International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-5, March 2019

An Artificial Immune System Source-Based Immunization Approach with Centralized Monitoring and Tag Scaling for Misbehavior Detection in Mobile Ad-Hoc Networks

Nitin Tyagi, Manas Kumar Mishra

Abstract*: *In Mobile Ad-hoc network where node act as router. The network is helpless against for those nodes whose behavior is susceptible due to bad behavior. For detecting the bad behavior, misbehavior detection system is proposed. In proposed work it inculcates the concept of artificial immune system (AIS) to detect malicious node in mobile ad-hoc network. The goal is to build a system that, like its natural counterpart, automatically learns, and detects new misbehavior. In proposed work We used the concept of negative selection for provide the secure network and clonal selection is for detecting the malicious node based on Round Trip Time in mobile ad-hoc networks with centralized monitoring using the concept of tagging. Proposed strategy tried and confirmed for differing number of node and within the sight of varying percentage of malicious node.

Index Terms*: *MANET, Problematic node, Threshold, Scaling, Tagging.

I. INTRODUCTION

In MOBILE *ad hoc* networks pre-existing infrastructure is not needed, it can be created anywhere as per requirement. Nodes can communicate each other because every node act as router. So, for communication it's required that every node participate in common routing protocol, such as Ad hoc On-Demand Distance Vector (AODV) Routing. If all node participates in routing protocol correctly then only AODV work well. This is tough to ensure in ad hoc environment. Misbehaving in network occurs due to two reason software or hardware. In Ad-hoc network routing is achieved by node present in open environment, we think the badly behave to be aggravated. Although few malicious nodes want to bring down the network slow. An wide-ranging of misbehavior node is given in [1][2][3][4].In simulation the proposed approach identify node as faulty those do not forward route request, data, respond to the route request or Acknowledgement during the calculated threshold based on round trip time. Numerous specialists proposed the thoughts of intrusion detections to protect routing protocol in MANET. Anyway, basic cryptographic IDSs used to raise control overhead by transmitting extra security data through routing packet. Also, the framework less structure in MANET decreases the usage of underwriting specialists infeasible. Thusly, the general example at present is the lightweight computing algorithm. In intrusion detection framework in case once a node recognized as malicious, by then that node won't be considered in next time. This observation isn't correct once in a while, it may be that node is recognized as attacker on some parameter without a second's pause, such a significant number of analysts are moving in the direction of this bearing they monitor the node on various parameter and a short time later identified as malicious. Really when a node is boycotted, it won't be considered in future. So, in judgement process that should be compare it from other thought also. We chose AODV protocol since this protocol being considered for standardization for MANETs. Artificial Immune systems (AIS)[5] are described as a great deal of idea that imitates something like one of HIS thoughts and ideologies . Introduced AIS interruption location philosophy can recognize attack in a disseminated and self-organizing way, which infers that fundamental administration focuses around the security system are excessive when AISs are connected. This good position overhauls the limit of the strategy in sparing MANETs and tending to the requirements and challenges of such system. Self and non-self-cell are most important part of IS that are available in our body. The IS is divided into two category first is the innate IS and adaptive IS[6].The basic objective of this research is to develop hybrid approach that can address the trouble of verifying MANET with high security and system execution rates. In proposed work we actualized "negative selection" is utilized for finding out about the secured framework and "clonal selection" is utilized for quicker optional reaction to rehashed trouble making. Our strategy is tried and confirmed for differing number of node and within the sight of varying percentage of malicious node. In this paper, Section II gives look into research background and terminology on AODV and the natural IS. Section III gives the proposed approach. Section IV gives simulation result and discussion. Section V makes conclusion and describes what we will do in future.

II. RESEARCH BACKGROUND

This segment reveals insight into three fundamental research background issues, to be specific, the weakness of AODV routing protocol, Immune system and literature survey. AODV has numerous qualities, for example, the capacity of self-beginning, loop free, scale to countless node and ready to avoid congested route.

Manuscript published on 30 March 2019.
***Correspondence Author(s)
Nitin Tyagi, CEA, GLA University, Mathura, India.
Manas Kumar Mishra, CEA, GLA University, Mathura, India.

However, in AODV routing protocol during route establishment process when a node sends route request packet (RREQ), decreases its protocol helpless against a flooding-based attack known as resource consumption attack (RCA)[7]. Figure 1 exhibits the working of AODV [8] when no attack is presented in the system. At the point when source S need to set up a route to destination at that point source communicate the RREQ packet to every one of its neighbors who are one jump away, on the off chance that neighboring node having the route to destination, at that point they reply else they again communicate the RREQ bundle to next node, process repeat till intermediate node or destination node D, reaction with the new route through Route reply (RREP) packet to source node S.

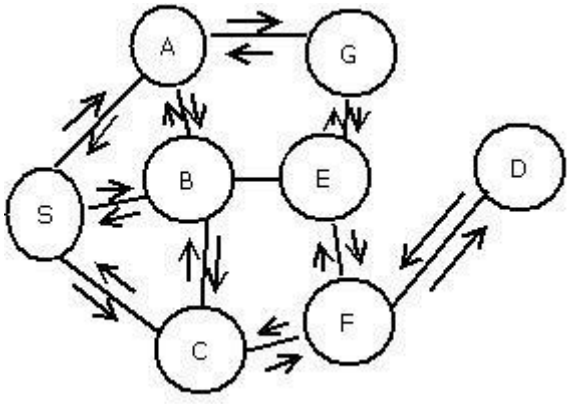

Figure 1. Working of AODV

AODV is on demand routing protocol when source start to establish path to the destination then it communicates the RREQ to their one hop away node on the off chance that node is destination or having route to destination, at that point it sends RREP to source. On the off chance that middle of the route node isn't having route to destination at that point 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 nodes 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 presents 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 Ongoing inquiries about have demonstrated an expanding enthusiasm for the utilization of Human immune system (HIS) 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. It is additionally known to be a helpful, dispersed, and auto-authorization framework. 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 frameworks. This exploration field is known as AIS[5]. HIS is a perfect security that defends 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 Artificial Immune System. 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. 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 [9][10] stays in utilization. In [10] 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 matures 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 [10] 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. In [11] proposed the Genetic Artificial Immune system (GAIS). In this the partner of lymphocyte is identified as an artificial lymphocyte.

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

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.

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[12]. Danger concept is additional self/non-self-hypothesis that contrasts as of different speculations in what way the framework 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 focus of this section is summarization of the previously proposed works for identification of the malicious nodes in the MANETs. In [13]author proposed the method to distinguish and moderate the impact of nodes that don't forward packets. Watchdog decides the misbehaviour of nodes by replicating packet to be sent into a cushion and observing the conduct of the neighbouring 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 [14]author proposed the misbehaviour 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 misbehaviour. Each node monitors its neighbouring node and gathers one protocol trace per monitored neighboured. 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 [6] 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 removes the requirement of primer learning and recognizes misbehaviour node effectively. In [15], they used the concept of negative selection utilizing clone selection in setting of the self– nonself judgement model for misbehaviour detection in MANET. The results demonstrate that clone selection gives a quicker reaction to the repetitive misbehaviour. 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 neighbouring 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. [16] In this paper, each node having detector that keeps up a dataset of normal behaviour collected during the normal behaviour and abnormal behaviour of the system created arbitrarily. Subsequent to gathering normal behaviour, the finder begins to monitor the correspondence among the neighbouring nodes. In the event that if the behaviour of any node is suspicious then immediately the procedure of cooperative decision is initiated by counselling with neighbouring detector to take a last decision about the associated node. Strength is the trading of recognition results among the neighbouring nodes expands the detection accuracy. But this method suffers from correspondence overhead over the system. In [17] this paper author tries to solve the misbehaviour 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 claims 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 misbehaviour detection based on watchdogs. [7] 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.

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

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[18] This paper author work in the direction of three limitation of watchdog i.e.: still watchdog neglect to recognize pernicious conduct with the nearness of ambiguous impact and partial dropping author. EAACK is comprised of three noteworthy parts ACK, SECURE ACK- Improved version of TWOACK, Misbehaviour report authentication (MRA). The MRA scheme works in surrounding to verify whether the destination node has gotten the comprehensive lost packet through another route. A key supplant component can be received to kill the necessity of pre-distributed keys. Other cryptography procedures can likewise be actualized.

[19]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[20], this paper, the Packet storage time attack (PST) is displayed and the PST attack has been broke down utilizing AIS standards and measurements including packet loss, delay and battery power. The source figures the node EE of the attacker node and contrasts the esteem and its very own energy. if the EE node happens to be greater than EE source the presence of the attacker is confirmed. Drawback of this methodology if source compute the EE node every time then congestion is high in network. The arrangement proposed is powerful and opt AIS standards for instance of how AIS can be connected to MANET accordingly diminishing the impacts of security occasions dependent on this attack type including futile battery consumption.

Mapping from Immune System to detection system for AODV

Every routing protocol runs in two phases, firstly in learning phase first take all positive cases for training purpose. After the completion of training, node can leave the environment and can proceed in second phase where detection and tagging function performed. In detection and tagging process node may uncovered misbehavior nodes. Monitor nodes are monitor the behavior of new selected antigen represents the behavior of good or bad. If an antigen behavior is detected by centralized monitor node on the basis of different parameter, in this process a list of problematic nodes is prepared on an interval and those nodes found maximum number of time problematic they will be considered as problematic node and send a list of all problematic node in the network, so that from next time no one considered that corresponding node. This generates the clonal selection process in the node that made the arrangement.

III. PROPOSED APPROACH

The proposed calculation pursues centralized monitoring using the concept of Source based Immunization with Source observing and Tag Scaling. A reactive methodology as having a learning stage influences the calculation to have an expansive computational overhead. As the MANET topology is dynamic, along these lines it isn't effective to learn things already. In the event that a node conduct isn't known previously, that node is problematic after some time. The boycotted node could have a path error. In such situations, structuring a security algorithm dependent on the learning stage is inefficient. Accordingly, the security algorithm proposed in this paper is a reactive one which precisely confirms certifiable instances of path error and recognizes a problematic node. In this approach we apply the concept of source-based Immunization with centralized monitoring and tag transfer because if the network is too long and source-based immunization with source monitoring then the problematic node identification is source dependent and makes the detection scope very limited. For long network if centralized monitoring and tag transfer is done then identification of problematic node scope is good but due to centralized monitoring node detection scope is high.

Identification of Problematic Nodes

Centralized Monitoring Node will perform the identification and prepare a list of potential problematic node (PPN). The Centralized Monitoring Node will randomly choose a Destination in a Sector of 30^0 in whole network and prepare a list of problematic nodes (number of times identified as problematic). The behavior of nodes on the basis of threshold and sequence number. However, it will not perform Route Selection. Any Source interested to send data, will establish route as earlier. However, it will not identify the PPN and will seek the list of Problematic Nodes from the centralized monitoring node. For example in following figure suppose M is the monitoring node and D is destination then it decide the range and in first range node A, B, C, D, E, F, H, K, P comes then it identifies suppose node K is a problematic node and in second range(node comes P, A, B, K, H, J, G, I) the again it identify supposed node K is problematic the it keep a record of problematic node that how many times they act as a problematic node and on the basis of this decision source node decided that which path has to follow.

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

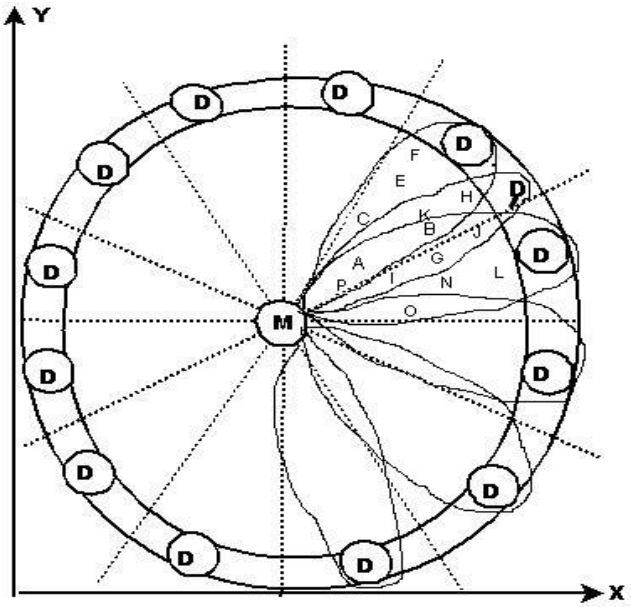

Figure 2: Centralized monitoring node

Threshold Calculation

The System Model and Assumptions

In this work, we expect that the network is similar i.e. all node comprises a similar hardware and software configuration. The radio transceivers of all node of the network work under a similar setup all through the lifetime of the system. One of the parameters to detect problematic node is threshold is based on round trip time (RTT) which is based on waiting time to acquire channel, propagation time, process time at every node and waiting time in queue. Since process time and waiting time in the queue, most of the research article consider as negligible. Here we are putting waiting time in consideration for calculation of threshold. Due to mobility nature of nodes within the network it is difficult to estimate the RTT among two nodes; therefore, the proposed approach is taking as average RTT time to establish the threshold to decide the malicious node. The round-trip time can be defined as follows:

$$RTT=Tt+Tp+Tq+Tprocess+Ttack+Tpack \quad (1)$$

Since most of the works considers Tq, Tprocess and Ttack as negligible time. If the size of the waiting queue is large in every node then we cannot neglect the waiting as negligible. Therefore the round trip time will be defined as follows: RTT = Tq+ Tt +2Tp, While the calculation of the Tq is as follows: In every of node queue follow M/M/1/K model, is categorized by the following assumption:

Route request arrive as per a Poisson procedure with parameter λt, or comparably, the time between entry, t, has an exponential distribution with parameter λ, i.e. for t≥0, the probability density function is

$$f(t)=\lambda e^{-\lambda t} \quad (2)$$

The service time s has an exponential distribution with parameter μ i.e., for s≥0, the probability density function is

$$g(s)=\mu e^{-\lambda t} \quad (3)$$

The buffer of node is of k size.

By (2), the distribution of inter arrival time is exponential, hence the average inter arrival time

Average arrival time=1/λ , Average process time=1/μ,

Average arrival rate(ρ)= λ/ μ (4)

Waiting time in the queue Tq =Lq / λe (5)

Aaverage load in queue

Lq = 0*(P0 + P1) + 1* P2 + 2* P3 +(k-1) Pk

Pk=ρn*(1-ρ)/1-(1-ρk+1)

λe = λ [1-Pk]

So Tq = Lq / λ [1-Pk]

Therefore the threshold will be TH =Tt +2 TP +Tq (6)

The value of TH will be as average RTT as threshold of RTT values between two successive nodes.

Route Finding

AODV routing protocol is based on demand driven, when it requires the route, the source node send RREQ packet to all neighbor nodes and save the time of sending the RREQ. Since the recording of the time is based on their own clock, therefore the synchronization of the time does not require. The recording of the time based on their own clock happens at every node for the RREQ and RREP. The transitional node likewise forwards the RREQ message and spare RREQ time of its sending time. At the point when the RREQ message ranges to the destination node, it sends the RREP message with upgraded saved path. At the point when the middle of the route node gets the RREP message, it spares the time of getting of RREP. Our hypothesis depends on the RTT of the route request and reply. Since RTT include all the time defined in equation (1). But for misbehaving node detection, simulation considers the threshold time based on the time included in equation (6). The RTT can be calculated as follows:

$$RTT = T_{RREP}-T_{RREQ} \quad (7)$$

Calculation of RTT

In this segment, we disclose the approach to compute the RTT. RTT is the time between node send RREQ to the destination and get RREP from that.

Given all RTT values between node in the route and the destination, RTT between two progressive nodes, say A and B, can be figured as follows:

$$RTT_{A,B} = RTT_A - RTT_B \quad (8)$$

Where RTT_A is the RTT among node A and the destination, and RTT_B is the RTT among node B and the destination.

For example, as shown in figure3: the route from source (A) to destination (D) pass through node B, and C so which routing path includes:

A → B →C→ D

Let $T(A)_{RREQ}$, $T(B)_{RREQ}$, $T(C)_{RREQ}$ and $T(D)_{RREQ}$ are the time of RREQ at respective nodes, while $T(A)_{RREP}$, $T(B)_{RREP}$, $T(C)_{RREP}$ and $T(D)_{RREP}$ are the time of RREP at respective nodes. Therefore the calculation of RTT for every node A, B, C and D will be calculated based on equation (7) as followed:

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

$RTT_A = T(A)_{RREP} - T(A)_{RREQ}$, $RTT_B = T(B)_{RREP} - T(B)_{RREQ}$, $RTT_C = T(C)_{RREP} - T(C)_{RREQ}$and $RTT_D = T(D)_{RREP} - T(D)_{RREQ}$. And the RTT values among two successive nodes along the path will be calculated based on equation (8):

$RTT_{A,B} = RTT_A - RTT_B$, $RTT_{B,C} = RTT_B - RTT_C$, and $RTT_{C,D} = RTT_C - RTT_D$

Under normal circumstances, $RTT_{A,B}$, $RTT_{B,C}$, $RTT_{C,D}$ are similar value in range. If there is a problematic node, the RTT value may impressively higher than another progressive RTT values.

Source node behaves as the Immunizing node

- Identification of Potential Problematic Nodes (PPN) and Tagging
- Centralized Monitoring Node will perform the identification and prepare a list of PPN
- Used by Source Nodes during Route Selection

Tag Transfer

- PN and SPN Identified on Current Route done by Source - During Data Transfer

Tag scaling

- Tag scaling done by Centralized Monitoring Node based on tag given by all sources

Tag Reuse

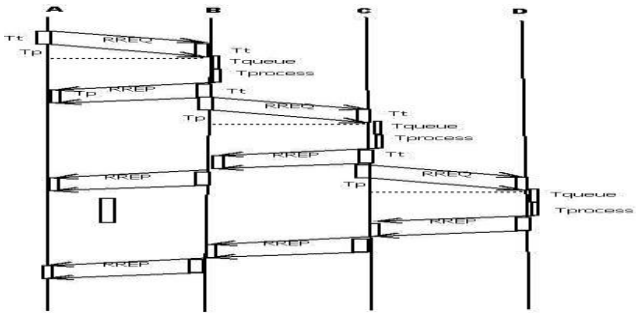

Figure 3: RREQ Packet send and receive time mechanism

Used by Source Nodes during Route Establishments

Algorithm:

1. The Centralized Monitoring Node Will Randomly Choose a Destination in a Sector of 30^0 and will perform the process of Route Establishment for PPN identification and tagging. However, it will not perform Route Selection

2. During Route Establishment:

Centralized Monitoring Node will perform the identification of Potential Problematic Node (PPN) and Tagging and prepare a list of PPN.

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 (FRN)

- Nodes sends quick response to RREQ of source.
- Sequence No in RREQ and RREP.
- Threshold depicting minimum RTT for a valid response.

3. Tag Scaling:

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

Sender send RREQ & wait for a time period (T_w) and accept and analyze all the RREP packet received with in the time period.

T_w =Max Hop * Ideal RTT in a Hop

Max hop may be decided on the basis of Network Statistics/User Defined

$$=(1.2* \frac{Diagonal\ of\ target\ area}{Transmission\ time\ range}) * (2*\frac{Transmission\ range}{speed\ of\ propagation}) \quad (9)$$

Estimate average hop RTT over all n path=$\frac{\sum_{i=1}^{n} RTTi}{\sum_{i=1}^{n} hopi}$

(10)

Estimate RTT of each node on each path using the time stamp of packets at each node

- For each node

If (Estimated RTT>Average hop RTT * hop of that particular node)

Then Node is identified and tagged as NCN

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

- Sequence number of RREP send by node earlier and RREP sequence number receive from destination by that node differs than the node is tagged as FRN.

Min RTT = 1/3 * RTT_{ideal}=1/3* $(2*\frac{Transmission\ range}{speed\ of\ propagation})$ (11)

- Estimate RTT of each node on each path using the time stamp of packets at each node
- For each node

If (Estimated RTT<Min RTT)

Then Node is identified and tagged as FRN

Based on tag given by all sources centralized node does the final tagging for whole network nodes as follows,

- Tag scaling done by Centralized Monitoring Node based on tag given by all sources
- If a node is tagged below 25% times by all sources, it is treated as Non-problematic

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

- If a node is tagged above 25% and below 50% times by all sources, it is treated as Problematic (PN)
- If a node is tagged above 50% and below 60% times by all sources, it is treated as Less Severely Problematic (LPN)
- If a node is tagged above 60% times by all sources, it is treated as Severely Problematic (SPN)

Best Route Selection:

- All Routes without any SPN, will be considered as candidate routes
- For each candidate route the Route Pain is estimated
  Route Pain = (0.5 * (No. of PN + 1.25 * No. of LSPN) + 0.25 *(No. of NCN + No. of FRN) + 0.25* Hop count) (12)
- Best Route is selected having the Minimum Route Pain

During Data Transfer:

If ACK is not received

Then the immediate upstream node initiates a Danger Signal (DS) to source

- Sender sends a probe packet (activate the immune response) to the identified node

If ACK is received

Then Initiate Tag Scaling if the node is already tagged

Then if the tag is PN then the tag is scaled up and tagged as LSPN and initiate Route repair

Else if

the tag is LSPN then the tag is scaled up and tagged as SPN and initiate Route repair

Else

It is tagged from normal node to PN and initiate Route repair

4. Tag Reuse:

Used by Source Nodes during Route Establishments

- No route reply is entertained through the earlier tagged SPN nodes
- Routes with PN tagged nodes can participate in the Route Establishment. However, they influence the selection criteria by 50%

IV. SIMULATION AND RESULT DISCUSSION

Framework 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 1 exhibits the reproduction parameters used in the sort out setup.

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

Table1: Simulation Parameters

Simulator	Ns2.35
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 introduced in this paper depends on the accompanying 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.

Comparison of proposed approach with existing approach

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

In this highest speed of node is varied from 5 to 20 m/s, and problematic node is settled to 10%. To simulate the packet delivery ratio, we compared proposed approach with existing approach for different number of nodes. In figure 4 result shows that proposed approach performs well in comparison to AODV and AISBA [20] for less speed as well high speed. The packet delivery ratio in proposed approach is high for varying number of speeds, because we first identify the problematic node and tagging on the basis of centralized monitoring decision. Centralized monitoring is performed so there is less overhead on source because he gets the problematic node list fromcentralised monitoring node. When source established the route, the route is identified on the basis of less route pain so packet delivery ratio(PDR) is increases in proposed approach. Second, we consider the routing overhead of the proposed approach and compare it with existing approach and AODV for the various number of nodes. The outcomes are shown in the Figure5.it's very well may be seen that the routing overhead of existing and the proposed approach for the various number of node increments when the node speed increments. In addition, the proposed approach can even now recognize problematic node effectively while keeping a routing overhead somewhat higher than that of AISBA[20]. For whatever length of the network node is increment at that point there is high routing overhead in contrast with existing approach on account of higher mobility and a high number of nodes. this is because at the time of routing source use the

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

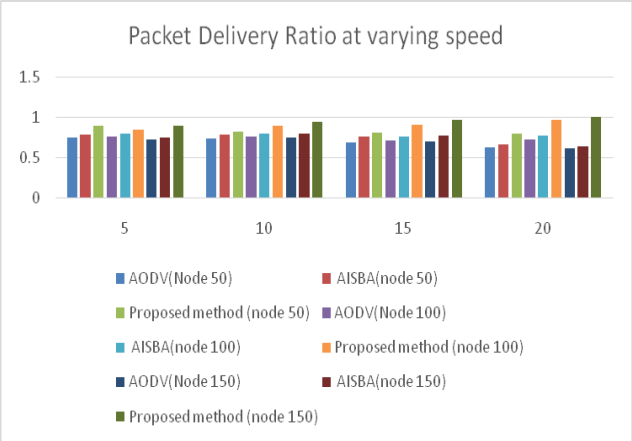

Figure 4: Packet Delivery Ratio at varying speed

correct node on the basis of list received from centralized monitor node. Source only has to tag only those nodes whose behavior is found susceptible during data transfer. Third, we consider the end-to-end delay of the proposed approach and existing approach for the various number of nodes. The outcomes are shown in the Figure6.

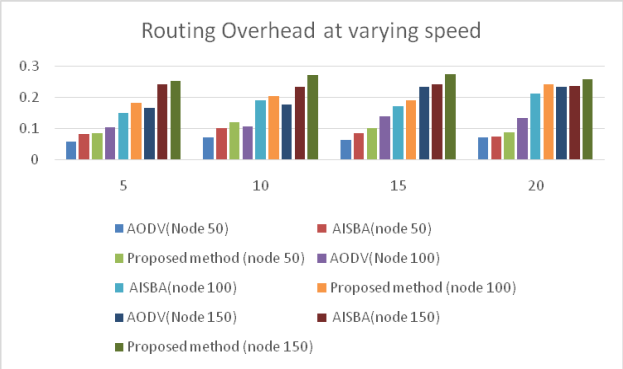

Figure 5: Routing Overhead at varying speed

it very well may be seen that the average end-to-end delay caused by the Proposed approach is higher than that brought about by existing approach in all cases. This is recognized to the way that the proposed approach requires more time to recognize and follow the problematic node, which isn't the situation for existing, since the existing approach is considering only few parameters for problematic node detection mechanism

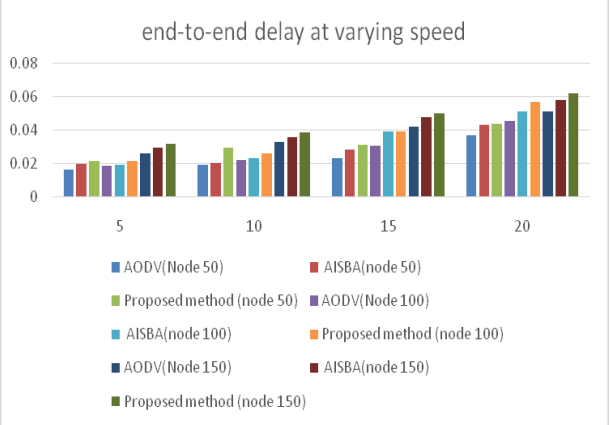

Figure 6: end-to-end delay at varying speed

.

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

First, we study the packet delivery ratio of the proposed approach and AODV with varying percentage of problematic node from 10% to 40%.the maximum speed of node is taken as 20m/s. the outcomes are shown in Figure7, it can be seen that AODV suffer more in comparison with AISBA [20]and proposed approach ,when the problematic node percentage varies. Our approach shows higher packet delivery ratio in compare of AISBA. The contribution of this paper is that the use of bio-inspired algorithms gives better performance compared to existing one. The packet delivery ratio better even in the presence of problematic nodes. Even in the case when 40% nodes are problematic the proposed scheme still successful detects those problematic nodes while keeping the packet delivery ratio50% approximately. It may be because of tagging done in different mode**.**

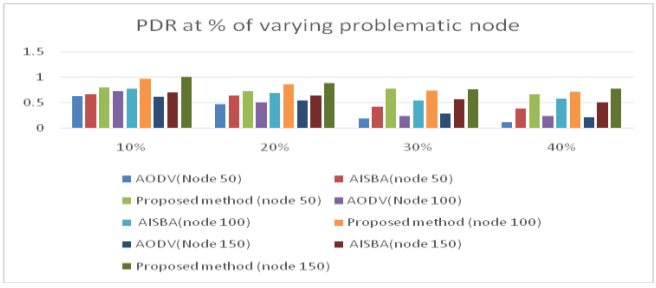

Figure 7: Packet delivery ratio at % of varying problematic node

Second, we study the routing of the proposed approach and AODV with varying percentage of malicious node from 10% to 40%.the maximum speed of node is taken as 20m/s. The result is shown in Figure 8. It can be observed that when the number of problematic node increase, existing approach produces the lowest routing overhead compared with proposed approach. This is attributed to fact that our approach is performing well in term of security mechanism. We have studied the effect of varying speed on routing overhead. As expected, it was found that the routing overhead of the proposed approaches reaches the highest value when the varying speed is maximum, this is attributed to fact that the detection of proposed scheme fast when the speed is increased.

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

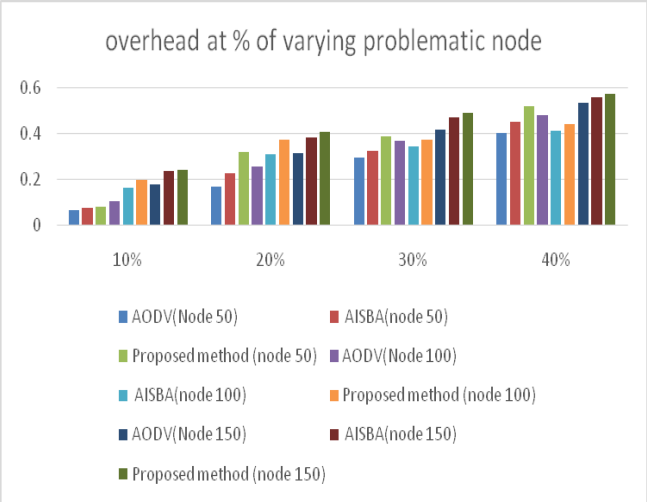

Figure 8: Routing overhead at % of varying problematic node

Thirdly, we study the End-to-End Delay of the proposed approach and existing approach with varying percentage of malicious node from 10% to 40%.the maximum speed of node is taken as 20m/s. the result are shown in Figure9.

It can be observed that proposed approach incurred a little bit more end-to-end delay compared to [20]. This is attributed to fact that the proposed approach taken more time to detect problematic node. Therefore, a trade-off must be made between end-to-end delay and packet delivery ratio. Even in the case that there are more problematic nodes in the network. In proposed approach due to tag changing of the problematic node and considering the route pain for route establishment, end to end delay is higher shown at varying percentage of problematic node.

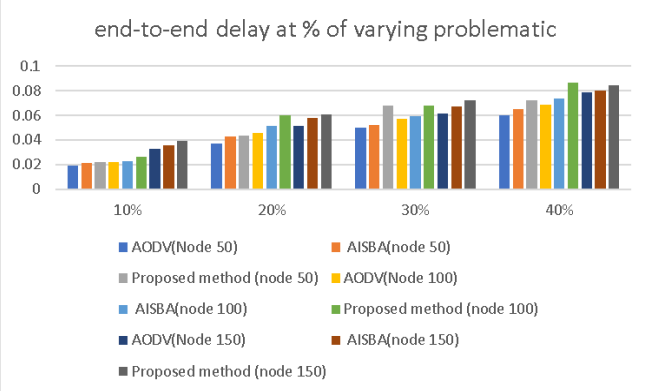

Figure 9: end-to-end delay at % of varying problematic node

V. CONCLUSION AND FUTURE WORK

In this work, we proposed another IDS strategy assigned for MANETs. The inspiration for our work is to build up an IDS that can distinguish making the problematic node. We introduced the approach to identification of problematic node based on round trip time in MANET with centralized monitoring using the concept of tagging. When we compare our strategy with existing IDS then we get the good result in term of packet delivery ratio in the presence of 10% to 40% problematic node. Results show that routing overhead is increased because of centralized monitoring, so in our future work we can reduce the overhead by the concept of decentralized monitoring system.

REFERENCES

1. S. Singh, S. C. Dutta, and D. K. Singh, "A study on Recent Research Trends in MANET," vol. 3, no. 3, pp. 1654–1658, 2012.
2. S. Sahu and S. K. Shandilya, "A comprehensive survey on intrusion detection in manet," Int. J. Inf. Technol. Knowl. Manag., vol. 2, no. 2, pp. 305–310, 2010.
3. M. S. Alnaghes, "A Survey on Some Currently Existing Intrusion Detection Systems for Mobile Ad Hoc Networks," pp. 12–18, 2015.
4. A. S. Hosgouda and P. M. S. Shobha, "A Survey on Black Hole Attack Detection in MANET Using AODV Protocol," vol. 4, no. 1, pp. 415–420, 2015.
5. 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.
6. 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.
7. 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.
8. R. Bai and M. Singhal, "DOA: DSR over AODV Routing for Mobile Ad Hoc Networks," IEEE Trans. Mob. Comput., vol. 5, no. 10, pp. 1403–1416, 2006.
9. 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.
10. W. Ma, D. Tran, and D. Sharma, "Negative Selection with Antigen Feedback in Intrusion Detection."
11. A. J. Graaff and A. Engelbrecht, "Optimised Coverage of Non-self with Evolved Lymphocytes in an Artificial Immune System," no. May 2014, 2006.
12. V. Cutello, G. Narzisi, G. Nicosia, and M. Pavone, "Clonal Selection Algorithms : A Comparative Case Study Using Effective Mutation Potentials," pp. 13–28, 2005.
13. 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.
14. J. Le Boudec, "An Artificial Immune System Approach to Misbehavior Detection in Mobile Ad-Hoc Networks," vol. 2004, pp. 96–111, 2004.
15. 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.
16. A. Byrski and M. Carvalho, "Agent-Based Immunological Intrusion Detection System for Mobile Ad-Hoc Networks," pp. 584–593, 2008.
17. 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.
18. 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.
19. 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.
20. L. E. Jim and M. A. Gregory, "Utilisation of DANGER and PAMP signals to detect a MANET Packet Storage Time Attack," Australian Journal of Telecommunications and the Digital Economy vol. 5, no. 2, pp. 61–74.2017

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

AUTHORS PROFILE

Nitin Tyagi is pursuing Ph.D. from GLA University Mathura. His area of interest is MANET. He is life time member of CSI.

Manas Kumar Mishra did his Ph.D. from MNNIT Allahabad. His area of interest is wireless sensor network, MANET and VANET. He has published many research articles in reputed journals and conferences. Presently he is associated with GLA University, Mathura as Associate Professor.

GLA University, Mathura, India

nitin.tyagi@gla.ac.in, manas.mishra@gla.ac.in