International Journal of Future Generation Communication and Networking
Vol. 12, No. 4 (2019), pp.1-16
http://dx.doi.org/10.33832/ijfgcn.2019.12.4.01

PROBLEMATIC NODE IDENTIFICATION WITH NEGATIVE SELECTION, DANGER THEORY AND CLONAL SELECTION USING SOURCE BASED IMMUNIZATION WITH TAG SCALING IN MOBILE AD-HOC NETWORK

Nitin Tyagi[1], Manas Kumar Mishra[2]

Department of CEA GLA University, India
[1]nitin.tyagi@gla.ac.in, [2]manas.mishra@gla.ac.in

***Abstract*— Manet is prone to different types of malicious attacks. Security in MANET is hard to achieve because of its dynamic nature. However, identification of potential problematic nodes can help in avoiding the usage of these during data transfer. An early detection of these problematic nodes can substantially enhance the preventive approach for security. Human Immune System (HIS) approach has been greatly used in detection of problematic nodes in MANET. Hence, we propose an approach for problematic node identification with negative selection, danger theory and clonal selection using source-based immunization. We tag the nodes as problematic based on monitoring of their behavior by the source node. Further, we propose tag scaling to capture the severity of the malicious intent based on behavior. The proposed work has been simulated and presented with the results being compared with the existing approaches. The simulation results revel that the proposed work has a better packet delivery ratio in presence of malicious nodes.**

***Keywords*— MANET, Problematic node, Threshold, Scaling, Tagging**

1. INTRODUCTION

Over the most recent couple of decades, the researcher has concentrated in the field of Mobile Ad-hoc network (MANET), where number of mobile nodes accomplish routing in infrastructure less mobile network. The decentralization and MANET features increase the uses of its application in unpleasant organized zones, for example, disaster management and earth-quake and borders, where there is need of established network in any moment. However, Routing protocols can be effectively attacked once the helpless point of the focused network protocols is recognized.

Many researchers proposed the ideas of intrusion detections to defend the routing protocol of MANET [1-4]. However simple cryptographic IDs[5] used to rise control overhead by transmitting additional security information through routing packet. In addition, the infrastructure less structure in MANET reduces the utilization of endorsement authorities infeasible. Along these lines, the general pattern at present is the lightweight computing algorithm[6].

In intrusion detection system in case once a node is recognized as malicious, by then that node won't be considered in next time. This discernment isn't gainful from time to time, it may be that node is recognized as attacker on some parameter during

Received: April 10, 2019
Reviewed: June 9, 2019
Accepted: July 12, 2019

this snapshot of time, such huge numbers of researcher are progressing in the direction of this heading they monitor the node on various parameter and a short time later take decision. Genuinely when a node is boycotted, it won't be considered in future. So secondary idea ought to be expected to distinguish the malicious node. We chose Ad hoc On-Demand Distance Vector (AODV) protocol since this convention being considered for standardization for MANETs.

Artificial Immune Systems (AIS) are portrayed as a ton of idea that imitate something like one of HIS thoughts and philosophies[7]. Introduced AIS intrusion detection methodology can recognize attack in a disseminated and self-sorting out way, which suggests that central organization focuses around the security system are excessive when AISs are connected. This great position upgrades the limit of the technique in cure the MANETs and tending to the requirements and challenges of such network.

2. RESEARCH BACKGROUND

This section gives the detailed discussion of AODV protocol, relationship of HIS and our proposed approach and literature survey.

AODV: AODV has many attributes such as the capability of the loop-free, self-starting, scale to a large number of mobile nodes and able to avoid congested route. However, in AODV routing protocol during route establishment process when a node sends route request packet, reduces its protocol vulnerable to a flooding-based attack known as Resource Consumption Attack (RCA)[8]. When source node want to established a route to destination then source broadcast the RREQ packet to all its neighbors who are one hop away, if neighboring node having the route to destination in their routing table then they reply otherwise they again broadcast the RREQ packet to next node, process repeat till middle node or destination node , response with the fresh route through Route Reply(RREP)packet to source node .

AODV is on demand routing protocol when source initiate to established route to the destination then it broadcast the RREQ to their one hop away node if node is destination or having path to destination then it sends RREP to source. If intermediate node is not having route to destination in their routing table then forward the RREQ to next node. during this process source wait for a time period to get the RREP, if source not received the RREP within in time period then it again broadcast the RREQ message with greater time out to receive RREP to next hop for established the route to destination. Broadcast id and source IP information which every RREQ packet contains make a difference between RREQ packet from other packet broadcast by same source node to find alternate route. Intermediate node who receive the same RREQ packet earlier simply discard the current packet. Due to this mechanism AODV helps the genuine node to avoid network overflow and unnecessary power consumption. However, when an attacker present in the network the attacker node can utilizing the broadcasting stage in AODV and continuous flooding the network with fake RREQ packet with different IDs. Attacker node can also choose the long path to the destination and can harm the system.

HUMAN IMMUNE SYSTEM(HIS): Ongoing inquiries about have demonstrated an expanding enthusiasm for the utilization of human immune system as a wellspring of motivation to take care of complex issues. The human immune system profits by incredible data handling capacities including models distinguishing proof, learning, and remembrance[9]. It is additionally known to be a helpful, dispersed, and auto-authoritative system. Thus, HIS has pulled in huge enthusiasm to be utilized as a motivation metaphor particularly in the field of defense and security of data innovation systems. This exploration field is known as AIS.

ARTIFICIAL IMMUNE SYSTEM: HIS is a perfect security that defend the human body from different foreign pathogens, for example, infections and microscopic organisms. It can identify obscure pathogens following a dynamic learning methodology. The reality of applying hypothetical immune principals as intrusion detection system to secure another compute network has increased wide circulation during lasts years under a research field called AIS. Diverse models have been produced copying distinctive parts of the HIS. Application territories of AIS have secured various areas, for example, extortion recognition, robotics, machine learning, and PC security in a huge part. This section gives a overview of a few AIS models created to take care of intrusion detection problems.

NEGATIVE SELECTION: In biological immune system in bone marrow, T-cells are at first shaped and on development they change their position to the thymus. The period of T-cell advancement is described via articulations given by T-cell receptors. At whatever point the Pre-T-cells and thymus cells collaborate this land thymus cells collaborate this prompt Pre-T-cell augmentation and disparity. At that point these T-cells experience negative selection to wipe out T-cells that activated by self in the thymus. Despite the fact that varieties of negative selection have been introduced, the procedure explained in [10][11] stays in utilization.

In [11] proposed a method to create valuable identifiers that are haphazardly delivered and matchless antigen is put into a finder space known as feedback detector. The feedback detector will be disposed of on the off chance that it matches self-strings. When the feedback detector mature it will be used to coordinate antigens. At the point when the feedback detector secures a competition on additional antigens, it turns into a authentic detector. Basic Evolutionary NSA and fundamental ENSA [11] are NSA varieties and the usefulness of Simple ENSA is to produce indicators prepared to do distinguishing degenerate information. At the point when an indicator tries to coordinate information it can prompt wayward or anomalous changes in the indicator and this locator will be disposed of. The advancement of the up and coming age of locators happens through change, positive choice and negative choice. Such developmental beginning circles to produce locators until the point that a disobedient alteration is taken note.

In Elementary Evolutionary NSA, notwithstanding the cutting-edge locator set a haphazardly produced locator is likewise included. By including the extra locator ventures can occur in the worldwide space too. ENSA discovers its utilization in equipment/programming isolation in embedded system. As a utilization of this model, a system called Lightweight Immune System was produced to identify intrusion on a distributed environment. Williams et al: utilized this model to distinguish PC infections and network intrusion [12].

In [13] proposed the Genetic Artificial Immune system (GAIS). In this the partner of lymphocyte is identified as an artificial lymphocyte. The artificial lymphocyte presents in four conditions: mature, immature, high priority and low priority. The bit string of an artificial lymphocyte is haphazardly produced and completed to experience either positive/ negative selection. In view of the Hamming distance of the closest self-example to an artificial lymphocyte, it will be allotted a threshold value. At whatever point a match occurs with a non-self-design the Hit counter of an artificial lymphocyte is increased to locate its coordinating proportion.

CLONAL SELECTION: As indicated by the Clonal selection Concept once the first lymphocyte is started by official to the antigen, clonal development of first lymphocyte happens. during the growth of lymphocyte, if any clone with antigen receptors relates to the atoms of the life form's very own body, it will be wiped out. With the clonal development of B-cells the normal similarity expanded for the antigen that started the clonal extension through resemblance development. In this manner, the B-cells all the more adequately react to antigens. Substantial hyper-change what's more, the Selective component prompt resemblance development. Substantial hyper-transformation prompts a randomness of antibodies by acquainting arbitrary changes with the genes. Just those genes with a higher accord for the experienced antigen will survive. CLONALG was at first presented in[14].

DANGER THEORY: Danger concept is additional self/non-self-hypothesis that contrasts as of different speculations in what way the system ought to react. The notable normal for Danger Theory originates from the guideline that the immune system does not react to non-self but rather responds to danger. This hypothesis develops out of the thought that there is no compelling reason to jump upon everything outside. In this theory, danger is estimated by the distress signals sent by cells in case of damage or unnatural death.

The Danger Theory has its very own draw backs and [7] proposed uses of the Danger Theory that feature:

-To show danger signal proximity of an Antigen Presenting Cell is essential.
-A danger flag does not need to be dangerous.
-Danger signals can be positive or negative.
-An evaluation of closeness might be utilized to copy the danger zone.

LITERATURE SURVEY: The focus of this section is summarization of the previously proposed works for identification of the malicious nodes in the MANETs. In [15]author proposed the method to distinguish and moderate the impact of nodes that don't forward packets. Watchdog decides the misbehavior of nodes by replicating packet to be sent into a cushion and observing the conduct of the neighboring nodes to these packets. In the event that the quantity of time node movement isn't up to the check then it illuminates to pathrator. The Strength of this paper present another interruption location strategy i.e. watchdog that can distinguish getting out of hand node and keep its data into pathrator so that next time nobody sends the message to the malignant node. In any case, this paper does not recognize a making trouble node within the presence of receiver /ambiguous collision, partial dropping, collusion, wrong misbehaving report; and limited transmission power. So, to resolve such issue many more work has been proposed.

In [16]author proposed the misbehavior detection approach in DSR by using the benefit of an AIS. If the relating antigen is coordinated with any antibody the AIS mark a node as "suspicious". The negative selection algorithm is utilized for finding out about the ensured system, however it doesn't give the reworking to misbehavior. Each node monitors its neighboring node and gathers one protocol trace per monitored neighbored. The bone marrow antibodies are made during disconnected learning stage, and these antibodies are utilized to monitor the communication between nodes. In the event that they coordinate antigens from the node, characterize the node as suspicious utilizing negative selection. In [17] author extend their work and add new AIS approach i.e. Virtual thymus, clustering, danger signal approach and memory detection. The methodology utilizing virtual thymus remove the requirement of primer learning and recognizes misbehavior node effectively.

In [9], they used the concept of negative selection utilizing clone selection in setting of the self– no self judgement model for misbehavior detection in MANET. The results demonstrate that clone selection gives a quicker reaction to the to the repetitive misbehavior. Strength is the combination of qualities catches the communications among the node precisely that prompts increment in detection correctness. The problem in this scheme that each node needs to constantly screen the traffic among the neighboring node that outcomes in more utilization of power resources. The security arrangement that requires earlier preparing before its arrangement struggle with the moment organization of MANETs, as correspondence in MANETs, is normally set up in crisis conditions or on request basis.

In [18] this paper author tries to solve the misbehavior detection problem faces by watchdog with the novel immuno-inspired energy effective approach in ad hoc wireless networks. Proposed approach is motivated by co-stimulatory signals present in the Biological immune system. Author claim that his approach is energy saving for data packet in comparison to watchdog monitoring.

The energy efficiency enhancement is just about two requests of greatness, whenever contrasted with misbehavior detection based on watchdogs

[19] This paper has used the advantages of one of the Danger Theory based AIS interruption identification calculations called DCA to distinguish the resource consumption attack over MANET. DCA has been connected to another mobile intrusion detection and prevention architecture called MANET. Strength of this paper MDCA, where every node in MANET to identify the attack locally with no requirement for mobile agent. But the threshold should be examined in a well a mannered which avoids the research to fall into high false positive rates.

In [20]author proposed an strategy by considering the environment of AIS and routing protocol which he has taken is AODV.to del with wormhole attack an AIS strategy is used which is inspired by HIS. the good thing is in this paper the proposed strategy is not for only AODV, it will be work well for all routing protocol with slight modification to secure network against wormhole attack. According to proposed method the simulation results shows that efficiency increased in comparison of AODV routing protocol in term of packet delivery ratio, throughput, end to end delay and the number of deleted packets by the attacker.

In [21] author not just recognize attack, it additionally distinguishes the range and augmentation of attack. This proposed system distinguishes the attack is more clear by utilizing the fuzzy logic technique. The system likewise contains IPS mechanism system which gets contribution from fuzzy logic and gives the safe information correspondence over the network. IPS likewise monitor for the traffic of black hole and gray hole attacks. The outcome obviously demonstrated this strategy identifies the attack in a proficient way when contrasted with existing technique. Future work author suggests the decrease of jitter value which is more in presence of IPS, which is a direct result of route updation when attack is present. [22]The proposed calculation motivated by dendritic cells to process the alert signal and to judge from that point whether there is malicious intent or not. In this method, the intrusion detection is identified with the harm that can happen in the system, involved by internal or external. This identification is possible using the concept of dendritic cells with context information representing the state at that environment.

In[23] this paper, the Packet storage time attack is shown and the PST attack has been destitute down using AIS standards and estimations including packet loss, delay and battery power. The source figures the node EE node of the attacker node and differentiations the regard and its own one energy. in the event that the EE node happens to be more prominent than EE source the presence of the attacker is confirmed. Downside of this strategy in the event that source process the EE node unfailingly, at that point congestion is high in network. The plan proposed is incredible and pick AIS principles for example of how AIS can be associated with MANET as needs be reducing the effects of security events subject to this attack type including futile battery consumption.

MAPPING FROM IMMUNE SYSTEM AND AODV: Basically, routing protocol complete in two phases .in first phase it accepts all positive information for training and after the completion of training node moves to another phase where detection and tagging function performed. In detection and tagging process node identify misbehaving nodes. Source node act as Monitor node and monitor the behavior of new selected antigen represents the behavior of good or bad. If any antigen behavior is detected by monitor node on the basis of different parameter it will make a list of all problematic node which tagged earlier as problematic node. Because source node act as monitor node, at the time of route establishment source node use the concept of clonal selection process in the node that made the arrangement.

3. PROPOSED APPROACH

Most of the intrusion detection systems proposed in literature determine the malicious intent of the nodes and once categorized as malicious, these nodes are not considered for future routing exercises. However, the Ad-hoc nature of MANET makes its constituent parameters highly variable and thus, decision based on these varying parameters would be vulnerable and must have the adaptability to change. Therefore, we propose a source based adaptable problematic node identification approach, to identify, categories, and scale the severity of malicious intent. The proposed approach categorizes the problematic nodes onto different categories based on predefined threshold values, and tag them. The respective category tags the nodes belong to governs their usability in future routing decisions. The work derives motivation from HIS and thus, provides the scope for the curing of a problematic node based on tag scaling. Moreover, the approach changes the tag of problematic node to that of a normal node abased on the favorable behavior of the node. Further, the tag scaling also helps to dynamically changing the tag of a normal node to that of a malicious node based on doubtful behavior of the node.

The System Model and Assumptions

- **Homogenous Network**
  In proposed work network is considered as homogenous i.e. all the nodes have similar hardware and software configuration. The radio transceivers of the nodes work under a similar setup all through the lifetime of the system.
- **Sender is aware of the address of the destination**
  All the senders of the data packets are assumed to be aware of the destination and its address.
- **Each node knows its neighbourhood and maintains a routing table**
  Each node is assumed to maintain a routing table on-demand and thus, also knows it neighbourhood.
- **Each Sender maintains a list of problematic nodes**
  Once a node is tagged as problematic, the sender maintains the status of the tag for route selection and also tag scaling.

Calculation of Round-Trip Time (RTT): RTT is the time between sender node sending RREQ towards the destination and the receiving of the corresponding RREP at the sender node. Given all RTT values between node in the route and the destination, RTT between two progressive nodes, say A and B, can be calculated as follows:

$$RTT_{A,B} = RTT_A - RTT_B \tag{1}$$

Immunization: The proposed method assumes the Sender node to behave as the immunizing node. During the route establishment stage, the route reply from a node, if deviates from the predefined threshold, will lead to the tagging of the concerned node as a Potential Problematic Node (PPN). In addition, during data transfer stage, depending on the time taken for the transmission of the ACK message, the previously defined tag can be scaled to that of, a Problematic Node (PN), Less Severely Problematic Node (LSPN) or Severely Problematic Node (SPN), depending on the severity of misbehavior and the previous tag value. Further, these tag values can be used as a parameter to decide the usage of the tagged node for future routing exercises, by the sender.

The immunization modelling is based on the following intuitive reasoning,

- **Identification of Potential Problematic Nodes (PPN) and Tagging**
    - **Congested/Non-Cooperating Node (NCN)**
        - Nodes takes more time to respond to RREQ of source.
            - Threshold based on collective information on all possible path with in a time period.
    - **Nodes with Malicious Intent (Black Hole/ Worm Hole)/Too near location/Potential older response, Fast Responding Node (FRN)**
        - Nodes sends quick response to RREQ of source.
            - Sequence No out of bound in RREQ and RREP.
            - Threshold depicting minimum RTT for a valid response.

Node Tagging and Tag Scaling: The sender being the immunization node uses certain network parameters to predict the behavior of the nodes other than the destination as problematic and also tag these nodes for future considerations. These tagging of the nodes are to be performed during route establishment and also during data transfer. The problematic node tagging during route establishment is based on the intuition that a node with malicious intent will try to seize the opportunity to be on the optimal route by responding faster than normal. Moreover, in case of non-malicious intent node responding faster than normal might happen in cases where the forwarder node is very close to the sender node, thus making the progress of the packet very limited, which is again not an advisable option for routing. On the contrary, nodes who tend to delay relying or replying to the RREQ packets can be considered to be either overloaded and congested or have the potential of being a selfish node. Thus, we try to model these instances using Average RTT over multiple path RREQ-RREP pair.

Apart from this, during data transfer, if any upstream node does not receive any ACK packet for a particular data packet after predefined number of retries, the upstream node assumes that either the downstream node has move out of its coverage area or might have deliberately misbehaving. Thus, in both the cases the upstream node generates a danger signal to make the sender aware of the misbehavior. On receiving the danger signal the sender initiates the validation process and sends a probe packet to the identified node. If the identified node does not respond to this probe packet then the sender could not validate the misbehavior, however, it categorizes the node as problematic so that the node's participation in future route selections are limited. However, if the node responds to the probe packet with an ACK, then its misbehavior is validated and the sender initiates tag scaling, to tag the node with more severity of problematic intention, to further limit/obsolete the participation of this node in future route selections.

3.1 DURING ROUTE ESTABLISHMENT: NEGATIVE SELECTION

When the sender wants to send data packets to a destination and doesn't have the route, it sends RREQ packet to all its neighbor nodes. Each RREQ packet contains a sequence number to avoid looping. It stores the timestamp of the RREQ. Each RREQ packet will have a maximum hop counter and equal number of fields for both the node id and corresponding timestamp entries to be made by all the nodes in the route to destination. All the intermediate nodes forward the RREQ packet, decrements the hop counter and also enters its node id timestamp of forwarding the packet. Eventually, the destination receives multiple copies of the RREQ packet. The destination replies to these RREQ packets with multiple RREP packets having the hop counter, node ids, and the timestamps of the intermediate nodes, to the Sender. The sender on receiving the multiple RREP packets (within a predefined waiting time), process them for the detection of the problematic nodes and subsequent tagging on different routes. Further, this tagging information are used for the selection of the best route from the Sender to the destination.

3.1.1 NEGATIVE SELECTION: TAGGING

3.1.1.1 Sender broadcast RREQ with a Seq No. after storing the Timestamp of it and waits for a time period (Tw). where,

Tw = Max Hop * Ideal RTT in a Hop

$$= (1.2 * \frac{\text{Diagonal of target area}}{\text{Transmission time range}}) * (2*\frac{\text{Transmission range}}{\text{speed of propagation}}) \quad (2)$$

However, Max hop may be decided on the basis of Network Statistics or can be user defined.

3.1.1.2 All intermediate nodes append their respective Timestamps to the RREQ packet and broadcast it.

3.1.1.3 The Destination node replies to all the RREQ packets received with in a time frame (Tw/2) with RREP packets after appending its Timestamp.

3.1.1.4 All intermediate nodes append their respective Timestamps to the RREP packet and forward it through the nodes from which the corresponding RREQ packets were received.

3.1.1.5 The Sender waiting for a time period (Tw), accepts and analyse all the RREP packet received with in the time period. It estimates, Average hop RTT over all n

$$\text{path}=\frac{\sum_{i=1}^{n} \text{RTTi}}{\sum_{i=1}^{n} \text{hopi}} \quad (3)$$

where, RTTi and hopi are the RTT and hop of the ith path between the sender and destination.

3.1.1.6 The Sender estimates RTT of each node on each path using the timestamp of packets appended by each node in the RREQ and subsequent RREP, and also the hop distance from itself.

3.1.1.7 **Case 1:** A node is potential problematic and takes more time to response to RREQ of source

```
For each node
      If (Estimated RTT>Average hop RTT * hop of that particular node)
       then
      If (the Node is already tagged)
      then
      Tag Scaling is initiated
      Else the Node is identified and tagged as NCN
      Else the Node is identified as normal and remains untagged
```

3.1.1.8 **Case2:** A node is potential problematic and takes less time to response to RREQ of source

```
For each node
If (Estimated RTT<Min RTT)
then
The Node is identified and tagged as FRN Where,
```

Min RTT = 1/3 * RTTideal

$$=1/3* (2*\frac{\text{Transmission range}}{\text{speed of propagation}}) \quad (4)$$

3.1.1.9 **Case3:** A node is potential problematic and responses out of bound to RREQ of source to gain route

```
For each node
If (The Sequence number of RREP send by node differs with the RREP sequence number received from destination by a node)
then
```

The Node is identified and tagged as FRN

3.1.2 BEST ROUTE SELECTION

3.1.2.1 After tagging process is over the sender considers all Routes without any SPN and estimates the corresponding route pain.

3.1.2.2 For each candidate route, say Routei, the corresponding Route Pain

Route Pain = (0.5 * (No. of PN on Routei + 1.25 * No. of LSPN on Routei) + 0.25 *(No. of NCN on Routei + No. of FRN on Routei) + 0.25 * Hop count) (5)

Best Route is the Route having the Minimum Route Pain

3.2 DURING DATA TRANSFER: DANGER THEORY

After selection of the best route, the sender sends data packets to the destination which are forwarded by the downstream nodes. Similarly, the corresponding ACKs are forwarded by the upstream nodes on the route and are received by the sender. The sender waits for a predefined time to receive the ACK from the destination. If it does not receive the desired ACK, then there is a high probability that an intermediate node has either started behaving or has increased its ante as a problematic node. Analogous to His, the upstream node to the node identified as the non-respondent node takes the responsibility to inform the sender of such situation. Hence, the upstream node sends a Danger Signal (DS) to the sender to intimate about the node. As an immune response, the sender sends a Probe Packet targeted to the identified problematic node and waits for the response. If the ACK is not received for the Probe Packet, then the link to the node is assumed to be lost and the Route repair process is initiated. However, if the ACK is received against the Probe packet, it goes to reflect that the node has deliberately ignored the forwarding of the previous ACK against the data packet, and therefore, necessitates tag scaling.

3.2.1 IMMUNE RESPONSE: TAG SCALING

```
3.2.1.1 If (ACK is not received for a data packet within a timeframe) then
        The immediate upstream node initiates a Danger Signal (DS) to the
        source with the information about the identified node
3.2.1.2 On receiving a DS, the Sender sends a Probe Packet (to activate the
        immune response) to the identified node
3.2.1.3 If (ACK to the Probe Packet is received) then
      Initiate Tag Scaling if the node is already tagged
              If (the tag is PN) then
          The tag is scaled up and the node is tagged as LSPN and initiates
          Route repair
                                Else If (the tag is LSPN) then
          The tag is scaled up and the node is tagged as  SPN and initiates
          Route repair
        Else the node is tagged as PN and initiates Route repair
      Else
      The link to the node is assumed to be lost and doesn’t change its tag and
      initiates   Route repair
```

3.3 TAG REUSE: CLONAL SELECTION

Once the nodes are tagged, the next biggest challenge is to reuse this tagging information to evade the negative impact of these problematic nodes. Therefore, the Route Selection metric, Route Pain considers only those routes that are free from SPN nodes. Further, the pain also usages different weights for various categories of Problematic Nodes.

3.3.1 CLONAL SELECTION: TAG REUSE

3.3.1.1 No RREP is entertained through the earlier tagged SPN nodes.

3.3.1.2 Routes with PN and LSPN tagged nodes can participate in the Route Establishment. However, their influence in the selection criteria is limited to 50%. However, the LSPN Nodes impact in the Route Selection is relatively 25% more than the PN Nodes.

3.3.1.3 The NCN and FRN impact the selection metric by 25%.

4. SIMULATION AND RESULT DISCUSSION

System Simulator (NS-2.35) has a particularly rich part library. In particular, we portray the recreation in the 1500 m×1500 m area, random waypoint mobility model; node movement speed is varying i.e. 5,10,15,20 m/s. These enlargements fuse the exhibiting of an IEEE 802.11/MAC. Table I exhibits the reproduction parameters used in the sort out setup

Table I. Simulation Parameters

Simulator	Ns 2.35
Number of nodes	50,100,150
Number of Problematic nodes	10 % to 40%
Area Size	1500m*1500m
Transmission range	200m
Speed of node	5m/s-20m/s
Node Mobility Model	Random Waypoint

The simulation presented in this paper is based on the following parameter as follows:

a) At varying speed under the fixed percentage of mobile node for the network consisting 50,100 and 150 nodes.

b) At fixed speed under the varying percentage of mobile node for the network consisting 50,100 and 150 nodes.

c) At varying speed under the fixed percentage of mobile node for the network consisting 50 ,100 and 150 nodes:

In this situation, the highest speed of the node is varied from 5 to 20 m/s, and the component of the dimension of the problematic node is stable to 10%. In the first place, the packet delivery ratio of the AODV, existing methodology and proposed approach for the different number of nodes. The outcomes show up in the Figure:1. It can also be seen that the packet delivery ratio of the proposed methodology and AISBA for the diverse number of nodes to some degree diminishes when the node speed increments. As observed in Figure:1, using the packet delivery ratio, the calculation execution was assessed and our proposed methodology gave a higher packet delivery ratio in comparison with the AISBA and AODV. The execution improvement discovered utilizing our methodology, with this situation when contrasted with AISBA and AODV, features the potential for AIS calculations to be successfully used in MANET. The packet delivery ratio benefitted from the ID and held information of problematic node. The proposed philosophy shows that a higher packet delivery ratio analyzed AISBA and AODV when the system is close to nothing anyway as long as the system is extending the packet delivery ratio is fairly less, perhaps a prompt outcome of tagging process.

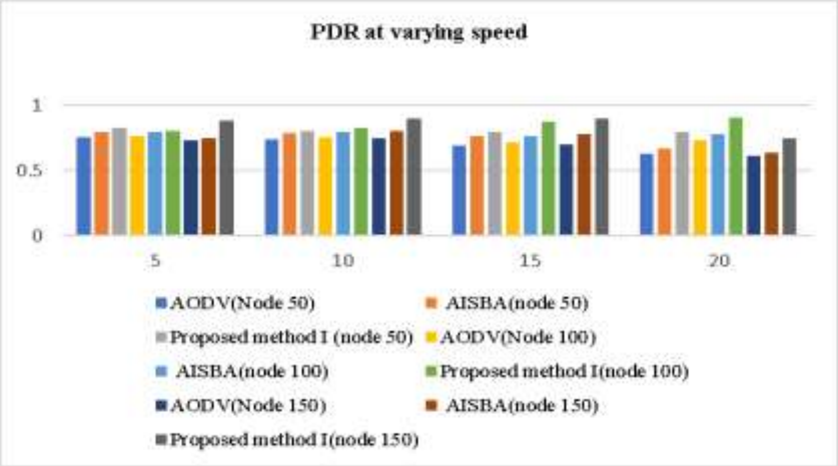

Fig. 1 Packet Delivery Ratio at varying speed

Second, we consider the routing overhead of the proposed methodology and contrast it and existing methodology and AODV for the different number of nodes. The results are appeared in the Figure2.it might be seen that the directing overhead of existing and the proposed methodology for the different number of nodes increases when the node speed increases. What's more, the proposed methodology can even now identify problematic node viably while keeping a routing overhead to some degree higher than that of AISBA [23]. For whatever length of the system node is addition by then there is higher routing overhead interestingly with existing methodology by virtue of higher mobility and a high number of nodes. The reason behind this in AISBA it will consider the case of sequence number but in proposed approach on every phase tagging process is there in number of times so overhead is increasing in our approach. Source node act as monitor node so it's clear from results that when the number of nodes is increasing then overall routing overhead is increasing.

Third, we consider the end-to-end delay of the proposed methodology and existing methodology for the different number of nodes. The results are appeared in the Figure 3. It might be seen that the average end-to-end delay brought about by the Proposed methodology is higher than that realized by existing methodology in all cases. This is perceived to the manner in which that the proposed methodology requires more opportunity to perceive and pursue the problematic node, which isn't the circumstance for existing, since the current methodology is thinking about just couple of parameters for problematic node detection mechanism.

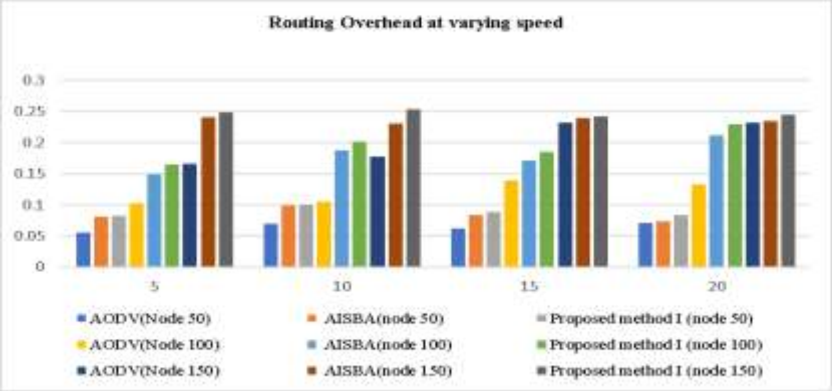

Fig. 2. Routing Overhead at varying speed

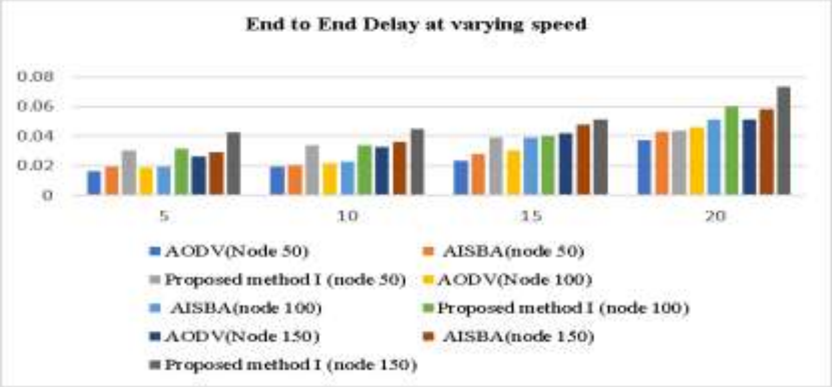

Fig. 3 end-to-end delay at varying speed

b) At fixed speed under the varying percentage of mobile node for the network consisting 50,100 and 150 nodes

To begin with, we contemplate the packet delivery ratio of the proposed methodology and AODV with changing level of Problematic node from 10% to 40%. The greatest speed of node is taken as 20m/s. The results are shown in Figure4, it tends to be seen that AODV endure more in comparison with AISBA and in our proposed systems, when the problematic node changes their level from 10% to 40%. Our approach demonstrates higher packet delivery ratio in comparison of AISBA. The commitment of this paper is that the utilization bio-inspired calculations gives better execution contrasted with existing one. The packet delivery ratio better even within the sight of problematic node. Indeed, even for the situation when 40% node are problematic the proposed plan still fruitful identify those problematic nodes. it might be possible because of applying the concept of checking node severity at different stage like route establishment and data transfer.

Second, we are studying the routing of the proposed methodology and AODV with a percentage of malicious node varying from 10% to 40%. The maximum node speed is taken as 20m/s. Figure 5 shows that, if the number of problem nodes increases, the existing methodology produces the lowest overhead routing compared to the methodology proposed.

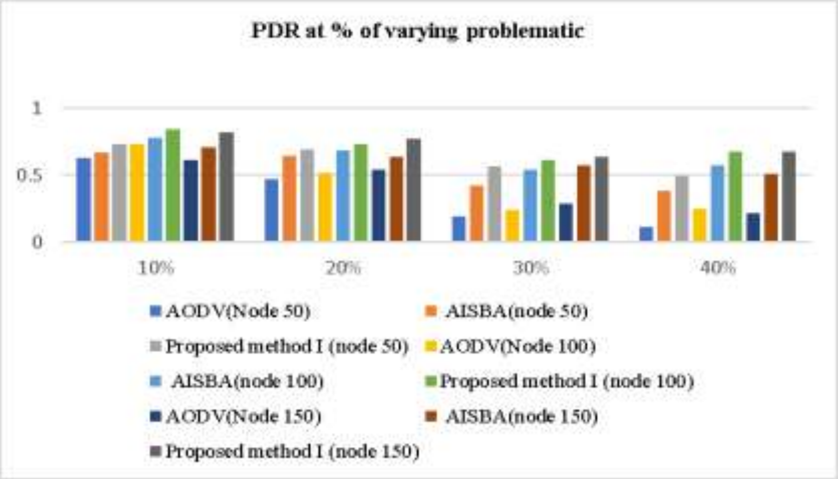

Fig. 4. PDR at % of varying problematic node

This is attributed to the fact that in terms of the security mechanism our methodology performs well. We studied the effect of varying speed on the overhead routing.as expected, it was found that the overhead routing over the proposed methodologies reaches the highest value when the varying speed is maximum, this is attributed to the fact that the detection of the proposed scheme rapidly increases the speed.

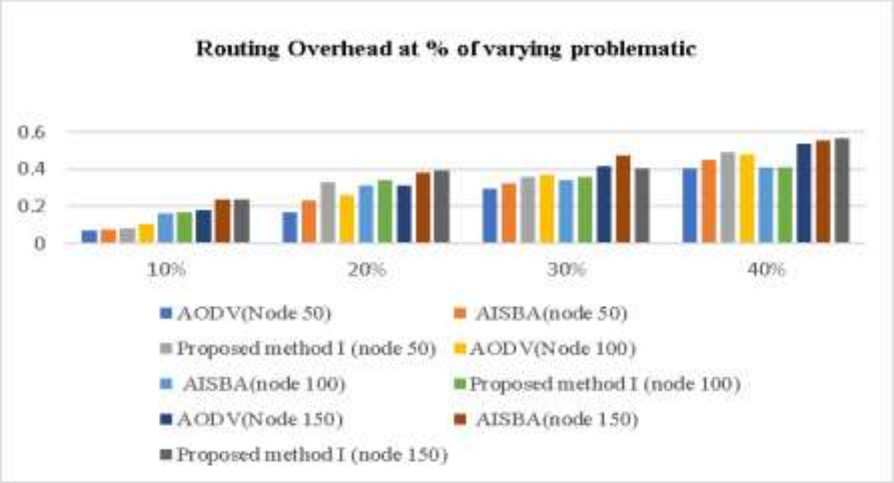

Fig. 5. Routing Overhead at % of varying problematic node

Third, we are studying the end-to-end delay of the proposed methodology and existing methodology with a varying percentage of problematic node from 10% to 40%. The maximum node speed is taken as 20m/s. Figure6 shows the result. Compared to AISBA, it can be observed that the proposed methodology incurred a bit more end-to-end delay.
This is due to the fact that it took more time for the proposed methodology to detect problem nodes. A trade-off between end-to-end delay and packet delivery ratio must therefore be made. Even if the node in the network is more problematic. In the proposed methodology due to tag changes in the problem node and consideration of route pain for route setting, end-to-end delay is shown higher at different percentages of problematic node.

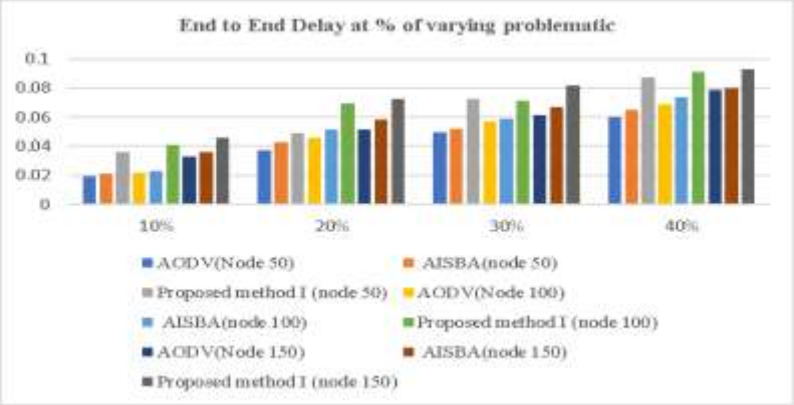

Fig. 6 end-to-end delay at % of varying problematic node

5. CONCLUSION AND FUTURE WORK

In this work we have presented an methodology for problematic node identification with Negative Selection, Danger Theory and Clonal Selection using Source Based Immunization with Tag Scaling in MANET. The sender monitors the response from the intermediate nodes during route establishment and tagged them as potential problematic node, based on the status of their response. Further, to reflect the misbehavior during data transfer, the danger theory methodology has been adapted. In this methodology we proposed the usage of danger signal, prob packet, the corresponding acknowledgement to capture the severity of the malicious intent. The proposed methodology was simulated and the results were compared with AODV and AISBA.it has been observed that the early detection of problematic node and its severity grading by the proposed methodology increased the packet deliver ratio as compare to the existing methodology. however, due to route selection based on multiple path and severity grading during data transfer, the average end to end delay and routing overhead increased as compared to other methodologies. the propose methodology used the source node as monitoring node thus the problematic node tagging is solely dependent on the observation made by the source node. A global observation might enhance the reliability and effectiveness of tagging. Hence the monitoring of the behavior of the nodes by dedicated monitoring nodes can generate a global inference about the behavior of these problematic nodes. Therefore, in future work we would like to explore the usage of centralized as well as grid-based monitoring nodes for similar solutions.

REFERENCES

[1] T. S. Bharati, R. Kumar, J. M. Islamia, and N. Delhi, “Intrusion Detection System for Manet Using Machine Learning and,” vol. 6, no. 12, pp. 1–8, 2015.

[2] a Mishra, K. Nadkarni, and a Patcha, “Intrusion Detection in Wireless Ad Hoc Networks,” Wirel. Commun. IEEE, vol. 11, no. 1, pp. 48–60, 2004.

[3] E. M. Shakshuki, N. Kang, and T. R. Sheltami, “EAACKA secure intrusion-detection system for MANETs,” IEEE Trans. Ind. Electron., vol. 60, no. 3, pp. 1089–1098, 2013.

[4] I. Ntroduction, “Enhanced Intrusion Detection System with On-Demand Routing Protocol using Hybrid Cryptographic Technique for MANETs,” vol. 5, no. 8, pp. 125–133, 2014.

[5] S. Zhao, A. Aggarwal, R. Frost, and X. Bai, “A survey of applications of identity-based cryptography in mobile ad-hoc networks,” IEEE Commun. Surv. Tutorials, vol. 14, no. 2, pp. 380–399, 2012.

[6] S. Abbas, M. Merabti, D. Llewellyn-Jones, and K. Kifayat, “Lightweight sybil attack detection in MANETs,” IEEE Syst. J., vol. 7, no. 2, pp. 236–248, 2013.

[7] U. Aickelin, P. Bentley, S. Cayzer, K. Jungwon, and J. McLeod, “Danger Theory: The Link between AIS and IDS?,” Lect. Notes Comput. Sci., vol. 2787, pp. 147–155, 2003.

[8] “Danger Theory Based Model to Prevent Sleep Deprivation Attacks in MANETs 1,” vol. 9359, no. 12, pp. 61–64, 2015.

[9] J. Y. Le Boudec and S. Sarafijanovic, “An artificial immune system approach to misbehavior detection in mobile ad hoc networks,” Biol. Inspired Approaches To Adv. Inf. Technol., vol. 3141, no. 5, pp.

396–411, 2004.

[10] M. Ayara, J. Timmis, R. de Lemos, L. N. de Castro, and R. Duncan, “Negative selection: How to generate detectors,” Proc. 1st Int. Conf. Artif. Immune Syst., vol. 1, pp. 89–98, 2002.

[11] W. Ma, D. Tran, and D. Sharma, “Negative Selection with Antigen Feedback in Intrusion Detection.”

[12] “a380212.pdf.” .

[13] A. J. Graaff and A. Engelbrecht, “Optimised Coverage of Non-self with Evolved Lymphocytes in an Artificial Immune System,” no. May 2014, 2006.

[14] V. Cutello, G. Narzisi, G. Nicosia, and M. Pavone, “Clonal Selection Algorithms : A Comparative Case Study Using Effective Mutation Potentials,” pp. 13–28, 2005.

[15] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” Proc. 6th Annu. Int. Conf. Mob. Comput. Netw. MobiCom 00, vol. 1, no. 18, pp. 255–265, 2000.

[16] J. Le Boudec, “An Artificial Immune System Approach to Misbehavior Detection in Mobile Ad-Hoc Networks,” vol. 2004, pp. 96–111, 2004.

[17] S. Sarafijanovic and J.-Y. Le Boudec, “An artificial immune system for misbehavior detection in mobile ad-hoc networks with virtual thymus, clustering, danger signal, and memory detectors,” {AISB} 2004 {S}ymposium {T}he {I}mmune {S}ystem {C}ognition, vol. 2004, no. 5005, pp. 45–46, 2004.

[18] M. Drozda, S. Schildt, S. Schaust, and H. Szczerbicka, “An Immuno-Inspired Approach to Misbehavior Detection in Ad Hoc Wireless Networks,” Arxiv Prepr. arXiv10013113, p. 15, 2010.

[19] M. Abdelhaq, R. Hassan, and R. Alsaqour, “Using dendritic cell algorithm to detect the resource consumption attack over MANET,” Commun. Comput. Inf. Sci., vol. 181 CCIS, no. PART 3, pp. 429–442, 2011.

[20] T. Scholar, “Modification in Routing Mechanism of AODV for Defending Blackhole and Wormhole Attacks.”

[21] V. B. E, M. K. Priyan, C. Gokulnath, and P. U. D. G, “Fuzzy Based Intrusion Detection Systems in MANET,” Procedia - Procedia Comput. Sci., vol. 50, pp. 109–114, 2015.

[22] A. Khannous, C. E. D. Sti, and M. Bouhorma, “A New Approach to Artificial Immune System for Intrusion Detection of the Mobile Ad Hoc Networks FST of Tangier Morocco,” Int. J. Comput. Appl. (0975 – 8887), vol. 92, no. 15, pp. 50–53, 2014.

[23] L. E. Jim and M. A. Gregory, “Utilisation of DANGER and PAMP signals to detect a MANET Packet Storage Time Attack,” vol. 5, no. 2, pp. 61–74.2017.