Implementing Trust Aware Routing Protocol for Privacy Preservation in MANET

Shubham Joshi
Research Scholar, Mewar University
Chittorgarh

Durgesh Kumar Mishra
Research Supervisor, Professor SAIT
Indore.

Abstract: The path of privacy preservation is important, and some ad-hoc networks require strong privacy protection. For the ad-hoc security purpose several schemes are proposed. Since data packs and control packs are still connected and distinct, neither it can be completely unassembled. The paper implements a stronger trust aware routing protocol (TARP) to maintain privacy on mobile ad hoc networks (MANET). We are describing the unobservable safety routing scheme for providing complete non-linkability and content invisibility. It’s effective because it’s used to combine signature group and identity-based encryption to identify a route. System security shows that the trust-aware routing protocol serves security and protects from attackers.

Keywords: MANET, Privacy preservation routing protocol, Group signature, Trust management, ID based encryption.

I. INTRODUCTION

The privacy of Mobile ad hoc networks (MANET) is more demanding. In wired networks, one has to get fixed a cable that eavesdrops on communications. The attackers need a proper transmitter to get a wireless signal undetected. Devices in wired network such as desktop computers are always static. Therefore, in a wired network, does not required any protection the user's movement behavior and movement patterns, and this sensitive information should be kept secret [1].

MANET dynamic configuration and infrastructure architecture transfer the data by containing the operating node. The ammonia presented centralized controller shows the path of routing, which begins with the mechanism of node interaction for packet transition [2]. In general, nodes of MANET responsible for forwarding packages and generate a network. In addition, without centralized administration MANET requires nodes to cooperate with the default authenticity. The attack existence reduces network life and disrupts data transmission [3].

Additional information on cooperation mechanisms should be assigned to resource sharing. Therefore, reliability is necessary to ensure only resources are share between reliable nodes. The MANET'S unpredictable nature creates attack vulnerabilities that threaten security. Due to this create a safe environment using trust management protocol (TMP). The protocol developments increases trust level [4] [5]. To improve safety employs TMP, which promotes prevention and identification-based approaches. The detection methods based on TMP identify abnormality of schemes. So the trust renewal protocols are an active area of research.

The goal is to inherit the nodes function is a power, computing power, battery life and other nodes, affecting the selfish node (SN) by [6]. Therefore, the preservation of resources is important for processing the SN. Moving and relocating a SN is avoids nasty nodes. For resource allocation, intruders acquire information about dynamic changes, providing effective data delivery. Because of the nasty nodes quality of network is low [7]. The paper presents a scheme for assessing trust energy model. Collecting a neighboring log and maintaining a route using log reports. Therefore, the extended trust recognition routing protocol implemented in this paper. The novelty of the protocol is the use of direct and indirect trust tracking schemes for a neighbor's log result and ensuring reliability by matching the ID.

II. RELATED WORK

M. S. Pathan et al. [8] reliable combination of schemes of QoS routing was proposed. They find a trust mechanism by mitigating nodes exhibiting various packet transfer mechanism. R. Hingane et al. [9] opinion-based trust model (TM) is proposed that works based on network properties. This model helps to an opinion estimation that helps you get the safest route. In [10] implement AASR protocol against neighboring node attacks. This method is authenticated routing and trust-based model. Jawhar. I et al. [11] a trust-based routing Protocol (TRP) for special and sensor-based TRAS networks was introduced. It detected multi-pass paths for achieving enhanced communication security. The trust factor increases when nodes successfully enter in transferring data process using the confirmation mechanism.

J. Shet et al. [12] a trust-based system assesses node reliability and capability according to multidimensional test values. A. Chakrabarti et al. [13] propose a three-tiered architecture, its trust-based framework that distinguishes between illegal and legal nodes. M. Mahmoud, et al [14] suggests a TETO protocol to encourage node collaboration and establish stable routes. It uses to encourage node collaboration and processes payment. Sripriya. G, et al. [15] the threshold scheme for managing public keys on-demand protocol of vector routing to improve performance and ensure high security. AV. Kumar et al [16] TRP scheme on Q-learning is proposed. It's a promising, as it increases the coefficient of package delivery and time is reduces for choosing a route. U. Venkanna, et al [17] solution reveals malicious and SN behavior by dynamically calculating the confidence and energy values.

M. Malathi, et. al. [18] proposed remarkable parameters to ensure path reliability. Its main factor is the unintentional generation of nodes that fail to model. S. N. Shah, et. al [19] reliable routing schemes proposes that combine the QoS and social trust. R. H. Jhaveri, et al [20] suggests an improved pattern detection mechanism that tries pull of adversaries to perform packet forwarding violations. R. J. et al. [21] to detect suspicious activity before starting to drop data from a malicious node, a pattern detection mechanism is proposed. S. Sarkar, et al. [22] a safe multi-beam route Protocol on Markov chain for MANET is proposed. S. Nageswara et al [23], proposes new calculation of QoS trust in MANET. P. Sethuraman et al. [24] Bayesian probabilities are introduced and to handle uncertainties to obtain sophisticated forms of confidence calculations. Ahmed. M, et al [25], proposes a flood factor-based framework. B. Rajkumar, et al [26], proposes threshold revocation technique on CA distribution and trust.

Cho. J. H, et al [27], proposes trust based fully decentralized approach for security mechanism. Xia. H, et al [28], a dynamic confidence prediction model for evaluating node reliability is presented. R. Mylsamy, et al. [29] preference-based on trust and head selection (2PTH) algorithm introduced for communication Privacy between malicious nodes. R. Ferdous, et al. [30] proposes selecting cluster heads algorithm on effective trust model. This algorithm is to select reliable stable cluster heads that can provide secure communication through collaborative nodes.

III. TRUST AWARE ROUTING PROTOCOL

This section describes the implemented system in Fig.1, first the network is created and then node initialization is done. The system collects information from log reports of neighbor to find out the frequency of successful / unsuccessful packet transfers. Calculation of trust value (TV) based on comparison of sequence packet identifiers on log records of nodes. Essentially, AODV is a reaction routing protocol that establishes the route when needed by using number of destination to get the latest path, AODV shows destination route. However, the calculated destination node becomes unreliable because of malfunction report generation. System reliability is calculated through mobility, hybrid energy rating and package delivery success rate.

The maximum TV is then selected for transferring packets. In these estimates, the route must be reliable, and safe. In addition, estimation of the distance to the target calculations using the RSSI, it is guaranteed that the locate the trust node with the communication distance. Nodes in MANET are moves anywhere.

A node that sends packets called a source node (SN) and receives the data called destination node (DN). Value of trust is maximum, the data transmission is safe. In this approach, calculation of TV is combination of observations. SN selection and extraction of neighbor node uses RSSI. The node's reliability then updated and calculates package, the sequence's identity with the corresponding rate of speed and mobility. Highest reliable node is selecting as the mediator node for delivering packages to the target node. The implementation is assessed by PDR, throughput and false positive results.

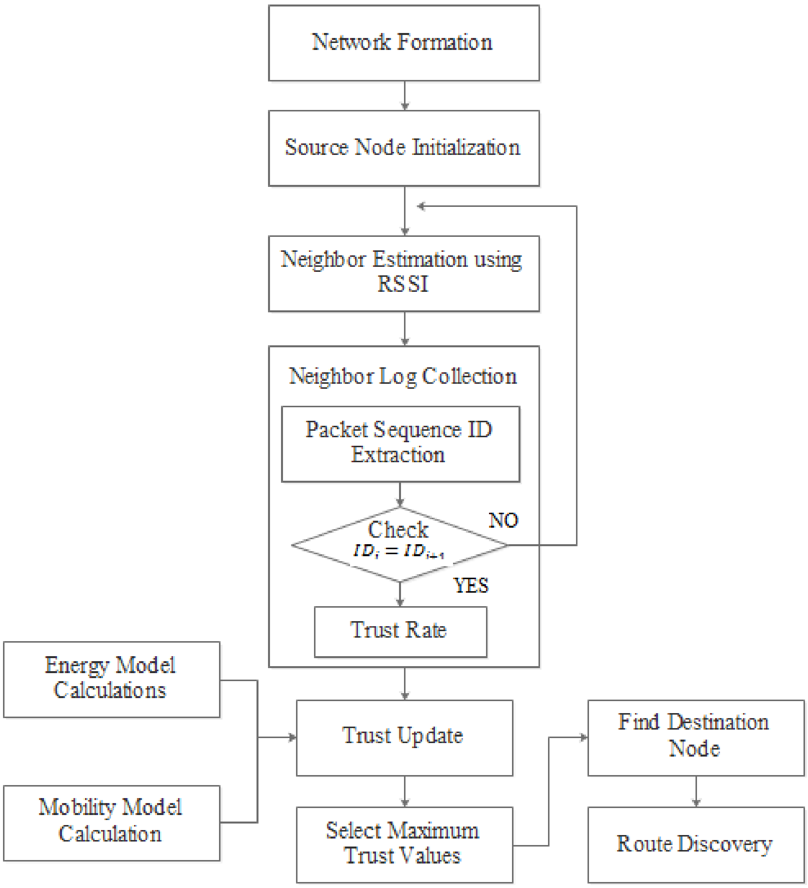

Figure 1: Proposed System Diagram

A) *Collection of neighbor log*

Estimation of Neighbor is the first step in calculating a node's trust value. Assessment based on distance RSSI identifies sites located near the original Node.

Algorithm of collection of neighbor log

Input: Node N
Output: Trust Rate (TR)

1. Collect the neighbor node (NN) and list the input nodes.
2. Log information collection of specific neighbor node
3. Get sequence ID of packet from log report
4. Strength calculation of source node S and current node i
5. if (strength between S and i < Range) then
6. Packet ID of N Node = Extract the ID from log report
7. If Packet $ID_{N(i)}$ Node = = Packet $ID_{N(i+1)}$
8. Compute TR
9. Else
10. Go to step 1
11. End if
12. Else
13. Go to step 1
14. End if
15. End for

The TV for a given node is on energy, mobility, and trust rates. Therefore, the proposed study includes three phases of energy *(E)* model, trust rate *(TR)* calculation, and mobility *(M)* model.

B) Computation of trust rate

As input graphs and nodes are provide for the algorithm of neighboring log collection. The list of NN is built for input. Information is then collected on all nodes. Calculation of RSSI method is [31]:

$$D_{s,i} = RSSI(N, G_i) \quad (1)$$

Where, $D_{s,i}$ is the strength of signal between s and i node, G_i is i node of graph. Trust levels calculation is:

$$TR_i = \frac{1}{3}\,(b_{s,i}(h) \times b_{s,i}(h))(ps_r + rs_r + rqs_r) \quad (2)$$

$$TR_i = \frac{1}{3}\left(b_{s,i}(h) \times b_{s,i}(h)\right)\left(\frac{np_s}{np_s+np_f} + \frac{nrp_s}{nrp_s+nrp_f} + \frac{nr_s}{nr_s+nr_f}\right) \quad (3)$$

Where, TR_i is a rate of trust, $b_{s,i}(h)$ is belief function indicates the 0 to 1 state. The level 0 indicates an unknown state, and 1 indicates a known state. The ps_r is packet rate between successful packet transmissions (np_s) and failed packet transmissions(np_f). rs_r Reply success rate is ratio of safe transmission. The number of successful reply packets (nrp_s) and a number of failed reply packets (nrp_f). Request success rate rqs_r is the ratio of successful request transmission to the overall request transmission. Improved network life based on accumulated E and M of nodes.

C) Energy Estimation

Energy is defined as a node's ability to transmit data. The main task is find neighborhood and maintains the route. We evaluate the model as a proposed approach:

$$E_{m,n} = [(Pi_{m,n} \times Ti_{m,n}) + (Pr_{m,n} \times Tr_{m,n}) + (Pt_{m,n} \times Tt_{m,n})] \quad (4)$$

Where, $Pi_{m,n}$, $Pr_{m,n}$, $Pt_{m,n}$ is a power consumption level during idle, reply and transmission stages. To transmit the packets select the node, update node energy to send remaining packets. Overall energy $Ei_{m,n}$ updated as follows:

$$Ei_{m,n} = Ei_{m,n} - E_{m,n} \quad (5)$$

D) Mobility Function

The mobility function describes a moving node. Calculation of distance between nodes is done by using constant value K and transmission and reception as follows:

$$d = \sqrt[4]{K.Pt/Pr} \quad (6)$$

Velocity of neighbor is,

$$\bar{V} = \Delta d/\Delta t \quad (7)$$

The functions of mobility is calculate from,

$$M_i = \bar{V}TR_i + d \quad (8)$$

Using estimates of energy, TR, and mobility from (3), (4), and (8), the TV calculation is:

$$TC_{s,i} = E_{s,i} + TR_i - M_i \quad (9)$$

Compare ID of packets with nodes, if both identities match, calculate the TR using request, response, and packet delivery rates, and the calculated TR used as input in trust process.

E) Trust Update

Trust between nodes is important for packet forwarding, as MANET can have malicious or rogue nodes. The malicious node causes packet drops. We are investigating the impact of nasty nodes on package drop. Ensuring reliability through both direct and indirect methods of observation effectively reduces the breakdown of packages in the intended operation.

Direct Observation:

The observer node directly estimates the TV using the Bayesian framework, which assumes that the Observer node overhauls the forwarded packet and finds malicious behavior. The distribution function follows the beta function:

$$Beta(\theta;\alpha,\beta) = \frac{\theta^{\alpha-1}(1-\theta)^{\beta-1}}{\int_0^1 \theta^{\alpha-1}(1-\theta)^{\beta-1}d\theta} \quad (10)$$

The expected function or penalty coefficient would be:

$$E_{s,i} = E_n(\Theta) = \frac{\alpha_n}{\alpha_n+\beta_n} \quad (11)$$

The greater the weight of the punishment factor indicates huge misbehavior due to lower trust value. A deduction of penalty coefficient refers TR as

$$TR = E_n(\Theta) \quad (12)$$

A monitoring basis on identifying malicious behavior reduces trust. But the implementation of trust-aware routing protocols is calculates the level of trust by matching sequence IDs, which ensures secure data sending.

Indirect Observation

Shafterian theory calculates the belief function in three sets as:

$$h = \{trust\}, \quad \bar{\bar{h}} = \{untrust\}, \qquad u = \{trust\ or\ untrust\}$$

I observation the belief function is, if the node *A* observed *B* node is trusted node:

$$\text{b (h)} = \text{TR}$$
$$\text{b }(\bar{\bar{h}}) = 0$$
$$\text{b (u)} = 1 - \text{TR} \quad (13)$$

I observation the belief function is, if the node *A* observed *B* node is untrusted node:

$$\text{b (h)} = 0$$
$$\text{b }(\bar{\bar{h}}) = 1$$
$$\text{b (u)} = 1 - \text{TR} \quad (14)$$

IV. RESULT AND DISCUSSION

This section examines the proposed TARP protocol and the existing trusted ROUTING MECHANISM NON-COOPERATIVE MANET (TRUNCMAN) [32], DICOTIDS [34] and REPUTATION-BASED RBT protocol [33] are compared. Calculate the performance using following parameters: PDR, throughput, and false positive results. The implemented system uses network simulator (NS-2) shows in Table 1.

Parameter	Values
Simulator	NS-2
Routing Protocol	TARP
Nodes number	100
Packet size in byte	512
Simulation time	600
Data rate in mbps	2

A) Packet Delivery Ratio (PDR)

The PDR calculates using packets number is sending and received.

$$PDR = \frac{Number\ of\ packets\ received}{Number\ of\ packets\ transmitted} \times 100 \quad (15)$$

Since packages are quick send in a short time if buffer empty or free. The trust calculation easily identifies nodes misbehavior. Implemented system PDR is better than the existing scheme fig. 2 and 3. Proposed TARP compared with TRUNCMAN and AODV using node, the proposed TARP delivers 8.93 and 4.64% better than AODV and TRUNCMAN. Similarly, a proposed TARP with TRUNCMAN and AODV on discarded packets shows that TARP indicates 86.11 and 54.58% less for a low malicious coefficient and offers 36.9 and 21.4% less for a high malicious coefficient, respectively, because of three-series trust simulation (Energy, mobility, confidence level).

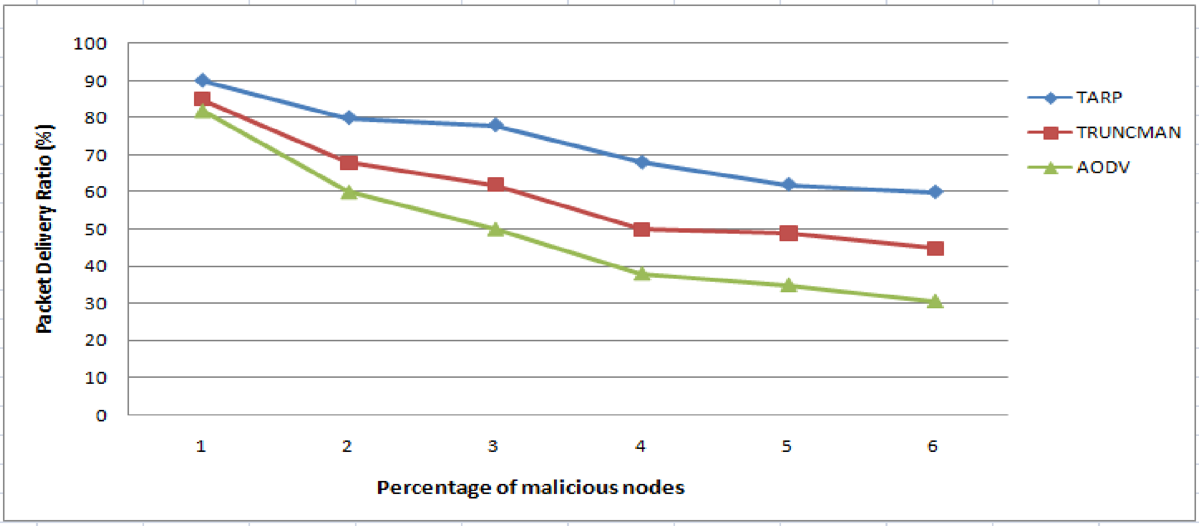

Figure 2: PDR of node

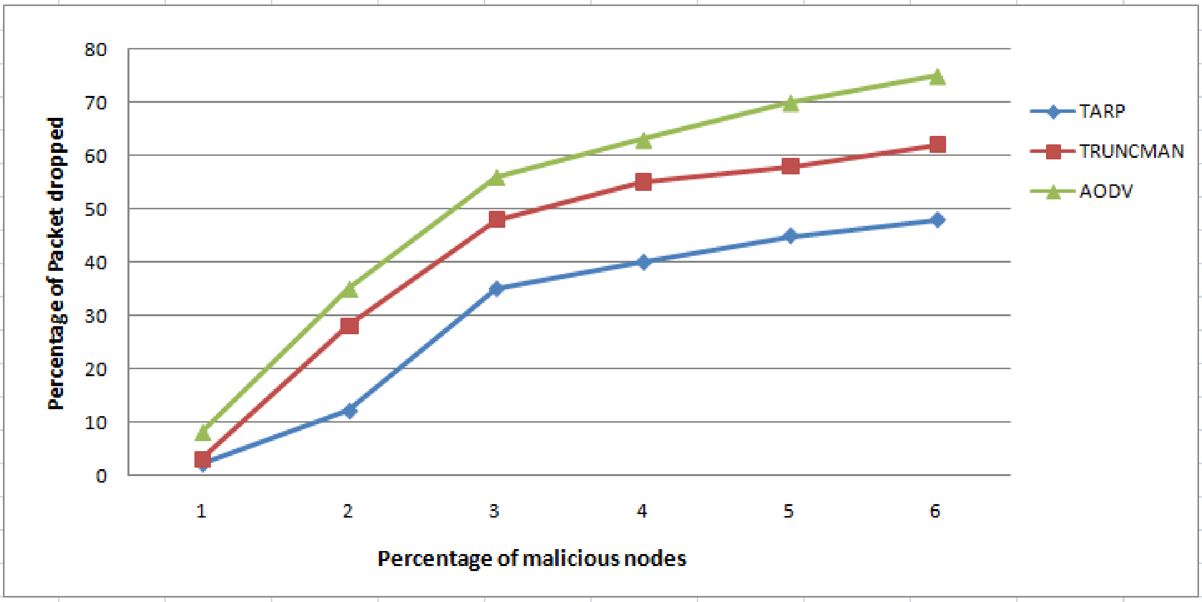

Figure 3: Discarded packets

B) Throughput

Throughput is defined as the total volume of data packets that the target node receives correctly every second. It provides information on whether packages not delivered correctly. To prevent malicious attacks from occurring, evaluate the TV of node. Figure 4 shows that T2AR performance has increased compared to RBT and in this no RBT variation in network size.

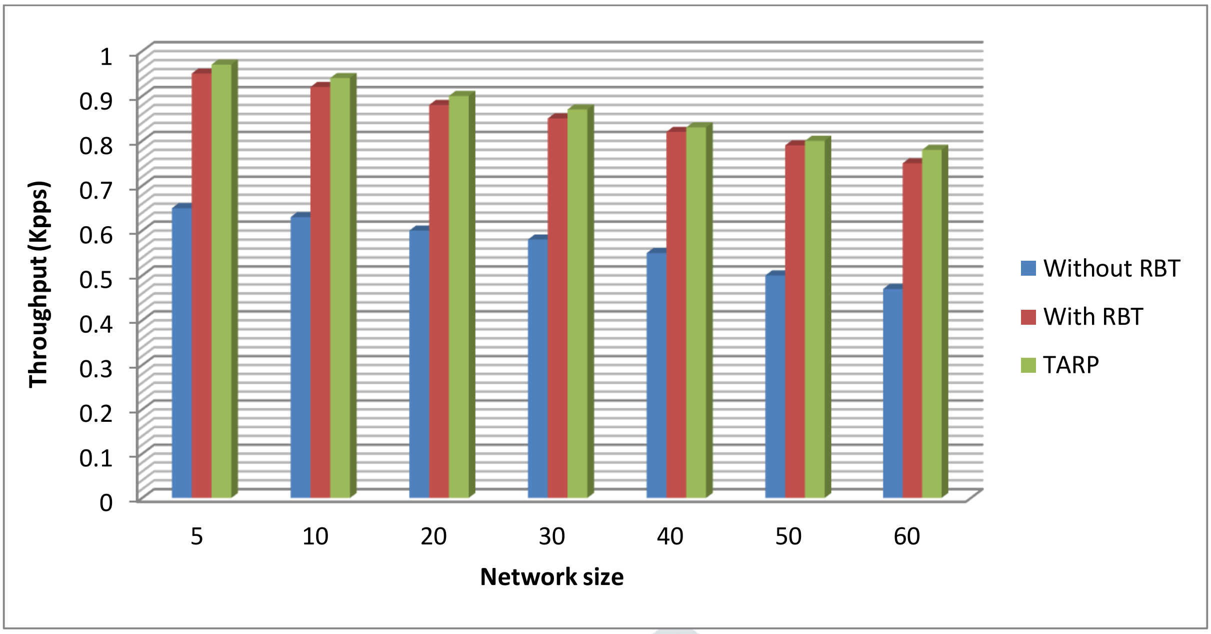

Figure 4: Throughput

C) False Positive

The probability of detecting a bad behavior node from total node represents a false positive. Fig. 5 shows a simulation and false positive results. False-positive results seem to be effectively reduced when simulator is increased. This indicates TARP reduces false-positive performance.

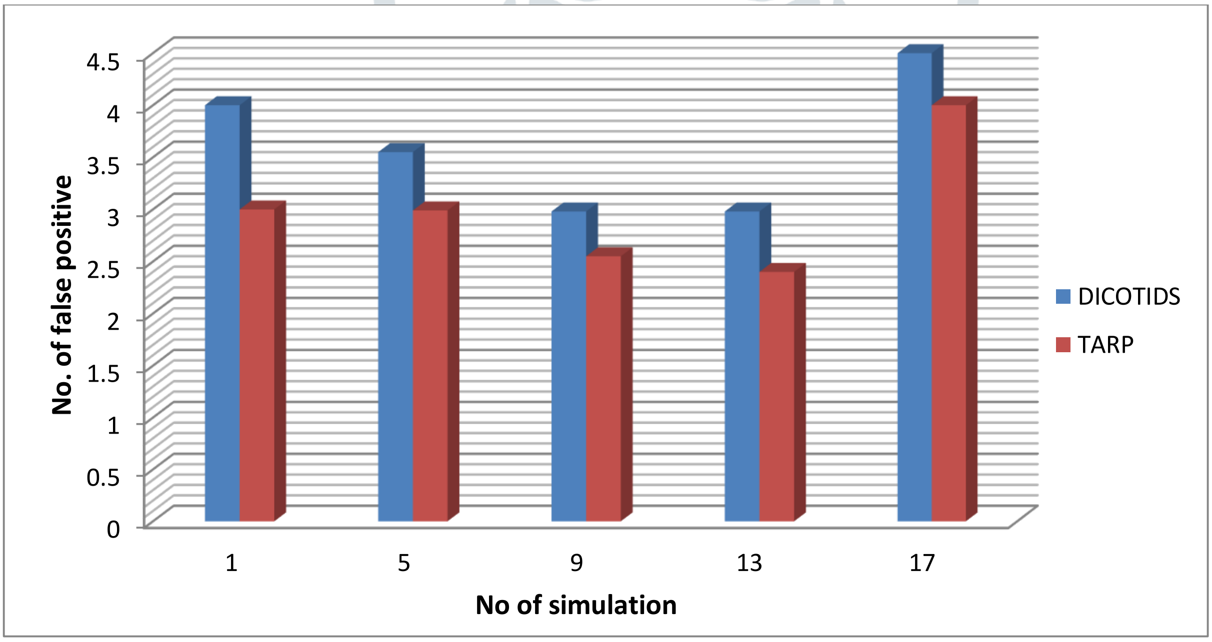

Figure 5: False positives ratio

V. CONCLUSION AND FUTURE WORK

The paper proposes TARP to improve trusting level of nodes and transfers data very safely. The system corrects the AODV by adding constraints, based on stability and energy and mobility. Information about trust guarantees obtained from Reputation-based routing protocol peers that provide less PDR and throughput as the malicious node ratio increases. TARP suggested collecting logarithmic information from NN using observation. Verification of ID based on TR calculation increase trust compared to traditional models. Implemented system made it possible to achieve fewer false positives. In future we will improve security using the location key management Protocol.

REFERANCES

1. Al Mazrouei, M.S., Narayanaswami, S., 2011. Mobile ad hoc networks: a simulation based security evaluation and intrusion prevention. In: Internet Technology and Secured Transactions (ICITST), 2011 International Conference for, pp. 308–313.
2. Lavanya K N, Dr.DeepaAnand, "Trust Based Routing Scheme for MANETs in Adversarial Environment through AASR Protocol", International Journal of Research in Computer Applications and Robotics, Vol.3 Issue.5, May 2015,
3. Dr.S.Revathi, Dr.T.R.Rangaswamy, "Secure Route Discovery using Opinion Based Method in MANET", International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501,Vol.5, No.1, February 2015
4. K. Chakravarthy, B. DurgaAnuja, "Trust Based Routing Protocol for Multi-Hop Wireless Networks", International Journal of Advance Research inComputer Science and Management Studies, Volume 2, Issue 10, October 2014
5. A.PravinRenold, R.Parthasarathy, "Source based Trusted AODV Routing Protocol for Mobile Ad hoc Networks",ICACCI'12, August 3-5, 2012, Chennai, T Nadu, India.
6. Lafta, H.A., Al-Salih, A.M.M.S., 2014. Efficient routing protocol in the mobile ad-hoc network (MANET) by using genetic algorithm (GA). IOSR J. Comput. Eng. 16 (1), 47–54.
7. Wei, Z., Tang, H., Yu, F.R., Wang, M., Mason, P., 2014. Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning. Veh. Technol. IEEE Trans. 63 (9), 4647–4658.
8. Pathan, M.S.; Zhu, N.; He, J.; Zardari, Z.A.; Memon, M.Q.; Hussain, M.I. An Efficient Trust-Based Scheme for Secure and Quality of Service Routing in MANETs. Future Internet 2018.
9. Rashmi Hinge and Jigyasu Dubey, Opinion based trusted AODV routing protocol for MANET. In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies (ICTCS '16). 2016.
10. Lavanya K N, Dr. Deepa Anand, "Trust Based Routing Scheme for MANETs in Adversarial Environment through AASR Protocol", International Journal of Research in Computer Applications and Robotics, Vol. 3 Issue. 5, May 2015, Pg.: 100--107.
11. I. Jawhar, F. Mohammed, J. A. Jaroodi and N. Mohamed, "TRAS: A Trust-Based Routing Protocol for Ad Hoc and Sensor Networks," 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), New York, NY, 2016, pp. 382-387, doi: 10.1109/BigDataSecurity-HPSC-IDS.2016.58.
12. J. Shet and D. Shetty, "Multidimensional trust-based energy aware routing protocols in multihop wireless networks," 2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kannur, 2017, pp. 1520-1523, doi: 10.1109/ICICICT1.2017.8342796.
13. Chakrabarti A., Parekh V., Ruia A, A Trust Based Routing Scheme for Wireless Sensor Networks. In: Meghanathan N., Chaki N., Nagamalai D. (eds) Advances in Computer Science and Information Technology. Networks and Communications. CCSIT 2012. Social Informatics and Telecommunications Engineering, vol 84. Springer, Berlin, Heidelberg
14. Mahmoud, Mohamed & Shen, Xuemin. (2011). Trust-Based and Energy-Aware Incentive Routing Protocol for Multi-Hop Wireless Networks. IEEE International Conference on Communications. 1-5. 10.1109/icc.2011.5963403.
15. G. Sripriya, Dr. T. Santha, A Secure Trust based Routing Protocol for Scheme Enhancing Quality of Service in Mobile Ad-Hoc Networks, International Journal of Engineering & Technology, 7 (4.28) (2018) 717 -722
16. Kumar AV, and Jeyapal A. Self-adaptive trust based ABR protocol for MANETs using Q-learning. Thescientificworldjournal. 2014, DOI: 10.1155/2014/452362.
17. Venkanna, U., Agarwal, J.K. & Velusamy, R.L. A Cooperative Routing for MANET Based on Distributed Trust and Energy Management. Wireless Pers Commun 81, 961–979 (2015). https://doi.org/10.1007/s11277-014-2165-5
18. M. Malathi, S. Jayashri, Robust against route failure using power proficient reliable routing in MANET, Alexandria Eng. J. (2016), http://dx.doi.org/10.1016/j.aej.2016.10.004
19. S. N. Shah and R. H. Jhaveri, "A trust-based scheme against Packet dropping attacks in MANETs," 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Bangalore, 2016, pp. 68-75, doi: 10.1109/ICATCCT.2016.7911967.
20. Jhaveri, R.H.; Patel, N.M.; Jinwala, D.C. A Composite Trust Model for Secure Routing in Mobile Ad-Hoc Networks. In Ad Hoc Netw.; Ortiz, J.H., de la Cruz, A.P., Eds.; InTech: London, UK, 2017; ISBN 978-953-51-3109-0
21. Jhaveri Rutvij & Patel Narendra, Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks: Secure Routing in MANETs Using Enhanced Trust Model. International Journal of Communication Systems. (2016). 30. 10.1002/dac.3148.
22. S. Sarkar, R. Datta, A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks, Ad Hoc Networks (2015), http://dx.doi.org/10.1016/j.adhoc.2015.08.020
23. Sirisala, Nageswara & Chigarapalle, Shoba, A novel QoS trust computation in MANETs using fuzzy petri nets. International Journal of Intelligent Engineering and Systems. (2017). 10. 116-125. 10.22266/ijies2017.0430.13.

24. Sethuraman, Priya & Kannan, N, Refined trust energy-ad hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET. Wireless Networks (2016). 23. 10.1007/s11276-016-1284-1.
25. Ahmed, M.N.; Abdullah, A.H.; Chizari, H.; Kaiwartya, O. Flooding Factor based Trust Management Framework for secure data transmission in MANETs. J. King Saud Univ. Comput. Inf. Sci. 2017, 29, 269–280.
26. Rajkumar, B.; Narsimha, G. Trust Based Certificate Revocation for Secure Routing in MANET. Procedia Comput. Sci. 2016, 92, 431–441.
27. Cho, J.-H.; Chen, I.-R.; Kevin, S.J. Trust threshold based public key management in mobile ad hoc networks. Ad Hoc Netw. 2016, 44, 58–75.
28. Xia, H.; Jia, Z.; Li, X.; Ju, L.; Sha, E.H.-M. Trust prediction and trust-based source routing in mobile ad hoc networks. Ad Hoc Netw. 2013, 11, 2096–2114.
29. Mylsamy, R.; Sankaranarayanan, S. A Preference-Based Protocol for Trust and Head Selection for Cluster-Based MANET. Wirel. Pers. Commun. 2016, 86, 1611–1627.
30. R. Ferdous, V. Muthukkumarasamy and E. Sithirasenan, "Trust-Based Cluster Head Selection Algorithm for Mobile Ad Hoc Networks," 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, Changsha, 2011, pp. 589-596, doi: 10.1109/TrustCom.2011.76.
31. Saadoune M, Hajami A, Allali H (2014) Distance's quantification algorithm in AODV protocol. Int J Comput Sci Inform Technol 6(6):177–188
32. Thanigaivel G, Kumar NA, Yogesh P (2012) TRUNCMAN: trust based routing mechanism using non-cooperative movement in mobile ad-hoc network. In: Second international conference on digital information and communication technology and it's applications (DICTAP), pp 261–266
33. Banerjee A, Neogy S, Chowdhury C (2012) Reputation based trust management system for MANET. In: Third international conference on emerging applications of information technology (EAIT), pp 376–381
34. Mutlu S, Yilmaz G (2013) Simulation and performance analysis of distributed cooperative trust based intrusion detection framework for MANETs. J Aeronaut Sp Technol/Hava Uzay Teknol Derg 6(2):49–57