IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 23, 2020, accepted January 10, 2021, date of publication January 18, 2021, date of current version January 26, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3052464

Saturation Throughput Analysis of Steganography in the IEEE 802.11p Protocol in the Presence of Non-Ideal Transmission Channel

AKRAM A. ALMOHAMMEDI, (Graduate Student Member, IEEE), AND VLADIMIR SHEPELEV
Automobile Transportation Department, South Ural State University, 454080 Chelyabinsk, Russia
Corresponding author: Akram A. Almohammedi (akrama2810@gmail.com)

ABSTRACT Vehicular network is a communication technology designed to provide comfort and improve life safety and driving efficiency on the road. In vehicular network, trustworthy communication is very important as fake applications may lead to disastrous road accidents. Several information hiding methods are used to enable vehicles to communicate secretly or to covertly report a misbehaving vehicle. The work in this paper focuses on a performance analysis based on 2-D Markov chain model for the system throughput of steganographic scheme in relation to the IEEE 802.11p standard. This model studies wireless padding (WiPad) that is used to hide data into the padding of packets at the physical layer of wireless local area networks (WLANs). The analytical study is under non-saturated conditions with non-ideal transmission channel. The study also considers the rate of packet arrival with the first order of buffer memory, back-off timer freezing, back-off phases, and short retry limit to satisfy the IEEE 802.11p specifications. It emphasizes that taking these factors into account are significant in modelling the system throughput of the steganographic channel. These factors typically provide a precise channel access estimation, yield more accurate findings of system throughput, use the channel efficiently, prevent overestimation of saturation throughput, and ensure that no packet is served indefinitely. The model is validated by comparing the numerical and simulation results under different network parameters. Analytical and simulation results stated that the values of the system throughput of the steganographic channel based on data and control frames are low as the vehicles number n, traffic arrival rate λ, packet size, and the value of Bit Error Rate (BER) increase.

INDEX TERMS Vehicular network, IEEE 802.11p, steganographic channel, non-ideal transmission channel, BER.

I. INTRODUCTION

Vehicular network is a communication technology that allows vehicles to exchange information wirelessly. IEEE 802.11p is a protocol developed to enable communications on vehicular network at Physical Layer (PHY) and Lower Medium Access Control Layer (MAC). IEEE 802.11p's PHY was inherited from IEEE 802.11a PHY on the basis of Orthogonal Frequency Division Multiplex (OFDM) technology with some modifications to make it ideal for high-speed vehicular network. Communications in vehicular network can be either among vehicles (V2V), Vehicle-to-Infrastructure (V2I), or hybrid communications. Dedicated Short Range Communication (DSRC) under the 5.9 GHz band is the standard that facilitates the communication over vehicular network [1], [2]. Due to the revolution in wireless communication technology and the heterogeneous network, vehicular network has become one of the Internet of Things (IoT) applications called Internet of Vehicle (IoV) [3]. In order for a vehicle to be a part of the IoV, it requires a device called on-board unit (OBU). The device enables a vehicle to exchange messages with nearby vehicles or infrastructure, mainly for road safety, traffic control, infotainment and driving efficiency purposes (for more information on the vehicular network, refer to references [2], [4]). Trustworthy communication in IoV is therefore very critical, as fake applications may lead to catastrophic road accidents. If a driver misbehaves in a specific zone, other vehicle should send a

The associate editor coordinating the review of this manuscript and approving it for publication was Jose Saldana.

report to the authority [5], [6]. Owing to the shared nature of medium access scheme in the IoV, the reporting message might be revealed by the misbehaving vehicle. In this case, the offender may take retaliatory action against the reporting driver. Therefore, the reporting message should be encrypted and readable only by the reporter and the authority in order to make it undetectable by the reported driver. Moreover, service applications can also be transmitted over IoV, thus, vehicles sometimes need to communicate with each other covertly. So, to transmit hidden data and make it undetectable by unauthorized party, several data hiding techniques such as steganography, cryptography, and watermarking were developed and are in use today. In this work, we focus on one such data hiding techniques called network steganography.

The primary goal of network steganography is to conceal the presence of secure data, so it becomes difficult for an unauthorized party to discover the confidential data. Network steganography is a technique used to hide a secret message in any media and transmit it securely over the communication network. This media can be audio, video, text or image, etc [6]. Previously, the IEEE 802.11 protocols for Wireless Local Area Networks (WLANs) were not used for data hiding due to a short transmission range. For instance, the transmission range for 802.11a/b/g is 30 m indoors and 100 m outdoors, and it is doubled for 802.11n, while currently the transmission range for 802.11p is up to 1000 m [4], [7]. In June 2010, Russian spies used IEEE 802.11 to exchange secret messages among them in the USA [8]. WLAN is also one of many approaches used in the military field to deliver data among soldiers on the battleground.

A data hiding approach based on bit padding of OFDM symbols at the PHY of the IEEE 802.11p protocol is presented and discussed in this paper. The number of encoded bits for each symbol usually varies from 24 up to 216. This is based on the transmission data rate at the PHY layer, as it is possible to insert 27 bytes into each OFDM symbol. According to the frame structure, up to 210 bits per frame can be assigned for a secret message (see section III for more details). In fact, the steganographic technique that uses the principle of frame padding in the PHY of WLANs is called Wireless Padding (WiPad). The work in this paper evaluates the system throughput performance of the steganographic technique based on 2-D Markov chain model under non-saturated conditions. To the best of our knowledge, no body has previously evaluated the system throughput performance of the steganography over vehicular network based on the Markov chain under non-saturated conditions in the presence of error-prone channels. In order to represent the empty buffer in the MAC layer when no packet is ready for transmission, an idle state is added to the model. The key benefits of choosing unsaturated conditions in these models are that (i) actual networks are mostly unsaturated, (ii) to take into account the inter arrival time and burstiness in the network, and (iii) saturated conditions mostly lead to unsteady network [9]–[11]. To avoid overestimating saturated throughput, the model considers non-ideal transmission channel. A Gaussian wireless error channel is assumed where a constant channel Bit Error Rate (BER) should be predefined and every bit has the same probability of bit error in this model. This paper focuses on service applications. Therefore, the channel access mechanism used in this analytical model is the RTS/CTS method, which undergoes unicast mode. Besides, the back-off timer freezing, the packet arrival rate, the existence of first order buffer memory and the *M/M/1* queue are taken into account in order to provide a precise channel access estimation, use the channel efficiently, and analyze the time performance. Moreover, back-off phases and short retry limit for packet transmission are assumed in the analysis to meet the IEEE 802.11p specifications and to ensure that no packet is served indefinitely.

The remaining part of paper is organized as follows: the related works are introduced in section II. Section III presents the approach. Section IV describes the model analysis. Section V offers the performance evaluation of the model. The conclusion is provided in section VI.

II. RELATED WORKS

Data padding is implemented at any layer of the Open System Interconnection Reference Model (OSI RM), and it is mostly used to hide messages only in the network layer, transport layer, and data link. In [12], the authors introduced padding of the Internet Protocol and transmission control protocol (TCP) headers in the context of active wardens. For data hiding, each of these fields provides up to 31 bits per frame. A steganographic scheme called PadSteg was designed by the authors in [13]. This scheme was developed on the basis of padding Ethernet frames and worked in accordance with protocols such as address resolution protocol (ARP) and TCP. The IPv6 frame padding method for covering the information was offered in [14]. The authors provide a pair of channels and 256 bpp as steganographic bandwidth. The authors in [15] introduced a steganography method for IEEE 802.11 via using intentionally corrupted checksums frames to set up hidden communications. The performance evaluation of this method was presented in [16]. In [7], [17], the authors studied steganography in IEEE 802.11 OFDM symbols. They proposed a performance analysis based on 2-D Markov chain model for the system throughput of steganographic scheme of IEEE 802.11 a/g standards considering error-prone channel. However, the authors in [7], [17] assumed saturated condition and analysed it based on the basic access method.

The authors in [18] proposed two methods for information hiding called subliminal channels and steganography. These methods were used to allow vehicles to send reporting messages about misbehaving driver. The beacon message was used to report a misbehaving driver in this study. The beacon message typically includes the status of the transmitter such as position, speed, direction, and so on. The purpose of this work was to report the misbehaving vehicle covertly, either via the signature (subliminal channel) or within a hidden message (steganography). In [19], the authors offered a trust-based distributed authentication (TDA) technique based on

a global trust server and vehicle action to evade collision attacks. This technique guarantees both V2V and V2I communication security in the network. The work in this paper also introduced a channel state routing protocol (CSRP) to provide reliable communication over VANETs. Reliable vehicles were distinguished based on the OBU energy and the channel state of the vehicle to provide seamless communication. The authors provided reliable communication by eliminating collision attacks and enhanced the secured packets transmission among vehicles. The authors in [20] proposed a new security-aware routing method named VANSec. This method was based on trust management over VANETs. The main goal of this method was to detect malicious information and false vehicles. The authors in this work studied several performance metrics as shown in the results such as end-to-end delay (EED), average link duration (ALD), and normalized routing overhead (NRO).

The authors in [21] offered a new steganographic approach called adversarial embedding (ADV-EMB). This approach fulfilled the target of hiding information and it is fooling a convolutional neural network (CNN)-based steganalyzer. The offered approach in [21] functions under the ordinary framework to reduce distortion. Particularly, ADV-EMB approach modified the costs of image elements based on the inclination back broadcasted from the goal of CNN steganalyzer. Thus, the direction of the adjustment gains a higher probability of being similar like the reverse sign of the inclination. This process generates the adversarial stego images. The authors in [22] introduced a novel scheme for creating image by non-secret information (containers) according to Deep Convolutional Generative Adversarial Networks (DCGAN). This method enabled the authors to produce more setganalysis-secure information embedding employing standard steganography processes. The authors employed the DCGAN framework in the field of steganography, such as practical methods to hide secret information within another non-secret information (stego-container). In [23], the authors introduced a new scheme that uses a convolutional neural network (CNN) and a generative adversarial network (GAN) to fulfil a coverless steganography.

III. THE APPROACH

OFDM is used by IEEE 802.11a/g/p protocols at the PHY layer, and the PHY layer of IEEE 802.11 network comprises of two sublayers. These sublayers include PLCP (PHY Layer Convergence Procedure) and PHY Medium Dependent (PMD). The transmission data rate at the PHY layer is set up by determining a specific bits number equivalent to every OFDM symbol. The transmission data rate may differ from 6 Mbps for 24 bits number per symbol up to 54 Mbps for 216 number of bits per symbol as shown in Table 1. Fig. 1 displays 3 frames that are subjected to padding include SERVICE, TAIL, and PSDU (Physical layer Service Data Unit). SERVICE and TAIL have a fixed length, 16 bits and 6 bits respectively. Whereas the length of the MAC frame of PSDU may differs relying on user data and ciphers.

TABLE 1. 802.11 a/g/p OFDM PHY parameters.

Rate R [Mbit/s]	Modulation	Code rate	Number of bits per symbol – N_{BpS}	Factorization of N_{BpS} into primes
6	BPSK	½	24	$2^3 3$
9	BPSK	¾	36	$2^2 3^2$
12	QPSK	½	48	$2^4 3$
18	QPSK	¾	72	$2^3 3^2$
24	16-QAM	½	96	$2^4 3$
36	16-QAM	¾	144	$2^4 3^2$
48	64-QAM	2/3	192	$2^6 3$
54	64-QAM	¾	216	$2^3 3^3$

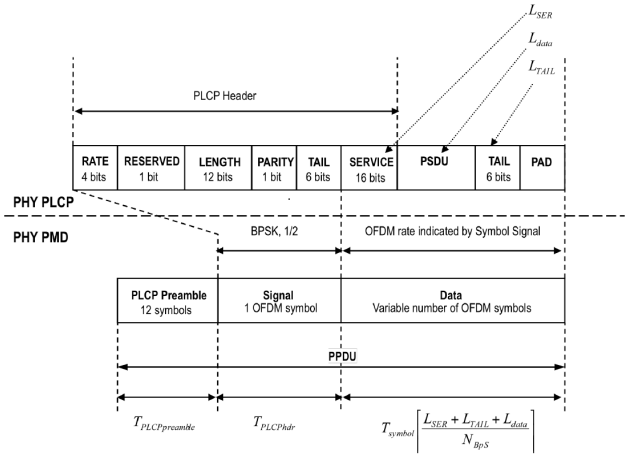

FIGURE 1. The structure of 802.11a/g/p PPDU for ERP-OFDM networks.

The number of bits per symbol is factorised into primes for each data rate R, as in Table 1. So, by using this information, a minimum mutual multiple can be calculated as $2^6 3^3 = 1728$. Thus, for all rates, the maximum number of padding bytes that can be used is:

$$L_\alpha = \frac{2^6 3^3}{8}\alpha - 2 = 216\alpha - 2 \tag{1}$$

where α is a positive integer. In every frame, padding is available, thereby, the main target frames for hiding communication are the ones that are often transmitted such as control packets (RTS/CTS/ACK). Usually, all padding bits values are zero [7]. In this work, all padding bits values are assumed to be employed for steganographic aims.

IV. THE MODEL

This analytical model is based on the IEEE 802.11p standard specifications. The work in this paper considers non-saturated conditions. In order to represent the empty queue in the MAC layer when no packet is ready for transmission, an idle state is added to the model. The key benefits of choosing unsaturated conditions in these models are that (i) actual networks are mostly unsaturated, (ii) to take into account the inter arrival time and burstiness in the network, and (iii) saturated conditions mostly lead to unsteady network [9]–[11]. The number of vehicles n in the network compete for channel based on the contention-based medium

TABLE 2. Used in the analysis notations.

Notations	Description	Notations	Description
n	Number of vehicles	T_i	Idle slot duration
τ	Packet Transmission probability	T_s	Duration for successful packet transmission
p_f	Probability of transmitting a packet with failure due to collision and frame error,		
p_{coll}	Probability of packet collision transmission	T_c	Duration for packet transmission with collision
q	Probability of at least one packet in the buffer	T_{RTS_ERR}	Duration for transmitting an RTS packet unsuccessfully due to frame error
I_i	Unavailability of ith packet transmissions in the buffer	T_{CTS_ERR}	Duration for transmitting an CTS packet unsuccessfully due to frame error
p_{err}	Probability of frame error	T_{ACK_ERR}	Duration for transmitting an ACK packet unsuccessfully due to frame error
p_{BER}	Bit error rate probability	T_{DATA_ERR}	Duration for transmitting a data packet unsuccessfully due to frame error
$p_{rts\ err}$	Probability of RTS frame error rate	T_{RTS}	Time duration to transmit an RTS packet
p_{cts_err}	Probability of CTS frame error rate	T_{CTS}	Time duration to transmit an CTS packet
p_{ack_err}	Probability of ACK frame error rate	T_{ACK}	Time duration to transmit an ACK packet
p_{data_err}	Probability of data frame error rate	T_{SIFS}	Time duration of SIFS (Short Inter-Frame Space)
L_{rts}	RTS packet size	T_{DIFS}	Time duration of DIFS (DCF Inter-Frame Space)
L_{cts}	CTS packet size	T_{EIFS}	Time duration of EIFS (Extended Inter-frame Space)
L_{ack}	ACK packet size	δ	Propagation delay
L_{data}	Data packet size	T_{slot}	The average duration of the logical time slot that might be spent per state considering state of an idle, a successful transmission, a collision or a frame error
p_i	probability of idle channel,	T_{symbol}	Duration of a transmission of an OFDM symbol in 802.11p
p_s	probability of successful packet transmission	L_{ser}	OFDM PHY layer service field size
p_{RTS_ERR}	probability of transmitting an RTS packet unsuccessfully due to the frame error	L_{tail}	OFDM PHY layer tail fields size
p_{CTS_ERR}	probability of transmitting an CTS packet unsuccessfully due to the frame error	N_{BpS}	The number of encoded bites per one symbol
p_{ACK_ERR}	probability of transmitting an ACK packet unsuccessfully due to the frame error	CW	Contention window
p_f	Probability of transmitting a packet with failure due to collision and frame error,	w_i	Contention window size for a packet in the ith backoff stage
p_b	probability of buy channel	T_i	Idle slot duration
p_c	probability of transmitting a packet with collision	T_s	Duration for successful packet transmission

access control. The model considers a non-ideal transmission channel to prevent overestimation of saturated throughput. The worst-case scenario for frame error rate – FER is considered, where errors in the transmission channel are randomly distributed. Thus, Gaussian wireless error channel is assumed where a constant channel Bit Error Rate (BER) should be predefined and every bit has the same probability of bit error in this model. Besides, the back-off timer freezing, the rate of packet arrival, the existence of first order buffer memory and the M/M/1 queue are taken into account in order to provide a precise channel access estimation, use the channel efficiently, and analyze the time performance. In addition, back-off phases and short retry limit for packet transmission are considered in this model to satisfy the IEEE 802.11p specification and to ensure that no packet is served indefinitely. Vehicles communicate in ad hoc mode and the channel access mechanism used in this analytical model is the RTS/CTS method (EDCA mechanism), which undergoes unicast mode. All vehicles share the transmission range and the network does not have any hidden terminals. The significant notations and variables used in the analysis are summarized in Table 2 for convenience.

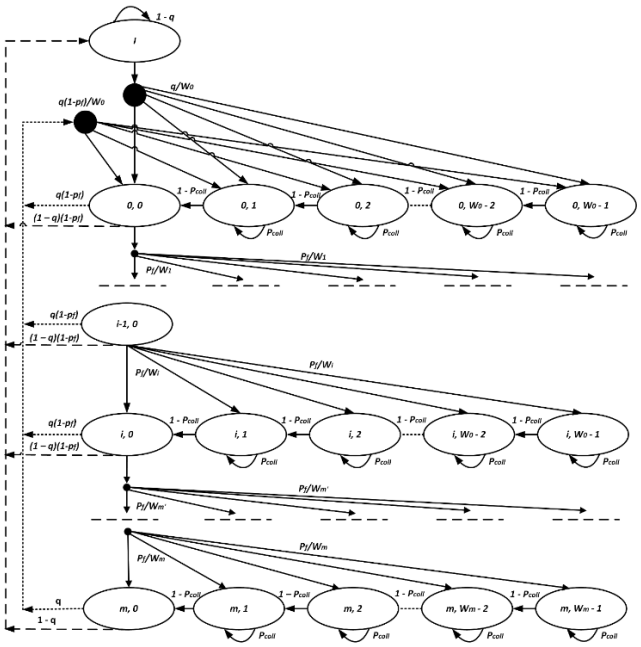

FIGURE 2. Markov Chain Model of the packets transmission process.

A. PROBABILITY OF FRAME TRANSMISSION T

A 2-D Markov chain model is designed to evaluate the probability of frame transmission τ, as shown in Fig. 2. For any given station at time slot t, let s(t) and b(t) be the random variables representing the back-off phases $(0, 1, 2, \ldots, m)$ and the value of the back-off timer $(0, 1, 2, \ldots, W_i - 1)$, respectively. Usually, the back-off timer's maximum value

depends on the back-off phases, so, these random variables are not independent.

$$W_i = \begin{cases} 2^{\mathrm{i}} W_0, & i \le m' \\ 2^{m'} W_0, & i > m' \end{cases} \tag{2}$$

W_0 is the initial size of the contention window, $W_0 = (CW_{min} + 1)$, while m' is the maximum number where the contention window may increase according to the followings, $W_{m'} = 2^{m'} W_0 = (CW_{max} + 1)$. The m' value is 5 in this study. Let m represents the maximum number for back-off phases. However, the two-dimensional $(s\,(t)\,,\, b(t))$ processes are evaluated with discrete-time Markov chain, where the channel status changes. Let (i, k) represents the state process. The state transition diagram of the 2-D Markov chain is shown in Fig. 2, and the non-null transition probabilities are expressed by (3).

The first and second cases in (3) denote that the back-off timer decreases when the channel is sensed idle, otherwise the back-off timer is frozen. The third case in (3) denotes that when the unsuccessful packet transmission occurs, the back-off stage increases from $i-1$ to i and doubles the CWs sizes values as well. The fourth case in (3) denotes that when the packet is successfully transmitted, the node initializes the back-off stage and the CWs sizes values as well. The fifth case in (3) denotes that when the retry limit is exhausted, the maximum back-off stage and the CWs sizes values are reset to the minimum values, after that if there is a packet in the queue for transmission, the node initiates the back-off procedure from the first stage.

Here, the non-null transition probabilities describe the unavailability of packet transmissions in the buffer which is redirected into idle state (I) after a successful transmission.

$$\begin{cases} P(I|i,0) = (1-p_f)(1-q), & 0 \le i \le m-1 \\ P(I|m,0) = 1-q \\ P(I|I) = 1-q \\ P(0,k|I) = q/W_0, & 0 \le k \le W_0 - 1 \end{cases} \tag{4}$$

The first case in (4) represents that when the packet is successfully transmitted and there are no more packets in the queue for transmission, the node enters the idle state. The second case in (4) represents that when the retry limit is exhausted, the maximum back-off stage m and CWs sizes values are reset to the minimum values. After that, if there are no more packets in the queue for transmission, the node enters the idle state. The third and fourth cases in (4) represent that when no new packet arrives at the queue for transmission, the node remains in the idle state. Otherwise, the node moves from the idle state to the back-off state k by initially uniformly choosing back-off timer value in the range $[0, W_0 - 1]$.

Let $b_{i,k} = lim_{t\to\infty} P\{s\,(t) = i, b\,(t) = k\}$ represents the Markov chain's stationary distribution, where $i \in (0,m)$, $k \in (0, w_i - 1)$. Note that:

$$\begin{aligned} b_{i-1,0}.p_f &= b_{i,0} \to b_{i,0} = p_f^i.b_{0,0} \quad 0 < i \le m \\ b_{m,0} &= p_f b_{m-1,0} \end{aligned} \tag{5}$$

Owing to the chain regularities, for each $k \in (1, W_i - 1)$, the idle and back-off states of packets transmission in the stationary distribution are represented by b_I and $b_{i,k}$ and defined as (7) and (8).

$$b_{i,k} = \frac{W_i - k}{W_i\,(1 - p_{coll})} \times \begin{cases} q(1-p_f)\sum_{i=0}^{m-1} b_{i,0} + q b_{m,0} + q b_I, & i = 0 \\ p_f.b_{i-1,0}, & 0 < i \le m \end{cases} \tag{6}$$

$$b_{i,k} = \frac{W_i - k}{W_i} \frac{1}{(1 - p_{coll})} b_{i,0}, \quad for\ 0 \le i \le m,\ 1 \le k \le W_i - 1 \tag{7}$$

$$b_I = (1-q)\,(1-p) \sum_{i=0}^{m-1} b_{i,0} + (1-q)\, b_{m,0} + (1-q)\, b_I \tag{8}$$

From (8), we get (9):

$$b_I = \frac{1-q}{q} b_{0,0} \tag{9}$$

Thus, by using the stationary distribution normalization condition, then

$$\begin{aligned} 1 &= \sum_{i=0}^{m} \sum_{k=0}^{W_i - 1} b_{i,k} + b_I \\ 1 &= \sum_{i=0}^{m} b_{i,0} + \sum_{i=0}^{m} \sum_{k=1}^{W_i - 1} b_{i,k} + b_I \\ 1 &= \sum_{i=0}^{m} b_{i,0} + \sum_{i=0}^{m} \sum_{k=1}^{W_i - 1} \frac{W_i - k}{W_i} \frac{1}{(1 - p_{coll})} b_{i,0} + b_I \\ 1 &= \sum_{i=0}^{m} b_{i,0} + \frac{1}{1 - p_{coll}} \sum_{i=0}^{m} b_{i,0} \frac{W_i - 1}{2} + b_I \\ 1 &= \sum_{i=0}^{m} b_{i,0} + \frac{1}{1 - p_{coll}} \sum_{i=0}^{m} b_{i,0} \frac{W_i - 1}{2} + \frac{1-q}{q} b_{0,0} \\ 1 &= \sum_{i=0}^{m} p_f^i b_{0,0} + \frac{1}{2\,(1 - p_{coll})} \\ &\quad \times \left[\sum_{i=0}^{m} (2p_f)^i W b_{0,0} - \sum_{i=0}^{m} p_f^i b_{0,0} \right] + \frac{1-q}{q} b_{0,0} \end{aligned} \tag{10}$$

From (10), we get (11), which relies on the values of m and m'

$$b_{0,0} = \begin{cases} \dfrac{2(1-p_f)(1-p_{coll})(1-2p_f)q}{£}, & m \le m' \\ \dfrac{2(1-p_f)(1-p_{coll})(1-2p_f)q}{¥}, & m > m' \end{cases} \tag{11}$$

where:

$$\begin{aligned} £ &= (1-2p_f)(1-2p_{coll})(1-p_f^{m+1})q \\ &\quad + W_0(1-p_f)(-(2p_f)^{m+1})q \end{aligned}$$

$$+2(1-p_f)(1-p_{coll})(1-2p_f)(1-q) \quad (12)$$

And:

$$\begin{aligned}¥ = {} & (1-2p_f)(1-2p_{coll})(1-p_f^{m+1})q \\ & + W_0(1-p_f)(1-(2p_f)^{m'+1})q \\ & + 2^{m'}W_0p_f^{m'+1}\left(1-p_f^{m-m'}\right)(1-2p_f)\,q \\ & + 2(1-p_f)(1-p_{coll})(1-2p_f)q \end{aligned} \quad (13)$$

We can now compute the frame transmission probability τ where a node is able to transmit a frame in a random selected time slot. The node allows to transmit a packet when the back-off time counter is equal to zero ($b_{i,0}$) irrespective of the back-off phase, as in (14).

$$\tau = \sum_{i=0}^{m} b_{i,0} = b_{0,0}\frac{1-{p_f}^{m+1}}{1-p_f} \quad (14)$$

Equation (14) displays that the τ value relies on the failure p_f probability, conditional collision p_{coll}, and probability of at least one frame in buffer q. The probability of collision may happen when at least two nodes are transmitting frames in the same time slot.

B. FAILURE AND COLLISION PROBABILITIES

The probability of transmission failure of the packet p_f is derived by (15):

$$p_f = 1-(1-p_{coll})(1-p_{err}) \quad (15)$$

where the probability of frame error for packet transmission is represented by p_{err}

$$\begin{aligned} p_{err} = 1 - {} & \left(1-p_{rts_{err}}\right)\left(1-p_{cts_{err}}\right) \\ & \times \left(1-p_{data_{err}}\right).\left(1-p_{ack\_err}\right) \end{aligned} \quad (16)$$

where p_{rts_err},p_{cts_err},p_{data_err} and p_{ack_err} represent the Frame Error Rate (FERs) for RTS/CTS/DATA/ACK frames error respectively. These errors probability are calculated from bit error probability (i.e. BER) p_{BER} by (17) [24]:

$$\begin{cases} p_{rts\_err} = 1-(1-p_{BER})^{L_{rts}} \\ p_{cts\_err} = 1-(1-p_{BER})^{L_{cts}} \\ p_{data\_err} = 1-(1-p_{BER})^{L_{data}} \\ p_{ack\_err} = 1-(1-p_{BER})^{L_{ack}} \end{cases} \quad (17)$$

where the bit error rate (p_{BER}) can be obtained by calculating the bit-energy-to-noise ratio. QPSK modulation scheme is the common modulation used for 802.11p protocol in vehicular network, hence, p_{BER} for QPSK modulation can be computed by (18) [25]:

$$p_{BER} = Q\left(2\frac{E_b}{N_o}\right) \quad (18)$$

where $\frac{E_b}{N_o}$ denotes the bit-energy-to-noise ratio of received signal and *Q-function* is given by (19):

$$Q(x) = \int_x^{\infty} \frac{1}{\sqrt{2\pi}} e^{\frac{-t^2}{2}}\,dt \quad (19)$$

The probability of packet collision transmission p_{coll} packets is defined as follows:

$$p_{coll} = 1-(1-\tau)^{n-1} \quad (20)$$

Then,

$$p_f = 1-(1-\tau)^{n-1}(1-p_{err}) \quad (21)$$

From equations (14), (20), and (21), we can compute the packets transmission and failure probabilities by solving the two unknown variables, τ and p_f, using numerical techniques.

C. LOAD EQUATION Q

The researchers usually assume the Poisson distribution model in vehicular network, where the traffic arrival rate is distributed exponentially. Thus, with Poisson process, the load equation of queue probability q is given by (22) [26]:

$$q = 1-e^{-2\lambda T_{slot}^{802.11p}} \quad (22)$$

However, equation (22) only studies the rate of traffic arrival while overlooking the existence of the buffer memory. In order to understand the buffer correlation with Poisson arrivals, every vehicle has an *M/G/1* queue [27]. In this correlation, the queuing model does not function smoothly owing to the complexity of the deviation of the mean MAC time estimate. Therefore, equation (23) offers a more sophisticated method taking into account the existence of traffic arrival along with the buffer memory. Then, the new load equation of queue probability q is given by (23) [11], [28]:

$$q = (1-e^{-\lambda T_{slot}^{802.11p}})(1+q_{tmp})/(1+(1-e^{-\lambda T_{slot}^{802.11p}})q_{tmp}) \quad (23)$$

where, $q_{tmp} = (p_f+(1-p_f)p_f)/(1-p_f)^2$

$$\begin{cases} P(i,k|i,k+1) = 1-p_{coll}, & 0 \le k \le W_i-2,\ 0 \le i \le m \\ P(i,k|i,k) = p_{coll}, & 1 \le k \le W_i-1,\ 0 \le i \le m \\ P(i,k|i-1,0) = p_f/W_i, & 0 \le k \le W_i-1,\ 1 \le i \le m \\ P(0,k|i,0) = (1-p_f)/W_0, & 0 \le k \le W_0-1, 0 \le i \le m \\ P(0,k|m,0) = 1/W_0, & 0 \le k \le W_0-1, \end{cases} \quad (3)$$

D. RTS/CTS/DATA/ACK TRANSMISSION TIME ANALYSIS

The channel state during the contention-based MAC process in every time slot will be in one of the following stages, either idle, collision transmission, successful transmission, or failure transmission owing to the frame error. Hence, the channel states probabilities are expressed by (24), as shown at the bottom of the next page. The time slot durations states for the packet transmission process via the contention-based MAC for RTS/CTS/DATA/ACK frames are displayed in Fig. 3. The transmission time is therefore determined, as in (25), as shown at the bottom of the next page, using unicast mode.

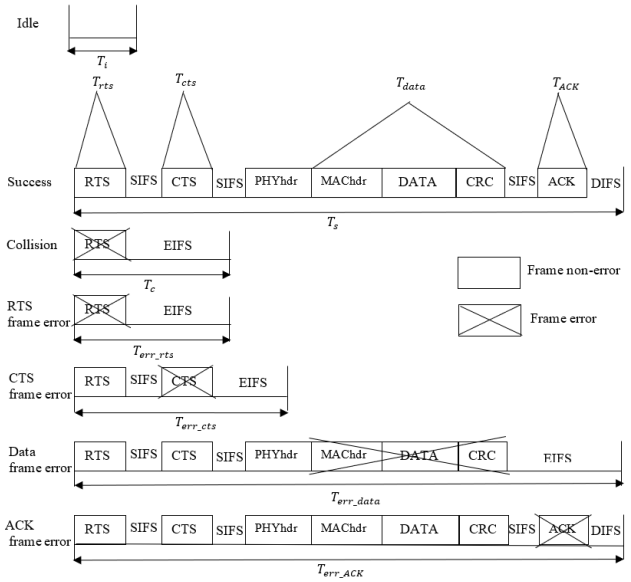

FIGURE 3. The length of time slots for the channel states of RTS/CTS/DATA/ACK packets.

Where $T_{data} = L_{pld}/R$, L_{pld} denotes the data frame payload and R is the transmission data rate. T_{rts}, T_{cts}, T_{data} and T_{ack} are PHY-layer dependent and the transmission of packet in the unit of OFDM symbols is expressed by (26), as shown at the bottom of the next page [24]: Therefore, the logical time slots duration $T_{slot}^{802.11p}$ per state over the channel should be derived to compute the system throughput, and this is expressed by:

$$\begin{aligned} T_{slot}^{802.11p} &= p_i T_i + p_s T_s + p_c T_c + p_{RTS_{ERR}} T_{RTS_{ERR}} \\ &\quad + p_{CTS\_ERR} T_{CTS\_ERR} + p_{DATA\_ERR} T_{DATA\_ERR} \\ &\quad + p_{ACK\_ERR} T_{ACK\_ERR} \end{aligned} \tag{27}$$

Finally, the system throughput S will be equal to

$$S = \frac{p_s * L_{pld}}{T_{slot}^{802.11p}} \tag{28}$$

E. STEGANOGRAPHIC CHANNEL CAPACITY AND SATURATION THROUGHPUT

The steganographic channel capacity based on data packets is calculated by (29):

$$c_{data} = N_{BpS} \left| \frac{L_{ser} + L_{tail} + L_{data}}{N_{BpS}} \right| - (L_{ser} + L_{tail} + L_{data}) \tag{29}$$

The steganographic channel capacity of control packets (RTS/CTS/ACK) is determined by (30):

$$\begin{cases} c_{rts} = N_{BpS} \left| \dfrac{L_{ser} + L_{tail} + L_{rts}}{N_{BpS}} \right| - (L_{ser} + L_{tail} + L_{rts}) \\ c_{cts} = N_{BpS} \left| \dfrac{L_{ser} + L_{tail} + L_{cts}}{N_{BpS}} \right| - (L_{ser} + L_{tail} + L_{cts}) \\ c_{ack} = N_{BpS} \left| \dfrac{L_{ser} + L_{tail} + L_{ack}}{N_{BpS}} \right| - (L_{ser} + L_{tail} + L_{ack}) \end{cases} \tag{30}$$

Finally, the system throughput of a steganographic channel for data and control packets is respectively expressed by (31):

$$\begin{cases} S_{data\_steg} = \dfrac{c_{data} \cdot S}{n \cdot L_{pld}} \\ S_{rts\_steg} = \dfrac{c_{rts} \cdot S}{n \cdot L_{pld}} \\ S_{cts\_steg} = \dfrac{c_{cts} \cdot S}{n \cdot L_{pld}} \\ S_{ack\_steg} = \dfrac{c_{ack} \cdot S}{n \cdot L_{pld}} \end{cases} \tag{31}$$

V. PERFORMANCE EVALUATION

This section presesnts the numerical and simulation results of IEEE 802.11p to study the system throughput of the steganographic technique (WiPad) in the presence of non-ideal transmission channel. MATLAB is used to carry out the numerical results, whereas Simulation of Urban Mobility (SUMO) and network simulator (ns-2.34) are employed to execute the simulations results to validate the analytical model. In the vehicular environment, traffic mobility and network are simulated by SUMO and NS-2, respectively. Shah Alam highway is considered to represent a highway environment as shown in Fig. 4. The selected area in Shah Alam highway is around 1 km and covered by 1 MAGs/MAARs. The study includes 100 vehicles with a 60 km/h speed. The vehicles contain a GPS and a single-radio WAVE communication device. Rate of traffic arrival λ and vehicles n are generated at the MAC layer based on the Poisson distribution. the rate of traffic arrival λ and the vehicles number n are changed from 10 to 100. The transmission data rate R and packet sizes L are also varied in this analysis. Thereby, the traffic density

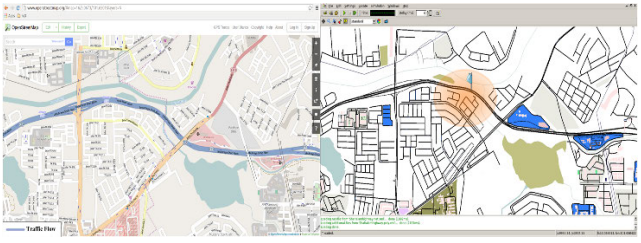

FIGURE 4. SUMO Simulator for Vehicular Traffic Simulation (Shah Alam Highway).

TABLE 3. Typical parameters values.

Parameters	values
Transmission data rate	3, 4.5, 6, 9, 12, 18, 24, 27 Mbps
MAC header	272 bits
PHY header	128 bits
packet size	214, 430, 646, 862, 1078, 1294, 1510, 1726 bytes
RTS	160 bits
CTS	112 bits
ACK	112 bits
SIFS	16 μs
Time slot σ	9 μs
DIFS	34 μs
Propagation delay δ	1 μs
L_{ser}	16 bits
L_{tail}	6 bits
T_{symbol} (μs)	4
N_{BpS}	24
BER	0, 10^{-5}, 10^{-4}
CW_{max}	15
CW_{min}	1023
Short retry limit	5
Long retry limit	7
Frequency	5.9 GHz

could be affected by several factors in this study. Vehicular communications often faces various obstacles like channel fading, path loss, and thermal noise, leading to poor channel quality. Consequently, channel conditions are considered in this study. The Bit Error Rate (BER) values for channel conditions studied in this analysis are BER = 0, 10^{-5}, 10^{-4}. All vehicles share the transmission range and the network does not have any hidden terminals. Table 3 summarizes the analytical and simulation models parameters.

The effect of vehicles number and the rate of traffic arrival on the steganographic channel system throughput based on data and ACK frames given various error-prone channel conditions are shown in Figs. 5 - 7. The packet size in Figs. 5 - 7 is constant, $L = 1000$ bytes. The traffic arrival rate in Figs. 5 and 6 is fixed $\lambda = 10$ pps, while the number of vehicles in Fig. 7 is $n = 30$ vehicle. The figures display that the error-prone channel condition has significant impact on the system throughput performance. It can be observed in Fig. 5 - 7 that the values of the steganographic channel system throughput for data and ACK frames are low as vehicles number, rate of traffic arrival λ, and the value of BER increase. For instance, when the number of vehicles is constant $n = 80$ *vehicle* and the error-prone channel condition is varied BER = 0, 10^{-5}, 10^{-4}, the values of the steganographic channel system throughput of data frame are 0.10761 Kbps, 0.099436 Kbps, 0.048639 Kbps, respectively, as shown in Fig. 5. Figure 6 displays that when the number of vehicles is $n = 80$ *vehicle* and the error-prone channel condition is varied BER = 0, 10^{-5}, 10^{-4}, the values of the steganographic channel system throughput of ACK frame are 0.05978 Kbps, 0.05524 Kbps, 0.02702 Kbps, respectively. Moreover, when the traffic arrival rate λ is 60 and the BER = 0, 10^{-5}, 10^{-4}, the values of the steganographic channel system throughput for data frame are 0.28568 Kbps,

$$\begin{cases} p_i = (1-\tau)^n \\ p_s = n\tau(1-\tau)^{n-1}(1-p_{rts\_err})(1-p_{cts\_err})(1-p_{data\_err})(1-p_{ack\_err}) \\ p_c = 1-(1-\tau_s)^n - n\tau_s(1-\tau_s)^{n-1} \\ p_{RTS\_ERR} = n\tau(1-\tau)^{n-1} p_{rts\_err} \\ p_{CTS\_ERR} = n\tau(1-\tau)^{n-1}(1-p_{rts\_err})p_{cts\_err} \\ p_{DATA\_ERR} = n\tau(1-\tau)^{n-1}\left(1-p_{rts\_err}\right)\left(1-p_{cts\_err}\right)p_{data\_err} \\ p_{ACK\_ERR} = n\tau(1-\tau)^{n-1}\left(1-p_{rts\_err}\right)\left(1-p_{cts\_err}\right)\left(1-p_{data\_err}\right)p_{ack\_err} \end{cases} \tag{24}$$

$$\begin{cases} T_i = T_\sigma \\ T_s = T_{rts} + T_{cts} + T_h + T_{data} + T_{ack} + 4\delta + 3T_{SIFS} + T_{DIFS} \\ T_c = T_{rts} + \delta + T_{EIFS} \\ T_{RTS\_ERR} = T_{rts} + \delta + T_{EIFS} \\ T_{CTS\_ERR} = T_{rts} + T_{SIFS} + T_{cts} + 2\delta + T_{EIFS} \\ T_{DATA\_ERR} = T_{rts} + T_{cts} + T_h + T_{data} + 2T_{SIFS} + 3\delta + T_{EIFS} \\ T_{ACK\_ERR} = T_s \end{cases} \tag{25}$$

$$\begin{cases} T_{rts} = T_{symbol}\left\lceil \dfrac{L_{ser} + L_{tail} + L_{rts}}{N_{BpS}} \right\rceil \\ T_{cts} = T_{symbol}\left\lceil \dfrac{L_{ser} + L_{tail} + L_{cts}}{N_{BpS}} \right\rceil \\ T_{data} = T_{symbol}\left\lceil \dfrac{L_{ser} + L_{tail} + L_{data}}{N_{BpS}} \right\rceil \\ T_{ack} = T_{symbol}\left\lceil \dfrac{L_{ser} + L_{tail} + L_{ack}}{N_{BpS}} \right\rceil \end{cases} \tag{26}$$

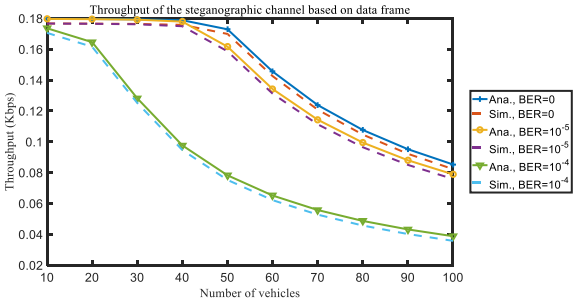

FIGURE 5. Steganographic channel System throughput based on data frame versus number of vehicles under various error-prone channel conditions.

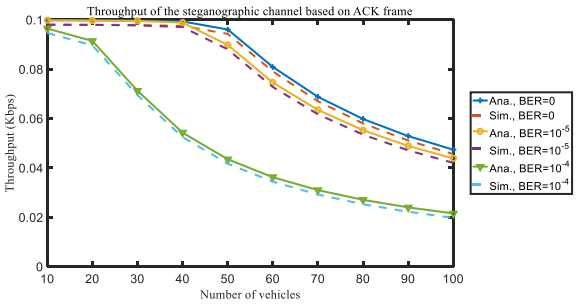

FIGURE 6. Steganographic channel System throughput based on ACK frame versus number of vehicles under various error-prone channel conditions.

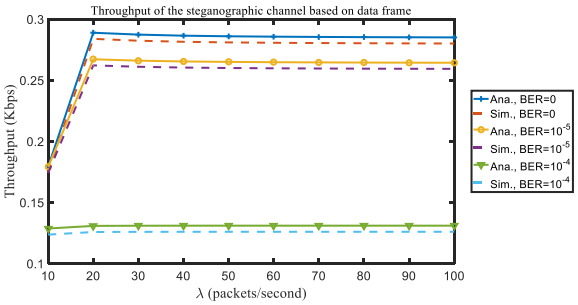

FIGURE 7. Steganographic channel System throughput based on data frame versus packet arrival rate under various error-prone channel conditions.

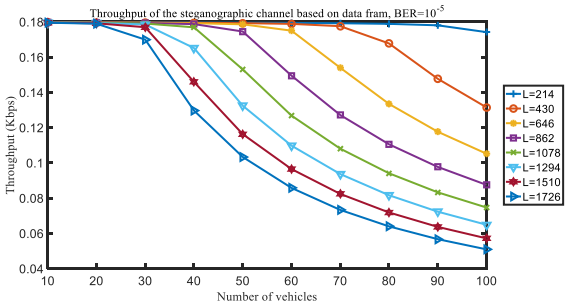

FIGURE 8. Steganographic channel System throughput based on data frame versus number of vehicles under various packet sizes.

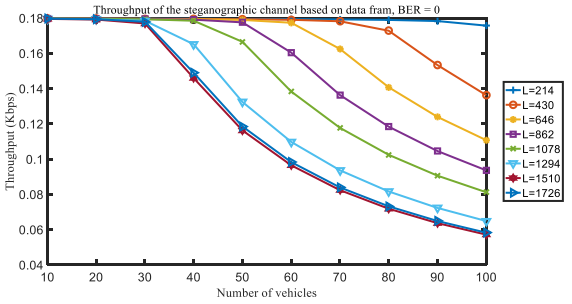

FIGURE 9. Steganographic channel System throughput based on data frame versus number of vehicles under various packet sizes.

0.26479 Kbps, and 0.13103 Kbps, respectively, as presented in Fig. 7. Consequently, Figs. 5 – 7 display that when the channel is in a bad condition (*i.e.*$BER = 10^{-4}$), more vehicles and more traffic arrival rate decrease the system throughput of the steganographic channel to the lower level. Finally, the simulation and analytical results presented in Figs. 5 - 7 are relatively matched, and this validates the correctness of the proposed analytical model.

In these upcoming figures, we don't study the simulation results as the accuracy of the model is validated in the previous Figs. 5 - 7. Figs. 8 and 9 explains the influence of number of vehicles, packet size, and channel conditions on the system throughput of the steganographic channel based on data frame. The traffic arrival rate in Figs. 8 and 9 is constant $\lambda = 10$ pps. The channel conditions are BER $= 0$ and 10^{-5} in Figs. 8 and 9, respectively. An interesting observation from Figs. 8 and 9 is that along with an increase in the vehicles number and packet size, the system throughput of the steganographic channel decreases. Instead, when the number of vehicle and the packet size increase, the channel is saturated and congested, and that cause more packet collisions, thus the system throughput of the steganographic channel dramatically degrades at all channel BER values. In addition, when the channel is in a bad condition (i.e. $BER = 10^{-5}$), the value of the system throughput of the steganographic channel is low compared to the value when the channel is ideal, BER $= 0$. For simplicity, in Fig. 8 when the number of vehicles is 60, the packet size is 1078 bytes, and the value of channel condition BER is 10^{-5}, then the value of the system throughput of the steganographic channel is 0.12677 Kbps, while it is 0.1383 Kbps when the channel condition BER is 0 as in Fig. 9.

Figs. 10 and 11 illustrate the effect of number of vehicle n and the transmission data rate R on the steganographic channel system throughput for data and ACK packets, respectively. The traffic arrival rate, the channel conditions and the packet size are $\lambda = 10$ pps, BER $= 10^{-5}$, and $L = 1000$ bytes, respectively, in Figs. 10 and 11. It can be found from Figs. 10 and 11 that the value of the steganographic channel system throughput for data and ACK packets is low when the channel capacity R is small and the network size (number of vehicle) is large. This is due to the fact that in the large network size with small channel capacity R, the channel is in saturated and congested condition causing

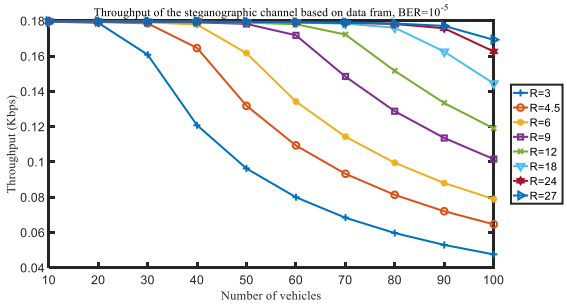

FIGURE 10. Steganographic channel System throughput based on data frame versus number of vehicles under various transmission data rate.

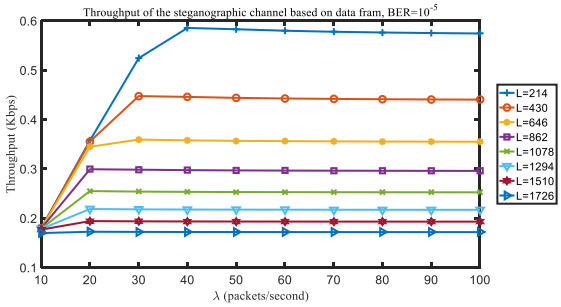

FIGURE 12. Steganographic channel System throughput based on data frame versus packet arrival rate under various packet size.

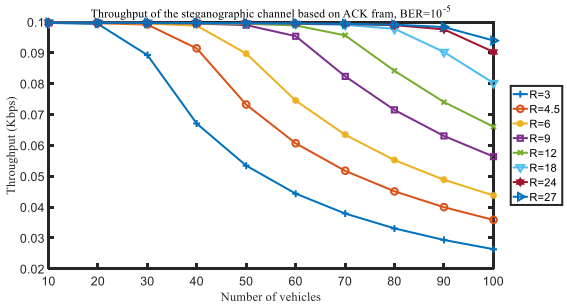

FIGURE 11. Steganographic channel System throughput based on ACK frame versus number of vehicles under various transmission data rate.

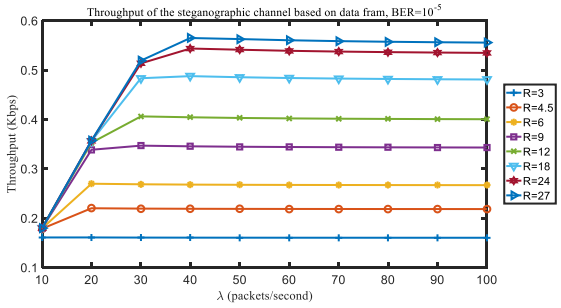

FIGURE 13. Steganographic channel System throughput based on data frame versus packet arrival rate under various transmission data rate.

a higher probability of packet collision, and thereby the system throughput of the steganographic channel significantly degrades. For instance, when the number of vehicle $n = 40$ and the channel capacity $R = 3$ Mbps, the value of the steganographic channel system throughput for data frame is 0.12073 Kbps, while it is 0.17929 Kbps when the channel bandwidth is $R = 12$ Mbps with same number of vehicle, as shown in Fig. 10. Moreover, when the number of vehicles is $n = 20$, and the channel capacity R is 6 Mbps, the value of the steganographic channel system throughput of data frame is 0.17946 Kbps, while it is 0.099436 Kbps when the number of vehicle is $n = 80$ with same channel capacity. This also displays that the performance of the system throughput of the steganographic channel is inversely proportional to the number of vehicles (network size) even if the transmission data rate increases.

In Figs. 12 and 13, the impact of traffic arrival rate λ, packet size L, and transmission data rate R on system throughput of the steganographic channel is presented. The number of vehicle and the channel conditions are $n = 30$ and BER $= 10^{-5}$, respectively, in Figs. 12 and 13. It can be found from Figs. 12 and 13 that system throughput of the steganographic channel strongly depends on traffic arrival rate, packet size, and channel capacity. Accordingly, it is observed that along with the increasing the rate of traffic arrival, the steganographic channel system throughput increases as well when the traffic arrival rate is still light $\lambda \leq 30pps$. When the traffic arrival rate increases from light to heavy $\lambda > 30pps$, the fast saturation level of occupying the channel is shown in Figs. 12 and 13, seeing that the system throughput of the steganographic channel reaches the maximum value and its graph becomes flat. This is due to the fact that with the increasing the rate of traffic arrival, the possibility to fully occupy the channel also increases. In addition, with increasing the packet size, the fast saturation level of occupying the channel is shown in Fig. 12. In contrast, along with decreasing the channel capacity R, the fast saturation level of occupying the channel is shown in Fig. 13.

VI. CONCLUSION

This paper has proposed a steganographic scheme called WiPad to evaluate the system throughput performance of the steganographic channel of IEEE 802.11p scheme over vehicular network. We initially analyse the IEEE 802.11p protocol based on 2-D Markov chain model under non-saturated conditions with non-ideal transmission channel. The study of 802.11p scheme is used to derive the probabilities of transmission, successful transmission, failure transmission, and collisions. After that, based on these derivations, the performance metric of the system throughput of the steganographic channel is formulated and computed. The impact of various parameters such as channel conditions, rate of packet arrival, vehicles number, packets sizes, and transmission data rate are studied to evaluate and understand the system throughput performance of the steganographic channel of IEEE 802.11p protocol over vehicular network. Analytical and simulation results stated that the values of the steganographic channel system throughput for data and control frames are low as the

rate of traffic arrival λ, vehicles number n, packet size, and the value of BER increase. In addition, the study display that the value of the system throughput of the steganographic channel based on data and control frames decreases when the channel capacity R is small, and the network size is large.

For future work, the model performance will be evaluated in the real vehicular network environment (testbed evaluation) and it would be interesting to evaluate it in the presence of hidden terminals.

REFERENCES

[1] L. Hu and Z. Dai, "Performance and reliability analysis of prioritized safety messages broadcasting in DSRC with hidden terminals," *IEEE Access*, vol. 8, pp. 177112–177124, 2020.

[2] L. Hu, H. Wang, and Y. Zhao, "Performance analysis of DSRC-based vehicular safety communication in imperfect channels," *IEEE Access*, vol. 8, pp. 107399–107408, 2020.

[3] S. Yu, J. Lee, K. Park, A. K. Das, and Y. Park, "IoV-SMAP: Secure and efficient message authentication protocol for IoV in smart city environment," *IEEE Access*, vol. 8, pp. 167875–167886, 2020.

[4] A. A. Almohammedi, N. K. Noordin, A. Sali, F. Hashim, and M. Balfaqih, "An adaptive multi-channel assignment and coordination scheme for IEEE 802.11P/1609.4 in vehicular ad-hoc networks," *IEEE Access*, vol. 6, pp. 2781–2802, 2018.

[5] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "Misbehavior detection and efficient revocation within VANET," *J. Inf. Secur. Appl.*, vol. 46, pp. 193–209, Jun. 2019.

[6] N. Singh, J. Bhardwaj, and G. Raghav, "Network steganography and its techniques: A survey," *Int. J. Comput. Appl.*, vol. 174, no. 2, pp. 8–14, Sep. 2017.

[7] K. Szczypiorski and W. Mazurczyk, "Steganography in IEEE 802.11 OFDM symbols," *Secur. Commun. Netw.*, vol. 9, no. 2, pp. 118–129, Jan. 2016.

[8] BBC News. *FBI Allegations Against 'Russian Spies' in US*. Accessed: Oct. 11, 2020. [Online]. Available: https://www.bbc.com/news/10442869

[9] C. Song, G. Tan, C. Yu, N. Ding, and F. Zhang, "APDM: An adaptive multi-priority distributed multichannel MAC protocol for vehicular ad hoc networks in unsaturated conditions," *Comput. Commun.*, vol. 104, pp. 119–133, May 2017.

[10] N. Gupta and C. S. Rai, "Performance evaluation of IEEE 802.11 DCF in single hop ad hoc networks," *Wireless Pers. Commun.*, vol. 79, no. 3, pp. 2171–2193, Dec. 2014.

[11] F. Daneshgaran, M. Laddomada, F. Mesiti, and M. Mondin, "Unsaturated throughput analysis of IEEE 802.11 in presence of non ideal transmission channel and capture effects," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1276–1286, Apr. 2008.

[12] G. Fisk, M. Fisk, C. Papadopoulos, and J. Neil, "Eliminating steganography in Internet traffic with active wardens," in *Proc. Int. Workshop Inf. Hiding*, 2002, pp. 18–35.

[13] B. Jankowski, W. Mazurczyk, and K. Szczypiorski, "Information hiding using improper frame padding," in *Proc. 14th Int. Telecommun. Netw. Strategy Planning Symp. (NETWORKS)*, Sep. 2010, pp. 1–6.

[14] N. B. Lucena, G. Lewandowski, and S. J. Chapin, "Covert channels in IPv6," in *Proc. Int. Workshop Privacy Enhancing Technol.*, 2005, pp. 147–166.

[15] K. Szczypiorski, "HICCUPS: Hidden communication system for corrupted networks," in *Proc. Int. Multi-Conf. Adv. Comput. Syst.*, 2003, pp. 31–40.

[16] K. Szczypiorski, "A performance analysis of HICCUPS—A steganographic system for WLAN," *Telecommun. Syst.*, vol. 49, no. 2, pp. 255–259, 2012.

[17] K. Szczypiorski and W. Mazurczyk, "Hiding data in OFDM symbols of IEEE 802.11 networks," in *Proc. Int. Conf. Multimedia Inf. Netw. Secur.*, Nov. 2010, pp. 835–840.

[18] J. M. D. Fuentes, J. Blasco, A. I. González-Tablas, and L. González-Manzano, "Applying information hiding in VANETs to covertly report misbehaving vehicles," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 2, Feb. 2014, Art. no. 120626.

[19] A. M. R. Tolba, "Trust-based distributed authentication method for collision attack avoidance in VANETs," *IEEE Access*, vol. 6, pp. 62747–62755, 2018.

[20] S. Ahmed, M. U. Rehman, A. Ishtiaq, S. Khan, A. Ali, and S. Begum, "VANSec: Attack-resistant VANET security algorithm in terms of trust computation error and normalized routing overhead," *J. Sensors*, vol. 2018, pp. 1–17, Jul. 2018.

[21] W. Tang, B. Li, S. Tan, M. Barni, and J. Huang, "CNN-based adversarial embedding for image steganography," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 8, pp. 2074–2087, Aug. 2019.

[22] D. Volkhonskiy, I. Nazarov, and E. Burnaev, "Steganographic generative adversarial networks," in *Proc. 12th Int. Conf. Mach. Vis. (ICMV)*, Jan. 2020, Art. no. 114333.

[23] J. Qin, J. Wang, Y. Tan, H. Huang, X. Xiang, and Z. He, "Coverless image steganography based on generative adversarial network," *Mathematics*, vol. 8, no. 9, p. 1394, Aug. 2020.

[24] *IEEE Standard for Telecommunications and Information Exchange Between Systems—LAN/MAN Specific Requirements—Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High Speed Physical Layer in the 5 GHz Band*, IEEE Standard 802.11a-20-08-1999, Aug. 1999.

[25] T. S. Rappaport, *Wireless Communications: Principles and Practice*, vol. 2. Upper Saddle River, NJ, USA: Prentice-Hall PTR, 1996.

[26] D. Malone, K. Duffy, and D. Leith, "Modeling the 802.11 distributed coordination function in nonsaturated heterogeneous conditions," *IEEE/ACM Trans. Netw.*, vol. 15, no. 1, pp. 159–172, Feb. 2007.

[27] K. Duffy and A. Ganesh, "Modeling the impact of buffering on 802.11," *IEEE Commun. Lett.*, vol. 11, no. 2, pp. 219–221, Feb. 2007.

[28] W. Dong, W. Zhang, X. Chen, and G. Wei, "A new load equation for 802.11 MAC performance evaluation under non-saturated conditions," in *Proc. 1st IEEE Int. Conf. Commun. China (ICCC)*, Aug. 2012, pp. 428–432.

AKRAM A. ALMOHAMMEDI (Graduate Student Member, IEEE) received the B.Sc. degree in electronics engineering from Infrastructure University Kuala Lumpur, Malaysia, in 2012, the M.Sc. degree in electrical and electronics engineering majoring in computer and communication system from the Universiti Kebangsaan Malaysia, Malaysia, and the PhD degree in wireless communications and networks engineering from the University Putra Malaysia (UPM), in 2019. He is currently a Senior Researcher with South Ural State University (SUSU), Russia. His research interests include the Internet of Vehicle, the Internet of Things, multi-channel MAC, steganography, and wireless sensor networks.

VLADIMIR SHEPELEV received the Ph.D. degree from Chelyabinsk State Agroengineering University, Russia, in 2000. Since 2007, he has been a Technical Scientist with LLC NTK-Logistics Transport and Logistic Company. He is currently an Associate Professor with South Ural State University (SUSU). He is also working in a project entitled Development of an Intelligent Digital Platform for the Management of Transportation Systems of Cities based on Artificial Intelligence. He has published several articles, books, and patents. His research interests include the Internet of Things (IoT), real time traffic management, and the Internet of Vehicles (IoV).