IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 6 Issue 5, May 2019
ISSN (Online) 2348 – 7968
www.ijiset.com

Jamming Attack Model and Detection of Transmissions Using Cognitive Radio Network in Vehicular Network

S. Divyashree[1], Dr. D. Geetha[2]
[1]M.E. Scholar Adhiyamaan College of Engineering Hosur-635109
[2]Assistant Professor Adhiyamaan College of Engineering Hosur-635109

Abstract
The safety applications in vehicular ad hoc network (VANET) which is vulnerable to denial of service (DoS) attacks, such as jamming attack. It raises a jammer to interfere with legitimate wireless communications, and to degrade the overall Quality of Service (QoS) of the network. Cognitive Radio (CR) is a form of wireless communication in which transceiver can intelligently detect which communication channels are in use and which are not, and instantly move into vacant channels while avoiding occupied ones. The proposed model has two distinct information exchange system layouts. One is dynamic (vehicle to vehicle) and another is semi-dynamic (vehicle to Road-Side- Unit). For the vehicle-2- vehicle communication, the proposed model assumes that vehicles can communicate with each other using available wireless resources. This detection model is used with the help of cognitive radio mechanism, in which the problem that occurs when communication through high road density is higher due to high load on road, message communication get overhead due to less amount of network bandwidth to overcome this issue Cognitive Radio bandwidth is utilized for data transmission by channel sensing and messages are transmitted through Cognitive Radio channels. This detection method will distinguish the causes of failed transmissions, such as collisions, interferences, and jamming attacks accurately. Finally, we evaluate our detection method with both analytical analysis and network simulations.
Key Terms—*VANET, jamming, MAC, QoS ,,vehicular networks.*

I. INTRODUCTION

The individual has seen an awesome improvement of system correspondences which give a huge number of administrations supporting everyday life. Vehicular ad-hoc network (VANET) has especially been brought to attention by its role in Intelligent Transportation System (ITS). The communication in VANET uses direct mode for connecting vehicle to vehicle (V2V) and/or vehicle to infrastructure (V2I) and, reversely, I2V. These modes of communication allow ITS to support safe and convenient transport system such as warnings about traffic and road conditions (e.g., emergency braking, congestion, accidents, ice on road, destruction sites) and infotainment (e.g., entertainment services on board, local information). Individually, two kinds of applications are briefed as safety applications and non-safety applications.
Adjacent to normal qualities of remote systems, vehicular systems have some of a kind ones that make challenges in designing and implementing networks. For examples, time constraints of urgent safety-related information need to be exchanged in driving; scale of the network may reach hundreds of vehicles; high mobility of vehicles creates dynamic network topology and limits connection duration. These challenges are not only for designing protocol but also for securing the communication.
The nature of wireless communication makes it exposed to attackers, thus it is prone to be eavesdropped, deliberated by man-in-middle hackers, and disturbed or overwhelmed resources by DoS attacks. Moreover, the earth is astute for selfish members to endeavor to possess a greater number of assets than others. As a type of wireless communication networks, vehicular networks are vulnerable to all of these attacks.
Almost safety applications work based on real time information included in periodically exchanged packets of nearby vehicles, called beacons. Therefore, beacons play vital role in maintaining the operation of safety applications and the whole ITS systems as well. They are prone to be victims of attacks at lower layers (physical and medium access control attacks) due to their limited packet length and short lifespan. Limited packet length does not allow complex cryptography, and it requires more time for complex computation if the attack comes from higher level (e.g., manipulating content). Jamming attack is a common type of attacks at lower layers.
Keeping in mind the end goal to recognize sticking in remote systems, diverse discovery techniques have been proposed. They can be classified into two kinds of detection methods: threshold-based detection method and MAC-based detection method. Most of the related works detect jamming based on observing network performance metrics such as packet delivery ratio (PDR). Methods that detect jamming by comparing these metrics in normal scenario and jammed scenario are defined as threshold based detection methods. Besides, there are MAC-based detection methods that detect jamming based on observing medium access process of vehicles.
In threshold-based methods, a threshold value is chosen for a metric as a boundary to differentiate between normal scenario and jammed scenario (i.e., presence of jamming attack). Therefore, estimating this threshold accurately is a necessary task that enhances performance of the method in term of probability of detection. To this aim, we propose an analytical model to evaluate the network performance considering the medium access contention.
Contrasted with limit based recognition strategies, based detection methods are more suitable for vehicular networks. The multichannel operation, which is specifically proposed for vehicular network in order to support both safety applications and non-safety applications, allows us to observe a complete medium access process of fix number of beacons within predefined duration. Vehicles frequently change from one control channel (CCH) for safety services to one of several service channels (SCHs) for other services every interval of 50 ms. Each vehicle broadcasts a beacon each CCH interval (CCHI). Any misbehavior during the medium access process of beacons results in unreasonable events that are observed during each CCHI.

Therefore, the jamming attack can be detected at the end of each CCHI.

In this paper, we focus on beacon jamming attack, one kind of DoS attacks, which targets blocking any beacon exchange within its transmission range by broadcasting radio signal in the channel. We propose a MAC-based jamming detection method for the standard IEEE 802.11p where the attack is detected real time at the end of each CCHI. In our method, the decision of the detector (monitor) depends on the number of nearby vehicles, the number of successful transmissions and failed transmissions.

Our commitments in this paper are two folds. Firstly, we propose an analytical model which helps to estimate PDR threshold more accurately in threshold-based detection methods. We study the feasibility of the existing threshold-based methods to detect jamming in real-time applications. From our analysis, these methods are not suitable for safety applications. Hence, secondly, we propose a real time and MAC-based detection method specified for these applications. Our realtime detection method reduces the probability of false alarms and time for the monitor to measure the average network performance that encountered in threshold-based method. It differentiates three phenomena contention collision, interference and jamming attacks in communication. This is the first time that the problem of differentiating the three phenomena is concerned in literature when we target a feasible jamming detection solution.

In this paper, we accomplish our detection method by integrating a Collision and Interference differentiation scheme into the previous CJD method. Our detection method includes solution for Contention Collision, Jamming and Interference Differentiation (CJID). Furthermore, our method is studied in platoon scenario and general scenario with vehicle mobility. It can be implemented for both central monitor and distributed vehicles.

II. RELATED WORKS

Among remote correspondence assaults, jamming is a huge threat for vehicular networks due to its simple requirement of devices, real time attack and hard to detect especially at lower layers (PHY and MAC) [20]. Jamming can be either constant jamming which continuously emits radio signals not following any rule of communication protocol, or reactive jamming on which jammer transmits radio signal upon sensing a transmission in radio medium. Reactive jamming is more dangerous and harder to detect as it conforms to legitimate transmission.

The jamming attack causes degradation on packet delivery ratio (PDR) measured at a receiver. Based on how much the degradation is, the jamming can be detected. PDR is the ratio of error-free received packets and total received packets. PDRs encountered in normal scenario and jammed scenario are studied experimentally and/or analytically in jamming attack models. In wireless networks, several jamming attack models accompanying detection methods have been proposed.

In remote sensor organizes, some sticking recognition systems at PHY and MAC layers are additionally proposed. Li et al proposed jamming attack detection based on percentage of incurred collisions. Slotted Aloha protocol is chosen as the random access protocol in their work.

Three parameters: packet delivery rate, bad packet ratio and energy consumption amount are sampled and recorded in initial system to create threshold levels. When system is operating, the monitor can identify abnormalities by comparing current parameter levels with these threshold levels. Radio Frequency (RF) jamming attacks on VANETs were studied experimentally in indoor and outdoor .Obtained outputs of these models or experimental results are reference values to differentiate a jamming attack and normal network condition. The detection methods that compare observed PDR to a certain reference value are referred as threshold-based detection methods. Obviously, in order to achieve high detection efficiency, the reference values used for jamming detection should be accurate. However, almost existing works investigate only the case of one transmitter without consideration of medium access contention. In vehicular environment, we cannot neglect medium access contention among vehicles because broadcast is the main communication mode supporting safety applications. Therefore, in the first part of our work, we propose an analytical model to estimate the threshold in consideration of the contention.

Diverse sticking assault models in remote systems and distinctive estimations serving sticking assault recognition are considered in crafted by Xu et al. According to their analysis, the measurements of signal strength and carrier sensing time, under certain circumstances, are not powerful statistic to detect jamming as the difference between normal scenario and jammed scenario is indistinct. While PDR is a powerful metric for detecting jamming attacks.

Anyways, it is unable to discriminate between jamming attack and other natural causes of PDR degradation. Therefore, they propose jamming detection with consistency checks that combine measurement of PDR and signal strength and/or PDR and location. An experimental study of RF jamming attacks on VANETs was conducted. PDR in normal scenario and PDR under impacts of different types of jamming attacks are obtained from experiments. Sufyan et al. propose analytical models of jammers. Numerical results from their models are used for detecting and classifying different types of jammers. However, all mentioned above related works and their models focus on communication between two nodes and no medium access contentions. Their proposals are suitable for general wireless networks but not feasible for broadcasting in vehicular networks.

All existing studies of threshold-based jamming detection in vehicular networks have only focused on analyzing impact of jamming attacks in scenario of communication between two vehicles while beacons, the basic messages maintaining operation of ITS services, are not considered in their works. Due to the importance of beacons and its vulnerability to jamming attacks, we investigate the impact of jamming attacks on beacons. Respectively, all beacon-related issues including broadcast, medium access contention and physical parameters are taken into account in our study. We evaluate the impact of reactive jammer on PDR metric, with contention during medium access process following the standard IEEE 802.11p, multi-channel operation specified in the standard IEEE 1609.4 and physical parameters. The reference value (threshold) of average PDR in normal scenario is obtained from our analysis. However, PDR must be measured during a specified window of time. The time window should be long enough for measuring a tolerant average PDR. Moreover, our analysis shows an overlap in standard deviation of PDR statistics in normal scenario and jammed scenario. Therefore, even the threshold to claim an attack is determined accurately, false alarms cannot be avoided. Threshold-based detection methods are likely unsuitable for real-time applications in vehicular networks.

Aside from above edge based recognition techniques, there are other detection methods in vehicular networks that address medium access contention in their works . Hamied et al. propose a constant jamming detection method which is based on error distribution. They show that there is an correlation between error reception time and the correct reception time when there is constant jamming attack in the network. This correlation is counted by a metric called correlation coefficient. The attack is figured out if the correlation coefficient passes a threshold. However, again, the issue of threshold identification is not investigated. Author proposed a jamming detection method that

can detect a missing of one beacon from a vehicle in a platoon. Based on received beacons, the monitor (detector) divides vehicles into groups whose beacons only collide to beacons sent from members of the same group. Whenever there is a missing of exactly one beacon in at least one group, an alarm will be raised. This method can detect only if there is exactly one beacon in a group is jammed. In fact, due to the nature of radio communication, the jammer interferes not only a vehicle but also several nearby vehicles. The method cannot distinguish between collisions of beacons in a group and a multiple jamming attack (transmissions of more than one vehicle in a group is jammed). An overhearing mechanism based on cross-layer approach is proposed to detect the malicious activity of nodes. Comparing observed number of forwarded packets from neighbors and predicted number
calculated from physical and MAC parameters, the monitor node can detect misbehavior nodes. However, the mechanism is not suitable for beacons. Beacons need only singlehop communication while the mechanism operates essentially based on routing protocol.
Effect of impedances on remote correspondence, and in addition relief to obstructions have been truly examined. Authors in consider the mitigation of cochannel interference in Bluetooth piconets. Cross technology interference is analyzed in the work. Three heuristic approaches are proposed in order to efficiently solve this interference in large-scale network scenarios. However, in the scope of this paper, we firstly discuss the detection of jamming that can be considered as an intentional interference.
As interference sometimes causes failed transmissions, then communication is interrupted. Therefore, it has impact on the number of missing beacons that the monitor overhears every CCHI. Taking into account interference, we enhance our method with a Collision - Interference Differentiation (CID) scheme. A failed transmission can be a result of interference, contention collision or jamming attack. Together, our detection method CJD and CID scheme solve the problem of determining the reason of a failed transmission. Hence, jamming attacks can be detected accurately with low probability of false alarm. Moreover, it does not require any modification to the existing infrastructure and the method can be implemented for both central and distributed detection. Multi-channel operation is a typical suggestion for vehicular networks. However, in our understanding, there are not many studies of jamming attacks addressing multi-channel operation in vehicular networks. Due to the unawareness of switching channel of higher level, nodes or vehicles likely contend for medium at the beginning of every control channel interval. This impact on communication using the standard IEEE 802.11p is considered in performance evaluation of MAC protocol. The performance evaluation of our detection method is carried out analytically under an assumption that vehicles start contending at the same time.
However, we do not use this assumption in our simulations.

III.PROPOSED SYSTEM

In This Prosposed System, we overcome a particular class of DoS attacks. The nature of wireless communication makes it exposed to attackers, thus it is prone to be eavesdropped, deliberated by man-in-middle hackers, and disturbed or overwhelmed resources by DoS attacks.

MEMORYLESS JAMMERS:

A memoryless jammer produces jamming signals specifically the idle time between successive signals is drawn from an exponential distribution specified by the jamming pulse rate R, which is describes as the number of jamming pulses that the jammer generates per second. The probability that a jamming signal is produced during a time interval t0 is (1 ¡ e¡Rt0); this is, indeed, the jamming probability qi for all i. Since qi is independent of i, the failure probability Pi is also independent of i; let p denote this common failure probability. We obtain that

p = Pc + (1 ¡ Pc)(1 ¡ e¡R(DATA+ACK));

where DATA and ACK refer to the duration of a data and ACK packet, respectively. The DATA term includes both payload length L as well as any headers.
Reactive Jammers:
We specify a reactive jammer by its jamming probability q, which is the probability that the jammer jams an ongoing packet transmission that has not undergone a collision.
Since the jamming probability is independent of the backoff stage, the failure probability is also constant for all backoff stages. Let this probability be p. We obtain:

p = Pc + (1 ¡ Pc)q

The steady state transmission probability ¿ is given by the same equation (3). Solving (4), (3), and Pc = 1¡(1¡¿)n¡1 yields ¿ . The probability of success of a given transmission, Ps, is given by Ps = n¿(1¡¿)n¡1(1¡q), while Ttr and Tid are DIFS + SIFS + DATA + ACK and ¾, respectively.
The above equations in conjunction with Equations of Section III-A give us the throughput of the system. The rate of a reactive jammer with jamming probability q is given by

$$R = \frac{qn\tau(1-\tau)^{n-1}w}{E[\text{length of a timeslot}]},$$

where w is the length of a jamming pulse.

Omniscient Jammers:

An Omniscient jammer that is knowledgable of the present state of each 802.11 node and accepts a jamming strategy that minimizes system throughput subject to constraints on the jamming rate.While a completely omniscient jammer may not be realizable in practice, effective approximations can be implemented. An accurate analysis of omniscient jammers would provide a useful lower bound on the system throughput of 802.11 against all jammers and a measure for MAC resiliency. Here, we provide a partial analysis of an omniscient jammer, proving interesting properties of an optimal omniscient jammer and characterize certain special cases.
We first make several observations about an optimal omniscient jammer: (a) An optimal omniscient jammer only jams separate out the transmission probability of N as ¿0, letting ¿ be the common transmission probability of other nodes.

METHODOLOGY:

Algorithm Used:

Collisions-Interferences Differentiation Algorithm:
Fast and accurate collision detection between general geometric models is a fundamental problem in modeling, robotics, manufacturing and computer-simulated environments. Most of the earlier algorithm are either restricted to a class of geometric models, say convex polytopes, or are not fast enough for practical applications. We present an e_cient and accurate algorithm for collision detection between general polygonal models in dynamic environments. The algorithm makes use of hierarchical representations along with frame to frame coherence to rapidly detect collisions. It is ro- bust and has been implemented as part of public domain packages. In practice, it can accurately detect all the contacts between large complex geometries composed of hundreds of thousands of polygons at interactive rates. The asymptotic gain in the time complexity when using collision detection depends heavily on the task by investigating three prominent problems for wireless networks, i.e. the maximal independent set (MIS), broadcasting and coloring problem.

IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 6 Issue 5, May 2019
ISSN (Online) 2348 – 7968
www.ijiset.com

DETECTION-SYSTEM:

In order to discover jamming attacks reliably in VANet, nodes need to have the capacity to estimate the channel condition and adjust their transmitting frequency (beacons) accordingly. We accept DBFC Algorithm proposed 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 an uncommon 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.

RSU PLACEMENT & DEPLOYMENT

IEEE 802.11p Standards grants up to 27 Mbps data-exchange rate along with 1000 meter in radius apart between nodes. We introduce 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 neighborsat least- along the road all the time. We will use R to refer to any RSU and RNi to refer to immediate neighbors of R on both sides.

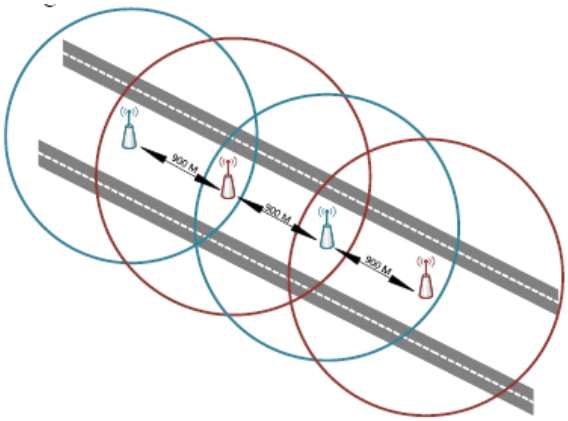

Figure 1:Proposed Road-Side Units (RSUs) Placement technique

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

BEACON PACKET FORMAT:

There is no standards or restrictions respecting the contents of the beacons packets, many researchers proposed 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. Based on the proposed format, each beacon has to include essential data such as (Source Address, beacon Frequency, Sequence Number

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

Vehicle OBU's Beacon Packet Content

We started the previous beacon format to be produced and transmitted by all OBUs (Oi) . We have implemented a simpler format to be generated by Ri to reduce network congestion and increase successful transmission. We exclude unnecessary data in beacons produced 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.

COGNITIVE RADIO WITH VANET

VANET is a special class of MANET, with nodes in VANET generally representing highly mobile vehicles. Cognitive radio network on the other hand is a method which addresses the spectrum scarcity in the network. While mobile nodes move in a random manner in VANET, spectrums are being utilized in a high density environment. A general idea of how to incorporate cognitive radio network with VANET is discussed in this section. A large amount of spectral congestion due to high vehicle density might affect the performance of the network. cognitive radio system is proposed to spatially and temporarily add additional radio channels to VANET when there is a high vehicle density. This framework allows high priority safety messages and secondary VANET applications to be transmitted successfully without much delay and with increased performance. A distributed channel coordination scheme that exploits the data transmission rate and the range of various frequencies is proposed for vehicle-to-vehicle communication

IV.RESULT ANALYSIS

After running experiments we go from the Packet Trace File (PTR). Chart relation between the number of nodes and the delivered beacons. We see that in a normal ca nodes receive at least 30 Beacons per sec comply with safety-related applications re When the number of nodes increases in the ne numbers of received beacons follow. We no simulating a network with high number of nodes) in a small area leads to a slight inc drop rate due to communication congestions colliding.

The simulation is done using NS2 simulator for detection of maliciousness level for group of nodes. The values of PDR and Max_PDR are simulated. Fig. 3shows the malicious level for the group of nodes. Fig. shows the true detection ratio for various types of configurations. Fig. shows the false detection ratio for various types of configuration.

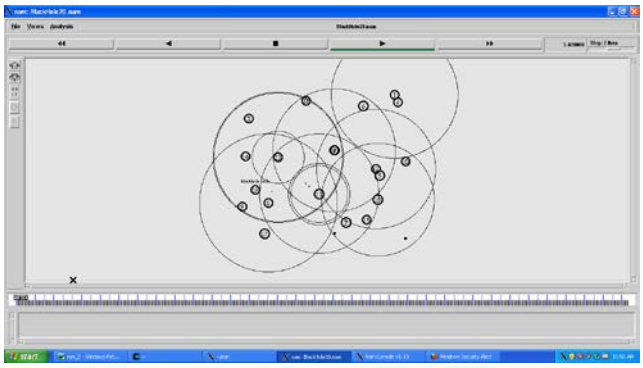

Figure 4.7 Jamming Detection

CONCLUSION:

Earlier, We discussed different types of jamming and many jamming detection techniques. The proposed system works as, authenticate that the node is legitimate node or jammer node and then monitor the behavior of members to detect the maliciousness level of cluster members. The packet delivery ratio selected as metric for determining the maliciousness level of nodes. A threshold value 75% is set to determine the maliciousness level of the jammer. The simulation results shows us to achieve the high jammer detection rate and low false detection rate.

REFERENCES

[1] Ieee standard for information technology– local and metropolitan area networks– specific requirements– part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 6: Wireless access in vehicular environments. IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009), pages 1–51, July 2010.

[2] Ieee standard for wireless access in vehicular environments (wave)– multi-channel operation. IEEE Std 1609.4-2010 (Revision of IEEE Std 1609.4-2006), pages 1–89, Feb 2011.

[3] A. Benslimane, A. El yakoubi, and M. Bouhorma. Analysis of jamming effects on ieee 802.11 wireless networks. In 2011 IEEE International Conference on Communications (ICC), pages 1–5, June 2011.

[4] Murat C¸akirolu and Ahmet Turan ¨ Ozcerit. Jamming detection mechanisms for wireless sensor networks. In Proceedings of the 3rd international conference on Scalable information systems, page 4. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering),2008.

5] Claudia Campolo, Antonella Molinaro, Alexey Vinel, and Yan Zhang. Modeling prioritized broadcasting in multichannel vehicular networks. Vehicular Technology, IEEE Transactions on, 61(2):687–701, 2012.

[6] Jocelyne Elias, Stefano Paris, and Marwan Krunz. Cross-technology interference mitigation in body area networks: An optimization approach. IEEE Transactions on Vehicular Technology, 64(9):4144–4157, 2015.

[7] Richard Gilles Engoulou, Martine Bella¨ ıche, Samuel Pierre, and Alejandro Quintero. Vanet security surveys. Computer Communications, 44:1–13, 2014.

[8] Ali Hamieh, Jalel Ben-Othman, and Lynda Mokdad. Detection of radio interference attacks in vanet. In Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE, pages 1–5. IEEE, 2009.

[9] Hannes Hartenstein and Kenneth Laberteaux. VANET vehicular applications and inter-networking technologies, volume 1. John Wiley & Sons, 2009.

[10] A. Hussain, N.A. Saqib, U. Qamar, M. Zia, and H. Mahmood. Protocolaware radio frequency jamming in wi-fi and commercial wireless networks. Communications and Networks, Journal of, 16(4):397–406, Aug 2014.

[11] Daniel Jiang, Qi Chen, and Luca Delgrossi. Optimal data rate selection for vehicle safety communications. In Proceedings of the Fifth ACM International Workshop on VehiculAr Inter-NETworking, VANET '08, pages 30–38, New York, NY, USA, 2008. ACM.

[12] Daniel Krajzewicz, Jakob Erdmann, Michael Behrisch, and Laura Bieker. Recent development and applications of SUMO - Simulation of Urban MObility. International Journal On Advances in Systems and Measurements, 5(3&4):128–138, December 2012.

[13] Seung-Hwan Lee, Hyung-Sin Kim, and Yong-Hwan Lee. Mitigation of co-channel interference in bluetooth piconets. IEEE Transactions on Wireless Communications, 11(4):1249–1254, 2012.

[14] Mingyan Li, Iordanis Koutsopoulos, and Radha Poovendran. Optimal jamming attack strategies and network defense policies in wireless sensor networks. IEEE Transactions on Mobile Computing, 9(8):1119– 1133, 2010.

[15] Jiajia Liu, Yuichi Kawamoto, Hiroki Nishiyama, Nei Kato, and Naoto Kadowaki. Device-to-device communications achieve efficient load balancing in lte-advanced networks. IEEE Wireless Communications, 21(2):57–65, 2014.

[16] Jiajia Liu, Hiroki Nishiyama, Nei Kato, and Jun Guo. On the outage probability of device-to-device-communication-enabled multichannel cellular networks: An rss-threshold-based perspective. IEEE Journal on Selected Areas in Communications, 34(1):163–175, 2016.

[17] Nikita Lyamin, Alexey V Vinel, Magnus Jonsson, and Jonathan Loo. Real-time detection of denial-of-service attacks in ieee 802.11 p vehicular networks. IEEE Communications letters, 18(1):110–113, 2014.

[18] Huong Nguyen Minh and Abderrahim Benslimane. Polling scheme for reliable broadcasting in vehicular networks. In Communications (ICC), 2014 IEEE International Conference on, pages 330–335. IEEE, 2014. [19] H. Nguyen-Minh, A. Benslimane, and A. Rachedi. Jamming detection on 802.11p under multi-channel operation in vehicular networks. In Wireless and Mobile Computing, Networking and Communications (WiMob), 2015 IEEE 11th International Conference on, pages 764–770, Oct 2015.

[20] Konstantinos Pelechrinis, Marios Iliofotou, and Srikanth V Krishnamurthy. Denial of service attacks in wireless networks: The case of jammers. Communications Surveys & Tutorials, IEEE, 13(2):245–257, 2011.

[21] Oscar Punal, Carlos Pereira, Ana Aguiar, and James Gross. Experimental characterization and modeling of rf jamming attacks on vanets. Vehicular Technology, IEEE Transactions on, 64(2):524–540, 2015.

[22] Abderrezak Rachedi and Abderrahim Benslimane. Toward a crosslayer monitoring process for mobile ad hoc networks. Security and communication networks, 2(4):351–368, 2009.

[23] Henrik Schulze and Christian Lders. Basics of Digital Communications, pages 1–49. John Wiley Sons, Ltd, 2006.

[24] M. Segata, S. Joerer, B. Bloessl, C. Sommer, F. Dressler, and R. L. Cigno. Plexe: A platooning extension for veins. In Vehicular Networking Conference (VNC), 2014 IEEE, pages 53–60, Dec 2014.