iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** I **Month of publication:** January 2018

DOI: http://doi.org/10.22214/ijraset.2018.1446

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

Outlier Nodes Detection in MANET's: A Trust Management Approach.

Renu Popli[1], Dr. Kanwal Garg[2], Sahil Batra[3]
[1, 2, 3]*DCSA, KUK, GIMT, KANIPLA*

Abstract: ***In MANETs due to lack of pre-deployed infrastructure, there is a need of cooperation among nodes for achieving any kind of network operations. But sometimes nodes refuse to cooperate because of some selfish or malicious purposes. Such types of misbehaviors in the network recognized as outliers. Outlier detection in MANETs deals with detection of all kind of misbehaving nodes which do not work properly due to selfishness or malicious intentions. To identify these outlier nodes, an algorithm is proposed which is based upon trust management in the network. The algorithm calculates trust value of each node in the network and the nodes which have lowest trust values are selected as outlier nodes. The effectiveness of the algorithm is proved by showing results in different simulation runs.***
Keywords: MANET, Routing, Outlier node, Trust, Classifier, Security.

I. INTRODUCTION

Mobile ad hoc networks consist of mobile devices communicating over wireless links without any support from a fixed infrastructure. Mobile ad hoc networks are applicable to a wide variety of applications[9]that includes disaster recovery or tactical communication, connection of multiple mobile users in an area at low cost with the use of laptops, portable devices such as PDAs (Personal Digital Assistants), mobile phones, media players, etc. An important property of ad hoc network is the multi-hop capability. A mobile node, which lies outside the transmission range of its specific destination, would need to relay its information flow through other mobile nodes. This implies that mobile nodes in ad hoc networks bear routing functionality so that they can act both as routers and hosts. An ad hoc network can be deployed in an area where support for mobile communication is not available, probably due to high deployment costs or disaster destruction. The typical application of ad hoc networks includes battle field communication, emergency relief etc.

Establishing trust[13] among distributed network nodes is considered as effective mechanism to deal with node's misbehavior. The examples of misbehavior are - not forwarding packets, selective packet dropping, packet modification, message fabrication, false route advertisements, fake link break messages, and timing misbehavior like adding delay in the communication. As the proportion of misbehaving nodes increases, it results into decreased network throughput and network partitioning. Outlier detection in MANETs deals with all kinds of misbehavior and selfish activities [12] in the network.

In this paper, a trust based outlier detection algorithm is proposed for mobile ad hoc networks. In this approach, each node observe and record the abnormal behavior of their neighboring nodes. Based on the observations, trust value is calculated for the neighbors. In the next stage, the trust information is exchanged between immediate neighbors. After getting the trust information from other nodes, each node then updates its own trust data set. The updated trust information is further exchanged with the neighbors. The process continues, till there are no more updates.

The rest of the paper is organized as follows: in section II, a survey of related work is given. In section III, outlier detection algorithm is proposed. The effectiveness of the algorithm is presented in section IV through simulation. And conclusion is given in section V.

II. LITERATURE SURVEY

The existence of selfishness and malicious behaviors has motivated research in the area of misbehavior detection for mobile ad-hoc networks. Besides misbehavior detection, trust management is another well-studied method that can be used to secure MANETs. The main purpose of trust management is to evaluate the behaviors of other nodes, and thus build a reputation for each node based on the result of behavioral assessment.

Blaze et al. [8] justified that for communication systems, the trust management problem is an important part of security. There are a various approaches to trust management in MANETs that suits well for their adaptive and self-organizing nature. Sun Y.L. et al.

[15] presented an information theoretic framework to quantitatively measure trust and model trust propagation in ad hoc networks. In the proposed framework, trust is a measure of uncertainty with its value represented by entropy.

H. Luo et al. [4] proposed a trust model, in which an entity is trusted if any K trusted entities claim so within a time period. The number K is determined using number of legitimate neighbors, service availability and the current state of the network. In some scenarios, this coupling may result in conflicting goals. A scheme proposed by A. Weimerskirch and G. Thonet [2] makes use of references and recommendations to derive a trust relationship. Other works such as [5], [7], [10], and [11], narrow down their scope to authenticated routing schemes for MANETs using cryptographic schemes.

A. Pirzada and C. Macdonald [1] proposed a distributed trust model that provides a system for measurement of reliability and trustworthiness of a node in an ad hoc network. However, the scheme does not take the limitations of a device into consideration when computing trust.

In order to reduce the adverse effects of misbehaving nodes an acknowledgement based 2ACK scheme is proposed byK Balakrishnan et al. [6]. Here the strategy is: when some data is forwarded by a node through the next hop, the next hop connection's destination node sends back an uncommon two-bounce affirmation called 2ACK to demonstrate that the information packet has been received positively. Misbehavior is identified by applying a hash code authentication mechanism.

In order to analyze the dynamic communication between regular nodes and misbehaving nodes, an efficient framework is designed by Sumati Ramakrishna Gowda et al. [14]. In this framework, regular nodes do cooperation and takes decision based on the belief system whereas the misbehaving nodes identifies the risk of being caught and behave accordingly. The proposed framework provided a solution of mixed strategy to achieve equilibrium.

Wenjia Li and Anupam Joshi [16] analyzed that both the malicious behaviors and the faulty behaviors are generally equally treated as misbehaviors by most of the traditional misbehavior detection mechanisms. They developed a policy based malicious node detection scheme in which a context information is added to distinguish both type of nodes. A multi-dimensional trust management scheme is deployed in SMART[18] to better assess the trustworthiness of nodes in MANETs. Compared to the traditional single-dimensional trust management mechanisms, the trustworthiness of a node is judged from different perspectives and each perspective of the trustworthiness is derived from different sets of misbehaviors according to the nature of those misbehaviors.

Wenjia Li et al. [17] proposed and evaluated a collaborative, gossip-based outlier detection algorithm for mobile ad hoc networks. In this approach, all the nodes in MANETs observe the behavior of their neighbors. Each node calculates its local view of outliers amongst the neighboring nodes. In the next step, the nodes exchange their local views with their immediate neighbors. Then they will update their local views if they find that outlier lists from other nodes are more accurate than theirs. This process continues, with each node updating its neighbors when it's current view of the outliers changes, and halts when there are no more changes.

III. PROPOSED WORK

Here the aim is to identify outlier nodes from the mobile ad hoc network. This is accomplished collectively in three layers given below. Each layer has its specific task in achieving the objective.

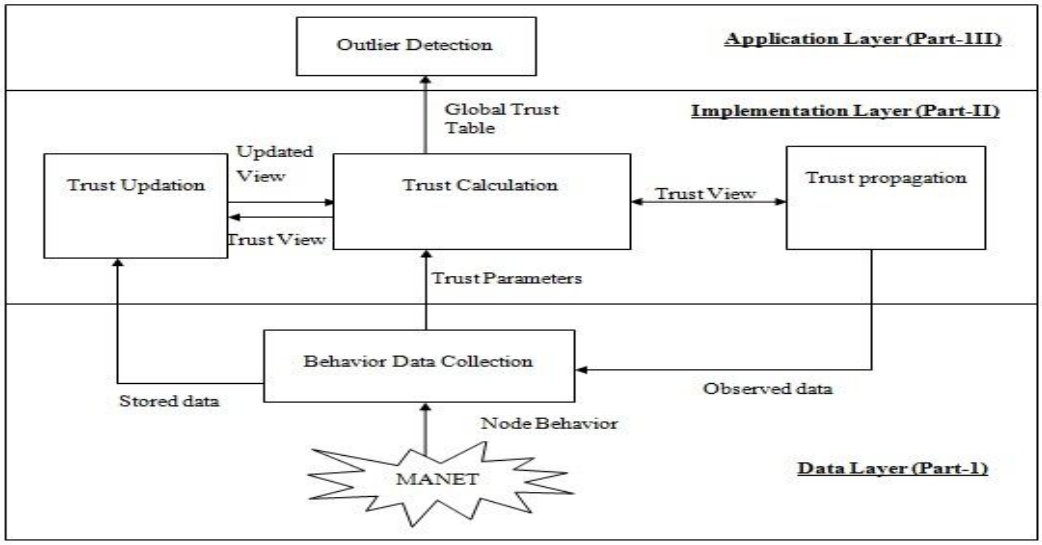


Figure 1: Three layer structure of outlier detection in MANETs

The description of each layer is given below:

A. Data layer

In this layer, each node in the network collects data based on behavior of the nodes. Data is collected in the form of various parameters which are used to compute trust value. Three parameters are taken to evaluate trust value. These are packet drop rate(PDR), packet modification rate(PMOR), and packet misroute rate(PMIR) and can be defined as follows :

$$PMOR = \frac{\text{no. of packets modified}}{\text{total no. of packets}}$$

$$PMIR = \frac{\text{no. of packets misrouted}}{\text{total no. of packets}}$$

$$PDR = \frac{\text{no. of packets dropped}}{\text{total no. of packets}}$$

B. Implementation layer or trust layer

This layer deals with trust generation, trust exchange and updation.

1) *Trust generation*: Trust is generated based upon the collection of data from the data layer. Trust is collected based on three dimensions which are knowledge, experience and recommendations. The trust is calculated as follows:

$$T_{A,B}=F(K_{A,B},E_{A,B},R_{A,B})$$

Here trust of node A over node B is defined as a function containing three parameters. Each node calculates its trust over its neighboring nodes by using the three parameters which are calculated in data layer. This type of trust is called direct trust and it constitute the knowledge part of trust function. For calculating experience value, the data set is fed into the KNN classifier which reasons about the stored information and helps in classifying the trustworthy and untrustworthy nodes. The classification is fully based upon the past observations and the results are stored in the classifier. KNN classifier is the most accurate classifier in identification of outlier nodes with an accuracy rate of 99.5%[3]. The recommendations from the neighboring nodes helps in achieving the improved trust value. There commendations improve the trust evaluation process for nodes that do not succeed in observing their neighbors due to resource constraints or link outages. For calculating recommendations, there is one common neighbor of different nodes.

2) *Trust propagation and updation:* After generating trust value of the neighboring nodes, trust is exchanged with the neighboring nodes .Instead of forwarding the trust information to all nodes in the network, it is exchanged with the neighbors only which helps in reducing the congestion in the network. Based upon the obtained trust data set, each node updates its trust data set to obtain the trust information of all nodes in the network. The algorithm T_merge is given below for updating trust.

C. Application layer

This layer deals with identification of nodes which are not working properly in the network. This identification is based on the datasets obtained from the implementation layer. From the data sets the nodes are arranged in the increasing order of their trust values. The top k no. of nodes are stated as outlier nodes. The value of k is application specific.

1) *Algorithm for identifying outlier nodes in MANETs:* Here an algorithm is proposed for the identification of outlier nodes in a mobile ad hoc network. The network consists of n nodes out of which k outlier nodes are identified.
2) *Input parameters:* PDR,PMIR,PMOR, Total no. of nodes (n), No. of outlier nodes (k)
3) *Output parameters:* list of outlier nodes in the network
4) *Outlier Detection Algorithm in MANET(OUTM)*:

Steps:

At every node in the network, do the following:

Step 1: Generate trust table of its neighbors.
Step2: Exchange trust table with its neighboring nodes.
Step 3: trust tables are updated according to trust updation algorithm (T_merge)
If Updated table= previous trust table
then
Global Trust Table(GTT) is obtained.
else
goto step 2

Step4: Select top K nodes as outlier nodes.
Step: Stop

T_merge: T_merge is an algorithm for merging the table at a node with its neighboring tables and as a result, tables are updated.
Input parameters: Trust table T_A
Output parameters: Updated trust table T_A'
Upon reception of T_B
T_merge(T_A,T_B)
Steps:

Step 1:Merge T_A and T_B according to the following rules:
case1: If node m is in both T_A and T_B, then
take average of the two values and add its entry to the table T_A'
case 2: If node m is in either of T_A or T_B, then
add an entry of m to the table T_A'
Step 2: Stop.

IV. SIMULATION RESULTS AND COMPARISON

The proposed algorithm (OUTM) is simulated by using MATLab as a simulation tool. While simulating the algorithm k nodes are presented as outlier nodes among n nodes. And the results are obtained in various simulation runs. For evaluating performance of the algorithm, three parameters are chosen. These parameters are:

1) *Precision:* it is the fraction of retrieved data that are relevant to the query.
2) *Recall:* it is the fraction of data that is relevant to the query that is successfully retrieved.
3) *Fmeasure:* it is a balanced score that combines precision and recall by harmonic mean.

These parameters are calculated as follows:

$$\text{Precision} = \frac{\text{Relevant Data}}{\text{Retrieved Data}}$$

$$\text{Recall} = \frac{\text{Retrieved Data}}{\text{Relevant Data}}$$

$$\text{Fmeasure} = \frac{(2 * \text{precision} * \text{recall})}{(\text{precision} + \text{recall})}$$

To prove effectiveness of the algorithm the proposed algorithm is compared with an outlier detection approach SMART described in section 2. The proposed work is simulated under the following simulated environment:

Table 1
SIMULATION PARAMETERS

Simulation parameters	Values
Network area	100x100
Total no. Of nodes	50
Transmission range	60m
Simulation time	10 units
No. Of malicious nodes	5,10,20

After simulation the results are obtained as follows:

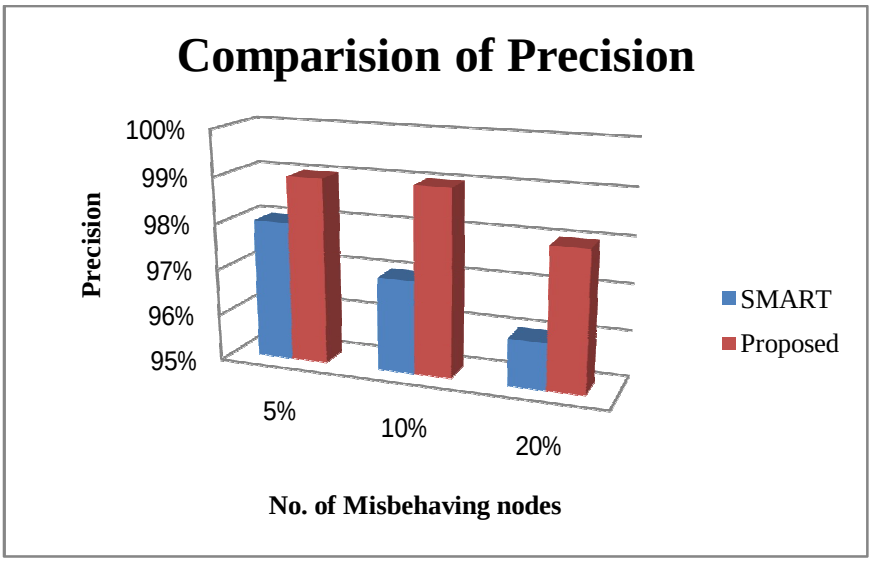


Figure 2:Effect of percentage of misbehaving nodes over precision

Figure 2 and figure 3 explains that as the percentage of malicious nodes increases, the precision as well as recall value of proposed algorithm and SMART gets reduced. This is true because it is more likely to receive incorrect messages from others when there are a higher number of misbehaving nodes. But the proposed algorithm still has higher precision and recall values as compared to SMART.

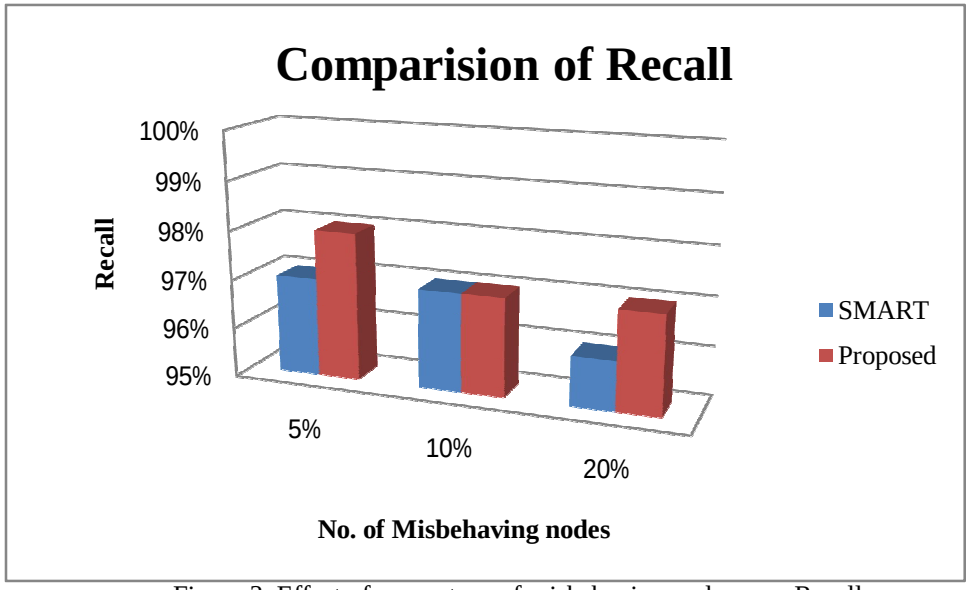


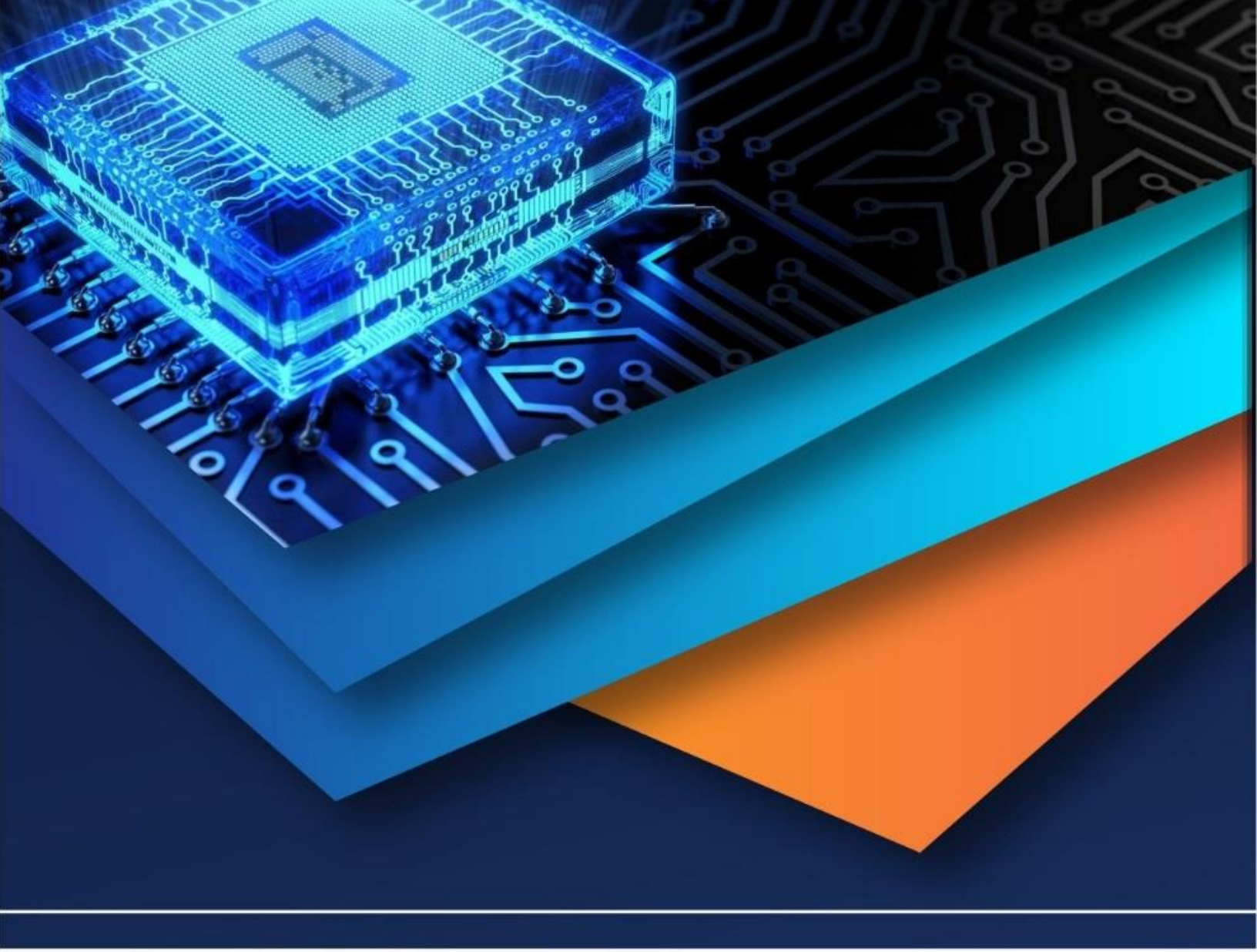
Figure 3: Effect of percentage of misbehaving nodes over Recall

III. CONCLUSION

In MANETs, an outlier node is described as a node which does not work properly in the network. The inadequate nature of the nodes may be due to some selfishness or malicious reasons. Trust management is the most effective scheme used recently to provide security in mobile ad-hoc networks. In this paper an algorithm is proposed to detect outlier nodes by using the approach of trust management. A multi-dimensional trust based on knowledge, experience and recommendation is calculated. Global trust is generated at every node which contains trust information about all the nodes by exchange of local trust information among neighboring nodes in the network. The nodes which have low trust values are recognized as outliers. The proposed algorithm is simulated and compared with an existing algorithm of outlier detection in MANETs. The result shows the improvement in identifying malicious nodes out of total nodes in MANET.

REFERENCES

[1] A.Pirzada and C. Macdonald.,"Establishing Trust in Pure Ad Hoc networks.", In Proc. of 27th Australasian Computer Science Conference (ACSC'04), Dunedin, New Zealand, 26(1), pages 47-54, January 2004.
[2] A. Weimerskirch and G. Thonet., "A Distributed Lightweight Authentication Model for Ad Hoc Networks.", In the Proc. of the Fourth International Conference on Information Security and Cryptology, Korea, December 6-7, 2001.
[3] Ali Feizollah, Nor BadrulAnuar, RosliSalleh, FairuzAmalina, Ra'ufRidzuanMa'arof, ShahaboddinShamshirband," A Study of Machine Learning Classifiers for Anomaly-Based Mobile Botnet detection", Malaysian Journal of Computer Science. Vol. 26(4), 2013, pp251-265.
[4] H. Luo, P.Zerfos, J. Kong, S.Lu, and L. Zhang. "Self Securing Ad Hoc Wireless Networks.", In Proc. Of The Seventh IEEE Symposium on Computers and Communications (ISCC) Italy, July 1-4, 2002.
[5] J. Binkley and W. Trost. ,"Authenticated Ad Hoc Routing at the Link Layer for Mobile Systems.", Wireless Networks 7, pages 139-145, 2001, Kluwer Academic Publishers.
[6] K Balakrishnan, J Deng, and P K Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks", Proc. IEEE Wireless Comm. And Networking, pp. 2137- 2142, 2005
[7] L. Venkatraman and D.P. Agrawal.. "An Optimized Inter- Router Authentication Scheme for Ad Hoc Networks." , In Proc. Of the 13th International Conference on Wireless Communications, pages129-1, Calgary, Canada, July 2001.
[8] M. Blaze, J. Feigenbaum, and J. Lacy., "Decentralized trust management.", In Proc. of the 17th IEEE Computer Society Symposium on Security and Privacy, 1996, pp. 164–173.
[9] Okeke, S. S. N., Nwabueze, C. A, "Mobile Ad hoc Network (MANET) Architecture And Implementation Analysis", Natural and Applied Sciences Journal 2010, Vol. 11 No. 1.
[10] P. Papadimitratos and Z. J Haas., "Secure Routing for Mobile Ad Hoc Networks." In Proc. of the SCS Communication Networks and Distributed Systems Modeling and Simulations Conference, San Antonio, TX, January 27-31, 2002.
[11] S. Marti, T. Giuli, K. Lai, and M. Baker.,"Mitigiating Routing Misbehavior in Mobile Ad Hoc Networks.", In Proc. Of the ACM International Conference on Mobile Computing and Networking (MobiCom), 2000.
[12] S.Sugitha, M.Preetha, "A Survey on Misbehavior Report Authentication Scheme of Selfish node Detection Using Collaborative Approach in MANET", IJECS,2016,vol. 6, issue 5, pp 5381-5384.
[13] Sandeep A. Thorat, P. J. Kulkarni," Design Issues in Trust Based Routing for MANET", 5th ICCCNT – 2014, Hefei, China
[14] Sumati Ramakrishna Gowda, P.S Hiremath, Sumati, "SMBP: Framework For Surveillance Of Malicious Behavior Pattern In Mobile Ad-hoc Network", International Journal of Advanced Research in Computer Science and Software Engineering 3(11), November - 2013, pp. 520-528
[15] Sun Y.L., Wei Yu , Zhu Han ,Liu, K.J.R., "Information theoretic framework of trust modeling and evaluation for ad hoc networks", Selected Areas in Communications, IEEE , 2006 ,vol. 24 , Issue 2, pp. 305 – 317.
[16] Wenjia Li and Anupam Joshi, "Outlier Detection in Ad Hoc Networks Using Dempster-Shafer Theory", IEEE, Tenth International Conference on Mobile Data Management: Systems, Services and Middleware,2009, pp-112-121.
[17] Wenjia Li, Anupam Joshi and Tim Finin, "Coping With Node Misbehaviors In Ad-hoc Networks: A Multi- Dimensional Trust Management Approach", Eleventh International Conference on Mobile Data Management, IEEE 2010.
[18] Wenjia Li, Anupam Joshi, and Tim Finin," SMART: An SVM-based Misbehavior Detection and Trust Management Framework for Mobile Ad hoc Networks", UMBC TECH REPORT CS-TR-11-01.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY