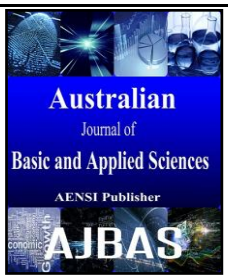
**Australian Journal of Basic and Applied Sciences**, 9(15) Special 2015, Pages: 89-92

ISSN:1991-8178

**Australian Journal of Basic and Applied Sciences**

Journal home page: www.ajbasweb.com




# Clustering Model to Filter Dishonest Recommendation Attacks using Recommendation based Trust Model in MANETs

[1]S. Saravanan, [2]M. Ramakrishnan, [3]A. Adithya Vinayak, [4]S.M. Lokesh

[1]*Assistant Professor, Computer Science And Engineering Department, R.M.K. College of Engineering and Technology, Chennai, India*
[2]*Professor, School of Information Technology, Madurai Kamaraj University, Madurai, India*
[3]*Student, Computer Science and Engineering Department, R.M.K. College of Engineering and Technology, Chennai, India*
[4]*Student, Computer Science and Engineering Department, R.M.K. College of Engineering and Technology, Chennai, India*

**ARTICLE INFO**

***Article history:***
*Received 10 March 2015*
*Received in revised from 20 March*
*Accepted 25 March 2015*
*Available online 10 April 2015*

***Keywords:***
*Mobile Ad Hoc Network, Distributed Networks, trust, clustering, routing*

**ABSTRACT**

Establishing trust among the Distributed network is a challenging task in the MANETs. The main objective of the paper is to make an efficient data delivery in the MANETs. Five attacks such as Bad mouthing, Ballot stuffing, selective misbehavior, time dependent, location dependent against trust establishment methods are identified and the defense techniques were developed. The honesty of recommending node is evaluated over a period of time to mitigate the influence of bad behavior of the same node over a time. The efficiency and the security of the MANETs are being improved. The Defense techniques were developed for the attacks and the honesty of recommending node is evaluated. We can still improve the performance and the security.

**© 2015 AENSI Publisher All rights reserved**.

**To Cite This Article:** S. Saravanan, M. Ramakrishnan, A. Adithya Vinayak, S.M. Lokesh, Clustering Model to Filter Dishonest Recommendation Attacks using Recommendation based Trust Model in MANETs. ***Aust. J. Basic & Appl. Sci.,*** *9(15): 89-92, 2015*

## INTRODUCTION

Mobile Ad hoc networks (MANETs) is a group of mobile nodes that are dynamically connected with each other by means of a wireless medium. There are many lack of security and performance measure when sending a packet from the source to the destination in the network. As it is the emerging methodology in the worldwide. They are further being derived to the VANET, iMANET, SPANs. Many researchers have proposed various model for the MANET and they either have one drawback which is only one can be considered security either the performance.

In this paper we have introduced a proposed iTrust, a probabilistic misbehavior detection scheme, for a secured DTN routing towards efficient trust establishment. The concept of the iTrust model is being introducing a periodically available trusted authority (TA) to judge the node's behavior based on the collected routing evidences and probabilistically checking. This improves the security and the efficiency of the packet delivery in the MANET.

***Related works:***

In the recent years many models are being proposed regarding the MANET security such as CORE model (Antesar Shabut, 2014) which gets the positive recommendation and remove the negative node from the network but it was not being tested in the Ballot Stuffing attack. Trust Based Intensive model (Wang, 2008) which works by reducing the impact of the false recommendation but it doesn't support the bad mouthing attack. Fuzzy model (luo, 2009) works with the help of quantify and evaluation the trustworthy of the node in the network it lack with the performance measure on the selfish nodes in the network (Soltanali, 2007) Motivate the cooperation in the node works by encouraging the cooperation between the two node in the direct observation method. (Buchegger, 2004) The personal experience of the node is being considered in this method it maintain a threshold value and it reject the node if the value fall below the threshold. The drawback of this method is that it disseminates the false recommendation.

***Attack in recommendation trust model:***

The recommendation trust model are prone to the following types of attack in order to defend from these attack we have implemented the iTrust model.

***3.1.Bad Mouthing Attack(BMA):***

In this attack, conspiring nodes propagate unfairly negative rating of good nodes with an ill intent to tarnish their reputation in the network. Such

**Corresponding Author:** S. Saravanan, Assistant Professor, Computer Science And Engineering Department, R.M.K. College of Engineering and Technology, Chennai, India.
E-mail: saran.mecse@gmail.com

collusive behavior may lead to the blocking of valid paths in the network by confusing the trust and the reputation.

### *3.2.Ballot stuffing Attack(BSA):*

Propagative of unfairly positive ratings for some poorly performing nodes by collusive node in the networks leads to ballot stuffing attack. The intention of collusive nodes is to mislead the trust mechanism and cause it to malfunction in accurately reporting the trustworthy of assessed node.

### *3.3.Selective Misbehavior Attack(SMA):*

This attack victimizes some trusted node by propagating false rating for them, while at the same time acting normal to other nodes. This type of behavior can be very difficult to detect for the trust mechanism.

### *3.4.Time-dependent Attack(TDA):*

This attack make participating node to change their behavior by time. Node can behave normally for a period of time and they may change else misbehave in the other period of time.

### *3.5.Location-dependent Attack(LDA):*

This attack exploits mobility property of the MANETs, where a node behaves differently according to its location. This attack originates from the subjective property of trust where behavior at one location cannot affect the trustworthy on the other location.

### *Proposed model:*

The existing system is as of the following. There are two common ways to establish trust in computer networks. First, when the subject can directly observe the agent's behavior, direct trust can be established. Second, indirect trust can be established when the subject receives recommendations from other entities about the agent.

Based on the previous interaction of the subject and the agent the direct trust is being established. The observation is often described by two variables: s denoting the number of successful interactions and f denoting the number of failed interactions.

Indirect Trust: Trust can transit through third parties. For example, if A has established a recommendation trust relationship with B and B has established a trust relationship with Y, then A can trust Y to a certain degree if B tells A its trust opinion (i.e. recommendation) about Y. This phenomenon is called trust propagation. Indirect trust is established through trust propagations. Two key factors determine indirect trust. The first is when and from whom the subject can collect recommendations.

Recommendation trust is a special type of direct trust. It is for trust relationship {subject: agent, making correct recommendations}. When the subject can judge whether a recommendation is correct or not, the subject calculates the recommendation trust from values, where the numbers of good and bad recommendations are received from the agent, respectively. This judgment is often done by checking consistence between observations and recommendations, or among multiple recommendations.

This existing system has the drawback of the following 1)The mobile node may experience bad channel condition at a certain location and has low trust value associated with packet forwarding.2)An incompetent entity may become competent due to environmental changes.

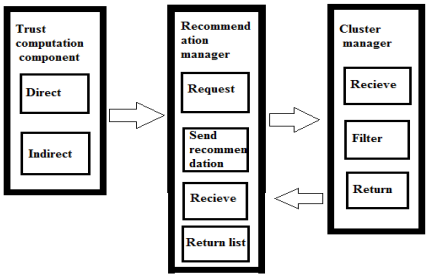



**Fig. 1:** System Architecture.

In order to overcome this drawback we have implemented a new concept iTrust model in which we compare two malicious node detection methods. In the first method, only direct and indirect trust is used. In the second case direct, indirect and recommendation trust is used. The proposed filtering technique takes the consideration of MANET characteristics that change over time. The honesty of recommending node is evaluated over a period of time to mitigate the influence of bad behavior of the same node over a time. Dynamic clustering over a period of time can filter out deviated ratings from the list of recommendations.

The iTrust model is a probabilistic misbehavior detection scheme, for the secured DTN routing mechanism towards efficient trust establishment. The main idea of iTrust based model is to introduce a periodically available trusted authority (TA) to predict the node behavior based on the collected routing evidences and probabilistically checking the node.

### *4.1. Algorithm:*

1. Initialize :
a. Initialize node memory(in packet)
b. Initialize the update timer
2. Send request for allocate replica
3. If node selfish
a. Give wrong reply or no response]
4. If not
a. Send correct reply
5. If reply is received by originator
a. Process the reply
b. And make the route

6. If timer is triggered
a. Send the query for checking
7. If node is correspond node then sends the query reply
8. Originator checks the query reply
a. And forms the SCF tree
b. And allocates priority and replica according to the tree

With the above algorithm the selfish node in the network are being eliminated based on the trust value of the node which was early evaluated.

## RESULT AND DISCUSSIONS

The simulation is being done using the open source software NS2 the performance of the proposed model has a very good variation comparing to the existing model.

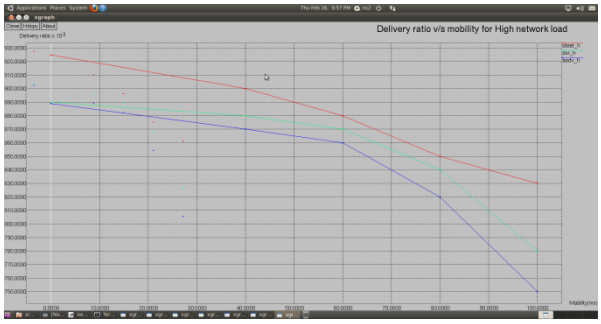



**Fig. 2:** Delivery ratio v/s mobility for high network load.

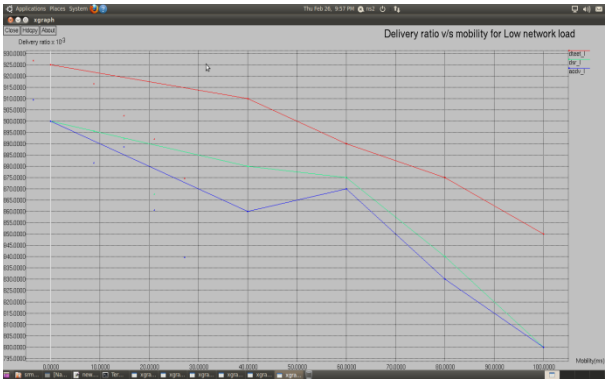



**Fig. 3:** Delivery ratio v/s mobility for low network load.

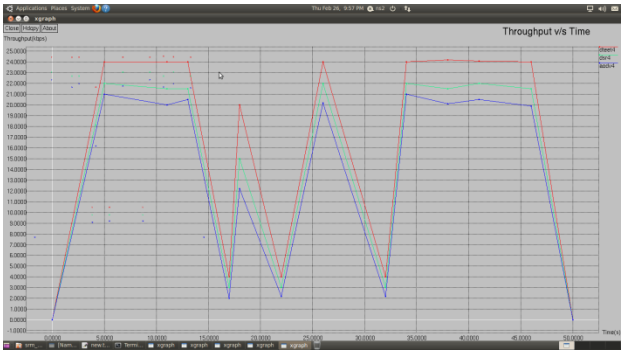



**Fig. 4:** Throughput v/s Time.

The relationship between the delivery ratio with respect to the mobility in the High network and low network load of the proposed model has a higher value than that of existing model.

The proposed model graph relation of time with respect to the energy and throughput has a positive recommendation with the existing model.

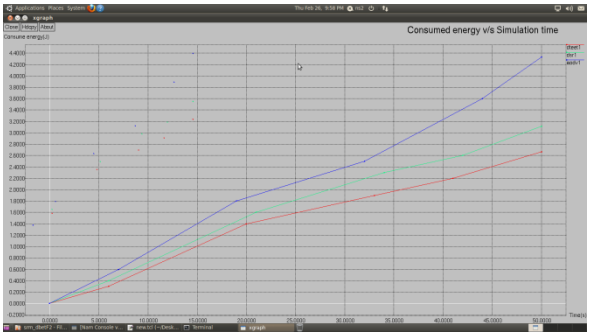



**Fig. 5:** Comsumed energy v/s Simulation time

***Conclusion:***

We know that the security in the MANETs is a challenging issue. In this paper we proposed and implemented an iTrust model which has the ability to detect the attack of the node with the direct, indirect, recommendation method and delivery the packet from the source to the destination with improved security and efficiency. Five attacks such as Bad mouthing, Ballot stuffing, selective misbehavior, time dependent, location dependent against trust establishment methods are identified and the defense techniques were developed. The Effectiveness of the attacks and the defense is demonstrated in the scenarios of securing routing protocols and detecting malicious nodes in MANET. As of the future works we can still improve the security of the MANETs.

## ACKNOWLEDGMENT

For all the effort behind this paper work, first & foremost, I would like to express our sincere appreciation to the staff of Computer Science and Engineering Department, for their extended help 7 suggestion at every stage of this paper. It is a great sense of gratitude that I acknowledge the support and time to time suggestion provided by my highly indebted guide Professor Dr. M.RAMAKRISHNAN and to my respected head of department (HoD) Dr.N.SANKAR RAM. Finally, I Pay sincere thanks to all those who directly and indirectly helped me towards the successful completion of this paper.

## REFERENCES

Antesar Shabut, M., P. Keshav Dhal, K. Sanat Bista, U. Irfan Awan, 2014. ”Recommendation Based trust model with an efficient defence scheme for MANETs” Mobile computing, IEEE transaction.

Buchegger, S. and J.Y. Le Boudec, 2004. ”A robust reputation system for P2P and mobile ad hoc networks”, proc.P2PEcon’04.

Cho, J.H., A. Swami and R. Chen, 2011. ”A survey on trust management for mobile ad hoc network”, communication survey & tutorials, IEEE, 13: 562-583.

Li, W., J. Parker and A. Joshi, 2012. ”Security through collaboration and trust in manet”, Mobile networks and application, pp: 342-352.

luo, J., X. Liu and M. Fan, 2009. “A trust model based on fuzzy recommendation for mobile ad-hoc network”, computer networks, 53: 2396-2407.

Michiardi, P. and R. Molva, 2000. CORE: ”A Collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks”, communication and multimedia security conference, pp: 107-121,202.

Shengbo Yang, Chai Kiat Yeo and Bu Sung Lee, 2012. “Toward Reliable Data Delivery for Highly Dynamic Mobile Ad Hoc Networks”, IEEE Transactions on mobile computing, Vol. 11, No. 1.

Soltanali, S., S. Pirahesh, S. Niksefat and M. Sabaei, 2007. ”An efficient scheme to motivate coopeation on mobile ad hoc networks”, pp: 98-98.

Wang, K., M. Wu and S. Shen, 2008. “A trust evaluation method for node cooperation in mobile ad hoc network”, Information technology:new generation, pp: 1000-1005.