MIMO Techniques for Jamming Threat Suppression in Vehicular Networks

Dimitrios Kosmanos[1], Nikolas Prodromou[1], Antonios Argyriou[1], Leandros A. Maglaras[2], Senior Member, IEEE and Helge Janicke[2]

Abstract

Vehicular Ad Hoc networks have emerged as a promising field of research and development, since they will be able to accommodate a variety of applications, ranging from infotainment, to traffic management and road safety. A specific security-related concern that Vehicular Ad Hoc networks face is how to keep communication alive in the presence of Radio Frequency jamming, especially during emergency situations. Multiple Input Multiple Output techniques are proved to be able to improve some crucial parameters of vehicular communications such as communication range and throughput. In this article we investigate how Multiple Input Multiple Output techniques can be used in Vehicular Ad Hoc networks as active defense mechanisms in order to avoid jamming threats. For this reason, a variation of Spatial Multiplexing is proposed, namely vSP4, that achieves not only high throughput, but also a stable diversity gain, upon the interference of a malicious jammer.

I. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) have emerged as a promising field of research [1], [2], where advances in wireless and mobile ad-hoc networks can be applied to real-life problems (traffic jams, fuel consumption, pollutant emissions, and road accidents). Vehicles may utilize a variety of wireless technologies to communicate with other devices, but the dominant is Dedicated Short-Range Communication (DSRC) [3], which is designed to support a variety of applications based on vehicular communications. VANETs are currently the center of attention for car manufacturers, technology companies and transportation authorities. The basic idea behind Vehicular Communications is to help broaden the range of perception of the driver and help with autonomous assistance applications.

[1] Department of Electrical & Computer Engineering, University of Thessaly, Volos, Greece (dikosman,niprodro@uth.gr,anargyr)@uth.gr

[2] School of Computer Science and Informatics, University, Leicester, UK (leandros.maglaras, heljanic)@dmu.ac.uk

VANETs can be considered as mobile *ad hoc* networks that are utilized to enhance traffic safety and provide comfort applications to drivers. The unique features of VANETs include fast-moving vehicles that follow pre-determined paths (*i.e.*, roads) though having a high diversity of mobility patterns, along with messages that have different priority levels. For example, messages for comfort and infotainment applications have low priority, while messages for traffic safety applications require timely and reliable message delivery [4]. Hybrid Vanets can accommodate vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. This enables several other forms of communication, such as vehicle-to-broadband cloud (V2B), where the vehicle communicates with a monitoring data center and vehicle-to-human (V2H) to communicate with vulnerable road users, e.g. pedestrians or bicycles [5]. Except from uninterrupted and reliable connectivity one of the major issues that Vanets have to face is security [6].

As cars become more interconnected one of the main challenges that manufacturers have to face is security. Especially for safety applications where early warning of the driver is crucial, it is essential to ensure that life-critical information cannot be modified or dropped by an attacker. Vehicular security threats target all the three major components of security: Confidentiality, integrity and availability (CIA) [7]. A specific security-related concern that VANETs face is maintaining communication during an RF jamming attack. As reported in [8] it is proved that constant, periodic and reactive RF jamming has significant impact on vehicular communications through extensive measurements in an anechoic user. Specifically in [8] the impact of the reaction delay and interfering signal duration on the effectiveness of the reactive jammer is also quantified. Hence, jamming-aware communications, protocols and applications, as well as effective jamming detection and reaction strategies are of great need.

Regarding jamming in VANETs, the main purpose of previous works was to analyze threats and focus on the effects of RF jamming [9], [10]. Most of previous works deal with the early and correct detection of malicious nodes [11] or develop some techniques that use frequency hopping [12] in order to find an interference free channel. These methods are too complicated to be implemented in a real environment, especially when more sophisticated jamming attacks have to be addressed (e.g. a reactive jammer). Also usually in RF Jamming attacks all communication channels are blocked and techniques like frequency hopping do not have any positive effect.

II. Motivation

To combat RF Jamming effectively in this paper we propose the use of MIMO. MIMO systems, although thoroughly investigated, are mostly focused on how to improve some parameters of vehicular communications e.g., communication range, throughput etc. Previous work mainly focuses on explaining the benefits of using MIMO in VANETs [13], examine propagation models [14], [15] and OFDM-based MIMO systems [16]. Previous works did not study MIMO systems as an active defense mechanism that overcomes different types of RF jamming attacks. Only recently active anti-jamming MIMO based techniques were introduced. Authors in [17] present a MIMO-based anti-jamming technique that uses pre-rotation or beamforming of the jamming signal in order to improve sender signal decodability. The method is difficult to be implemented in a VANET scenario since the channel conditions are changing very frequently and multiple pilots must be used by the sender and the jammer for real time channel tracking. In another work in [18] the authors proposed a cooperative interference mitigation scheme combined with MIMO for jamming suppression. This method is based on the channel information ratio, that is provided from the probing of the channel. In VANETs, the frequently changing channel would generate a large number of probes, overloading the channel. Authors in [19] use MIMO and interference cancellation in order to support communication in the presence of strong interference. However, only random interference is considered and the proposed method is not tailored to reactive RF jammers. Last, in [20] an improved MIMO channel estimation for interference cancellation is exploited to combat reactive jamming. However, a quite complicated method based on Kalman filter and basis expansion model (BEM) with a large number of iterations for convergence is used to track the channel of the jammer, making the method difficult to be employed in real situations.

This article investigates MIMO systems for improving robustness in RF continuous and reactive jamming threats and simultaneously achieving higher throughput rates in VANETs. In this paper, the MIMO scheme with instantaneous Channel State Information (CSI) per received packet at the receiver and without knowledge for the channel of jammer is used. We show that using MIMO the suppressing of the jamming signal can be successful without using a jamming detection phase and regardless of the type and structure of the jamming signal. Our proposed scheme named $vSP4$, that combines the Alamouti with Spatial Multiplexing (SM) [21], nearly doubles the throughput and also decreases the silence time almost by a factor of two when compared to the classic *cSP*4 scheme, in the presence of a malicious jammer. Another contribution of this paper is a new framework for VANET simulations that combines three known simulators for obtaining more realistic results.

III. System Model

A. System Description

Simulation Framework: For evaluating the proposed defense mechanisms, the VEINS simulator is used [22]. This open-source framework consists of two well-known simulators: OMNET++ an event-based network simulator and SUMO, a road traffic simulator. Furthermore, instead of using the existing PHY layer of OMNET++, the GEMV (a Geometry-based Efficient propagation Model for V2V) [23] tool was integrated into the VEINS network simulator. GEMV calculates a propagation model that separates links into Line-of-sight LOS and non-LOS (NLOSv, and NLOSb) link types and calculates deterministically the large-scale signal variation (i.e., path loss and shadowing) for each link type. Furthermore, GEMV employs a simple geometry-based small-scale signal variation model that calculates the additional stochastic signal variation based on the information about the surrounding objects. GEMV was configured and modified to be portable to the VEINS simulator and incorporated into this. Figure 1 illustrates the instantaneous SNR vs distance calculated by integration of GEMV-VEINS compared with this calculated by VEINS simulator. GEMV uses a more detailed propagation model to calculate the SNR that takes into account the 'quality' of the links taking into account the physical obstacles (e.g. building, cars) compared to simple log-distance model that is used in VEINS. The proposed VEINS-GEMV integrated simulation framework allows more realistic simulations since the SNR is affected not only from the distance among vehicles, but also from the small-scale and the large-scale variations of the wireless medium.

Channel Model and PHY Modulation: For simulations the 802.11p MAC and PHY parameters at 5.9GHz (10Mhz) are used. Please refer to Table II for details of specific parameter values. Also, Rayleigh fading channels with Additive White Gaussian Noise (AWGN) ($\tilde{w}$), being stable during the transmission of 10 symbols is assumed. In our scenario 10 packets per second are transmitted. The average SNR is calculated for each second. For the transmission of 5* 10^3 symbols the modulation that was used in simulations is QPSK/16-QAM and the data rates that were used are 3Mbps for packet header and 6Mbps for packet payload which are currently supported by VEINS project. A modulation and coding scheme (MCS) with m

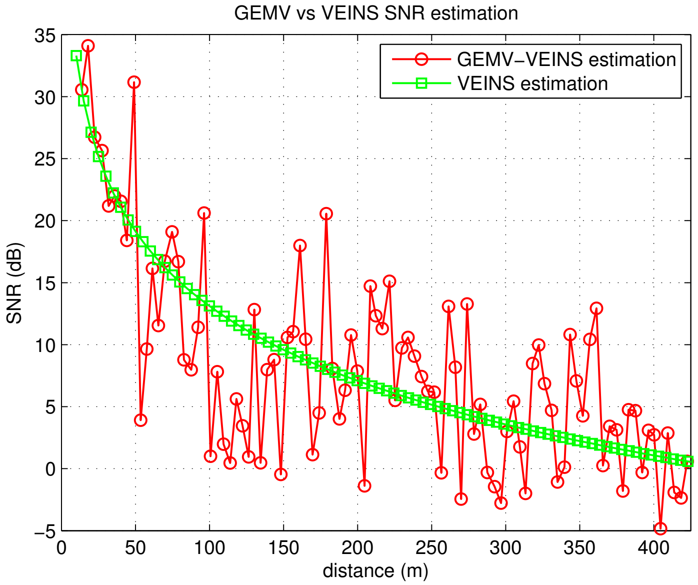

Fig. 1: GEMV-VEINS SNR vs Distance estimation.

bits/symbol is used by the transmitter and the jammer while its optimal value is determined by each node independently. For the evaluation of MIMO for suppressing jamming effects we use three different MIMO schemes.

MIMO Model: For all the MIMO schemes we assume that K is the number of symbols that are transmitted in the duration of T time slots, P_T is the power of transmitted signal and σ_n^2 is the uncorrelated equal noise power at the receiver. We also use Forward Error Correction (FEC) coding at the transmitter assuming perfect instantaneous channel knowledge at the receiver. Moreover, n_R is the number of received antennas, n_T is the number of transmitted antennas, while the variable n_A describes how many antennas are used for sending multiple copies of the same symbol with the MIMO schemes for increasing the diversity gain. We assume that $h_{Tx,Rx}$ is the channel between the transmitter (Tx) and receiver (Rx). The systems we test are: a 2x2 Alamouti scheme in section (IV-A), a 2x2 SM in section (IV-B) and a enchanced 4x4 combination of Alamouti and SM scheme in section (IV-C).

IV. The Proposed Defense System

A. Classic Alamouti algorithm

One of the most popular techniques for improving reliability in MIMO systems is the Alamouti Space-Time Block Coding (STBC) technique [24]. STBC is a technique used in wireless communications to transmit multiple copies of a data stream across a number of antennas to improve reliability. Alamouti requires at least 2 transmit antennas [21]. It does not improve throughput in terms of absolute numbers, but achieves significantly lower Bit Error Rate (BER). With Alamouti, 2 symbols are transmitted orthogonally as illustrated in Table I. We use a 2x2 MIMO Alamouti scheme in which $(K = 2)$ number of symbols are transmitted in the duration of T time slots $(T = 2)$.

Tx(antenna)Id/TimeSlot	T1	T2
Tx1	u_1	u_2
Tx2	$-u_2*$	u_1*

TABLE I: Alamouti scheme

Due to orthogonal transmission with Alamouti, the two transmitted symbols do not interfere with each other. Each symbol is communicated over a different independent channel realization, improving the overal system reliability. The received signal can be written as:

$$\vec{y} = \begin{bmatrix} y_{11} \\ y_{21}^* \\ y_{12} \\ y_{22}^* \end{bmatrix} = \begin{bmatrix} h_{11} & h_{21} \\ h_{21}^* & -h_{11}^* \\ h_{12} & h_{22} \\ h_{22}^* & -h_{12}^* \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} + \vec{w} \tag{1}$$

In the above equation the y_{11} and y_{12} denote the received symbols at antenna element $no.1$ and 2 at the first time slot $T1$ (Table I) and similarly y_{21}^* and y_{22}^* represent the received symbols at antenna element $no.1$ and 2 at the second time slot $T2$. Using the diversity- multiplexing tradeoff (DMT) [25], we can see that the rate for symbols sent with the 2x2 MIMO Alamouti scheme is ($r = K/T = 1$ symbols/time-slots) and the diversity gain is $d = 1$. So the DMT tradeoff is (1,1).

Decoding with Maximum Ratio Combining (MRC), combines signals using a weight factor in order to achieve higher average SNR [21]. If we denote as $H = \begin{bmatrix} h_{11} & h_{21} \\ h_{21}^* & -h_{11}^* \\ h_{12} & h_{22} \\ h_{22}^* & -h_{12}^* \end{bmatrix}$ and the inverted matrix product as $(H^H H)^{-1} = \begin{bmatrix} \frac{1}{|h_{11}|^2+|h_{21}|^2+|h_{12}|^2+|h_{22}|^2} & 0 \\ 0 & \frac{1}{|h_{11}|^2+|h_{21}|^2+|h_{12}|^2+|h_{22}|^2} \end{bmatrix}$, the proposed signal $\tilde{r}$ is:

$$\tilde{r} = H^H (H^H H)^{-1} \vec{\tilde{y}} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} + \vec{w} \tag{2}$$

Because MRC decoding is used, as the number of receive antennas is increased, the overall performance is also improved. Finally, after calculating the throughput of the Alamouti scheme, we see that the instantaneous capacity is:

$$C_{Alamouti} = \frac{K}{T} \log(\det(I + \frac{P_T}{r\sigma_n^2 n_T}(H^H H))) \tag{3}$$

From the above equation we can conclude that the capacity of the Alamouti scheme depending on the rate of the symbols that are transmitted in each time slot (i.e., $r = K/T$). Consequently, if the rate with Alamouti increases, then the capacity of this scheme is also increased. Finally, for the 2x2 MIMO Alamouti scheme the capacity is: $C_{Alamouti} >= C_{SISO}$, where SISO is a Single (antenna) Input- Single (antenna) Output scheme.

B. Classic Spatial Multiplexing

The method which offers the highest throughput is SM. The reason is that each antenna transmits a different symbol during each time slot. So in case of 2, 4 or N antennas in general, the throughput is doubled, quadrupled or increased by N times respectively. However, in poor channel conditions SM achieves low SNR and so high BER. The MIMO channel with SM is:

$$\vec{y} = H\vec{x} + \vec{w} \tag{4}$$

By applying Least Squares Equalization to the channel matrix H, we have have to by multiply with the pseudo-inverse matrix:

$$H^{\dagger} = (H^H H)^{-1} H^H \tag{5}$$

The sufficient statistic that is used for detection is then

$$\vec{r} = (H^H H)^{-1} H^H \vec{y} = x + (H^H H)^{-1} H^H \vec{w}, \tag{6}$$

which is also known as the zero-forcing method.

For a 2x2 MIMO SM scheme the received signals that reach at antenna 1 and 2 , can be written:

$$y_j = \sum_{i=1}^{2} h_{ij} x_i + w_j, j = 1,2 \tag{7}$$

From the above equation, we notice that the received copies of the symbols x_1 and x_2 are 2. So, the multiplexing gain of the SM using the DMT tradeoff is 2, while the diversity gain is 0 (2,0).

Calculating the capacity of SM scheme we have:

$$C_{SM} = \log(\det(I + \frac{P_T}{\sigma_n^2 n_T}(H^H H))) = \sum_{i=1}^{\min(n_R,n_T)} \log(1 + \frac{P_T \lambda_i^2}{\sigma_n^2 n_T}) \tag{8}$$

In the above equation λ_i^2 are the eigenvalues of the $(H^H H)$ matrix [21]. For our 2x2 MIMO example, compared with the capacity of Alamouti scheme with SM can conclude that $C_{SM} = 2 * C_{Alamouti}$ in the high SNR regime.

C. Enhanced version of Spatial Multiplexing

In this work, the classic version of SM is enhanced for our particular application with a combination of SM and Alamouti. More specifically users may choose a slower but more reliable transmission technique, by selecting how many different symbols will be transmitted in each time slot. The remaining antennas repeat these symbols achieving higher probability of successful decoding. For example, in a $4x4$ MIMO system, with classic SM, 4 symbols would be transmitted per time slot. In our system $r = 2$ symbols per time slot are transmitted in order not only to double the maximum throughput but also to provide a more robust communication by increasing the probability of successful decoding by a factor of 2. So the DMT tradeoff for this $(vSP4)$ scheme is (2,2), where the diversity gain is $d = 2$. In our system, in order two symbols x_1,x_2 to be transmitted, each odd numbered antenna transmits the x_1 symbol and all the even numbered antennas transmit the x_2 symbol. So the received signals, for our 4x4 MIMO enchanced version of SM are:

$$y_j = \sum_{i=1}^{2} (h_{ij} x_i) + h_{3j} x_1 + h_{4j} x_2 + w_j, j = 1,...,4 \tag{9}$$

The DMT tradeoff for this 4x4 MIMO SM variant $(vSP4)$ is $(2,2)$ while the DMT tradeoff for the 4x4 classic SM scheme is $(4,0)$. The comparison of the diversity gains and multiplexing gains for the 4x4 MIMO Alamouti and SM schemes is:

$$Diversity_{(vSP4)} = 2 * Diversity_{(Alamouti)} \tag{10}$$

$$Multiplex_{(SM)} = 2 * Multiplex_{(vSP4)} = 4 * Multiplex_{Alamouti} \tag{11}$$

From the above equations, it is obvious that using the $vSP4$ scheme we increase the diversity gain by a factor of 2 and decrease the multiplexing gain by a factor of two too, comparing with the classic 4x4 SM MIMO scheme. The calculations of the capacity of the proposed communication scheme lead to:

$$C_{vSP4} = \sum_{i=1}^{\min(n_T/n_A, n_R/n_A)} \log(1 + \frac{P_T \lambda_i^2}{\sigma_n^2 n_T}) \tag{12}$$

In the above equation the new 4x4 channel matrix H is used and λ_i^2 are the eigenvalues of the $(H^H H)$ matrix [21]. We also use $(n_R = n_T = 4, n_A = 2)$ and $\min_{(n_T/n_A, n_R/n_A)} = 2$. Comparing the capacities of the schemes: $vSP4$ (C_{vSP4}), 2x2 SM (C_{2x2SM}), 4x4 SM (C_{4x4SM}) and a 2x2 Alamouti $(C_{2x2Alamouti})$ scheme in which 2 symbols per 2 time slots are transmitted, *assuming ideal channel conditions* between Tx and Rx for all the schemes:

$$C_{vSP4} = C_{2x2SM} = \frac{C_{4x4SM}}{2} > C_{2x2Alamouti} \tag{13}$$

Consequently, $vSP4$ is a method that almost doubles the diversity, increases the reliability compared with the classic SM scheme and also decreases the overall throughput of the system.

Practical Considerations: The proposed defense system is based on MIMO signal processing techniques. MIMO enjoys widespread applicability in most wireless systems today. Hence, out proposed system is amenable to a practical real-time implementation and operation without affecting other aspects of the wireless transmission system. Furthermore, there is no need for additional algorithms or processing besides the MIMO receiver processing.

V. Performance Evaluation

Methods compared. In order to evaluate the performance of the proposed defense mechanism $vSP4$, we compare it with the $2x2$ MIMO classic version of SM ($cSP2$) and the $4x4$ MIMO classic version of SM ($cSP4$). We also compare a 2x2 MIMO Alamouti (STBC) technique with a classic SISO system and with a $2x2$ classic SM scheme.

Performance metrics. As performance metrics we used the Throughput vs SNR, the Throughput vs Time (Silence Time), the Throughput vs Distance (Silence Range), the Throughput vs SNR and the PER (Packet Error Rate $= \frac{Packets_{lost}}{Packets_{sent}}$) vs Time. Silence Time is the time duration of the complete disruption of communication due to strong jamming, while Silence Range is the range in meters in which the communication is impossible. It is important to note that in our throughput results we exclude of course packet losses in order to ensure that we measure the actual volume of successfully communicated data per second in the presence of a jammer. In this paper we do not investigate additional algorithms like packet re-transmission (ARQ) or forward error correction (FEC) that can be employed at the PHY or the link layer. These schemes are well-known and well-investigated and they distract from the main idea of the simulation which is the use of MIMO signal processing for enjoying throughput improvements in the presence of a wireless jammer.

A. Simulation Setup

For our experiments, we used the parameters of the real experiments that were conducted in [8]. More specifically, the same road in the outskirts of the city of Aachen as shown in Figure 3 was used. Several other parameters that are illustrated in Table II are also tuned in order to better represent the scenarios of the real experiments conducted in [8]. The side road in which the Jammer (Jn) is located, is also the same. For our *evaluation scenarios* the Rx follows the Tx keeping a constant distance. The first time steps and the last time steps of our simulation can be mapped to the distances about 150m between $Rx-Jn$ and the Jn approaches the pair $Tx-Rx$ at about distance 5m at the middle (70sec) of the simulation, increasing strongly the jamming effect. Also, in V-C subsection *(Experiment 2)* we evaluate the use of a reactive jammer with $T_{detection} = 12\mu s$ and $T_{duration} = 84\mu s$ at the standard of [8].

PARAMETER	**VALUE**
Transmitter Power	17.48 dBm
Jammer Power	16.75 dBm
Packet Generation rate [packets/s]	10
Simulation Symbols Number	5000
Data rates in experiments	6Mbps
Packet Payload	400B

TABLE II: Simulation Parameters

B. MIMO- Defense Mechanism (Experiment1)

To highlight the negative effects that a jammer induces in vehicular communication and how the MIMO techniques effectively suppress these effects, we compare the performance of MIMO techniques for short and long distances between the $Tx-Rx$ pair. Also, Figures 2(c) and 2(d) demonstrate the silence time of communication which is caused by the presence of a jammer in the side road.

As expected, while $Tx-Rx$ distance increases from $20m$ to $100m$, the RF jamming impact also increases dramatically, as seen in Figures 2(c) and 2(d). Also, the improved performance and the benefits of the MIMO system when compared to the SISO system are significant. For short distances, where there is the least impact in communication, the Alamouti technique manages to suppress the silence range of the RF jamming threat from the distance above $10m$ (see Figure 2(a)). As we can also see in Figure 2(c) the silence time of communication is reduced to only a few seconds by using the Alamouti technique. For inter-vehicle distances of $100m$ the silence range is $20m$ which is almost double compared to the silence range for inter-vehicle distances of $20m$. This situation is also graphically represented in Figure 3. Silence range extends considerably for the other two techniques, $35m$ for SISO and $75m$ for SM.

In time domain, communication with the Alamouti technique is affected for a duration of $20s$ for inter-vehicle distance $100m$ (see Figure 2(d)) while for inter-vehicle distance $20m$, the disruption of communication is only about $2s$ (see Figure 2(c)). On the other hand, using SM scheme the communication is affected for about $10s$ for distance $20m$ and the corruption of communication is dramatically increased at $30s$ for distance $100m$.

The first main conclusion from these figures is the stable performance of the Alamouti scheme for all the possible distances $Rx-Jn$, $Tx-Rx$, the elimination of the jamming effect for inter-vehicles distances lower than $20m$ with the presence of a jammer $20m$ away at least from the receiver. Furthermore, besides throughput we are also interested in higher reliability of the system under the presence of malicious jammers. Notably for emergency situations, it is very important the silence range to be very low. For this reason, an interesting result of our simulation study is that SM achieves the best throughput in jammming free areas, but the worst silence range (time) in jamming areas. .

C. Reactive Jammer (Experiment2)

To evaluate the performance of a more intelligent jammer, we implemented a reactive algorithm. The reactive jammer is designed to start transmitting upon sensing energy above a certain threshold. We set the latter to -86 dBm as we empirically determined it to be a good trade-off between jammer sensitivity and false transmission detection rate. If the detected energy exceeds

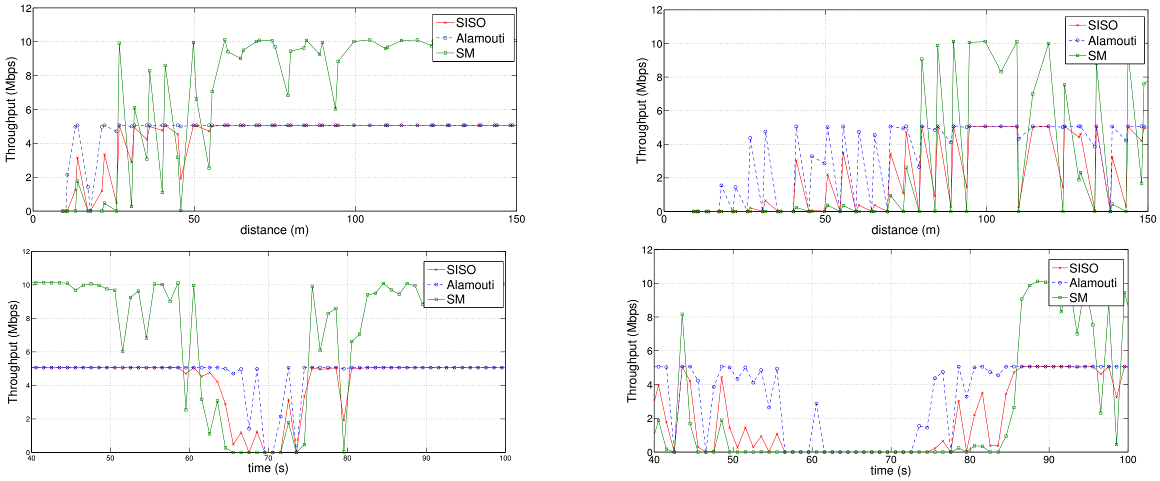

Fig. 2: Experiment 1 results. Throughput of 2x2 MIMO system.

(a) Throughput to $Rx-Jn$ pair distance. $Tx-Rx$ pair distance =20m,

(b) Throughput to $Rx-Jn$ pair distance. $Tx-Rx$ pair distance =100m,

(c) Throughput to Time. $Tx-Rx$ pair distance=20m,

(d) Throughput to Time. $Tx-Rx$ pair distance =100m

Payload data rate= 6Mbps (4-PSK, FEC = 1/2), packet payload = 400B.

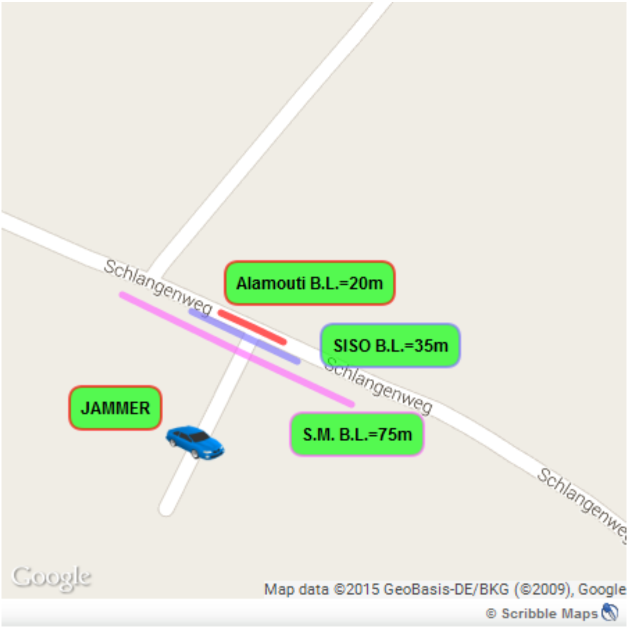

Fig. 3: Experiment 1, graphical representation.

Graphically Representation of Silence range- Blockage line.

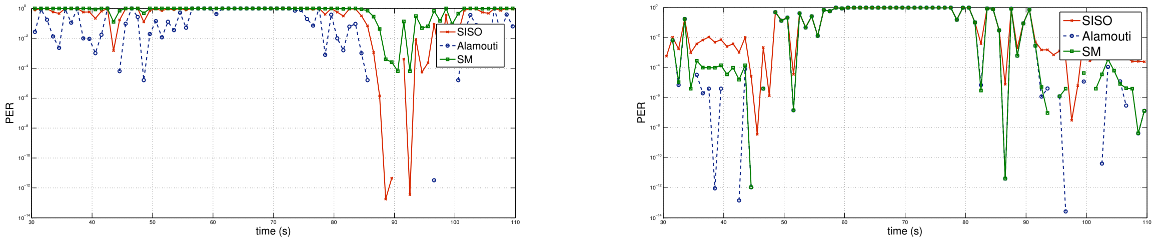

Fig. 4: Experiment 2 results. PER of Continuous jammer and Reactive jammer for 2x2 MIMO schemes of Experiment 1. $Tx-Rx$ pair distance=100m. Payload data rate= 6Mbps (4-PSK, FEC = 1/2), packet payload = 400B.

(a) PER to Time (Continuous Jammer), (b) PER to Time (Reactive Jammer)

the threshold during a certain time span ($T_{detection}$= $12\mu s$), an ongoing 802.11p transmission is assumed by the jammer and starts its transmission for a duration of ($T_{duration}$= $84\mu s$). The reactive jammer is designed in order to achieve jamming the header of 802.11p frame from Tx to the Rx.

From Figures 4(a) and 4(b), we can see that the PER of the transmission between Tx-Rx with the presence of a continuous jammer in Figure 4(a) and a in Figure 4(b) with the presence of an reactive jammer. For time slots that the distance between Jn-Rx is quite large the performance of reactive jammer is lower than that of the continuous jammer, mainly because the reactive jammer is not sensing the ongoing transmissions at these time slots. At the small distances Jn-Rx it is obvious that the silence time for the MIMO Alamouti and SM is about the same for the continuous and the reactive jammer. Only for the SISO scheme the PER is smaller for the continuous jammer than the PER of the reactive jammer at about 90 sec. This behavior is justified because our MIMO defense scheme does not use a detection phase of the jammer but uses the multiple antennas continuously in order to suppress the jamming effects. The main characteristic of reactive jammer is to avoid detection from the Rx's CCA mechanism of the 802.11p protocol PHY. Since we observed the same behavior between the reactive and the continuous jammer for our MIMO schemes, we will use the continuous jammer for the rest of our experiments. So we can assume that our MIMO defense scheme suppress all types of jamming. The ineffectiveness of reactive jammer compared with a continous jammer can also be seen for a platoon of vehicles at the Figure 19(a),(b) of [8].

D. SM Variants (Experiment3)

The results of Experiment1 allow us to introduce the last set of experiments, and more specifically the use of a $4x4$ MIMO system. Alamouti's performance, as described above, can almost eliminate the silence range for inter-vehicle distances about $20m$ for a $2x2$ MIMO system. On the other hand, the SM scheme achieves significant throughput in jamming-free areas but higher silence range when used in jamming areas for the majority of the simulations. So these final simulations focus on trying to identify the optimal trade off between diversity and spatial multiplexing gain by comparing SM variants, that were described in IV-B, IV-C subsections. In Figures 5(a) - 5(b), the schemes are:

- $2x2$ MIMO SM ($cSP2$), transmitting 2 symbols/timeslot.
- $4x4$ MIMO SM ($cSP4$), transmitting 4 symbols/timeslot.
- $4x4$ MIMO SM variant ($vSP4$), transmitting 2 symbols/ timeslot.

The first conclusion based on the simulation that we conducted is that the SNR gain of $vSP4$ method is significant compared to the other two. Figure 5(a) demonstrates how $cSP4$ provides better throughput compared to $cSP2$ and $vSP4$, only for large SNR values.

On the other hand, using $vSP4$ the throughput is almost doubled compared to $cSP4$, at the middle SNR values in Figure 5(a). In Figure 5(b), the throughput of the SM variants versus time is presented. It can be seen that as the distance from a jammer remains relatively short, the optimal scheme is $vSP4$ achieving a throughput of $10Mbps$. When the jammer is removed from the effective zone of communication, the best solution is the $cSP4$ that achieves the best throughput for $20Mbps$ when compared to the other schemes.

The most interesting result in these figures is that $vSP4$ doubles the throughput and significantly reduces the RF jamming silence range. Our goal is to illustrate the need for more complex and advanced, full adaptive algorithms that will select dynamically the optimal version of SM depending on the operating regime, e.x. diversity or throughput.

Concluding the results from this subsection figures, it is obvious that as the distance from a jammer remains relatively short, the best solution that combines better throughput and diversity is $vSP4$, presenting a stable throughput value at about $10Mbps$. $vSP4$ also reduces the silence time at about 12s, while for $cSP4$ and $cSP2$ the silence time is 30s and 20s respectively. So, while a higher order SM system is used, the throughput is increased with good channel conditions but the negative implication is that the silence range is also increased in the presence of RF jamming.

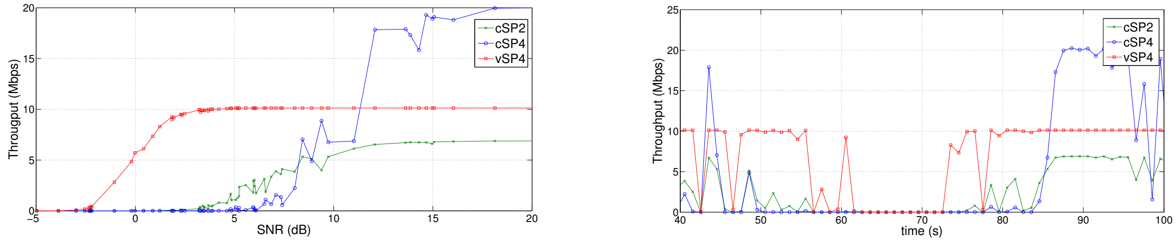

Fig. 5: Experiment 3 results. Comparison of SM variants and higher order MIMO. $Tx-Rx$ pair distance=100m. Payload data rate= 6Mbps (4PSK, FEC = 1/2), packet payload = 400B.
(a) Throughput to SNR, (b) Throughput to Time

These results confirm the fact that the classic version of SM is not suitable for suppressing the jamming effects.

VI. CONCLUSIONS

In this paper we proposed the use of MIMO to increase the throughput and reliability in VANETs that experience RF jamming attacks. The first novelty of this paper is the introduction of a new simulation framework that combines three different well-known simulators. The first one is the traffic simulator SUMO [26], the second is the network simulator OMNET++ [27] and the third is the GEMV [23], a Geometry-based propagation model that is integrated in the VEINS simulator [22].

The second contribution is as set of extensive simulations that represent real conditions. We showed that the Alamouti scheme retains a stable performance despite the inter-vehicle distance $Tx-Rx$ and the presence of a malicious jammer in very close distances. Moreover we showed that it can eliminate completely the silence range for small inter-vehicle distances. Last, by conducting experiments using a reactive jammer in addition to a continuous, we showed that the Alamouti scheme can suppress the jamming effect regardless the type of jamming signal and that SM achieves the best throughput in jammming free areas, but the worst silence range (time) in jamming areas .

The third contribution of this paper is a new technique that is a combination of the SM and the Alamouti scheme, namely $vSP4$, that achieves not only the throughput to be sustainable, but also double the reliability from the classic SM decreasing the silence time at the same time, under the presence of a malicious jammer.

Our future work will focus on designing a dynamic, fully adaptive scheme that will select the optimal MIMO transmission mode depending on the total interference level. Also we plan to use our novel simulation model [28] which is capable to handle secured messages in order to simulate more realistic situations.

References

[1] H. Hartenstein and K. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *Communications Magazine, IEEE*, vol. 46, no. 6, pp. 164–171, 2008.

[2] M. L. Sichitiu and M. Kihl, "Inter-vehicle communication systems: a survey," *Communications Surveys & Tutorials, IEEE*, vol. 10, no. 2, pp. 88–105, 2008.

[3] Y. L. Morgan, "Notes on dsrc & wave standards suite: Its architecture, design, and characteristics," *Communications Surveys & Tutorials, IEEE*, vol. 12, no. 4, pp. 504–518, 2010.

[4] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *J. Netw. Comput. Appl.*, vol. 37, pp. 380–392, January 2014.

[5] S. Mitra and A. Mondal, "Secure inter-vehicle communication: A need for evolution of vanet towards the internet of vehicles," in *Connectivity Frameworks for Smart Devices*. Springer, 2016, pp. 63–96.

[6] L. A. Maglaras, "A novel distributed intrusion detection system for vehicular ad hoc networks," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 6, no. 4, 2015.

[7] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (vanets): status, results, and challenges," *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2012.

[8] O. Punal, C. Pereira, A. Aguiar, and J. Gross, "Experimental characterization and modeling of rf jamming attacks on vanets," *Vehicular Technology, IEEE Transactions on*, vol. 64, no. 2, pp. 524–540, Feb 2015.

[9] C. Pereira and A. Aguiar, "A realistic rf jamming model for vehicular networks: Design and validation," in *Personal Indoor and Mobile Radio Communications (PIMRC), 2013 IEEE 24th International Symposium on*. IEEE, 2013, pp. 1868–1872.

[10] A. M. Malla and R. K. Sahu, "Security attacks with an effective solution for dos attacks in vanet," *International Journal of Computer Applications*, vol. 66, no. 22, pp. 45–49, 2013.

[11] K. Verma, H. Hasbullah, and A. Kumar, "Prevention of dos attacks in vanet," *Wireless personal communications*, vol. 73, no. 1, pp. 95–126, 2013.

[12] X. Liu, Z. Fang, and L. Shi, "Securing vehicular ad hoc networks," in *Pervasive Computing and Applications, 2007. ICPCA 2007. 2nd International Conference on*. IEEE, 2007, pp. 424–429.

[13] A. El-Keyi, T. ElBatt, F. Bai, and C. Saraydar, "Mimo vanets: Research challenges and opportunities," in *Computing, Networking and Communications (ICNC), 2012 International Conference on*. IEEE, 2012, pp. 670–676.

[14] A. Theodorakopoulos, P. Papaioannou, T. Abbas, and F. Tufvesson, "A geometry based stochastic model for mimo v2v channel simulation in cross-junction scenario," in *ITS Telecommunications (ITST), 2013 13th International Conference on*. IEEE, 2013, pp. 290–295.

[15] W. Viriyasitavat, M. Boban, H.-M. Tsai, and A. Vasilakos, "Vehicular communications: Survey and challenges of channel and propagation models," *Vehicular Technology Magazine, IEEE*, vol. 10, no. 2, pp. 55–66, 2015.

[16] A. B. Al-Khalil, A. Al-Sherbaz, and S. Turner, "Enhancing the physical layer in v2v communication using ofdm–mimo techniques," *architecture*, vol. 1, p. 10, 2013.

[17] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. T. Hou, "Mimo-based jamming resilient communication in wireless networks," in *INFOCOM, 2014 Proceedings IEEE*. IEEE, 2014, pp. 2697–2706.

[18] H. Yantian, L. Ming, Y. Xu, H. Thomas, and L. Wenjing, "Cooperative cross-technology interference mitigation for heterogeneous multi-hop networks," in *INFOCOM, 2014 Proceedings IEEE*. IEEE, 2014, pp. 880–888.

[19] S. Gollakota, F. Adib, D. Katabi, and S. Seshan, "Clearing the rf smog: making 802.11 n robust to cross-technology interference," *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4, pp. 170–181, 2011.

[20] H. S. L. Meng Chuan Mah and A. W. C. Tan, "Improved channel estimation for mimo interference cancellation," *Communications Letters, IEEE*, vol. 19, no. 8, pp. 1355 – 1357, 2015.

[21] D. Tse and P. Viswanath, *Pervasive Computing and Applications*. Cambridge University Press, 2005.

[22] C. Sommer, R. German, and F. Dressler, "Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis," *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, pp. 3–15, January 2011.

[23] M. Boban, J. Barros, and O. Tonguz, "Geometry-based vehicle-to-vehicle channel modeling for large-scale simulation," *Vehicular Technology, IEEE Transactions on*, vol. 63, no. 9, pp. 4146–4164, 2014.

[24] S. Alamouti, "A simple transmit diversity technique for wireless communications," *Journal on Selected Areas in Communications*, vol. 16, no. 8, p. 14511458, 1998.

[25] A. Lozano and N. Jindal, "Transmit diversity vs. spatial multiplexing in modern mimo systems," vol. 9. IEEE, 2010, pp. 186 – 197.

[26] D. Krajzewicz, J. Erdmann, M. Behrisch, and L. Bieker, "Recent development and applications of SUMO - Simulation of Urban MObility," *International Journal On Advances in Systems and Measurements*, vol. 5, no. 3&4, pp. 128–138, December 2012.

[27] A. Varga, "The omnet++ descrete event simulation system," in *Proceedings of the European Simulation Multiconference(ESM 2001)*, 2001.

[28] R. Riebl, M. Monz, S. Varga, L. A. Maglaras, H. Janicke, A. H. Al-Bayatti, and C. Facchi, "Improved security performance for vanet simulations," in *4th IFAC Symposium on Telematics Applications, (TA 2016)*. IFAC, 2016.