Journal of Network and Information Security
7 (1), June 2019, 20-24
http://www.publishingindia.com/jnis

Energy Efficient Secure Routing Framework Based on Multidimensional Trust Evaluation for MANET

Renu[1*] and Sanjeev Sharma[2]
[1,2]Rajiv Gandhi Technological University, Bhopal, Madhya Pradesh, India.
Email: renutrivedi@rediffmail.com
*Corresponding Author

Abstract: Very popular MANET works with some functions like data exchange, communication management and routing etc. based on the cooperation. Assess the trustworthiness of the nodes became important since trust is the pillar for cooperation. For secure routing, an efficient trust management mechanism should be implemented in such a way that it could not change the basic nature of network. Mobility, battery limitation and the computational complexities make the trust evaluation a challenging task. To manage the energy during inside attack this paper proposes a trust based energy efficient routing approach, as the extension of our previous work [10] by including various dimensions of trust such as initial trust, behavioral and recommended trust. Most favourite Ad-hoc On-demand Distance Vector (AODV) Routing protocol is used as a representative in the proposed framework. In this paper, a multidimensional trust evaluation security solution is proposed to make minimal changes to the functioning of AODV and achieved an increased level of security and reliability.

Keywords: AODV, Direct trust, Multidimensional trust, Security, Secure Routing, Trust.

I. Introduction

A major challenge in MANETs is to ensure secured routing process. Previously cryptography based schemes are used to protect routing information which is not feasible for real MANETs due to high mobility, heavy computational overhead and malicious node detection where nodes frequently joining and leaving the networks [2]. Power consumption is also a crucial aspect to increase the lifetime of nodes in MANETs. The paper presents energy-efficient and secure routing model in which the most important task is to establish trust between nodes who are neighbors and making a routing path. In this proposal an extra data structure "Trust Table" is used to check trustworthiness of nodes. The table maintains the entry of multiple dimensions of trust; Initial trust, direct trust and recommended trust. The initial trust value is found from the overall royalty in terms of battery and distance of the nodes, behavioral trust is obtained using previous direct interactions between the evaluating and evaluated WN, and the recommend trust value is asked from the recommending nodes based on its behavior in a network as perceived by evaluating nodes in the network. Final trust value is used to forward the packet by maintaining a trust value for each neighbour node to choose the optimized path between two nodes.

The rest of the paper is arranged as follows: Section II presents all related work on trust based routing protocols for MANETs. Section III describes the aim and objective of proposed work and Section IV describes the multidimensional trust based routing protocols for MANETs. NS2 simulator is used to highlight the benefits of multidimensional trust based AODV and at last Section VI concludes the paper.

II. Literature Survey

All previous work was based on the assumption that all nodes in the network are trustworthy and cooperative during the routing process. This assumption open the door for vulnerability [1] in the routing protocols. As explained earlier, the nodes are not so powerful in terms of resources and infrastructure. These constraints restrict the use of cryptographic algorithms. Because cryptosystems need to be executed with high processing, storage and power consumption. Although crypto based schemes are proposed to protect routing information from being tinkered by the adversary, such an approach may not be practical for real MANETs. Jared Cordasco *et al.* [2] presented comparison between Cryptographic and Trust-based Methods for MANET Routing Security. In [3] [4] [23], several potential problems including node compromise, computational overload attacks and energy consumption attacks were presented. Some work was contributed on "lightweight" security mechanisms using trust by [11, 12, 13, 14, 15, 22], They provide general ideas for trust evaluation in networks by applying different approaches. Wang and Varadharajan [21] present a trust evaluating approach

to unfamiliar peers which calculates the probability of achieving a successful transaction according to the feed backs given by other nodes. The simplest form of computing reputation scores is simply to sum the number of positive ratings and negative ratings separately, and to keep a total score as the positive score minus the negative score. Some researchers Pirzada and McDonald [19] proposed a trust model to establish trust in pure MANETs. The trust computation is based on monitoring data delivery in the network. Yan, Zhang and Virtanen [18] proposed a trust model for secure routing evaluation in MANET. The authors defined a large trust evaluation matrix based on statistic data collected during the network communication. Virendra, *et al.* [9, 12] proposed a pair-wise trust evaluation scheme in MANETs. In [20] Arvind Sharma and Dr. Neeraj Kumar. propose a new way to compute trust relationship to identifying malicious nodes in MANETs. Trust based mechanism includes the notion of friends, acquaintances and strangers. These algorithms/protocols are not suitable for MANET having limited resources like battery power, storage capacity and processing capacity. Xia *et al.* [13] proposed *A light-weight trust-enhanced routing protocol (TeAOMDV)* to get two-way trusted route by general monitoring information to get the trust value.

III. Motivation and Objective of Proposed Work

We identified some work by Yan, Zhang and Virtanen [18] in the literature moving in multi criteria trust evaluation. Additionally, we found that *energy* is also an important component for the overall performance of the network. As a part of the literature survey, we observe that integration of different dimension of trust in the composition of a trust metric would improve the performance of a trust-based scheme. Considering all these fact into the account we modify our previous trust-based routing scheme [22]. In our previous work, we proposed trust based security model to identify misbehavior of the node by comparing the value threshold, However, this model was based single trust evaluation dimension to quantify and predict reliability among nodes. This single measure is not enough satisfactory in case of selfish behavior, malicious intent, limited resources and physical failures of dynamic MANETs. In addition, we suggest modifications in the route discovery, trust update and trust recommendation procedures.

IV. Proposed Work

Trust Evaluation and management consider three major components knowledge about current resources, experience with that particular and the recommended value obtained from others. The paper moved forward by considering these component as Fig. 1, where each dimension has its defined metrics.

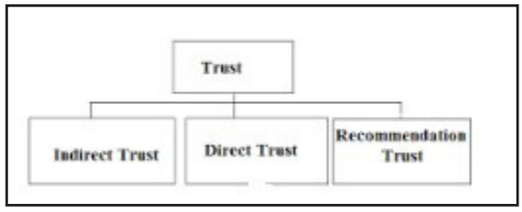

Fig. 1: Various Dimensions of Trust to Achieve Secure Routing

The trust grading scheme recorded the nodes' level of trustworthiness using three sub modules. As shown in Fig. 2, nodes are distributed in given area, each node runs with an energy observer, honesty calculator in terms of success full packet delivered, distance estimator. All nodes are associated with trust supervisor. Energy observer will calculate remaining energy of neighbour nodes, Distance watcher will maintain distance between nodes. Trust table will keep entries of trust level for neighbouring nodes to forward the packet.

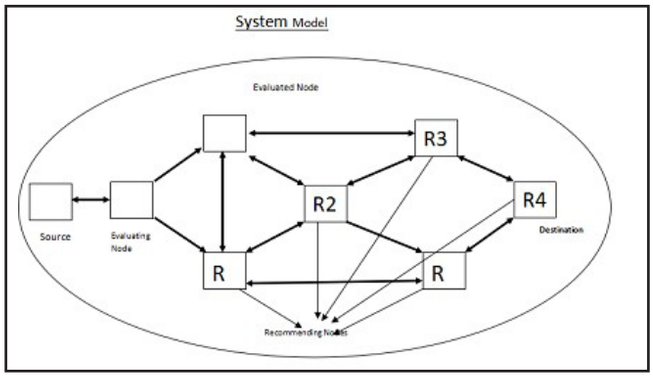

Fig. 2: System Model

In trust based scheme, each node needs to record trust value of its neighbor nodes in a special data structure called "Trust Table" having multiple behavior attributes.

Trust Management Model: (Trust Calculation of Neighbour): The total trust value is computed based on the multiple attributes associated with direct, Behavioral and Recommended Trusts. Direct trust is based on the current battery power, distance and computing power. Behavioral value is attained from immediate one hope nodes reflected regularly in the trust database. The updated trust value is forwarded to all other nodes. Now either these three components individually or a combination of them can be used in computing the trust. Some nodes may or may not already know each other before they join the network. Besides the direct interaction experience in the network, the pre-shared knowledge, if any, is also quite important for a node to implement trust evaluation and should be taken into account in a trust model.

Total Trust: The total trust is computed from IT, BT and RT. The total trust will be useful in upgrading or degrading the trust

value. Proposed scheme consist of the following sub modules:

- Initial Trust Computation
- Behavioral Trust Computation
- Recommended Trust Manager

i) Initial Trust Computation: For calculating initial trust value three factors will be considered that are Battery percentage and distance. Hence initial trust can be calculated based upon aggregation of these factors.

Algorithm for Initial Trust Computation for the Neighbors

1. *Request Battery Percentage:*

To send a message of k-bit with a distance of d, energy consumption can be calculated by Et = Ee(k, d) + Ea(k, d).

➢ Start

If Et is higher than a threshold
Then
T=Th, (high trust value)
Else
If Et is lower than a threshold
Then
T=Th, (low trust value)
Hence trust value is proportional to Battery percentage.

2. *Compute the Distance:*

This component will keep track of distance between nodes.

➢ Start

If D between evaluated node and subject node is less than a threshold

Then
T=Th, (high trust value)
Else
if distance between subject node and evaluated node is high,
Then
T=Tl, (low trust value)

Hence trust value is inversely proportional to distance between nodes.

Send T values from step 1 and 2 for getting Initial trust value.

Finally the aggregated value will go to Trust Calculation Module.

ii) Behavioral Trust Computation: The behavior trust is retrieved by direct association and experience of one node to another node. The constant for calculating behavior trust can be mentioned by *Honest delivery ratio and History interaction count.*

Algorithm

1. *Honest Delivery Ratio:*
If HDR is higher than a threshold
Then
T=Th, (high trust value)
Else
If HDR is lower than a threshold
Then
T=Th, (low trust value)
Hence trust value is proportional to HDR.

2. *Compute History Interaction Count:*

➢ Start

If HIC between evaluated node and subject node is very frequent
Then
T=Th, (high trust value)
Else
if HIC between subject node and evaluated node is less,
Then
T=Tl, (low trust value)
Hence trust value is inversely proportional to distance between nodes.
Honest delivery ratio

Send T values from step 1 and 2 for getting behavioral trust.

Finally the aggregated value will go to Trust Calculation Module for processing.

iii) Manager: The Recommendation Trust RT is obtained from the common neighbors of any two neighboring nodes. All the common neighbors will share their trust value or judgment about a specific node to compute the RT as shown in the Fig. 3.

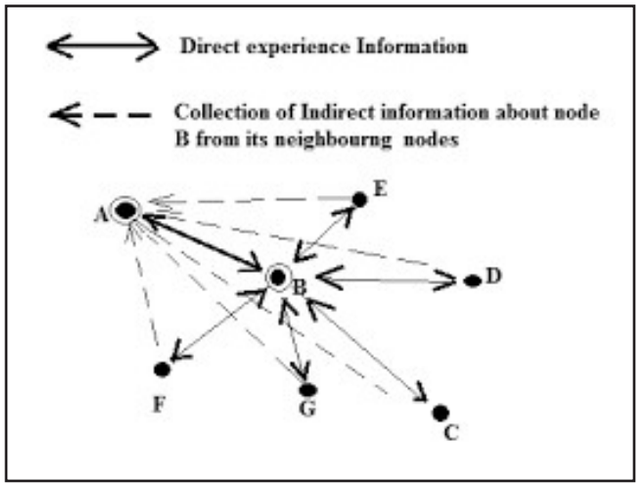

Fig. 3: Recommended Trust Computation

Algorithm

1. For all Recommendation Request Do.
2. Request to all one hope neighbours.
3. Disseminate Recommendation replies Rm, where Rm is Recommendation sent by node m.
4. Construct the Recommendation list L={R1, R2,R3,...,Rn}.
5. Send L to the Indirect Trust Calculation Module for processing.
6. Receive the Recommendation Trust value.
7. Compute the final RT by adding all received values.

V. Result and Comparison

In this paper ns2 is used to perform simulations. Parameter are given in Table I, total area size of 1000x1000m2 with 70 randomly distributed nodes in the MANET'S. The simulation work for 100s time.

Table I: Parameters

Parameter	Value
Simulator	NS-2
No of Nodes	150-200
Mobility	60m/s
Pause Time	2sec
Pkt size	512 bytes
Pkt Rate	4pkt/sec

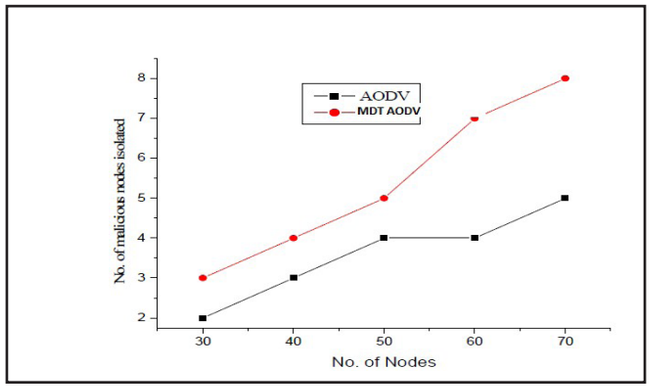

Fig. 4: Malicious Node Detected in Both the Routing Algorithms

Based on the trust based routing, the algo can obtain better results than adhoc on demand routing protocol which is shown in Fig. 4 and 5. In MD trust based approach packet drop ratio will be reduced and packet delivery ratio will be increased as in the below Table II.

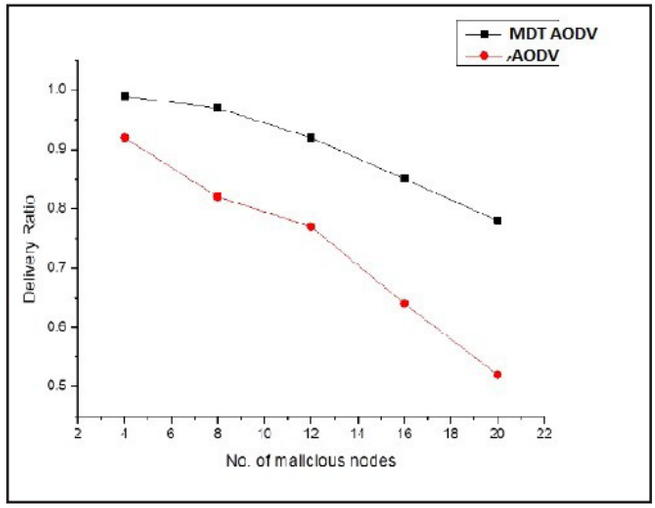

Fig. 5: No of Packet Drop in Both the Routing Algorithms

Table II: Comparison Between AODV and Proposed Multidimensional Trust Based AODV

Parameters	AODV	MDT AODV
Routing	Reactive	Reactive
Throughput	Low	High
Energy overhead	High	Low
PDR	Low	High
Security	low	High

VI. Conclusion

A multi attribute based trust evaluation framework is proposed as an extension of simple AODV to select the most secure route to manage the characteristics of MANET. The presented work included various dimensions of trust such as direct trust, behavioral and recommendation trust with the intention to fill the gap of dishonest recommendation for neighbours and energy efficiency which was not yet covered. We took a simulation scenario with different parameters and applied direct, indirect and TP, the cumulative values can be obtained to choose a next node. Proposed scheme is *Attack-tolerant, Cooperative*, *Flexible*, *Lightweight and Scalable as well as Compatible* to the rapidly growing network size. In this model no need of authentication mechanism. There is low possibility of false recommendation attack. It also requires less battery consumption.

References

[1] N. Pissinou, T. Ghosh, and K. Makki, "Collaborative trust-based secure routing in multihop ad hoc net-

works," in Networking 2004. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications, 2004.

[2] J. Cordasco, and S. Wetzel, "Cryptographic versus trust-based methods for MANET routing security," *Electronic Notes in Theoretical Computer Science*, vol. 197, no. 2, pp. 131-140, 2008.

[3] R. Mishra, S. Sharma, and R. Agrawal, "Vulnerabilities and security for ad-hoc networks," in *Proceedings of the IEEE International Conference on Networking and Information Technology*, pp. 192-196, April 2010.

[4] H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," *IEEE Communications Magazine*, vol. 40, no. 10, pp. 70-75, 2002.

[5] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shield, and E. M. Belding-Royar, "A secure routing protocol for ad hoc networks," in *Proceedings of ICNP'02*, 2002.

[6] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," *IEEE Wireless Communications*, IEEE, vol. 14, no. 5, pp. 85-91, 2007.

[7] M. G. Zapata, and N. Asokan, "Securing ad hoc routing protocols," in *Proceedings of the ACM Workshop on Wireless Security (WiSE'02)*, ACM Press, 2002.

[8] L. Zhou, and Z. J. Haas, "Securing ad hoc networks," *IEEE Network*, vol. 13, no. 6, pp. 24-30, 1999.

[9] K. Meka, M. Virendra, and S. Upadhyaya, "Trust based routing decisions in mobile ad-hoc networks," in *Proceedings of the Workshop on Secure Knowledge Management (SKM'2006),* 2006.

[10] R. Mishra, I. Kaur, and S. Sharma, "New trust based security method for mobile ad-hoc networks," *International Journal of Computer Science and Security (IJCSS),* vol. 4, no. 3, pp. 346-351, June-July 2010.

[11] X. Li, M. R. Lyu, and J. Liu, "A trust model based routing protocol for secure ad hoc networks," in *Proceedings of the IEEE Aerospace Conference (IEEEAC)*, pp. 1286-1295, 2004.

[12] M. Virendra, M. Jadliwala, M. Chandrasekaran, and S. Upadhyaya, "Quantifying trust in ad-hoc networks," in *Proceedings of the IEEE International Conference on Integration of Knowledge Intensive Multi-Agent Systems (KIMAS)*, pp. 65-71, 2005.

[13] M. G. Zapata, and N. Asokan, "Securing ad hoc routing protocol," in *Proceedings of the 3rd ACM Workshop on Wireless Security*, pp. 1-10, 2002.

[14] 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.

[15] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc network," in *Proceedings of the 6th Annual conference on Mobile Computing and Networking*, pp. 255-265, 2000.

[16] Z. Liu, A. W. Joy, and R. A. Thompson, "A dynamic trust model for mobile ad hoc networks," in *Proceedings of the 10th IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS),* pp. 80-85, 2004.

[17] L. Eschenuer, V. D. Gligor, and J. Baras, "On trust establishment in mobile ad-hoc networks," *Security Protocols: 10th International Workshop*, pp. 47-62, 2002.

[18] Z. Yan, P. Zhang, and T. Virtanen, "Trust evaluation based security solution in ad hoc networks," 2011.

[19] A. A. Pirzada, and C. McDonald, "Trusted route discovery with TORA protocol," in *Proceedings of the Second Annual Conference on Communication Networks and Services Research (CNSR'04)*, IEEE, 2004.

[20] A. Sharma, and N. Kumar, "Trust based theoretical framework for mobile ad-hoc networks," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 6, pp. 905-909, 2013.

[21] Y. Wang, and V. Varadharajan, "Trust2: Developing trust in peer-to-peer environments," in *Proceedings of the IEEE International Conference on Services Computing*," IEEE, vol. 1, pp. 24-31, 2005. DOI: 10.1109/SCC.2005.104

[22] M. S. Khan, M. I. Khan, S.-U.-R. Malik, O. Khalid, M. Azim, and N. Javaid, "MATF: A multi-attribute trust framework for MANETs," *EURASIP Journal on Wireless Communications and Networking*, vol. 2016, no. 1, p. 1, 2016.

[23] S. Saxena, G. Sanyal, S. Srivastava, and R. Amin, "Preventing from cross-VM side-channel attack using new replacement method," *Wireless Personal Communications*, vol. 97, no. 3, pp. 4827-4854, 2017. DOI: 10.1007/s11277-017-4753-7

[24] Z. Yan, P. Zhang, and T. Virtanen, "Trust evaluation based security solution in ad hoc networks," in *Proceedings of the Seventh Nordic Workshop on Secure IT Systems 2003*, Norway, 2003.