Mitigation of Jamming Attack in Vehicular Ad hoc Network

Rohini Rawat¹, Dr. Deepti Sharma²,

M-Tech Student, Department of CSE, Advance Institute of Technology and Mgt, Palwal, Haryana, India¹
HOD, Department of CSE, Advance Institute of Technology and Mgt. Palwal, Haryana, India²

Abstract— Vehicular Ad-hoc Network (VANET) is taking more attention in automotive industry due to the safety concern of human lives on roads. Security is one of the safety aspects in VANET. To be secure, network availability must be obtained at all times since availability of the network is critically needed when a node sends any life critical information to other nodes. However, it can be expected that security attacks are likely to increase in the coming future due to more and more wireless applications being developed and deployed onto the well-known expose nature of the wireless medium. In this respect, the network availability is exposed to many types of attacks. In this paper, jamming attack on network availability is presented and also provide a RTS/CTS mechanism to mitigate the jamming attack in VANET. A model to secure the VANET from the jamming attacks has been developed and gives a possible solution to overcome the attacks have been discussed.

Keywords—Vehicular Ad hoc Network (VANET); security; availability; security attack; Jamming Attack

I. INTRODUCTION

Vehicular Ad-hoc Network (VANET) is a kind of networks in which vehicle nodes can communicate in multihop fashion with each other on the road [6]. Vehicular Ad-hoc Networks have recently drawn interest of researchers and industry due to their potential to improve road safety and traffic coordination[7]. The packets that are exchanged require timely and reliable delivery which poses a real challenge to VANETs. Security is a vital issue where little interruption, such as intermittent disconnections can create problem to the users. This is particularly crucial if critical life information is being communicated between a sender and a receiver. In this paper, we consider a particular class of DoS attacks called Jamming. In fact, the vehicle nodes in vehicle ad hoc networks share a wireless medium. Thus, a radio signal can be jammed or interfered, which causes the message to be corrupted or lost. If the attacker has a powerful transmitter, a signal can be generated that will be strong enough to engulf the targeted signals and disrupt communications. Jamming decreases the performance of network by affecting its throughput, network load, end to end delay etc. There are many different attack strategies, a jammer can performed, exposed below [5]:

II. LITERATURE REVIEW

Mario Strasser et al. considers the problem of how can two devices that do not share any secrets establish a shared secret key over a wireless radio channel in the presence of a communication jammer. An inherent challenge in solving this problem was that known anti-jamming techniques (e.g., frequency hopping or direct-sequence spread spectrum) which should support device communication during the key establishment required that devices should shared a secret spreading key (or code) prior to the start of their communication. This requirement created a circular dependency between anti jamming spread-spectrum communication and key establishment. The author proposed an Uncoordinated Frequency Hopping (UFH) scheme that breaks the dependency and enables key establishment in the presence of a communication jammer. The author performed a detailed analysis of UFH scheme and showed its feasibility, both in terms of execution time and resource requirements[1].

Hasbullah H. et al. explained the need to obtain network availability all the time in order to ensure security. Authors categorized DOS attacks into three categories: 1) Basic Level (overwhelm node resources). 2) Extended level (jamming the channel). And 3) Distributed Denial of Services (DDOS). A proposed solution was given based on relying on utilizing the On-Board-Unit (OBU) that each vehicle is equipped with. OBU is supposed to make a decision as to prevent a DOS attacks using one of the proposed techniques (switching channels, technology or use frequency hopping) to avoid DOS attack[2].

S. Babar et al. studied jamming attack intensively. It classified jamming attack into active and reactive jamming. Authors evaluated the impact of different types of jammers using NS2 simulation. The data was analyzed to show that reactive jamming is more difficult to detect than other attacks because of the intelligent behaviour. The paper contribution suggested using the behavioural modelling and analysis tools to understand jamming attacks behaviours to develop an efficient defence strategy[3].

Longquan Li et al. represents Self-Healing Wireless Networks under Insider Jamming Attacks in 2014 In this work, they
design a protocol that was capable of self-healing wireless networks under jamming attacks. The protocol identified and excluded an insider jammer and then restores normal data communications among benign nodes despite the presence of jamming by an initially unknown compromised node. The proposed scheme integrate key management, jammer identification and jammer isolation in one system. Finally, they evaluated the protocol with USRP devices and GNU Radio in the context of jammer localization. The experiments showed that the proposed protocol must identify and isolate the insider jammer with high accuracy[4].

III. PROPOSED METHOD
The RTS/CTS mechanism is a handshaking process that minimizes the occurrence of collisions when hidden nodes are operating on the network. The working mechanism of RTS/CTS implementation is shown in figure 1.

The AP mobile node receives RTS data from Mobile node A and replies to it with a CTS frame while authenticating it to send data. Meanwhile, the Mobile Node B receives the CTS frame since the Mobile Node A is sending data and the mechanism informs the mobile Node B that the AP is transmitting or receiving data at that time frame. This makes Mobile Node B to wait for a particular time. When a jamming attack is launched on the network, fake RTS frames are sent to the AP mobile node that keeps the medium busy and prevents other nodes from being able to commence with legitimate MAC operations, or introduces packet collisions causing forced and repeated back offs.

The algorithm is as follows:

1. Deploy the nodes.
2. Use RTS & CTS frames for reliable communication.
3. Set the maximum number of packets to be sent by the requesting node/replying node as a Packet_Threshold.
4. Check for each requesting/replying node
   
   If Packet_Sent > Packet_Threshold
   then
   Declare the node as the attacker node.
   
5. Display the list of blocked nodes in the network. The blocked node will not be able to participate in the further transmissions.

IV. SYSTEM MODEL
A. Description of the First Scenario
This scenario consists of 100 mobile nodes deployed randomly in the area of 50*50 km. Nodes move in this area on the basis of random waypoint mobility model with a constant speed of 10 m/s. With the help of this algorithm, random trajectories of the mobile nodes have been set. The ad-hoc routing protocol is changed accordingly as per the requirements of the simulation study in order to analyze the results under a particular protocol i.e. AODV or DSR. Here, the start time is taken as 10 seconds and the stop time is set to the end of the simulation. The packet inter-arrival time and the packet size is set to 0.03 seconds (exponential) and 2000 (exponential).

The scenarios are simulated and analysed on the basis of two parameters- Throughput and Delay.
1. Throughput- Represents the total number of bits (in bits/sec) forwarded from wireless LAN layers to the higher layers in all WLAN nodes of the network.
2. Delay- Represents the end to end delay of all the packets received by the wireless LAN Macs of all the WLAN nodes in the network and forwarded to the higher layers.

The simulation was performed for 300 seconds while the number of seeds used was 300 in order to provide 1 hour simulation performance.

B. Description of the Attack Scenario
Here, we have placed two jammer nodes in order to engage the physical jamming attack in the network.
The physical jamming is launched by continuous transmissions and/or by ensuring packet collisions at the receiver. The jammers leading to these attacks can deny complete access to the channel by monopolizing the wireless medium. The nodes trying hard to communicate have an unusually large carrier sensing time waiting for the channel to become idle. The jammer used here is mobile pulse jammer. Jammers also need to be configured according to the network’s requirements. Here, the trajectory of the jammer nodes is set to VECTOR. The jammer bandwidth is set to 100000 and the jammer base band frequency is taken as 2402. The pulse width is taken as 2.0. The start time and the stop time are set to 10 seconds and end of the simulation respectively.

C. Description of the Third Scenario
In order to implement the proposed technique for the detection of the physical jamming attack, following detection technique is proposed.

Proposed Technique
In order to enhance the throughput of the entire network, the presence of the jammer node is very necessary to be stated. Various techniques were opted for the discovery, prevention and mitigation of the jamming attack. In order to enhance the throughput and decrease the delay as compare to the existing approaches, a meliorated detection mechanism is proposed in this dissertation, for the detection of the physical jamming attack.
1. In case, if packet size exceeded to a particular RTS threshold, that packet would have to wait for a particular RTS/CTS interval in order to completely forward that packet to its destination. So, the buffer size is taken as 10240000.
2. Also, high data rate of 54 mbps is taken which were previously 11 mbps during the simple and the attack scenario.
3. The value of the physical characteristics is set to Extended Rate PHY.
4. So, apart from performing the modifications in the data rate and buffer size for the prevention of penalties caused by the drawbacks of the existing techniques and in order to improvise the throughput, improved AODV parameters are also adopted. Here, the active route timeout is taken as 30 seconds.

V. PERFORMANCE RESULTS
Scenario 1 represents the scenario with no malicious event and normal network state, scenario 2 represents the network that is under the jamming attack and scenario 3 represents the mobile jammers and implementation of the proposed method.

A. Throughput
It is clearly seen that the jamming attack decreases the overall network throughput in comparison to the normal network state. However, the entire network throughput is increased once the proposed unified mechanism is implemented.

Figure 3: Throughput of all three scenarios at 100 nodes
Figure 4: Throughput of all three scenarios at 200 nodes

B. End To End Delay

In first scenario of 100 nodes of our experimentation, packets delay with peak value of approx. 0.010 seconds. In second scenario which is with jamming attack, packets delay increases to value of approx. 0.35 seconds. In first scenario of 200 nodes of our experimentation, packets delay is approx. 0.0020 seconds. In second scenario which is with jamming attack, packets delay increases to value of approx. 0.30 seconds.

Figure 5: Delay of all three scenarios at 100 nodes

The recovery of the end to end delay decreases with our proposed mechanism by elimination of the jamming attack as end to end delay comes to similar to the value 0.000256 seconds. Thus our proposed mechanism eliminates jamming attack in network.

VI. CONCLUSION AND FUTURE WORK

The unified mechanism is implemented on the selected nodes on the network and deployed in the specific area. The findings of the research clearly states that, the implementation of such unified mechanisms have a significant impact on the overall network through positively. On the other hand, the implementation of such mechanisms does not only mitigate the jamming attack effects, it also increases the overall performance above the normal state of the network. We consider future research work focused on using real time attacks which is needed to ascertain greater degree of detection of specific vulnerabilities in both Mobile and ad hoc Sensor networks.

REFERENCE


