International Journal of Scientific Research & Engineering Trends
Volume 5, Issue5, Sep-Oct-2019, ISSN (Online): 2395-566X

Estbt- Enhance Secure Trust Based Transmission for Mobile Ad-Hoc Network

Shailendra shrivastava
Dept. of CSE,
Swami Vivekanand College of Science and Technology Bhopal, India
shailendrargpm@gmail.com

Sushma Kushwaha
Dept.of CSE,
Swami Vivekanand College of Science and Technology Bhopal, India
Sushma.svcst@gmail.com

Abstract **- Mobile Ad-Hoc network is most popular in current scenario but when this network popular increased as well as so many attacked or unauthorized access increased. In this article will analysis about secure and trust based communication. In any case, constructing a trust model that receives recommendation by different hubs in the system is a testing issue because of the danger of dishonest recommendation like bad-mouthing, ballot-stuffing and collusion. The attacks caused by badly behaving nodes when increasing recommendations in the existing trust models. A recommendation based trust model demonstrate with a protection plan, which uses clustering technique to powerfully filter out attacks related to dishonest recommendations between certain time in view of number of cooperation, similarity of data and closeness between the hubs. The model is observationally tried under a few mobile and separated topologies in which hubs encounter changes in their neighborhood prompting regular course changes. The experimental investigation exhibits vigor and precision of the trust demonstrate in a dynamic MANET condition. This model can be extended by weighting recommendations based on time and location to mitigate the influence of location and time dependent attacks.**

Keywords **- Mobile ad hoc networks, dishonest recommendation, recommendation management.**

I. INTRODUCTION

Trust as a social concept can be defined as the degree of subjective belief about the behaviour of a particular entity. Trust is being increasingly adopted as an important concept to design and analyze security problems in distributed systems to guide decision making. Trust in MANETs is the opinion held by one node (known as evaluating node) about another node (known as evaluated node), based upon the node's past behaviour and recommendations from other nodes (known as recommending nodes) in the network.[1]

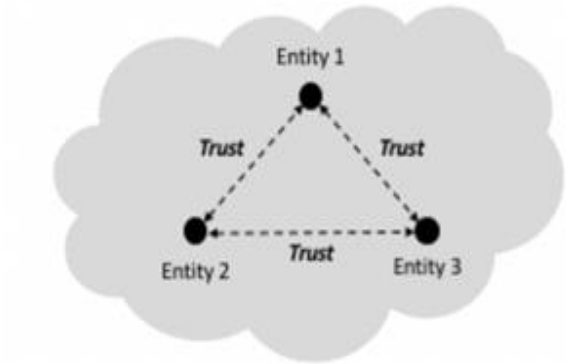

Fig.1. Full Trust Model.

MANET's applications are increasing in future network paradigms including vehicular and mesh networks. Many civilian and military services are demanding MANET applications, ranging from emergency rescue services such as hurricane and earthquake disasters to exchanging critical information on the battlefield or even home and personal area networking. The formation and sustained existence of MANET services are mainly based on an individual node's cooperation in packet forwarding. Due to the unique characteristics and demanding use, MANETs are vulnerable to attacks launched by misbehaving nodes. One of the approved mechanisms to improve security in MANETs is to use trust management techniques to deal with the misbehaving nodes and stimulate them to cooperate.[4][5]

1.Time Dependent Attack (TDA)
This attack makes participating nodes to change their behavior by time. Nodes can behave normally for a period of time and can misbehave by providing unfair ratings at other times. This attack also has its roots in the subjective property of trust.

2.Location-Dependent Attack (LDA)
This attack exploits mobility property of MANETs, where a node behaves differently according to its location. This attack originates from the subjective property of trust where behaviors at one location cannot affect evaluating trust worthiness of nodes at another location.

II. RELATED WORK

Authors in propose RFS Trust, a trust model based on fuzzy recommendation similarity, which is presented to quantify and evaluate the trustworthiness of nodes. They use similarity theory to evaluate the recommendation relationships between nodes. That is, the higher the degree of similarity between the evaluating node and the recommending node, the more consistent is the evaluation between the two nodes.

In this model, only one type of situation is considered when selfish nodes attack is present and the performance of the model is not tested against other attacks related to recommendation.[3] In an attempt to increase the honesty of utilizing recommendations, Li et al in include a confidence value in their evaluation by combining two values: trust and confidence into a single value called trustworthiness. They utilize the trustworthiness value to put weight on recommendations in which a recommending node with higher trustworthiness value is given more weight. Collusion attack in providing false recommendation is not considered by this work, and this may cause incorrect evaluation of the received recommendations.

III. PROBLEM STATEMENTS

1. False negative and false positive problems in evaluating the recommendation's trustworthiness and their impact on the network performance are poor. Majority rule could actually be harmful as some nodes can collude to perform an attack, and not provide an honest judgment about other nodes.
2. The selection of acceptability is a trade-off between obtaining more accurate trust worthiness value and the convergence time required to obtain it.

IV. PROPOSED SOLUTION

As we know without trust we can communication but problem in secure communication between source and destination so in our proposed solution we will communicate with trust based routing some step given below:-

- In the first step we will configure node and design a network with node to node communication.
- In the second step a node we will decide for transmit packets as we know that name is Source.
- A trust Algorithm will use for find Neighbor Node
- A threshold value for check node trust for communication
- Check Trust according their time and place
- Select Maximum Trust Value
- Find Destination Node
- If not found node repeat Route Discovery

V. TRUST CALCULATION

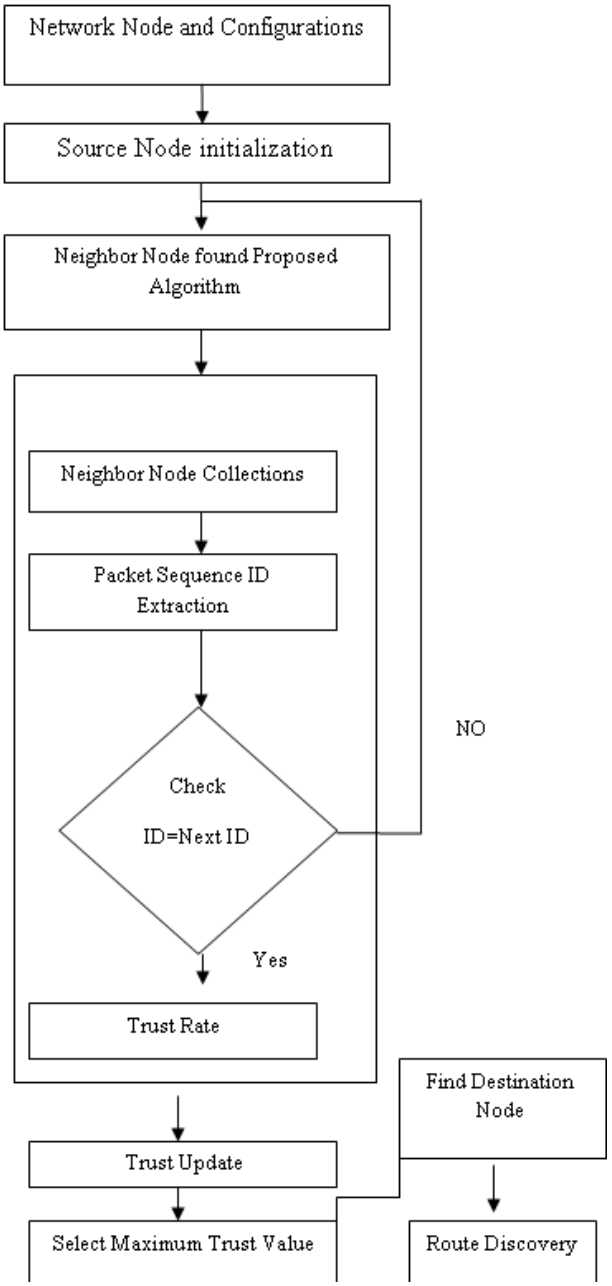

Fig.2. Flowchart or Algorithm.

Input: Source node Ns, Destination node Nd, Graph G
Output: Routing Path Rp
Procedure:
TRi←NeighborLogCollection(Ns,G)TRi←Neighbor LogCollection(Ns,G)
For i = 0, 1, 2 … n Then
Calculate trust value by using Eq. 4
End For
SN = MAX (TCs)

Rp←Rp∪SNRp←Rp∪SN
G←G′∉SN G←G′∉SN
If (Nd!=SN)(Nd!=SN) then
Update Energy Eis,SN
Ns = SN
Repeat from TR i
End If
Return Rp

VI. RESULT ANALYSIS

The simulation is conducted using NS2 simulator, an open-source discrete event simulator designed to support research in computer networking. It involves various modules to help test several network components such as packet, node routing, and application and transport layer protocols.NS2 fractures permit us to extend the DSR routing protocols that supports MANET architecture.

Table I. Simulation Configuration.

Parameter	Default Value
Simulation Area	700m * 700m
Simulation Time	500 seconds
Number of vehicles	50
Communication range	250m
Node Speed	10 m/hr
Visualization Tool	nam
Routing Protocol	DSR
MAC layer	IEEE 802.11 p
Source-destination pairs	15
Application	CBR
Packet Size	512 B

1. Throughput Vs Dishonest Recommendation

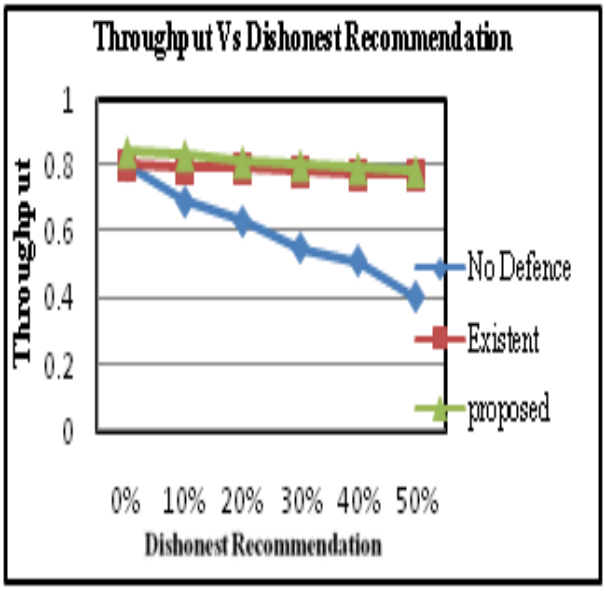

Fig.3. Throughput Vs Dishonest Recommendation.

2. Packet Loss Vs Dishonest Recommendation

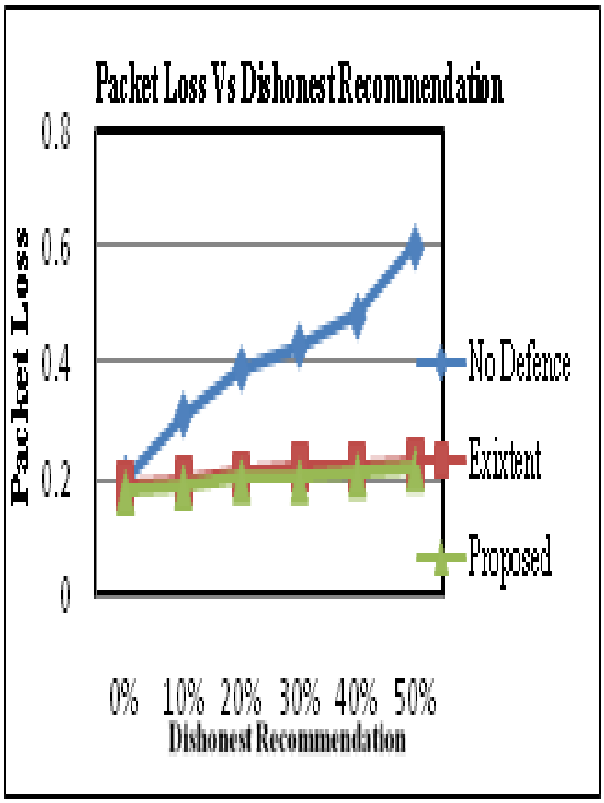

Fig.4. Packet Loss's Dishonest Recommendation.

VII. CONCLUSION

Performance of our approach is measured on the basis Throughput, Packet Loss, Good and Bad Node Trust value vs. dishonest recommendation. We are comparing between Existent A recommendation based trust model in dishonest nodes and Proposed approach Enhance Secure Trust Based Transmission (ESTBT) hare No Defense is common scenario for both approach. After applying our proposed work we improved these parameters Recommendation based trust system has is a framework to sift through the raising hell hubs while chasing down a package transport course. In any case, constructing a trust model that receives recommendation by different hubs in the system is a testing issue because of the danger of dishonest recommendation like bad-mouthing, ballot-stuffing and collusion. The attacks caused by badly behaving nodes when increasing recommendations in the existing trust models.

REFERENCES

[1]. Mangesh M Ghonge "Selfish Attack Detection in Mobile Ad hoc Networks" 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS).

[2]. Neena Vath Veeraiah "selfish node detection IDSM based approach using individual master cluster node" 2018 2nd International Conference on Inventive Systems and Control (ICISC).
[3]. sujit kumar das "selfish node detection and its behaviour in WSN(wireless sensor network)" Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT).
[4]. Tameem Eissa "Trust-Based Routing Mechanism in MANET: Design and Implementation" October 2013, Volume 18, Issue 5, pp 666–677
[5]. https://www.sciencedirect.com/science/article/abs/pii/S1570870515000530.
[6]. Ryma Abassi "A trust management based security mechanism against collusion attacks in a MANET environment" 2014 Ninth International Conference on Availability, Reliability and Security 325-332 IEEE
[7]. Sapna B. Kulkarni "Trust value updation algorithm for multicast routing algorithm for cluster based MANET ieeexplore.ieee.org/document/8299962
[8]. M. J. Atallah, K. Pantazopoulos, J. R. Rice, and E. ESpafford, "Secure outsourcing of scientific computations," Trends in Software Engineering, vol. 54, pp. 215-272
[9]. Jin Li, Gansen Zhao, Xiaofeng Chen, Dongqing Xie, "Fine-grained Data Access Control Systems with User Accountability in Cloud Computing", IEEE International Conference on Cloud Computing Technology and Science, 2010.
[10]. Younis A. Younis, Kashif Kifayat, Madjid Merabti, "An access control model for cloud computing", Elsevier journal of information security and applications, 2014.
[11]. C. Wang, Q. Wang, K. Ren, N. Cao, W. LouToward secure and dependable storage services in cloud computing IEEE Trans. Services Comput., 5 (2) (2012), pp. 220-232.
[12]. Duncan, Adrian, Sadie Creese, and Michael Goldsmith . "Insider attacks in cloud computing." Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE,201
[13]. Pearson S. and A. Benameur: Security and trust issues arising from cloud computing. IEEE Second International Conference on Cloud Computing Technology and Science, CloudCom, pp. 693-702, 2010
[14]. [10].M. M. Hassan, K. Lin, X. Yue, and J. Wan, "A multimedia healthcare data sharing approach throughcloud-based body area network," Future Generation Computer Systems, vol. 66, pp. 48–58, 2017
[15]. H.Yu, S.Liu, A.C.Kot, C.Miao, and C.Leung, ''Dynamic witness selection for trustworthy distributed cooperative sensing in cognitive radio networks'', Communication Technology (ICCT), 2011 IEEE 13th In-ternational Conference on, pp. 1-6, 2011.
[16]. J.Cai, P.Yi, J.Chen,Z.Wang, and N.Liu,''An adaptive approach to detecting black and gray hole attacks in ad hoc network,''Advanced In-formation Networking and Applications (AINA), 2010 24th IEEE Interna-tional Conference on, pp. 775-780, 2010.
[17]. K.Hoffman, D.Zage, and C.Nita-Rotaru, ''A survey of attack and defense techniques for reputation system,s'' ACM Computing Surveys (CSUR, 42, (1), pp. 1, 2010
[18]. A.Jøsang, R.Ismail, and C.Boyd, ''A survey of trust and reputation systems for online service provision,''Decision support systems, 43, (2), pp. 618-644, 2007.
[19]. Y.Ma,H.Lu,Z.Gan, ''An Improved Direct Trust Evaluation Algo-rithm for the Context-Aware Trust Model, ''Innovative Mobile and In-ternet Services in Ubiquitous Computing (IMIS), 2013 Seventh International Conference on, pp.196-201, 2013
[20]. Yongli Ren, Gang Li, Jun Zhang, and Wanlei Zhou, "Lazy Collabora-tive Filtering for Data Sets with Missing Values", IEEE Transactions on Cybernetics, VOL. 43, NO. 6, pp. 1822-1834, DECEMBER 2013
[21]. G.Theodorakopoulosand J.S.Baras, ''Trust evaluation in ad-hoc networks,''Proc.3rd ACM workshop on Wireless security, pp.1-10,
[22]. G.V.Crosby, L. Hesterand,N.Pissinou, ''Location-aware, Trust-based Detection and Isolation of Compromised Nodes in Wireless Sensor Networks,''International Journal of Network Security, 12, (2), pp. 107-117, 2011.
[23]. M.K.Denko, T.Sun, and I.Woungang, ''Trust management in ubiqui-tous computing: A Bayesian approach,'' Computer Communications, 34, (3), pp. 398-406, 2011.
[24]. E.M.Daly, and M. Haahr, ''Social network analysis for information flow in disconnected delay-tolerant MANETs,'' Mobile Computing, IEEE Transactions on, 8, (5), pp. 606-621, 2009.
[25]. T.Issariyakul and E.Hossain,''Introduction to network simulator NS2,''Springer, 2011.
[26]. C.Bettstetter, G.Resta, and P.Santi, ''The node distribution of the random waypoint mobility model for wireless ad hoc networks,''Mo-bile Computing, IEEE Transactions on, 2, (3), pp. 257-269, 2003.