts, US, 2000.
[17] N.Nasser and Y.Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in proc. IEEE Int. Conf. Commun., Glasgow, Scotland, Jun. 24-28, 2007
[18] J.Parker, J.Undercoffer, J.Pinkston, and A.Joshi, "On intrusion detection and response for mobile ad hoc networks," in proc. IEEE Int.Conf.Perform.,Comput.,Commun.,
[19] A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad-hoc networks," in *Proc. Radio Wireless Conf.*, 2003,
[20] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, A. Mahmoud, "Video Transmission Enhancement in Presence of Misbehaving Nodes in MANETs", International Journal of Multimedia Systems, Springer,, 2009.