An Efficient Trust and Energy Aware Protocol Using TAODV-ACO in MANETs

Ambidi Naveena(✉) and Katta Rama Linga Reddy

Electronics and Telematics Department,
G.Narayanamma Institute of Technology and Science, Hyderabad, India
ambidinaveena@yahoo.com, kattareddy2000@yahoo.com

Abstract. Mobile Ad-Hoc Network (MANET) is a relationship of the mobile nodes with constrained transmission range and asset with no fixed infrastructure. But, malicious attack of node reduce the trust-level nodes that lead to insecure in delivering data. The increments in attacks cause extreme energy consumption that tends to a decrease in network-lifetime. The security and routing issues are concentrated by introducing trust aware ad-hoc protocols. In this research proposal, Trust-Aware ad-hoc Routing (T2AR) with Ant Colony Optimization (ACO) is used for maximizing the trust level based on trust-rate, energy, mobility based malicious behavior prediction. Ad-hoc On-Demand Distance Vector (AODV) uses two processes to find and maintain routes: the route detection process and the route maintenance. Hence, the T2AR-AODV-ACO methodology precisely transmits data from source to destination (S-D) by executing better throughput, routing overhead, end-to-end delay and energy consumption in trust aware ad-hoc routing.

Keywords: Ad-hoc On Demand Distance Vector · Ant Colony Optimization · Mobile Ad-Hoc Network · Trust-Aware ad-hoc Routing

1 Introduction

Trust management for MANET has risen as dynamic research region, which is appeared by the expansion of trust protocol to help mobile gathering based applications lately [1]. The social trust came from the communication network to get a composite trust metrics as a reason for evaluating trust of mobile nodes in MANETs [2]. The interruption location and reaction on the reliability of a Cyber-Physical System (CPS) including sensors, actuators, control units and physical objects for controlling and securing a physical foundation are major drawbacks in Trust-based MANETs [3].

A dependable Routing Protocol (RP) for improved reliability, quality and security of communication in portable adhoc networks and sensor systems are utilized for level calculation for finding the best route between nodes [4]. The distributed mobile nodes incorporated with the ad-hoc mobile network in such a way it prevent and identify best route and misbehaving nodes while transmitting data packets to destination [5]. The Payload based mutual authentication (PAWN) performs on optimal percentage of cluster heads election, authentication and allows to communicate with nearby nodes using cluster head based tokens for limiting the energy consumption [6].

S. Balaji et al. (Eds.): ICICV 2019, LNDECT 33, pp. 591–598, 2020.
https://doi.org/10.1007/978-3-030-28364-3_60

A Sybil attack recognizable scheme for a cluster based hierarchical network mainly organized to check and detect forest fires. However, if one or more identities of a Sybil node moves via. the detection procedure, they eventually detect the packet loss and malicious nodes in the networks [7]. A data gathering system called MAMS where Mobile Agents (MAs) and a Mobile Server (MS) agreeably assemble data. MAs gather information over the WSN and restore this to the MS [8]. A quick occasion distinguishing calculation named RENDEZVOUS quicken the on-screen character's discovery procedure while keeping the vitality utilization of sensor nodes to a base [9]. The advancement of trust instruments, gives a short summary of traditional trust procedures and underline the difficulties of trust scheme in WSNs. The trust esteem transmission and evaluation perform low in reducing the energy consumption [10].

To overcome this problem, T2AR-AODV-ACO energy-model based evaluation of trust scheme is presented in this paper. The AODV organize the sequential information for the neighbor log-collection. The lack of positional updates during the mobility of nodes is not effective, hence the optimization techniques is used in the paper. The curiosity shows in T2AR is in the usage of immediate and indirect trust observation schemes on neighbor-log results and trust affirmation by methods sequence ID planning. The execution of the proposed methodology evaluated in terms of end-to-end delay, energy consumption, routing overhead and throughput.

The remaining paper is presented as follows: Sect. 2, a brief description about related works. Section 3, presents a review on "Trust aware ad-hoc RP along with ACO" Methodology consists of neighbor estimation, trust update and distance calculation using RSSI techniques in MANETs. Section 4, demonstrated the simulation-parameters and Experimental results of the "Trust aware ad-hoc RP" and Sect. 5 designates the conclusion of this research work.

2 Related Work

Yan and Wang [11] proposed a structure for the Attribute based encryption (ABE) model to help information get to checking of the individual portable nodes. The worked of trust display dependent on the suggestion is the testing assignment due to attackers and packet loss in networks.

Saha and Mitra [12] implemented a new trust based on demand RP that can be modified to the individual energy surrounding of the nodes in a MANET. The selection of the secure and reliable node helps in detecting and reducing wormhole and rushing attack, which is different based on the packet drops. The working process of system model is complicated, and this increased the delay in the network.

Bijon et al. [13] presented a trust based packets sharing model in the MANET based on the existence of uncertainty. The multiple recommendations techniques reduce traffic, successfully reflect uncertainty, and adapts human-like behavior. The extra time required for the signal recommendation and also it is difficult to propagate recommendation in the opposite direction.

Shabut et al. [14] presented an energy aware and social trust inspired multidimensional trust management models, which was executed to accomplish Quality of Services (QoS) parameters by overcoming ad-hoc network challenges. The specific routing method does not use the routing process in a network, hence it provided less throughput and increased the delay of the node.

Patel et al. [15] introduced the trust value based algorithm to identify and defense gray-hole attack by clustering technique. The trust management model computes the trust rate of the wireless nodes through peer-to-peer and link evaluation in Trust ad-hoc networks. The trust value calculation didn't achieve better efficiency in this work.

3 Ad-Hoc RP Based on Trust Aware Using AODV-ACO

In this research work, the T2AR protocol is implemented for improving the node's trust-level in an environment of MANETs. For the most part, the proposed method optimizes the functions of AODV route reply and request directing calculation with the limitations of trust-rate, energy, portability based false/malicious activities in network.

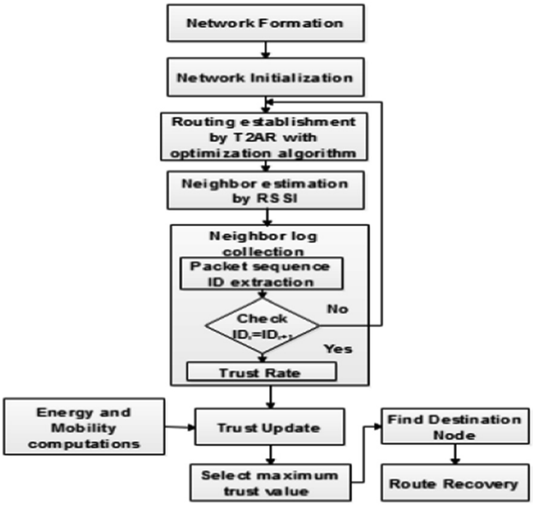
Network Formation
Network Initialization
Routing establishment by T2AR with optimization algorithm
Neighbor estimation by RSSI
Neighbor log collection
Packet sequence ID extraction
Check $ID_i=ID_{i+1}$
No
Yes
Trust Rate
Energy and Mobility computations
Trust Update
Select maximum trust value
Find Destination Node
Route Recovery

Fig. 1. Overview of the proposed work

The trust value is surveyed through the crossover estimations of the energy, mobility and achievement rate of the packet delivery. The over-all flow diagram of the proposed technique is presented in Fig. 1. The working principle of the T2AR-AODV-ACO methodology is described in the below five steps.

1. The neighbor detecting and route maintenance rely upon the log gathering from the nodes, which give the proper trust rate values. Further, the trust rate is every so often refreshed via the locational information to update the security-level of the nodes.
2. The routing establishment developed by using T2AR with ACO optimization algorithms.
3. The use of immediate or indirect perception procedures followed by the grouping ID coordinating to expand the trust-level.

3.1 Trust Model in the Networks

In this section, T2AR-AODV-ACO trust model is explained briefly. The fundamental objective of the model is to give joined solutions for determining the best routing path and energy of packets sent. The trust display how to figure the trust of the routing path by utilizing the trust estimation of each and every nodes. The trust display makes the communication among trust calculation and network statistics. The primary commitment is to determine solutions to the uniform energy consumption for every one of the nodes to build and arrange its lifetime. The trust architecture comprises of two phases: trust advancement and trust calculation for routing process. In trust arrangement of action arrange, each node gathers the network measurements like packet sent, and data packet dropped, etc., in light of which trust of a node is resolved. The requested routing-path comprises the node as an intermediary node, though the gathering of statistics is calculated continuously. Once the route/way from S-D is demanded, all the intermediate nodes determine their trust rated values [17].

3.2 Trust Based AODV RP in Ad-Hoc Networks

The incorporation of trust model show with AODV calculation is done so as to prevent the malignant characteristics and uniform use of system resources. The AODV routing is changed dependent on the followings:

- RREP packet is send by AODV-RP for every RREQ data to make the destination sends various RREP packet for RREQ.
- The improvement of RREP packet structure is increased in the path to have trust value.
- The storing of the trust-esteem for every section of S-D is suitable for the routing table.
- AODV sends demand to instruct the directing way at consistent time period. Henceforth, at normal interval, source node will have different ways each with its trust an incentive from which one with the most extreme trust is chosen.

3.3 Trust Based Route Optimization Using ACO Algorithm

ACO algorithm takes fascination based on the qualities of ants in nature and from the related field of ACO to determine the issues of routing in sensor networks. The important source of inspiration is found in the limit of particular sorts of ants to look through the base way between their nest and a nourishment sources utilizing Pheromone (Impulsive Chemical Substance). Insects leave clues of pheromone as they migrate between sources to destination. Ants astoundingly go over the range of high pheromone powers searching for sustenance. The larger amount of pheromone is received, when the minimum path is done quicker. The positive establishment process allows the colony to reach the shortest path.

4 Result and Discussion

The T2AR-AODV-ACO method is processed in NS2 to improve better energy model and routing for transmission of data using AODV RP with ACO optimization algorithm. The ACO calculation is utilized to get the upgraded way and transmit information packets to the destination. This area gives a definite perspective on the outcome that are obtained utilizing T2AR-AODV-ACO. The T2AR-AODV-ACO procedure is utilized for giving trust estimation in the nodes of the message packets. The experimental results is calculated by taking the parameters as Through-put, routing-overhead, delay and energy-consumption compared with TERP methodology, which is implemented. The execution is determined by estimating the throughput, routing overhead, delay and energy consumption parameters.

Comparison analysis of T2AR-AODV-ACO is evaluated by varying the number of malicious nodes 1, 2, 3, 4 and 5. The Figs. 2, 3, 4 and 5 shows the comparison of the Throughput, Routing Overhead, delay and energy Consumption between existing methods. Throughput increased 7% in T2AR-AODV-ACO than TERP Methodology.

Delay decreased 6% in T2AR-AODV-ACO compared to TERP Methodology. The routing overhead decreased 8% in T2AR-AODV-ACO compared to TERP methodology. Energy Consumption decreased 7% in T2AR-AODV-ACO than TERP methodology [16]. Therefore, the QoS parameter values such as Throughput, routing overhead, delay and energy consumption of TERP implemented and theoretically referred in below cited paper [16].

Comparative analysis of T2AR-AODV-ACO evaluated by varying the nodes 20, 40, 60, 80 and 100. The Figs. 2, 3, 4 and 5 shows the comparison of the throughput, routing overhead, delay and energy Consumption between TERP existing methods.

The comparison of nodes vs. throughput between T2AR-AODV-ACO and TERP is plotted in Fig. 2. The throughput value increased in T2AR-AODV-ACO method, when compared with the TERP method with different malicious nodes 1, 2, 3, 4 and 5.

The comparison of nodes vs. routing overhead between T2AR-AODV-ACO and TERP is plotted in Fig. 3. The routing overhead decreased in T2AR-AODV-ACO method, when compared with the TERP method by varying different 20, 40, 60 80 and 100 Nodes.

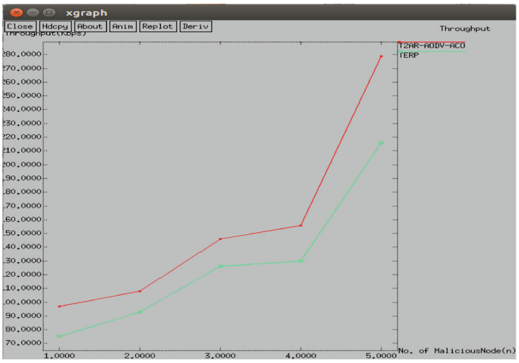

Fig. 2. Malicious node vs. Throughput

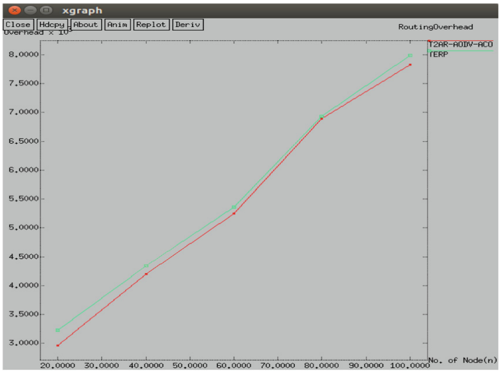

Fig. 3. Node vs. routing overhead

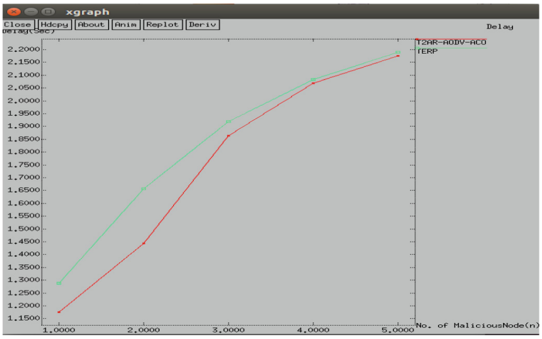

Fig. 4. Malicious node vs. delay

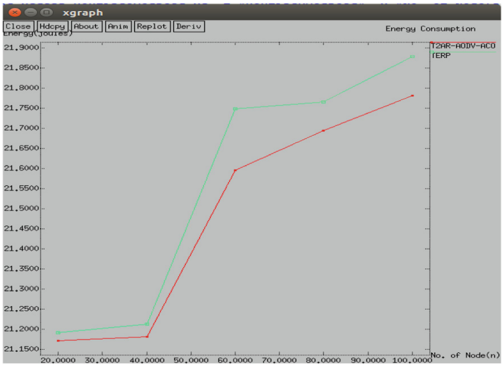

Fig. 5. Node vs. Energy consumption

The comparison of nodes vs. delay between T2AR-AODV-ACO and TERP is plotted in Fig. 4. The delay decreased in T2AR-AODV-ACO method, when compared with the TERP method by varying different 20, 40, 60 80 and 100 Nodes.

The comparison of nodes vs. energy between T2AR-AODV-ACO and TERP is plotted in Fig. 5. The energy consumption decreased in T2AR-AODV-ACO method, when compared with the TERP method by varying different malicious nodes 1, 2, 3, 4 and 5.

Thus, T2AR-AODV-ACO techniques effectively used for transferring trusted data packet from S-D in sensor networks with increase in throughput by decreasing routing overhead, delay and energy consumption. The simulation parameters of T2AR-TERP Methodology is explained as follows, the simulation start time and ending time is 0.0–5.0. The fixed nodes such as 20, 40, 60, 80 and 100 nodes are randomly distributed in the area. Here, each data packet starts its journey from a random location to a random destination with randomly selected speed. In traffic model, the Constant-bit rate (CBR) traffic sources are used with 802_11 MAC Type. Antenna model used is Omni Antenna with 28 ms minimum speed and Initial transmit and receive power is 0.660 and 0.395 W.

5 Conclusion

The "T2AR-AODV-ACO" methodology used for Trust based secured route path between the source node and the destination node. The Trust based AODV RP with ACO optimization is used for maintaining energy and secured trust based routing in ad-hoc networks. Thus, overall methodology provides better results in term of throughput, routing overhead, end-to-end delay and energy consumption in trust aware ad-hoc routing compared to TERP methodology by varying the no. of fixed nodes and malicious nodes. The hybrid trust based security can be further enhanced by using optimization and also by detecting the malicious nodes in the trust based ad-hoc networks.

References

1. Chen, R., Guo, J., Bao, F., Cho, J.H.: Trust management in mobile ad hoc networks for bias minimization and application performance maximization. Ad Hoc Netw. **19**, 59–74 (2014)
2. Chen, R., Guo, J., Bao, F., Cho, J.H.: Integrated social and quality of service trust management of mobile groups in ad hoc networks. In: Proceedings of IEEE 9th International Conference on Information, Communications & Signal Processing, pp. 1–5 (2013)
3. Mitchell, R., Chen, I.R.: Effect of intrusion detection and response on reliability of cyber physical systems. IEEE Trans. Reliab. **62**, 199–210 (2013)
4. Jawhar, I., Trabelsi, Z., Al-Jaroodi, J.: Towards more reliable and secure source routing in mobile ad hoc and sensor networks. Telecommun. Syst. **55**, 81–91 (2014)
5. Wen, D., Huai-Min, W., Yan, J., Peng, Z.O.U.: A recommendation-based peer-to-peer trust model. J. Softw. **15**, 571–583 (2004)
6. Jan, M., Nanda, P., Usman, M., He, X.: PAWN: a payload-based mutual authentication scheme for wireless sensor networks. Concurr. Comput. Pract. Exp. **29**, e3986 (2017)
7. Jan, M.A., Nanda, P., He, X., Liu, R.P.: A Sybil attack detection scheme for a forest wildfire monitoring application. Future Gener. Comput. Syst. **80**, 613–626 (2018)

8. Dong, M., Ota, K., Yang, L.T., Chang, S., Zhu, H., Zhou, Z.: Mobile agent-based energy-aware and user-centric data collection in wireless sensor networks. Comput. Netw. **74**, 58–70 (2014)
9. Paul, B., Marcombes, S., David, A., Struijk, L.N.A., Le Moullec, Y.: A context-aware user interface for wireless personal-area network assistive environments. Wireless Pers. Commun. **69**, 427–447 (2013)
10. Yu, Y., Li, K., Zhou, W., Li, P.: Trust mechanisms in wireless sensor networks: attack analysis and countermeasures. J. Netw. Comput. Appl. **35**, 867–880 (2012)
11. Yan, Z., Wang, M.: Protect pervasive social networking based on two-dimensional trust levels. IEEE Syst. J. **11**, 207–218 (2017)
12. Saha, H.N., Mitra, P.: Intelligent energy aware fidelity based on-demand secure RP for MANET. Int. J. Comput. Netw. Inf. Secur. **10**, 48–64 (2018)
13. Bijon, K.Z., Haque, M.M., Hasan, R.: A trust based Information sharing model (TRUISM) in MANET in the presence of uncertainty. In: Proceedings of IEEE Twelfth Annual International Conference on Privacy, Security and Trust (PST), pp. 347–354 (2014)
14. Shabut, A.M., Kaiser, M.S., Dahal, K.P., Chen, W.: A multidimensional trust evaluation model for MANETs. J. Netw. Comput. Appl. **123**, 32–41 (2018)
15. Patel, N.J.K., Tripathi, K.: Trust value based algorithm to identify and defense gray-hole and black-hole attack present in MANET using clustering method. Int. J. Sci. Res. Sci. Eng. Technol. **4**, 281–287 (2018)
16. Sivakumara, D., Jeganb, J., Selvakumarc, K.: Cuckoo search based Reliable Energy and Trust aware Routing Protocol (CRETRP) for wireless sensor network. Int. J. Control Theory Appl. **10**, 121–134 (2017)
17. Patel, V.H., Zaveri, M.A., Rath, H.K.: Trust based routing in mobile ad-hoc networks. Lect. Notes Softw. Eng. **3**(4), 318 (2015)