International Journal of Electrical Electronics & Computer Science Engineering
Volume 5, Issue 1 (February, 2018) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

Outlier Detection using Data Mining in Trust Based Clustered MANET's

Renu Popli[1], Dr. Kanwal Garg[2], Sahil Batra[3]
[1]Ph.D Scholar, [2]Assistant Professor, DCSA, Kurukshetra University, Kurukshetra, Haryana, India
[3]Assistant Professor, GIMT Kanipla, Kurukshetra, Haryana, India
[1]renu_popli@yahoo.co.in,[2]gargkanwal@gmail.com,[3]sahil.batra23@gmail.com

Abstract: ***Due to lack of pre-deployed infrastructure, nodes in MANETs are required to relay data packets for other nodes to enable multi-hop communication between nodes that are not in radio range with each other. However, whether for selfish or malicious purposes, a node may refuse to cooperate during the network operations or even attempt to interrupt them, both of which are recognized as misbehaviors. In general, this problem can be viewed as an instance of detecting nodes whose behaviour is an outlier when compared to others. In this paper, a classifier approach of data mining is used to classify outlier nodes and regular nodes in MANETs. The algorithm uses trust management to mitigate the security loopholes caused by various misbehaviors in clustered MANETs. Clustering of nodes in MANETs helps in effective utilization of resources. To validate the proposed model, an extensive performance study is conducted using MATLab simulator. The results show that the proposed model outperforms the previous schemes.***

Keywords: MANET, Data Mining, Outlier, Trust, Classifier, Cluster Head.

I. INTRODUCTION

Mobile Ad-Hoc Networks (MANETs) is a collection of wireless mobile nodes dynamically forming a temporary network without the use of existing network infra-structure or centralized administration [4]. In such a network, each mobile node operates not only as a host but also as a router, forwarding packets for other mobile nodes in the network. MANETs are highly vulnerable to attacks than wired networks due to the open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and lack of a clear line of defense [13].

Clustering of nodes within the network helps in better utilization of resources by reducing the amount of information propagated inside the network. The idea behind clustering is to group the network nodes into a number of overlapping clusters. Basically 3 types of nodes are present in a cluster.

i) Cluster Head-It is a leader node that is responsible for managing nodes within a cluster and co-ordinate with other clusters by providing inter and intra cluster communication.

ii) Cluster Member-these are ordinary nodes.

iii) Cluster Gateway-is a non cluster head node with inter cluster links. Its main purpose is to provide inter cluster communication among nodes in different clusters.

In this proposed system, the nodes trust value is generated using three different perspectives of trust. The trust is based on previous individual experiences of the node and on the recommendations of its neighbors. The recommendation improves the trust evaluation process for nodes that do not succeed in observing their neighbors due to resource constraints or link outages. The ability of assessing the trust level of its neighbors brings several advantages. First, a node can detect and isolate malicious behaviors, avoiding relaying packets to malicious neighbors. Secondly, cooperation is encouraged by selecting the neighbors with higher trust levels.

This method is effective and every node in the cluster maintains the table about node's behaviour of their neighboring nodes. By this way the malicious nodes are identified in the cluster in efficient manner.

II. LITERATURE STUDY

In mobile ad hoc networks, the existence of selfishness and malicious behaviour has motivated the research in the area of outlier detection in mobile ad hoc networks. Trust management is another well studied method that can be used to secure MANETs. The main aim of trust management is to evaluate the behaviour of other nodes, and thus build a reputation for each node based on the result of behavioral assessment. The selection of outlier nodes in Clustered MANETs involve selection of outlier node within cluster and inter clusters. The literature work regarding trust management and outlier detection in clustered MANET is given below:

An information theoretic framework was presented in [9], to quantitavely 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.

A collaborative, gossip based outlier detection algorithm in mobile ad hoc network was introduced by [12]. In this, each node observes the behaviour of their neighbours and generate a local view of their outliers among neighbours. This local view is then exchanged among neighbours and then there will be updation in their local views if outlier node list from other nodes is found to be more accurate.

International Journal of Electrical Electronics & Computer Science Engineering
Volume 5, Issue 1 (February, 2018) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

They also differentiate malicious behaviour from faulty behaviour in their policy based mechanism [11]. In policy based misbehavior detection approach, context information about nodes is used to determine whether the misbehavior is because of malicious activity or not.

A trust model based on human trust was developed by [3]. The trust is based on the previous individual experiences and on the recommendations of others. The authors introduced the concept of relationship maturity which makes the model very efficient in mobile scenarios. But the trust calculation is limited to the neighborhood only, within the radio range of a node. There is no information provided about the global trust value.

A multi-dimensional trust management framework was defined in [10] to introduce three different dimensions of trust to better evaluate the trustworthiness of nodes in MANETs. Each dimension justified a specific behaviour of node such as cooperation, well behaving and honesty.

The concepts and properties of trust was defined by [5] and they derived some unique characteristics of trust in MANETs. In this, correlation between social trust and node trust is described by providing a survey of various trust management schemes developed for MANETs.

A distributed trust-based framework was introduced by [1]. Their proposed mechanism reduces the likelihood of compromised nodes or malicious nodes from being selected as cluster heads. They have introduced a framework and a mechanism to address a potentially significant security breach.

The authors in [2] presented a scheme that helps in accurate diagnosis of malicious attacks in ad hoc networks. Their scheme employs crosslayer interactions based on observations at various networking layers to decrease the number of false positives.

The concept of cluster based algorithm was extended by [7] and they evaluated the cluster based algorithm for trust authority distribution in tactical mobile ad hoc networks. The two crucial points for the communication overhead are the number of changes of TA nodes and the frequency of the cluster algorithm messages.

A trust based self-organizing clustering algorithm was proposed by [6] they have used the trust evaluation mechanism depending on the behaviour of a node towards proper functionality of the network. The originality of their work consists of combining different metrics for quantifying trust and the use of Dempster-Shafer theory in order to predict the trust of mobile node more accurately.

III. PROPOSED WORK: IDENTIFICATION OF OUTLIER NODE BASED ON CLASSIFIER USING TRUST IN CLUSTERED MANET

In this, a model is proposed to detect the outlier node in the clustered MANET. First of all, network is divided into clusters and cluster head is selected in every cluster. Every CH generates a trust table of their cluster members and exchanges it with other CHs in the network. At every CH, the trust table is updated to generate global trust table out of which outlier nodes are selected. These three steps are shown below:

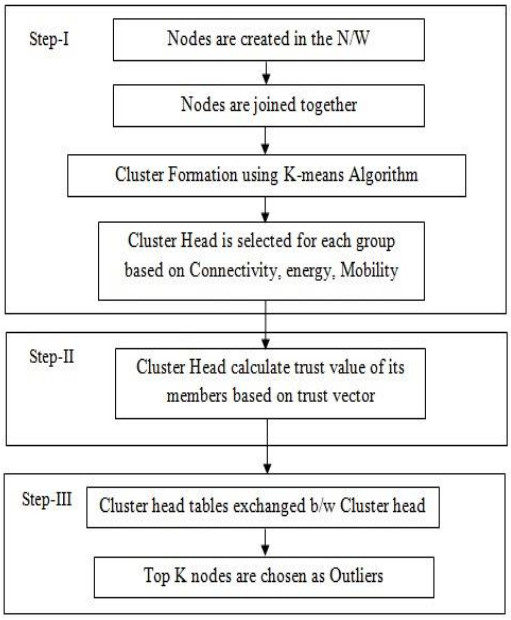

Fig. 1. Model to Detect the Outlier Nodes

The core components of the proposed work are:

- Cluster formation
- Trust generation at CH
- Global outlier detection

A. Cluster Formation:

The concept of K-mean algorithm is used for making clusters. In data mining, k-means clustering is defined as: Given a set of n data points in d-dimensional space R_d and an integer k and the problem is to determine a set of k points in R_d, called centers, so as to minimize the mean squared distance from each data point to its nearest center. The advantage of using K-mean in MANETs is to obtain manageable and distributed clusters which will cover all the nodes in the network. To extract maximum utilization of resources, it is desired that the nodes should be fully connected to their cluster heads i.e. connectivity of cluster

International Journal of Electrical Electronics & Computer Science Engineering
Volume 5, Issue 1 (February, 2018) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

head should be high within cluster as well as CH energy should be high. A node closest to centre is having the highest connectivity with all the nodes in the cluster.

The main features of clustering model are:

1. Clusters are formed based on K-mean approach.
2. Cluster head is a node nearest to the center of the cluster. Cluster head is chosen based upon the following parameters:
   a) Strong connectivity
   b) High energy
   c) High trustworthiness
3. Cluster head maintains the behaviour of its cluster members.

B. Trust Generation:

At each CH, trust table of cluster members is maintained. Trust is generated by using vector model of trust. The vector model of trust is defined as follows:

Trust vector of node A to node B is:

$V(A \rightarrow B) = [{}_AE_B, {}_AK_B, {}_AR_B]$

Where ${}_AE_B$, ${}_AK_B$, ${}_AR_B$ are node A's evaluation of experience, knowledge and recommendation to node B, respectively. These are also called three dimensions of trust.

In order to normalize trust vector, trust weight vector is introduced. The elements of weight vector are real numbers in the range [0,1] and the sum of all elements is equal to 1.

The normalization of trust vector can be defined as

${}_AT_B = W_E * {}_AE_B + W_K * {}_AK_B + W_R * {}_AR_B$

Where W_A is node A's trust weight vector which consists of three weight elements according to three dimensions of trust vector respectively. ${}_AT_B$ is single trust value of node A on node B corresponding to the normalized trust vector. In other words we define trust as the value that reflects the behaviour history i.e. experience that a node has about a specific neighbor. This information is used as an expectation of its neighbor future behaviour. The experience is calculated by using output of the KNN classifier which provides decision based on the past observations. This definition is extended to include recommendations of others as well. Therefore similar to the concept of human trust, the computation of the trust level of a given neighbor is based on previous experiences and also on the opinion of other neighbors.

C. Global Outlier Detection:

This subsection describes intra-cluster outlier detection and inter-cluster outlier detection. CH is responsible for managing all the communications. CH talks to its own cluster members to generate trust table of cluster nodes and then CH talks to other CHs in the network to update their tables into global trust table. The algorithm of global outlier detection is given below:

Input: no. of clusters, no. of nodes, cluster head
Output: list of outlier nodes in the network

Step 1: At every node within a cluster, do the following:
a) Generate behaviour table of the neighbors
b) Send their tables to their CH
Step2: At every CH, do the following:
a) Generate trust table of their neighbors using three dimensional trust.
b) Exchange their trust tables with other clusters in the network.
c) Trust tables are updated according to the trust updation algorithm.
If Updated trust table= previous trust table
then
Global Trust Table(GTT) is obtained.
else
goto step1
Step3: Sort the GTT in increasing order.
Step4: Generate list of outlier nodes by selecting top k nodes.
Step5: Add the outlier nodes to the black list.

Fig. 2. Algorithm of Global Outlier Detection

IV. SIMULATION RESULTS

The correctness of the proposed model is presented through simulation. We use MATLAB as the simulation tool. An analysis of the impact of the most relevant parameters on the trust level evaluation process is performed. Three parameters for evaluating performance are:

Precision: it is the fraction of retrieved documents that are relevant to the query.

Recall: it is the fraction of the document that is relevant to the query that is successfully retrieved.

Fmeasure: it is a balanced score that combines precision and recall by harmonic mean.

These parameters are calculated as follows:

International Journal of Electrical Electronics & Computer Science Engineering
Volume 5, Issue 1 (February, 2018) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

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

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

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

The proposed work is simulated under the following simulated environment:

Table1. Simulation Parameters

Simulation Parameters	Values
Network Area	100x100
Total No. of Nodes	50
Transmission Range	60m
Simulation Time	10 Units
Speed	10m/S
No. of Malicious Nodes	5,10,20

The performance of proposed model is observed and compared with our previously proposed algorithm OUTM [8] of outlier detection in MANET under different simulation scenarios. To evaluate the performance of the proposed model, observations are taken by varying percentage of misbehaving nodes. The simulation results are shown in figure 3, figure 4 and figure 5 below.

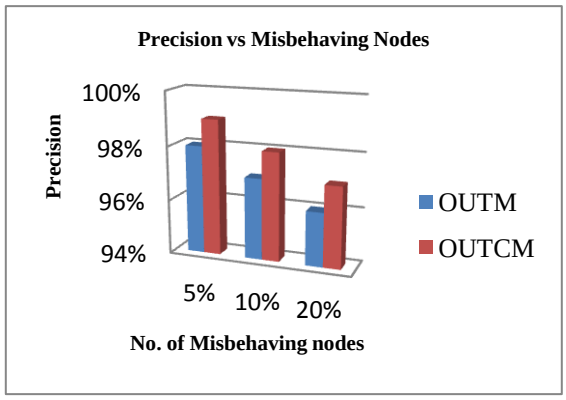

Fig. 3. Effect of Misbehaving Nodes Over Precision

The simulation results show that:

1. In general, proposed model achieves a good performance in terms of accuracy by correctly detecting outlier nodes, even when no. of misbehaving nodes in the network increases.
2. The proposed algorithm has reduced the time to generate list of outlier nodes as the amount of computations at every node gets reduced.

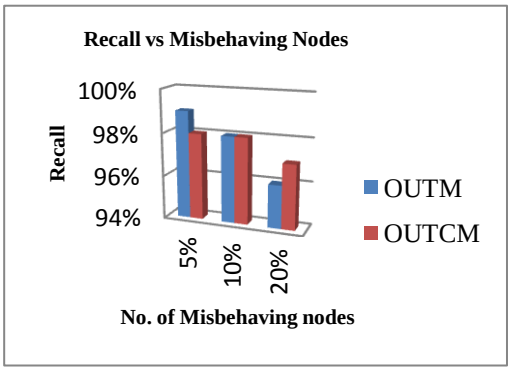

Fig. 4. Effect of Misbehaving Nodes Over Recall

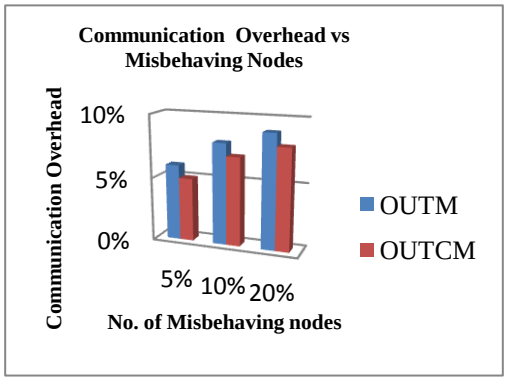

Fig. 5. Effect of Misbehaving Nodes Over Communication Overhead

It is assumed that if there are n no. of nodes in the network and on an average every node has m no. of neighbors then the computation time required to generate the trust table at every node is t1=n*m*p where p is the time taken to calculate trust parameters. After clustering, if there are k no. of clusters and each cluster is having on an average l no. of cluster members then the computation time required to generate the trust table is t2=k*(l-1)*p where t2<t1 as k<n.

V. CONCLUSION

The proposed algorithm is able to identify outlier nodes using trust values of the nodes in cluster based MANETs. The clusters are formed using K-mean algorithm which results into generation of k cluster centers with which nodes are attached. The node which is nearest to the cluster center is taken as CH based upon two parameters: energy and connectivity. CHs maintains trust table of their cluster members. The trust value is evaluated by using three different perspective of the trust: knowledge, experience and recommendations. The trust tables are

exchanged among all CHs in the network and are updated into global trust tables. The list of k outlier nodes are selected from the global trust table which are added to the black list. The nodes which are added to the black list do not participate in the CH selection further. The accuracy of the proposed work is measured by finding precision, recall and fmeasure values of the algorithm and simulation results shows improved performance under different scenarios.

In future, Some specific types of attacks may be included. Efforts can be included to eliminate the outlier node.

VI. REFERENCES

[1] Crosby, G., Pissinou, N. and Gadze, J. 2006. A framework for trust-based cluster head election in wireless sensor networks. Proc. of DSSNS, 10-22.

[2] Jim Parker, Anand Patwardhan, and Anupam Joshi. 2006. Detecting wireless misbehaviour through cross-layer analysis. Proc. of CCNC. 30-36.

[3] Pedro B. Velloso, Rafael P. Laufer, Daniel de O. Cunha, Otto Carlos M. B. Duarte, and Guy Pujolle, "Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model", IEEE Transactions on Network and Service Management, vol. 7, no. 3, september 2010.

[4] Prasant Mohapatra , Davis Srikanth V. Krishnamurthy, "Ad hoc networks Technologies and P rot ocols"2005.

[5] Prasanta Gogoi, D.K. Bhattacharyya, B. Borah and Jugal K. Kalita, "A Survey of Outlier Detection Methods in Network Anomaly Identification", The Computer Journal, Vol. 54 No. 4, 2011.

[6] Pushpita Chatterjee. 2009. Trust based clustering and secure routing scheme for mobile ad hoc networks. International Journal of Computer Networks and Communications, 1(2), 84-97.

[7] Reidt, S. and Wolthusen, S. 2007. An evaluation of cluster head TA distribution mechanisms in tactical MANET environments. Proc. of ITANIS, 27-36.

[8] Renu Popli, Dr. Kanwal Garg, Sahil Batra, "Outlier Nodes Detection in MANET's: A Trust Management Approach.", Volume 6, Issue I, International Journal for Research in Applied Science and Engineering Technology (IJRASET) Page No:-3216-3221, ISSN : 2321-9653, www.ijraset.com.

[9] 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 Journal on Feb. 2006 ,Volume:24 , Issue: 2, pp. 305 – 317.

[10] 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.

[11] Wenjia Li, Anupam Joshi and Tim Finin, "Policy-Based Malicious Peer Detection In Ad-hoc Networks.", In Proceedings of 12th IEEE International Conference on Computational Science and Engineering, CSE 2009, Vol. 3, pp. 76–82.

[12] Wenjia Li, James Parker, Anupam Joshi, "Security Through Collaboration And Trust In MANETs", Mobile Networks and applications, springer, Vol. 17 Issues 3, June 2012, pp. 342-352.

[13] Yuvraj Singh and Sanjay Kumar Jena, "Intrusion Detect ion System for Det ect ing Malicious Nodes in Mobile Ad hoc Networks", Internat ional Conference on Parallel, Dist ributed Comput ing technologies and Applicat ions (PDCTA-2011), V0L. 203 CCIS , pp. 410- 419, 2011.