Fuzzy Based Trust Evaluation Model for Enhancing Security in MANETs

Renu Popli, Vikas Juneja, Kanwal Garg, D.V. Gupta

Abstract: ***Due to decentralized, self organized and open nature of mobile ad-hoc networks, nodes are vulnerable to various kinds of attacks. The successful data transmission in such type of networks depends upon the cooperation among the nodes. The cooperation can be achieved using trust information of the nodes. In this paper, a fuzzy logic based trust model is proposed and implemented to mitigate the effects of vampire attack. A single vampire attack can significantly exhaust the resources of a network such as battery power etc. The performance of the proposed work is measured using three performance criterions such as precision, recall and communication overhead.***

Index Terms: MANETs, EWMA, Vampire attack, fuzzy logic, trust.

I. INTRODUCTION

Mobile Ad-hoc Network is a peer to peer, self organized, multi-hop network. Due to open and unmanaged network characteristics, nodes in MANETs are highly vulnerable to different types of attacks. MANETs are widely used in information sharing and distributed collaborations. These functions require that the nodes in MANETs should co-operate among themselves [8]. Generally, MANETs are deployed in resource constrained environment, which increases the number of compromised nodes.

Due to the Ad-hoc infrastructure, MANETs are greatly affected by Denial of Service (DoS) attacks. To improve survivability of the nodes in such type of network, a great deal of research has been performed. There are two types of attacks [3] in wireless networks such as a routing disruption and resource depletion attack. A routing disruption attack performs modification of the routing paths such as Sybil attack, Worm hole attack etc. On the other hand, in the resource depletion attack, main focus is on the consumption of various resources such as battery power. For example, the most prominent DoS attack aims to consume battery power of the node completely. These types of attacks are mainly known as "Vampire attacks", as they consume the battery power of the nodes by creating routing loops [12] or misguiding the nodes. These nodes affect the entire system from functioning well.

Manuscript published on 30 June 2019.
***** Correspondence Author (s)
Renu Popli, Assistant Professor, of Department of Computer Science & Engineering in JMIT, Radaur (Distt. Yamunanagar) Haryana.
Vikas Juneja, Assistant Professor, of Department of Information Technology in JMIT, Radaur (Distt. Yamunanagar) Haryana
Kanwal Garg, Assistant Professor in Department Of Computer Science And Application, Kurukshetra University Kurukshetra.
D.V. Gupta, Professor & Head, Department of Mathematics, College of Engineering Roorkee (COER), Roorkee

Generally, in all these types of attacks, the behaviour of the nodes gets changed from the normal observed behaviour. Hence misbehavior detection methods act as a significant role in finding out any kind of attacks.

II. LITERATURE REVIEW

The presence of malicious and selfish behaviors has stimulated the research in the field of misbehavior detection in MANETs. Trust management plays a significant role in detection of misbehaving or malicious nodes. In trust management approaches, a reputation score is assigned to the nodes in the network which is based on their behaviour analysis. There exist various approaches of trust management in MANETs which are mainly focused on the dynamic and self organized behaviour of the nodes. Blaze et al. [6] justified that for communication systems, the trust management problem is an important part of security. Luo et al. [4] presented a trust based system, in which the value of trust is judged based on the opinions of K trusted entities in a specified time. The value of K depends upon the current state of the network as well as number of valid neighbors. However, this may sometimes lead to conflicts in the network. Sun Y.L. et al. [10] introduced an information theory based approach which assigned a quantitative metric to trust. The authors explained propagation of trust within ad hoc environments. The trust is assigned an uncertain value which is calculated by entropy as defined in the approach. H. A. Pirzada and C. Macdonald [1] presented a distributed trust system which was utilized to measure trustworthiness and reliability of the nodes in MANETs. However, the authors did not analyze the resource constraints of the concerned device while calculating trust. K Balakrishnan et al. [5] reduced the undesirable effects of malicious nodes by introduction of an acknowledgement based 2ACK approach. In this, when the data travelled from source to destination through some intermediate nodes, the destination node throws back an unusual two-bounce acknowledgement which is called as 2ACK to ensure successful receiving of data. A hash code based authentication mechanism is applied to identify misbehavior. To differentiate the dynamic behaviour between regular nodes and misbehaving nodes, a framework is designed by Sumati Ramakrishna Gowda et al. [9]. In this proposed framework, regular nodes do cooperation and takes decision based on the belief system whereas the misbehaving node 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 [14] differentiated nodes into two categories based on their behaviors such as malicious nodes and faulty nodes.

They developed a malicious node detection approach based upon some policies in which context information is added to differentiate both type of nodes. Another trust management approach based on different dimensions was adopted in [15] SMART for evaluation of the trust value of the nodes in more accurate manner. Renu Popli et al. [7] proposed a security solution by identifying outlier nodes from the untrusted environment of MANETs. The authors used the concept of three dimensional trust evaluations of the nodes to analyze their behaviour. The nodes were identified as outiers based on their trust values. Wenjia Li et al. [15] described an outlier detection algorithm based on gossip approach in mobile ad hoc networks. In this, all the nodes monitor the behavior of their neighbors. All the nodes compute their local trust table containing trust information of the neighboring nodes. Then the tables are exchanged with direct neighbors only. The local tables are updated if the outlier lists obtained from the other nodes contains more accurate information. This process goes on, till a global view of the outliers is obtained.

Vikas Juneja et al. [13] identified various strategies of detection and prevention for vampire attack in wireless networks. The life span of the nodes can be increased only by detecting and preventing the vampire attacks from the network. S.Kaul, H.Samuel, J.Anand, proposed an Energy Weight Monitoring Algorithm (EWMA), [11] which was used to reduce the effects of two different types of vampire attacks such as carousel and stretch attack. This method is based on the concept of energy level. Mainly, there are two phases in this approach which are Network configuration and communication phase. The authors proposed a DoS (Denial of Service) attack mitigation approach where the node is selected for forwarding of packets only if it sends a huge number of packets using other nodes. Hence it helps in identification of regular nodes from misbehaving nodes. This is because; an ordinary node always performs its task well while a malicious node might not. If a malicious node discards the packets, neighbors are able to detect it and then malicious node is isolated.

III. FUZZY BASED TRUST COMPUTATION

In any distributed networks where the cooperation among the nodes is very important, trust is considered to be an essential requirement. Trust is described as a reliance of one node over the other node. The value of trust shows the reliability of one node over the other node. A node may completely depend on the other node, but this is not feasible in real time environment. Thus, the value of trust can be represented as a probability value that lies in the range of 0 and 1. Hence trust calculation is best described as fuzzy approach [2].

In the dynamic environment of MANETs, the location of nodes is not fixed. Hence to calculate trust value, the mobility of nodes is taken as an important parameter. As nodes are mobile, the trust information also updates rapidly. Thus trust is a dynamic entity which can be represented as a continuous variable whose value ranges between 0 and 1.

In this proposed system, the trust value of the nodes is generated periodically using two different perspectives of trust. The trust value is calculated using previous individual experience of the nodes and the current behaviour of theirs neighbors.

After calculating the trust value of the nodes, the fuzzy member function is used which define five different fuzzy levels such as Very Low, Low, Medium, High and Very High. The value of trust lies between 0 and 1. The fuzzy member function assigns each node to one of the five levels. These five fuzzy levels describe the behaviour of nodes based on their trust values as shown in the table 1 given below.

TABLE1. NODE BEHAVIOUR TABLE BASED ON FUZZY LEVELS

Trust value	Fuzzy Levels	Node Behaviour
0 to 0.2	Very Low	Misbehaving node
0.2 to 0.4	Low	Non co-operative node
0.4 to 0.6	Medium	Regular Node
0.6 to 0.8	High	Co-opertaive Node
0.8 to 1.0	Very High	Highly Trustworthy Node

In MANETs, if a node A wants to transmit data or packets through node B, node A may not be confident of the trustworthiness of the node B. Hence node A relies on the previous experiences with node B which is stored as one of the fuzzy levels. Then node A takes decision based on the obtained information.

A. Trust Calculation

Trust is calculated based on the probability value of trustworthiness of one node over the other node. Trust value of a node for the other node depends upon some parameters. These parameters depend on the context for which trust is calculated.

In the proposed work, three parameters are chosen by taking into consideration the concept of vampire attack. The vampire node can be detected by calculating three trust parameters such as packet drop rate of the node, the percentage of battery discharge of the node and the number of link requests initiated by a node. These are defined as follows:

1) Packet Drop Rate (PDR): This parameter is calculated as the ratio of number of packets dropped to the total number of packets. The trustworthy nodes forward all the packets received by it, whereas malicious nodes drop a large number of packets.

2) Battery Discharge Rate (BDR): This parameter of a node relies on functioning of the network. An active node seems to be busy and consumes more power. In the same way, the nodes with malicious or selfish intention are found to be more active as compared to the other nodes.

3) Number of link requests (NLR): The Vampire node try to make connection with multiple nodes concurrently. As a result, the number of link requests originated by the node will be exceptionally high.

Thus by using the above parameters, trust value is calculated as:

$$T(A,B)= \sum_{i=1}^{k}(W_i P_i(A,B)) \qquad (1)$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

Where W_i is the weight associated with a parameter P_i by node A for node B. The values of the weights are application specific. The aggregated values of different parameters define the trustworthiness of the node.

B. Vampire Detection

In MANETs, each node maintains the trust table of the neighboring nodes. The trust tables are exchanged and updated whenever a node join or leave the network. In MANETs, if a node wants to transfer data, it first checks its trust table containing neighbor's trust information to assure the trustworthy path for the data.

For calculating the trust value, the values of the above three parameters are needed. In the proposed work, these values are calculated by taking random values using rand() function. A node is found hostile if it has lower value of trust, high battery consumption rate and a large number of link requests. hence that node is isolated from the network. The steps are given below:

Steps:

1) For every node in the network, compute three trust parameters PDR, BDR, NLR.
2) Using trust equation 1, calculate trust value of the nodes.
3) Sort the routing table in decreasing order of the trustworthiness values of the nodes.
4) The node which has higher trust value, less battery discharge rate and small number of connection requests are taken for routing.
5) The node which has lower trust value, high battery discharge rate and large number of connection requests are isolated from the network.

IV. SIMULATION RESULTS

The correctness of the proposed model is presented through simulation. The proposed model is compared with an existing model of trust [15]. For performing simulation, MATLAB version R2014a is used. The proposed work is simulated under the following simulated environment:

To evaluate the proposed trust system, three performance factors are chosen. These parameters are defined as:

- Precision: it is measurement of the relevant data among the retrieved data.
- Recall: it is measurement of relevant data that is retrieved over the total set of data.
- Communication Overhead: It is measured by the number of packets handled by the proposed system over the total number of packets in the network.

These parameters are calculated as follows:

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

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

To analyze the performance of the proposed system, observations are taken by varying percentage of misbehaving nodes. The simulation results are presented below:

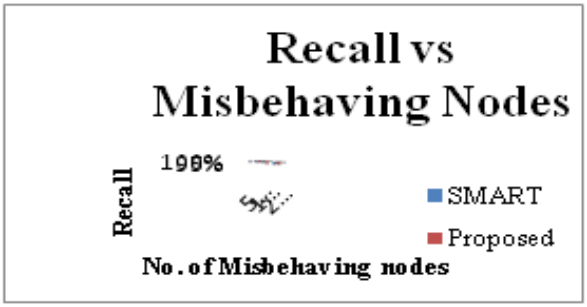

Figure 1: Effect of Misbehavior over Recall

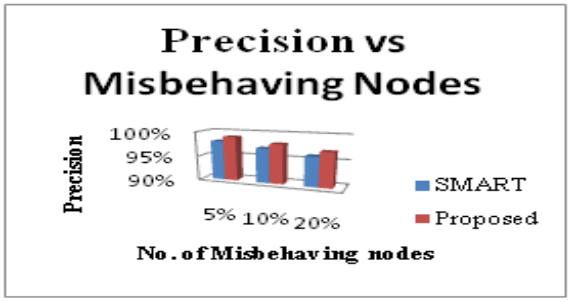

Figure 2: Effect of Misbehavior over Recall

TABLE 2: SIMULATION PARAMETERS

Simulation parameters	Values
Network area	100x100
Total no. of nodes	50
Communication range	40m
Simulation time	10 units
Mobility	5-10m/s
No. of malicious nodes	5%, 10%, 20%

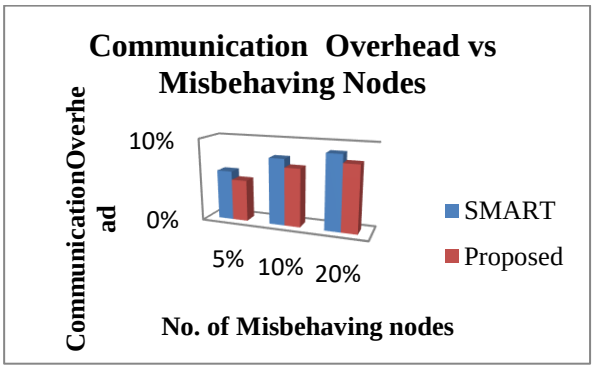

Figure 3: Effect of Misbehavior over CO

The results shown in Figure 1, Figure 2 and Figure 3 describe the effect of percentage of misbehaving nodes over the precision, Recall and Computation Overhead. These parameters represent the accuracy of the system in finding out malicious nodes from the network. The proposed system provides more accuracy and less computation overhead as compared to the existing trust model on increasing the percentage of malicious nodes.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

V. CONCLUSION

In this paper, a security solution using fuzzy based trust evaluation model in an untrusted environment of MANETs is proposed. The proposed work is mainly focused on the mitigation of vampire attack which affects the network functioning immensely. The performance of the model is measured by taking different number of malicious nodes. The simulation results for precision, recall and communication overhead are obtained. The results show the improvement in the calculated parameters.

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, Vol. 26, Issue 1, January 2004, pp. 47-54.
2. Ashish Kumar Jain, Vrinda Tokekar and Shailendra Shrivastava, "Security Enhancement in MANETs using Fuzzy-Based Trust Computation against black hole attacks", Information and Communication Technology, Advances in Intelligent Systems and Computing, 2017, pp. 39-47.
3. G. Vijayanand, R. Muralidharan, "Overcome vampire attacks problem in wireless ad-hoc sensor network by using distance vector protocols", International Journal of Computer Science and Mobile Applications, Vol.2, Issue 1, January- 2014, pp. 115-120.
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. K Balakrishnan, J Deng, and P K Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks", Proc. IEEE Wireless Comm. And Networking,pp. 2005, pp. 2137- 2142.
6. 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.
7. Renu Popli, Dr. Kanwal Garg, Sahil Batra, "Outlier Nodes Detection in MANET's: A Trust Management Approach" International Journal for Research in Applied Science & Engineering Technology (IJRASET), Vol. 6, Issue I, January 2018, pp. 3216-3221.
8. Renu Popli, Dr. Kanwal Garg, Sahil Batra," Outlier Detection using Data Mining in Trust Based Clustered MANET's", International Journal of Electrical Electronics & Computer Science Engineering, Vol. 5, Issue 1, February, 2018, pp. 2454-1222.
9. 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 Vol. 3, Issue 11, November -2013, pp. 520-528.
10. 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, vol. 24 , Issue 2, 2006, pp. 305 – 317.
11. S.Kaul, H.Samuel, J.Anand," Defending against Vampire attacks in wireless sensor networks", International Journal of Communication Engineering Applications, Vol. 5, Article C084, March 2014.
12. Vikas Juneja, Dr. D.V. Gupta, "Strategies for Detection and Prevention of Vampire Attack in WSN", International Journal of Advances in Computer and Electronics Engineering, Vol. 02 Issue2, February 2017, pp. 13-16.
13. Vikas Juneja, DV Gupta, "Security Against Vampire attack in Adhoc wireless sensor network: Detection and Prevention Techniques", International Conference on Wireless Intelligent and Distributed Environment for Communication, Springer, 2018.
14. 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.
15. 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.
16. 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.

AUTHORS PROFILE

Dr. Renu Popli is an Assistant Professor, of Department of Computer Science & Engineering in JMIT, Radaur (Distt. Yamunanagar) Haryana. She completed her P.hD at Kurukshetra University, Kurukshetra. Her area of interest includes in Network Security.

Vikas Juneja is an Assistant Professor, of Department of Information Technology in JMIT, Radaur (Distt. Yamunanagar) Haryana. He completed his M.E. in CSE at NITTTR, Chandigarh. His area of interest includes in Cryptography and Network Security.

.

Dr Kanwal Garg presently working as Assistant Professor in Department Of Computer Science And Application, Kurukshetra University Kurukshetra. Apart from district topper in senior secondary examination and Kurukshetra University topper in under graduation examination, he had completed his post graduation & doctorate from GJU S&T, Hisar under the faculty of Engineering and Technology. Owe the credit of more than 45 research papers published in international & national journals, conference & seminar. He attended 12 workshops/faculty Development Programme/winter/summer school and 01 Orientation Programme to enhance his curriculum. His area of expertise is Data Bases, Data Mining, & warehousing. Approximately 11 year of experience in teaching industry and administration. During this tenure he is actively involved in organizing co-curricular & social activities

Dr. D V Gupta, Professor & Head, Department of Mathematics, College of Engineering Roorkee (COER), Roorkee . Dr. Gupta obtained his Ph.D in Mathematics in the year 1991from Roorkee University (presently known as IIT Roorkee) . He has published several research papers in International / National / Journals / Conferences & also written several other aticles of general interest. He has supervised & also supervising various research scholars for their Ph. D programme . He has a teaching, research & administrative experience of more than 30 years.