Jamming Attack Detection in a Pair of RF Communicating Vehicles Using Unsupervised Machine Learning

Dimitrios Karagiannis and Antonios Argyriou

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

May 15, 2018

Abstract—**Wireless radio frequency (RF) jamming, both intentional and unintentional, poses a serious threat for wireless networks and wireless communications in general. Vehicular adhoc 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.**

Keywords-Vehicular Ad-Hoc Network (VANET), Jamming Attack, Machine Learning, Security.

I. 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 wireless communication, these connections are vulnerable to a variety of attacks [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, especially 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.

II. 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 techniques to detect the existence of reactive and constant jammers.

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 labelled as malicious, whereas if they are between a low and a high threshold value the packets are labelled 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 send to vehicle in order to stop the communication with the malicious node and another message will be send 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.

III. System Model

A. Topology

The topology we adopt in our work (Figure 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.

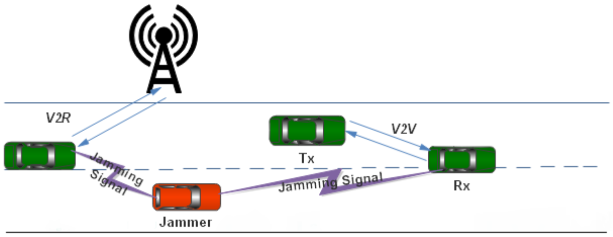

Figure 1: Topology

B. 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:

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

In the above h is a complex Gaussian random variable capturing Rayleigh fading, and x_s, x_j are the symbols that are transmitted (from the transmitter and the jammer), which in our case are equal to -1 or $+1$ because we assume BPSK modulation due to the fact that it is the most robust modulation scheme in high interference environments. P_s and P_j are the transmission power per symbol of the useful and of the jamming signal respectively and *w* is the channel noise. The terms d_s, d_j correspond to the distance between the transmitter and the receiver and between the jammer and the receiver.

IV. Proposed Detection System Based on Unsupervised Learning

In our work we assume that the measurement of the relative speed between the jamming vehicle and its target can be approximated and is available. To make our detection method more robust, apart from the metrics used in previous works (e.g. [10], [3]) as features, we introduce an additional one. Our goal is to evaluate whether this new metric improves the detection results under various scenarios without adding extra complexity to our model.

Apart from the RSV metric, our method uses a series of cross-layer metrics such as the RSSI, PDR and SINR, which are jointly processed with a unsupervised machine learning technique, namely the k-means algorithm. We assume that the simulations are conducted for a pre-determined period of time in which the speed of the R_x - T_x pair remains unchanged and is always greater than zero. Under this assumption, three different categories, based on the value of the relative speed, can be formed:

- Having relative speed that is equal to zero and remains unchanged, while the traveling speed of the R_x - T_x pair is stable and non-zero, indicates the existence of a jammer that follows the pair with the same speed.
- Having relative speed that is equal to the traveling speed of the R_x - T_x pair, that is relative speed not equal to zero and unaltered according to our previous assumption, indicates the absence of a moving jammer.
- Having relative speed that is not equal to zero for a period of time and then becomes zero while remaining unchanged, indicates the existence of a jammer that follows the R_x - T_x pair with the same speed after reaching it.

Based on these basic observations we developed an algorithm, that depending on the variations of the relative speed, generates a new metric, namely the RSV metric, that will be used in k-means unsupervised learning algorithm.

A. Proposed Algorithm

Algorithm 1 consists of two main *if* branches so that the existence of a jammer may be identified, primarily, by observing whether the relative speed is equal to zero or not, while taking into account the assumptions previously made for the traveling speed of the R_x - T_x pair. The algorithm iterates through all the values of the relative speed that have been collected and are stored into the Δu array. Starting from the first *if* branch, a comparison is made between each current value and the next entry in the array. If a change is observed, the new metric, that is refered to as *rsv*, receives a value equal to *A*, thus indicating a possible attack. If no change is observed, then the *rsv* receives a value equal to *NA*. The *NA* and *A* values are two extreme and distinct values able to differentiate attack from no attack cases. Moving on to the second *if* branch, the values of the Δu array that are equal to zero indicate a jamming attack, thus a value of *A* is, always, inserted into *rsv*.

Algorithm 1 RSV Algorithm

```
$N =$ number of observations
$rsv = matrix(nrow = 1, ncol = N)$
$i = 1$
while $(i < N)$ do
    if $\Delta u[i] \neq 0$ then
        if $\Delta u[i]$ == $\Delta u[i+1]$ && hasNext == T then
            $rsv \leftarrow NA$
        else if $\Delta u[i] \neq \Delta u[i+1]$ && hasNext == T then
            $rsv \leftarrow A$
        else if $\Delta u[i]$ == $\Delta u[i-1]$ then
            $rsv \leftarrow NA$
        else
            $rsv \leftarrow A$
        end if
    else if $\Delta u[i]$ == $0$ then
        $rsv \leftarrow A$
    end if
end while
```

B. Unsupervised Learning Algorithm

The unsupervised learning algorithm used in our work is the k-means algorithm, one of the most popular algorithms for unsupervised learning. It is selected because it works efficiently with large data sets, such as the ones that could derive from an urban environment containing the measurements that will be used in machine learning, without excessive memory requirements. In our case, a dataset of a total of 3000 measurements is utilized for simulation, a number, however, that could potentially be significantly bigger when the RF jamming attack detection scheme is applied under real-life conditions. It is important to clarify that our method does not rely on specific characteristics of k-means and so it can be easily implemented based on any type of partitioning clustering method.

V. Simulation Setup

A. Scenarios

In our work we have created three different scenarios - namely the **Interference Scenario**, the **Smart Attack Scenario** and the **Constant Attack Scenario** - each representing a jamming attack case that could potentially affect a VANET in real-life.

In the Interference Scenario, we assume that a moving and malicious jammer is not present in the network so as to check the efficiency of our method in differentiating jamming from interference, that is intentional from unintentional jamming, which, as it is already stated in Section I, is believed to be a very important and vital differentiation for the preservation of the V2V communication. The R_x - T_x pair travels, when, at some point, passes through an area with significant RF interference by which its communication is affected. The RF interference could be caused by a random source such as a malfunctioning device, i.e a defective router. In the Smart Attack Scenario, the jammer starts following the R_x - T_x pair while transmitting a jamming signal. It is considered as a smart jammer due to the fact that when it reaches its target at a distance of about $d = 15m$, retreats to a safe position and transmits periodically, aiming at remaining undetected for as long as possible. Alternatively, in a real-life situation, the jammer could keep changing its transmission power, hence achieving the same communication disruption without the need to constantly change its distance from the target. The safe position that the jammer retreats to as well as the rate according to which the jamming signal is transmitted, are randomly chosen in each simulation. In the Constant Attack Scenario, we examine the case of a constant jammer that follows the R_x - T_x pair while transmitting its jamming signal continuously without any intention to remain undetected, as opposed to the Smart Attack Scenario.

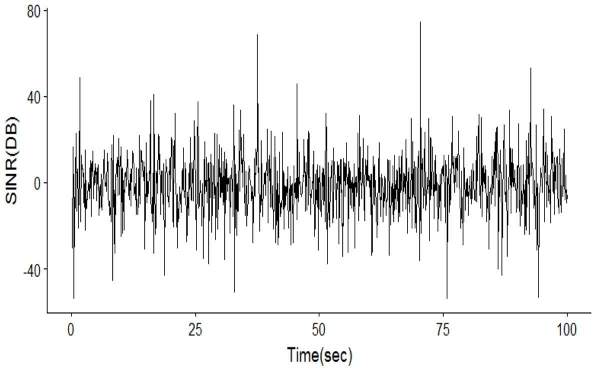

Figure 2: SINR vs Time for the Rician Fading Model in the Interference Scenario

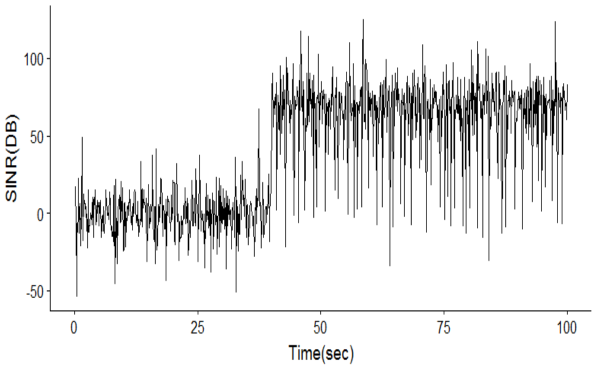

Figure 3: SINR vs Time for the Rician Fading Model in the Smart Attack Scenario

Figures 2 - 4 present the SINR versus time plots, for each scenario previously described, based on the measurements collected at the receiver R_x, and aim at highlighting the impact of different attack methods on the received signal. We choose to present only the SINR related plots due to the fact that they graphically represent the effect of intentional or unintentional jamming in wireless communication in a more efficient and interpretable way, compared to the PDR or RSSI related plots.

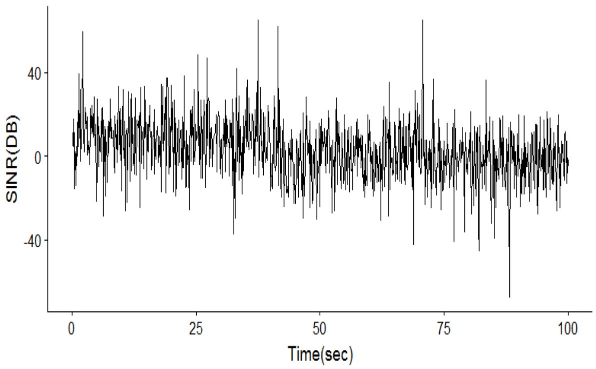

Figure 4: SINR vs Time for the Rician Fading Model in the Constant Attack Scenario

B. *Detection System Assumptions*

The number of clusters that is used is an important parameter that affects the interpretation of the simulation results. By using 2 clusters in the k-means algorithm, we practically, aim at identifying the existence (through intentional jamming detection) or absence (through unintentional jamming detection) of a jammer that affects the transmission of the useful signal. On the other hand, by using 3 clusters we can also examine the unique characteristics of each attack scenario, for instance a more intense attack when the jammer is close to the target or temporary no jamming attack if there is a jammer that periodically transmits its signal. Our investigation indicated *that the use of more than three clusters does not provide us with better interpretable results for each scenario nor it increases the jamming detection accuracy.*

Regarding the details of our simulation setup, the speed of the R_x - T_x pair is measured in meters per second and is bound to 15 m/sec ($\approx 54km/h$) and 20 m/sec ($\approx 72km/h$) respectively, thus representing medium and higher speed in a real-life urban environment. The distance between R_x and T_x is presumed not to be greater than 35 meters, which is a reasonable value for an urban environment such as the one we are considering. The initial distance between the jammer and the R_x -T_x pair is set to be equal to 200 meters so as to examine the effect of the jamming signal in the communication as the jammer gradually approaches its target.

The power of the transmitted signals, both from R_x and from J_x, is measured in milliwatt (mW) and is converted in the dBm scale. Both the jammer and the transmitter send out a signal using a power equal to 100 mW in our simulations. It is important to point out that reducing the power with which the jammer transmits its signal makes the detection easier, thus we have chosen to use the same power for both the jammer and the transmitter in order to test a more challenging case.

Both the useful and the jamming signal consist of packets that are 500 bits long. For each one of the three scenarios, the simulation is executed for a total of 1000 rounds, hence achieving the transmission of 1000 packets (with each one being 500 bits long) in total. Using a sampling period of 0.1 sec, we simulate the system for 100 seconds (for each scenario) and obtain 1000 measurements (for each scenario). Our simulator is written in the R programming language, using the open source, integrated development environment (IDE) for R, namely R-Studio.

Case	K-means Features	Speed	Clusters
A	RSSI, PDR, SINR, RSV	15m/s	2
B	RSSI, PDR, SINR	15m/s	2
C	RSSI, PDR, SINR, RSV	15m/s	3
D	RSSI, PDR, SINR	15m/s	3
E	RSSI, PDR, SINR, RSV	20m/s	2
F	RSSI, PDR, SINR	20m/s	2
G	RSSI, PDR, SINR, RSV	20m/s	3
H	RSSI, PDR, SINR	20m/s	3

Table I: Table summarizing the cases created and examined, based on the metrics used as features in the k-means algorithm, the traveling speed of the R_x - T_x pair and the number of clusters

VI. Simulation Results

The goal of our simulations is to underline the significance of the proposed RSV metric in clustering under various circumstances. For that reason, a series of cases is introduced in Table I, regarding the type of metrics used as features in clustering, the number of clusters and the traveling speed of the R_x - T_x pair under which the measurements were collected. For each case, we execute a simulation, which lasts 300 seconds and is equally split every 100 seconds in the three scenarios - starting from the Smart Attack Scenario, moving on to the Interference Scenario and concluding with the Constant Attack Scenario - previously discussed in subsection V-A.

In order to present the simulation results in a comprehensive yet interpretable way we will use a a mixture of tables and figures. Each table will be associated with a certain speed value and will contain all 3000 measurements grouped into 2 or 3 clusters based on the k-means features used in the current case that is examined. The figures are utilized in order to visualize the clustering results for each table. Each figure represents the SINR versus time plot that derives from the application of the k-means algorithm in each simulation. When using a number of 2 clusters, the red color is used to visualize the cluster of unintentional jamming attack, while the black color is used to visualize the cluster of intentional jamming. When using a number of 3 clusters, the green color is used for the pigmentation of the unintentional jamming cluster, the black is used to colorize cases that temporarily show no signs of intentional or unintentional jamming attack and the red for the respective cases affected by the presence of a jammer. Based on the cases of Table I, a total number of eight tables (one for each case) and their corresponding figures will be presented.

A. ***Case A***: *Use of the RSV metric, 15m/s data and 2 clusters*

Starting from Case A, where the RSV metric is used as an extra feature in the k-means algorithm, we can see that for a number of $k = 2$ clusters and for measurements collected under a speed of 15m/s, there is a clear differentiation between cases of intentional and unintentional jamming. However, there is an issue in identifying the measurements collected while the jammer remained temporarily idle *(these are the measurements that belong to the Smart Attack Scenario and can be identified in Figure 5 by the increased value of SINR between $t = 50sec$ and $t = 100sec$ approximately)*, which is expected due to the number of clusters selected. This is dealt with in a following case where the number of clusters is increased to three. All 2000 measurements, therefore, belonging to each one of the two attack scenarios, namely the Smart Attack and Constant Attack scenarios, are grouped into the Attack cluster, whereas the remaining 1000 that belong to the Interference Scenario are grouped into the Interference cluster. The previous results can be visualized in Figure 5 where, as it is already stated, the red color is used to represent the Interference cluster while the black color is used for the Attack cluster.

Cluster Type	Interference Scenario	Smart Attack Scenario	Constant Attack Scenario
Interference	1000	0	0
Attack	0	1000	1000

Table II: Clustering results for Case A

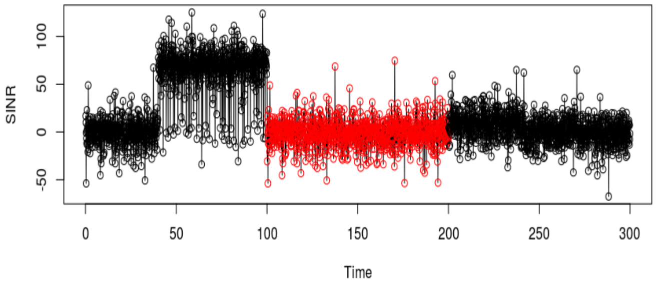

Figure 5: SINR vs Time plot using RSSI, PDR, SINR and RSV as clustering features, with a number of $k = 2$ clusters and for a speed of 15m/s

B. ***Case B***: *Omission of the RSV metric, 15m/s data and 2 clusters*

In order to highlight the significance of the RSV metric, we examine Case B in which the proposed metric is omitted. This case acts as a comparison to the preceding one, with the traveling speed of the R_x - T_x pair and the number of clusters remaining unchanged.

Cluster Type	Interference Scenario	Smart Attack Scenario	Constant Attack Scenario
Interference	991	444	987
Attack	9	556	13

Table III: Clustering results for Case B

From both the Table III and Figure 6, it is evident that omitting the RSV metric from clustering leads to a grouping

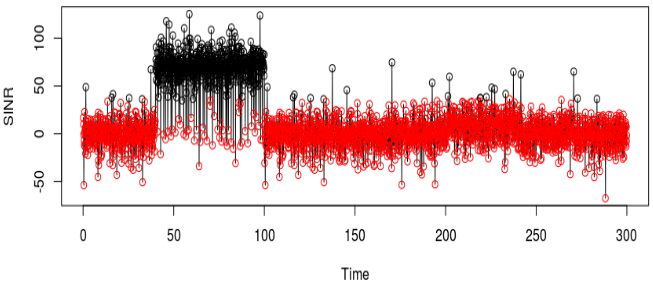

Figure 6: SINR vs Time plot using RSSI, PDR, SINR as clustering features, with a number of $k = 2$ clusters and for a speed of 15m/s

that differs significantly from the one previously presented in Table II of Case A. From the 1000 measurements of the Interference Scenario, 9 are clustered as intentional attack cases, while a total of 1431 measurements from both the Smart Attack and the Constant Attack scenarios is clustered as unintentional attack cases. As a consequence, the significance of the RVS metric in differentiating intentional from unintentional jamming while using a number of $k = 2$ clusters is evident.

C. ***Case C***: *Use of the RSV metric, 15m/s data and 3 clusters*

As it is already stated, the use of $k = 3$ clusters enables us to identify the certain characteristics of each scenario. Introducing Case C, where the RSV metric is used as an extra feature in unsupervised learning, we are able not only to distinguish cases of interference from cases of intentional jamming but also identify the measurements collected while the jammer remained temporarily idle, thus solving the problem that was previously described in the case of $k = 2$ clusters.

Cluster Type	Interference Scenario	Smart Attack Scenario	Constant Attack Scenario
Interference	1000	0	0
Attack	0	445	989
Not Attack	0	555	11

Table IV: Clustering results for Case C

From Table IV we can see that all 1000 collected measurements, while examining the Interference Scenario, are correctly grouped into the interference cluster. On the other hand, for the Smart Attack Scenario we expect to have two clusters of measurements, one containing the data collected while the jammer was active and the jamming signal was affecting the R_x - T_x communication and a second containing the data collected when the jammer was temporarily idle. From the 1000 measurements of the Smart Attack Scenario, 445 are grouped into the attack cluster while the remaining 555 into the non-attack cluster. Regarding the Constant Attack Scenario, we can see that 11 measurements are grouped into the cluster of non-attack, indicating that at some point the jammer remained idle. It is already stated, however, that in the case of the Constant Attack Scenario, the jammer transmits the disrupting signal continuously without pause and without the intention to stay undetected, hence we can see that k-means has wrongly placed these measurements in the non-attack cluster. The preceding observations can be visualized in Figure 7.

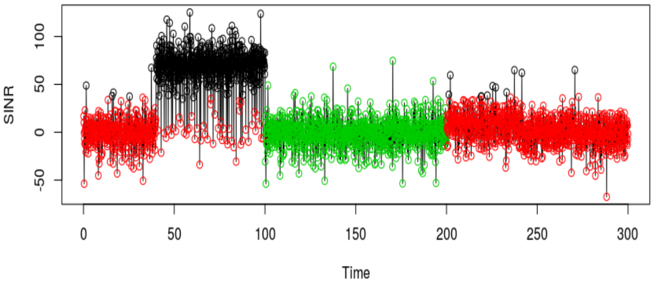

Figure 7: SINR vs Time plot using RSSI, PDR, SINR and RSV as clustering features, with a number of $k = 3$ clusters and for a speed of 15m/s

Following the colorization options described at the beginning of this section, the green color represents the interference cluster, the black color the cluster of non-attack and the red color the cluster of attack. Once more the significance of the RSV metric is evident and leads not only to a perfect differentiation between cases of intentional and unintentional jamming but also to an highly accurate demarcation between cases of interference, cases of intentional jamming and cases with total absence of jamming.

D. ***Case D***: *Omission of the RSV metric, 15m/s data and 3 clusters*

The crucial role of our proposed metric is further highlighted if we compare the results obtained in the previous case with the ones that we obtain in the current case, namely Case D, in which the RSV metric is omitted from the unsupervised learning process, while both the number of clusters and the traveling speed of the R_x - T_x pair remain the same as before.

Cluster Type	Interference Scenario	Smart Attack Scenario	Constant Attack Scenario
Interference	463	219	575
Attack	532	235	419
non-attack	5	546	6

Table V: Clustering results for Case D

From Table V it can be seen that not using the RSV metric as an extra feature in the k-means algorithm, leads to results that differ significantly compared to the results of Table IV. There is not a clear separation between cases of intentional and unintentional jamming, as 532 measurements from the Interference Scenario are wrongly grouped in the attack cluster and 219 measurements from the Smart Attack Scenario and 575 measurements from the Constant Attack Scenario are incorrectly placed into the interference cluster. Moreover, the differentiation between jamming cases (both intentional and unintentional) and cases without jamming is, also, not very accurate as it can be seen from the contents of the non-attack cluster in the case of the Interference and the Constant Attack scenarios. All the above are visualized in Figure 8, where, again, the black color is used for the pigmentation of the non-attack cluster, the red color for the attack cluster and the green color for the interference cluster.

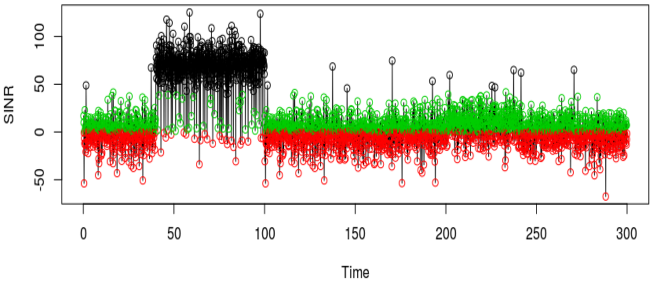

Figure 8: SINR vs Time plot using RSSI, PDR, SINR as clustering features, with a number of $k = 3$ clusters and for a speed of 15m/s

E. Case E: *Use of the RSV metric, 20m/s data and 2 clusters*

Having evaluated the performance of our proposed detection scheme using data collected under a speed of 15m/s, we now proceed into a different traveling speed value, that of 20m/s, so as to examine its behavior while testing cases with fairly high speed. As previously, we will begin by examining the case in which the RSV metric is used in clustering while having selected a number of $k = 2$ clusters. Using the RSV metric along with a number of two clusters, as it is already stated, enables us to separate cases of intentional from cases of unintentional jamming, without, however, providing us with further information about the characteristics of the current scenario examined (i.e the periodic jamming of the Smart Attack Scenario), a problem that is confronted with the use of $k = 3$ clusters.

From the contents of Table VI, it is evident that the use of the proposed metric as an extra feature leads to the creation of two clusters, clearly separated among each other. All 1000 measurements belonging to the Interference Scenario are placed into the interference cluster, while all 2000 measurements from the Smart Attack and the Constant Attack Scenarios are placed into the attack cluster. Once more, the problem with the use of $k = 2$ clusters is that we are not able to identify the measurements of the Smart Attack Scenario that were collected while the jammer remained idle temporarily (a certain characteristic of the Smart Attack Scenario).

Cluster Type	Interference Scenario	Smart Attack Scenario	Constant Attack Scenario
Interference	1000	0	0
Attack	0	1000	1000

Table VI: Clustering results for Case E

The results are visualized in Figure 9, in which the red color corresponds to the interference cluster and the black color to the attack cluster.

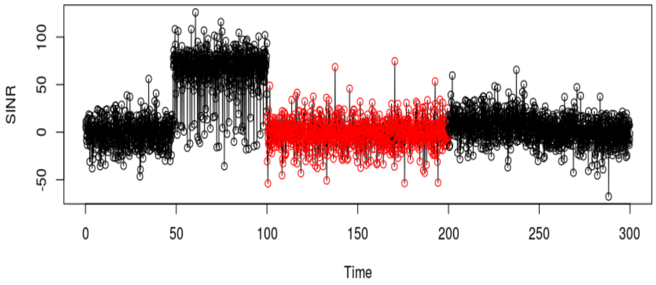

Figure 9: SINR vs Time plot using RSSI, PDR, SINR and RSV as clustering features, with a number of $k = 2$ clusters and for a speed of 20m/s

F. Case F: *Omission of the RSV metric, 20m/s data and 2 clusters*

When the RSV metric is omitted, the results obtained are similar to the ones presented in Table III. From the 1000 measurements of the Interference Scenario, 9 are incorrectly clustered as intentional jamming attack cases, while a total of 1504 measurements from both the Smart Attack and the Constant Attack Scenarios is clustered as unintentional jamming attack cases and can be visualized in Figure 10.

Cluster Type	Interference Scenario	Smart Attack Scenario	Constant Attack Scenario
Interference	991	521	983
Attack	9	479	17

Table VII: Clustering results for Case F

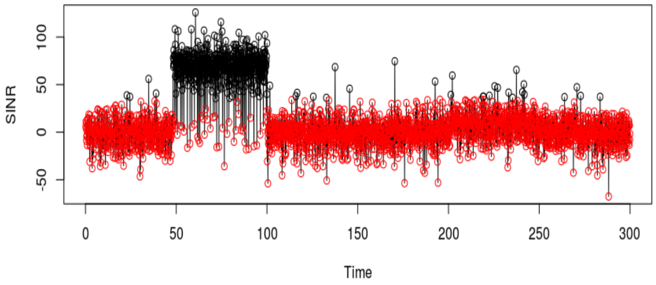

Figure 10: SINR vs Time plot using RSSI, PDR, SINR as clustering features, with a number of $k = 2$ clusters and for a speed of 20m/s

G. Case G: *Use of the RSV metric, 20m/s data and 3 clusters*

As seen previously, the use of an extra cluster helps us extract the unique characteristics of each scenario and resolve the issue described in the case of $k = 2$ clusters. Using the RSV metric, not only a clear separation among cases of intentional and cases of unintentional jamming is achieved, but also an identification of cases with no jamming affecting the wireless communication (i.e idle jammer in the Smart Attack Scenario).

Cluster Type	Interference Scenario	Smart Attack Scenario	Constant Attack Scenario
Interference	1000	0	0
Attack	0	521	984
Not Attack	0	479	16

Table VIII: Clustering results for Case G

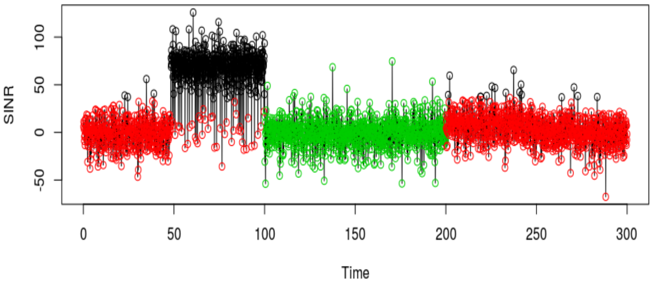

Figure 11: SINR vs Time plot using RSSI, PDR, SINR and RSV as clustering features, with a number of $k = 3$ clusters and for a speed of 20m/s

From Table VIII we observe that the distinction between intentional and unintentional jamming is clear when the RSV metric is used in clustering, as all 1000 measurements from the Interference Scenario are correctly grouped into the respective interference cluster, which contains no other measurements from the two attack scenarios. Apart from that, the measurements of the Smart Attack Scenario collected while the jammer is temporarily idle are also identified and can be visualized in Figure 11, along with the other clustering results, presented in black, with the interference cluster using the green color and the attack cluster the red color.

*H. **Case H**: Omission of the RSV metric, 20m/s data and 3 clusters*

The last case evaluates the performance of our RF jamming attack detection scheme when omitting the RSV metric from unsupervised learning and while the traveling speed of the R_x - T_x pair as well as the number of clusters remain the same as before.

Cluster Type	Interference Scenario	Smart Attack Scenario	Constant Attack Scenario
Interference	463	260	596
Attack	531	268	396
Not Attack	6	472	8

Table IX: Clustering results for Case G

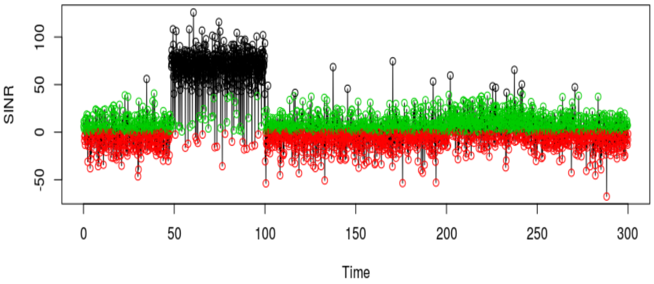

Figure 12: SINR vs Time plot using RSSI, PDR, SINR as clustering features, with a number of $k = 3$ clusters and for a speed of 20m/s

Both from Table VIII and from the Figure 12 it is evident that omitting the RSV metric leads to results that differ significantly from the respective ones in Case G (Table VIII). Regarding the differentiation between cases of intentional and unintentional jamming, we can see that from the Interference Scenario only 463 measurements are correctly grouped into the interference cluster, while for the Smart Attack and the Constant Attack Scenarios, a total of 856 measurements is incorrectly clustered as unintentional attack. In addition to that, there are some measurements from the Interference and the Constant Attack Scenarios that are, also, incorrectly clustered as no jamming attack cases, that is the separation between jamming attack (intentional or unintentional) cases and cases with no jamming is not very accurate. Once more, the attack cluster is colorized red, the interference cluster green and the no attack cluster black.

VII. CONCLUSIONS

In this paper, we presented a method for detecting and clustering cases of a specific type of DDoS attack, namely the RF jamming attack, based on unsupervised machine learning and by exploiting a novel metric, the variations of the relative speed (RSV) between the vehicle of the jammer and the vehicle of the receiver. To evaluate the significance of the proposed metric, we implemented three different attack scenarios - two with a moving jammer present and one with interference only. Our approach is, not only, able to differentiate malicious and intentional RF jamming from unintentional jamming (interference) but can also identify the certain characteristics of each jamming case.

Through our evaluation, we were able to establish the crucial role of the relative speed and its variations in efficiently achieving jamming detection. Additionally, we showed that a system based only on typical wireless receiver measurements from the physical and the network layer, such as PDR, SINR and RSSI, cannot accurately distinguish interference from intentional jamming cases nor identify the unique characteristics of an attack.

As part of our future work, we intend to explore the idea of using the proposed metric in supervised machine learning framework so as to be able to predict a jamming attack before it even starts, based on previous knowledge. Furthermore, we deem as critical to improve and extend our algorithm, used in order to create the RSV metric, so as to be able to work with data collected under a speed value that might change throughout the course of the simulation, as it could happen in a real-life environment.

References

[1] Ikechukwu K Azogu, Michael T Ferreira, Jonathan A Larcom, and Hong Liu. A new anti-jamming strategy for vanet metrics-directed security defense. In *Globecom Workshops (GC Wkshps), 2013 IEEE*, pages 1344–1349. IEEE, 2013.

[2] Norbert Bißmeyer, Christian Stresing, and Kpatcha M Bayarou. Intrusion detection in vanets through verification of vehicle movement data. In *Vehicular Networking Conference (VNC), 2010 IEEE*, pages 166–173. IEEE, 2010.

[3] Jyoti Grover, Nitesh Kumar Prajapati, Vijay Laxmi, and Manoj Singh Gaur. Machine learning approach for multiple misbehavior detection in vanet. *Advances in Computing and Communications*, pages 644–653, 2011.

[4] 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.

[5] Hamssa Hasrouny, Abed Ellatif Samhat, Carole Bassil, and Anis Laouiti. Vanet security challenges and solutions: A survey. *Vehicular Communications*, 2017.

[6] Sharaf Malebary, Wenyuan Xu, and Chin-Tser Huang. Jamming mobility in 802.11 p networks: Modeling, evaluation, and detection. In *Performance Computing and Communications Conference (IPCCC), 2016 IEEE 35th International*, pages 1–7. IEEE, 2016.

[7] Lynda Mokdad, Jalel Ben-Othman, and Anh Tuan Nguyen. Djavan: Detecting jamming attacks in vehicle ad hoc networks. *Performance Evaluation*, 87:47–59, 2015.

[8] Anh Tuan Nguyen, Lynda Mokdad, and Jalel Ben Othman. Solution of detecting jamming attacks in vehicle ad hoc networks. In *Proceedings of the 16th ACM international conference on Modeling, analysis & simulation of wireless and mobile systems*, pages 405–410. ACM, 2013.

[9] Oscar Puñal, Ana Aguiar, and James Gross. In vanets we trust?: characterizing rf jamming in vehicular networks. In *Proceedings of the ninth ACM international workshop on Vehicular inter-networking, systems, and applications*, pages 83–92. ACM, 2012.

[10] Oscar Puñal, Ismet Aktaş, Caj-Julian Schnelke, Gloria Abidin, Klaus Wehrle, and James Gross. Machine learning-based jamming detection for ieee 802.11: Design and experimental evaluation. In *A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th International Symposium on*, pages 1–10. IEEE, 2014.

[11] Abdul Quyoom, Raja Ali, Devki Nandan Gouttam, and Harish Sharma. A novel mechanism of detection of denial of service attack (dos) in vanet using malicious and irrelevant packet detection algorithm (mipda). In *Computing, Communication & Automation (ICCCA), 2015 International Conference on*, pages 414–419. IEEE, 2015.

[12] S RoselinMary, M Maheshwari, and M Thamaraiselvan. Early detection of dos attacks in vanet using attacked packet detection algorithm (apda). In *Information Communication and Embedded Systems (ICICES), 2013 International Conference on*, pages 237–240. IEEE, 2013.

[13] Mohammed O Shafiq, Arshad Ali, Ejaz Ahmed, Hafiz F Ahmed, and Hiroki Suguri. Detection and prevention of distributed denial of services attacks by collaborative effort of software agents, first prototype implementation. In *Parallel and Distributed Computing and Networks: Proceedings of the 23rd IASTED International Multi Conference on Applied Informatics*. IASTED, 2005.

[14] Mehreen Shaikh and Abid H Syed. A survey on jamming attacks, detection and defending strategies in wireless sensor networks.

[15] Wenyuan Xu, Wade Trappe, Yanyong Zhang, and Timothy Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, pages 46–57. ACM, 2005.