Vehicular Communications 13 (2018) 56–63

Contents lists available at ScienceDirect

Vehicular Communications

www.elsevier.com/locate/vehcom

Jamming attack detection in a pair of RF communicating vehicles using unsupervised machine learning

Dimitrios Karagiannis *, Antonios Argyriou

Department of Electrical and Computer Engineering, University of Thessaly, Greece

ARTICLE INFO

Article history:
Received 29 September 2017
Received in revised form 1 April 2018
Accepted 13 May 2018
Available online xxxx

Keywords:
Vehicular ad-hoc network (VANET)
Jamming attack
Machine learning
Security

ABSTRACT

Wireless radio frequency (RF) jamming, both intentional and unintentional, poses a serious threat for wireless networks and wireless communications in general. Vehicular ad-hoc networks (VANET) are a subset of the wireless networks that incorporate modern safety-critical applications, that are vulnerable to jamming attacks. To preserve the secure communication and to increase its robustness against that type of attacks, an accurate detection scheme must be adopted. In this paper we present a jamming detection approach for wireless vehicular networks that leverages the use of unsupervised machine learning. The proposed method, utilizes a new metric, that is the variations of the relative speed between the jammer and the receiver, along with parameters that can be obtained from the on-board wireless communication devices at the receiver vehicle. Through unsupervised learning with clustering, we are able to differentiate intentional from unintentional jamming as well as identify the unique characteristics of each jamming attack. The proposed method is applied to three different real-life scenarios with extensive simulations being presented.

1. Introduction & motivation

Vehicular ad-hoc networks (VANET) have attracted again the interest of the research community because they are envisioned as a critical element of autonomous vehicles. Optimized operation of autonomous vehicles depends on the frequent exchange of safety messages between the vehicles, namely V2V communication, as well as between the vehicles and the roadside units (RSU) or infrastructure, namely V2I communication. Due to the nature of the wireless communication, these connections are vulnerable to a variety of attacks [5], [11]. These attacks aim at degrading the performance of the network and create opportunities that can be exploited by the attacker.

The RF jamming attack [4] is an attack particularly challenging to detect in every wireless network. In addition to that, the consistent and swift changes in topology as well as the high mobility of the communicating nodes, that characterize a VANET, all contribute in making the detection even more challenging. Moreover, the successful detection of a jamming attack may be obstructed by several conditions that might occur in an urban environment, such as interference caused by other wireless nodes, poor link conditions etc. They can all lead to false-positive detection or to an overall detection failure. The situation may be further deteriorated by the presence of a variety of different jammers [14].

Although there have been several experimental approaches for jamming detection [1], [4], [7], [8], [9], [10], [11], [15], only [3], [10] suggest the use of machine learning. In this paper, we introduce a new metric to be used – along with other metrics obtained from the on-board communication devices – as an extra feature in unsupervised learning so as to make the detection of potential RF jamming attacks more robust and efficient. The proposed metric, namely Relative Speed Variations (RSV), derives from the variations of the relative speed between the vehicles of the jammer and the target and is used, along with other cross-layer metrics, as an extra feature in the unsupervised method of clustering. Through clustering we are able to differentiate cases of intentional from cases of unintentional jamming (or interference) as well as extract the specific characteristics of each attack. For the validation of our approach, three different attack scenarios are investigated.

The main motivation behind proposing and utilizing the RSV metric is that we want to determine whether jamming is due to an intentional and malicious jammer or whether it is caused unintentionally by a random source. This distinction however, is difficult to be achieved using only the metrics previously utilized in literature, such as the Signal to Noise and Interference Ratio (SINR), the Packet Delivery Ratio (PDR) and the Received Signal Strength and Interference (RSSI). This differentiation is very important, es-

* Corresponding author.
E-mail address: dimikara@inf.uth.gr (D. Karagiannis).

https://doi.org/10.1016/j.vehcom.2018.05.001
2214-2096/

pecially in an urban environment, such as the one we examine, because it enables us to confront the problem in a more efficient manner. For instance, if jamming is correctly identified as interference, that is the collected jamming measurements are grouped into the interference cluster accurately, the vehicles could preserve their communication either by changing their channel (channel surfing) or by temporarily altering their route (route alteration). On the other hand, if intentional jamming is incorrectly identified as interference, the preceding solutions can not deal with the jammer effectively, who could also use the new channel or follow its targets in their new route. Besides the above, the distinction between cases of intentional and unintentional jamming is arguably more demanding and difficult than the simple differentiation between cases of intentional jamming and cases where there is a complete absence of jamming and has not been closely examined in previous related works.

The rest of this paper is structured as follows: Section 2 provides an overview of the related work in the domain of attack (not only jamming) detection, Section 3 is dedicated to the description of our topology and the channel model, Section 4 describes the proposed detection system, Section 5 describes the simulation setup and the assumptions being made, Section 6 presents the simulation results and finally Section 7 summarizes the significance of our approach and concludes our work.

2. Related work

Azogu et al. [1] have implemented a mechanism called Hideaway Strategy which uses the Packet Sending Ratio (PSR) metric to determine if the network is under a jamming attack, for the duration of which the nodes should remain inactive.

Bißmeyer et al. [2] base their detection scheme on the notion that a certain space will be occupied by only one vehicle at a certain time, utilizing the vehicle movement data.

Grover et al. [3] propose a machine learning based methodology to detect and classify several misbehaviors in VANETs. Using a series of metrics as features, a differentiation between malicious and not malicious nodes was achieved.

Hamieh et al. [4] propose a detection scheme that compares the calculated value of the correlation coefficient (CC) with the error probability (EP) and considers the network under jamming attack if CC $>$ EP.

Malebary et al. [6] propose a two-phase jamming detection method. In the initialization phase, the values of the RSS, the Packet Delivery/Send Ratio (PDSR) and Packet Loss Ratio (PLR) are calculated by the RSUs in a jammer-free network. Furthermore, a max value for the Received Signal Strength (RSS) is obtained for every PDSR value as well as two threshold values, equal to the maximum PDSR and to the minimum PLR respectively. In the second phase, when a PDSR value is lower than the defined threshold and a PLR value is higher than the respective threshold, a consistency check is conducted to determine whether the low PDSR value is consistent with the RSS value assigned in phase one, thus determining a jamming or no jamming situation.

Mokdad et al. [7], [8] propose a scheme for detecting a jamming attack in vehicular ad-hoc networks that depends on the variations of the PDR.

Puñal et al. [9] study the impact of RF jamming attacks in vehicular communications by creating a series of indoor and outdoor jamming scenarios under different jamming behaviors (constant, reactive and pilot jamming).

Puñal et al. [10] use several channel – Noise and Channel Busy Ratio (CBR), performance – Packet Delivery Ratio (PDR) and Maximum Inactive Time (Max IT) – and signal – Received Signal Strength (RSS) – metrics in combination with machine learning to detect the existence of reactive and constant jammers.

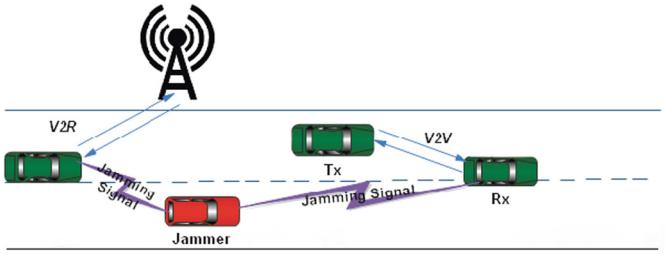

Fig. 1. Topology.

Quyoom et al. [11] and RoselinMary et al. [12] detect irrelevant and malicious packages by calculating the frequency, that is the number of broadcast packets per second, and the velocity of the vehicle that these packets are sent from. If the frequency and the velocity are both high and above a threshold then the packets are labeled as malicious, whereas if they are between a low and a high threshold value the packets are labeled as real.

Shafiq et al. [13] propose an attack detection approach based on the number of packets that are received. Each vehicle counts the number of messages it receives for a period of 10 seconds and at the end of which, it sends the number of packets along with the sender's Internet Protocol (IP) address to a module called comparator, which, in turn, compares the number of packets from each IP address to a threshold number. If an IP has a number of packets greater than the threshold value, then a message will be sent to vehicle in order to stop the communication with the malicious node and another message will be sent to the RSU to inform it about the jammer's existence. Finally, the RSU informs all the other nodes in its area of coverage about the jammer.

Xu et al. [15] state the inability of the PDR alone to differentiate jamming from interference cases and utilizes signal strength measurements and location information to determine if the PDR value is due to jamming or interference.

3. System model

3.1. Topology

The topology we adopt in our work (Fig. 1) involves a moving vehicle, namely R_x, that serves as the target of the jammer, another vehicle or a RSU (namely T_x) that is used as the transmitter of the useful signal and the jamming vehicle, namely J_x, that tries to intervene in the communication between R_x and T_x. In our work, we examine the case of communication between vehicles, that is V2V communication, therefore both the transmitter R_x and the receiver T_x are traveling vehicles.

The R_x–T_x pair travels at a constant speed, namely u_{R_x,T_x}, that is bound to the limitations of an urban environment. Upon spotting its target, the jammer begins following it adopting a smart or constant behavior. The smart jamming case involves a jammer that transmits its signal periodically from a secure distance whereas in the constant jamming case the jammer transmits its signal in an uninterrupted way without any intention to remain undetected, as opposed to the first jamming case.

3.2. Rician fading model

In our work, we adopt the Rician fading model, that is a channel model that includes path loss and also Rayleigh fading. When a signal is transmitted, whether it is a useful signal or a jamming one, this channel adds fading in addition to thermal noise. The baseband signal at the receiver is:

$$y = (h + \frac{1}{d_s^2}) * x_s * P_s + (h + \frac{1}{d_j^2}) * x_j * P_j + w \quad (1)$$