Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET

Aishwarya Sagar Anand Ukey[1], Meenu Chawla[2]

[1] Department Of Computer Science & Engineering, Maulana Azad National Institute of Technology, Bhopal , Madhya Pradesh, India

[2] Department Of Computer Science & Engineering, Maulana Azad National Institute of Technology, Bhopal , Madhya Pradesh, India

Abstract

Mobile Ad hoc NETwork (MANET) is self configuring network of mobile node connected by wireless links and considered as network without infrastructure. Routing protocol plays a crucial role for effective communication between mobile nodes and operates on the basic assumption that nodes are fully cooperative. Because of open structure and limited battery-based energy some nodes (i.e. selfish or malicious) may not cooperate correctly. After becoming part of active path, theses nodes start refusing to forward or drop data packets thereby degrades the performance of network. In this paper, a new reputation based approach is proposed that deals with such routing misbehavior and consists of detection and isolation of misbehaving nodes. Proposed approach can be integrated on top of any source routing protocol and based on sending acknowledgement packets and counting the number of data packets of active path.

Keywords: *Mobile Ad hoc Networks, Routing Misbehavior, Non-cooperation, Selfish, Malicious, Reputation*

1. Introduction

MANET consists of wireless mobile nodes that form a temporary network without the aid fixed infrastructure or central administration. Nodes can communicates directly to other nodes within their transmission range. Nodes outside the transmission range are communicated via intermediate nodes such that it forms a multihop scenario. In multi-hop transmission, a packet is forwarded from one node to another, until it reaches the destination with the help of using routing protocol. For proper functioning of the network cooperation between nodes is required. Here cooperation refers to performing the network functions collectively by nodes for benefit of other nodes. But because of open infrastructure and mobility of nodes, non-cooperation may occurs which can severely degrades the performance of network.

MANET is vulnerable to various types of attacks because of open infrastructure, dynamic network topology, lack of central administration and limited battery-based energy of mobile nodes. These attacks can be classified as external attacks and internal attacks. Several schemes had been proposed previously that solely aimed on detection and prevention of external attacks. But most of these schemes become worthless when the malicious nodes already entered the network or some nodes in the network are compromised by attacker. Such attacks are more dangerous as these are initiated from inside the network and because of this the first defense line of network become ineffective. Since internal attacks are performed by participating malicious nodes which behave well before they are compromised therefore it becomes very difficult to detect.

Routing protocols are generally necessary for maintaining effective communication between distinct nodes. Routing protocol not only discovers network topology but also built the route for forwarding data packets and dynamically maintains routes between any pair of communicating nodes. Routing protocols are designed to adapt frequent changes in the network due to mobility of nodes. Several ad hoc routing protocols have been proposed in literature and can be classified [1] into proactive, reactive and hybrids protocols.

The basic problem with most of the routing protocols is that they trust all nodes of network and based on the assumption that nodes will behave or cooperate properly but there might be a situation where some nodes are not behaving properly. Most adhoc network routing protocols becomes inefficient and shows dropped performance while dealing with large number of misbehaving nodes. Such misbehaving nodes support the flow of route discovery traffic but interrupt the data flow, causing the routing protocol to restart the route-discovery process or to select an alternative route if one is available. The newly selected routes may still include some of misbehaving nodes, and hence the new route will also fail. This process will continue until the source concludes that data cannot be further transferred. Proposed work focus on such misbehavior for its detection and isolation from network.

2. Node Misbehavior Model

Routing protocols basically performs two important functions: Routing function and Data-Forwarding function. Routing function performs routes discovery and routes maintenance activity. Data-Forwarding function is concerned with forwarding data packets toward the destination through the established route. In order to work properly, routing protocols need trusted working environments which are not always available and in such a situation network will be vulnerable to various attacks launched by misbehaving nodes. Both routing and data-forwarding function would be affected with the presence of misbehaving nodes. Node's misbehavior can be classified [2] into following:

- Malfunctioning: These nodes suffer from hardware failures or software errors.
- Selfish: These nodes refuse to forward or drop data packet and can be defined into three types [3] (i.e. SN1, SN2 and SN3). SN1 nodes take participation in the route discovery and route maintenance phases but refuses to forward data packets to save its resources. SN2 nodes neither participate in the route discovery phase nor in data-forwarding phase. Instead they use their resource only for transmissions of their own packets. SN3 nodes behave properly if its energy level lies between full energy-level E and certain threshold T1. They behave like node of type SN2 if energy level lies between threshold T1 and another threshold T2 and if energy level falls below T2, they behave like node of type SN1.
- Malicious: These nodes use their resource and aims to weaken other nodes or whole network by trying to participate in all established routes thereby forcing other nodes to use a malicious route which is under their control. After being selected in the requested route, they cause serious attacks either by dropping all received packets as in case of Black Hole attack [4], or selectively dropping packets in case of Gray Hole attack [5]. For convenience such malicious nodes are referred as MN nodes.

SN2 type nodes do not pose significant threat therefore can simply be ignored by the routing protocol. On the other hand SN1, SN3 and MN nodes (defined in section II) are much more dangerous to routing protocols. These nodes interrupt the data flow by either by dropping or refusing to forward the data packets thus forcing routing protocol to restart the route-discovery or to select an alternative route if it is available which in turn may again include some malicious nodes, therefore the new route will also fail. This process form a loop which enforce source to conclude that data cannot be further transferred. This proposed work aimed on the detection and isolation of such SN1 type selfish nodes and MN type malicious nodes. SN3 type selfish nodes will be detected only when they behaves similar to SN1 type nodes.

3. Related Work

To prevent routing misbehavior or selfishness in MANETs, various solutions have been proposed previously which can be roughly classified [6] as:

- Secure routing based scheme: aims at securing the establishment and maintenance of routes.
- Credit based scheme: specifically address forwarding of packets for other nodes.
- Reputation based scheme: aim at reactively detecting misbehavior and proactively isolating misbehaved nodes to prevent further damage.

This section briefly describes some previously proposed reputation based schemes as proposed approach is also reputation based.

Marti [7] proposed a reputation-based scheme in which two modules (i.e. watchdog and pathrater) are added on at each node. Watchdog module maintains a buffer of recently sent or forwarded data packets. Buffer is cleared only when watchdog overhears the same packet being forwarded by the next hop node over the medium and if a data packet remains in the buffer too long, the next hop neighbor is suspected to be misbehaving. Based on watchdog's suspicion, Pathrater module maintains a rating for every other node in the network and calculates a path metric by averaging the node ratings in the path and then chooses the best path. Main advantage of this scheme is that it can detect misbehavior at the forwarding level as well as in link level. But it might not detect misbehavior in presence of ambiguous collisions, receiver collisions, limited transmission power, false misbehavior and partial dropping.

Buchegger [8] proposed CONFIDANT protocol which is based on selective altruism and Utilitarianism. In

CONFIDENT, trust relationships and routing decisions are based on experienced, observed, or reported routing and forwarding behavior of other nodes. It consists of four modules: The Monitor, the Reputation System, the Path Manager, and the Trust Manager. Each node monitors the behavior of its next-hop node continuously and if a suspicious activity is detected, information of the suspicion is passed to the Reputation System. The Reputation System changes the rating of the suspected node which depends on how significant and how frequent the activity is and if rating of a node becomes less than certain threshold, control is passed to the Path Manager. Path Manager then controls the route cache. Warning messages in the form alarm message are propagated to other nodes by the Trust Manager. The pitfall of CONFIDANT includes deciding the criterion for choosing threshold value is difficult. Deciding the criteria for maintaining the friends list by Trust Manager is difficult. It can also generate false ALARMS. There might be a situation where two nodes declare each other misbehaving through ALARM messages.

To prevent selfishness in MANET, Balakrishnan [9] proposed a TWOACK scheme which can be implemented as an add-on to any source routing protocol. Instead of detecting particular misbehaving node, TWOACK scheme detects misbehaving link and then seeks to alleviate the problem of routing misbehavior by notifying the routing protocol to avoid them in future routes. It is done by sending back a TWOACK packet on successful reception of every data packet, which is assigned a fixed route of two hops in the direction opposite to that of data packets. Basic drawback of this scheme includes it cannot distinguish exactly which particular node is misbehaving node. Sometime well behaving nodes became part of misbehaving link and therefore can not be further used the network. Thus a lot of well behaved node may be avoided by network which results in losing of well behaved routes.

Vijaya [10] proposed another acknowledgement based scheme similar to TWOACK scheme, which is also integrated on top of any source routing protocols. This scheme detects the misbehaving link, eliminate it and choose the other path for transmitting the data. The main idea is to send 2ACK packet which is assigned a fixed route of two hops back in the opposite direction of the data traffic route and to reduce the additional routing overhead, a fraction of the data packets will be acknowledged via a 2ACK packet. This fraction is termed as Rack and by varying the Rack, overhead due to 2ACK packets can be dynamically tuned. This scheme also consists of multicasting method by which sender can broadcast information of misbehaving nodes so that other nodes can avoid path containing misbehaving nodes and take another path for the data transmission. Although routing overhead caused by transmission of acknowledgement packets is minimized but this scheme also suffers to detect the particular misbehaving node.

Usha and Radha [11] proposed extension to the TWOACK scheme, in which each node must send back a normal Ack to its immediate source node after receipt of any kind of packet. This scheme requires an end to end Ack packet (i.e. Nack) to be sent between the source and the destination. On receipt of the data packets sent by the source, destination responds with a Nack packet. The Nack would reach the source from the destination with the help of the path, which is found in the actual message packet, delivered to the destination. If a node is found to be misbehaving in the pre calculated path, the intermediate nodes are free to divert the Nack packet through alternative paths and this path will be stored in the Nack packet along with the older path, which is extracted from the original message. On receipt of the Nack packet, the source node compares the two paths that are in the Nack packet. If variation is found, then the node in the source to destination path, from where the path varies in the destination to source path is isolated and that particular node is marked as a potential misbehaving node by the source node otherwise source node concludes no potential misbehaving nodes in the path. Possible drawback includes lot of routing overhead because of Ack and Nack packets. Also due to nodes mobility probability of Nack packet reaching to source becomes smaller with the large number of intermediate nodes between source and destination.

Zeshan [12] proposed a two-fold approach for detection and isolation of nodes that drops data packets. First approach attempts to detect the misbehavior of nodes and will identify the malicious activity in network. It is done by sending an ACK packet by each intermediate node to its source node for confirming the successful reception of data packets. If the source node does not get ACK packet by intermediate nodes then source node send again its packet for destination after a specific time. If same activity was observed again then source node broadcast a packet to declare the malicious activity in the network. Other approach identifies exactly which intermediate node is doing malicious activity. It is done by monitoring the intermediate nodes of active route by the nodes near to active path which lies in their transmission range and by the nodes which are on the active route. Since monitoring nodes are in promiscuous mode and are in the transmission range of intermediate nodes of active route, they can receive all the packets sent along the active route. Monitoring nodes count the number of packet coming into and going out of the nodes of active route. Each monitoring node maintain a list of sent and dropped packets and when number of dropped packets by a particular node exceeds certain threshold, the monitoring node in that range declares that node as misbehaving node and broadcast this information. Upon receiving broadcast packet all neighboring nodes will cancel their transmission to that particular node and enter it into the list of misbehaving nodes. Main disadvantage of this scheme includes the overhead due to transmissions of acknowledgement packets by every intermediate node to the source and working of all nodes in promiscuous mode.

4. Proposed Approach

4.1 Assumption

Following assumptions are made in the proposed scheme:

- All nodes may work in promiscuous mode.
- Misbehaving nodes do not drop acknowledgement packets.
- Misbehaving nodes do not work in groups.
- Misbehaving nodes do not send or forward false acknowledgement packet.

4.2 Logical grouping and Ack packet transmission

In this proposed scheme, as soon as the active route is found, all nodes of active route are logically grouped into N sets (i.e. S1, S2,….,SN) where N=n/3 (n is number of nodes on active route) such that set S1 contains first three consecutive node, set S2 contains next three consecutive nodes and so on. For convenience we refer first nodes, middle node and last node of a set as LNode, MNode, and RNode respectively. Last set SN may contain one, two or three nodes. It behaves normally if contains three nodes. If it contains two nodes then first node act as LNode and second one as RNode. If it contains single node then that node act as RNode. The sets are grouped in a total of M = N-1 groups where two consecutive sets form a group with groups G1, G2… GM such that group GM = SN-1+SN. In a set, each RNode acknowledges its LNode by sending ACK-1 packet for successful reception of data packets. In a group, RNode of second set acknowledges LNode of its first set by sending ACK-2 packet for successful reception of data packet.

Thus in all, each group consists of two sets and each set consists of three consecutive nodes. First node of a group receives two acknowledgement packets (i.e. ACK-1 from RNode of its first set and ACK-2 packet from RNode of its second set). For example if S→ N1→ N2→ N3→ N4→ N5→ N6→ N7→ D be the active path then the nodes of active path forms three sets (i.e. S1, S2,S3) and two groups (i.e. G1,G2) as shown below :

Set S1= S→ N1→ N2

Set S2 =N3→ N4→ N5

Set S3 = N6→ N7→ D

Group G1 = Set S1 + Set S2
Group G2 = Set S2 + Set S3

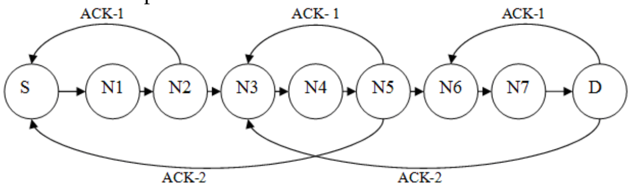

Fig. 1 Logical Grouping of Nodes

4.3 Algorithm

In proposed approach, each node maintains a LIST which consists of ID of every data packets sent or forwarded. After forwarding data packet to the next hop along the active route, LNode of every group will make an entry of forwarded data packet in the LIST and wait for ACK-1 and ACK-2 packet which are sent from RNode of first set and RNode of second set respectively. Also ACK-1 and ACK-2 packet must be received within time T1 and T2 respectively. From here execution of proposed algorithm starts which is as follow:

```
BEGIN
For each group {
        For each set
        If
        ACK-1 is not received within T1
        Then
        LNode observe the behavior of MNode for time
        T3 by rating the behavior
                And if
                Rating fall certain threshold TS1
                Then
                LNode declares its MNode as
                misbehaving node
                Else
                LNode declares its RNode as
                misbehaving node
        Else
        Wait for ACK-2 for T2
        End For

        If
        ACK-2 is not received within T2
        Then
        After T2 both MNode automatically goes to
        promiscuous mode and start rating the behavior
of      their RNodes till T4
                And if
                Rating falls below threshold TS2
                Then
                MNode declares its RNode as
                misbehaving node
                Else
                LNode of second set is declared as
                misbehaving node
        Else
        LNode deletes the ID of corresponding data
        packet from the LIST
}
End For
END
```

4.4 Details

Proposed approach includes following three steps:

- Detection of malicious group: Before identifying malicious or misbehaving node, network should be aware that some malicious activity is present or not. Suppose S→ N1→ N2→ N3→ N4→ N5→ N6→ N7→ D be the active route discovered by any source routing protocol (i.e. Dynamic Source Routing protocol [13]). As active route is discovered, source node S will start proposed algorithm and forms N number of sets and each set consists of three consecutive nodes (i.e. LNode, MNode and RNode respectively). LNode and RNode of any set act as temporary source and temporary destination. After forwarding data packet to next hop along the active route, each LNode makes an entry of forwarded data packet in LIST and then waits for two acknowledgement packets (i.e. ACK-1, ACK-2). If any ACK-1 or ACK-2 packet is not received within their time limit T1 and T2 respectively, that group is considered as malicious group.

- Identification of particular misbehaving node: If ACK-1 is received within time T1 then LNode waits for ACK-2 else observers its MNode for time T3 by rating the behavior and if rating falls threshold TS1, LNode declares its MNode as misbehaving nodes and if not, LNode declares its RNode as misbehaving nodes and then flood this information. If ACK-2 is not received within time T2, then after time T2 both MNode of that group automatically goes into promiscuous mode and starts observing their next hop nodes (i.e. RNode) for time T4. As now both MNode are in promiscuous mode, therefore can counts the number of packets coming into and going out its RNode and when it is found that number of dropped packets exceeds threshold TS2 within time T4 then that RNode is declared as misbehaving node otherwise LNode of second set is declared as misbehaving node. Finally information of misbehaving node is flooded across the network.

- Isolation and mitigation of misbehaving node: Each node of network maintains a LIST of misbehaving nodes. Thus upon receiving information of misbehaving nodes, each node update their LIST and avoid using detected misbehaving node for time T5. With the expiration of time T5, the entry of misbehaving node is temporarily deleted from the LIST thereby giving a chance to previously declared misbehaving nodes to be used by network again and if the same node is caught as misbehaving node more than certain number of time (i.e. TS3) then that node is permanently isolated from network.

Now in order to minimize additional routing overhead due to transmission of acknowledgement packets, a fraction of data packets will be acknowledged via a single acknowledgement packet. We refer this fraction of data packets as FRACK and by varying the FRACK, routing overhead due to transmissions of ACK-1 and ACK-2 packets can be dynamically tuned.

4.5 Comparison with other Acknowledgement based schemes

From Table I, it is concluded that proposed approach drastically reduced the routing overhead as compared to previous ack based scheme due to lesser transmission of acknowledgement packets with increasing number of nodes on active route.

Table 1 Comparison with other Ack based scheme

S.No	***Scheme***	***Detects malicious link/nodes***	***Ack packet transmitted with 'n' nodes on active path***
1.	TWOACK: Preventing Selfishness in Mobile Ad hoc Networks [9]	link	n-2

2.	Secure 2Ack Routing Protocol In Mobile Ad Hoc Networks [10]	link	n-2
3.	Co-operative Approach to Detect Misbehaving Nodes in Manet [11]	node	n
4.	Adding Security against Packet Dropping Attack in Manet [12]	node	n-1
5.	Proposed approach	node	~(2n/3)-1

5. Conclusions

Mobile Ad Hoc Network has been an active research area over the past few years, due to their widespread application in military and civilian communications. But it is also vulnerable to various types of attacks. Misbehavior of nodes may cause severe damage, even fails whole of the network. In this paper, investigation is done on the misbehavior of nodes and a new approach is proposed for detection and isolation of misbehaving nodes. Proposed approach can be integrated on top of any source routing protocol such as DSR and is based on sending acknowledgement packets for reception of data packets and using promiscuous mode for counting the number of data packet such that it overcomes the problem of misbehaving nodes. Also proposed approach has lesser routing overhead and more advantageous than previous similar schemes because it requires lesser number of acknowledgement packet transmission.

To show the effectiveness and results of proposed approach, implementation work on Network Simulator 2 is still in progress. Future works will includes some authentication mechanism to make sure that the ACK packets are genuine and also includes mechanism to punish misbehaving nodes.

References

[1] C. Mbarushimana, and A. Shahrabi, “Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad Hoc Networks,” in Proc. of the 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW '07), May 2007, pp. 679–684.

[2] Kargl, S. Schlott, A. Klenk, A. Geiss, and M. Weber, “Securing Adhoc Routing Protocols,” in Proc. of the 30th EUROMICRO Conference (EUROMICRO'04), August 2004, pp. 514–519.

[3] Abdelaziz Babakhouya, Yacine Challal, and Abdelmadjid Bouabdallah, "A Simulation Analysis of Routing Misbehaviour in Mobile Ad Hoc Networks," in Proc. of the Second International Conference on Next Generation Mobile Applications, Services, and Technologies, September 2008, pp. 592-597.

[4] Mohammad Al-Shurman, Seong-Moo Yoo, and Seungjin Park, “Black hole attack in mobile Ad Hoc networks,” in Proc. of the 42nd annual Southeast regional conference, ACM Southeast Regional Conference, April 2004, pp. 96–97.

[5] J. Sen, M.G. Chandra, S.G. Harihara, H. Reddy, and P. Balamuralidhar, “A mechanism for detection of gray hole attack in mobile Ad Hoc networks,” in Proc. of the 6th International Conference on Information, Communications & Signal Processing, December 2007, pp. 1-5.

[6] S. Zhong, J. Chen, and Y. Yang, “Sprite: A Simple, Cheat Proof, Credit- Based System for Mobile Ad-Hoc Networks,” in Proc. of IEEE INFOCOM’03, March 2003, pp. 1987-1997.

[7] S. Marti, T. Giuli, K. Lai, and M. Baker, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” in Proc. of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom 2000), August 2000, pp. 255-265.

[8] Sonja Buchegger Jean-Yves Le Boudec, “Performance Analysis of the CONFIDANT Protocol Cooperation Of Nodes Fairness In Dynamic Ad-hoc NeTworks" in Proc. IEEE/ACM Workshop Mobile Ad Hoc Netw. Comput. (MobiHoc 2002), June 2002, pp. 226-236.

[9] K. Balakrishnan, D. Jing and V. K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad hoc Networks," in Proc. of Wireless Communications and Networking Conference (WCNC’05), vol. 4, March 2005, pp. 2137-2142.

[10] K.Vijaya “Secure 2Ack Routing Protocol In Mobile Ad Hoc Networks,” TENCON 2008, IEEE Region 10 Conference, November 2008, pp. 1-7.

[11] S. Usha, S. Radha, "Co-operative Approach to Detect Misbehaving Nodes in MANET Using Multi-hop Acknowledgement Scheme," in 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies, December 2009, pp. 576-578.

[12] Muhammad Zeshan, Shoab A. Khan, Ahmad Raza Cheema, and Attique Ahmed, "Adding Security against Packet Dropping Attack in Mobile Ad Hoc Networks," in 2008 International Seminar on Future Information Technology and Management Engineering, November 2008, pp. 568-572.

[13] D.B. Johnson, D.A. Maltz, and Y. Hu, “The Dynamic Source Routing Protocol for Mobile ad-hoc Networks (DSR),” IETF Internet Draft, July 2004.