Middle-East Journal of Scientific Research
24 (Special Issue on Innovations in Information, Embedded and Communication Systems): 83-89, 2016
ISSN 1990-9233; © IDOSI Publications, 2016
DOI: 10.5829/idosi.mejsr.2016.24.IIECS.23144

A Robust Approach for Jamming Attack Detection in VANET

S.K. Bhavithra, K.P. Vijayakumar and P. Ganeshkumar

Department of Information Technology,
PSNA College of Engineering and Technology, Dindigul, India

Abstract: A vehicular ad hoc network (VANET) is an extension of *mobile ad hoc network* (MANET), where vehicles communicate with each other forming intelligent transport system (ITS). In upcoming generation it is predicted that all the vehicles will be facilitated by means of radio communication interface. This interface can be interrupted by means of jamming which prevents authenticated vehicles from sending and receiving information. In the proposed work, the presence of jamming is identified by using fuzzy algorithm for both localized and non-localized vehicles. Vehicles are localized using localizability-aided-localization (LAL) approach. If the jamming attack is identified in a chosen path on which the information to be sent to the receiver vehicle, then information is sent in an alternate path.

Key words: VANET · Jamming Attack · LAL · Fuzzy

INTRODUCTION

Vehicular ad hoc network (VANET) is an advanced form of Mobile ad hoc networks (MANET) where mobile nodes are replaced by vehicles in VANET. These vehicles communicate with each other forming an intelligent system. Communication is done in VANET by means of communication unit. Generally there are two modes of communication in VANET: (i) vehicles can communicate with each other for the purpose of exchanging the information among them which is termed as vehicle-to-vehicle (V2V) communication, and (ii) vehicle communicate with the infrastructure that is present along the road which is termed as vehicle to infrastructure (V2I) communication [1]. Thus they exchange information for the purpose of providing warning messages in places of threat, any damages in road, traffic jam etc., and thus VANET is termed as intelligent transport system which takes place in the day-to-day life.

These communication between vehicles are interrupted by several kinds of attack. One of the most important attacks is jamming attack which occurs in physical and MAC layer of the OSI model. Jamming attack is a kind of denial of service (DOS) attack which is the threat to availability of the network.

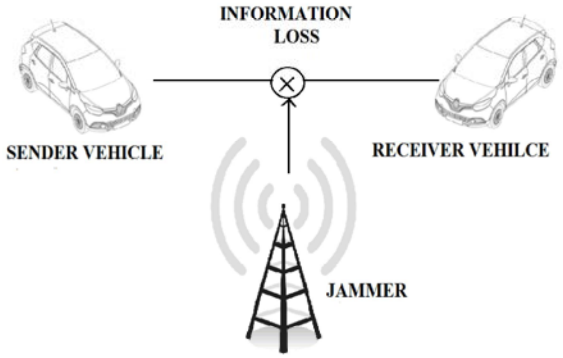

Fig. 1: Jamming Attack

A jammer as shown in Fig. 1 is an entity who is purposefully trying to disrupt the physical transmission and reception of wireless channel communications. A jammer continuously emits radio frequency signals in a wireless medium so that legitimate traffic will be completely blocked. A jammer can be a vehicle or even the road side unit can be a jammer.

In general, when authenticated sender wants to transmit data to receiver then a path is established between sender and receiver. In presence of jammer, the sender vehicle cannot send packet to receiver vehicle and

Corresponding Auhor: S.K. Bhavithra, Department of Information Technology,
PSNA College of Engineering and Technology, Dindigul, India.

the information sent along the path has been lost. Even though both sender and receiver are legitimate vehicle, there will be no transmission of packets between them, and the emergency information cannot be reached to the receiver vehicle in a reasonable amount of time causing inefficiency and uncomfortableness during travel. Thus jamming attack is considered to be most serious attack and it has to be detected as early as possible.

Thus jamming attack detection is more important because the safety-related and real time information has to be send to the receiver vehicle in time. There should not be any delay. Whereas in presence of jamming the information is not delivered in time. This causes huge problem which is concerned with the life of passengers. Thus an efficient approach is needed for determination of the jamming attack both for localized and non-localized vehicles but whereas in paper [1-3] focuses only on the vehicles within the communication range. The objective of the work is to detect the presence of jamming attack for both localized and non-localized vehicles where non-localized vehicles are localized using Localizability-aided-localization (LAL) approach and jamming attack is identified with help of fuzzy logic using three parameters like Packet drop ratio, delay and throughput.In order to provide security for the packet sent RSA algorithm is used for providing security to the information sent to receiver vehicle. Finally, LAL Perimeter Stateless Routing protocol is used for the mitigation of jamming attack.

The rest of the paper is organized as follows, the section 2 discusses the related work. The proposed work is presented in section 3. The section 4 discusses the simulation result. Finally the section 5 concludes this paper.

Related Work: Many researches have been performed on detecting jamming attacks in vehicular ad hoc networks. In this section, the brief description on recent and other relevant works for jamming attack detection is discussed. In [1] the vehicles within the communication range is considered and by using decrease in PDR value the jamming attack has been determined. It uses Markov Chain model to calculate loss probabilities, dropped packets, means of corrupted and non-corrupted packets. Numerical results are done using Gauss- Seidel method where both sender and attacker nodes are kept stable. The limitations are it detects the presence of jamming only during line-of-sight conditions and communication range is limited. There is no security provided in the work.

It is used to detect a particular class of jamming attack where the jammer transmits only when valid radio signals come from its radio hardware. Its detection model is based on the error distribution measurement. Correlation coefficient is measured as a relationship among the two parameters. Thus it is measured the between error and the correct reception time for the purpose of identifying the presence of jamming attack [2].

In wireless ad hoc networks physical jamming, virtual jamming and collision probability are considered. Here the principle of collision is used for estimating the presence of jamming attack. It is said that collisions that occur due to hidden & exposed terminal and network congestion is similar to the collisions that occur due to jamming attack, hence it is most difficult to determine the presence of jamming attack [4]. VADD is based on the idea of carry and forward. The most important issue is in selecting a forwarding path has been chosen with the smallest packet delivery delay. It is used to forward the packet to the best path with the lowest data delivery delay. The results of VADD [3] are shown with the help of parameters like protocol overhead, packet delay and packet delivery ratio. Generally VANET supports a range of 1000m to achieve performance in communication and the limitation here is that it uses only short range wireless channel which covers only about 100m-250m. Though the vehicle outside this particular range cannot be communicated.

The jamming attack in [5] is determined in a platoon. Platoon is nothing but it is an example of vehicular ad hoc networks. It deals with “jamming” of position messages (beacons) exchanged by vehicles periodically in a platooning scenario. With the help of two different attacker model it determines probabilities of attack detection and false alarm. The parameter used in the detection of denial of service attacks is packet error ratio (PER). Only two types of jamming is considered: random jamming and on-off jamming. It also uses only a short range communication and outside the range the packets are not transmitted which a major limitation. Vehicular ad hoc network is called as intelligent transport system. In [6] Location-Based Routing Algorithm along with Direction Cluster-Based Flooding (LORA-DCBF) has been used. The parameters used are end to end delay, routing overhead and delivery ratio. It has three main advantages that are 1) local information for improving routing efficiency 2) minimizes flooding by disseminating the packets 3) the two cluster heads which operate in the limited area. Here the communication range is limited since the vehicle that move out of the region, the cluster head cannot be able to communicate with that particular vehicle and hence the communication is interrupted. In wireless sensor network an intrusion detection system is made in [7] and the jamming attack is estimated based on two parameters PDR and RSSI in a cluster based network. A novel approach has been proposed for jamming attack detection in [8] where the behaviour of each nodes are estimated and jamming attack is determined by the cluster head among each clusters.

Thus researches have focused only on the localized vehicles for the determination of jamming attack. But in real world the vehicles may go out of range and the information cannot be delivered in a reasonable amount of time. Hence the proposed work enables in identifying the location of non-localized vehicle and transferring the information successfully to that particular vehicle even in the presence of jamming attack.

Proposed Work: In proposed work, the attack model is kept mobile, where all vehicles are considered to be moving. The presence of jamming attack is determined with help of 3 parameters which are packet drop ratio, delay and throughput.

Recursion Algorithm: Recursion algorithm is used for estimation of space priority and buffer sharing. The recursion algorithm is a type of iteration algorithm which calls itself which calls the loop with small value and it performs operations for the particular input given at a time and outputs the result.

It overcomes the overhead of DJAVAN [1] where it used markov chain process for the estimation of distance between the vehicular nodes which is a memory less process. Space priority is distance between the vehicular nodes in the network. It is estimated for transfer of information to the receiver. Buffer sharing denotes the amount of data sent to the receiver vehicle in the network. Both the estimation of space priority and buffer sharing are estimated during run time.

Securing The Messages: The messages are transmitted in a wireless channel in VANET. Since these wireless channels are prone to several kinds of threats and attacks, the message has to be delivered to the receiver vehicle in a secured manner. For providing security to the data sent RSA algorithm is used. RSA is most widely used public-key cryptography and it is considered to be the most secured since it uses two random prime numbers for producing private and public keys.

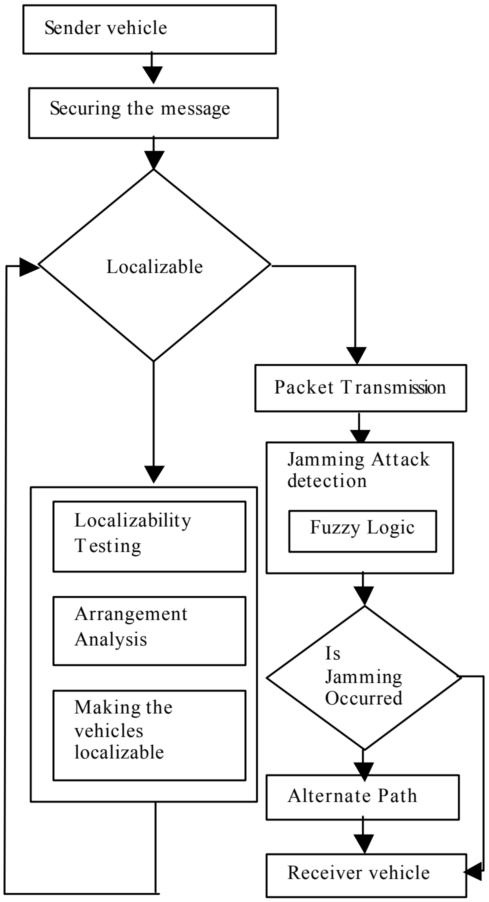

Fig. 2: Flow chart of proposed work

Input: Consider S as the Sender vehicle and R as receiver vehicle where both have separate set of public and private key which has to be transmitted in a public channel in secured manner, these are to be followed:

Step 1: Both S and R publish their public key into the communication medium.

Step 2: Now S receives R's public key from the communication medium.

Step 3: S encrypts the message M using R's public key and it produces a message which is secured $M_{s.}$

Step 4: This message M_s is transmitted in the communication medium.

Step 5: Once the message M_s is received the receiver vehicle R decrypts the message using its private key which produces the original message M.

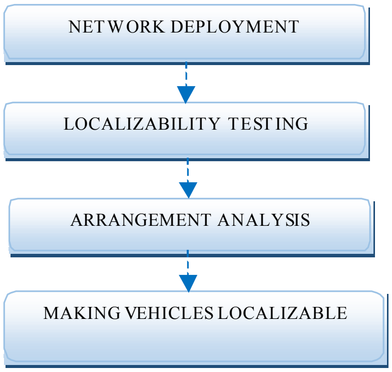

Fig. 3: Structure Analysis

Structure Analysis: In existing approach, the detection of jamming attack are limited only to localized vehicular nodes or the vehicular nodes within the communication range. But it is necessary to transmit the information to receiver within a reasonable amount of time. For making the transmission quicker, we have to know the exact location of the vehicular nodes and also transmit the packet to the vehicular nodes which are outside the cover area i.e., the non-localized vehicular nodes. The position of the non-localized vehicles are identified using Global Positioning System (GPS) and Localizability aided localization (LAL) approach is used to make the non-localized vehicles as localized. It involves 3 steps as in Fig. 2 making the receiver vehicle localizable.

Step1: Localizability testing of vehicles:

Vehicles move in a random manner in a vehicular ad hoc network, some vehicular nodes are localized under the specified communication range and rest of the vehicles are outside of the specified communication range i.e., they are non-localized. Using LAL approach, vehicle localization is performed to identify the location of the vehicles which are localized and non-localized.

Step 2: Analysis of the arrangement of vehicles:

This step is done to identify the most exact location of the vehicles and hence this approach is considered to be the most important fine-grained step. In order to implement this step, a graph is constructed based on the distance between the vehicles. This graph is decomposed in a manner the two edges are connected. These vehicles are then organized in tree structure where the root node is sending Periodic beacons (P_B). These Periodic beacons (P_B) nodes are RSU which is used to find the exact location, speed, movement of the vehicles. Then the adjustments in the tree stricture are carried out from the root node to every leaf node.

Step 3: Making the vehicles localizable:

The vehicles are organized in the tree and tree is constructed based on the location of vehicles. If the vehicles within the range, then find the location using periodic beacons and if vehicles lie outside the range, then find the location of vehicles of the neighbor vehicle by sending a beacon signals and identify the location. This step is repeated until making the receiver vehicle localizable by using location and localization technique. Once the location of the receiver vehicle is identified and localized, the information is sent to the vehicle within the reasonable amount of time. Since vehicular ad hoc network is an intelligent transport system and is concerned with safety of passengers the information has to be sent quickly to the receiver vehicle.

Input: A 2- edge connected graph G_i, and localizability Vector of vehicles.

Output: Making non-localized vehicles localizable.

```
1)  if $G_i$ is $G_A$ then
2)   for each non-localizable vehicles $v_i$ belongs to $G_i$
3)   do
4)   if vehicle in vertex vi has localizable neighbour
5)   then
6)   Add $v_i$ into a set VD.
7)   end if
8)   end for
9)   for each vehicles $v_i$ belongs to VD
10)  do
11)  Add edges according 1)
12)  Mark $v_i$ localizable.
13)  end for
14) end if
15)  flag $\leftarrow$ 1
16)  while not all vehicles in $G_i$ are localizable and flag ==1
17)  do
18)  flag $\leftarrow$ 0
19)  for non-localizable vehicles $v_i$ belongs to $G_i$
20)  do
21)  x= amount of localizable 2-hop neighbours
22)  if x > 3 then
23)  Add edges according 2)
24)  Mark $v_i$ as localizable.
25)  flag $\leftarrow$ 1
26) Apply 3)
27)  end if
28)  end for
29) end while
30)  for each vertex $v_k$ marked non-localizable in $G_i$
```

```
31) do
32) Vertex augmentation $v^2_K$
33) end for
```

- Some non-localizable vehicles have a localizable neighbour. Such localizable neighbour has at least three vertex-disjoint paths to three P_B. Adding two edges which connect two neighbour vehicles (of the localizable one) on different vertex-disjoint paths to the non-localizable vehicles is enough to make the non-localizable vehicle localizable. Only one edge is needed if a non-localizable vehicle has two localizable neighbours in GA.
- If a non-localizable vehicle has three or more vehicles in two-hop distance, connecting it to three localizable vehicles makes it localizable.
- Some vehicles are not localizable in the original network topology due to the lack of P_B. If three vehicles are adjusted to be localizable in a fully rigid component, the vehicle is immediately localizable without extra manipulation.

Jamming Attack Detection: Once analyzing the location of the vehicular nodes, the encrypted information is sent into the communication channel and the attack is identified in the running time environment. The parameters used in the identification of the attack are loss ratio, delay and throughput. The trace file is generated while execution of the program and awk scripting is used to retrieve the values that are stored in the trace file. The values of the parameters are sent as the input to the fuzzy algorithm which determines the presence of the attack. Once jamming attack is identified it can be mitigated by the use of LAL perimeter stateless routing protocol.

Pseudo Code:

```
1)  Define a Network with N number of vehicular nodes
2)  Set the Sender vehicle S and Receiver vehicle R
3)  Set Prenode=S as Present Node
4)  While PreNode <> DestNode [Repeat Steps 5 to 24]
5)  Identify the list of neighboring vehicular nodes to PreNode called Pe(1),Pe(2).....Pe(M)
6)  {
7)  For i=1 to M
    {
8)  Identify the Analysis parameter for each Neighbor vehicle called Packet Drop Ratio, Delay , Throughput
9)  If (Fuzzy(Packet Drop Ratio (Pe(i)), Low), Fuzzy (Delay(Pe(i)), Low) and Fuzzy (Throughput (Pe(i)), High)
10) {
11) Set Priority(Pe(i))=High
12) }
13) Else If ( Fuzzy (Packet Drop Ratio (Pe(i)), Medium),Fuzzy(Delay(Pe(i)), Medium and Fuzzy (Throughput (Pe(i), Medium)
14) {
15) Set Priority(Pe(i))=Medium
16) }
17) Else If (Fuzzy(Packet Drop Ratio (Pe(i)), High), Fuzzy(Delay(Pe(i)), High and Fuzzy (Throughput(Pe(i),Low)
18) {
19) Set Priority (Pe(i))=Low. (Vehicle causing jamming is found)
20) }
21) }
22) Find the Vehicle with MinPriority called JN
23) Set PreNode= JN (JAMMED NODE)
24) }
```

Jamming Attack Mitigation: Once the attack has been identified by using fuzzy logic, it is necessary to send the messages to particular receiver vehicle since it carries real-time information. Hence the attack should be mitigated by successfully transmitting the messages to the receiver vehicle. The attack is mitigated by using LAL perimeter stateless routing protocol.

This protocol exploits the position and connectivity in VANET, by using the position of vehicles for message forwarding mechanism to particular receiver vehicle. It forwards packets to vehicles which are closer to the receiver vehicle.

Simulation Results: This session shows simulation results of my proposed work which has been implemented in NS2 software version 2.3.5 [9-11]. Every vehicular node move in a random manner with no stop time. In this simulation setup vehicular nodes are randomly deployed. All vehicular nodes in the network have same transmission range of 300 meters . Proposed system uses three metrics to determine the presence of jamming attack namely 1) Packet Drop Ratio 2)Delay 3)Throughput which are calculated for different time and different messages sent across the VANET.

Packet Drop Ratio (PDR): Packet Drop Ratio is the number of packets lost across the network without reaching the destination vehicle. The Fig. 4 shows that in DJAVAN [1] the number of packets dropped has been increased since it forwards to nearest RSU, whereas in proposed using LAL the packet decreased has been increased since the attack is mitigated.

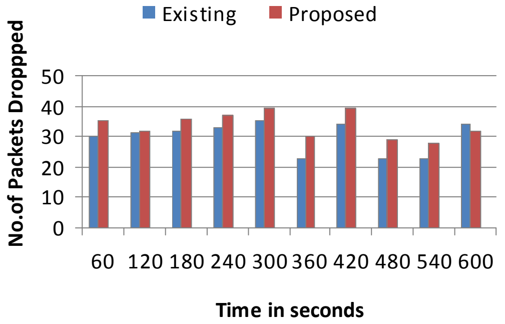

Fig. 4: Packet Drop Ratio

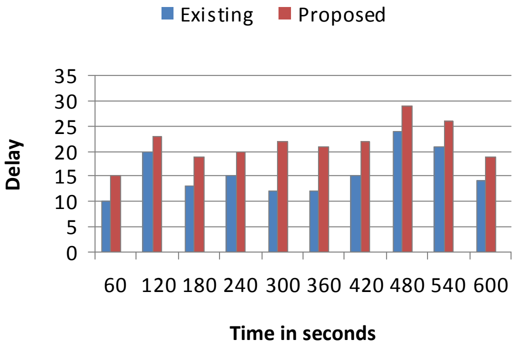

Fig. 5: Delay

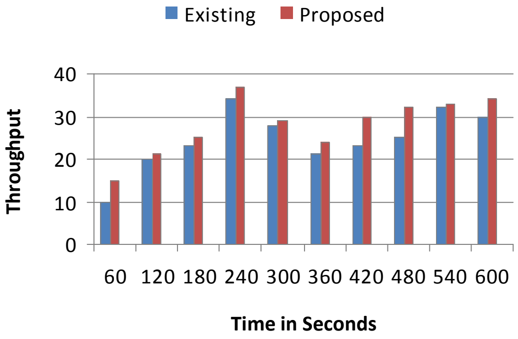

Fig. 6: Throughput

Delay: Delay is time required for our message to reach the destination. Thus the delay has been decreased in the existing approaches whereas delay in proposed system is more since there is successful transmission of packet since the information has been reached to the receiver vehicle as in Fig. 5.

Throughput: Throughput is the number of successful message reached to the destination vehicle. In proposed work, the throughput has been drastically increased which denotes the best performance of the system as shown in Fig. 6

CONCLUSION

VANETs due to nature of distributed systems are vulnerable to several kinds of attack. The most important is Denial of Service attack such as greedy behavior and jamming attack. The goal of jammer is disrupt the communication between authenticated sender and receiver vehicle in transferring the messages among them, which decreases overall QoS. Detecting such an attack is most important but VANET does not have centralized management and it is that vehicles move in a high speed form dynamic topology. Thus the solution has to be made in a distributed manner and should be implemented despite of physical and MAC layer features to avoid the definition of firmware.

Thus a robust approach has been designed for the determination of jamming attack in VANET. RSA algorithm is proposed for maintaining security of the information sent along the communication channel. In existing approach, for the determination of jamming attack the communication ranges are kept limited and only within the range the presence of jamming attack has been determined but by using Localizability-Aided-Localization approach for determining the location of the vehicles and making non-localized vehicles as localizable. Fuzzy logic is used for estimation of the presence of jamming attack. On determining the presence of jamming attack LAL perimeter stateless routing protocol has been used for choosing an alternate path to reach the receiver vehicle. The simulation result of the proposed work is quite promising where the presence of jamming attack is estimated with high degree of confidence. The future work focus on implementing game theory using a reaction mechanism and to cope up with several kinds of attacks.

ACKNOWLEDGMENT

This work is based upon research project – Implementation of processing power calculator in Ad Hoc network nodes to obtain overall energy consumption (processing+radio), AICTE research project under Research Promotion Schemes (RPS):File No.:20/AICTE/RIFD/RPS(POLICY-1)20/2013-14.

REFERENCES

1. Lynda Mokdada, Jalel Ben-Othman and Anh Tuan Nguyena, 2015. DJAVAN: Detecting jamming attacks in Vehicle Ad hoc Networks, Elsevier., L. Mokdad et al. Performance Evaluation., 87: 47-59.

2. Hamieh, A., J. Ben-othman and L. Mokdad, 2009. Detection of Radio Interference Attacks in VANET, Global Telecommunications Conference, pp: 1-5.
3. Jing Zhao and Guohong Cao, 2008. VADD: Vehicle-Assisted Data Delivery in Vehicular Ad Hoc Networks, Vehicular Technology, IEEE Transactions, 57(3): 1910-1922.
4. Geethapriya Thamilarasu, Sumita Mishra and Ramalingam Sridhar, XXXX. Improving Reliability of Jamming Attack Detection in Ad hoc Networks, International Journal of Communication Networks and Information Security (IJCNIS), 3(1).
5. Nikita Lyamin, Alexey Vinel, Magnus Jonsson and Jonathan Loo, 2014. Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks, IEEE Communications Letters, 18(1).
6. Momeni, S., 2008. Iran Univ. of Sci. & Technol., Tehran Fathy, M.2008. “VANET’s Commuincation, Spread Spectrum Techinques and Applications, IEEE, pp: 587-591.
7. Ganeshkumar, P., K.P. Vijayakumar and M. Anandaraj, 2016. A novel jammer detection framework for cluster-based wireless sensor networks, EURASIP Journal on Wireless Communications and Networking.
8. Vijayakumar, K.P., P. Ganeshkumar and M. Anandaraj, 2015. A. novel jamming detection technique for wireless sensor networks, KSII Transactions On Internet And Information Systems, 9(10).
9. ITSSv6 Project. [Online]. Available: http:// www.lara.prd.fr/ projects/itssv6
10. http://www.isi.edu/nsnam/ns/ns-tutorial/index.html
11. Tutorial - Marc Greis's tutorial