Trustworthy Vehicular Communication Employing Multidimensional Diversification for Moving-target Defense

Esraa M. Ghourab[1], Effat Samir[1], Mohamed Azab[2,3,*], and Mohamed Eltoweissy[3]

[1]*Electrical Engineering Department, Alexandria University, Alexandria 21544, Egypt*
[2]*Computer and Information Sciences Department, Virginia Military Institute, Lexington, VA, USA*
[3]*Informatics Research Institute, City of Scientific Research and Technological Applications, Alexandria, Egypt*
E-mail: Esraa.M.Ghourab@mena.vt.edu; effat_samir@mena.vt.edu; mazab@vt.edu; eltoweissymy@vmi.edu
[*]*Corresponding Author*

Received 30 September 2018; Accepted 01 October 2018;
Publication 06 November 2018

Abstract

Enabling trustworthy Vehicle to Vehicle (V2V) communication given the wireless medium and the highly dynamic nature of the vehicular environment is a hard challenge. Eavesdropping and signal jamming in such highly dynamic environment is a real problem. This paper proposes a nature inspired multidimensional Moving-Target Defense (MTD) that employs real time spatiotemporal diversity to obfuscate wireless signals against attacker reach. In space: the mechanism manipulates the wireless transmission pattern and configuration to confuse eavesdroppers. In Time: we manipulate the transmission payload, by intentionally injecting some fake data into the real transmission. Further, the mechanism changes the data transmission granularity over time from fine to coarse grained data chunks. As a case study, we assumed the direct transmission model across dynamic multi-paths relayed communication via vehicles traveling on a multi-lane road. The system is evaluated based

Journal of Cyber Security and Mobility, Vol. 8_2, 133–164. *River Publishers*
doi: 10.13052/jcsm2245-1439.821

on a complete analysis of the system model and comprehensive simulated scenarios. Results showed the effectiveness of the presented approach with an increased confusion factor, a massive reduction in the intercept probability and clear increase in the channel secrecy.

Keywords: Security, Diversity, Moving target defense, Vehicle to Vehicle (V2V) communication.

1 Introduction

Smart grids, Smart buildings, Smart infrastructure, Smart cities and many more are examples for the evolution supporting our future of our current lifestyle. Wireless communication is the supporting pillar enabling such evolution. Ensuring wireless communication security and resilience against attacks and eavesdroppers is the main concern of the modern research community.

Vehicle to vehicle communication is long been considered as an enabler for many services supporting Smart cities [1, 2]. Nowadays, there are many vehicles to vehicle (V2V) applications, such as emergency braking, velocity adjustment to avoid vehicles crash, effective transportation to avoid passage congestion, hazardous location notifications transmitted to the road/site station [3–5]. In V2V networks, the transmitted data propagates from the source vehicle to reach destination vehicle in relatively high-speeds subject to the road conditions. Smart V2V communications impose a challenge in designing robust communication systems to overcome the deterioration offered by rapid wireless channel variations. The broadcast nature of the radio propagation and the heterogeneous environment in V2V, makes the data transmission vulnerable to eavesdropping attacks. User's data can be easily overheard, altered, or blocked by malicious parties.

Unfortunately, many studies proved that eavesdroppers and attackers can still decrypt the heavily encrypted data, even with the deployment of computationally expensive resources [20]. This paper introduces a Moving Target Defense (MTD) technique and a real-time attacker-confusing model. This model ensures security and reliability of the data transmitted during V2V communication on a highway. A traffic flow model relying on Nagel-Schreckenberg rules for Cellular Automata (CA) is used to generate the base for road mapping, and vehicle behavior patterns including location and speed [6, 7]. The proposed traffic flow model introduces a group of random vehicles moving in a two-lane highway. The proposed model applies a runtime

diversification mechanism for signals transmitted between random source and destination by controlling the active relays "vehicles" across the path.

This model aims to increase the attacker's confusion through a multi-dimensional diversity employment across time and space. The spatiotemporal diversification is introduced by run-time content manipulation, path alternation, and data granularity change. In time, the system alternate between real and fake data sources to obfuscate the transmitted content. Further, the system changes the data chunk granularity. In space: the system uses a real-time shuffler to establish random paths depending on the vehicle's position across the road lanes. The goal is to distribute the users' data (real/fake) over the entire physical space. Such diversification makes it almost impossible for an eavesdropper to get meaningful portion of the transmission.

In this paper, a mathematical model with detailed mathematical derivation is built to define and organize the V2V manipulations over the available road lanes. Furthermore, our motivation is to strike a security versus reliability trade off (SRT) in V2V cooperative systems. Therefore, this model induces enough confusion to the eavesdropper and complicates the signal tracking in the runtime to enhance the system security and reliability.

Further, we used Channel secrecy to evaluate the system effectiveness. Channel secrecy was presented by [8] to determine the relationship between the channel capacity of the main link (from source to destination) and the wiretap link (from source to eavesdropper). Recently, many studies focus on studying various techniques for selecting the best communication relays and its influence on the system's channel secrecy. Various studies presented different systems like Decode-and-Forward (DF) and Amplify-and-Forward (AF) that depend on selecting the optimal number of vehicular transmission relays and showed their influence on the channel secrecy and intercept probability without a direct link [9]. In this paper, we assumed the direct transmission model across dynamic multi-paths relayed communication via vehicles traveling on a multi-lane road.

The main contributions of this paper can be summarized as follow:

- Presenting a spatiotemporal moving-target defense that uses a mixture of real and fake data scattered via diversified paths relayed via traveling vehicles across multiple lane roads.
- Derive a mathematical closed-form expression for the channel-secrecy capacity, outage probability, and intercept probability for the proposed direct transmission model with fake/real data alternation.

- Evaluating the proposed system security by measuring the induced level of confusion, followed by a case study for the intercept probability, the channel secrecy capacity, outage probability and SRT.
- Studying different data transmission scenarios with respect to the channel secrecy capacity and the intercept probability in V2V communication.

The paper is organized as follows: Section 2 describes the threat model of the proposed security model. Section 3 describes the proposed V2V single/dual-hop cooperative system model, using moving target defense through the diversification of dynamic multi-paths followed with the fake data injection mechanism. Section 4 illustrates the security evaluation of our proposed system model with a detailed derivation of the used mathematical equations. Section 5 presents numerical results to confirm the advantages of our proposed V2V system. Finally, the conclusion of the presented work is in Section 6.

2 Threat Model

In vehicular communication environment, there are various kinds of attackers including Compromised-Key Attack, Eavesdropping, Man-in-Middle attack, and Denial-of-Service attack [10]. Most of these attacks are either passive attackers by which they can hear the data and observe the operation without interfering with the working system, or active attackers who usually intend to severely change the transferred data preventing legitimate users to access or use it.

In this work, we propose a multi-dimensional MtD against attacks relying on the static nature of wireless communication regardless of their objectives. We assume a powerful eavesdropper where attacker exists in a multiple locations across the road. In this scenario, eavesdropper can act as normal user remotely controlling multiple vehicles across the road.

In the proposed model, we present a multi-dimensional MtD manipulating wireless transmission across time and space. The presented approach uses fake/real data injection, path diversification, data size change. Thereby, it will be very hard for a powerful attacker to determine the path where the data chunks are sent. Even if he succeeded to determine some of the used paths, he won't determine the rest because of the frequent dynamic behavior change of the model. Moreover, in case the attacker was able to obtain any of the sent data chunks, he will not be able to distinguish whether the obtained the fake or real one.

3 System Model

In this section, a dynamic data transmission scenario in V2V systems is presented based on a MTD mechanism. Figure 2 shows how the source vehicle communicates with the destination vehicle by exploiting the nearby moving vehicles on the highway. It depicts how each vehicle negotiates with its neighbors to find the nearest vehicles in order to build diverse paths to create a moving target defense system. These paths vary at each time instant according to a certain lookup table that is filled from the dynamic traffic flow model presented in Section 3.1. Each path might consist of a single or multiple vehicles to assist the data transmission from the source to destination. The objective of this identification lookup table is to determine the distance between the nearby vehicles. In other words, vehicles can communicate with the closest vehicle if the separated distance between them was less than a maximum tolerance. Moreover, this model, unlike the traditional broadcast signals, offers an additional beneficial advantage, which is the network congestion reduction.

3.1 Vehicular Traffic Flow Cellular Automata Model

Nagel-Schreckenberg rules describe a group of vehicles moving on a highway, composed of two crossable lanes. During the simulation running, the vehicles behavior across the road including their updated velocities and positions are calculated. The simulated road is assumed to be with length (*L*) cells. Either zero or only one vehicle occupies each cell of the road at different time instants. The model constrains that the vehicles velocity cannot exceed a specified maximum velocity (V_{max}). During the simulation time, any vehicle (i) on the road is defined by its position (X_i) and velocity (V_i). The empty sites in front of the i^{th} vehicle; i.e. gap between any two consecutive vehicles is denoted by $d_i(t) = X_{i+1} - X_i - 1$. The movement of vehicle (*i*) from time step *t* to $t + 1$ is then defined by Nagel-Schreckenberg model four rules as follow:

$$Acceleration : V_i(t) = min(V_i(t) + 1, V_{max}) \quad (1)$$

$$Deceleration : V_i(t) = min(d_i(t), V_i(t)) \quad (2)$$

$$Randomizedbraking : V_i(t+1) = min(V_i(t) - 1, 0) \quad (3)$$

$$Movement : X_i(t+1) = X_i(t) + (V_i(t+1) \quad (4)$$

At each discrete time step t to $t + 1$, both the position and velocities of all the vehicles must be updated. During the vehicles movement across the road, they

might change their location from one lane to the other. The rules for updating the vehicles location with respect to the road lanes is as follows [6]:

$$Incentive\ criterion : V_i(t) = min(V_i + 1, V_{max} \tag{5}$$

$$Safety\ constraint\ 1 : d_{pred} > d_i \tag{6}$$

$$Safety\ constraint\ 2 : d_{succ} > d_{safe} \tag{7}$$

where d_{pred} and d_{succ} are the gaps between the targeted vehicle (i) and the preceding vehicle and the succeeding vehicle in the target lane respectively; and d_{safe} is the maximum possible gap of the preceding and succeeding vehicles in the target lane. Figure 3, shows a detailed flow chart of the described traffic flow model.

3.2 Benign Employment Real Fake Data Mechanism

This section presents a dynamic data transmission scenario in V2V systems based on two different security levels, MTD and benign employment for real and fake data.

Figure 1 shows a schematic diagram of multi-hop direct transmission scenario consists of a single source (requested vehicle) S and multi-vehicles

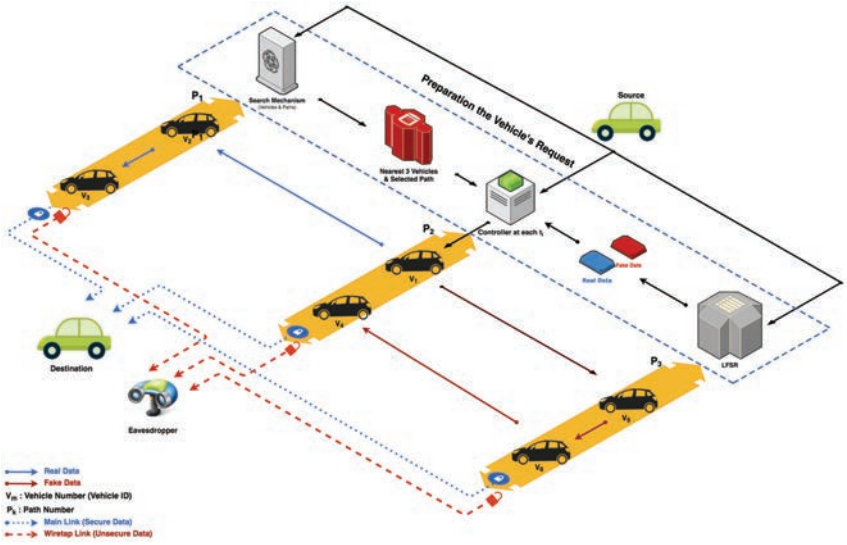

Figure 1 Benign Employment Real Fake Data Mechanism system Model in presence of an eavesdropper.

which assist requested vehicle (source) to deliver the transmitted signal to its legitimate destination securely. Due to the wireless nature and the broadcast process, the eavesdropper may be able to overhear some or all the transmitted data based on his capabilities. Our scenario considers the worst case which composed of multi-eavesdroppers whom cooperate together to catch meaningful information.

From Figure 1, it's obvious that the system operates on two channels: the main channel from the source vehicle to the destination vehicle, and a wiretap channel from source vehicle to any illegal user (Eavesdroppers).

The source node transmits the message to the legitimate destination node using M different hops (based on the assisted vehicles on the selected path) as demonstrated in Figure 2. In the first hop, source node request to send data to selected vehicle at time instant t_i, the controller start to search about the nearest three vehicles at each time instant t_i. Consequently, a shuffling sequence of the transmitted data alternate between real and fake data based on the dynamic

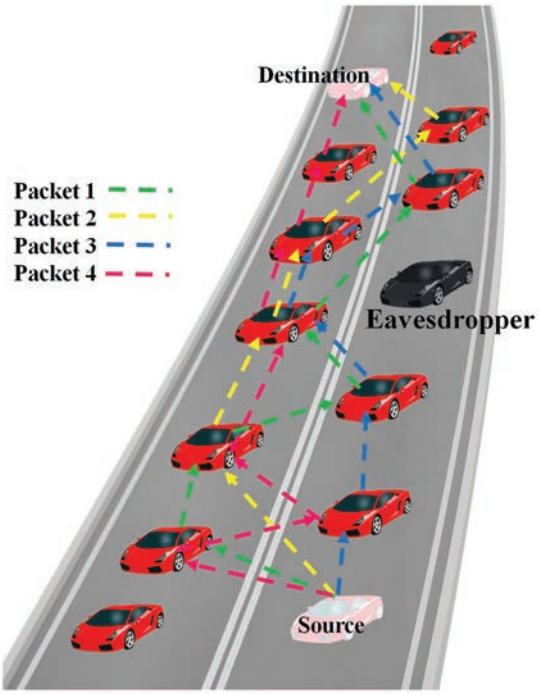

Figure 2 A simple V2V communication scenario based on diversification active paths in presence of an eavesdropper.

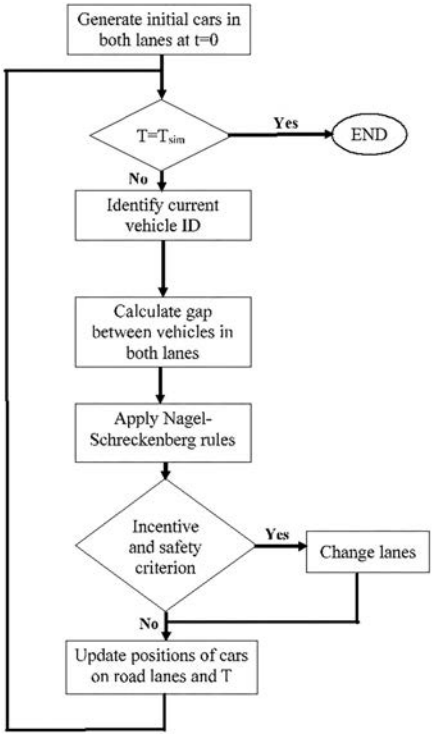

Figure 3 Proposed traffic flow model flow chart.

filled table from Linear Feedback Shift Register (LFSR). From this context, the controller decides the second hob to transmit data (either Coarse-grained Chunks or Fine-grained Chunks). The number of total hobs decided based on the search engine at each time instant to select the best candidate in the transmission process. Generally, our system model composed of L vehicles existed on different 2 lanes to create I paths.

In Coarse-grained Chunks data, source node divides its message to elements and sends every element to distinct directional path during every part covering disjoint space instead of broadcasting them. Figure 1 depicts that the source start to multi-casting the partial signals $x_{s,q}$ in each hob, towards a various paths $P_p|P = 1, 2, \ldots, I$ where q is the Coarse-grained Chunks data. Each hob denotes to the total number of used vehicles that it has in multi-hob direct transmission.

Whereas during the Fine-grained Chunks data, source select a specified path and transmit data as whole bulk. Figure 1 depicts that the source node

start to multi-casting the whole signal $x_{s,z}$ in each hob, towards a certain path $P_p|P = 1, 2, \ldots, I$, where z is the Fine-grained Chunks data. Each hob denotes to the total number of used vehicles that it has in multi-hob direct transmission.

We will investigate two various scenarios for these chunk data. When these untrusted existed vehicles try to attack the received partial messages individually; or these untrusted existed vehicles work together to intercept the arrived message at the destination.

For simplicity, in the analysis, we assume that we have five different paths to transmit the partial messages. The trusted fading channels assumed to be frequency-flat fading which denoted by h_{sd} modeled as a Gaussian random variable with mean μ_{sd} and a variance σ^2_{sd}. The fading channels from source node at the each hob at each time instant t_i towards p-paths is denoted by h_{sd_i}. while, the untrusted fading channels assumed to be frequency-flat fading which denoted by h_{se} modeled as a Gaussian random variable with mean μ_{se} and a variance σ^2_{se}. The fading channels from source node towards eavesdropper is denoted by h_{se}. Additionally, the channel gains h_{sd_i} and h_{se} are independent and identically distributed (iid) with exponentially random variable distribution. Finally, we have additive white Gaussian noise in all transmission hobs with the same variance N_o.

4 The Proposed Security Evaluation Model

4.1 Proposed Vehicle-to-Vehicle Confusion Sequence Description

As mentioned before, a real-time diversification is realized by giving the source vehicle the right to send the transmitted signals through multiple paths relayed through the surrounding selected vehicles. At each time instant, **spatial diversity** is induced by manipulating the path selection of the available vehicles. While, **temporal** diversity is induced by the aid of the dynamically generated Look-Up Table (LUT).

The proposed security model uses the dynamic time-based LUT randomly filled with the available nearby vehicles in both lanes. Such randomization dynamically assigns different paths for the packets to be transmitted in this time slot. The dynamic change of such table, and the continuous change in the vehicles positions increase the level of confusion to a great extent.

Figure 4 shows a flowchart for the proposed model, which is used to fulfill the dynamic LUT. For better understanding the proposed model, Table 1 shows an illustrative example for different vehicle availability in the road lanes and

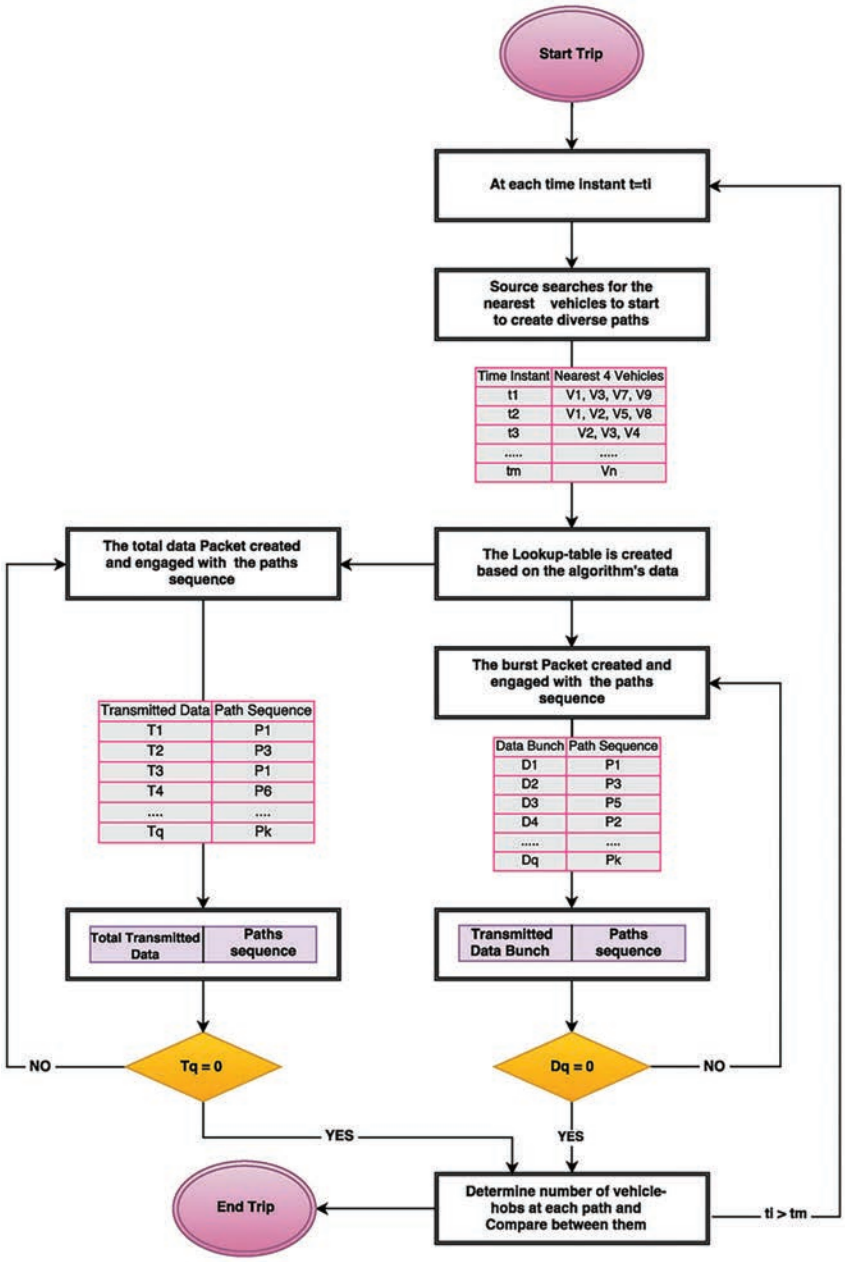

Figure 4 Flowchart of data and paths shuffling of V2V system during different time instant.

Table 1 Example of channel priorities for sending the Real (R) and Fake (F) data

Time Instant t_i	Nearest Vehicles	Data Chunk	Path Sequence	Priority
t_1	V_1, V_3, V_7, V_9	D_q	P_1, P_2, P_3	R
t_2	V_1, V_2, V_5, V_8	T_q	P_1	F
t_3	V_2, V_3, V_4	T_q	P_5	R
..	..	..	..	..
..	..	..	..	..
t_N	V_L	D_q/T_q	P_I	R/F

how they are used to fill the LUT, creating the random paths. The selected vehicles as relays in the LUT are based on the nearest vehicles in both lanes. The appropriately engaged vehicles are used to build adequate and possible paths with single/multi vehicle-hops. To increase the depth of confusion, we consider two scenarios where we change the data representation granularity. We use coarse grained and fine grained data chunks.

4.2 Randomization Procedure

The shuffling sequence of the transmitted data changes in both time and frequency directions over the available channel spectrum. Moreover, the priority of sending real data in the different channel spectrum changes at each time instant according to the shuffling sequence of the LFSR.

To better understand the proposed shuffling model, Table 2 shows an illustrative example of the different paths-availability and how they are filled according to the generated data traffic sequence at each time instant.

Based on the nearest vehicles and the appropriate created paths at each time slot, the dynamic LUT is generated to determine whether the system will send real or fake data, or both (in case there is more than one available path). This LUT is filled using a shift for LFSR contents at each time instance. The channel priority assignment is based on the LFSR contents.

We use Confusion Factor (CF) to indicate how much harder for an eavesdropper to synchronize his pattern and attack-window to eavesdrop/intercept the transmitted data.

As per the number of manipulations induced over time and space increase, cracking this pattern becomes almost impossible for anyone with no pre-knowledge of the system's real-time configuration pattern. Therefore, based on the DBF technique and the illustrated MTD security model, we have multiple-security levels which makes the interception process almost tends to zero.

Next section presents the security derivation for the proposed system model with Single and Multi Eavesdropper's availability and with the above-mentioned MTD randomization technique.

5 Security Evaluation

This section presents a traditional wireless system model and analyzes the SRT in the Rayleigh fading channels. In Figure 1 source node at each hob transmits a signal by transmitting power P_t and data rate R_d given by the Shannon capacity.

The physical layer security improvement by using C_s was examined by authors in Ref. [8, 11–18]. Typically, the transmission system is secure when the destination node can reliably communicate with the source node, while eavesdropper fails to decode the transmitting signal. To be specific, due to the broadcast nature, eavesdropper might succeed to overhear and decode the transmitted signal *x*, which is transmitted by power P_t and rate R_d.

5.1 Single Eavesdropper

According to Wyner's results [8] and Shannon capacity [19], the main channel secrecy capacity C_{sd} at each node (at each hop) is given by the following equation:

$$C_{sd} = log_2\left(1 + |h_{sd}|^2 \frac{\gamma}{d_{sd}^a}\right), \tag{8}$$

where, $\gamma = P_t/\sigma_n^2$, is the Signal to Noise Ratio (SNR). The total channel secrecy capacity from source node to the desired destination node is given by

$$C_{sd_{tot}} = \sum_{p=1}^{I}\sum_{i=1}^{T} log_2\left(1 + |h_{sd_{(i,p)}}|^2 \frac{\gamma}{d_{sd_p}^a}\right), \tag{9}$$

Similarly, the wiretap channel secrecy capacity C_{se} is given by the following equation:

$$C_{se} = log_2\left(1 + |h_{se}|^2 \frac{\gamma}{d_{se}^a}\right), \tag{10}$$

(1) ***Security Analysis:*** The intercept event occurred when the wiretap capacity C_{se} becomes higher than the data rate R_d [8, 19]. Therefore, the intercept probability $(P_{intercept})$ of the direct transmission is described as follow

$$P_{intercept} = P_r(C_{se} > R_d), \tag{11}$$

By substituting Equation (10) in Equation (11), the intercept probability becomes

$$P_{intercept} = P_r(|h_{se}|^2 > (\alpha\, d_{se}^a)), \tag{12}$$

where, $\alpha = (2^{R_d} - 1)/\gamma$. Let $\Gamma_2 = \alpha d_{se}^a$. Since $|h_{se}|^2$ follows an exponential distribution, the intercept probability becomes as follow

$$P_{intercept} = \exp\left(-\frac{\Gamma_2}{\sigma_{se}^2}\right), \tag{13}$$

(2) ***Reliability Analysis:*** As shown in the previousequations, when R_d increases (or P_t decrease), the systemsecurity should be improved; i.e, the intercept probabilityreduces. Such improvement will overcome the cost of transmission reliability degradation; i.e, outage probability increases. specifically, the outage probability of the mainlink increases, when R_d increases.
Therefore, the outage probability (P_{out}) of a direct transmission from main link [19] is obtained as follows

$$\begin{aligned} P_{out} &= P_r(C_{sd_{tot}} < R_d) \\ &= P_r\left(\sum_{p=1}^{I}\sum_{i=1}^{T}|h_{sd_{(i,p)}}|^2 > (\alpha\, d_{sdp}^a)\right), \\ &= 1 - \prod_{p=1}^{I}\exp\left(-\frac{\Gamma_{1_p}}{\sigma_{sd}^2}\right), \end{aligned} \tag{14}$$

where, $\Gamma_1 = \alpha d_{sd_p}^a$. Combining Equations (13) and (14) yields to

$$P_{out} = 1 - (P_{intercept})^{(\Gamma_p \sigma_{se}^2/\sigma_{sd}^2)} * \prod_{p=2}^{I-1}\exp\left(-\frac{\Gamma_{1_p}}{\sigma_{sd}^2}\right), \tag{15}$$

where, $\Gamma_p = \Gamma_{1p}/\Gamma_2$ is the distance ratio between the $S-D$ and $S-E$ links. For simplicity, we assumed that the main link $|h_{sd}|^2$ and wiretap link $|h_{se}|^2$ are independent and identically distributed (i.i.d.) random variables.

In this paper we denote the ratio between the channel gain of the main to wiretap links by $\lambda_{me} = \sigma_d^2/\sigma_e^2$. Throughout this paper, we refer to λ_{me} as the main-to-eavesdropper ratio *(MER)*. Thereof we can simplify Equation (15) by the following

$$P_{out} = 1 - (P_{intercept})^{(\Gamma_p/\lambda_{me})} * \prod_{p=2}^{I-1}\exp\left(-\frac{\Gamma_{1_p}}{\sigma_{sd}^2}\right), \tag{16}$$

where $0 \leq P_{intercept} \leq 1, \lambda > 1$, and $\Gamma > 0$. It is observed from Equation (16) that any increase in $P_{intercept}$ will reduce P_{out}. This proves the tradeoff relation between the security and reliability. SRT essentially hinges on λ_{me}, Γ and the number of paths, but it is independent of P_t and R_d. Therefore, as the distance ratio Γ increased, the OP significantly increased. Moreover, when we select more paths to transmit data between transmitter and receiver, the intercept probability will be decreased in case of coarse-chunk data. Specifically, as the exploited active paths increase the attacking process will be harder, as per if the attacker succeed to select the correct path with real data; which is difficult process and required much time, he will catch non meaningful data. On the other hand, as we send different data on different paths, the overall rate will be increased. This approach not applicable in long distance separations as per the direct transmission failed to sustain the requirements. Therefore, our assumption is valid in this scenario as the distances between vehicles on the road is relatively small.

5.2 Multi Eavesdropper

According to Wyner's results [8] and Shannon capacity [19], the main channel secrecy capacity C_{sd} at each node (at each hop) is given by the following equation:

$$C_{sd} = log_2 \left(1 + |h_{sd}|^2 \frac{\gamma}{d_{sd}^a}\right), \tag{17}$$

where, $\gamma = P_t/\sigma_n^2$, is the Signal to Noise Ratio (SNR). The total channel secrecy capacity from source node to the desired destination node is given by

$$C_{sd_{tot}} = \sum_{p=1}^{I} \sum_{i=1}^{T} log_2 \left(1 + |h_{sd_{(i,p)}}|^2 \frac{\gamma}{d_{sd_p}^a}\right), \tag{18}$$

Similarly, the wiretap channel secrecy capacity C_{se} is given by the following equation:

$$C_{se} = log_2 \left(1 + |h_{se}|^2 \frac{\gamma}{d_{se}^a}\right). \tag{19}$$

The total channel secrecy capacity from source node to the eavesdropper to consider the worst case scenario is given by

$$C_{se_{tot}} = \sum_{k=1}^{K} log_2 \left(1 + |h_{se_k}|^2 \frac{\gamma}{d_{se_k}^a}\right), \tag{20}$$

Where, *K* is the number of active cooperated eavesdropper, $k = 1, 2, 3, \ldots, K$

1) ***Security Analysis:*** The intercept event occurred when the wiretap capacity C_{se} becomes higher than the data rate *Rd* [8, 19]. Therefore, the IP $P_{intercept}$ of the direct transmission is described as follow

$$P_{intercept} = Pr(C_{se_{tot}} > R_d), \tag{21}$$

By substituting Equation (19) in Equation (21), the IP becomes

$$P_{intercept} = \sum_{k=1}^{K} P_r(|h_{se_k}|^2 > (\alpha\, d^a_{se_k})), \tag{22}$$

where, $\alpha = (2^{R_d} - 1)/\gamma$. Let $\Gamma_{2_k} = \alpha d^a_{se_k}$. Since $|h_{se_k}|^2$ follows an exponential distribution, the IP becomes as follow

$$P_{intercept} = \prod_{k=1}^{K} \exp\left(-\frac{\Gamma_{2_k}}{\sigma^2_{se_p}}\right), \tag{23}$$

2) ***Reliability Analysis:*** As shown in the previous equations, when R_d increases (or P_t decrease), the system security should be improved; i.e, the IP reduces. Such improvement will overcome the cost of transmission reliability degradation; i.e, OP increases. specifically, the OP of the main link $(S - D)$ increases, when R_d increases.
Therefore, the OP P_{out} of a direct transmission from $S - D$ link [19] is obtained as follows

$$\begin{aligned} P_{out} &= P_r(C_{sd_{tot}} < R_d) \\ &= P_r\left(\sum_{p=1}^{I}\sum_{i=1}^{T} |h_{sd_{(i,p)}}|^2 > (\alpha\, d^a_{sdp})\right), \\ &= 1 - \prod_{p=1}^{I} \exp\left(-\frac{\Gamma_{1_p}}{\sigma^2_{sd}}\right), \end{aligned} \tag{24}$$

where, $\Gamma_1 = \alpha d^a_{sd_p}$. Combining Equations (23) and (24) yields to

$$\begin{aligned} P_{out} &= 1 - (P_{intercept})^{(\Gamma_r \sigma^2_{se}/\sigma^2_{sd})} \\ &\quad * \prod_{p=2}^{I-1} \exp\left(-\frac{\Gamma_{1_p}}{\sigma^2_{sd}}\right) * \prod_{k=2}^{K-1} \exp\left(-\frac{\Gamma_{2_k}}{\sigma^2_{sd}}\right), \end{aligned} \tag{25}$$

where, $\Gamma_r = \Gamma_{1_p}/\Gamma_{2_k}$, is the distance ratio between the $S-D$ and $S-E$ links.

In this paper we denote the ratio between the channel gain of the main to wiretap links by $\lambda_{me} = \sigma_{sd}^2/\sigma_{se}^2$. Throughout this paper, we refer to λ_{me} as the main-to-eavesdropper ratio (MER). Thereof we can simplify Equation (25) by the following

$$P_{out} = 1 - (P_{intercept})^{(\Gamma_p/\lambda_{me})} * \prod_{p=2}^{I-1} \exp\left(-\frac{\Gamma_{1_p}}{\sigma_{sd}^2}\right) * \prod_{k=2}^{K-1} \exp\left(-\frac{\Gamma_{2_k}}{\sigma_{se}^2}\right). \quad (26)$$

where $0 \leq P_{intercept} \leq 1, \lambda_{me} > 0$, and $\Gamma > 0$. It is observed from Equation (26) that any increase in $P_{intercept}$ will reduce P_{out}. This proves the tradeoff relation between the security and reliability. SRT essentially hinges on λ_{me}, Γ, the number of paths and the number of active eavesdroppers, but it is independent of P_t and R_d. Therefore, its obviously that as the number of used paths increased, the attacker probability to intercept meaningful information becomes harder. Whenever, as the number of the active eavesdroppers increased the intercept probability will be increases.

6 Results

This section demonstrates the simulation results, showing the performance of the proposed V2V system model with Monte Carlo simulation. Table 2 shows the detailed parameters used in this model. Using Nagel-Schreckenberg model, the vehicles capacity within the road cells can be determined at any time instant during the simulation running. Figure 5, shows the calculated road capacity during the simulation time. These values are important for the estimation of the possible paths between the vehicles for successful file transmission.

AS we mentioned before, the main target of our model is to confuse the attacker and harden the process of obtaining the transmitted data chunks.

Table 2 Simulation Parameters

Parameters	Value
Road Length (L)	1000 cells
Number of road lanes	2 lanes
Maximum car velocity (V_{max})	5 cells
Minimum transmission rate (Rd)	2 bits/S/Hz

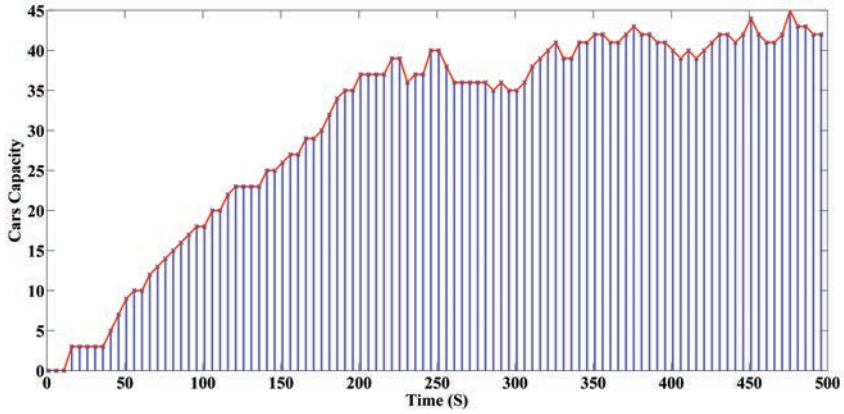

Figure 5 Vehicles capacity within the road lanes.

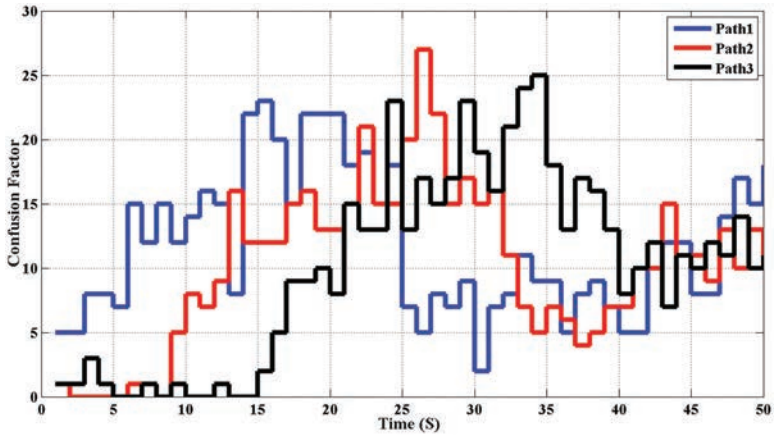

Figure 6 Vehicles capacity within the road lanes.

Confusion Factor (CF) is defined as metrics often used by researchers working in the encryption domain to evaluate the strength of their mechanisms. It mainly measures the complexity level for the attacker to attack the signals. The attacker may succeed to overhear the transmitted data if he follows the same variation of the CF pattern.

Figures 6 and 7 depict the CF of the calculated paths at certain time instant (ti) using a certain numerical algorithm. It is obvious that each path varies dynamically according to the available vehicles in each lane based on the generated lookup table data. Wherein, CF is obtained from the selection

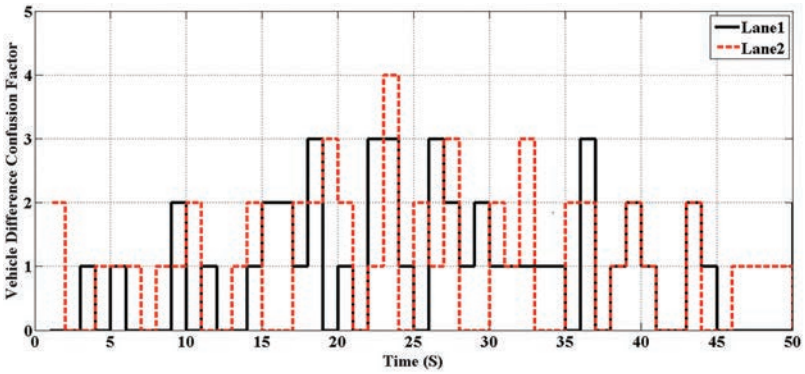

Figure 7 Vehicles capacity within the road lanes.

of random paths; there is no clue which path is better than the other. In the proposed scenario, the exploited randomization technique resulted in a maximum variation points shown in the CF graph belongs to path 2. While, random vehicles in path 1 follow a different pattern which make path 2 and path 3 have higher CF. Figure 6 shows the variations of CF during the whole trip from lane 1 to lane 2 cross a different random selected paths.

Figure 7 illustrates the variation difference in CF for the vehicle hops for each lane at any time instant. In other words, the CF of the vehicles variation in both lanes at any time is calculated to utilize whether the transmitted data type was fine- or coarse-grained. Although the increase of the CF leads to significant channel secrecy enhancement, the system reliability decreased. We discuss the channel secrecy and system reliability for the proposed V2V system next.

In order to determine the proposed system performance, the intercept probability for the two data transmission scenarios is depicted in Figure 8. It shows that the intercept probability of the proposed V2V system model in case of fine-grained chunks of data, is better than coarse-grained chunks of data. Additionally, it can be noticed that the intercept probability is decreasing in a uniform fashion with respect to the MER increase.

Figure 9 illustrates the outage probability of our proposed V2V system model for both data transmission scenarios. This figure shows that the outage probability in case of data transmission as a coarse-grained chunk through a single path, is better than representing it as a set of fine-grained chunks sent through multi-paths. Wireless channel problems such as scattering and fading is the main reason behind that. The fine-grained data chunks will face

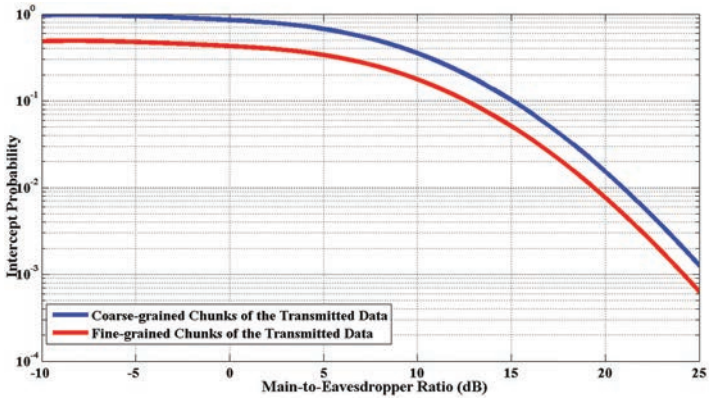

Figure 8 Vehicles capacity within the road lanes.

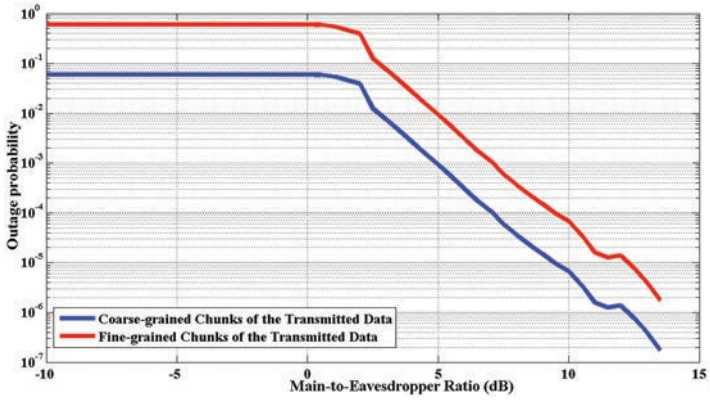

Figure 9 Vehicles capacity within the road lanes.

more difficulties and high chance of failure reducing the overall reliability. The outage probability follows different pattern than the intercept probability with the variation of MER. The outage probability decreases with the increase of MER.

6.1 Single Eavesdropper

Figure 10 illustrates the proposed V2V ergodic channel secrecy capacity comparison between our presented system model in [20] and our new real/fake data injection; taking into consideration the aforementioned two scenarios of the transmitted data in case of single eavesdropper; i.e. coarse-grained and

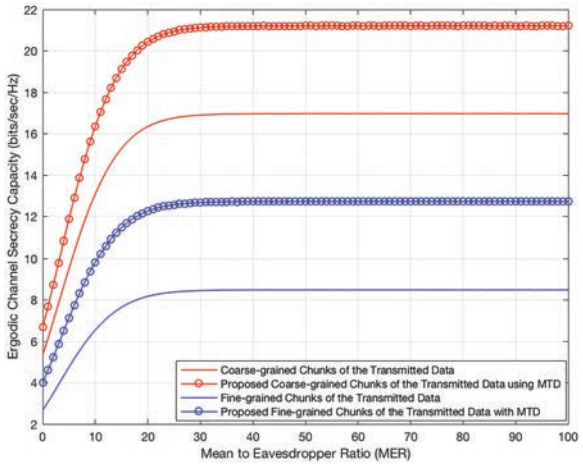

Figure 10 Ergodic channel secrecy capacity C_S versus MER of proposed V2V model, comparison of proposed system model with different transmitted data type using Real/Fake data injection in case of single eavesdropper.

fine-grained data chunks. Figure 10 demonstrates that the channel secrecy capacity is enhanced in case of transmitting data as fine-grained chunks using multi-paths from the source to the destination vehicles. Moreover, the benign employment of real/fake data asset the rose improvement in the overall channel secrecy capacity as it increases the attacker window which reduces its opportunity to attack the real data in the appropriate path. This confirms that if the eavesdropper succeeds to pick up a certain path (data flow), it is very difficult to be able to pick the rest of the data. Therefore, the picked data will not be understandable for him. From this context, our proposed model achieves highest channel secrecy capacity in case of transmitting Coarse-grained chunks using the above-mentioned spatiotemporal diversity approach.

Figure 11 depicts the intercept probability for the two data transmission scenarios. It shows that the attacker opportunity to attack a meaningful data in the illustrated V2V system model in case of alternate between real/fake data injection is mere reduce. Furthermore, it's obvious from Figure 11 that the intercept probability of multi-cast the transmitted data as fine-grained chunks, is lower than coarse-grained chunks of data whether in case of real-time shuffler to alternate between the injected fake data or without it. Additionally, it can be noticed that the intercept probability is decreasing as the

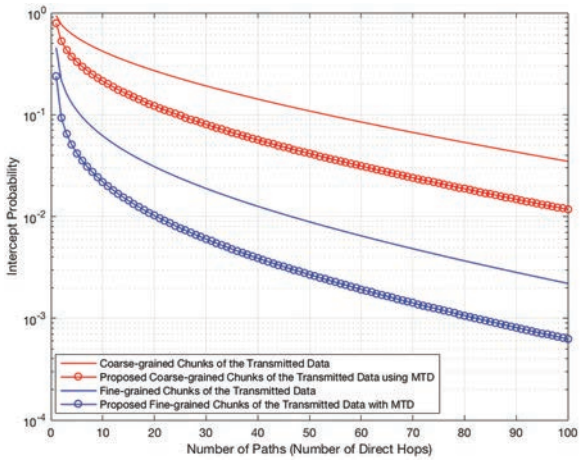

Figure 11 Intercept probability $P_{intercept}$ versus the number of used paths $I - Paths$ of Proposed V2V model, comparison of proposed system model with different transmitted data type using Real/Fake data injection in case of single eavesdropper.

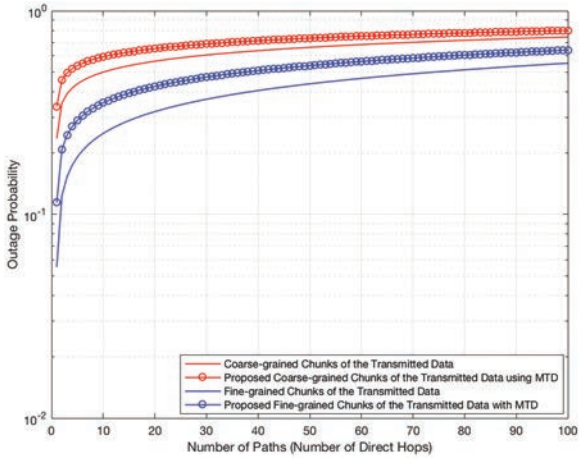

Figure 12 Outage Probability P_{out} versus the number of used paths $I - Paths$ of Proposed V2V model, comparison of proposed system model with different transmitted data type using Real/Fake data injection in case of single eavesdropper.

number of selected paths increased as per the attacker window of opportunity increased too.

Figure 12 illustrates the outage probability of our proposed V2V system model for both data transmission scenarios and compare between the previous

presented model in [20] and the real-time fake data injection. This figure shows that the outage probability is significantly increased as the number of used paths increase as per the probability of losing data due to the wireless channel problems is increased. This Wireless channel problems are for example scattering and fading's the main reason behind the reduction of the overall reliability. In our assumption, we consider a high way traffic vehicles, which guarantees that the distance between each consecutive vehicles is relatively small. From this context, the tradeoff between the security and reliability become a vital role. How can we transmit data between legitimate users securely with a good overall system reliability? Therefore, we study this tradeoff relation and compare it with the previous approach.

Figure 13 presents the trade-off relation between the outage and intercept probability in the proposed V2V system model. The outage probability from Equation 14 is inversely proportion with the number of used paths, thereof as the number of used paths increased the overall system reliability decreased. Additionally, if we injected much fake data, the eavesdropper will be confused and the confusion factor will be increased but the overall rate will be reduced. Therefor, it's obviously that Figure 12 follow the opposite direction of Figure 11. The fine-grained data chunks will face less difficulties and small chance of failure increasing the overall reliability.

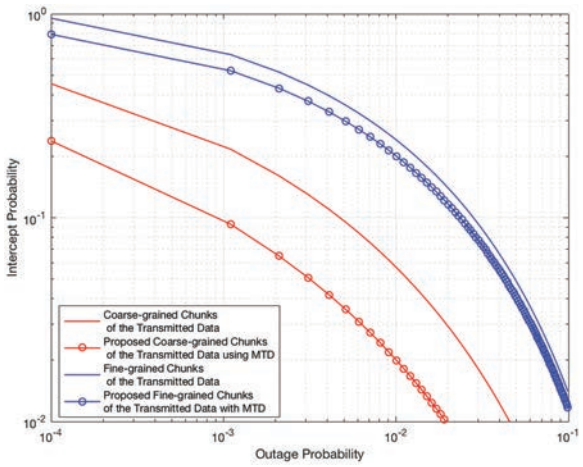

Figure 13 Intercept probability $P_{intercept}$ versus Outage Probability P_{out} of Proposed V2V model, comparison of proposed system model with different transmitted data type using Real/Fake data injection in case of single eavesdropper.

Therefore, Figure 13 shows that while the intercept probability increases, the outage probability decreases, and vice versa. In other words, when the CF increases the secrecy is much better, but the overall system reliability is reduced. With the increase of the eavesdropper's confusion probability as the CF increases, the probability of data lost due to the fading nature of the channel also increases. Therefore, the outage probability increase as the CF increase.

Security at the physical layer is usually less costly than the upper layers and stronger as well. However, that might come with a cost on the reliability. The reliability here referees the physical channel. The negative effect on the reliability shown in the figures, can be compensated-for by reliable data transfer at the transport layer. Indeed, this will add to the traffic load. However, it may be a reasonable price to pay for the added security.

6.2 Multi Eavesdropper

Figure 14 illustrates the proposed V2V ergodic channel secrecy capacity comparison between our presented system model in [20] and our new real/fake data injection; taking into consideration the aforementioned two scenarios of the transmitted data in case of single eavesdropper. Figure 10 demonstrates that the channel secrecy capacity is lower than the channel secrecy capacity illustrated in Figure 10 as per the wiretap channel increased due to the cooperation between $K - eavesdropper$ to catch more data than it was only

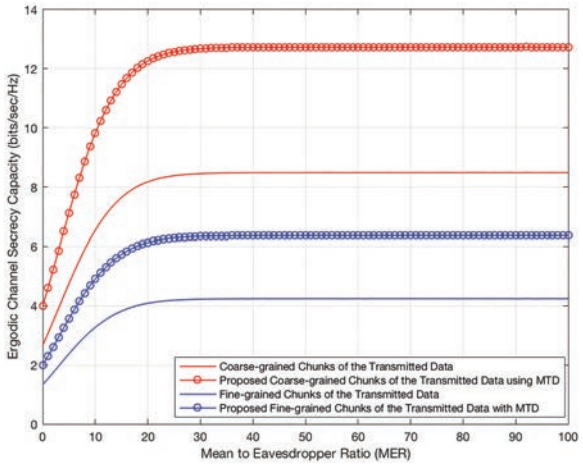

Figure 14 Ergodic channel secrecy capacity C_S versus *MER* of proposed V2V model, comparison of proposed system model with different transmitted data type using Real/Fake data injection in case of multi eavesdropper.

single eavesdropper. However, the presented system model combine between two different level of security; benign employment of real/fake data injection with multi-casting the transmitted data using Coarse-grained chunks increase the overall channel secrecy capacity even with k-eavesdroppers. This injection increases the attacker window which reduces its opportunity to attack the real data in the appropriate path. This confirms that if the cooperated eavesdroppers succeed to overhear a certain path (data flow), it is difficult to be able to pick the rest of the data. Therefore, the selected data will not be understandable to them. From this context, our proposed model achieves the highest channel secrecy capacity in both cases either with single or multi eavesdroppers using the above-mentioned **spatiotemporal diversity** approach.

Figure 15 depicts the intercept probability for the two data transmission scenarios in case of existing multi eavesdroppers. It shows that the attacker opportunity to attack a meaningful data in the illustrated V2V system model in case of alternate between real/fake data injection is merely reduced but with the increment of the cooperated eavesdroppers, the increament of their opportunity to overhear almost most of the transmitted data. Furthermore, it's obvious from Figure 15 that the intercept probability of multi-cast the transmitted data as fine-grained chunks, is lower than coarse-grained chunks of data whether in case of real-time shuffler to alternate between the injected fake data or without it. On the words, when $K \rightarrow \infty \Rightarrow P_{intercept} \rightarrow 1$.

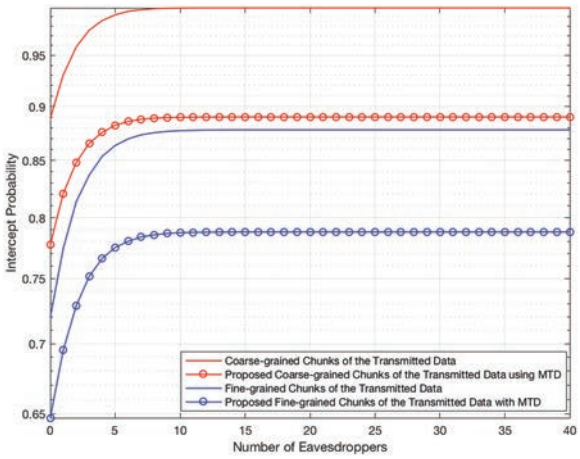

Figure 15 Intercept probability $P_{intercept}$ versus the cooperated eavesdroppers $K - eavesdropper$ of proposed V2V model, comparison of proposed system model with different transmitted data type using Real/Fake data injection in case of multi eavesdropper.

Figure 13 presents the trade-off relation between the outage and intercept probability in the proposed V2V system model. The outage probability from Equation (26) is inversely proportion with the number of used paths and the intercept probability is directly proportional with the number of active eavesdroppers, thereof as the number of used paths increased the overall system reliability decreased. Whereas when the number of active eavesdroppers increased, the probability of attack a meaningful data increased, then the overall intercept probability will be increased. Additionally, if we injected many fake data, the eavesdropper will be confused and the confusion factor will be increased but the overall rate will be reduced.

Therefore, Figure 16 shows that while the intercept probability increases, the outage probability decreases, and vice versa. Comparing Figure 13 with Figure 14, its clearly appeared the when the active eavesdropper whom cooperated with each others increase, the intercept probability will be increase, then the overall security versus Reliability will be worse than the tradeof relation illustrated in Figure 13. In other words, when the CF increases the secrecy is much better, but the overall system reliability is reduced. With the increase of the eavesdropper's confusion probability as the CF increases, the probability of data lost due to the fading nature of the channel also increases. Therefore, the outage probability increase as the CF increase.

Therefore, as a conclusion, From Equation 26 its obviously that as the number of used paths increase, the attacker probability to intercept meaningful

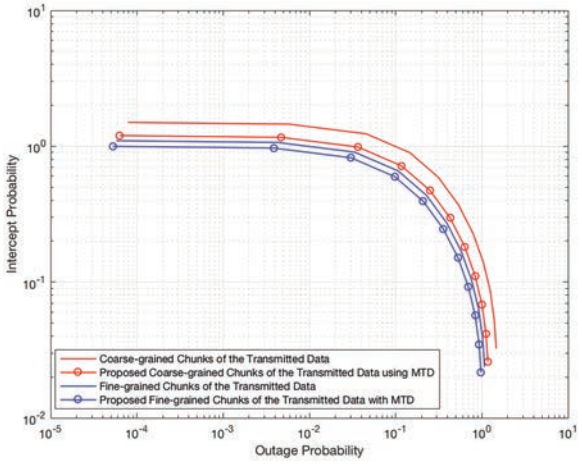

Figure 16 Intercept probability $P_{intercept}$ versus Outage Probability P_{out} of Proposed V2V model, comparison of proposed system model with different transmitted data type using Real/Fake data injection in case of multi eavesdropper.

information becomes harder. Whenever, as the number of the cooperated eavesdroppers increase the intercept probability will increases. On other words, when $I \rightarrow \infty \Rightarrow P_{intercept} \rightarrow 0$. While, when $K \rightarrow \infty \Rightarrow P_{intercept} \rightarrow 1$

7 Conclusion

This paper introduced a spatiotemporal diversity as a Moving target Defense (MtD) mechanism to secure V2V wireless communication. The presented mechanism induce MtD through, wireless communication characteristics manipulation, data transmission path diversification, data-chunk granularity change, and alternating data transmission between real and fake data sources. The goal is to obfuscate the user's data and to increase the attacker's confusion. A mathematical model was built to define and organize the V2V signal manipulations over a two-lane road. A traffic flow model based on Nagel-Schreckenberg rules for cellular automata was developed to generate the base for road mapping vehicle location and speed as a base for run-time diversification induction across time and space. Using Monte Carlo simulation, results showed that there is an inverse proportional relationship between security and reliability. Moreover, simulations showed that with the increase of diversification dimensionality the system becomes more effective. The presented MtD managed to increase the channel secrecy, attacker confusion, and minimize the intercept probability to a great extent. Our future work includes employing machine-learning mechanisms to control diversity manipulation towards optimal security and reliability tradeoff.

Acknowledgment

Authors would like to express their appreciation for the "IoT and cyber Security lab", VMI, Lexington, VA, USA and Smart-CI, Alexandria University, Egypt; for supporting and hosting the activities related to this manuscript.

References

[1] Alotaibi, E. R., and Hamdi, K. A. (2016). Secrecy outage probability analysis for cooperative communication with relay selection under non-identical distribution. In *2016 IEEE Wireless Communications and Networking Conference (WCNC)*, 1–6. IEEE.

[2] Laneman, J. N., Tse, D. N., and Wornell, G. W. (2004). Cooperative diversity in wireless networks: Efficient protocols and outage behavior. *IEEE Transactions on Information theory,* 50(12), 3062–3080.

[3] Cheng, L., Stancil, D. D., and Bai, F. (2013). A roadside scattering model for the vehicle-to-vehicle communication channel. *IEEE Journal on Selected Areas in Communications*, 31(9), 449–459.

[4] Maxemchuk, N. F., Tientrakool, P., and Willke, T. L. (2009). The role of communications in cyber-physical vehicle applications. In *Automotive Informatics and Communicative Systems: Principles in Vehicular Networks and Data Exchange*, 139–161. IGI Global.

[5] Boban, M., Barros, J., and Tonguz, O. K. (2014). Geometry-based vehicle-to-vehicle channel modeling for large-scale simulation. *IEEE Transactions on Vehicular Technology*, 63(9), 4146–4164.

[6] Bette, H. M., Habel, L., Emig, T., and Schreckenberg, M. (2017). Mechanisms of jamming in the Nagel-Schreckenberg model for traffic flow. *Physical Review E*, 95(1), 012311.

[7] Makowiec, D., and Miklaszewski, W. (2006). Nagel-Schreckenberg model of traffic–study of diversity of car rules. In *International Conference on Computational Science*, 256–263. Springer, Berlin, Heidelberg.

[8] Leung-Yan-Cheong, S., and Hellman, M. (1978). The Gaussian wire-tap channel. *IEEE transactions on information theory*, 24(4), 451–456.

[9] Ghourab, E. M., Azab, M., Feteiha, M. F., and El-Sayed, H. (2018). A Novel Approach to Enhance the Physical Layer Channel Security of Wireless Cooperative Vehicular Communication Using Decode-and-Forward Best Relaying Selection. *Wireless Communications and Mobile Computing, 2018*.

[10] Singh, C., Kaur, R., & Kaur, M. Review of security enhancement techniques for Wireless Sensor Network.

[11] Feteiha, M. F., Uysal, M., and Ahmad, A. R. (2011). Cooperative inter-vehicular communications in highway traffic. In *2011 24th Canadian Conference on Electrical and Computer Engineering (CCECE)*, 000460–000465. IEEE.

[12] Ochiai, H., Mitran, P., and Tarokh, V. (2004). Design and analysis of collaborative diversity protocols for wireless sensor networks. In *2004 IEEE 60th Vehicular technology conference, 2004. VTC2004-Fall.* 7, 4645–4649. IEEE.

[13] Ma, X., and Giannakis, G. B. (2003). Maximum-diversity transmissions over doubly selective wireless channels. *IEEE Transactions on Information Theory*, 49(7), 1832–1840.

[14] Cui, S., Goldsmith, A. J., and Bahai, A. (2005). Energy-constrained modulation optimization. *IEEE transactions on wireless communications*, 4(5), 2349–2360.
[15] Patel, C. S., Stuber, G. L., and Pratt, T. G. (2006). Statistical properties of amplify and forward relay fading channels. *IEEE Transactions on Vehicular Technology*, 55(1), 1–9.
[16] Akki, A. S., and Haber, F. (1986). A statistical model of mobile-to-mobile land communication channel. *IEEE transactions on vehicular technology*, 35(1), 2–7.
[17] Khisti, A., and Wornell, G. W. (2010). Secure transmission with multiple antennas I: The MISOME wiretap channel. *IEEE Transactions on Information Theory*, 56(7), 3088–3104.
[18] Wyner, A. D. (1975). The wire−tap channel. *Bell system technical journal*, 54(8), 1355–1387.
[19] Shannon, C. E. (2001). A mathematical theory of communication. *ACM SIGMOBILE mobile computing and communications review*, 5(1), 3–55.
[20] Ghourab, E. M., Samir, E., Azab, M., and Eltoweissy, M. (2018). Diversity-Based Moving-Target Defense for Secure Wireless Vehicular Communications. In *2018 IEEE Security and Privacy Workshops (SPW)*, 287–292. IEEE.

Biographies

Esraa M. Ghourab is one of the founders and a researcher at the IoT Cyber Security Lab, SmartCI, Faculty of Engineering, Alexandria University, Egypt. She worked with the lab team members towards a set of innovative research and business-oriented projects related to Cyber Security, Smart IoT systems, Software Defined Secure wireless communication.

She supervised young researchers working on their 1st papers. Esraa received her M.Sc in Communication Engineering, in 2018 and B.S in

Electrical Communication Engineering Major with, GPA 3.85 in 2014, from Alexandria University. Currently, her research interests cross cuts the areas of Vehicular Wireless Communication, Trustworthy wireless signals, and Moving-target Defense for secure wireless data exchange.

Effat Samir is a Research assistant at Faculty of Engineering, Alexandria University, Egypt. Effat received her Bsc. and M.Sc. in Communication and Electronics Engineering in 2013 and 2017 from Faculty of engineering, Alexandria University. She has worked in multiple research projects focusing on both physical and application layers. She has 2 book chapters among various publications in archival journals and conference proceedings. During her master studies she developed an interest in the IT physical layer; specially Nanotechnology field with a major interest in Nano-sensors fabrication, characterization, and calibration. Further, her recent crosscuts are oriented more in the IT application layer. She developed a huge research interests lie in the area of Vehicular Ad-Hoc Networks, Internet of Things (IoT), and Machine learning techniques.

Mohamed Azab is an assistant professor at The CIS, Virginia Military Institute. He is also affiliated with The City of Scientific Research and Technological Applications, The SmartCI Research Center, VT-MENA, (Virginia

Tech- Middle East and North Africa), College of Engineering Alexandria University, Alexandria, Egypt.

Mohamed received his Ph.D. in Computer Engineering in 2013 from The Bradley Department of Electrical and Computer Engineering at Virginia Tech, Blacksburg, USA.

He has multiple provisional patents, book chapters among various publications in archival journals and respected conference proceedings.

His research interests lie in the area of cyber security and trustworthy engineering ranging from theory to design to implementation. His recent research crosscuts the areas Software Defined Networking (SDN) architectures and protocols, high performance and cloud computing, ubiquitous Internet of Things (IoT), and Cyber-Physical systems (CPS).

Mohamed is the founder of the Cyber Security and IoT lab. Hosting Mohamed's Ph.D. and Masters students research activities.

Mohamed acted as a keynote speaker in multiple prestigious conferences. He served on multiple conference and workshop program and steering committees.

Mohamed Eltoweissy is Department Head and Professor of Computer and Information Sciences at Virginia Military Institute. He is also a Professor affiliated with The Bradley Department of Electrical and Computer Engineering at Virginia Tech.

Eltoweissy served as Chief Scientist for Secure Cyber Systems at Pacific Northwest National Laboratory. He also served on the faculty of James Madison University.

Eltoweissy co-founded several start-up companies including Video Semantics and Teradata Science.

Eltoweissy's current interests crosscut the areas of network security and resilience, cooperative autonomic systems, and networking architecture and protocols.

Eltoweissy has over 175 publications in archival journals and respected books and conference proceedings and an extensive funding record. He also served on the editorial board of IEEE Transactions on Computers (the flagship and oldest Transactions of the IEEE Computer Society) as well as other reputable journals.

In addition, Eltoweissy is active as an invited speaker at both the national and international levels. Eltoweissy received several awards and recognition for research, education, service, and entrepreneurship, including best paper awards, top placements at Cyber Security competitions, and a nomination for the Virginia SCHEV Outstanding Faculty Awards, the highest honor for faculty in Virginia. Eltoweissy is a senior member of IEEE and ACM.