Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 2, pp: (40-46), Month: May - August 2016, Available at: www.noveltyjournals.com

Overcoming the Drawbacks of Jammer Affected Cluster in VANET Using Artificial Bee Colony Algorithm

[1]A. Jeeva, [2]J. Jayavel

[2]Teaching Fellow, [1,2] Information Technology, Anna University Regional Campus, Coimbatore, India

Abstract: **The Vehicular Adhoc Networks (VANETs) are constructed by the set of communicating vehicles equipped with wireless network devices that are interconnect each other without any pre-existing infrastructure (Ad-Hoc mode). Security in VANETs protects the network from the action of hackers. The VANETs cluster, which facing a jamming attack, is a type of the security breach which *degrades* the performance of the dynamic network. In this work, a swarm based defense technique, Artificial Bee Colony (ABC) algorithm is used to find the alternate path between the cluster nodes which are attacked by jammers. For each cluster node employee bee and onlooker bee are broadcasted for defining communication by calculating the probability of fittest value of destination node. Once the jammers are detected the alternative path is defined and data is transmitted through those links.**

Keywords: **Artificial Bee Colony algorithm, Vehicular Adhoc Network.**

I. INTRODUCTION

A. Overview of Vanet:

The recent development in the domain of wireless communication facilitates the creation of new system like Vehicular Adhoc NETworks(VANETs). The management process of resource and breach in security are complicated in adhoc network because the networks are changeable. Especially the physical and the MAC layers are more vulnerable than other layers because they are built on distributed systems and fluctuating radio channel. Thus, it is not easy to know when the transmitted data packets are not properly reached the destination, when there is any attack is happened. The Vehicular Adhoc NETwork (VANET) participant elements are vehicle and Mobile Adhoc NETwork (MANET) participant elements are mobiles that is the main difference between the VANET and MANET networks. VANET network communications are usually occurred between the vehicles to vehicle or vehicle to infrastructure and frequency over these communication channels are approximately 5.9GHz [1].It can be defined as nodes or vehicles and when a car or other transportation vehicles get in or out the topology it makes the change. Beside, using this mode, vehicles can directly make a connection with each other without any proper structure over them. Thus, VANET can be defined as a collection of connected vehicles hosts that are connected by wireless network interfaces. It forms a temporary network topology without any stable infrastructure or consolidated administration. In this network, the vehicles are equipped with wireless transmitters/receivers using antennas that can broadcast the vehicle coverage to all other vehicles in that same network. Besides, the network can be viewed as a random like nonentity graph at a specific time. This random graph is created due to the vehicle movements, and their present area etc. and their transmitter/receiver coverage area patterns, the battery power levels of transmission, and the co-channel collision levels are also used to provide the better communication over the network.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 2, pp: (40-46), Month: May - August 2016, Available at: www.noveltyjournals.com

B. DoS Attacks:

One of the main challenge in designing VANETs, is their vulnerability to Denial-Of-Service (DoS) attacks [4]. In the wireless networks, there is a lack of research for preventing such attacks in VANET networks. Due to deployment in different environments such as highway, high density vehicle places and they are exposed to be attacked by malicious intruders.

Two major DoS attacks are:

- Greedy behaviour
- Jamming attacks.

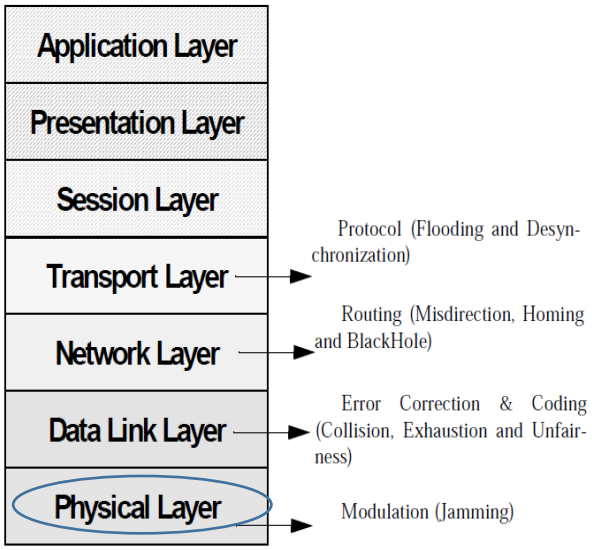


Fig.1 DoS attacks in various layers of the VANET networks.

The physical layer attacks are mainly in modulation that is mentioned

C. Swarm Based Intelligence:

Swarm Intelligence, is an algorithm that models the collective behavior of social insects, namely the ants, bees, birds, slime mold, etc. Ant system is the type of swarm intelligence it is used to form an evolutionary algorithm. The initial set of node agents traverse throughout the nodes in a random manner, and once they reach their destinations, they deposit pheromone on trails is used to make the communication indirectly with the other ants. The probability that the route taken by the follower ant is depend on the amount of pheromone left by the previous ant agents. Thus Artificial Bee Colony (ABC) which is also a swarm intelligence based optimization approach (Dervis 2005) is used to detect jamming attack. It is a heuristic algorithm based on swarm intelligence rather than evolutionary process.

II. LITERATURE SURVEY

The measure of correlation between errors and correct reception time is used to detect the presence of interference in Vehicular Adhoc NETworks. The Correlation Coefficient (cc) that means the similarity and dissimilarity between the nodes that is used in the process of corresponds to a statistical measures of relation between two random variables. Which is explained by Lynda Mokdad et al [1].

As per the research of Dervis Karaboga [2] about the swarm based intelligence, it is shown that the intelligent agents or swarms are self-organised.

The intrusion detection techniques are defined by Ashish B. Raut et al. [10], about intrusion detection over unsecured VANET by using validation process over network.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 2, pp: (40-46), Month: May - August 2016, Available at: www.noveltyjournals.com

III. PROPOSED METHOD

A. System Architecture:

The input of the system is a jammer affected cluster. The broadcast of bees can be done in many ways. As the objective of the system is to compare and analyze the required range for the transmission. The jammer affected cluster is examined and find the alternative path by using artificial bee colony algorithm. The broadcasting of bees is the initial step to find the alternative path.

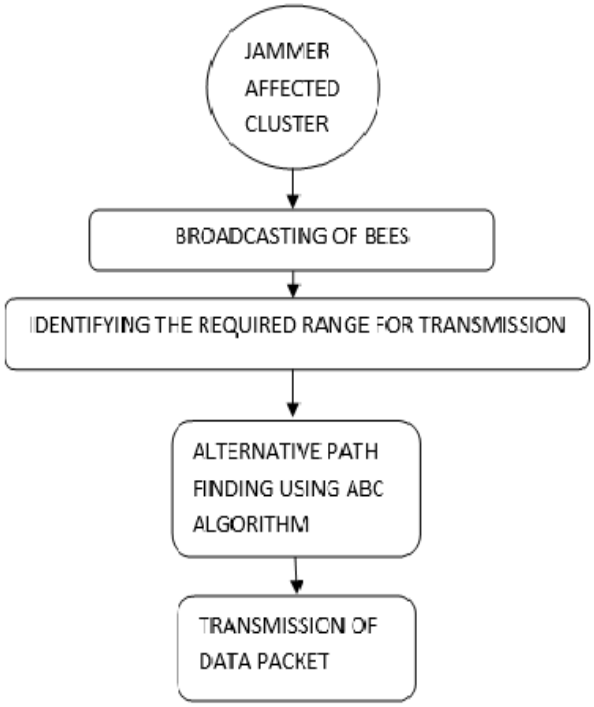


Fig.2 The diagram depicts the bee broadcasting among the jammer affected cluster

B. Configuration of nodes:

Initially a topology which consists up of 100 vehicles in a considered cluster is made into a VANET network design. The employee bees and onlooker bees are set up into each node to collect information and to update the status of each node in the network. In ABC algorithm, the various positions of a food source represents a possible solution to the optimization problem and the nectar amount of a food source is equal to the quality (fitness) of the associated solution. The valid number of solutions in the population is depends on the number of employed bees or the onlookers bees of the same population.

C. Jammer Affected Cluster:

Constant jammers:

A constant jammer continuously produces high-power unwanted noise that represents random bits and also this bits are produced randomly. The bit generator does not pursue any media access control (MAC) protocol and that works independent of the vehicular network channel sensing or traffic on the channel.

Random jammers:

A random jammer operates randomly in both sleep and jam intervals. At the time of sleep interval, it sleeps regardless of any traffic on the network, and during jam session, it acts as a constant or reactive jammer. That jammer does not possess any MAC protocol. The PDR increases when the sleep interval increases and the packet size decreases.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 2, pp: (40-46), Month: May - August 2016, Available at: www.noveltyjournals.com

D. Detection of jammers:

In the Vehicular Adhoc networks, when there occurs any jamming it can be detected in such a way, where an employee bee is assigned a work to transmit data packets to a particular node. If the designated is attacked by any jammer, then the packet is dropped after the time interval until that the employee bee waits to transmit the packet. Once the employee bee becomes unemployed bee before the time interval by dropping the packets then it is a successful transmission otherwise it is failed due to jamming. The following are the metrics to detect the jamming attack,

Distance:

Distance is calculated initially when the wireless sensor nodes are set in the network is distributed in a 2D plane, by using with Euclidean distance $Dij = \sqrt{(Xi - Xj)2\ (Yi - Yj)2}$ where i is the source vehicle , j is the destination vehicle, and (Xi,Yj) are the Cartesian coordinates of the vehicles.

Energy:

Detection probability and power usage by different jammers, such that constant jammers have highest discovering probability and highest power consumption while intelligent jammers are best for their least discovering probability and power consumption. In an optimal omniscient jammer is deliberated that jams ACK (acknowledgement) using probabilistic model. Moreover, it takes a pulse width of 22μs to jam ACK (acknowledgement) at a rate of 1 Mbps (Mega Bits per Second). However, the process of discover the transmission of ACK (acknowledgement) due to its very short length. Measurement between two random variables (random vehicles) is find out by Statistical correlation between them and it is used to discover a jamming attack. In this case, the correlation strongly exists between wrength and correct reaction time. Correlation coefficient and error probability (EP) could have the ability to define the threshold by highest value of slope that any couple of iteration. Certain predefined EP and estimated threshold is used to find the relationship and it is also to be checked. If the relation among the vehicle is within the threshold, then it is considered non-jammed, or else, it is jammed.

Packet delivery ratio:

Packet delivery ratio =

$$\frac{\textbf{No of packets correctly received}}{\textbf{Total no of packets received}}$$

For an Vehicular Adhoc environment the PDR ratio is depend on noise and inference the PDR measurement at the receiver side is the ratio of number of packets received and it is controlled by the cyclic redundancy check (CRC) to the total number of packets received.

PDR have two consistency checks, i.e., signal strength consistency check (SSCC) and location consistency check (LCC). PDR is directly proportional to the signal converse is not true. In case of LCC, an assumption is taken that all vehicles in the network have their neighborhood information from their upper routing layer. If a node observes low PDR, it compares it with that of its neighbor vehicles and decides whether the vehicle adhoc network channel is jammed or not. Moreover, the neighboring vehicles have to pass information about the location and update messages intermittently to the nearest neighbors. This is called communication overhead.

Packet loss ratio:

Packet loss occurs when the data packets are fail to reach their destination due to the data traffic or some other issues like overloading of data packets. Packet loss is different from the error types encountered in digital communication, the other main reason for the packet loss is unwanted noise over the network. Retransmitting missing packets causes the throughput of the connection to decrease. The sliding window protocols makes the throughput drop in the vehicular network and it's for acknowledgement of received packets.

THE MAIN STEPS OF THE ALGORITHM ARE GIVEN BELOW:

• Initialize.

• REPEAT.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 2, pp: (40-46), Month: May - August 2016, Available at: www.noveltyjournals.com

(a) Place the employed bees (initializing the process by sending the ACK) on the food sources in the memory;

(b) Place the onlooker bees on the food sources in the memory;

(c) Send the scouts to the search area for discovering new food sources.

• UNTIL (requirements are met).

Additionally, ABC consists of three control parameters:

a) ***Population size (SN)*** is the number of food sources (or solutions) in the population. SN is equal to the number of employed bees or onlooker bees.

b) ***Maximum Cycle Number (MCN)*** refers to the maximum number of generations.

c) ***Limit*** is used to diversify the search, to determine the number of allowable generations for which each non-improved food source is to be abandoned.

The Food Source Memory (FSM) is an augmented matrix of size SN *N comprised in each row, a vector representing a food source. Note that the vectors in FSM are sorted in ascending order, according to proximity cost function values.

$$FSM = \begin{bmatrix} x_1(1) & x_1(2) & \cdots & x_1(N) \\ x_2(1) & x_2(2) & \cdots & x_2(N) \\ \cdots & \cdots & \ddots & \cdots \\ x_{SN}(1) & x_{SN}(2) & \cdots & x_{SN}(N) \end{bmatrix} \begin{bmatrix} f(x_1) \\ f(x_2) \\ \vdots \\ f(x_{SN}) \end{bmatrix}$$

BASIC STEPS IN ABC ALGORITHM:

PHASE 1: EMPLOYEE BEES BROADCAST:

for $j = 1 \ldots SN$ **do**
  for $i = 1 \ldots N$ **do**
    $x'(i) = x_j(i) \pm r(x_j(i) - x_k(i)),$
    $\forall k \in (1, 2, \ldots, SN), \quad k \neq j$ and $r \sim (0, 1)$
  end for
  Calculate $f(x_i)$
  if $(f(x') \leq f(x_i))$ **then**
    $x_i = x'$
    $f(x_i) = f(x')$
  end if
end for

In this step, each employee bee is assigned to its food source and in turn, a new one is generated from its neighboring solution

PHASE 2: ONLOOKER BEES PHASE:

The onlooker bee has the same number of food sources as the employed. It initially calculates the selection probability of each food source generated by the employed bee in the previous step. The fittest food source is selected by the onlooker, using Roulette Wheel selection mechanism. The process of selection at the onlooker phase works as follows:

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 2, pp: (40-46), Month: May - August 2016, Available at: www.noveltyjournals.com

```
for i = 1 ... SN do
    r ~ (0, 1)
   sum_prob = 0
  j = 0
  while (sum_prob ≤ r) do
    sum_prob = sum_prob + p_j
    j = j + 1
  for k = 1 ... N do
    x'(j) = x_j(k) ± r(x_j(k) − x_j(m)),
    ∀m ∈ (1, 2, ..., SN)
  end for
  Calculate f(x_j)
  if (f(x') ≤ f(x_j)) then
      x_j = x'_j
      f(x_j) = f(x'_j)
  end if
end for
```

PHASE 3: SCOUT BEES BROADCAST

The scout bee carries out a random search to replace the abandoned food sources, using equation. The abandoned food source is one that cannot be improved upon after certain number of cycles, as determined by the limit parameter. Algorithm describes the process of the scout bee; In algorithm, Scout (i) is a vector of size (SN), which contain information related to the improvement of any of the food source during search.

```
for i = 1 ... SN do
  if (scout(i) = limit) then
    generate x_j using equation (3)
  end if
end for
```

The probability for the food sources to be selected increases with increase in its nectar quality.

ARTIFICIAL BEE COLONY ALGORITHM:

Input: Jammer affected cluster:

Output: shortest path between source and destination

Algorithm:

Initialize with random cluster

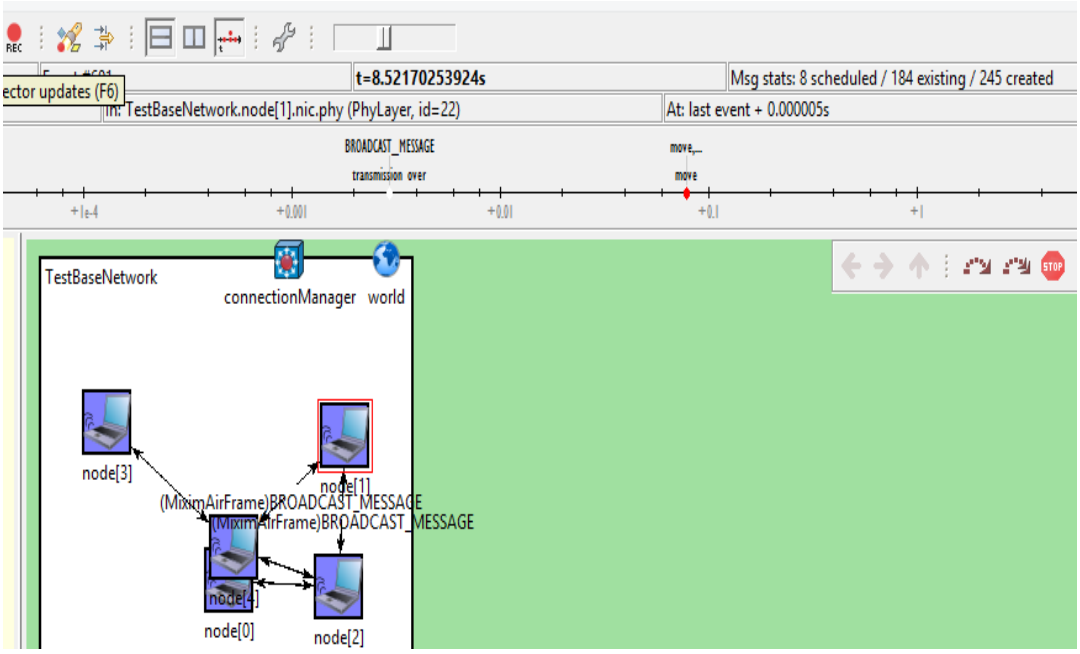
Repeat
Recruit bees for selected Cluster
Select fittest bees from each Patch
Assign remaining to search randomly
Until (Stopping Criterion)

Initialize

Repeat
Choose partial solutions
Expand partial solutions
Return to hive
Recruit nest mates
Until (Stopping criterion)

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 2, pp: (40-46), Month: May - August 2016, Available at: www.noveltyjournals.com

IV. ANALYSIS AND RESULT



The above pictures indicate the data packets transmission over the VANET nodes.

REFERENCES

[1] Lynda Pokdal, Jalel Ben-Othman, Anh Tuan Nauyen, "DJAVAN Detecting Jamming Attacks In Vehicle Adhoc Networks,"*El Savior Trans.*http://dx.doi.org/10.1016/j.peva.2015.01.003, *Feb* 2015.

[2] Dervish Karaboga, Bahriye Basturk "A Powerful And Efficient Algorithm ForNumerical Function Optimization: Artificial Bee Colony (ABC) Algorithm," Springer *Trans. Science + media, pp.459-471,*feb 2007

[3] Jaya Sehgal , Poonam Arora, "Delay Optimization In Vanet Using Ant Colony Optimization And Wi-Max", *Vol. 3, pp- 2278 – 8875,* Aug.2014

[4] Vikash Porwal, Rajeev Patel, Dr.r.k.Kapoor , "An Investigation Of Dos Flooding Attack In Vanet," International Journal of Advance Foundation and Research in Computer (IJAFRC), *Vol. 1, pp. 2348-4853, Dec. 2014*

[5] Pratik Gujar, Dr.P.R Balaji, "Bio-Inspired Routing Protocol For Vehicular Adhoc Networks," International Journal Of Advancements in Research & Technology, *vol.3, pp. 2278-7763, Apl. 2014*

[6] P. Saravanan, T. Arunkumar. "Bee Optimized Fuzzy Geographical Routing Protocol For Vanet" *Vol. 8, 2014*

[7] Hannes Hartenstein, Kenneth P Laberteaux "VANET: Vehicular Applications and Inter-Networking Technologies" *published in 2010*

[8] Salim Bitam, Abdelhamid Mellouk and Sherali Zeadally "Bio-Inspired Routing Algorithms Survey for Vehicular Ad-hoc Networks" *Dec 2014*

[9] R. Di Pietro, S. Guarino, N.V. Verde "Security In Wireless Ad-hoc Networks – A survey" http://dx.doi.org/10.1016/j.comcom.06.003 *Aug 2014*

[10] Ashish B. Raut1, Nandkishor P. Karlekar "A Survey on Efficient Intrusion Detection in Vehicular Ad-hoc Network" *vol-3, pp-416-419, Issue 12, Dec*

[11] Rutuja N. Kamble, Dr.P.R.Balaji, Dr.L.G.Malik, "Self Adaptive Broadcasting Algorithm for VANET using Bio Inspired Computing" *Vol.2, Issue. 3, Mar 2014.*