Available online at www.IJournalSE.org

Emerging Science Journal

Vol. 1, No. 4, December, 2017

Dynamic Detection of Secure Routes in Ad hoc Networks

Niloofar Movahedian Attar [a*]

[a] *Department of Computer Engineering, Iran University of Science and Technology (IUST), Tehran, Iran*

Abstract

The present paper focused on ad hoc networks with an emphasis on their dynamic nature. After an introduction to ad hoc networks, there are the AODV (Ad hoc On-demand Distance Vector) routing protocol with the node malicious behaviour and consequent damages to ad hoc networks. Then, trust is described as one of the solutions for identifying secure routes when there are malicious nodes in the network. Accordingly, the paper focuses on the proposed solutions that are based on the parameter trust and the prevention of the impact of malicious networks and vulnerable connections to identify a secure route. Then, an equation is presented to calculate trust using packet forwarding rate to select a secure route for sending data packets. The proposed model was implemented on OMNET++ to evaluate the network performance. The feature of the proposed method is better performance than of the methods TVAODV and AODV. Using the proposed method, packet delivery rate increases more significantly when malicious nodes increases than that of the basic method AODV and TVAODV. There is thus a lower packet dropping rate.

Keywords:

Adhoc Networks;
Secure Routing;
Malicious Node;
AODV.

Article History:

Received:	25	September	2017
Accepted:	22	December	2017

1- Introduction

Mobile ad hoc networks (MANETs) were first developed in 2000 in the United States for monitoring the battlefield and weapons. With the advancement in electronics and hardware, such networks are widely used in areas like military, emergency, taxi service, and environmental protection, due to their easy installation and use and their applicability in certain circumstances where wired networks cannot be used [1]. Unlike the wired networks that are all physically connected with a predetermined structure and no fixed infrastructure, node-to-node communication occurs through wireless connections in such networks [2] [3].

A mobile Ad hoc network consists of a number of cells that create a wide network. The network performance is thus completely dependent on the nodes collaboration, which in turn depends on the efficient and secure routing. The improvement of security and reliability in MANETs, especially in the routing, is of great importance and attracted many researchers from all over the world. Mobile Ad hoc networks are more vulnerable that structured wireless networks due to lack of central control and fixed infrastructure. Malicious nodes also may disrupt the performance of the whole system by dropping data packets. Hence, the present study proposed a method for identifying secure routes through trust supporting.

The proposed method has been designed and developed based on the AODV routing protocol that is an on-demand-based routing protocol and finds the route between source and destination based on the smallest number of steps. The protocol assumes that the nodes are fully functional and benevolent. So if there is a malicious node, the network fails or there would be problems with the packet delivery. In fact, identifying nodes is necessary to determine the secure routes. This identification requires checking the node's behaviour and calculating the node's trust value. The node's trust represents the ability of the node to collaborate with other nodes.

The proposed algorithm is an extension to the AODV routing protocol, which aims to identify a reliable and secure route for sending data. The proposed system improves the network performance. The simulator OMNET++ was used for evaluating the performance of the proposed method. The performance of this new solution was measured and compared to of the basic methods AODV and TVAODV [4], and the results obtained were analyzed.1.1 Subtitle 1

[*] **CONTACT:** Nilouattar@gmail.com

DOI: http://dx.doi.org/10.28991/ijse-01127

(Style: Times New Roman, 10pt, Bold, Title Case)

This study's aim is to get metal flow and distributions of equivalent stress on some special sections such as longitudinal and transverse sections under processing tube tension-reducing.

2- Mobile Ad hoc Networks (MANETs)

A mobile ad hoc network consists of a group of mobile nodes that communicate with each other without the presence of infrastructure in a wireless environment. There are several reasons for the development and common use of such networks, the most important of which are:

- Rapid development and expansion on any desired scale
- Simple and low cost implementation
- No need for fixed infrastructure, unlike other wireless networks
- Dynamic connectivity
- Each station itself can be a router
- Independence from central network administration

In such networks, nodes communicate directly with neighbor nodes (a node in the radio range of the node). If the destination node is outside the radio range of the source node, the intermediate nodes in the route are used to communicate. Intermediate nodes complete the packet exchange and delivery at the destination through Store and Forward (SnF). Hence, the network fails to accomplish the assigned task without the cooperation and interaction of the intermediate nodes for conducting exchanges. Despite the many advantages of MANETs, there are also limitations the most important of that are [2, 5, 6, 7]:

- Bandwidth limitation
- Energy limitation, and the use of battery as an energy supply
- Difficulty in maintaining security
- Error in route is caused overhead in the network despite wireless connectivity and node mobility
- Considerable delays in data transmission in large networks
- Lack of central controller

3- Malicious Behavior in and Damages to Mobile Ad hoc Networks

Many research studies in the field of wireless networks, especially MANETs, have focused on the issue of security to provide trust models for sustainable network performance when there are malicious nodes. Due to the unique features of such networks and their use in different situations, as well as the increasing need for such systems in military and civilian applications, MANETs are exposed to various types of attacks from selfish and malicious nodes to disrupt the network operation and reduce the network performance. MANETs are highly vulnerable to malicious nodes due to the lack of central control for node monitoring, node mobility, and dynamic connectivity [8].

There are various malicious attacks in MANETs. Malicious nodes can partially or wholly disrupt the network operation due to the features and limitations of MANETs. A malicious node can cause problems and reduce the network performance by delaying, deleting, or even manipulating the data packets. Such malicious behavior leads to various attacks described below.

Black hole attack: In this attack, the malicious node advertises itself as a trusted node in the transmission route during transferring routing packets. The black hole node the data packets and then throws them away. With the removal of data packs, the black hole reduces the efficiency and has a negative effect on the network by droping data packets [9].

Grey hole attack: The malicious node puts itself in the transmission route like in black hole attack, but it may only drop the data packets of a particular node, exhibit malicious behavior occasionally, or carry out a combination of both attacks to drop the packets of a particular node in a particular occasion.

4- Trust and Characteristics

The term “trust” is derived from social sciences and is defined as the degree of mental confidence in the behavior of a certain entity. There are different meanings: "firm belief in the reliability, truth, or ability of someone or something" and "a hope or expectation" in Oxford Dictionary [10], and “assured reliance on the character, ability, strength, or truth of someone or something” in Merriam-Webster Dictionary. In fact, trust means the expected behavior of an entity in a specific situation. It can be concluded that trust is considered as hope, expectation, and confidence in an entity and its behavior [11].

In the field communication and network, there is similar meaning with different views and definitions. According to Chu et al. [12], trust is a set of relations among entities that participate in a protocol. The relations are based on the evidence produced through the entities' previous interactions within a protocol. Based on social networks reported by Gulbeck [13], trust is a bridge for establishing trusted relations among individuals. According to Gulbeck, the concept of trust was derived from sociology into computer sciences as a security and cryptographic descriptor and a measure for security purposes.

Trust, security, and risk are in the same direction. Degrees of trust in a division are considered the probability of change in confidence from zero (no trust) to level one (full trust) is considered. Reliability is defined as a measure of the real probability that determines the expectation level, and a precise estimate of risk is closely related to the accuracy of estimated trust.

5- Models Proposed for Mobile Ad hoc Network Routing

The lack of central controller has provided many benefits, such as very simple installation and low cost development. However, this lack has caused some limitations as well, the most important of which are trust establishment and sustainability. The lack of central network administration poses new security issues for the trust implementation in MANETs. Many methods have thus been proposed for trust evaluation.

One of the methods is trust based on cryptography, an example of which is presented by Mamatha & Sharma [14]. In this research, a method was used called route protection and simple acknowledgement, through which the hash code source is added to the packet, and then the packet is encrypted and sent to the destination. The destination node sends an acknowledgement message to the sender for the correct packets received, and a confidentiality lost message for the wrong packets. The source changes the route after receiving the confidentiality lost message to an alternate route. The advantage of this method is to prevent denial-of-service attacks. The limitations are slow performance in high density circumstances and increased overhead. Nevertheless, the biggest limitation is the issue of key distribution for cryptography. The key distribution is very difficult due to the nature of ad hoc networks, the use of radio waves, data broadcasting, and given that network security depends on key and preserving key confidentiality). Accordingly, cryptographic solutions are not effective in maintaining trust sustainability and trust implementation due to the characteristics of ad hoc networks.

Another method is node monitoring. The node monitoring system developed from a kind of trust system based on human community to implement the characteristics of this system. The node monitoring system produces higher performance with fewer weaknesses than the previous method. Synge et al. (2015) proposed a trust model based on node monitoring with cryptography [15]. Despite the advantages of the trust model, there were still limitations on the key distribution for cryptography. There are other methods proposed on the basis [16, 17]. Sun et al. (2006) regarded trust as a measurable value and demonstrated the value of trust between two nodes using a trust evaluation function. This function is updated with trust evidence observations collected from direct neighbor node monitoring. In the studies, the beta distribution function is used to update the value of trust. They, in fact, aimed to provide a sustainable model against multiple attacks. Their limitations due to statistical calculations are exponentially reduced speed when several nodes are involved simultaneously and the low performance.

6- The Proposed Method

In the proposed method, the purpose is to detect those nodes that drop data packets during data transmission. In this regard, packet forwarding rate is used for trust evaluation. The forwarding rate refers to the number of packets that are correctly sent by the node that is supposed to receive data packets. Since the trust evaluation criterion is the forwarding rate and the purpose is to detect malicious nodes intentionally dropping data packets during data transmission, the pseudo code of the proposed method used in the trust evaluation is as follows:

```
1. Network started by assigning the initial trust value (0.5) to neighbor nodes
2. Route detection
3. Data transmission started by the source node after receiving the response to the routing message
4. Node being in the safe mode and listening to the line
5. Calculation of the number of the packets sent
6. Calculation of the number of the packets forwarded by the neighbor node
7. Calculation of trust using the ratio of the number of packets sent by the node to the number of the packets forwarded by the neighbor node at time t
8. If ($trust \geq 0.5$) then
9. Continuing data transmission from that route
10. Otherwise
11. Quarantining the malicious node and removing the node from the routing stream
12. Sending an alert message to the source node
13. Route detection by the source node without the malicious node
14.  End if.
```

The advantage of the proposed method is that there is a self-organizing decision-making process for trusting a node due to the dependence on the continuous function of the node and the node behavior. Therefore, the dynamic nature of MANETs results in no disruption and there is a distributed decision-making process for trusting a node.

The proposed method made it possible to indirectly detect some malicious nodes in the network and reduce the level of their trust after identifying them. The malicious behavior and the way in which the protocol works are described as follows:

Avoidance of packet manipulation attacks: The node supposed to send packets can detect the attack by a malicious node and reduce the trust value of that node by checking the packet header and comparing it with the packets sent before after analyzing the packet forwarded by the neighbor node.

Avoidance of overload and saving energy: As nodes in hop-by-hop route move to the neighbor nodes in the route to the destination in listening mode, there is no need to send an acknowledgment packet by the destination node to notify the source node of packet delivery. The trust calculation and evaluation begin from the source node, and each node evaluates the behavior of its neighbor node in terms of trust hop by hop. If there is malicious behavior detected during data transmission and the packet is not sent correctly, the neighbor node of the packet sender notifies that source node of it as the malicious node, and the source node detects a new route after broadcasting the route request message. And, another route is selected when the route response message is received. Hence, there is no need for acknowledgement packet, traffic injection, and spending more energy in the network to notify the node of packet delivery.

7- Simulation and Results

The simulation defaults were based on IEEE 802.11b with a media access control layer using OMNET ++ [18]. Network nodes move at normal speeds with a maximum speed of 5 m/s. The normal speed is the speed by that the maximum and minimum speed for each node is determined. The speed and direction of the nodes are randomly selected and the speed of each node changes between the maximum and minimum values. The route and density of the nodes in the simulation are such that the nodes move randomly and change their routes randomly, resulting in a changing density. The transfer protocol used in simulation was User Datagram Protocol (UDP) and the traffic model was Constant–Bit–Rate (CBR). The simulation parameters are shown in Table 1.

Table 1. Simulation parameters.

Simulation Area	670×670
Number of nodes	50
Transmission range	$250\ m$
Maximum speed of nodes	$5\ m/s$
Traffic model	CBR

Packet delivery rates were compared with the change in the number of malicious nodes in the proposed method and the basic method AODV in Figure 1. Given the trust evaluation function, the detection of malicious behavior and the removal of malicious nodes in the transmission resulted in a considerably higher packet delivery rate using the proposed method than of the AODV routing protocol. This protocol reduces packet delivery rate due to the lack of malicious node detection and high packet drop rates.

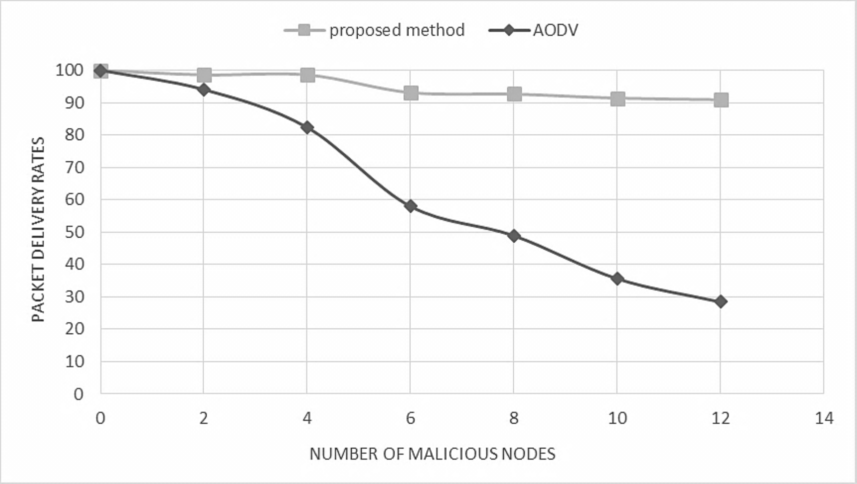

Figure 1. Packet delivery rates vs. number of malicious nodes.

In Figure 2, the packet drop rate is compared with the change in the number of malicious nodes in the proposed method and AODV. Malicious nodes start dropping data packets during data transmission when being in the route in MANETs. Such nodes are responsible for insecure routing in the network. In the proposed method, the avoidance of malicious behavior and the detection and removal of malicious nodes due to proper trust implementation resulted in the prevention of packet dropping and, consequently, secure data transmission.

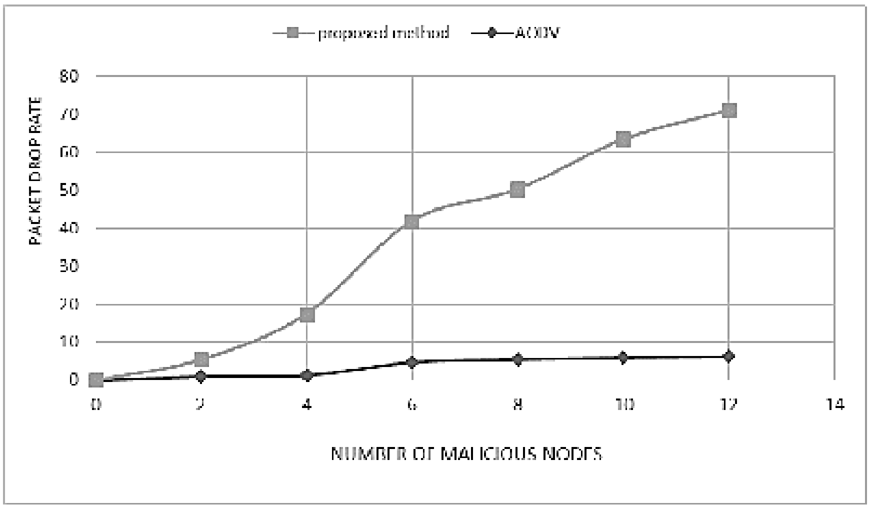

Figure 2. **Packet drop rate vs. number of malicious nodes.**

The proposed method were compared with the method TVAODV proposed by Wi Gung et al. [19] in terms of packet delivery rate with the change in the number of malicious nodes in Fig. 3. A trust vector was used in the TVAODV model. In this method, three parameters were defined for the development of trusted communications, including experience, knowledge, and recommendation. The trust vector of node A to node B is defined as Equation

$$V(A \rightarrow B) = [E_B^A, K_B^A, R_B^A] \tag{1}$$

Where, E_B^A, K_B^A, R_B^A experience, knowledge, and indirect trust recommended by A for B are obtained, respectively. E_B^A is obtained from the direct supervision of node A over node B, and is the ability of B to send packets. K_B^A is the probability that the packet can be successfully sent. R_B^A represents the views of the neighbors A and B about B. Given the non-use of the recommendations in the proposed method and that the decision making to trust a node depends on the continuous function of the node and its behavior, the detection and avoidance occur more rapidly.

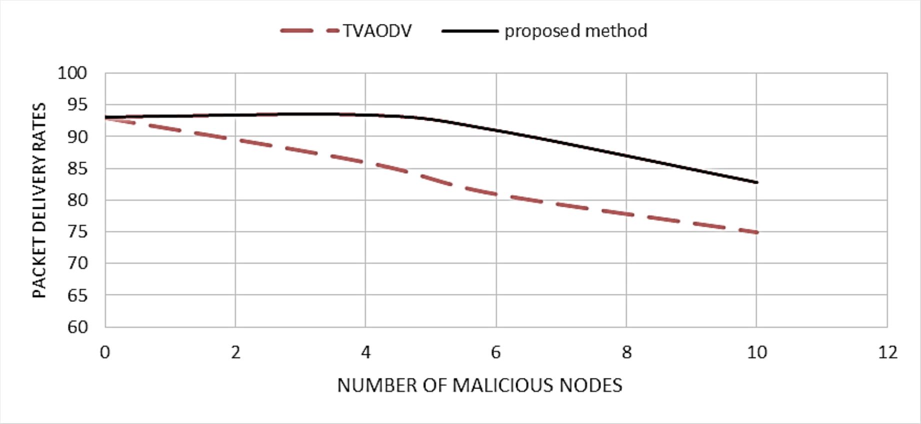

Figure 3. **Packet delivery rate vs. number of malicious nodes.**

8- Conclusion

The present paper proposed a method compatible with network conditions for identifying secure routes. It avoids the negative effects of malicious nodes and improves network performance in identifying secure routes with an extension to the AODV routing protocol. The simulation results revealed that the proposed method produces higher performance than of the basic method AODV and the extended method TVAODV. The method is capable of dynamically identifying secure routes.

9- References

[1] S.K. Dwivediand M.B. Ahmed, "Performance of Improved Trust Based Mobile Adhoc Network Routing Protocol for MANET'', International Journal of Innovative Research in Science, Engineering and Technology, Vol.5, Issue 6, June 2016.

[2] R. Haboub and M. Quzzif, "Secure and Reliable Routing In Mobile Adhoc Networks'', International Journal of Computer Science & Engineering Survey (IJCSES), Vol.3, No.1, 2012.

[3] M. Sardar and K. Majumder, "A New Trust Based Secure Routing Scheme in MANET", Advances in Intelligent Systems and Computing, pp. 321-328, 2014.

[4] W. Gong, Z. You, D. Chen, X. Zhao, M. Gu and K. Lam, "Trust Based Routing for Misbehavior Detection in Ad Hoc Networks", Journal of Networks, pp. 551-558, 2010.

[5] R.H. Jhaveri, S.J. Patel, and D.C. Jinwala, "DoS Attacks in Mobile Ad-hoc Networks: A Survey", Second International Conference on Advanced Computing & Communication Technologies, pp. 535-541, 2012.

[6] M.H. Moustafa, M.A. Youssef, and M.N. El-Derini, "MSR: A Multipath Secure Reliable Routing Protocol for WSNs", 9th IEEE/ACS International Conference on Computer Systems and Applications (AICCSA), pp. 54-59, 2011.

[7] N. Raza, M.U. Aftab, M.Q. Akbar "Mobile Adhoc Networks Applications and Challenges", Communications and Network, pp. 131-136, July 2016.

[8] H. Xia, Z. Jia, X. Li, L. Ju, and E.H.M. Sha, "Trust prediction and trust-based source routing in mobile ad hoc networks", Ad hoc Networks, pp. 2096-2114, 2013.

[9] M. Ebrahimi, S. Jamali " A Survey on Behavior and impact of Blackhole Attack in AODV protocol in Mobile Ad hoc Network", International journal of Computer Science & Network Solutions, pp. 20-27, mar 2016.

[10] Y.L. Sun, Z. Han, W. Yu, and K.J.R. Liu, "A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense against Attacks", IEEE INFOCOM, 2006.

[11] H. lie and M. Singhul, "Trust Management in Distributed Systems", Computers, IEEE Computer Society, pp. 45-53, 2007.

[12] J.H. Cho, A. Swami, and R.Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks", Comminucations Surveys & Totorials, IEEE, pp. 562-583, 2011.

[13] J. Golbek, "Computing with Trust: Definition, Properties, and Algorithms", Securecomm and Workshops, pp. 1-7, 2006.

[14] G.S. Mamatha and Dr. S.C. Sharma, "A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS", International Journal of Computer Science and Security (IJCSS), pp. 275-284, 2010.

[15] D. Singh, A. Singh, "Enhanced Secure Trusted AODV (ESTA) Protocol to Mitigate Black hole Attack in Mobile Ad Hoc Networks", future internet, pp. 342-362, 2015.

[16] Y. Sun, W. Yu, Z. Han, and K.J.R. Liu, "Trust Modeling and Evaluation for Ad Hoc Networks", Global Telecommunications Conference, Vol. 3, 2005.

[17] Y. Sun, W. Yu, Z. Han, and K.J.R. Liu, "Attacks on Trust Evaluation in Distributed Networks", 40th Annual Conference on Information Sciences and Systems, IEEE, pp. 1461-1466, 2006.

[18] http://omnetpp.org, accessed May. 2015.

[19] W. Gong, Z. You, D. Chen, X. Zhao, M. Gu and K. Lam, "Trust Based Routing for Misbehavior Detection in Ad Hoc Networks", Journal of Networks, pp. 551-558, 2010.