Available online at www.sciencedirect.com

ScienceDirect

Procedia Technology 10 (2013) 530 – 537

Procedia Technology

International Conference on Computational Intelligence: Modeling Techniques and Applications CIMTA) 2013

QoS of MANet Through Trust Based AODV Routing Protocol by Exclusion of Black Hole Attack

Radha Krishna Bar[a*] Jyotsna Kumar Mandal[b] and Moirangthem Marjit Singh[c]

[a,b]*Department of Computer Science & Engineering, University of Kalyani, Kalyani, Nadia,West Bengal, India*
[c]*Department of Computer Science & Engineering, North Eastern Regional Institute of Science & Technology(NERIST), Nirjuli, Arunachal Pradesh,India*

Abstract

Black hole attack is a common security issue encountered in Mobile Adhoc Network (MANet) routing protocol. In this paper a trust value for each node has been obtained depending upon the packet forwarding ability of the node. A rank is generated based on this trust value. In the route discovery step of the AODV routing protocol a path is chosen in such a way that more trusted nodes are involved. Also a node can be excluded which is not trusted from the route. Thus the packet is transferred through a more trusted path rather than the shortest path. Results of simulation through the use of OMNeT++ simulation software shows that higher threshold values gives less packet drops providing more reliable communication.

Keywords : Black hole attack; AODV; Trust value; MANet.

1. Introduction

Since MANet is fixed infrastructure less, it suffers from various attacks. Generally two types of attacks are there namely passive attack and active attack. In passive attack the attacker silently listens the communication channel to guess what communication is going on in that channel. It does not change or modify anything in the message. Thus the attacker may come to know the confidential information that is being transferred through the channel in the

* Corresponding author. Tel.: +919735485541.
E-mail address: rdhk_bar@yahoo.co.in.

doi:10.1016/j.protcy.2013.12.392

network. On the other hand in active attack the attacker can destroy, drop, and modify the original data. Black hole attack is one of the important attacks which is responsible for packet dropping that leads to packet loss. In black hole attack [6, 7, 8] the intermediate nodes initially behaves normally. It receives the RREQ from its neighbour node and also send back RREP response message to the RRRQ sender. Thus according to the traditional AODV routing protocol a high sequence number is also assigned to this node. Thus this node actively takes part in route discovery process of AODV routing. Thus the route is also established through this node. The source and the destination seem that the actual route is established, so they start to transmit the data. But then these malicious nodes deny forwarding the packet. This node swallows the packet. Thus the packets are dropped here rather than forwarding it to its original destination. This corresponding node is known as black hole node and this effect is the black hole attack. Obviously this black hole attack degrades the Quality of Service in terms of packet dropping. There are several techniques proposed by the researchers to handle this problem. Trust based routing is one of the widely accepted techniques. The rest of the paper is organized as follows. Section 2 deals with the proposed work. Results and performances are discussed in section 3. Conclusions are drawn in section 4 and references are given at end.

2. Related Work

The selection of more trusted route become an important aspect of Ad-hoc network. To provide a trust based routing protocol several trust evaluation models are proposed by various researchers. Jain, Jain and Sagar proposed Trusted AODV (TAODV) [15] where the nodes assist and trust each other in forwarding packets from one node to another to get a more trusted path. But it suffers from some assumptions, which a node may need to recover from its neighbor node. R. S. Mangrulkar, Pallavi V Chavan, S. N. Dagadkar proposed a model called Trust Based AODV (TBAODV) [14] initially a trust value 100 is set to all the nodes in the network. Then after transferring a packet from one node to another node this trust value is increased to 200. In this method a higher trust value is assigned when a node forward a packet. And this method is not so strong to detect a black hole node and to exclude it from its route.

In this paper the trust value of a node is calculated depending upon the packet forwarding ability and a weight factor. This weight factor is defined as the ratio of number of RREP set to the number of RREQ received by the node. This trust value is inserted in the routing table and the route discovery is done according to this trust value by avoiding a less trusted node.

3. Proposed Work

In the proposed work a new parameter known as 'trust value' is calculated against all the intermediate nodes. This trust value is calculated depending upon the ability to forward packets and the RREQ forwarding ability of a node. To obtain this ability the number of packets received and the number of packet sent is counted. Two weight factor W1 and W2 are introduced. W1 is the ratio of number of packets sent from a node to the number of packets received to that node. A high value of this ratio indicates that, the node has a greater ability to forward the packets. Thus the probability of loss of packets is less. The maximum value of W1 may be 1, where all the received packets are forwarded and no packet is dropped. From this value we can also detect the untrusted nodes in the network. The other weight vector W2 is the ratio of number of RREQ received to number of RREP sent. This ratio detects the nodes which continuously receive the RREQ from its neighbour nodes but never respond to that request by sending the reply i.e. the silent node. Thus the higher value of this ratio means that, the nodes can frequently respond to the route request of its neighbour node. Then this two weight factor is multiplied to get the trust value of that node. Here we check if any nodes have the W1 value greater than the threshold value. If it can send a packet then the trust value is increased otherwise it is decreased. This trust value is saved in the routing table of that node. And in the route discovery step of AODV routing protocol the path is established according to that trust value rather than the shortest path. Thus the less trusted node can be avoided during the route establishment in AODV routing protocol.

3.1. Algorithm

Step 1

Count the number of packet received at each node.
Count the number of packet sent by each node.
Count the number of RREQ received at each node.
Count the number of RREP sent by each node.

Step 2

Calculate the threshold value: $W_1 = \frac{Number\_of\_packet\_sent}{Number\_of\_packet\_received}$

Calculate the weight factor: $W_2 = \frac{Number\_of\_Rout\,\mathrm{Re}\,ply\_sent}{Number\_of\_Routequest\_received}$

Step 3

Increase the **ptrust** value when threshold value is greater than the threshold value.
Otherwise decrease the **ptrust** value.

Step 4

Calculate Trust Value = W_1*W_2***ptrust**

Step 5

Insert Trust value into Routeing Table.

Step 6

Route establishment according to Routeing Table.
Rest of the part is similar to the traditional AODV Routeing Protocol.

3.2. Simulation Environment

The OMNeT++ simulation software is used to simulate the proposed approach. OMNeT++ is an extensible, modular, component-based C++ simulation library and framework, primarily for building network simulators.

Network is meant in a broader sense that includes wired and wireless communication networks, on-chip networks, queuing networks, and so on. Domain-specific functionality such as support for sensor networks, wireless ad-hoc networks, Internet protocols, performance modelling, photonic networks, etc., is provided by model frameworks, developed as independent projects. OMNeT++ offers an Eclipse-based IDE, a graphical runtime environment, and a host of other tools. There are extensions for real-time simulation, network emulation, alternative programming languages (Java, C#), database integration, SystemC integration, and several other functions. OMNeT++[9] is a discrete event simulation environment. Its primary application area is the simulation of communication networks, but because of its generic and flexible architecture, is successfully used in other areas like the simulation of complex IT systems, queuing networks or hardware architectures as well. OMNeT++ provides component architecture for models. Components (modules) are programmed in C++, and then assembled into larger components and models using a high-level language (NED). Reusability of models comes for free. OMNeT++ has extensive GUI support, and due to its modular architecture, the simulation kernel (and models) can be embedded easily into our applications. Although OMNeT++ is not a network simulator itself, it is currently gaining widespread popularity as a network simulation.

3.3. Simulation Parameter

For simulation of the above proposed approach/technique we consider the following parameter values of the network and use the AODV routing protocol.

Table 1. Parameter value for simulation

Parameter	Value
No of nodes	50
Node separation	150
Node Mobility Type	Mass
Mobility Speed	50mps
Mobility change interval	5s
Channel time out	100s
Routeing Protocol	AODVUU

The snap shot of the simulation environment is shown in the figure 1 which shows the graphical interface visible during interactive execution of the simulation process. The simulation scenario is shown in figure 2.

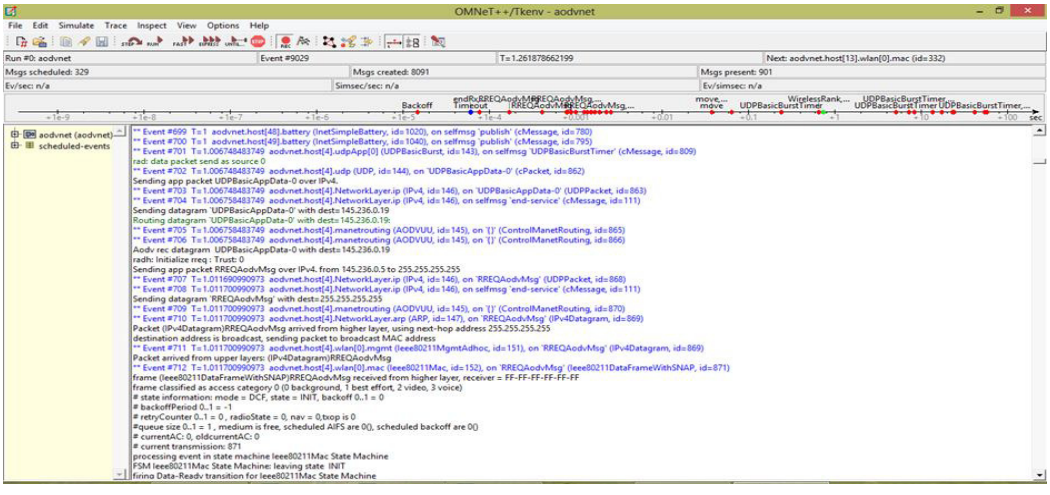

Figure 1. The graphical interface of interactive execution of simulation.

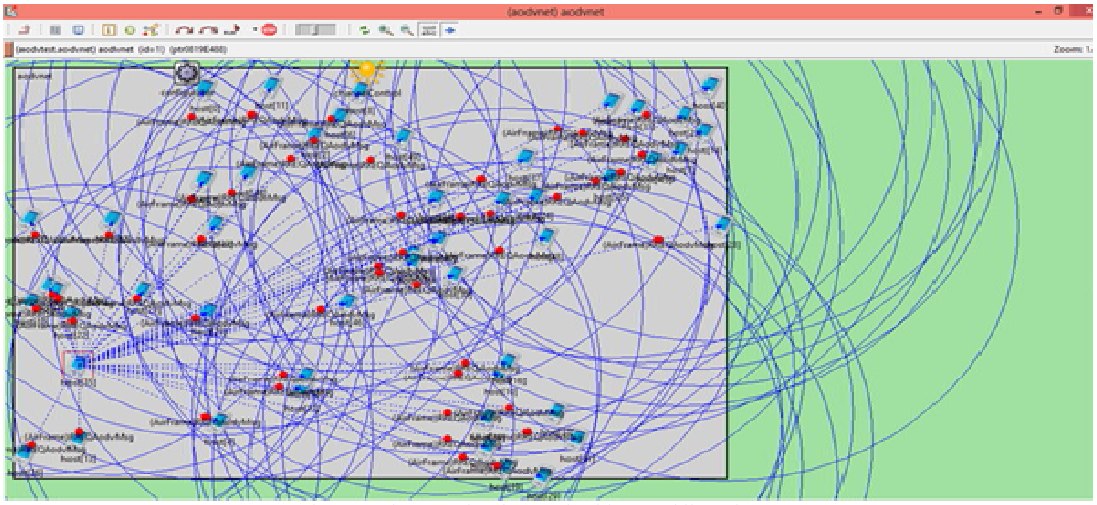

Figure 2. The scenario of network with 50 mobile nodes.

4. Result and Analysis

To evaluate the performance we apply the above approach/technique at difference threshold values. The threshold value indicates the ability to forward packets. A threshold value 0.8 means that the node is considered as trusted when it can forward at least 80 % of the received packet. Whenever the trust value of a node falls below this threshold value, it is identified as black hole node and that node is excluded from the route discovery process. The performance of the proposed technique is amazing. The trust value randomly varies from different node to node depending upon the different network parameters. The interesting observation is that the rate of packet loss changes significantly with the change of the trust value. The variation in the rate of packet loss and the trust value of each node is shown by the plot in figure 3. A node that has a greater trust value i.e. for a more trusted node the rate of packet loss is low and vice versa. This plot is obtained considering the threshold value as 0.75.

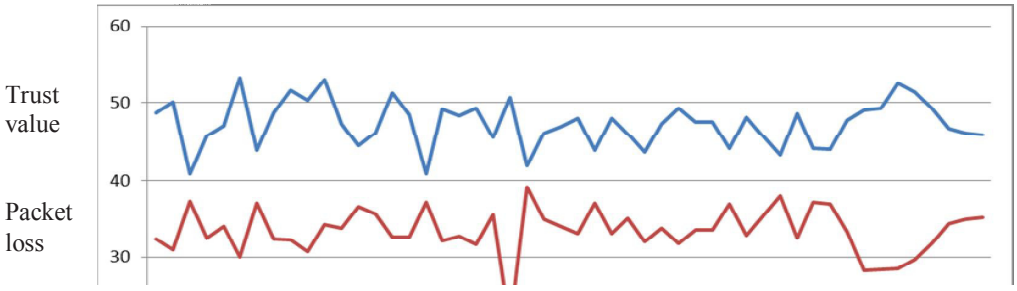

Figure 3. The variation of trust value and packet loss at each node.

Now the proposed technique has been simulated at different threshold values. They are 0.5, 0.6, 0.7, 0.8, and 0.9. For better observation here the number of nodes taken is 200. The percentage of untrusted nodes in the network, and the average packet loss is shown in table 2.

Table 2. Threshold value, % of untrusted nodes, average packet loss.

Threshold Value	% of untrusted node in the network	Average packet loss
0.9	5.7	0.007126
0.8	4.5	0.009895
0.7	4.2	0.011993
0.6	3.99	0.012842
0.5	3.81	0.016124

The plot of the values in table 2 is given in figure 4. For better visualization the threshold value is multiplied by 100 and average packet loss is multiplied by 1000.

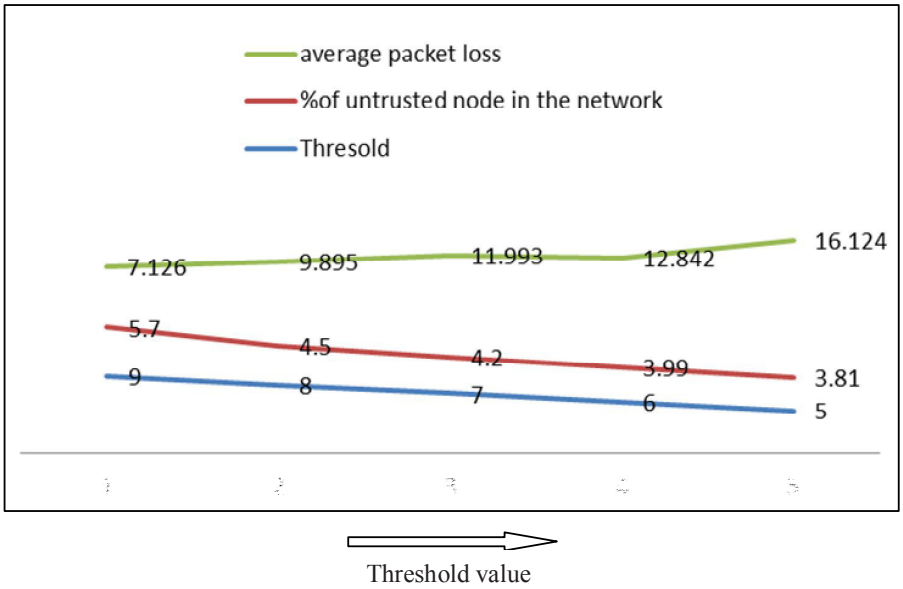

Fig. 4. Variation of average packet loss and % of untrusted nodes w.r.t. threshold value.

As there is gradual decrease in the threshold value, we allow the nodes with fewer packets forwarding capacity. Thus the packet loss is also increased correspondingly. The percentage of untrusted nodes in the network is also decreased significantly.

5. Conclusion

Trust management is important in ad hoc network because here any node can join and any node leaves away at any time. That is why the ad hoc network is too much sensitive towards various type of attack. Black hole attack is one of them, where certain node swallows all the packets in the network no packet is forwarded towards its original destination. Therefore the quality of service of the network becomes an important issue with respect to packet dropping. Here a trust value is calculated to each node and this value will be increased depending upon the ability to forward packet and ability to forward route request. Then this calculated trust value is inserted into the routing table. It is applied on AODV routing protocol. The trust value is calculated at every 0.07 second of interval and the new trust value is updated. In this way, the set of trusted nodes is maintained which is dynamic in nature. Depending upon the trust value and the threshold value the black hole node is identified and it is excluded from the route establishment process. At the time of route discovery if alternative trusted nodes are available it will always try to establish a path where more trusted nodes are involved. Here the route establishment is done according to the calculated trust value saved in the routing table rather than the traditional shortest path. Thus as it avoid the low trusted nodes, the average packet loss of the network is also decreased significantly. Thus the quality of service of the network is enhanced in terms of packet loss.

References

[1]. Chlamtac, I., Conti, M., and Liu, J. J.-N. Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks, 1(1), pp. 13–6 (2003)
[2] Arti Sehgal, Ruplai Ahuja, Sunil Kumari, A security architecture for Mobile Ad Hoc Networks, Proc. of the International Conference on Science and Engineering (ICSE 2011) , ISBN: 978-981-08-7931-0
[3]. C.Siva Ram Murthy and B.S manoj" Ad Hoc Wireless networks architecture and protocols" Pearson education, India 2005.
[4] Mohapatra Prasant, Krishnamurthy Srikanth "Ad hoc networks: technologies and protocols" Springer 2005
[5]. H. Yang, X. Meng and S. Lu: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks, ACM, 2002.

[6]. Dokurer, S. Ert, Y.M. ; Acar, C.E.” Performance analysis of ad-hoc networks under black hole attacks”, Proceedings. IEEE. pp. 148 – 153, 2007.
[7]. Perkins, C.E., Royer, E.M., "Ad-hoc on-demand distance vector routing”, www.cs.ucsb.edu/~ravenben/classes/papers/aodv-wmcsa99.pdf accessed on 25/03/2013.
[8]. Al-Shurman, M., Yoo, S., Park, S., "Black hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference pp. 96-97. (2004).
[9]. http://omnetpp.org/doc/omnetpp/ide-overview/ide-overview.html accessed on 10/02/2013.
[10]. Hothefa Sh.Jassim, Salman Yussof, “A Routing Protocol based on Trusted and shortest Path selection for Mobile Ad hoc Network”, IEEE 9th Malaysia International Conference on Communicate ions (2009).
[11]. A.Menaka Pushpa M.E., “ Trust Based Secure Routing in AODV Routing Protocol” (2009).
[12]. “TAODV: A Trusted AODV Routing protocol for Mobile ad hoc networks” (2009).
[13]. Kamal Deep Mekaetal ,“ Trust Based Routing Decisions In Mobile Ad Hoc Networks,” in the proceeding of The Second Secure Knowledge Management Workshop (SKM),2006.
[14] R. S. Mangrulkar, Pallavi V Chavan, S. N. Dagadkar, Improving Route Selection Mechanism using Trust Factor in AODV Routing Protocol for MaNeT, International Journal of Computer Applications (0975 – 8887) Volume 7– No.10, October 2010.
[15] Ankit Jain, Arnika Jain and Pramod Kumar Sagar Journal of Global Research in Computer Science 32-36 Vol.10 Issue 14 (Ver.1.0) November 2010.