Hindawi Publishing Corporation
Mobile Information Systems
Volume 2016, Article ID 8141204, 9 pages
http://dx.doi.org/10.1155/2016/8141204

Research Article

MIMO Techniques for Jamming Threat Suppression in Vehicular Networks

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

[1] *Department of Electrical & Computer Engineering, University of Thessaly, Volos, Greece*
[2] *School of Computer Science and Informatics, De Montfort University, Leicester, UK*

Correspondence should be addressed to Leandros A. Maglaras; leandros.maglaras@dmu.ac.uk

Received 15 April 2016; Accepted 9 October 2016

Academic Editor: Candelaria Hernández-Goya

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 proven 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, which achieves not only high throughput but also a stable diversity gain upon the interference of a malicious jammer.

1. 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.

VANETs can be considered as mobile ad hoc networks which are utilized to enhance traffic safety and provide comfort applications to drivers. The unique features of VANETs include fast-moving vehicles that follow predetermined paths (i.e., roads) though having 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, for example, 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. Particularly 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 proven 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.

2. 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, for example, communication range and throughput. Previous work mainly focuses on explaining the benefits of using MIMO in VANETs [13] and examining 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 antijamming MIMO-based techniques were introduced. Authors in [17] present a MIMO-based antijamming technique that uses prerotation 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, which is provided from the probing of the channel. In VANETs, the frequently changing channel would generate a large number of probes, overloading the channel. The 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, which combines the Alamouti scheme 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 cSP4 scheme in the presence of a malicious jammer. Another contribution of this paper is a new framework for VANET simulations which combines three known simulators for obtaining more realistic results.

3. System Model

3.1. 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 versus 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 which takes into account the "quality" of the links taking into account the physical obstacles (e.g., building and cars) compared to simple log-distance model which 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.

3.2. Channel Model and PHY Modulation. For simulations, the 802.11p MAC and PHY parameters at 5.9 GHz (10 MHz) are used. Please refer to Table 2 for details of specific parameter values. Also, Rayleigh fading channels with Additive

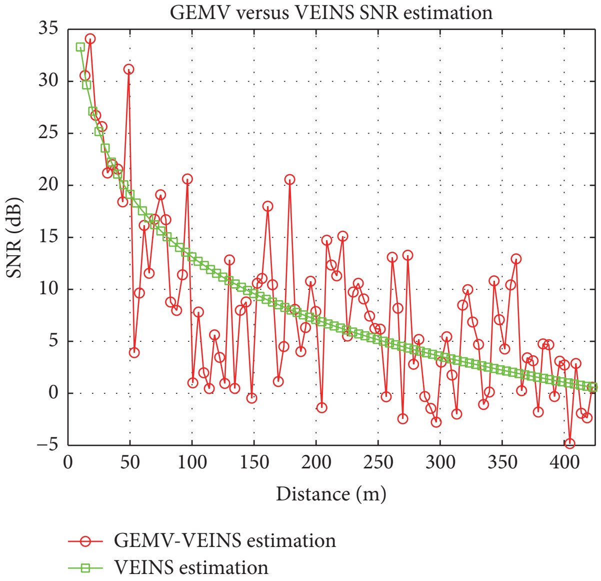


Figure 1: GEMV-VEINS SNR versus distance estimation.

White Gaussian Noise (AWGN) ($\widetilde{w}$), being stable during the transmission of 10 symbols, are 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 3 Mbps for packet header and 6 Mbps for packet payload which are currently supported by VEINS project. A modulation and coding scheme (MCS) with m 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.

3.3. MIMO Model. For all the MIMO schemes, we assume that K is the number of symbols which 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 and 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 $h_{\mathrm{Tx,Rx}}$ is the channel between the transmitter (Tx) and receiver (Rx). The systems we test are the following: a 2×2 Alamouti scheme in Section 4.1, a 2×2 SM in Section 4.2, and an enhanced 4 × 4 combination of Alamouti scheme and SM scheme in Section 4.3.

4. The Proposed Defense System

4.1. 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 1. We use a 2 × 2 MIMO Alamouti scheme in which ($K = 2$) a number of symbols are transmitted in the duration of T time slots ($T = 2$).

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 overall system reliability. The received signal can be written as

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

In the above equation, y_{11} and y_{12} denote the received symbols at antenna element number 1 and number 2 at the first time slot $T1$ (Table 1) and similarly y_{21}^{*} and y_{22}^{*} represent the received symbols at antenna element number 1 and number 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 2 × 2 MIMO Alamouti scheme is $r = K/T = 1$ symbols/time slots and the diversity gain is $d = 1$. So the DMT 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 have

$$H = \begin{bmatrix} h_{11} & h_{21} \\ h_{21}^{*} & -h_{11}^{*} \\ h_{12} & h_{22} \\ h_{22}^{*} & -h_{12}^{*} \end{bmatrix} \quad (2)$$

and the inverted matrix product is

$$\left(H^{H}H\right)^{-1} = \begin{bmatrix} \dfrac{1}{\left|h_{11}\right|^2 + \left|h_{21}\right|^2 + \left|h_{12}\right|^2 + \left|h_{22}\right|^2} & 0 \\ 0 & \dfrac{1}{\left|h_{11}\right|^2 + \left|h_{21}\right|^2 + \left|h_{12}\right|^2 + \left|h_{22}\right|^2} \end{bmatrix}, \quad (3)$$

Table 1: Alamouti scheme.

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

Table 2: Simulation parameters.

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	6 Mbps
Packet payload	400 B

the proposed signal $\tilde{r}$ is

$$\tilde{r} = H^H \left(H^H H\right)^{-1} \overrightarrow{\tilde{y}} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} + \vec{w}. \tag{4}$$

Because MRC decoding is used, as the number of received 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

$$C_{\text{Alamouti}} = \frac{K}{T} \log \left(\det \left(I + \frac{P_T}{r \sigma_n^2 n_T} \left(H^H H\right) \right) \right). \tag{5}$$

From the above equation, we can conclude that the capacity of the Alamouti scheme depends 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 2×2 MIMO Alamouti scheme, the capacity is $C_{\text{Alamouti}} \geq C_{\text{SISO}}$, where SISO is a Single (antenna) Input Single (antenna) Output scheme.

4.2. 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 very high BER. The MIMO channel with SM is

$$\vec{y} = H\vec{x} + \vec{w}. \tag{6}$$

By applying Least Squares Equalization to the channel matrix H, we have to multiply with the pseudoinverse matrix:

$$H^{\dagger} = \left(H^H H\right)^{-1} H^H. \tag{7}$$

The sufficient statistic that is used for detection is then

$$\vec{r} = \left(H^H H\right)^{-1} H^H \vec{y} = x + \left(H^H H\right)^{-1} H^H \vec{w}, \tag{8}$$

which is also known as the zero-forcing method.

For a 2×2 MIMO SM scheme, the received signals which are reached at antenna 1 and antenna 2 can be written as

$$y_j = \sum_{i=1}^{2} h_{ij} x_i + w_j, \quad j = 1, 2. \tag{9}$$

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 is 2, while the diversity gain is 0 $(2, 0)$.

Calculating the capacity of SM scheme, we have

$$\begin{aligned} C_{\text{SM}} &= \log \left(\det \left(I + \frac{P_T}{\sigma_n^2 n_T} \left(H^H H\right) \right) \right) \\ &= \sum_{i=1}^{\min(n_R, n_T)} \log \left(1 + \frac{P_T \lambda_i^2}{\sigma_n^2 n_T} \right). \end{aligned} \tag{10}$$

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

4.3. 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 4×4 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 for this (vSP4) scheme is $(2, 2)$, where the diversity gain is $d = 2$. In our system, in order for two symbols (x_1, x_2) to be transmitted, each odd numbered antenna transmits x_1 symbol and all the even numbered antennas transmit x_2 symbol. So the received signals, for our 4×4 MIMO enhanced version of SM, are

$$y_j = \sum_{i=1}^{2} \left(h_{ij} x_i\right) + h_{3j} x_1 + h_{4j} x_2 + w_j, \quad j = 1, \ldots, 4. \tag{11}$$

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

$$\begin{aligned} \text{Diversity}_{(\text{vSP4})} &= 2 * \text{Diversity}_{(\text{Alamouti})}, \\ \text{Multiplex}_{(\text{SM})} &= 2 * \text{Multiplex}_{(\text{vSP4})} \\ &= 4 * \text{Multiplex}_{\text{Alamouti}}. \end{aligned} \tag{12}$$

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, compared with the classic 4 × 4 SM MIMO scheme. The calculations of the capacity of the proposed communication scheme lead to

$$C_{\mathrm{vSP4}} = \sum_{i=1}^{\min(n_T/n_A, n_R/n_A)} \log\left(1 + \frac{P_T \lambda_i^2}{\sigma_n^2 n_T}\right). \quad (13)$$

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

$$C_{\mathrm{vSP4}} = C_{2\times 2\mathrm{SM}} = \frac{C_{4\times 4\mathrm{SM}}}{2} > C_{2\times 2\mathrm{Alamouti}}. \quad (14)$$

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, our proposed system is amenable to 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.

5. Performance Evaluation

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

Performance Metrics. As performance metrics we used the throughput versus SNR, the throughput versus time (silence time), the throughput versus distance (silence range), the throughput versus SNR, and the PER (Packet Error Rate = $\mathrm{Packets}_{\mathrm{lost}}/\mathrm{Packets}_{\mathrm{sent}}$) versus 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 retransmission (ARQ) or forward error correction (FEC) which can be employed at the PHY or the link layer. These schemes are well known and well investigated and they are distracted 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.

5.1. 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 2 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, Rx follows Tx, keeping a constant distance. The first time steps and the last time steps of our simulation can be mapped to the distances about 150 m between Rx and Jn and Jn approaches the pair Tx-Rx at about distance of 5 m at the middle (70 sec) of the simulation, increasing strongly the jamming effect. Also, in Section 5.3 (Experiment 2), we evaluate the use of a reactive jammer with $T_{\mathrm{detection}} = 12\,\mu\mathrm{s}$ and $T_{\mathrm{duration}} = 84\,\mu\mathrm{s}$ at the standard of [8].

5.2. MIMO Defense Mechanism (Experiment 1). To highlight the negative effects that a jammer induces in vehicular communication and how the MIMO techniques effectively suppress these effects, we compare the performances of MIMO techniques for short and long distances within 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 20 m to 100 m, 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 10 m (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 intervehicle distances of 100 m, the silence range is 20 m, which is almost double compared to the silence range for intervehicle distances of 20 m. This situation is also graphically represented in Figure 3. Silence range extends considerably for the other two techniques, 35 m for SISO and 75 m for SM.

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

The first main conclusion from these figures is the stable performance of the Alamouti scheme for all the possible distances of Rx-Jn and Tx-Rx and the elimination of the jamming effect for intervehicle distances lower than 20 m with the presence of a jammer 20 m 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 for the silence range to be very low. For this reason, an interesting result of our simulation study is

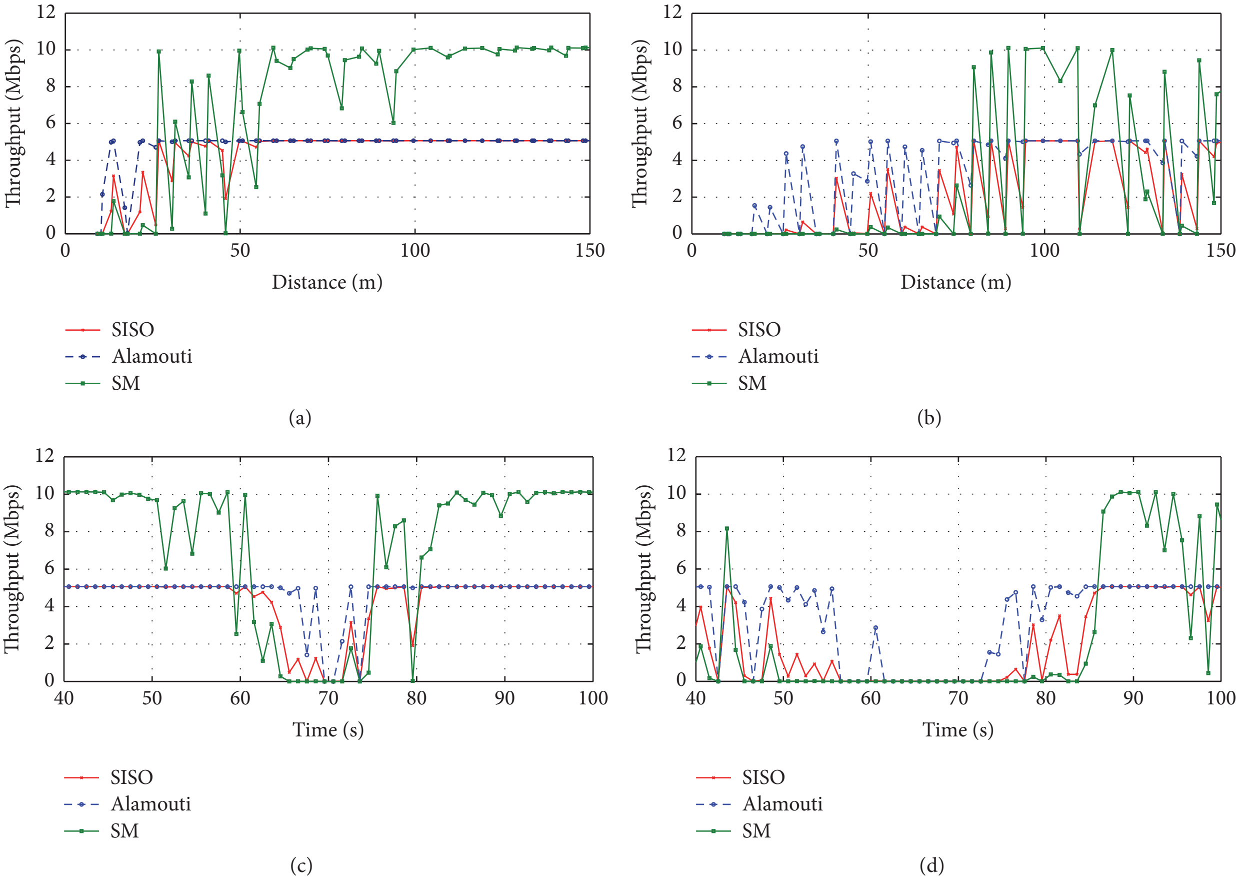


Figure 2: Experiment 1, results. Throughput of 2 × 2 MIMO system. (a) Throughput to Rx-Jn pair distance. Tx-Rx pair distance = 20 m. (b) Throughput to Rx-Jn pair distance. Tx-Rx pair distance = 100 m. (c) Throughput to time. Tx-Rx pair distance = 20 m. (d) Throughput to time. Tx-Rx pair distance = 100 m. Payload data rate = 6 Mbps (4-PSK, FEC = 1/2); packet payload = 400 B.

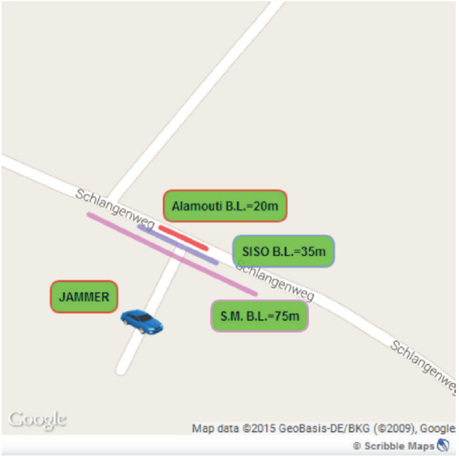
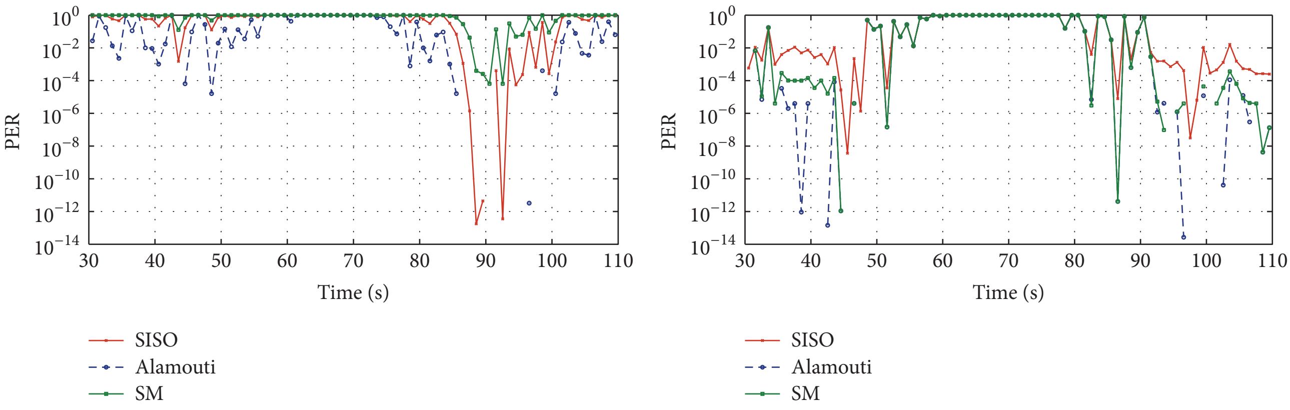


Figure 3: Experiment 1, graphical representation. Graphical representation of silence range, blockage line.

that SM achieves the best throughput in jamming-free areas but the worst silence range (time) in areas where jamming exists.

5.3. Reactive Jammer (Experiment 2). 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 tradeoff between jammer sensitivity and false transmission detection rate. If the detected energy exceeds the threshold during a certain time span ($T_{\text{detection}} = 12\,\mu$s), an ongoing 802.11p transmission is assumed by the jammer and starts its transmission for a duration of $T_{\text{duration}} = 84\,\mu$s. The reactive jammer is designed in order to achieve jamming the header of 802.11p frame from Tx to Rx.

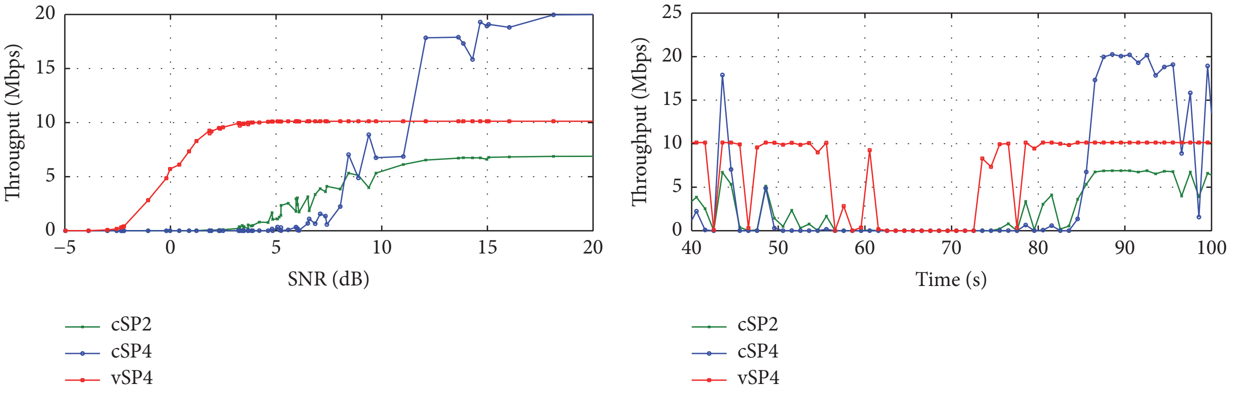
From Figures 4(a) and 4(b), we can see the PER of the transmission between Tx and Rx with the presence of a continuous jammer in Figure 4(a) and a reactive jammer in Figure 4(b) with the presence of an reactive jammer. For time slots where the distance between Jn and Rx is quite large, the performance 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. The PER of the continuous jammer is smaller than the PER



(a)

(b)

FIGURE 4: Experiment 2, results. PER of continuous jammer and reactive jammer for 2 × 2 MIMO schemes of Experiment 1. Tx-Rx pair distance = 100 m. Payload data rate = 6 Mbps (4-PSK, FEC = 1/2); packet payload = 400 B. (a) PER to time (continuous jammer); (b) PER to time (reactive jammer).



(a)

(b)

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

of the reactive jammer only for the SISO scheme 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 jammer 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 suppresses all types of jamming. The ineffectiveness of reactive jammer compared with a continuous jammer can also be seen for a platoon of vehicles at Figures 19(a) and 19(b) of [8].

5.4. SM Variants (Experiment 3). The results of Experiment 1 allow us to introduce the last set of experiments and more specifically the use of a 4 × 4 MIMO system. Alamouti's performance, as described above, can almost eliminate the silence range for intervehicle distances about 20 m for a 2 × 2 MIMO system. On the other hand, the SM scheme achieves significant throughput in jamming-free areas but higher silence range when used in areas where jamming exists for the majority of the simulations. So these final simulations focus on trying to identify the optimal tradeoff between diversity and spatial multiplexing gain by comparing SM variants, which were described in Sections 4.2 and 4.3. In Figures 5(a) and 5(b), the schemes are the following:

(i) 2 × 2 MIMO SM (cSP2), transmitting 2 symbols/timeslot

(ii) 4 × 4 MIMO SM (cSP4), transmitting 4 symbols/timeslot

(iii) 4 × 4 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 10 Mbps. When the jammer is removed from the effective zone of communication, the best solution is the cSP4 which achieves the best throughput for 20 Mbps 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, advanced, and full adaptive algorithms that will select dynamically the optimal version of SM depending on the operating regime, for example, diversity or throughput.

Summarizing the results of Experiment 3, 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 10 Mbps. vSP4 also reduces the silence time at about 12 s, while, for cSP4 and cSP2, the silence time is 30 s and 20 s, 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. These results confirm the fact that the classic version of SM is not suitable for suppressing the jamming effects.

6. Conclusions

In this paper, we proposed the use of MIMO to increase the throughput and reliability in VANETs which 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 a set of extensive simulations that represent real conditions. We showed that the Alamouti scheme retains a stable performance despite the intervehicle 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 intervehicle distances. Last, by conducting experiments using a reactive jammer in addition to a continuous jammer, we showed that the Alamouti scheme can suppress the jamming effect regardless of the type of jamming signal and that SM achieves the best throughput in jamming-free areas but the worst silence range (time) in areas where jamming exists.

The third contribution of this paper is a new technique which is a combination of the SM scheme and the Alamouti scheme, namely, vSP4, which not only achieves the throughput to be sustainable but also doubles the reliability from the classic SM, decreasing the silence time at the same time, with 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 able to handle secured messages in order to simulate more realistic situations.

Competing Interests

The authors declare that they have no competing interests.

References

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

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

[3] Y. L. Morgan, "Notes on DSRC & WAVE standards suite: its architecture, design, and characteristics," *IEEE Communications Surveys and Tutorials*, 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," *Journal of Network and Computer Applications*, vol. 37, no. 1, pp. 380–392, 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*, pp. 63–96, Springer, Berlin, Germany, 2016.

[6] L. A. Maglaras, "A novel distributed intrusion detection system for vehicular ad hoc networks," *International Journal of Advanced Computer Science and Applications*, 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] Ó. Puñal, C. Pereira, A. Aguiar, and J. Gross, "Experimental characterization and modeling of RF jamming attacks on VANETs," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 2, pp. 524–540, 2015.

[9] C. Pereira and A. Aguiar, "A realistic rf jamming model for vehicular networks: design and validation," in *Proceedings of the IEEE 24th International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC '13)*, pp. 1868–1872, London, UK, September 2013.

[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 *Proceedings of the 2nd International Conference on Pervasive Computing and Applications (ICPCA '07)*, pp. 424–429, IEEE, Birmingham, UK, July 2007.

[13] A. El-Keyi, T. ElBatt, F. Bai, and C. Saraydar, "MIMO VANETs: research challenges and opportunities," in *Proceedings of the 2012 International Conference on Computing, Networking and Communications (ICNC '12)*, pp. 670–676, IEEE, Kauai, Hawaii, USA, February 2012.

[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 *Proceedings of the 13th International Conference on ITS Telecommunications (ITST ’13)*, pp. 290–295, Tampere, Finland, November 2013.

[15] W. Viriyasitavat, M. Boban, H.-M. Tsai, and A. Vasilakos, “Vehicular communications: survey and challenges of channel and propagation models,” *IEEE Vehicular Technology Magazine*, 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, article 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 *Proceedings of the 33rd IEEE Conference on Computer Communications (IEEE INFOCOM ’14)*, pp. 2697–2706, Toronto, Canada, May 2014.

[18] Y. Hou, M. Li, X. Yuan, Y. T. Hou, and W. Lou, “Cooperative cross-technology interference mitigation for heterogeneous multi-hop networks,” in *Proceedings of the 33rd IEEE Conference on Computer Communications (IEEE INFOCOM ’14)*, pp. 880–888, IEEE, Toronto, Canada, May 2014.

[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] M. C. Mah, H. S. Lim, and A. W. C. Tan, “Improved channel estimation for mimo interference cancellation,” *IEEE Communications Letters*, vol. 19, no. 8, pp. 1355–1357, 2015.

[21] D. Tse and P. Viswanath, *Pervasive Computing and Applications*, Cambridge University Press, Cambridge, UK, 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, 2011.

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

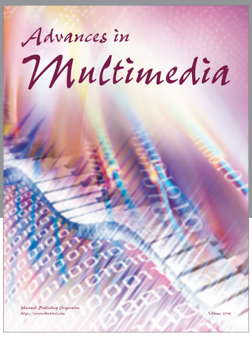
[24] S. M. Alamouti, “A simple transmit diversity technique for wireless communications,” *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 8, pp. 1451–1458, 1998.

[25] A. Lozano and N. Jindal, “Transmit diversity vs. spatial multiplexing in modern MIMO systems,” *IEEE Transactions on Wireless Communications*, vol. 9, no. 1, pp. 186–197, 2010.

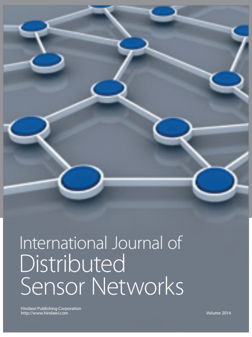
[26] D. Krajzewicz, J. Erdmann, M. Behrisch, and L. Bieker, “Recent development and applications of SUMO—simulation of urban mobility,” *International Journal on Advances in Systems and Measurements*, vol. 5, no. 3-4, pp. 128–138, 2012.

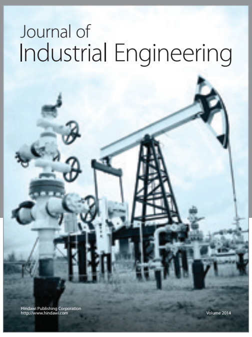
[27] A. Varga, “The omnet++ descrete event simulation system,” in *Proceedings of the European Simulation Multiconference (ESM ’01)*, Prague, Czech Republic, June 2001.

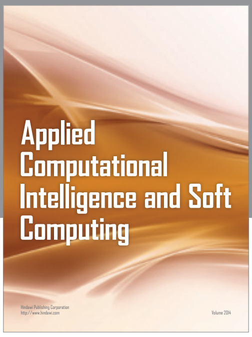
[28] R. Riebl, M. Monz, S. Varga et al., “Improved security performance for vanet simulations,” in *Proceedings of the 4th IFAC Symposium on Telematics Applications (TA ’16)*, Porto Alegre, Brazil, 2016.

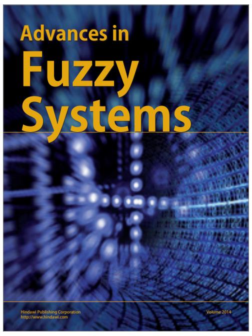

Advances in
Multimedia

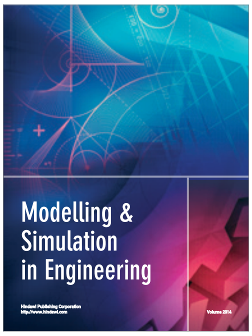
The Scientific
World Journal

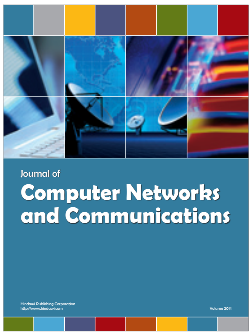

International Journal of
Distributed
Sensor Networks

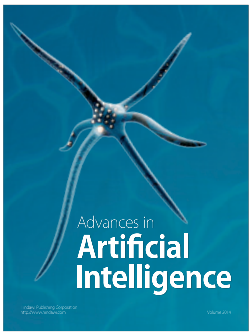

Journal of
Industrial Engineering

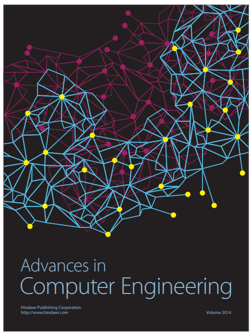

Applied
Computational
Intelligence and Soft
Computing


Advances in
Fuzzy
Systems

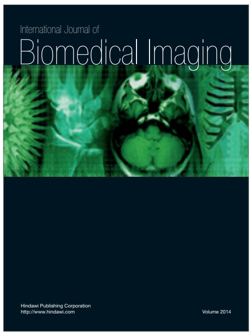

Modelling &
Simulation
in Engineering

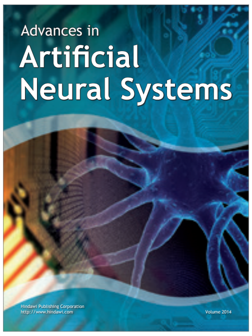

Journal of
Computer Networks
and Communications

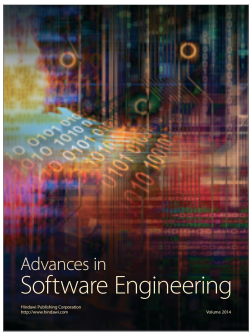

Advances in
Artificial
Intelligence


Advances in
Computer Engineering

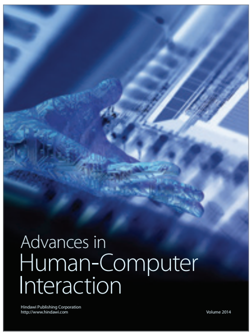
International Journal of
Computer Games
Technology

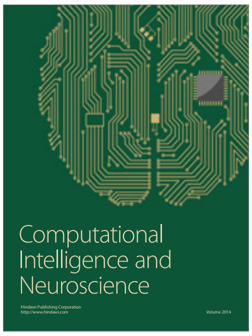

International Journal of
Biomedical Imaging


Advances in
Artificial
Neural Systems


Advances in
Software Engineering

Journal of
Robotics


Advances in
Human-Computer
Interaction


Computational
Intelligence and
Neuroscience

International Journal of
Reconfigurable
Computing

Journal of
Electrical and Computer
Engineering