ISSN (Online) : 0974-5645
ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 8(S2), 151–155, January 2015* DOI: 10.17485/ijst/2015/v8iS2/60285

A Framework for detecting Malicious Nodes in Mobile Adhoc Network

Y. Haripriya[1]*, K. V. Bindu Pavani[1], S. Lavanya[1] and V. Madhu Viswanatham[2]

[1]VIT University, Vellore, India; priyayjnm@gmail.com, binduwelcome@gmail.com, lavanya.sammeta605@gmail.com
[2]SCSE, VIT University, Vellore, India; vmadhuviswanatham@vit.ac.in

Abstract

A wireless network consists of nodes which cooperate with each other for transmission. In adhoc network the nodes are mobile forming temporary network dynamically. These networks don't provide special security mechanics where attacks are highly possible through malicious nodes. Malicious nodes don't cooperate with other nodes and acts selfishly by reserving the resources for its own use. This decreases the performance of the routing protocol in the network. In order to increase the performance of the routing the malicious nodes has to be detected and that route has to be prevented from routing. In the previous paper the malicious nodes are just simulated and analyzed. In this paper the malicious nodes are detected in prior to the routing using consensus based algorithm and then that route is prevented for transmitting data between nodes in mobile adhoc networks.

Keywords: Consensus Based Algorithm, Malicious Nodes, MANET, NS2, Security

1. Introduction

Wireless sensor network is a large network which consists of nodes that has sensor functions. The change in topology, broadcast network, resources make the wireless network different from the adhoc network. Whenever a node wants to send the data to another node, in between nodes called as co-operator node act as an intermediate for receiving or sending the packet to destination. AODV is the most efficient communication protocol in MANET's[4,12]. In AODV routing, data packets are sent to the destination node by checking the current route from the route table, as the position of the nodes always changes. The route in between the source node and destination is maintained until the source node requires it[13,19]. As the topology in mobile adhoc network always changes the route is rediscovered until the source node is active[10]. When destination or intermediate node moves, it propagates the error message generated by node and passed until it is reached to the source node[6,10,19]. To secure the mobile adhoc networks, malicious nodes has to be removed since the data packets accepted by the malicious nodes are dropped[7]. Due to this message dropping attack, the communication between the source and the destination cannot be done[16]. This malicious node reduces the performance of the routing and reduces the security to the data[17]. In this paper the consensus based algorithm is used for the detection and prevention of malicious nodes so that the route where malicious nodes are present can be avoided. This increases the efficiency and security in data transfer and also the performance of routing is increased.

2. Related Works

2.1 Reputation Based Technique

In this method a central authority network is maintained where it keeps on updating the reputation values of the particular node[10]. A positive feedback and negative feedback is created for the nodes. A request may be sent by the other nodes to the central authority for the reputation values of a node[29,30]. It keeps on updating every interval

*Author for correspondence

time. But this approach fails in distributed huge network because a single central authority cannot calculate the entire reputation values as the network is large. Prediction of the future reputation values cannot be done and pictorial representation is not possible.

2.2 Punishment Based Technique

The detecting and eliminating of malicious node can be done in four ways. The first step involves the detection of the malicious nodes in the network. The second step involves sending a message to the neighboring nodes about the presence of the malicious node. The third step involves the assigning the reputation values to the node. The fourth step involves detecting the best path for routing by detecting the malicious node[10]. The main drawback of this method is every time the reputation values are changed so it needs to update whenever there is a request from the other nodes.

2.3 Incentive and Eigen Trust Technique

It is a technique where a node will be charged for its own transmission of packets and compensated when it forwards the packets to the other nodes[10,31]. In order to decrease the charge of the transmission it purchases the packets from the other nodes to forward it to the destination node.

2.4 COOPMAC with ARQ

This generally operates in the MAC layer in the wireless networks it is based on the Automatic Repeat Request protocol. Let us consider where P node wants to send a packet to node R through node Q, node P sends a request packet to node Q[32]. Once the node Q sends an acknowledgement to node P to transfer the packet to node R then the node P forwards the packet to node R[10]. This is the method used to for transferring the packet with automatic repeat request for re transmission if there are any errors or packet loss.

2.5 Consensus Based Algorithms

This method is used for detection and elimination of the malicious nodes from the network[15]. CUSUM detects the malicious nodes and finds whether it is a false alarm or malicious node activity[10]. The false alarm probability is calculated using the global opinions by maximum cardinality approach.

3. Proposed System

3.1 Discovery of Route using AODV

The route in between the nodes is discovered by the entries in routing table. It is ensured that the routing table is the current updated routing table, as the nodes in network are not stable. The network topology always changes since the nodes in mobile adhoc network always moves. According the routing table the data packet is forwarded to the next destination or to the intermediate node. In the process of route initialization the route request (RREQ) and the route response (RREP) packets are created. The source nodes creates the RREQ packet which consists of IP address, sequence number, destination IP address and broadcast ID. This broadcast ID is incremented every time whenever source sends the request packet. In connection to the RREQ the RREP route response is sent back by the destination node. The RREQ is broadcasted to all the neighboring nodes for particular time limit. In this time limit the reverse route has to be created between source and destination nodes. If the route is not created within the time limit or the RREQ packet lost somewhere in the network then again the source node sends the RREQ packet and is broadcasted in network. When the reverse route has been established which means the RREQ has reached the destination node then the RREP packet follows the reverse route to reach to the source node. When it reaches to the source node the forward route has been established. When the forward route has been establish now both the nodes can exchange the data between each other.

3.2 Maintaining Route

After the route establishment the data is exchanged between the source and destination. But in this mobile adhoc network nodes are always mobile. If the source nodes moves from the current position then the route discovery is reinitiated as to find the new path using RREQ packet. Or in converse to it if the intermediate nodes or destination nodes move then RERR packet is generated and propagated to the predecessor nodes in the network until it reaches to the source node. When the source node receives the RERR packet then it reinitializes the route or stops sending data.

3.3 Malicious Nodes in AODV

The message passing attack is highly possible in the MANET's and it is highly harmful. This attack can be performed using the malicious nodes. These malicious

nodes accept the route request, route response or data packets and drops it while sending it to the next node. So these malicious nodes have to be detected and prevented in the network, as the goal of these malicious nodes is to stop the communication between the source and destination.

3.4 Consensus Based Algorithm

This method helps in detecting and preventing the malicious nodes from the wireless networks. In this method CUSUM and SPRT block has been used where CUSUM is used to find the malicious nodes and SPRT block is used to find whether the result sent by the CUSUM is false alarm or it is an activity of the malicious nodes. The false alarm is found by the global opinions which are formed using the maximum cardinality approach. This global opinion is the combination of all the local opinions in the Fusion center.

Consider a node n which acts as the malicious node to some nodes and acts as the honest node to other nodes. The $e_{m,n}$ value is calculated at regular intervals for every node and this value is sent to the Fusion center. Then it takes the necessary action against the malicious node. If the $e_{m,n}$ is 1 then that node is considered as the honest node otherwise zero. The list for the honest nodes are made by

$H_{M,C} = \text{argmax}_{H \in C} ||H||$ where $e_{m,n} = 1$ and for all n, m $\in$ H.

From $H_{M,C}$ repeatedly remove the nodes which are not trust worthy by an iterative approach. The nodes which have less global opinions are removed from the list. This is done until all the nodes in the array are honest nodes.

If the malicious nodes are found in the route then that route is dropped choose for another route in the network.

```
if (malicious == true ) { drop(p, DROP_RTR_
ROUTE_LOOP);
// DROP_RTR_ROUTE_LOOP is added for no
reason.
}
```

4. Simulation Result

The performance parameters used for comparing during simulation are throughput, data packets delivery ratio and packets lost. The throughput is the data delivery per unit time during communication between nodes.

Throughput = (No. of data packets Received * Packet size * 8) /Simulation Time

The packet loss can occur in MAC layer or network layer but mostly the packet loss is considered in network layer. The packet loss can be calculated as

Packet loss = Data Packet Sent – Data Packet Received

Packet delivery ratio is the ratio of data packets received from destination to the data packets originated from the source node.

PDF = (Data Packet Received/Data Packet Sent) * 100

The evaluation of the performance of the network is done using the ns-2.35 network simulator. In this simulation scenario we consider 50 nodes with random movement within the simulation area 1000m x 1000m. The simulation time for is 250 sec. Initially number of malicious considered are 0 then consider 1, 2, 3, 4, 5. The parameters that are considered for simulation are shown in the table 1.

The performance of AODV is found by introducing some malicious nodes into the network. The throughput, packet drop and the packet delivery ratios are calculated by considering different number of malicious nodes. The Figure 1 shows the throughput for the different no. of

Table 1. Performance Parameters used in Simulation

PARAMETER	VALUE
ROUTING PROTOCOL	AODV
NO. OF NODES	50
SPEED OF NODE MOBILITY	CBR
TYPE OF COMMUNICATION	10m/sec
SIMULATION AREA	1000m x 1000m
SIMULATION TIME	250 sec
PACKET SIZSE	512 bytes
NO. OF MALICIOUS NODES	0,1,2,3,4,5

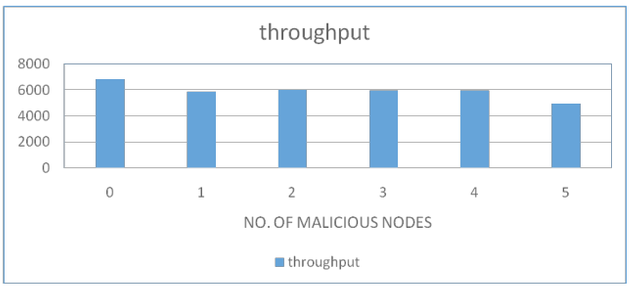

Figure 1. Throughput for different no. of malicious nodes.

malicious nodes in the network. This graph shows that when the malicious nodes are increased the through put of the network is also increased.

The Figure 2 shows the no. of packets sent and received by the mobile nodes in the network. For zero malicious nodes the packet drop is only one. But as the malicious nodes number increases the packets drop has been increasing but they are restricted to certain limit due identification of malicious nodes in prior.

In the Figure 3 the variation in packet delivery ratio has shown by increasing the number of malicious nodes in the network. This ratio in AODV routing is mostly restricted to 99% to 90%.

5. Conclusion

The techniques proposed are used to eliminate and identify the malicious nodes present in the particular network. Due to the presence of these nodes the performance, throughput, packet delivery ratio is reduced and the impact of the AODV protocol is dropped. These attacks make the node malicious so that the transmission of the packets from the source to destination never happens. The Consensus based algorithm helps to detect and prevent the malicious nodes and also provides the successful transmission of the packets between the nodes. This increases the network's performance, routing and the throughput and the results are carried out using ns2.

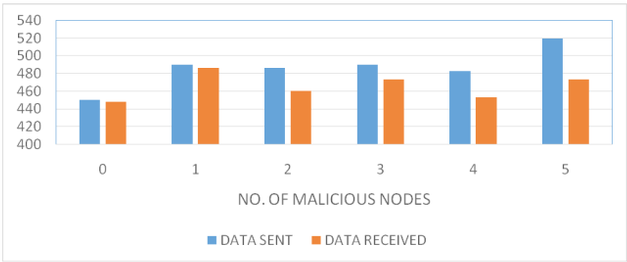

Figure 2. No. of packets sent and received under different no. of malicious nodes.

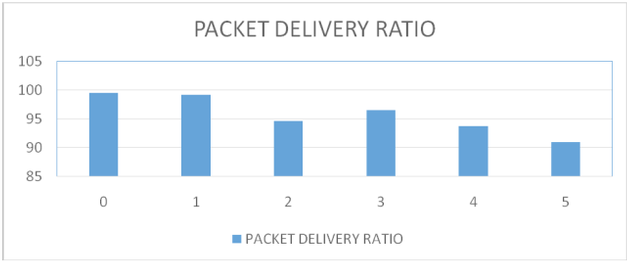

Figure 3. Packet delivery ratio under different no. of malicious nodes.

6. References

1. Dawood MZ, Zaman N, Khan AR, Salih M. Designing of energy efficient routing protocol for Wireless Sensor Network (WSN) Using Location Aware (LA) Algorithm. Journal of Information & Communication Technology. 2009; 3(2):56–70.
2. Ivanovitch MD, Silva, Guedes LA, Vasques F. Performance evaluation of a compression algorithm for wireless sensor networks in monitoring applications.
3. Nidharshini T, Janani V. Detection of duplicate nodes in wireless sensor networks using sequential probability ratio testing. International Journal of Advanced Research in Computer and Communication Engineering. 2012 Dec; 1(10):794–8.
4. Hariharan S, Precia J, Suriyakala CD, Shyry P. A Novel approach for detection of routes with misbehaving nodes in MANETs. ACEEE Int J on Network Security. 2011 Jan; 02(01):32-34.
5. Khedo KK, Perseedoss R and Mungur A. A wireless sensor network air pollution monitoring system. IJWMN. 2010 May; 2:31–45.
6. Sen J. A distributed trust management framework for detecting malicious packet dropping nodes in a mobile Ad Hoc network. IJNSA. 2010 Oct; 2(4):92–104.
7. Sen J, Chandra MG, Balamuralidhar P, Harihara SG, Reddy H. A distributed protocol for detection of packet dropping attack in mobile Ad Hoc networks.
8. Rathna R and Subramanian SA. Improving energy efficiency in wireless sensor networks through scheduling and routing. IJASSN. 2012 Jan; 2(1):21–7.
9. Silva IMD, Guedes LA, Vasques F. Performance Evaluation of a Compression Algorithm for Wireless Sensor Networks in Monitoring Applications. p. 672–8.
10. Gopal R, Parthasarathy V, Mani A. Techniques to identify and eliminate malicious nodes in cooperative wireless networks. 2013 International Conference on Computer Communication and Informatics (ICCCI -2013); 2013 Jan 09-11; Coimbatore, India.
11. Perkins CE, Royer EM. Adhoc-On Demand Distance Vector.
12. Khandakar A. Step by Step Procedural Comparison of DSR, AODV and DSDV Routing protocol. 2012 4th International Conference on Computer Engineering and Technology (ICCET 2012); 2012; Singapore. IACSIT Press.

13. Lokanath S, Thayur A. Implementation of AODV Protocol and Detection of Malicious Nodes in MANETs.
14. Cheng P, Chuah C-N, Liu X. Energy-aware node placement in wireless sensor networks.
15. Yu FR, Huang M, Tang H. Biologically Inspired Consensus-Based Spectrum Sensing in Mobile Ad Hoc Networks with Cognitive Radios. p. 26–30.
16. Khandelwal V, Goyal D. Black hole attack and detection method for aodv routing protocol in MANETs. IJARCET. 2013 Apr; 2(4):1555–9.
17. Rajaram A, Palaniswami S. Malicious node detection system for mobile adhoc networks. IJCSIT. 2010; 1(2):77–85.
18. Kaur J, Kumar V. An effectual defense method against gray hole attack in wireless sensor networks. IJCSIT. 2012; 3(3):4523–8.
19. Wadbude D, Richariya V. An efficient secure AODV routing protocol in MANET. IJEIT. 2012 Apr; 1(4):274–9.
20. Rathod P, Mody N, Gada D, Gogri R, Dedhia Z, Sanyal S, Abraham A. Security scheme for malicious node detection in mobile Ad Hoc networks.
21. Mathioudakis I, White NM, Harris NR, Merrett GV. Wireless sensor networks: a case study for energy efficient environmental monitoring**.**
22. Khetmal C, Kelkar S, Bhosale N. MANET: black hole node detection in AODV. International Journal of Computational Engineering Research. 2013; 03(6):79–85.
23. Manoj V, Raghavendiran N, Aaqib MM, Vijayan R. An approach for detection of malicious node using fuzzy based trust levels in manet. Proceedings of the 1st International Conference on Wireless Technologies for Humanitarian Relief; 2001. p. 447–80.
24. Kumar V, Sharma R, Kush A. Effect of malicious nodes on AODV in mobile Ad Hoc networks. International Journal of Computer Science and Management Research. 2012 Oct: 1(3):395–8.
25. Boukerche A, Araujo RB, Pazzi RWN. A fast and reliable protocol for wireless sensor networks in critical conditions monitoring applications. 157–64.
26. Priyambadasahu, Bisoy SK, Sahoo S. Detecting and isolating malicious node in AODV routing algorithm. International Journal of Computer Applications. 2013; 66(16):8–12.
27. Thakare AN, Joshi MY. Performance analysis of AODV & DSR routing protocol in mobile Ad hoc networks. IJCA Special Issue on Mobile Ad-hoc Networks MANETs. 2010; 4:211–8.
28. Khalil I, Bagchi S, Rotaru CN, Shroff N. UNMASK: Utilizing Neighbor Monitoring for Attack Mitigation in MultihopWireless Sensor Networks.
29. Ramzan Z, Seshadri V and Nachenberg C. Reputation-based security an analysis of real world effectiveness.
30. A survey of Reputation Based Schemes for MANET Abbas S, Merabti M and Llewellyn-Jones D. A survey of Reputation Based Schemes for MANET.
31. Abrams Z, McGrew R and Plotkin S. A non-Manipulable Trust System Based on Eigen Trust. 2005, Jul; 5(4):21–30.
32. Dehnie, Wayne and Tomasin. Detection of selfish nodes in networks using CoopMAC protocol with ARQ. Wireless Communications IEEE Transactions. 2010 Jun; 9:2328–37.
33. Marks M. A Survey of Multi-Objective Deployment in Wireless Sensor Networks.