International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 9, September - 2013

Mitigating Packet Dropping Attack in Mobile Ad Hoc Networks using 2-ACK scheme and Novel routing Algorithm

Sonali Gaikwad 1, Dr. D. S. Adane 2
Student, Dept. of C.S.E.,S.R.C.O.E.M.,Nagpur,India1
H.O.D., Dept. of M.C.A.,S.R.C.O.E.M.,Nagpur,india2

Abstract

Mitigating packet dropping attack in MANET is considered in this paper. Now a days there is lots of work done in Mobile Ad hoc Network (MANET). MANET is a assembly of different mobile nodes. They are connected with each other with a wireless link. Mobile Ad hoc Network is one of the most important and distinctive applications. On the opposing to traditional network architecture, In MANET every single mobile node works as transmitter as well as receiver, It does not require a fixed network infrastructure. Within the same communication range both nodes are communicate directly with each other. Otherwise, they trust on their neighbors to relay messages. Due to the self-configuring skill of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. However, the open nature and varied distribution of nodes make MANET susceptible to malicious or selfish attackers. In this case, it is important to develop efficient intrusion detection mechanisms to protect MANET from attacks. To protect MANET from attacks, we use 2-ACK scheme and Novel Routing Algorithm to make the efficient routing over the MANET.

Index Terms- Mobile Ad hoc Network , Packet Dropping Attack , 2ACK , Selfish , Malicious.

1. Introduction

A mobile ad hoc network (MANET) is a collection of mobile nodes (hosts) which communicate with each other through wireless link, which is ready to cooperate and forward each other's packets. In MANETs every node is honest and cooperative this is the basic norms for the design of routing protocols. That means, if any of node claims that it can reach any other node by a certain path or distance, the claim is true; similarly, if a node reports that any link break, the link will no longer to be used. While this hypothesis can fundamentally simplify the design and implementation of routing protocols, it temporarily introduces a vulnerability to several types of denial of service (DoS) attacks [1], particularly packet dropping attack. To introduce such attack, a selfish node can secretlydrop some or all data packet passing through it. Due to the deficiency of physical protection and consistent medium access mechanism, packet dropping attack is denote most destructive or a serious attack to the routing function in MANETs. A malicious node can easily join the network and compromise a sincere node then consequently start dropping packets that are expected to be transmitted in order to disrupt the regular communications.

Here we use 2ACK scheme to detect the selfish node eliminate them and choose the other path for transmitting the data. After choosing the other path for transmitting the packet there is a huge routing overhead is generated and this is the limitation of 2ACK scheme.
A Novel Routing Algorithm is used to reduce the routing overhead generated in 2ACK scheme. We propose a method to solve the above issue and increasing the efficiency of 2ACK scheme.

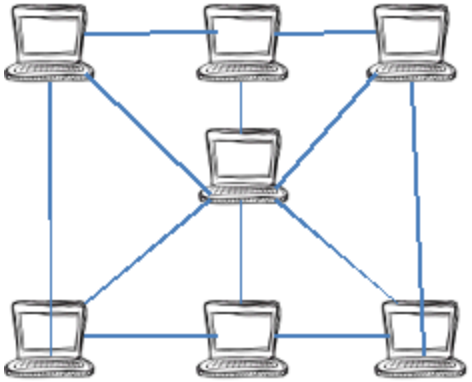


Fig 1.1. Shows the diagram of Mobile Ad hoc Network.

1.1 Problem for Packet Dropping.

The main reason for a packet can be dropped is due to MAC or network layers because of the following reasons:

- MAC level is limited due to which ,whenever if the buffer is full any new data packet coming from higher layers will be dropped. In MAC layer the size of packet's transmission buffer level is limited.
- Rules of IEEE 802.11 protocol's: If the retransmission tries or the one of its corresponding RTS (Request To Send) frame has reached the maximum permitted number, due to node's movement or collision, a data packet will be dropped.
- If it is degraded during transmission due to some occurrence specific to radio transmissions such as interference, hidden nodes and high bit error rate a data packet may be dropped or lost.

In addition to these causes, a selfish node may refuse to transmit a packet aiming to save its energetic resources in order to spread its lifetime or simply because its battery power is weak. Moreover a malicious node may intentionally drop the packets in order to provoke a collapse in network performances at network layer. Furthermore, it can modify the IEEE 802.11 MAC protocol's parameters to incite packet dropping. According to this analysis, the new challenges in MANETs still open the door for packet dropping problem. For example, how can we identify the important reason that a node to drop others' packets? In other words, how can we know the purpose of a node to accuse it as malicious, selfish or sincere?

The following **Fig.,1.2** shows the scenario for packet dropping and misrouting. Many packets are dropped due to the routing misbehaviour in MANETs.

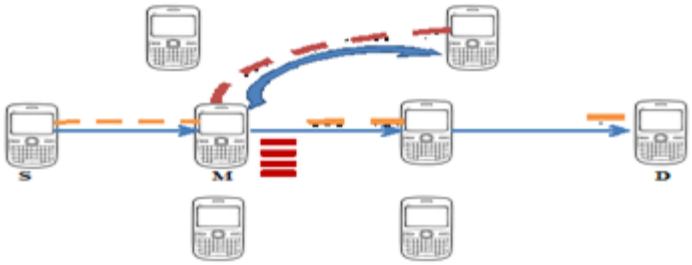


Fig. 1.2: Scenario of packet dropping attack in Manets

1.2Selfish Node.

There are 3 types of Selfish nodes:

- Selfish Nodes (SN1): These types of selfish nodes contribute in route creation but refuse to forward data packets.
- Selfish Nodes (SN2): These nodes participate in neither the route creation phase nor forward data packets. They only use their energy for broadcasts of their own packets.
- Selfish Nodes (SN3): Based on their energy levels , these nodes misbehave differently. When the energy lies between full energy E and a threshold T1, the node behaves properly. For an energy level between T1 and another lower threshold T2, it behaves like a node of type SN1. Finally, for an energy level lower than T2, it behaves like a node of type SN2. The relationship between T1, T2, and E is $T2 < T1 < E$. The presence of the SN2 type nodes is simply unnoticed by the routing protocol. Thus, these nodes do not pose a significant threat to the normal operation of the routing protocol, even though they may degrade network connectivity. On the other hand, SN1 and SN3 types of nodes are more dangerous to routing protocols.

II.Related Work

A lot of work has been done in the field of Mobile Ad-hoc Network. Routing has been one of the main problem in MANET because of dynamic nature of the network. So many authors have worked on routing problem in MANET.

1) Watchdog: Watchdog scheme is proposed byMarti *et al* [3].Its main aim to improve the output of network with the presence of selfish /malicious nodes.

Watchdog is used for detecting malicious node which misbehaves in network. Watchdog lasciviously attending to its next hop's transmission. It increases its failure counter, if a Watchdog node overhears, within a certain period of time that its next node fails to forward the packet. The Watchdog node reports it as misbehaving, whenever exceeds node's failure counter in a predefined threshold.

2) Ex-Watchdog: This scheme is proposed in [2] in which every node preserves a table containing information about all the path it is involved in. Each entry of this table stores the following information: identifiers of the source and destination nodes, the identifier of the path connecting the source to the destination and finally the sum of all packets sent, forwarded or received through this path. Upon receiving a message reporting an intermediate node as malicious, the source node will not increase the failure tally of this node immediately as the Watchdog does. However, it sends out a special message to the destination node through an alternative path. This message contains the same fields as each entry in the table except that the path identifier is replaced by the malicious node's address.

When the destination node receives this message, it checks first if there is a matching entry for the source and destination addresses in the table. If so, then it compares the sum value received and the one kept in its table. If the two values match then the accused node is not malicious since all the packets sent by the source are received at the destination. In contrast, if the two values are different, then a reaction mechanism is triggered. If no matching entry exists, then the reported node is malicious. As a result, a confirmation message is sent back to the source node. The absence of an alternative path to the destination makes the source unable to check the correctness of the report, and thus cannot recognize which node is malicious; the reporter or the reported.

3)Confidant: Buchegger [4] proposed CONFIDANT protocol which is based on selective altruism and Utilitarianism. In CONFIDENT, routing decision and trust relationships are based on practiced, perceived, or testified routing and forwarding performance of other nodes. It consists of four components: The Monitor, the Reputation System, the Trust Manager, and the Path Manager. Every node monitors the behavior of its next-hop node continuously and if a doubtful activity is identified, information of the doubt is passed to the Reputation System. The rating of the suspected node will be changes by the Reputation System 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.

III. Proposed Work

In order to detect misbehaving nodes, we suggested a network-layer scheme called 2-ACK, which can be implemented as a simple add-on to any source routing protocol such as ALOHA. When a node forwards a data packet, the nodes routing agent verifies that the packet is received successfully by the node that is two hops away on the source route. This is done through the use of a particular type of acknowledgment packets, termed 2-ACK packets. 2-ACK packets have a very similar functionality as the ACK packets on the Medium Access Control (MAC) layer or the TCP layer.

A node acknowledges the receipt of a data packet by sending back a two-hop 2-ACK packet along the active source route. If the data packet sender or forwarder does not receive a 2-ACK packet corresponding to a particular data packet that had been sent out, the forwarding link of next-hop's is claimed to be misbehaving and the forwarding route broken.

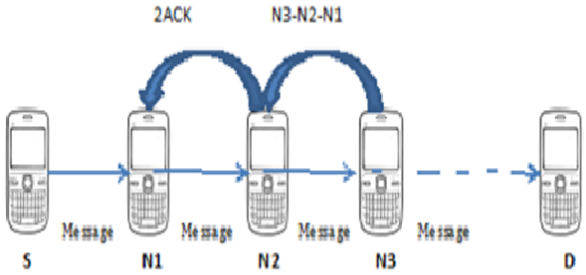


Fig. 2 :2-ACK Scheme

This 2ACK scheme is good but it has several limitations such as there is huge routing overhead generated due to the extra acknowledgement packet send and Decision obscurity if the requested node refuse to send back anAcknowledgment. In 2ACK scheme after detecting the selfish node it will choose the other path for transmitting the data due to which large routing overhead is generated. To reduce this limitation we will apply a Novel Routing algorithm.

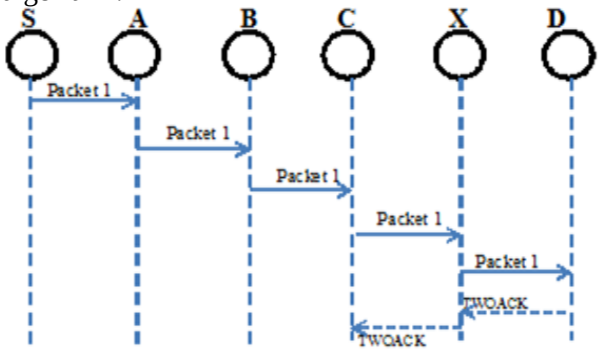


Fig. 3: 2-ACK Scheme: The Destination node is required to send back an Acknowledgement Packet that is in the form of Two-Hop

A. Novel Routing Algorithm:

In this algorithm message is shared at multiple node and then passes through common channel at the destination. We are using novel routing algorithm to make the routing efficient in MANET. The algorithm proposed the scheme to reduce the overhead and network stability. This method also maintain the Data confidentiality at various node. This type of environment is use to adapt to different traffic patterns.

Algorithm:

Whenever a mobile node wants to join the MANET it attends to the medium to find out a neighbor node *n*. After a neighbor node *n* is recognized the mobile host sends a request packet to *n* asking for its routing table which is sent back to the host. On this moment on the new mobile host can sends a packets and start routing in the MANET.

The physical location of a destination host *d* stored in the routing table is based on the routing protocol. The best possible route is chosen using a shortest path algorithm, if there is an entry in the routing table for host *d*. The route, contained a list of nodes and the consistent TTL's, the packet is attached which is sent to first host in the list. The mobile node sends a message to the adjacent fixed node that tries to find the destination node, if host *d* is not found in the routing table.

B. Environment Generation:

For environment generation we have used OMNET++ simulator. The environment was generated for different scenarios with each scenario having different number of static nodes.

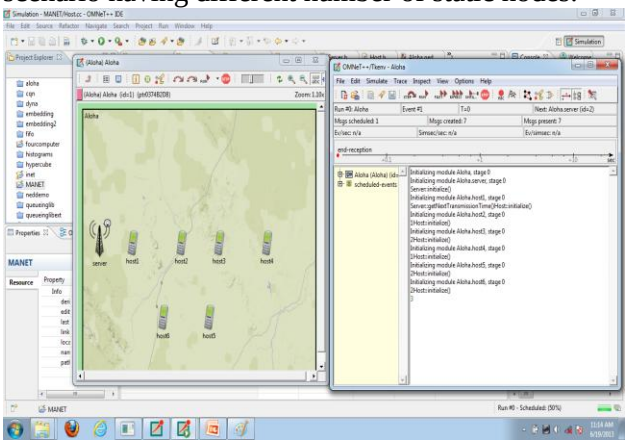


Fig 4: A setup of 6 Mobile nodes and 1 Server

IV. Experiment and Results

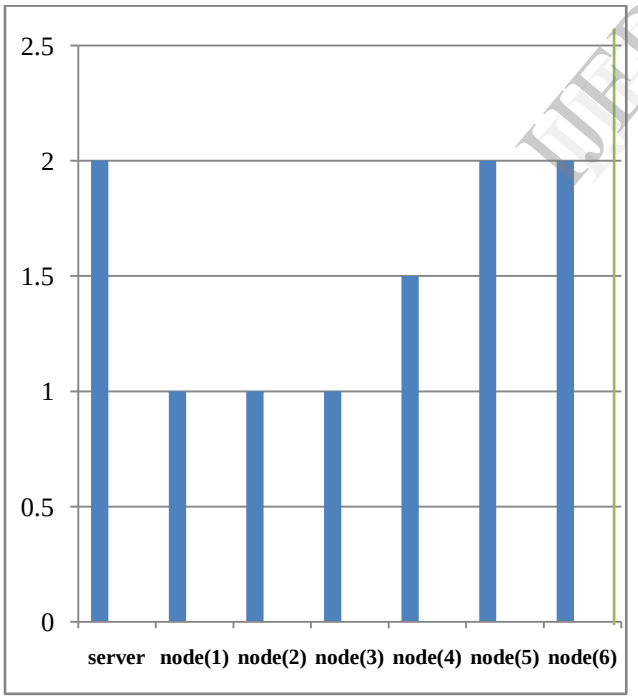
Assumptions

1. All the mobile nodes are kept static so that they are in the same range.

2. The complete 2-ACK scheme behavior has been explained by one source node, one destination node and five intermediate nodes.

3. Selfish Node behavior is induced for a certain period of time in a node and novel routing algorithm is then applied to remove selfish behavior from that node

4. Two routes are shown in this project for data packet transfer i.e. One route has all the nodes forwarding packets and sending acknowledgements whereas other route has a selfish node which sometimes forwards the packet and sometimes not.



The graph explains about the throughput (output) of the routing protocol.

Y-axis: It represents the end to end delay.
X-axis: it represents the node number

The above graph explain about end to end delay is very high in case when acknowledgement does not send by node in case of on Selfish nodes.

If node is working properly, we get acknowledgement in very short time.

V. Conclusion and future work

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. Suggested approach can be united on top of any source routing protocol such as ALOHA 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 2-ACK scheme. Also proposed approach ie., Novel Routing Algorithm has lesser routing overhead and more advantageous than previous similar schemes because it requires lesser number of acknowledgement packet transmission and it will also increase the efficiency of 2-ACK scheme.
To show the effectiveness and results of proposed approach, implementation work on OMNET++ simulator. 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] X. Wu and D. K. Y. Yau, Mitigating denial-of-service attacks inMANET by incentive-based packet filtering: A game-theoretic approach,*In Proc.* 3*rd International Conference on Security and Privacy inCommunications Networks*, Nice, France, September 2007.

[2] N. Nasser and Y. Chen, Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad Hoc Networks, *In Proc.Internationl Conference on Communication (ICC 07)*, Glasgow, June 2007.

[3] "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. 6th Annu. Int. Conf. MobileComputer.Network.*, Boston, MA, 2000, pp. 255–265 by S. Marti, T. J. Giuli, K. Lai, and M. Baker.

[4] "Performance Analysis of the CONFIDANT Protocol Cooperation Of Nodes Fairness In Dynamic Ad-hoc Networks" in Proc. IEEE/ACM , June 2002, by Sonja Buchegger Jean-Yves Le Boudec.

[5] Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges refferredIEEE paper bySoufieneDjahel, FaridNait-abdesselam, and Zonghua Zhang

[6] Capacity and Delay of Probing-Based Two-Hop Relay in MANETs.refferredIEEE paper by Jiajia Liu, *Student Member, IEEE, JuntaoGao, Student Member, IEEE, Xiaohong Jiang, Senior Member, IEEE,*HirokiNishiyama, *Member, IEEE, and Nei Kato, Senior Member, IEEE*

[7] TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks. refferredIEEE paper by KashyapBalakrishnan ,Jing Deng ,Pramod K. Varshney

[8] A Neighbor Coverage based Probabilistic Rebroadcast for Reducing Routing Overhead in Mobile Ad hoc Networks. refferredIEEE paper by Xin Ming Zhang, *Member, IEEE, En Bo Wang, Jing Jing Xia, and Dan Keun Sung, Senior Member IEEE*

[9] An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs.Referred IEEE paper by Kejun Liu, Jing Deng, Pramod K. Varshney, and KashyapBalakrishnan.

[10]A Novel Routing Algorithm for Ad Hoc Networks by Daniel Cˆamara , Antonio A.F. Loureiro

BIOGRAPHY

Miss. SonaliGaikwad has received his B.E. in Computer Science & Engineering from RTMNU, Nagpur in 2009. She is pursuing MTech in Computer Science and Engineering from ShriRamdeobaba College of Engineering and Management (Autonomous), Nagpur. Her research interest includes Ad-hoc Based Networking and MANET.