TRUST BASED METHODOLOGIES FOR PREVENTING ATTACKS IN MANET- A SURVEY

Amuthan A
Professor, Department of Computer Science & Engineering
Puducherry, India

Kaviarasan R
Research Scholar, Department of Computer Science & Engineering
Puducherry, India

Abstract: Optimal data routing is a significant functional part in the Mobile Adhoc NETworks. In order to achieve this, cooperation of nodes plays a vital role in the data routing process. Under single authority framework, the mobile nodes are adapting to its wireless environments. As many nodes cannot survive with each other due to the security issues in the network layer that lead to causes of faulty nodes, selfish nodes etc. With the increasing number of non-cooperative nodes, the network may results in partitioning. The overall functionality of the MANET in such a case will be degraded. Non-cooperation may be due to some fault, faced by a specific node. In this paper, we have discussed about the various trust based counter measures in identifying the malicious node by various researchers and have proposed a fuzzy based trusted cooperation node mechanism that distinguishes the trustworthy nodes and malicious nodes based on the disadvantages observed from literature. Each node estimates its neighboring node's information and the trust value. Based on the trust values, the classes for each node are defined and misbehaving nodes are detected**.**

Keywords: MANET, Trust, Threshold, Fuzzy, Security

I. INTRODUCTION

Mobile adhoc networks are rapidly deployable, self configuration. MANET [9] requires no existing infrastructure. It can be a standalone network or it can be connected to external networks (Internet).Each node in the ad hoc network acts as a router and forwards packets on behalf of other nodes, allowing nodes that are not within wireless range of each other to communicate over "multi-hop" paths. But security in MANET [11-12] is a challenging task due to its environmental scenario. Communication in this network plays a vital role as each and every packet which is been transmitted has to be sent in a secured way due its application. The main application of this network [10] is in the disaster recovery management and in military application. Security is the most essential required feature in this network as it has the following issues and challenges in constructing an efficient protocol for communication.

- Robustness: Frequent link breaks are common due to the dynamic moment of the nodes. So the protocol which is to be designed should be robust enough to provide high packet delivery ratio despite of frequent link breaks
- Efficiency: The designed protocol should provide high level of packet delivery ratio
- Control overhead: The designed protocol must flood minimum number of control packets in order to consume less bandwidth and energy. So that the networks life time can be increased
- Quality of Service: The QoS has to be kept in mind while designing a protocol as this network is been applied to military and disaster recovery management.
- Resource management: Adhoc Network has minimum bandwidth and energy and the resources have to be utilized properly in order to enhance the networks life time.
- Security and Reliability: The security should be an important feature in this network as it is prone to many types of attack. The designed protocol should be free from vulnerability.

The paper is been organized as follows; in Section II it discusses about the literature survey of the various researches, their techniques, advantages and their disadvantages. In Section III discusses about the designed proposed technique based upon the drawbacks observed from the researchers. In Section IV it discusses about the conclusion and future works and followed by the References utilized.

II. LITERATURE REVIEW

In this chapter various trust based mechanism has been designed by various researchers to prevent different types of attacks in Mobile Adhoc Networks

Nilesh N et al. designed [1] a technique by assigning a trust value to each node based upon their communication made with the next hop node. In the network first the Cluster is formed then the nodes with highest energy level is selected as trusted node in each cluster by the help of rand () function and is chosen as cluster head. Communication is carried out to the next hop node only through these trusted nodes. The malicious nodes in the network are identified through sent and received packets as well as route response is calculated. The number of packets (sent and received) is compared with the threshold value then the particular node is considered as malicious.

M.Poongodi et al. a system [2] involves the following stages for detecting the malicious nodes. Trust values computed based on direct observations (Nodes trust value)**.**Choosing voting participants based on hashing (To identify compromised node from uncompromised node)**.**Determine the decision about the node by voting (Normal nodes with malicious nodes is grouped together)**.** Aumann Agreement theorem (To calculate the truth and confidence values of the nodes and group into two distinct groups and then nodes communicates with each other)**.**Convergence towards truth based on bound of confidence (nodes are separated based on threshold into two groups)**.**Dual weight Trust (the nodes trust value is again updated based upon the behaviour of the node in the network)**.**Rekeying after every new request is received (New group id is generated and sent to cluster heads)

Nidhi lal et al.This technique[3] is used to identify whether packet drop is due to malicious or due to congestion

Step-1

- Authenticate the other node who sends the updated routing table information

Step-2

- The node measures the activity of the next working node (activities namely packet storing time and sending time of packet)

D= M-W

M- Sequence number of the node initiates updating

W- Sequence number of the current node

D- Trust value

  - If D is greater it is malicious
  - If D is smaller update the routing table information

N.Bhalaji et al proposed [4] a mechanism in calculating the trust value of the node by the total number of packets forwarded and received by each node. Based on the trust value the node is categorized into following

Nodes are classified into

- Known (trust level between companion and unknown)
- Unknown (Non trusted node)
- Companion (Trusted)

$$Te = tanh\,(R1 + R2 + A)$$

Te = Trust value
R1= Ratio between the number of packets actually forwarded and number of packets to be forwarded.
R2 = Ratio of number of packets received from a node but originated from others to total number of packets received from it.
A = Acknowledgement bit. (0 or 1)

Possibilities of node becoming

$$A\ (node\ x\ \rightarrow\ node\ y)\ = C\ when\ T\ \geq\ 0.6$$

$$A\ (node\ x\ \rightarrow\ node\ y)\ = K\ when\ 0.3\ \leq\ T\ <\ 0.6$$

$$A\ (node\ x\ \rightarrow\ node\ y)\ = UK\ when\ 0 < T\ \geq 0.3$$

Dilli Ravilla et al uses hashing algorithm [5] to ensure the integrity of packets which is being sent from the source to destination and also predicts the trust value of the node in the second phase. Hash algorithms are secure because, for a given algorithm, it is computationally infeasible to find a message that corresponds to a given message digest. Any change to a message will result in a different message digest with a very high probability**.** Secure Hashing Algorithm 512(HMAC-SHA512) is implemented for the Authentication and Data Integrity of the information being sent. It is used for Authentication and Data Integrity of the information being sent

Trust value is computed to identify the malicious node

- For every node, a timer is initiated while transferring the data.
- The trust value of the participating nodes is increased for every successful transmission and decreased for those nodes that do not send the data towards the destination

$$\text{Trust Value}\ = (\text{Sum of '1' or '0'})/\text{Total Sent Packets}$$

If, Trust Value < Decided Threshold, **Node is malicious**

Fang-Jiao Zhang et al. proposed a mechanism [6] in just for identifying the alternate path when suspicious activity of the node is identified. Source calculates the alternative path to destination. If the node is suspicious, the node should calculate the shortest path and send the information to the genuine node. The genuine node will compare the previously calculated number of hops with the malicious node count. If it varies it is considered as malicious node

Basant Subba et al proposed [7] hybrid IDS mechanism, Present Intrusion Detection Systems (IDSs) for MANETs require continuous monitoring which leads to rapid depletion of a node's battery life. To address this issue, they propose a new IDS scheme comprising a novel cluster leader election process and a hybrid IDS. The cluster leader election process uses the Vickrey–Clarke–Groves mechanism to elect the cluster leader which provides the intrusion detection service. The hybrid IDS comprises a threshold based lightweight module and a powerful anomaly based heavyweight module. Initially, only the lightweight module is activated. The decision to activate the heavyweight module is taken by modelling the intrusion detection process as an incomplete information non-cooperative game between the elected leader node and the potential malicious node.

Arvind Dhakaa et al proposed [8]a mechanism by adding sequence packets in the MAC layer and identifies the malicious node. Two packets which are Response sequence (Rseq) packet and Code Sequence Packet (Cseq). These packets are transmitted in the AODV-MAC [16] layer when a node wants to access the channel. Each intermediate node sends the Cseq to all its neighbours then neighbours intern send their Rseq to the intermediate node. If the Cseq and Rseq matches from the neighbour then the Intermediate node allow the connection to the network layer, Otherwise, it discard the node and send the information to all other nodes that particular node as malicious one. It checks the fix value of sequence packet in the Code sequence table. If seq packet matches with respective Cseq packet than the Rseq packet is accepted; otherwise it is discarded

The techniques which are above proposed by the researchers have found to have drawbacks like network overhead and nodes computational overhead. This indirectly reduces the network life time by consuming more energy and bandwidth of the network. It also fails in exactly predicting the nodes trust worthiness.

III. PROPOSED WORK

Based upon the drawbacks found in the literature a suitable fuzzy mechanism is being applied in identifying the malicious

Fuzzy Logic:

Fuzzy logic is a multi-valued logic in which the values of variables may be any real number between true (1) and false (0). Using fuzzy logic, an input space can be mapped into an output space. Fuzzy logic is used in situations where the available information is in form of partial truth that makes decision process very complicated. When it is difficult to identify an element whether it belongs to one set or another, fuzzy logic is the best option for making such decisions. Fuzzy logic is based on the fuzzy set theory. In Crisp Set theory, an element is either present or is not present in a set. On the other hand, fuzzy set theory deals with the degree of membership of an element in a particular set. An element may be the member of multiple sets at the same time. An element may partially be the member of set A and partially the member of set B. This implies that fuzzy set theory deals with the absence or presence of an element in a particular set. In addition it deals with the partial presence or partial absence of an element in a set as well. Membership function is used to define how each point in the input space is mapped to a membership value between 0 and 1. The input to the membership function is a crisp value and output is a fuzzy value between 0 and 1 that shows the degree of membership in a set. Fuzzy logic uses different logical operators to carry out its operations, such as AND, OR, and NOT. AND operation is equivalent to min (minimum) operation, OR operation can find the maximum of given inputs, and NOT is the complement operator.

Fuzzy sets and fuzzy operations are combined to create if-then rules. Fuzzy logic is composed of these if-then rules. The if-part of the rule is called the antecedent while then-part is called the consequent. A fuzzy logic system maps crisps inputs to crisp outputs. There are four components in a fuzzy logic system, namely rules, fuzzifier, inference mechanism, and defuzzifier as shown in Figure 1. Rules are basically if-then rules which must be evaluated during an input/output process. The output of the system depends on these rules. If-then rules are designed by the experts of a particular field. Fuzzifier is responsible to take crisp numbers as input and give fuzzy sets as output. The activation of rules is dependent on the output of fuzzifier. Inference mechanism maps fuzzy sets into fuzzy sets. Inference mechanism is the decision making part of fuzzy logic system. Defuzzifier maps the fuzzy output of inference mechanism into crisp numbers to make it usable for further processing by the system.

Fuzzy-Based Trust Model:

In the proposed work, A new method is introduced which maintains the reputation information of network nodes. The proposed system relies on firsthand information only that is the direct observations of a node. Second-hand information is not used in order to prevent the false-accusation and false-praising of a node by the information provider. Every node should rely on its own observations and not on others' recommendations because recommendation from others cannot be fully trusted. Second hand information is not used by the system; still it is able to detect non-cooperative nodes. Normal nodes can detect such nodes by direct observations and do not need other nodes to provide information about the presence of selfish nodes. Non-cooperative nodes are easily detected due to their bad behaviour. Even if they are new to the network, they become known to be as non-cooperative soon because such nodes show their greedy behaviour everywhere.

In the beginning, they may get some benefits from the network but for a short period of time after which they are declared non-cooperative. Other reason for not using second hand information is that if a node is non-cooperative to node 'A' only and cooperative to other nodes in the network, it is difficult for node 'A' to convince others about its non-cooperative behaviour, since that node is sincere to them while non-cooperative to node 'A' only. In such a situation, providing second hand

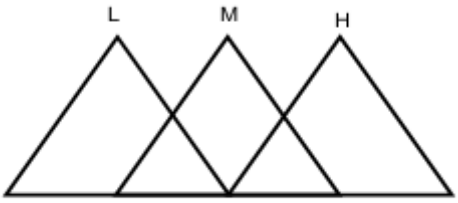
information to others is not useful. Using second-hand information, communication of control traffic is increased which is the wastage of available bandwidth. In order to decrease latency and increase through-put, sharing of second-hand information among mobile nodes is not encouraged. Using this method, every node computes the trust of MPR nodes present in its one-hop neighbourhood.

Inputs to the Fuzzy System

Fuzzy inputs to our proposed system are percentage of dropped data packets, percentage of dropped TC messages, and percentage of generated TC messages.

Percentage of Data Packets Dropped: One of the input parameters used for our proposed fuzzy scheme is the number of data packets dropped by NCB node. It can be calculated using the following formula:

Percentage of dropped data packets = (no. of data packets dropped*100) / total number of data packets send.

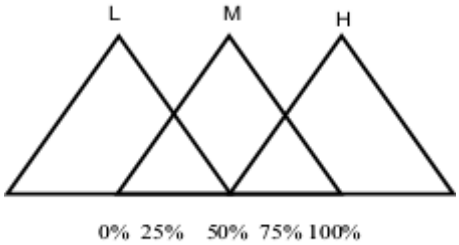


(a) Percentage of dropped Data messages

Figure 1: *Depicts the triangular membership functions for percentage of the data packets dropped while communicating through a network. The capital letters L, M, and H represent the low, medium and high percentage, respectively.*

Percentage of dropped TC messages: Number of TC messages dropped by the NCB node is another parameter used as input to fuzzy scheme. It can be calculated using the following formula:

Percentage of dropped TC messages = (number of TC messages dropped*100) / total number of TC messages forwarded.



(b) Percentage of dropped TC messages

Figure 2: *The percentage dropped TC messages is calculated*

Percentage of generated TC messages: Number of TC messages generated by MPR node as required by the specification of routing protocol is third parameter used as input to the fuzzy scheme. It can be compute as given below:

Percentage of generated TC messages = number of TC messages transmitted * 100/ total number of TC messages expected.

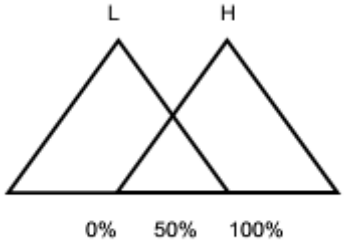


Figure 3: *The percentage generated TC message is calculated*

The corresponding percentages of data packets dropped are calculated by application of these membership functions. These percentages are used for the proposed fuzzy system to determine trust of a node. Based upon the three inputs, that is the percentage of dropped data packets, percentage of dropped TC messages and percentage.

Output of the Fuzzy System:

The fuzzy system has three inputs. There are seven levels of trust, varying from 0 to 0.6 representing most low to most high trust, respectively. By solving these membership functions, the trust for a node can be calculated, which is the main aim of the proposed work.

After calculating the trust of the MPR, computed trust is compared with the pre-defined threshold value. In our case the threshold value for is 0.3, means if the trust of the particular MPR is less than 0.3, that node should be declared as selfish and will be isolated from the active routes of the network.

A walk-through of the proposed system is presented with the help of a following example scenario.

For example, Node S has some data to be sent to node D. It is assumed for the sake of discussion that S already has a valid route to D and it is now going to start transmission. For a particular forwarding node F, node S keeps the account of forwarded and dropped packets and after a fixed time slot Trust Computation component computes the value of behaviour from Misbehaviour count (MC) and Nice behaviour count (NC) present in Computational Matrix. If the value of Behaviour is exceeded from a predefined threshold value, Trust Computation component computes the trust and stores the results. The inputs for fuzzy system are percentage of dropped data packets, percentage of dropped TC messages and percentage of generated TC messages. All these parameter will be calculated and pass on to the fuzzy system. The fuzzy system on the basis of these parameters will compute the trust of the MPR node.

IV. CONCLUSION AND FUTURE WORK

In this paper several countermeasures have been surveyed to prevent attacks in MANET but these methodologies have found to have drawback. As security is a big issue in this adhoc network a robust network has to be constructed by preventing the network from threats. We have overviewed the challenges and constructed a defensive mechanism with fuzzy logic to prevent the attack in MANET. Further this proposed work can be implemented in other sensor networks and VANETs to improvise the security in the network layer.

REFERENCES

[1] Nilesh N, Dangare and R.S. Mangrulkar, "Design and Implementation of trust based approach to mitigate various attacks in mobile Adhoc networks", In the proceedings of International Confernce on Information Security and Privacy, Nagpur, Elsiever, pp.342-349 , December 2015

[2] M.Poongodi and S.Bose, "Detection and Prevention system towards the truth of convergence on decision using Aumann agreement theorem", In the proceedings of the International Symposium on Big Data and Cloud Computing, Elsiever, pp. 244-251, 2015

[3] Nidhi lal, Shishupal Kumar, Aditya Saxena and Vijay Km. Chaurasiya, " Detection of malicious node behavior via I- Watchdog Protocol in MANET with DSDV routing Scheme", Elsiever, pp264-273, 2015.

[4] N.Bhalaji and A.Shanmugam, "Dynamic Trust Based Method to Mitigate Greyhole Attack in Mobile Adhoc Networks" In the international conference on Communication Technology and system design, Elsevier, pp.881-888, 2011

[5] Dilli Ravilla and Chandra Shekar Reddy Putta, " Enhancing the Security of MANETs Using Hash Algorithms" In the proceedings of the International Multi-Conference on Information Processing, Elsevier, pp.196-206, 2015

[6] Fang-Jiao Zhang, Li-Dong Zhai , Jin-Cui Yang and Xiang Cui, "Sinkhole attack detection based on redundancy mechanism in Adhoc networks" Information Technology and Quantitative Management, Elsevier, pp.711-720, 2014

[7] Basant Subba, Santosh Biswas and Sushanta Karmakar, "Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation" Engineering Science and Technology, Elseiver, 2015.

[8] Arvind Dhakaa, Amita Nandalb and Raghuveer S. Dhakac, "Gray and Black Hole Attack Identification using Control Packets in MANETs" In the Eleventh International Conference on Information Processing, Elsiever, pp 83-91, 2015

[9] S. Mclaughlin, D. Laurenson, and Y. Tan, "Mobile ad-hoc network." (Aug. 10 2006) uS Patent App. 11/351,777.

[10] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in Proc. Conf. Commun. Archit., Protocols Appl., 1994, pp. 234–244.

[11] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized link state routing protocol for ad hoc networks," inProc. IEEE Int. Multi Topic Conf. Technol., 2001, pp. 62–68.

[12] T. Clausen and P. Jacquet, "RFC 3626-Optimized Link State Rout-ing Protocol (OLSR)," pp. 75, 2003.

[13] D. Johnson, Y. Hu, and D. Maltz, "Rfc: 4728," Dynamic Source Routing Protocol (DSR) Mobile Ad Hoc Netw. IPV4, 2007. Available:http://tools.ietf.org/html/rfc4728

[14] C. Perkins and E. Royer "Ad-hoc on-demand distance vector routing," inProc. 2nd IEEE Workshop Mobile Comput. Syst. Appl., Feb. 1999, pp. 90–100.

[15] E. Gerhards-Padilla, N. Aschenbruck, P. Martini, M. Jahnke, and J. Tolle, "Detecting black hole attacks in tactical manets using topol-ogy graphs," inProc. 32nd IEEE Conf. Local Comput. Netw., Oct. 2007, pp. 1043–1052.