ATLANTIS PRESS
Advances in Intelligent Systems Research, volume 136
4th International Conference on Sensors, Mechatronics and Automation (ICSMA 2016)

A kind of Secure and Energy Conservation Routing Algorithm based on Trust Recommendation in Ad Hoc Networks

AoBo Ben[1, a], Mingming Zhang[2,b] and Li Du[3,c]

[1,2,3]College of Computer Science and Engineering, Northeastern University, Shenyang, China

[a]benaobo@163.com, [b]zmm5259@126.com, [c]duli26@126.com

Keywords: Ad Hoc networks, Network security, Trust recommendation mechanism, Energy conservation, Routing algorithm.

Abstract. Because of the open wireless channel, the dynamic change of network topology and the large energy consumptions, Ad Hoc networks are more vulnerable to security attacks and energy is easy to run out. In order to solve these problems, this paper proposes a kind of Secure and Energy Conservation Routing Algorithm based on Trust Recommendation (TREC-AODV). This algorithm can decrease energy consumption by adjusting the transmission radius dynamically, and can detect and isolate malicious nodes via a new trust recommendation mechanism. The simulation shows that the proposed algorithm not only can improve the capacity of energy conservation and robustness of the networks, but can enhance the security of the networks.

Introduction

There are many routing protocols for Ad Hoc networks[1], Ad hoc networks On-demand Distance Vector(AODV[2]) is an on-demand routing. It is an enhancement of destination-sequenced distance-vector routing protocol. The limited battery power and security attacks restrict the wide application of Ad Hoc network so that many relative researches are available in the literature. For the energy conservation issues, Energy efficient with secured reliable routing protocol [3] is based on the residual energy and effective intercept detection and correction. Energy-aware probability routing mechanism[4] uses a probability function to determine whether relay or drop the RREQ during the route discovery process. For the secure routing mechanisms, a detection and prevention mechanism with promiscuous mode[5] is proposed to detect malicious node and propagate the information of malicious node to all the other nodes in the network. MT-AODV[6] routing protocol is based on mutual trust mechanism to ensure the security of the network.

Based on the analysis of energy conservation and secure routing mechanisms, the paper proposes TREC-AODV protocol. It can not only improve the capacity of energy conservation and robustness of the network, but also have the ability to detect and isolate the malicious nodes.

Description of TREC-AODV Algorithm

TREC-AODV Algorithm includes transmission strategy design, trust recommendation mechanism and routing algorithm. Nodes are categorized into three types according to their behaviors: regular nodes, suspicious nodes and malicious nodes. Based on this categorization, it is assumed that all nodes are regular and well behaved initially.

Transmission Strategy. Due to the dynamic nature, all nodes are moving. It is assumed that each node can transmit or receive data within a maximum radius R, but both operations cannot occur simultaneously, each node has initial energy and nodes of network are uniformly distributed as Two dimensional Poisson stochastic point process.

Based on these assumptions, a strategy for transmission can be designed as follows:

(a) Source node transmits data to destination node within R.

(b) When destination node is moving out of the transmission range then calculates the closest position with the radius R and the transmission power at this position. If the node position is out of the radius R, its transmission power will be reduced until it is unequal to the transmission power.

(c) When meeting the requirement of step (b), data transmission will be continued, otherwise transmission will not be initiated.

Trust Recommendation Mechanism. In allusion to some problems existing in the current trust models, such as the incomplete consideration of trust factor and the overmuch node overhead, this paper puts forward an improved trust recommendation mechanism.

The proposed trust recommendation mechanism includes Direct Trust (DT) attribute and Recommendation Trust (RT) attribute. The trust value of nodes is composed by these two attributes after quantification. DT reflects the direct trust evaluation according to the historical interaction. RT reflects the recommendation trust evaluation from the third party nodes.

DT value is based on the history interaction with other nodes and takes effectiveness, stability and time factor into account. DT value expressed as Eq. 1, ***RF(K)*** represents incentive and penalty function, F_{ij} is the stability of node and ***TF(K)*** is the time decay function.

$$DT(i,j)=\frac{\sum_{k=1}^{n}\left(\left(\sum_{k=1}^{n}RF(k)\times F_{ij}\times TF(k)\right)\right)}{\sum_{k=1}^{n}TF(k)} \tag{1}$$

However, the evaluations from nodes to nodes are not all objective. There are defaming acts from some malicious nodes to their neighbor nodes and deliberately higher trust value of some malicious nodes. All of the above are caused by the singleness of the trusted source. In this paper, RT value is computed on the basic of the users collaborative filtering. It can be expressed as shown in Eq. 2, and ***Sim(i,k)*** is used to calculate the similarity.

$$RT(i,j)=\frac{\sum_{k\in N}T_d(k,j)\times Sim(i,k)}{\sum_{k\in N}Sim(i,k)} \tag{2}$$

Both DT and RT are important for certain nodes which could be selectively malicious. By combining these two values we arrive at a more holistic metric called NR. It is a weighted mean of DT and RT as given in Eq. 3, where ω_d=0.7, ω_r=0.3.

$$NR(i,j)=w_d\times DT(i,j)+w_r\times RT(i,j) \tag{3}$$

In the TREC-AODV algorithm, nodes maintain two important lists, such as neighbor nodes trust list and malicious nodes list. Neighbor nodes trust list is used to store all of the neighbor nodes trust values. At the beginning, there is no trust value so that it will be given an initial value, in this paper it is 0.7 (trust threshold value is 0.5). The malicious nodes list is empty initially as well. When trust module found malicious nodes then join it into the list. Malicious nodes in the list will not be taken into account in the routing process, which can reduce the probabilities of malicious nodes breaking down the links.

Routing Algorithm. Initially, we scan all the nodes present in the network by comparing transmission range of a node with transmission range of the network. If a node is moving out of the transmission range of the network during data transmission then we will minimize its energy accordingly. When a node receives a packet, we will check for duplicate packets and status of sequence number in the routing table during rebroadcast RREQ. If it is equal then the node is non-malicious, otherwise we will check its NR values as well as packet transfer rate by this node. Based on this process, behaviors of nodes can be easily identified. Maintenance of routing table and sequence number is same as AODV routing.

Simulation

In this section, we verify the TREC-AODV algorithm by NS2 and make comparisons with AODV and MT-AODV. All results are taken from the experiments in the network environment of black-hole node attacks. In the simulation, there are four performance indexes: malicious nodes isolated rate, packet delivery ratio, average energy consumption and end to end delay.

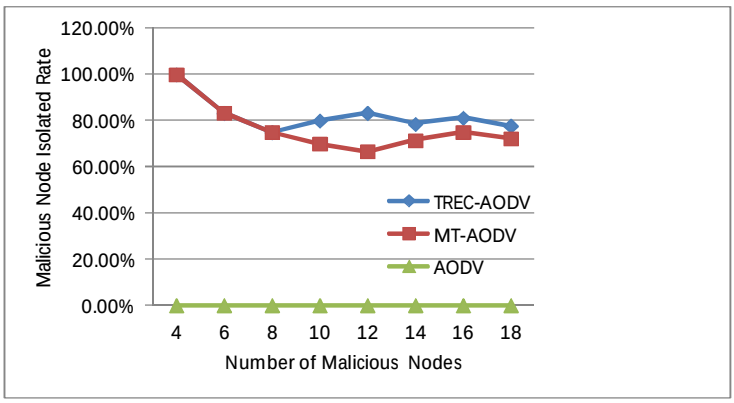

Fig. 1 Malicious node isolated rate of different protocols

In Fig. 1, it is shown that MT-AODV protocol and TREC-AODV algorithm have higher level of malicious node isolated rate and the later even has the level of 80% in average. Because AODV protocol without secure mechanism can't isolate malicious nodes and TREC-AODV algorithm uses the trust recommendation mechanism to isolate malicious node.

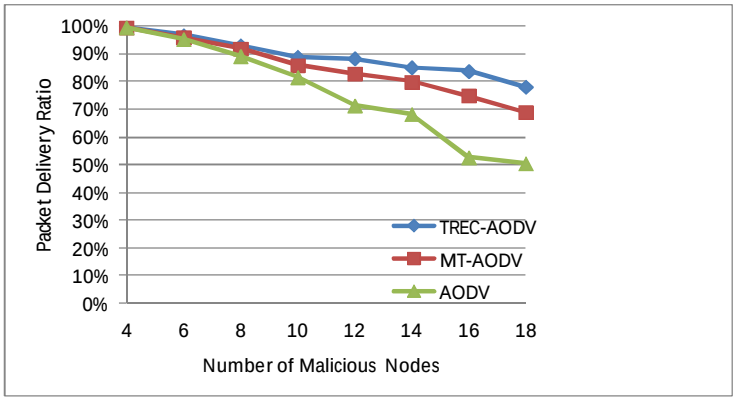

Fig. 2 Packet delivery ratio of different protocols

As shown in Fig. 2, the packet delivery ratio of TREC-AODV algorithm is higher than AODV protocol and MT-AODV protocol. This is because TREC-AODV algorithm can obstruct the malicious node to drop packets by isolating malicious node efficiently.

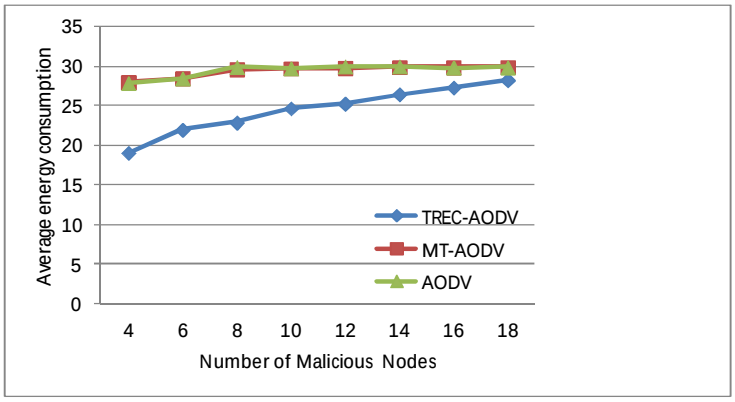

Fig. 3 Average energy consumption of different protocols

In Fig. 3, it is shown that the average energy consumption of TREC-AODV is the lowest. Because of adopting the energy conservation strategy, the average energy consumption of TREC-AODV algorithm, comparing with that of AODV protocol and MT-AODV protocol, can be reduced by 16%.

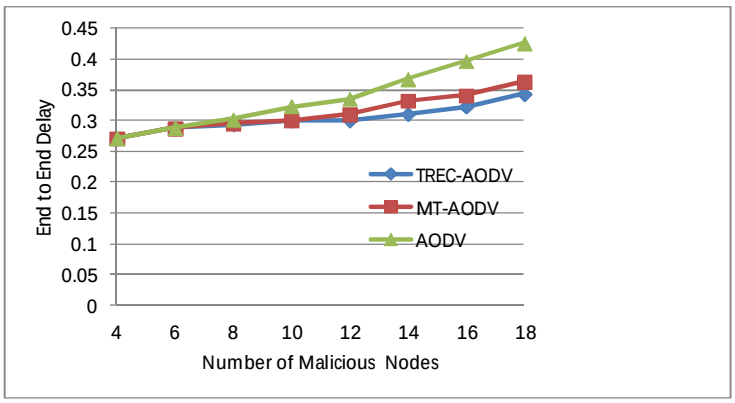

Fig. 4 End to end delay of different protocols

As shown in Fig. 4, the end to end delay of TREC-AODV is approximate to other protocols when there are small amount of malicious nodes. With the increasing number of malicious nodes, the end to end delay of TREC-AODV is lower than the other protocols. It is because that TREC-AODV can obstruct the malicious node to reduce the routing discovery frequency efficiently. Overall, the TREC-AODV has the lowest end to end delay, and it can be reduced by 9% in average comparing with AODV.

Conclusions

In this paper, the Secure and Energy Conservation Routing Algorithm based on Trust Recommendation (TREC-AODV) was designed to resolve the problem of security attack and large energy consumption in Ad Hoc networks. Comparing with original AODV and MT-AODV, the proposed algorithm has a better performance. By adopting the transmission radius adjusting strategy and trust recommendation mechanism, TREC-AODV not only can increase the capacity of energy conservation, but also can detect and isolate malicious nodes to enhance the security of networks.

Acknowledgements

This research was financially supported by the Key Laboratory of Medical Image Computing of Ministry of Education, Northeastern University.

References

[1] Fei Wang, Furong Wang, et al. COSR: A Reputation-Based Secure Route Protocol in MANET[J]. EURASIP Journal on Wireless Communications and Networking, Volume 2010, Vol.7:132-145.

[2] SINGH U., HODA M.N. : A Study of Ad Hoc Wireless Network Routing Based on Various AODV Routing Schemes. Proc. Int. Conf. on Information and Communication Technology (IICT), 26-28 July 2007.

[3] R. Vadivel, V. M. Bhaskaran. Energy efficient with secured reliable routing protocol for mobile ad-hoc networks [J], Procedia Technology, 2012 (4): 703–707.

[4] L. Cao, T. Dahlberg, and Y. Wang. Performance evaluation of energy efficient ad hoc routing protocols in Proc. IEEE Int. Conf. Performance, Comput., Commun., pp. 306-313, April 2007.

[5] Pramod Kumar Singh, Govind Sharma. An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET[C], 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications. 2012: 902-906.

[6] Yin Zhang. The improve routing protocol of AODV based on trust mechanism [D], Guangdong University of Technology in Chinese, 2012.