International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

Dempstershafer Theory and Encounter Based Trust Routing in Mobile Ad Hoc Network

S.G. Rameshkumar

Abstract*: Mobile Ad hoc Network (MANET) is a particularly disputed network because of its particular features, for example, active topography, decentralization, as well as neighbor depend routing. In MANET, any mobile nodes can connect or disappear arbitrarily; thus, mobile nodes cannot awake which node is it joined with, and this creates resources been dealt between unknown nodes that can be trusted or not. As a result, without any trustworthiness makes the main susceptibility in security concerned aspects of the MANET. In this situation, trust value employs a vital function in all network performance. This paper introduces DempsterShafer theory and Encounter based Trust Routing (DETR) in a MANET. In this scheme, the direct trust and indirect trust is used to compute the mobile node trust. The node cooperation and encounter rate parameters measure the node direct trust in the network. The node indirect trust is computed based on the neighbour node opinion using DempsterShafer theory. Simulation results demonstrate that DETR detecting untrustable nodes in the network.

Keywords*: DempsterShafer theory, Direct Trust, Encounter Rate, Indirect Trust, MANET.

I. INTRODUCTION

This MANET is a wireless network with lacking fixed infrastructure and contains numerous mobile nodes that depend on each other to continue the associated network. The mobile nodes have left the network lacking no limits; hence, networks topologies are dynamic. Military field emergency and tragedy situation need instant network configuration and confidential route concern for their transmission [1].

Generally, conventional MANET schemes are intended concentrating on the performance as well as efficiency [4]. Applying cryptography and authentication protocol have been proposed to make sure attributes, for example, integrity, confidentiality, etc. Though, those protocols necessitate a centralized third party, building them unfeasible for MANETs. Additionally, secure routing mechanisms cannot avoid malevolent or compromised nodes that are certified participants to the network since making any mischief. Consequently, the idea of trust is enclosed in to a calculating system to determine a probability or doubtfulness that an individual concerning another's a prospect performance for a confident action [5].

In this proposed model, direct trust as well as indirect trust is computing the node trust worth. Direct trust is computed by the cooperation rate and encounter rate. The neighbour node opinion is calculating the indirect trust using the Dempster Shafer theory. This trust value-based select the route provides better throughput efficiency and detect the untrustworthy nodes.

The remainder of the article is prepared as follows. Part 2 talks about related work. Part 3 establishes a DempsterShafer Theory and Encounter based Trust Routing in MANET. Part 4 presents a Simulation Analysis. Part 5 summarizes our conclusion.

II. RELATED WORKS

Generally, compute the trust value between anonymous nodes. Recommendation, observation, reputation, knowledge and context were utilized to measure the trust value [13]. The outcome received from the computation is then represented with the access rights to decide the action necessary [8]. Trust-Based Secure Routing provides better data transmission. The cooperative transmission is depending on the route choice-value designed for every route request path. It is helpful for upcoming transmission in the network. This scheme enhances network security and avoids a malevolent node attack in the network [2].

A hybrid trust management framework (HTMF) that combines the parameters of trust concern frame works and reputation-based frameworks and while removing the problems connected with each of the two classifications of frameworks [6]. A dynamic trust organization method is used to supervising the nodes' behaviors as well as measuring their trust values. This mechanism applies a hash algorithm for yielding recognizes labels for nodes to differentiate outside attackers from normal nodes in the network [7].

Reputation systems employ evaluations for estimating the reliability based on nodes behaviour in MANETs [9].On-demand secure routing scheme (ODSR) [3] detects malicious associations based on node authentication. However, it cannot check the node behavior in the network. Improved TWO Acknowledgement methods[10-11] that obviously sends a two-hop acknowledgement to confirm node collaboration. A cross layer frame work is introduced to better data distribution and elastic traffic in multi hop wireless network [12-13].

Manuscript published on January 30, 2020.
* Correspondence Author
S.G. Rameshkumar*, is working as Assistant Professor in the Department of Electrical Engineering at FEAT, Annamalai University, Chidambaram. Tamilnadu, India. Email: umamaheswari.phd6@gmail.com

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

III. DEMPSTERSHAFER THEORY AND ENCOUNTER BASED TRUST ROUTING IN MANET

The trust denotes to the impression that one node holds about another, depend on history experiences, awareness of entity behavior and/or suggestions from reliable entities. In this scheme, the trust worth is computed by direct trust and indirect trust. The source node C evaluates the node D direct trust based on the node cooperation rate and encounter rate. The cooperation rate (C_R) computation is given below.

$$C_R = \frac{F_R}{F_R + D_R} \quad (1)$$

Where, F_R represents the rate of mobile node D sending the data packet to the mobile node C and D_R represents the rate of dropped the packet to the mobile node C. Therefore the greater worth of C_R represents that the nodes can regularly react to the route request of its vicinity node. As a result, the possibility of drop of packets is fewer. From this worth, we can moreover notice the UN trusted nodes. In MANET, node mobility is an important factor because of high mobility nodes easily disconnected to the near node. As a result, less mobility nodes provide well communication in the network. Encounter Rate represents the set of new mobile node B qualified during time period T from it to (ti+1).

$$ER_D = \frac{|E_D|}{T} \quad (2)$$

Here $|E_D|$ denotes the number of the set E_B. The lowest value of ER_D represents the better trust node in the network. Direct trust computation is given below. Where, α and β represents the weight factor among 0 to1.

$$DT = (\alpha * C_R) + (\beta * ER_B) \quad (3)$$

This scheme evaluates the routing node indirect trust based on probability of neighbour node opinion. This is computed by DempsterShafertheory. It deals with uncertain knowledge. It aggregates confirmation from different sources and gets at a degree of opinion that takes into account all the presented confirmation. Every feasible jointly special actions of the same kind are counted in the frame of judgment **λ**. For example, mobile node C gives its judgment on mobile node D by allotting opinion over **λ**.This allotment function is called as the Mass Function mf: $2^{\lambda} \rightarrow [0, 1]$ of the mobile node i, indicated by m_C. The mobile node C notice, the probability that the mobile node D is trusted is suggested by an assurance interval[opinion(T), Possibility(T)]. Where,

$$\sum mf(\mathrm{A}) \mid A \subseteq \lambda = 1, mf(\phi) = 0 \quad (4)$$

The opinion task that confirms the mobile node Dis a Trustedis specified as:

$$Opinion(\mathrm{T}) = \sum \mathrm{A} \subseteq Tm(\mathrm{A}) \quad (5)$$

Possibility assurance that reports for every the notice that does not reject the given a suggestion:

$$Possibility(\mathrm{T}) = 1 - \sum \mathrm{A} \subseteq T = \phi m(\mathrm{A}) \quad (6)$$

For every probable suggestion tell Trusted the DempsterShafe rule of compounding is useful to join mobile node *C* observations m_C and node *D* observation m_D.

$$m1 \oplus m2(\mathrm{T}) = \frac{\sum_{A \cap \mathrm{A}_{k'} = A} m_C(\mathrm{A}_k) * m_D(\mathrm{A}_{k'})}{\sum_{A \cap \mathrm{A}_{k'} = \phi} m_C(\mathrm{A}_k) * m_D(\mathrm{A}_{k'})} \quad (7)$$

The direct trust the weight factor is allotted for cooperation rate and encounter rate. Similarly, the weights are allotted for computing indirect trust (IT).

$$IT = \frac{\sum_{A \cap \mathrm{A}_{k'} = A} [\alpha m_C(\mathrm{A}_k) * \beta m_D(\mathrm{A}_{k'})]}{\sum_{A \cap \mathrm{A}_{k'} = \phi} [\alpha m_C(\mathrm{A}_k) * \beta m_D(\mathrm{A}_{k'})]} \quad (8)$$

Finally, the complete trust is calculated by aggregating direct trust, and indirect trust formula is given below.

$$CT = DT + IT \quad (9)$$

During route discovery, the source node checks every complete node trust then the highest complete trust value node is selected as the route node. This working function follows until the source reaches the destination. Thus, the source sends the data via trustable nodes in the network.

IV. RESULTS AND DISCUSSION

In this scheme, the result evaluation is carried out using the network simulator -ns2.35. Here, we arbitrarily positioned 50 mobile nodes in the region 500m×500m. The random way-point mobility model is utilized for the node movement process. Constant Bit Rate is used for handling the traffic model. The Omni-directional transmitter is utilized for obtaining the signals from entire ways.The act of DETR is analyzed by using parameters Average Delay (AD), and throughput.

A. Average Delay(AD):

The AD represents the time distinction among packets sent and packets received. It is measured by Equation 10. Fig.1. shows the AD analysis of DETRand ODSR mechanisms.

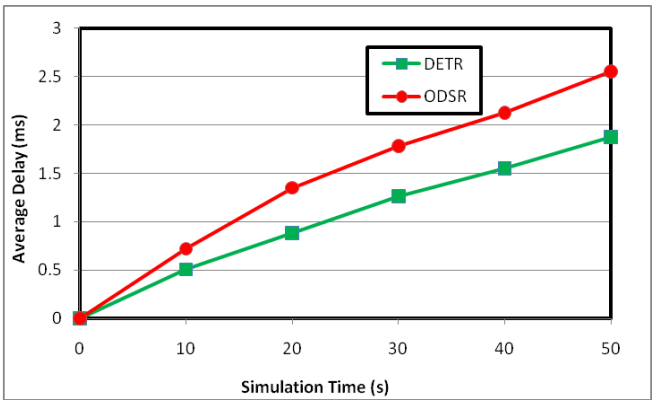

Fig. 1. Average delay of DETR and ODSR

$$\text{Average Delay}=\frac{\sum_0^n(\text{Packet Received Time-Packet Sent Time})}{n}$$

. Where, n represents the count of nodes. It reveals DETR has 36% lower delay for a node when compared to the ODSR mechanism Because of it transmits the data via trustable node.

B. Throughput:

Throughput represents the data packets successfully delivered across network per unit time. Throughput is obtained using Equation 11.

$$\text{Throughput}=\frac{\sum_0^n\text{Packets Received(n)} * \text{Packet size}}{\text{Time}}$$

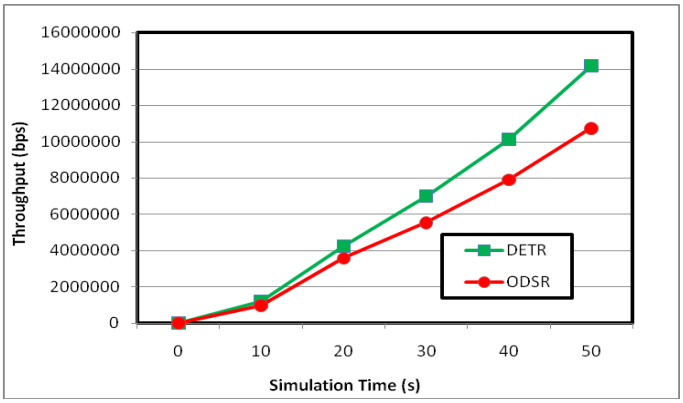

Fig. 2.Throughput of DETR and ODSR

Fig. 2. indicates the throughput analysis for DETR and ODSR mechanisms. It can be observed from Figure 2 amount of packets obtained effectively for each 1000 packets. Here, DETR is 24.17% better than the ODSR mechanism.

V. CONCLUSION

In In this paper, we introduced the Dempstershafer theory as well as Encounter based Trust Routing among anonymous nodes in the network. In this mechanism, the node trust is computed based on direct and indirect trust. These trust worth is used to compute the mobile node trust. The node cooperation and encounter rate parameters measure the node direct trust in the network. The node indirect trust is computed based on the neighbour node opinion using DempsterShafer theory. Simulation results demonstrate that DETR provides better throughput and minimizing network delay in the network.

REFERENCES

1. J.H. Cho, A. Swami, and R.Chen, "A survey on trust management for mobile ad hoc networks", *IEEE Communications Surveys & Tutorials*, vol.13, No. 4, 2010, pp. 562-583.
2. R. Li, J. Li, P. Liu, and J.Kato, "A novel hybrid trust management framework for MANETs," *IEEE International Conference on Distributed Computing Systems Workshops*, 2009, pp. 251-256.
3. B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks," *ACM Transactions on Information System Security*, Vol. 10, No. 4, 2008, pp.11–35.
4. K.S. Ramana, A.A. Chari, and N. Kasiviswanth, "Trust-based security routing in mobile ad-hoc networks", *International Journal on Computer Science and Engineering*, Vol. 2, No. 2, 2010, pp. 259-263.
5. H.S. Jassim, S. Yussof, T.S. Kiong,. S.P. Koh, and R. Ismail, " A Routing Protocol based on Trusted and shortest Path selection for Mobile Ad hoc Network", IEEE *9th Malaysia International Conference on Communications* , 2009, pp. 547-554.
6. R.S. Mangrulkar, and M. Atique, "Trust-based secured ad-hoc On-demand Distance Vector Routing protocol for mobile ad-hoc network", *Sixth International conference on Wireless Communication and Sensor Networks*, 2010, pp. 1-4.
7. W. Luo, W. Ma, and Q. Gao, "A dynamic trust management system for wireless sensor networks", *Security and Communication Networks*, Vol. 9, No. 7, 2016, pp. 613-621.
8. R.R. Sahoo, M. Singh, B. M. Sahoo, K. Majumder, S. Ray, and S. Sarkar, " A lightweight trust-based secure and energy-efficient clustering in wireless sensor network", *honey bee mating intelligence approach. Procedia Technology*, Vol. 10, 2013, pp. 515-523.
9. S. Ganeriwal, L. Balzano, and M. Srivastava "Reputation-based framework for high integrity sensor networks", *ACM Transctions on Sensor Networks*, Vol. 4, No. 3, 2008, pp. 1–37.
10. K. Liu, J. Deng, P. Varshney, and K. Balakrishnan, "An acknowledgment based approach for the detection of routing misbehavior in manets", *IEEE Transactions on Mobile Computing*, Vol. 6, No.5, 2007, pp.536–550.
11. K. Balaji, "Design and Analysis of Increasing throughput and minimising gross layer operations in IEEE 802.11 WLAN", *International Research Journal of Engineering and Technology*, 2016.
12. K. Balaji, "A frame work for integrated routing, scheduling and Traffic Management in MANET", *International Research Journal of Engineering and Technology*, Vol. 2, No. 9, 2015, pp. 2337-2344.
13. T.A. Shanmugasundaram, V. Vijayabaskar, "A novel approach for energy efficient clustering in heterogeneous w ireless sensor networks", *ARPN Journal of Engineering and Applied Sciences*, Vol. 10, No. 5, 2015, pp. 2172-2176.

AUTHORS PROFILE

S.G. Rameshkumar is working as Assistant Professor in the Department of Electrical Engineering at FEAT, Annamalai University, Chidambaram. He obtained his PG degree from Coimbatore Institute of Technology. Currently he is doing research in the area of wireless sensor networks. He is having 16 years of experience in teaching and research.