Real-Time Jamming Detection in Vehicular Network

Sharaf Malebary
Dept. of Computer Science & Engineering
University of South Carolina
Columbia, South Carolina USA
Sharaf_m2002@yahoo.com

Abstract— Intentional and unintentional radio interference are one of the most threats that disturb wireless networks and disrupting communication. Many papers have and still researching the jamming threat and their impact on wireless networks. In this paper we study the effect of launching jamming attack particularly in Vehicular-Ad hoc-Network (VANet). We build realistic jamming model and implement different jamming scenarios with respect to their mobility (Stationary, Random-Mobility and Targeted-Mobility) and behavior (Constant, Reactive and Random). We perform intensive experiments using NCTUns simulator to study the threat of jamming attack in urban and highway roads. Then we propose a new jamming detection scheme to allow each node in the vehicular network to detect jamming attack on its own. At the end of the paper, we run experiments to evaluate our detection method and ensure its feasibility and effectiveness.

Keywords— VANet; beacon; Security; Jamming Problem; Detection System; Vehicle Network; Jamming Behavior.

I. INTRODUCTION

The danger that drivers can face is not limited to vehicle malfunction but it includes road hazards, weather changes, and accidents on roads. The new era is moving toward making cars more intelligent to enhance drivers' safety. This can be achieved by utilizing cars to work as early warning devices against any type of hazards while driving. Implementing intelligent transportation system (ITS) was the first step to achieve this goal. ITS is a national program that intended to use modern computers and communications to make driving safer, smarter, faster and more convenient. To achieve these goals, ITS provides automatic toll collection, traveler information system, intelligent commercial vehicles and intelligent traffic control systems [2]. ITS is moving toward equipping cars with communication capabilities to allow vehicles to communicate and interact outside the boundaries of their own.

For the last 5 years, automakers and U.S. Department Of Transportation (DOT) have been investigating the feasibility of implementing VANet (Vehicle Ad hoc NETwork). The basic idea is to equip vehicles with communication capabilities to allow cars to act as nodes in a wireless network. As result, two different types of communications were introduced, vehicle-to-vehicle (V2V), and vehicles to Road Side Units (RSU). Many applications have been developed to make a use of the new technology. The purpose of some of these applications is to enhance drivers' comforts while others can be lives' savers. Just like any other new technology, researchers as well as industries have collaborated to ensure the feasibility of VANet. In this paper we focus in the security aspect –in particular- securing VANET against unwanted intentional threats, mainly jamming attacks.

Jamming attack is one of the hardest attacks that any type of wireless communication can face. Jamming problem in VANet is even harder than it is in any other type of network. Due to the nature of the network (Rapid Changes in topology and high mobility), jamming became a concern since no solution was yet to be found. Many researchers have conducted experiments, research the problem and proposed solutions. Though many aspects of VANet been researched, yet security remains a big concern.

In this paper, we propose a new system that utilizes beacons packets to alert nodes/drivers in the network of the presence of jamming attacks when driving into an affected zone. The system works as a real-time jamming detection system to identify jammers and alert drivers of the threat.

The paper is organized as follow; section 2 provides background information and related work. VANet communication overview is provided in section 3. In Section 4 we discuss jamming types, models, capabilities and their impact on the network. Our proposed solution will be given in section 5. Implementation and Evaluation will be discussed in section 6. Analysis and results discussion are given in section 7. Finally, the paper is concluded in section 8. Future work will be given at the end of the paper

II. BACKGROUND & RELATED WORK

The Research and Innovative Technology Administration (RITA) has acknowledged the need to utilize technology for safety purposes. Hence it dedicated and allocated 75 MHz in the 5.9 GHz frequency band licensed for Dedicated Short-Range Communication (DSRC) [1]. The DSRC spectrum is divided into seven 10 MHZ channels and support different data rate 6, 9, 12, 18, 21and 27Mbps. Some of these channels can be combined together to form a one 20 MHZ channel with 54 Mbps data rate if needed. Also, the central channel (178) is called control channel (CCH) which is used solely to broadcast safety related messages. All other channels are referred to as service channels (172 – 184 except 178 reserved for the CCH) see Figure 1.

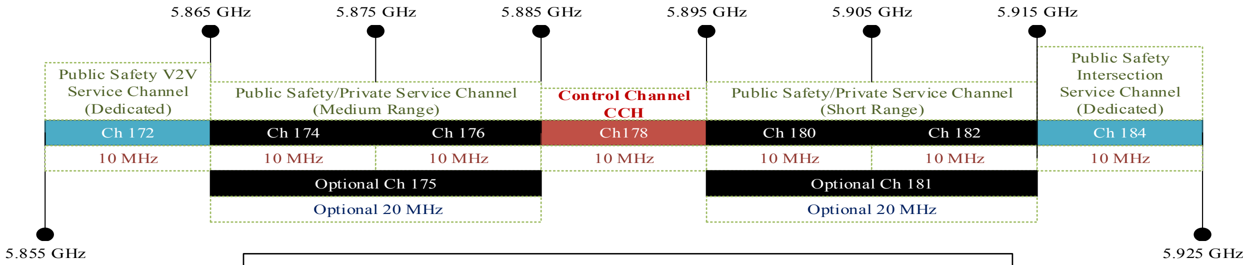


Figure 1: United States DSRC Band Plan channel allocation

The department (RITA) commitment highlights two critical points as their goal. One is that safety is the highest priority for the department and will form the central focus for the connected vehicle technologies. The other goal is that DSRC is the only available technology in the near-term that offers the latency, accuracy, and reliability needed for active safety [2]. Companies and Industries have acknowledged the importance and the capabilities of VANet. Thus started investing in improving all the aspects to increase its feasibility. In spite of the ongoing research efforts (academically and industrially), many security issues yet need to be addressed and resolved. Since VANet provides promising potential to enhance the safety of driving, hence it is essential to secure it against exploitation. At the same time, the Quality of Service (QoS) is very important to take in consideration when securing VANet against different security breaches.

Some issues that VANet may encounters are impersonation, jamming, in transit tampering and location tracking, etc. Despite the different types of attacks that may be carried out, they can only affect one or more of three main requirements that VANet should satisfy. Availability, privacy and non-repudiation are the three security requirement that researchers attempt to improve and protect [7]. The availability stands out to be the most crucial component since once it is compromised, other requirements will fail.

Due to the difficulty to trace and the rapid changes in the network topology, jamming attacks stands to be one of the most important attacks that VANet affected by. Jammers goal is to disrupt and damage the communications between nodes. These communications can be accident warning, road hazard, or emergency vehicle approaching messages. Failure to receive these messages by vehicles result in failing to slow down, re-route or stop the vehicles which may lead to a great loss.

Hamieh et al. [9] Proposed a new model based on the measure of the correlation among the error and the correct reception times in order to detect jamming attack when present. Another research paper [11] studied the beaconing frequency in VANET and proposed a new scheme called Distributed Beacon Frequency Control (DBFC) algorithm to reduce the beacon load and improve the channel condition by adjusting the transmit parameters according to the network condition.

Our work is based on utilizing beacons packets to real-time detect jammers or Denial of Service (DoS) attacks, hence we look into understand the contents and requirements of beacon packets. We focus the light in next section on explaining the different type of communications that VANet uses to grasp the network behaviors.

III. COMMUNICATION OVERVIEW

When dealing with Vehicular Network communications, we need to make distinction between different terms that we see, Hence we present in this section the most widely spread acronyms that any reader will come across when dealing with VANet research. WAVE, DSRC and 802.11p are the three different keywords that we need to distinguish between when dealing with VANET communications.

A. WAVE

(Wireless Access in Vehicular Environment) is one of IEEE1609 family of standards for Wireless Access in Vehicular Environment. The family of the IEEE1609 standards describe the architecture, communications model, protocols, security mechanisms, network services, multichannel operation, use of Provider Service Identifiers, and how they work with the physical layer and media access layer for high speed (up to 27 Mb/s) short range (up to 1000m) low latency wireless communications in the vehicular environment. The main architectural components defined by these standards are the On Board Unit (OBU), Road Side Unit (RSU) and WAVE interface. These standards also describe the functionality of applications that utilize WAVE in the WAVE environment [3].

B. DSRC

(Dedicated Short Range Communications) is a two-way short-to-medium-range wireless communications capability that allows very high critical data transmission in communications-based active safety applications. In Report and Order FCC-03-324, the Federal Communications Commission (FCC) allocated 75 MHz of spectrum in the 5.9 GHz band for use by Intelligent Transportations Systems (ITS) vehicle safety and mobility applications. DSRC based communications is a major research priority of the Joint Program Office (ITS JPO) at the U.S. Department of Transportation (U.S. DOT) Research and Innovative Technology Administration (RITA). The cross-modal program is conducting research using DSRC and other wireless communications technologies to ensure safe, interoperable connectivity to help prevent vehicular crashes of all types and to enhance mobility and environmental benefits across all transportation system modes.

The U.S. DOT's commitment to DSRC for active safety communications contributes to safer driving. Vehicle safety applications that use vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications need secure, wireless interface dependability in extreme weather conditions, and short time delays; all of which are facilitated by DSRC [4].

C. IEEE802.11p

Is an approved amendment to the IEEE 802.11 standard (an evolving family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE)). The amendment was approved to insert wireless access in vehicular environments (WAVE), a vehicular communication system. It defines enhancements to 802.11 required to support ITS applications. This includes data exchange between high-speed vehicles and between the vehicles and the roadside units in the licensed ITS band of 5.9 GHz (5.85-5.925 GHz). IEEE 1609 is a higher layer standard based on the IEEE 802.11p.

IV. Jamming models, threats & challenges

Jamming is a type of attack that intentionally attempts to interfere, disrupt, or block wireless communications. There are different jammers devices with different capabilities based on what they target. In this work, we focus exclusively on Jamming attacks targeting 802.11 communications – particularly transmitted and received packets. In order to evaluate jamming affect accurately we need to understand how they work.

Next we introduce different aspects that we considered when modeling jammers in a vehicular network.

Radio propagation model: We build our jamming model based on free-space and shadowing model which were used to model the received signal power. The difference between the two models is that shadowing model captures both path loss versus distance and attenuation due to object blockage (building, trees, hills, etc) while free-space can only be considered where buildings and natural obstacles are very limited. In this work, we research both models to ensure the feasibility of our work when considering either one.

Several variables in jamming characteristics impact the communication differently. In order to evaluate jammers affect accurately, we propose two classifications of jammers based on their mobility and behaviors.

A. ***Mobility classification***

Jammers can be divided into 3 different categories based on their mobility. Classifying jammers based on their mobility is crucial due to different types of nodes in VANET- stationary nodes (RSUs) and mobile nodes (vehicles). In order to solve the detection problem, we need to study the mobility of jammers. Hence, all jammers can be categorized under one of three following types –with respect to their mobility

1) Stationary

A Jammer who is not moving when launching the attack is considered stationary. A jammer can be standing on feet, sitting in a car (while the car is parked), or just sitting in a building. The effect of this type of jamming can only be in the same jammer's area at that time rather than jamming different areas. A stationary jammer has full control over their jamming location and distance between nodes N.

2) Targeting mobility

This is the same as the stationary jammer except that jammer is mobile (moving) while launching jamming attack. Jammer of this type might be in a car driving or walking in feet while the jammer device is on. The unique property of this type of jamming is that jammer is targeting a specific node (vehicle). The motive can be due to grudge, anger, envy, or just for sheer joy. Targeting-mobile jammers drive and stay in close range to one car to ensure the jamming affect.

3) Random mobility

Jammers in this category type is similar to the previous one (targeting mobility). The only difference is that jammer doesn't target a specific vehicle. Jammers of this type would be driving in their cars or motorcycles that keep them mobile. This type is very challenging to detect due to the high mobility and low constrains.

B. ***Behaviors classification***

Besides categorizing jammers based on their mobility, jammers can adopt different behaviors. Here we present the different behavior that jammers may adopt when launching attacks.

1) Constant

A constant jammer sends out random radio signals all the time at the wireless medium. This type of jammers does not follow any underlying MAC protocol. The objective of this type of behavior is to prevent legitimate user from accessing communication channels or corrupt the sent out data by creating interference.

2) Random

Jamming requires high power to emit signals to the wireless medium hence; jammers lifetimes are restricted due to energy failure problem. Thus, random jamming helps adversaries to launch jamming attacks for longer period. The attacker can alternate between going to sleep mode for t_S seconds then wake up and jam for t_J seconds. This allows jammers to have more control over energy consumption by altering t_S & t_J as needed. This type of jammers can follow any jamming mobility model when launching the attack.

3) Reactive

Most of jamming models target packets at the sender and prevent them from being transmitted. Reactive jammers behave a little differently by targeting packets that being transmitted to prevent the delivery at receiver nodes. Reactive jammers constantly listen to channel, and when jammer sense packets to be sent, he/she starts transmitting radio signals to cause collision and corrupt data that packet transfers.

In this section, we introduced 2 different classifications of jammers based on their mobility and behaviors. We also learned about the threat they carry upon launching jamming attacks. We presented a realistic jamming model that was used in our experiments to evaluate the affect. In the following section we propose jamming detection solution in VANet and explain the feasibility in the middle of challenges. More details about jamming models can be found at [10].

V. Proposed detection-system

In order to detect jamming attacks reliably in VANet, nodes need to have the ability to estimate the channel condition and adjust their transmitting frequency (beacons) accordingly. We adopt DBFC Algorithm proposed in [11] to update the transmitting beacon Frequency (*bF*) in the nodes. Our contribution is that we build a detection system based on utilizing the bF to detect jamming attacks quickly and reliably by nodes (OBUs & RSUs). We also propose a unique placement strategy to deploy RSUs on the roads to improve the delivery of warning messages around the network and enable RSUs to detect jamming attacks.

A. RSU placement & deployment

IEEE 802.11p Standards allows up to 27 Mbps data-exchange rate and 1000 meter in radius apart between nodes. We propose a new placement technique to be used when deploying RSUs on roads -compatible with the standards- to make the best use of nodes and their communication.

When placing RSUs in urban or highway areas we propose placing RSU every 900 meter along the road to ensure the availability of communication. Doing so, allows every RSU to communicate constantly and consistently with two neighbors- at least- along the road all the time. We will use *R* to refer to any RSU and RN_i to refer to immediate neighbors of *R* on both sides. Figure 2

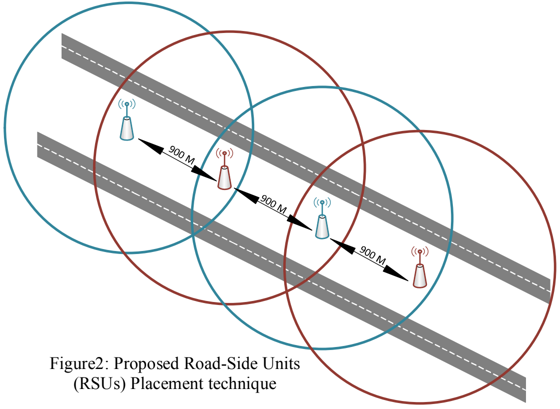


Figure2: Proposed Road-Side Units (RSUs) Placement technique

Implementing the proposed placement technique will allow each *R* to maintain a table for its both RN_i IDs and track changes in RN_i tables. Such a scenario can be easily implemented by periodically broadcasting beacons (beacons probing). We use the above suggested technique in placing as many R_x as desired at the deployment phase to propose a jamming detection system. More details regarding system detection design is giving in the following section.

B. Beacon packet format

Since, there is no standards or restrictions regarding the contents of the beacons packets, many researchers suggested different models to describe the contents and sizes of the beacons packets. In this paper we propose a simple model - with crucial yet small dataset- to form our beacons packets. We adopt the beacon format that was suggested by Humeng in their work [11]. Based on the proposed format, each beacon has to include essential data such as (Source Address, beacon Frequency, Sequence Number, etc) figure 3.

Source Address	Beacons Freq.	Sequence Num.	Time Stamp	Position, Speed, Direction, Acceleration

Figure3: Vehicle OBU's Beacon Packet Content

We implemented the previous beacon format to be generated and transmitted by all OBUs (O_i) . We also implemented a simpler format to be generated by R_i to reduce network congestion and increase successful transmission. We omit unnecessary data in beacons generated by OBUs (Speed, Direction, and Acceleration) and construct beacons packets for RSUs. Adopting 2 unique formats of beacon packets to be used by RSUs and OBUs will make it easier to identify –by receiver- whether the beacons were generated by RSU or OBU.

C. Detection system

Our detection system consists of two different schemes in which one will be implemented and adopted by OBUs and the other is solely for RSUs. For simplification, will refer to the two detection systems as OBU-DS and RSU-DS for distinction purposes.

1) RSU-DS design overview

Based on the proposed RSU placement technique, each RSU node will have two neighbors – highway- or more – urban- to communicate with constantly. Our system design depends on utilizing the RSUs placement and the periodic probing technique in exchanging messages to detect jammers. Figure 5

Aside from the previous jammers classification in section 4, there are two possibilities of jammers affect when launching an attack. Jammer can block all type of communications and entirely isolate nodes from the network. This can be achieved by jamming all the network frequencies. Jammers can also create noise to increase the packet drop rate and disrupts communication depending on the SNR. We will explain each case individually and how our detection system behaves in these cases.

- Full Jamming: Depending on jammer transmission power, frequency and distance from the node, jammers can block all communications coming in to a node causing Denial of Service (DoS). When jammers intention is to drop all packets and take a node out of the network, they transmit useless data on the network frequency at close distance to overload the node and block communications. When a node (RSU) stops receiving beacons packets from its both neighbors (one on each side), it triggers jamming flag which tells the node itself that it is jammed. Likewise, neighboring nodes which expects to receive beacons packets back from the jammed node will trigger a warning message with the compromised node's address. For all nodes (jammed and neighbors) they start broadcasting warning messages with the compromised RSU address and location. This will allow RSUs outside the jammed area to pickup and forward the warning message to all RSUs and incoming traffic. Hence drivers will be aware of the attack in the affected areas. Figure 4.
- Partly Jamming: Jammers whose intention is to increase the drop in the PDR and disrupt the communication will transmit radio signal that disrupt communication by decreasing the signal-to-noise ratio (SNR). When the number of received beacons drops below 20 beacons packets per second which corresponds to the requirement of safety-related applications [6], compromised nodes will trigger jamming flag. Neighboring nodes which receives lower beacons rate from the compromised node, will consider that node is under jamming attack. Hence, they will issue and broadcast warning messages with the infected node address and location and advise incoming vehicles of the threat. Figure 4

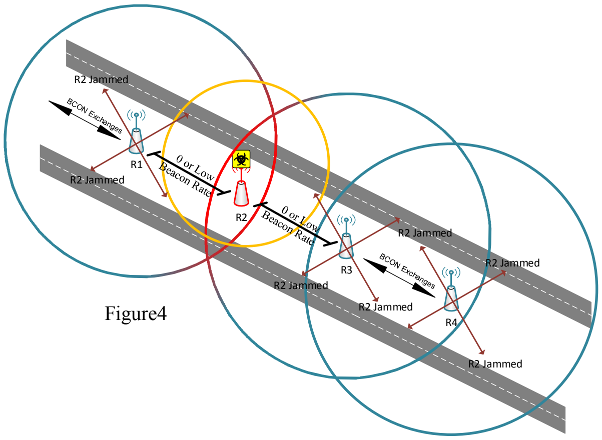


Figure4

The following flowchart1 explains how RSUs react when receiving beacons from any node in the network. More details regarding implementation are given in section 6.

Algorithm 1: RSU-DS Roadside Unit-Detection System

```
Data: b_ID:beacon source ID,
$N_{Local\_ID}$:RSU Node Local ID (address),
$N_{NR}$,$N_{NL}$: Neighbor RSU Nodes (righ,left),
$N_{NR}$_counter, $N_{NL}$_counter: counting received beacons
from each neighbor.
Input: b_ID, $N_{Local\_ID}$, $N_{NR}$, $N_{NL}$
Output: $N_{Local\_ID}$, $N_{NR}$, $N_{NL}$, Null
initialization;
while beacon packets received do
    if $b\_ID == N_{NR}$ then
        $N_{NR}$_counter++;
    else
        if $b\_ID == N_{NL}$ then
            $N_{NL}$_counter++
        end
    end
    if $N_{NR}\_counter$ && $N_{NL}\_counter < X$ then
        Return $N_{Local\_ID}$;
    else
        if $N_{NL}\_counter < X$ then
            Return $N_{NL\_ID}$
        else
            if $N_{NR}\_counter < X$ then
                Return $N_{NR\_ID}$
            end
        end
    end
    Return
end
```

Algorithm1: RSU-Detection Algorithm used by RSUs to detect jamming attacks

2) OBU-DS design overview

Vehicles (OBUs) update their beacon Frequency (*bF_t*) based on the proposed DBFC algorithm [11]. This will allow OBUs to adjust their beacon frequency prior transmission based on the channel's congestion condition. Each OBU will then calculate the beacon Received Rate over time t (*bRR_t*) using the formula 1 given in the flowchart2. Each OBU will compare its local *bRR* to the actual number of received beacons packets in time t. OBUs will determine whether jammer exists or not based on the comparison result. This will allow OBUs (Vehicles) to alert their driver of the reliability level of the network at any given time. Below is a flowchart describing the detection system model implemented in all OBUs.

Algorithm 2: OBU-DS On Board Unit-Detection System

```
Data: b_counter: received beacon counter from all nodes,
bF: beacons frequency (DBFC algorithm),
J: boolean jamming flag (true, false),
Tx: number of transmitted beacons,
bRR: beacon received ratio,
$N_{ID}$: node ID.
Input: bF, Tx
Output: $N_{ID}$, Null
initialization;
while beacon received do
    repeat
        listen to channel and update bF;
        b_counter++;
        bRR=(Tx/bF*b_counter);
        if $b\_counter < bRR$ then
            J==true
            return $N_{ID}$
        else
            J==false
        end
        return
    until $J==true$;
end
```

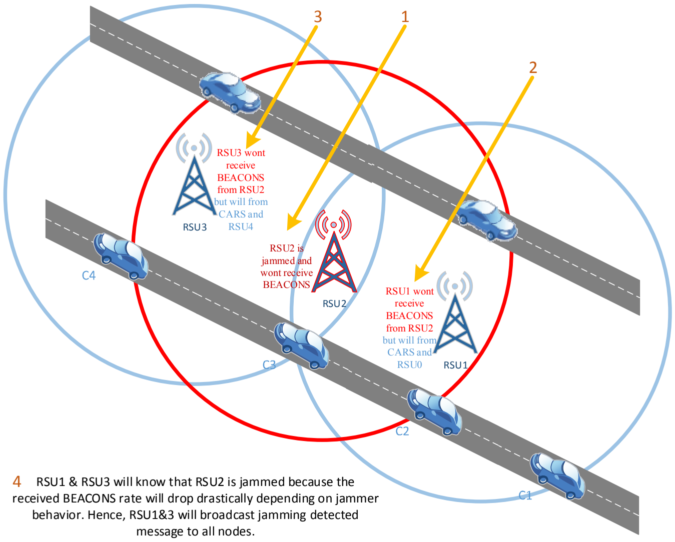
Algorithm2: OBU-Detection algorithm used by OBUs to detect jamming attacks

Our detection method allows each node to detect if it is under jamming attack. Each node acts as an individual detection system and it is the node's responsibility to detect when it is under attack. Hence, we avoid the communication overhead to detect jamming attacks by allowing nodes to participate and be part of the detection system. Each node that is under attack will broadcast jamming warning message (including position) to alert surrounding nodes of a potential jamming attack. Depending on the location and the frequency the jammer is using, close-by nodes (RSU and OBU) will be able to pick up the warning messages and re-broadcast them. Nodes (RSUs and OBUs located at the edge of the range of affected area) will continue to forward the warning messages further to warn incoming traffic before driving into the jammed area (through RSUs, OBUs or both). Our method works against all types of jammers regardless their mobility and behavior.

The hardest type of jamming to detect is mobile-targeting jammers adopting reactive behavior. That's because of the high mobility of the jammer and at the same time targeting one node (which makes it hard for the node to be heard when broadcasting warning message). Although the OBU will be able to detect the jammer, it will be hard to ensure the successful transmission of the warning message because of the jammer behavior. We prove that our detection system still works and detect even this particular jammer exist. When putting the two detection systems together in a network (OBU

& RSU –DS) RSU will be able to detect the jammer and broadcast the warning message to warn incoming traffic about the incident and the existence of the jammer. Hence, our method still works even at the worst case scenario.

In the next section we evaluate our detection method in a simulator environment (NCTUns). Results and discussion will be given also in the same section.


3
1
2
RSU3 wont receive BEACONS from RSU2 but will from CARS and RSU4
RSU3
RSU2 is jammed and wont receive BEACONS
RSU2
RSU1 wont receive BEACONS from RSU2 but will from CARS and RSU0
RSU1
C4
C3
C2
C1

4 RSU1 & RSU3 will know that RSU2 is jammed because the received BEACONS rate will drop drastically depending on jammer behavior. Hence, RSU1&3 will broadcast jamming detected message to all nodes.

Figure5: RSU Detection System using Periodic Probing Technique when RSU2 is under jamming attack

VI. IMPLIMINTATION & EVALUATION

We proposed 2 different detection systems, one in which will be implemented and used by RSUs and another by OBUs. The key difference between the two systems is how they detect jammers. OBU-DS main responsibility is to detect jammers and warn drivers of an existing attack. RSU-DS is also responsible –in addition to detection- to spread warning messages around to ensure nodes awareness of attacks. While both systems OBU and RSU –DS broadcast warning messages to notify drivers, OBU-DS only broadcast the messages and it is other nodes responsibility to receive it. On the other hand, RSU-DS will ensure the delivery of those messages through forwarding them to neighboring RSUs.

In our work we use the network simulator NCTUns 6.0 to implement the proposed systems and evaluate results. The simulator is a powerful tool that covers most network aspects. NCTUns also allows constructing new modules and customizing node's configurations and behaviors

- Simulation setup: We simulate a highway scenario with four lanes in which two lanes is going one direction and two going the opposite way. Each two lanes are 30 meters apart from the other 2 lanes (going opposite direction). This will allow us to apply our proposed RSU placement technique in the middle of the four lanes. Figure 2
- Nodes configuration: We have two different types of nodes to configure OBUs and RSUs. Each OBU is configured individually to get realistic results based on their (speed, direction, acceleration, position and distance from other node) Table1.
  - ➢ *On-Board Units:* We deploy 30 vehicles to act as OBUs according to 802.11p standards where 13 vehicles are driving in one direction in both lanes and the other 17 driving the opposite direction. Each vehicle was configured to not exceed 36 m/s (80.5mph) and accelerate/decelerate freely. Also, vehicles were placed to have an average distance of 500 meters between them when driving on the same lane.
  - ➢ *Road-Side Units:* 9 RSUs were deployed on the same Y-axis and 900meter apart on X-axis according to our proposed RSU placement technique figure 2. Each RSU was configured to use message-probing-technique to handle the exchange of beacons packets among neighboring RSUs. We added a (time-to-live) variable to each warning message to ensure its freshness when forwarding. The value of (time-to-live) was set to be MAX (60 minutes) which can be easily adjusted. All RSUs were configured to start their communication 1 second after the simulation starts to ensure proper communication.
- Communication setup: According to recent study many safety-related applications require a minimum of 20 beacons packets [6]. We adjusted the beacon format in the simulator as mentioned earlier to include all crucial information (speed, location, etc). We also adjusted how the simulator handles broadcasting and forwarding warning messages over the control channel (CCH) to correspond to our proposed technique.
- Simulation setup & Evaluation metrics: We simulate highway vehicle network scenarios where vehicles travel at high speed to clone a real world scenario. On-Board-Units were configured to behave in accordance to 802.11p standards and use DSRC standards for communications. We placed vehicles randomly on roads and their speed varies between 55-80 Mph. On the other hand, RSUs were placed on the highway where each RSU has 2 neighbors RSUs within communication range. This will allow RSUs to exchange beacon packets continuously using message-probing-technique. Each RSU was placed 900m away from its neighbor to comply with IEEE802.11p standards which states that the maximum range of beacons communication is up to 1000m [2]. Table2 depicts the 3 main cases we studied which each case ran multiple times with different arguments.

Table1: Simulation parameters

Parameter	Value
Simulation Time	400 Simulation Sec
Number of Lanes	4 lanes, 2 each direction
RSU	9
OBU	30
Transmission Power	28.8dbm
Receiver Sensitivity	-82.0dbm
ITS	IEEE 802.11p agent controlled
Traffic Type	UDP
Radio Propagation Model	Free Space and shadowing
MAC Protocol	IEEE 802.11p
Simulation Seed	Random- not fixed

Case Name	Type of Node	Dynamic Arguments	Jammer mobility	Jammer Behavior	Evaluation Metrics
Normal Case	RSUs & OBUs	Speed, Traffic, Unintentional Noise, Obstacles	N/A	N/A	beacons Packets (Transmitted, Delivered, Dropped, Collided)
With Jammer	RSUs, OBUs, Jammer	Speed, Distance, Jammer Tx power, Noise Level	Stationary, Mobile	Constant, Reactive, Random	beacons Packets (Transmitted, Delivered, Dropped, Collided)
With Detection System	RSUs, OBUs, Jammer	Speed, Distance, Jammer Tx power, Traffic, Noise Level	Stationary, Mobile	Constant, Reactive, Random	True Positive True Negative False Positive False Negative

Table2: Experiment cases where each case was run with different configurations multiple times

- Results: After running experiments we collected data from the Packet Trace File (PTR). Chart 1 shows the relation between the number of nodes and the number of delivered beacons. We see that in a normal case network, nodes receive at least 30 Beacons per seconds which comply with safety-related applications requirements. When the number of nodes increases in the network, the numbers of received beacons follow. We noticed that simulating a network with high number of nodes (100 nodes) in a small area leads to a slight increase in the drop rate due to communication congestions and packets colliding.

  We then simulated the same previous cases with additional node which was configured to behave as a jammer. When simulating jammer we took in consideration the different mobility and behaviors that jammers may adopt. We noticed a significant drop in the data packets including beacons packets. We also noticed that when simulating a stationary jammer, the results were almost similar when jammer is adopting a reactive or constant jamming behavior. That's because jamming affect will only shows while the attack is being launched (active). Likewise, mobile jamming will have the same affect when adopting constant or reactive jamming. The only difference is that jamming affect will take a place only in the affected area. Chart 1 shows different jamming impact (stationary & mobile) on the number of received beacons packets.

From the chart we can see how jammers affect the network by disrupting communication when launching their attack. We also noticed that when we simulate a mobile jammer going on the same direction and speed targeting one node, all packets get dropped whether it constant or reactive jammer.

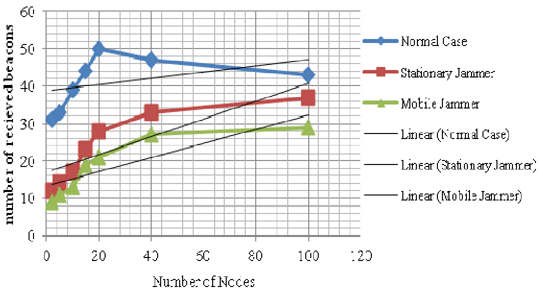


Chart1: different jamming impact on the received beacons

In our simulation we use the following metrics to evaluate the feasibility and effectiveness of the proposed detection systems:

(TN): Jammer detected but no jammer exists.
(TP): Jammer detected while they exist.
(FN): No jammer detected when no jammer exists.
(FP): No jammer detected but jammer actually exists

It is clear low FP and FN rates, together with high TP and TN rates, will result in good efficiency values.

VII. Analysis & Discussion

After collecting and analyzing data from all simulated cases, we found that in a normal case scenario the beacon exchange rate between nodes when they are in range exceeded 30 beacons packets per second. This is fully compatible with 802.11p and safety-related applications requirements. When jammers exist, the communications get disrupted and the number of beacons drops to below the suggested value for safety-related applications. Depending on jammers behavior and their mobility, the received beacon packets ranges between 0-17 beacons per second. When the number of received beacons drops to 0, all communications fail and all packets get dropped. After applying the detection systems in both RSUs and OBUs we found that we can detect jammers easily and efficiently. Table 3 shows the detection system accuracy –in percentage- when dealing with different jamming types and behaviors.

Few cases reported where detection system fails to either detect a jammer (False Positive) or issue false detection (False Negative). Most of these failures got reported either when the jamming node is starting to launch the attack or right before going into hibernation mode (reactive jammer). Also, noise level plays a major role causing the system to fail. Although, 802.11p is immune to unintentional noise because of high frequency used in communications, we still conducted experiments to check the feasibility of the proposed detection system when noise exists. We believe that failure of detection system can be as a result of logic error in the simulation. Theoretically, in a real world, when jammers first launch the attack the number of received beacon packets drop gradually until attacker reaches their full-affect. Vice versa, when jammers go into sleeping mode or stop the attack, the number of exchanged beacon packets increases gradually. In both case, the detection system will not detect a jammer until the rate of received beacons drops below the calculated value by the system.

Nodes	Jam Type	Received BCON/s	True Positive Detection	True Negative Detection	Notes
RSUs only	None	20b/s	N/A	N/A	Normal Case
RSUs only	Stationary Constant	0b/s	%100	%100	
RSUs only	Stationary Reactive	4b/s depending on jam interval	%98.7	%97.3	Jammer interval = 6s
RSUs only	Mobile Constant	0b/s at affected node	%99.2	%98	Jammer speed = 65mph
RSUs only	Mobile Reactive	9b/s at affected nodes	%97.4	%95.1	Jammer interval = 20s
RSUs, OBUs	None	Up to 40 b/s	N/A	N/A	Normal Case
RSUs, OBUs	1Stationary Constant	0b/s	%100	%100	At jammer location
RSUs, OBUs	1Stationary Reactive	19b/s depending on jam interval	%97.4	%96.7	Jammer interval = 6s
RSUs, OBUs	1 Mobile Constant	0b/s at affected node	%98.6	%96	Jammer speed = 65mph
RSUs, OBUs	1 Mobile Reactive	9b/s at affected nodes	%96.9	%93.3	Jammer interval = 20s

VIII. CONCLUSION

Vehicular network is a hot topic that has drawn much interest industrially and academically. Security aspect is still under research to provide a safe secured environment. Intentional jamming is one of the security aspects that is still open for research. The affect of jammers may lead to fatalities on roads depending on the jammers motive. All in all, intentional jamming is still an open problem that needs intensive work to protect and secure the communication in VANet.

In this work we have introduced a new strategy to be used when placing road-side-units on roads. We also proposed two new beacons formats to be generated by RSUs and OBUs during communication. We then built two detection systems in which one is used strictly by OBUs and the other by RSUs. The two detection systems –when applied together- gave promising results to accurately detect jammers with very low failure detection rate. Several cases reported when the detection systems failed to give correct results. These cases were mostly when jammers first launch the attack or right before going into sleeping mode. Despite these cases, OBU-DS and RSU-DS have proven their feasibility and showed promising results to warn drivers when jammers exist especially when combined together.

Future work

We plan in investigating more into solving the jamming problem. Our future work will be focusing in utilizing the proposed detection system to build a new protocol that enables nodes to communicate in the presence of jammers. Many people have proposed solutions to the jamming problem. We believe that none of these solutions is sufficient yet. We will investigate some of the proposed solutions and prove their faults or impact in the quality of service. Then we will perform an intensive research using our detection system as first step toward solving jamming problem in Vehicle communication.

References

[1] Y Qian, K Lu, and N Moayeri, "A Secure VANET MAC Protocol for DSRC Applications", IEEE Globecom, 2008

[2] U.S. Department of Transportation, IntelligentTransportation Systems (ITS) Home, http://www.its.dot.gov/index.htm

[3] U.S. Department of Transportation, IntelligentTransportation Systems (ITS), IEEE1609 Family of Standards for Wireless Access in Vehicular Environment (WAVE), http://www.standards.its.dot.gov/Factsheets/Factsheet/80

[4] U.S. Department of Transportation, IntelligentTransportation Systems (ITS), DSRC: The Future of Safer Driving, http://www.its.dot.gov/factsheets/dsrc_factsheet.htm

[5] National Highway Traffic Safety Administration, Laws & Regulations, Vehicles, http://www.nhtsa.gov

[6] M. Torrent-Moreno, "Inter-Vehicle Communications: Achieving Safety in a Distributed Wireless Environment: Challenges, Systems, and Protocols", PhD dissertation, Universitätsverlag, Karlsruhe, 2007.

[7] R Raw, M Kumar, and N Singh, "Security Challenges, Issues and Their Solutions for VANET", Vol.5, pp95-105, IJNSA 2013.

[8] Engine Control Unit, Working of ECU, http://en.wikipedia.org/wiki/Engine_control_unit.

[9] A. Hamieh, J. Othman, and L. Mokdad, "Detection of Radio Interference Attacks in VANET", IEEE, 2009.

[10]]W. Xu, W. Trappe, Y. Zhang, T. Wood, "The feasibility of Launching and Detecting Jamming Attacks in Wireless Networks", MobiHoc, 2005

[11] L.Humeng, Y. Xuemei, A. Li, W. Yuan, "Distributed Beacon Frequency Control Algorithm for VANETs (DBFC)", ISDEA, 2012.

[12] S. Malebary, W. Xu, "A Survey on Jamming in VANET", Vol.2, No.1, pp142-156, IJSRIT 2015.