Detection of Radio Interference Attacks in VANET

Ali Hamieh[±], Jalel Ben-Othman[±], Lynda Mokdad [∓]
[±]PRiSM – University of Versailles, France
[∓] LACL – University of Paris 12, France
[±]{ali.hamieh, jbo}@prism.uvsq.fr, [∓]mokdad@lamsade.dauphine.fr

***Abstract*—Due to their nature, Vehicular Ad hoc NETwork (VANET) is vulnerable to Denial of Service (DoS) attacks, such as jamming attack. The objective of a jammer is to interfere with legitimate wireless communications, and to degrade the overall QoS of the network. In this paper, we propose a model to detect a particular class of Jamming attack, in which the jammer transmits only when valid radio activity is signaled from its radio hardware. This detection model is based upon the measurement of error distribution.**

***Index Terms*—Vehicular Ad-Hoc Networks, Jamming Attack, Linear Regression.**

I. Introduction

In last few years, many projects have developed various systems for interconnecting the vehicles, for widening the driver's horizon to detect the incidents that cannot be observed by the driver or with common on board tools. The introduction of advanced on board sensors has made possible to detect critical driving conditions and these can also be passed on to other vehicles in the zone. To exchange such information the vehicles form an unstructured network, known as a Vehicular Ad hoc NETwork (VANET). The utilization of VANETs can improve road safety and the travel comfort by inter-vehicle communication [10].

VANET shares some common features with Mobile Ad Hoc Network (MANET). Both VANET and MANET are characterized by the movement and self-organization of the nodes. Nodes in MANET cannot always recharge their power and have irregular movement. While some nodes in VANET can recharge often, and their nodes are constrained by the road and traffic pattern. VANET is also characterized by high mobility and possibly large network.

The IEEE 1609 and IEEE 802.11p [18] task groups has developed an IEEE 802.11 WLAN based inter-vehicles communication system, named as Wireless Access in Vehicular Environments(WAVE). The frequency band used by this system is 5.9 GHz, regulated by FCC in the U.S. and by ETSI in Europe. The IEEE 802.11p standard specifies the Physical layer (PHY) and the basic MAC layer. All upper layers in WAVE system is regulated by the IEEE 1609 standard [20]. The IEEE 802.11p PHY is based on the Orthogonal Frequency-Division Multiplexing (OFDM) technology offering up to 27Mb/s data rate. The distance in WAVE system is from 300m to 1000m. The IEEE 802.11p MAC layer is the IEEE 802.11 DCF (Distributed Coordination Function), which is based on the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) scheme. The 802.11p use parts from the original standard together with the MAC amendment 802.11e for QoS support and the physical (PHY) layer supplement of 802.11a.

Security and privacy issues are critical in VANET as the networks are publicly available on the road at any time. Because most VANET messages are related to driving conditions and road safety, real-time processing of these messages is important. To guarantee the given real-time constraints the security systems of the infrastructure must be highly efficient in terms of computational and bandwidth needs. As, there is no feasible defense against jamming attacks measures must be taken to reduce denial-of-service attack efficacy. A security system in VANET should meet the following requirements [15]:

- Authentication: Enables a vehicle to ensure the legitimacy of the peer vehicle with which it exchange the information's about traffic.
- Availability: Ensures the survivability of communication channel despite Denial-of-Service (DoS) attacks. In fact, since this network uses the wireless medium for communication, it is susceptible to malicious exploitation at different layers. One of these attacks is a kind of denial of service attack (DoS) that interferes with the radio transmission channel, this is also known as a jamming attack.
- Non-repudiation: Ensures that the origin of a message cannot deny having sent the message such as accident messages.
- Privacy: The privacy of driver identity such as Big Brother identity and the location of the vehicle should be guarantee. Hence, privacy is a very crucial requirement in VANET.

In this paper, we focus on availability requirement for vehicular ad hoc network. We propose a model to detect the presence of Jamming attack in this network.
The shared nature of the wireless medium in VANET allows attackers to easily observe communications between wireless devices and launch simple DoS attacks against wireless networks by jamming or interfering com-

This work is supported by ANR (French Research National Agency) under CLADIS grant N. 05-SSIA-0018.

978-1-4244-4148-8/09/$25.00 ©2009

munication. Such attacks in the physical layer cannot be addressed through conventional security mechanisms. An attacker can simply disregard the medium access protocol and continually transmit in a wireless channel. By doing so, the attacker either prevents users from being able to commit legitimate MAC operations.

Because some jamming attack uses physical and mac layers, a brief description of these layers is given in next section.

The rest of the paper is organized as follows: Section II describes the physical and the mac layers of VANET. In Section III, overviews of the related work in the domain of Jamming are exposed. In Section IV, we introduce the correlation used in our proposed technique with the details of our method to detect a Jamming attack. The simulation models and numerical results are given in section V. Finally, we summarize the main contribution of our work and its perspectives in section VI.

II. PHY AND MAC LAYERS OF VANET

The VANET physical layer is based on the Orthogonal Frequency-Division Multiplexing (OFDM) technology [19]. OFDM is nowadays widely used for achieving high data rates as well as combating multipath fading in wireless communications. In this multi-carrier modulation scheme data is transmitted by dividing a single wideband stream into several smaller or narrowband parallel bit streams. Each narrowband stream is modulated onto an individual carrier. The narrowband channels are orthogonal vis--vis each other, and are transmitted simultaneously. In doing so, the symbol duration is increased proportionately, which reduces the effects of inter-symbol interference (ISI) induced by multipath Rayleigh-faded environments. The spectra of the subcarriers overlap each other, making OFDM more spectral efficient as opposed to conventional multicarrier communication schemes. In fact, at the physical layer a jammer needs to identify the presence of packets to launch jamming attack.

However, The VANET MAC layer is exactly the Distributed Coordination Function (DCF) in IEEE 802.11. DCF defines a distributed access algorithm based on the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) [19]. The goal of CSMA/CA protocol is to minimize the collisions and to guarantee a fair access to the channel. If a node have a packet to transmit, it senses the medium during an idle period which corresponds to a DIFS (Distributed Inter Frame Space). If the medium is busy, a random backoff interval is selected. The backoff time counter is decremented as long as the channel is idle, then stopped when a transmission is detected on the channel, and then reactivated when the channel is sensed idle again for more than a DIFS. The node transmits when the backoff time reaches 0. In addition, to avoid channel capture, a node must wait a random backoff time between two consecutive transmissions, even if the medium is sensed idle in the DIFS time. The backoff time is uniformly chosen in the interval $[0, CW - 1]$, where CW is the $Contention\ Window$ size. At the first transmission attempt CW is equal to CW_{min}, and it is doubled at each retransmission up to CW_{max}. If a node data transmission is successful, the node resets its CW to CW_{min}. The receiver acknowledges a successful reception by transmitting an ACK (ACKnowledge) frame. In fact, the jamming attack can be made at the mac layer. For example, an attacker simply sends wireless signal to jam ACK messages in the network. Data packets will simply be dropped once the sender reaches the retransmission limit. Hence, the attacks effectively degrade the QoS of the network by simply jamming a short control packet.

In the next section, we provide the previous work on the domain of jamming attacks.

III. RELATED WORK

In past the security issues were neglected in inter-vehicle communication research projects. At present the VSC project[1] has made considerable contribution. There are working groups within the EU's 6 Framework Programme's Research Project Willwarn [2], the German national research project NoW -Network on Wheels [3], the IEEE 1609.2 working group [17], and the SeVeCom project [19]. The general analysis and contributions to VANET security has been discussed by[4], [5], and [6]. Golle et al. proposed a scheme to detect malicious data in IVC [9]. Dotzer discussed privacy issues for vehicle communications in [10]. The paper [7] presents a security approach to VANET. Leinmueller et al. [8] discuses the impact of falsified position information on geographic routing. Many papers have been written about trust establishment and decentralized key management, such as [11], [12], [13] and [14].

We describe here the related work on the domain of jamming in the networks other than VANET. As the jamming attack in VANET has not been taken into consideration previously.

Xu et al. [23] propose two methods to react at jamming attacks: channel surfing and spatial retreats. The first technique has been inspired in some way from the frequency hopping technique. Unlike frequency hopping that takes place at the PHY layer, channel surfing takes place at the MAC layer. When a node detects that it is jammed it can switch its channel and send a beacon message on the new channel frequency band. It's non-jammed neighbors will detect the absence of this node and change its channel to get the beacons broadcasted in new channel. If no beacon is detected then they assume that the node just moved away. In the other side, if they sense a beacon they will inform the rest of the network at the initial channel to switch the channel. There are two possible approaches. At the first approach the whole network will eventually change channel while in the second approach only the boundary nodes of the jam region will change their channel and they will be used as relays for the rest of the network and the jammed area. In spatial retreats method, when a node detects that it is being jammed, it

978-1-4244-4148-8/09/$25.00 ©2009

firstly escapes from the jammed area and then tries to stay connected within the rest of the network in order to avoid the partition of the network reconstruction phase. More specifically, when a node senses that it is being jammed, it starts moving out of the jammed region and simultaneously runs the detection algorithm. When it detects that it has moved away the jamming area, it tries to stay connected with its previous neighbors. In order to stay connected it keeps moving at the boundary of the jammed area. If the node does not recognize that it is out of the jammed area and it continuous to move away, it could be out of the network partition that makes it impossible to stay connected.

Wood et al. [25] described various denial-of-service attacks against WSN nodes. In [24], the authors presented DEEJAM, a protocol for detecting and reaction after a jamming attack using IEEE 802.15.4-based hardware. It uses frame masking, channel hopping, packet fragmentation, and redundant encoding to eliminate most of the impact of jamming by a mote-class attacker. All of the components of DEEJAM must be used simultaneously to resist all types of jamming described in [4], resulting in energy consumption overheads exceeding 150%. Such overheads are extreme and can reduce network lifetime to a fraction of what it would be without them. In the case that a jamming attack is ongoing, this overhead is justified, but in the more likely case that there is no jamming attack, it might be prohibitively expensive.

Xu et al. [6] studied the feasibility of launching and detecting jamming attacks in wireless networks. Their paper shows that by using signal strength, carrier sensing time, or the packet delivery ratio individually, one is not able to definitively conclude the presence of a jammer. Therefore, to improve detection, the authors introduced the concept of consistency checking, where the packet delivery ratio is used to classify a radio link as having poor utility, and then a consistency check is performed to classify whether poor link quality is due to jamming. Two enhanced detection algorithms are presented: one considering signal strength as a consistency check, and the other taking into account location information as a consistency check. Though there are some issues those are critical for their performance, such like the frequency of the location advertisements, which need to be taken into a deeper consideration.

JAM [28] is a service for sensor networks, which detects jammed areas in the sensor networks and helps to bypass the jammed area, enabling routing within the sensor network to continue. This technique is only reliable in the presence of constant jamming and will not detect random or reactive jamming.

In [22], the use of low density parity check (LDPC) codes is proposed to cope with jamming. Further, an anti-jamming technique is proposed for 802.11b that involves the use of Reed-Solomon codes.

To the best of our knowledge our approach has not been proposed in the literature to detect jamming attack in VANET which is based on linear regression. Our method is described in the next section.

IV. Detection by Correlation

We assume that the jammer transmits only when valid radio activity is signaled from its radio hardware and the attacker jams the packet with p_{jam} probability. Using this strategy the attacker decreases its probability of detection. Thus, to differentiate this jamming scenario from legitimate scenarios, we have measured the dependence among the periods of error and correct reception times. In fact, the access to the channel of jammer is dependent of the access to the channel of active nodes. Thus, this dependence measure in jamming attack case is greater than in normal network activity. In order to measure this dependency, we have used the Correlation Coefficient which is a statistic measure of relation between two random variables. This correlation is exposed below.

A. Correlation

The correlation is a measure of the relationship among two random variables. The Correlation Coefficient (CC) between two random variables, X and Y, is defined as:

$$CC = \frac{cov(X,Y)}{\sigma_x \cdot \sigma_y} \tag{1}$$

The value of the correlation coefficient is between -1 and 1. The sign of CC indicates the direction of the *linear* pattern. Values of CC nearer to -1 or 1 indicate a "strong" correlation, when it is near 0 it indicates the absence of a useful relationship. It is possible that X and Y are related by a *linear* relation: $y = a \cdot x + b$. The *linear* regression is to determine an estimation of values a and b to quantify the value of this relation due to the correlation coefficient [27]. The value of a is estimated to be $\frac{cov(X,Y)}{var(X)}$.

The main advantages of the proposed model are its simplicity and efficiency for detecting jamming attack. Also, as our model is passive, there is no communication overhead. In addition, the required storage and computation overhead is very small. Therefore, the solution is easy to implement in existing devices.

The following subsections explain the proposed approach in detail.

B. Detection System

In this sub-section, we describe our model to detect the jamming attack in vehicular ad hoc networks. A transmission node measure the Error Probability (EP) and the Correlation Coefficient (CC). The CC is among the reception error time and the correct reception time. Thus, if the CC is larger than produced relative EP then the network is considered like jammed. The relation between CC and EP may measured by simulation, or by measurement of the regression in non-jammed network.

In fact, the system is composed of two phases:

a) Initialization Phase- It consists of calculating at the beginning the value of the threshold w, defined as the

978-1-4244-4148-8/09/$25.00 ©2009

maximum value of the slope that any pair of (CC, EP) should have. In fact, after a determined period of simulations, the value of w will be estimated from simulation. However, this w value can be also estimated theoretically in the following method: taking, $\varepsilon_i = cc_i - a \cdot ep_i - b$, as the difference between the line (estimated by the linear regression) and the point (cc_i, ep_i). Thus, the estimator of the residual variance $\hat{\sigma}^2_{\varepsilon_i}$ is

$$\hat{\sigma}^2_{\varepsilon_i} = \frac{1}{n-2} \cdot \Sigma^n_{i=1} \varepsilon^2_i \,.$$

Therefore, the variance of the slope a of the line, could be calculated using

$$\hat{\sigma}^2_a = \frac{\sigma^2_{\varepsilon_i}}{n \cdot var(EP)} \,,$$

where n is the number of simulations. In this case, we are in the Student-Test where the variance of a random variable is known and an unknown standard deviation. In the Student-test, for a given level of confidence α, the error over a can be estimated by:

$$\triangle a = \hat{\sigma}_a \cdot t^{n-2}_{(1-\alpha)/2} \,.$$

In our approach, we have taken, $t^{n-2}_{(1-\alpha)/2} = 3$, which corresponds to a 99.7% confidence level. Therefore, the proposed threshold is

$$w = \langle a \rangle + \triangle a \,,$$

where $\triangle a = 3 \cdot \frac{\hat{\sigma}_\varepsilon}{\sqrt{n \cdot var(EP)}}$.
We should notice that the threshold w is calculated in the non-jammed case.

b) Detection Phase- The transmission vehicle calculates the EP and

$$CC = \frac{cov(X,Y)}{\sigma_X \cdot \sigma_Y} \,.$$

$X(x_i; i = 1, \ldots, t)$ is the reception error time and $Y(y_i; i = 1, \ldots, t)$ is the correct reception time for the node, where t is the number of simulated points. Thus, if the CC is bigger than $w \cdot EP$, it means that the network is jammed.

V. Simulation

We use NS-2 [29] in order to evaluate our detection model in vehicular ad hoc network. In order to generate the simulation scenario and the vehicular mobility patterns, the SUMO [21] tool has been employed. The simulation was restricted to a 1km x 1km for vehicle placement and travel. The average speed of vehicles is 12.6 mps (45 kmph). Parameters in Table I are used in the simulations.

The shadowing channel model captures the variations in channel conditions over time and space by using a Gaussian random variable, X_{dB}, with zero mean and σ_{dB} standard deviation. The model is represented as:

$$[\tfrac{P_r(d)}{P_r(d_0)}]_{dB} = -10\beta log(\tfrac{d}{d_0}) + X_{dB}$$

SIMULATIONS PARAMETERS	
Transmission Rate (Mb/sec)	2
MAC Layer Protocol	802.11p
Average Speed of Vehicles (mps)	12.6
Routing Protocol	AODV
Simulations Area (m)	1000 x 1000
Transmission Range (m)	250
Radio Propagation Model	Shadowing
Traffic Model	CBR
Simulation Time (s)	30
Packets size (bytes)	1000

TABLE I
PARAMETERS OF THE SIMULATED VEHICULAR AD HOC NETWORK.

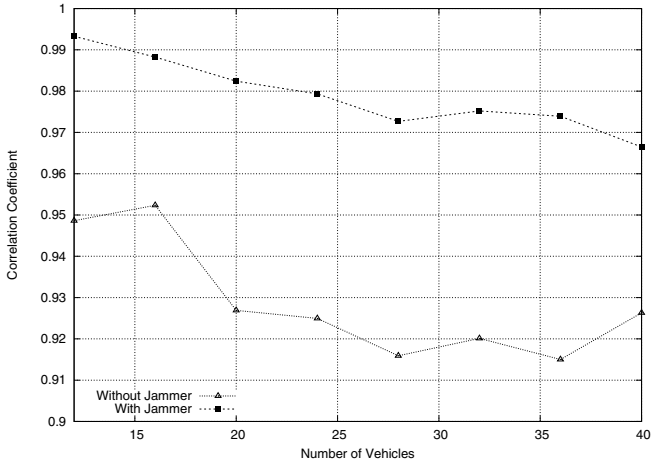

Fig. 1. Measure the Correlation Coefficient as a function of the number of vehicles.

β is called the Path Loss Exponent, d is the distance between the sender and receiver, $P_r(d)$ is the received power and $P_r(d_0)$ is the power at some reference distance d_0. For free space propagation β is 2 and we use this value in our simulations. The value of σ_{dB} is set to 4. The Ad-hoc On- Demand Distance Vector (AODV) was used as the routing protocol.
The nodes sending CBR (Constant Bit Rate) traffic. The frame length was set to 1000 bytes in the default case. Results are averaged over 30 simulations, 30s each. 802.11p was chosen as the MAC layer protocol. The data rate for each connection in the simulation is 2Mbps.

A. Model Simulation

In Fig. 1 (respectively Fig. 2), we present the simulation results obtained for the average Correlation Coefficient (CC) for all nodes as a function of the number of vehicles (respectively packet size). The CC is among the error and the correct reception times. The Error Probability of the jammed network is equal to the Error Probability of the normal network. Fig. {1,2} indicate that the CC in jamming case is bigger than the CC in normal case. These results are compatible with our idea for detecting jamming attack.
Thus, we can conclude from these results that our ap-

978-1-4244-4148-8/09/$25.00 ©2009

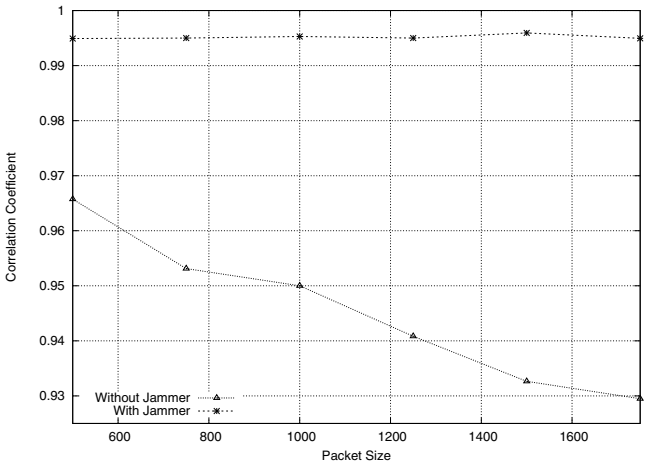

Fig. 2. Measure the Correlation Coefficient as a function of packet size.

proach can detect the jamming attack with a very high probability.

VI. Conclusions

Vehicular ad hoc networks (VANETs) are networks in which wireless mobile nodes establish temporarily network connectivity and perform routing functions under self-organization. Due to their nature, VANET is vulnerable to DoS attacks, such as jamming attack. The objective of a jammer is to interfere with legitimate wireless communications, and to degrade the overall QoS of the network.

In this study, we have proposed a new model based on the measure of correlation among the error and the correct reception times in order to detect the presence of jamming attack in vehicular ad hoc networks. The simulation results of the model are quite promising. In fact, we have been able to detect the presence of jamming with very high degree of confidence.

Our objective in the future is to use our approach to detect others DoS attacks, and to find an effective reaction mechanism to cope up with jamming.

References

[1] "US Vehicle Safety Communication Consortium," http: //www-nrd.nhtsa.dot.gov/pdf/nrd-12/CAMP3/ pages/VSCC.htm.

[2] The Willwarn Project. http://www.prevent-ip.org/willwarn.

[3] The Network on Wheels (NOW) Project. http://www.network-on-wheels.de.

[4] Albert Held and Rainer Kroh, "It-security and privacy for telematics services," in Workshop on Requirements for Mobile Privacy Security, University of London, UK, September 2002

[5] Jean-Pierre Hubaux, Srdjan C? apkun, and Jun Luo, "The security and privacy of smart vehicles," IEEE Security and Privacy, vol. 4, no. 3, pp. 49-55, 2004.

[6] Magda El Zarki, Sharad Mehrotra, Gene Tsudik, and Nalini Venkatasubramanian, "Security issues in a future vehicular network," in Proceedings of EuroWireless 2002, February 2002.

[7] Matthias Gerlach, "VaneSe - An approach to VANET security," in Proceedings of V2VCOM 2005, 2005.

[8] Tim Leinmuller, Elmar Schoch, Frank Kargl, and Christian Maihofer, "Influence of falsified position data on geographic adhoc routing," in ESAS 2005: Proceedings of the second European Workshop on Security and Privacy in Ad hoc and Sensor Networks, jul 2005.

[9] Philippe Golle, Dan Greene, and Jessica Staddon, "Detecting and correcting malicious data in vanets," in VANET '04: Proceedings of the first ACM workshop on Vehicular ad hoc networks. 2004, pp. 29-37, ACM Press.

[10] Florian Dotzer, "Privacy issues in vehicular ad hoc networks," in Workshop on Privacy Enhancing Technologies, Cavtat, Croatia, May 2005.

[11] Matt Blaze, Joan Feigenbaum, and Jack Lacy, "Decentralized trust management," in Proceedings of IEEE Symposium on Security and Privacy, 1996, number 96-17, pp. 164-173.

[12] Lidong Zhou and Zygmunt J. Haas, "Securing ad hoc networks," IEEE Network Magazine, vol. 13, no. 6, pp. 24-30, 1999.

[13] Laurent Eschenauer, Virgil Gligor, and John Baras, "On trust establishment in mobile ad-hoc networks," in Proceedings of the Security Protocols Workshop, April 2002.

[14] Christian Schwingenschlogl and Marc-Philipp Horn, "Building blocks for secure communication in ad-hoc networks," in Proceedings European Wireless, 2002.

[15] M. Raya, P. Papadimitratos, J.-P. Hubaux. Securing Vehicular Communications IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, 2006

[16] J. Y. Choi, M. Jakobsson, S. Wetzel. Balancing Auditability and Privacy in Vehicular Networks. ACM Workshop on Quality of Service and Security in Wireless and Mobile Networks (Q2Swinet)'05, Oct 2005.

[17] IEEE1609.2. IEEE trial-use standard for wireless access in vehicular environments - security services for applications and management messages, July 2006.

[18] IEEE Standard for Information technology -Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 3: Wireless Access in Vehicular Environments (WAVE), IEEE Draft Amendment P802.11p/D1.0, Feb. 2006

[19] The SeVeCom Project. http://www.sevecom.org/

[20] IEEE P1609.4, Wireless Access in Vehicular Environments (WAVE) Multi-Channel Operation, IEEE Draft Standard P1609.4/D08, Apr. 2006

[21] SUMO. http://sumo.sourceforge.net/

[22] G. Noubir and G. Lin. Low-power DoS attacks in data wireless lans and countermeasures. SIGMOBILE Mob. Comput. Commun. Rev., 7(3):2930, 2003.

[23] W. Xu, T. Wood, W.Trappe, and Y. Zhang. Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service. In Proceedings of the ACM Workshop on Wireless Security (WiSe), 2004.

[24] Anthony D. Wood, J. A. S., and Zhou, G. DEEJAM: Defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks. 4th IEEE Conference on Sensor and Ad Hoc Communications and Networks (2007).

[25] A. D.Wood and J. A. Stankovic. Denial of service in sensor networks. IEEE Computer, 35(10):54-62, 2002.

[26] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks. In Proceedings of MobiHoc'05, Urbana-Champaign, Illinois, USA.

[27] Dodge Y, Rousson V. 2004. Analyse de régression appliqué, Dunod.

[28] A.D. Wood, J.A., Stankovic, and S.H. Son. JAM: A Jammed-Area Mapping Service for Sensor Networks. In Real-Time Systems Symposium (RTSS), Cancun, Mexico, 2003.

[29] Fall K, Varadhan K. 2003. ns notes and documentation. UC Berkeley, LBL, USC/ISI, Xerox PARC.

978-1-4244-4148-8/09/$25.00 ©2009