# Blockchain-enabled FD-NOMA based Vehicular Network with Physical Layer Security

Ferheen Ayaz, Zhengguo Sheng, Ivan Weng-Hei Ho*, Daxin Tian†, and Zhiguo Ding‡
Department of Engineering and Design, University of Sussex, Brighton, UK
* Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong
† School of Transportation Science and Engineering, Beihang University, Beijing 100191, China
‡ School of Electrical and Electronic Engineering, University of Manchester, Manchester, UK
Email: f.ayaz@sussex.ac.uk

***Abstract*—Vehicular networks are vulnerable to large scale attacks. Blockchain, implemented upon application layer, is recommended as one of the effective security and privacy solutions for vehicular networks. However, due to an increasing complexity of connected nodes, heterogeneous environment and rising threats, a robust security solution across multiple layers is required. Motivated by the Physical Layer Security (PLS) which utilizes physical layer characteristics such as channel fading to ensure reliable and confidential transmission, in this paper we analyze the impact of PLS on a blockchain-enabled vehicular network with two types of physical layer attacks, i.e., jamming and eavesdropping. Throughout the analysis, a Full Duplex Non-Orthogonal Multiple Access (FD-NOMA) based vehicle-to-everything (V2X) is considered to reduce interference caused by jamming and meet 5G communication requirements. Simulation results show enhanced goodput of a blockckchain enabled vehicular network integrated with PLS as compared to the same solution without PLS.**

***Index Terms*—blockchain, FD-NOMA, physical layer security, secrecy rate, eavesdropper, goodput, data rate.**

## I. Introduction

Vehicular networks are one of the key elements in Intelligent Transportation System (ITS) to enable information exchange among vehicles, Road Side Units, base stations and other mobile devices. ITS performs an essential role in improving road safety by sending messages to recognized nodes in a vehicular network. However, the lack of security and privacy in ITS can threaten road safety. Security refers to the condition that a network is protected from adversarial attacks. Privacy means that only designated nodes in a network have permission to access or exchange information [1]. There are several attacks on security and privacy of vehicular networks. These attacks can be classified on the basis of the layer used by an attacker in a communications protocol stack [2]. For example, repudiation attack is performed on application layer [2], Denial-of-Service (DoS) and Sybil attack take place on network layer [3]. From physical layer's perspective, a vehicular network may suffer from the following attacks [1], [4]:

- **Jamming Attack:** It is caused when an attacker creates interference to disrupt the communications between sender and legitimate receiver.
- **Eavesdropping Attack:** It is caused when an eavesdropper intercepts the confidential transmission between sender and legitimate receiver.

TABLE I: Vehicular networks security and privacy offered by blockchain and PLS.

| **Requirement** | **Fulfilled by** |
|---|---|
| Only authorized nodes should communicate | Blockchain |
| Message must be authentic | Blockchain |
| SINR must be above a certain threshold | PLS |
| Communications must be confidential | Blockchain and PLS |

Security and privacy are usually managed at the upper layers of a communications protocol stack by using various techniques including blockchain and key based encryption [5]. A blockchain is a decentralized peer-to-peer electronic cash system, originally produced to validate and record transactions. Blockchain, implemented on application layer, has been considered as a potential solution to resolve security and privacy issues in vehicular networks [6]. It has been proven resilient against various attacks, such as repudiation [7], DoS, Sybil [8] and poisoning attack [9]. A permissioned blockchain not only ensures security but also privacy, by allowing only authorized nodes to join and communicate in a network [10]. However, physical layer attacks can still be successful in a blockchain-enabled network. For example, jamming can disrupt block announcement, thereby reducing its throughput [11]. An eavesdropper can attempt to intercept a confidential block generation. Physical Layer Security (PLS) is an effective approach to maintain secrecy [5] but may result in a decreased blockchain throughput.

Motivated by the latest advances in blockchain and the importance of security and privacy in vehicular communications, we study the effects of physical layer attacks on blockchain-enabled vehicular network. Additionally, due to increasing number of connected nodes, heterogeneous environment and

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 101006411, Royal Society Kan Tong Po International Fellowship (KTP\R1\201007). The research is also supported in part by the National Natural Science Foundation of China under Grant No. U20A20155, Beijing Municipal Natural Science Foundation under Grant No. L191001, Newton Advanced Fellowship under Grant No. 62061130221.

requirement of high communication rates, a Full Duplex Non-Orthogonal Multiple Access (FD-NOMA) based vehicle-to-everything (V2X) communications scenario is considered [12]. An FD-NOMA model fulfills the requirements of various Quality-of-Services (QoS) and multiple communication rates in V2X systems [13]. It also addresses the issue of low latency in existing Orthogonal Frequency Division Multiple Access (OFDMA) based fifth-generation (5G) technologies by simultaneous transmission and retrieval of data [14]. It is particularly suggested for V2X applications, e.g., navigation and emergency message dissemination [12]. Its roadmap for V2X based services has already been prepared by technical organizations, such as $3^{rd}$ Generation Partnership Project [15]. NOMA based techniques can also be used to provide security against jamming attack by nullifying co-channel interferences via Successive Interference Cancellation (SIC) [12].

### A. Related Works and Motivation

The relationship among blockchain throughput, data rate and Signal to Interference and Noise Ratio (SINR) is studied in [11] and [16]. SINR is a physical layer parameter and a function of distances between nodes in wireless communications. It can be severely degraded by attackers causing jamming and interference in signal transmission and therefore result in a reduced blockchain throughput. However, FD-NOMA can significantly improve SINR by SIC. Therefore, the performance of FD-NOMA for a secure blockchain based V2X system is worth investigating. Performance of FD-NOMA based V2X systems is analyzed in [12] assuming both Rayleigh and Rician channel models. The analysis does not take into account the traffic density, speeds or distances between moving nodes which greatly affect the reliability of signal transmission in V2X systems. SINR and PLS of a vehicular network is also analyzed considering double Rayleigh fading environment in [5]. Only one legitimate receiver and one eavesdropper is assumed to be presented within the communication range of sender, which is not very practical in high dense scenarios.

In presence of eavesdroppers, cryptographic schemes are used to maintain confidentiality. Although the privacy of V2X systems can be protected by implementing encrypted blocks and access control schemes, the possibility of wiretapping by eavesdropper cannot be avoided. Due to the broadcasting nature of both V2X systems and block announcement procedure, there still remains a possibility of break in confidentiality even when blockchain is used [17]. In [18], the nodes are allowed to register into a private blockchain only when the secrecy rate of physical layer exceeds a certain threshold. A blockchain based federated learning mechanism is proposed in [19]. Despite the privacy preserving nature of both federated learning and blockchain, an additional technique is applied to protect location privacy of nodes. In [16], PLS is recommended to prevent eclipse attack in a blockchain-based wireless network.

It can be concluded that some of the security and privacy requirements of V2X systems may not be met by blockchain alone. For example, if a blockchain uses voting consensus, the votes must also be encrypted in presence of an eavesdropper, which increases computation and communication overheads. Additionally, if all nodes broadcast their votes at the same time, the reliability of a transmission is severely reduced by interference. Table I highlights some key requirements of security and privacy fulfilled by blockchain and PLS. It shows that a cross-layer approach considering both physical layer aspects, e.g., SINR and secrecy rate, and application layer schemes, e.g., blockchain, can be utilized to provide robust security in vehicular networks. However, the feasibility analysis of an integrated approach is essentially required.

TABLE II: Key Notations.

| Notation | Definition |
|---|---|
| $g_{j,i}$ | Channel gain between node $j$ and node $i$ |
| $h_{j,i}$ | Channel coefficient between node $j$ and node $i$ |
| $s_{j,i}$ | Distance between node $j$ and node $i$ |
| $\gamma_{j,i}$ | SINR between node $j$ and node $i$ |
| $C_{j,i}$ | Secrecy rate between node $j$ and node $i$ |
| $p_i$ | Power of signal transmitted by node $i$ |
| $\alpha$ | Path loss exponent |
| $\eta$ | Coefficient of self-interference |
| $\beta_1$, $\beta_2$ | Threshold of $\gamma_{j,i}$, $C_{j,i}$ |
| $P_{out}$ | Outage probability |
| $\lambda$ | Blockchain throughput |
| $R$ | Data rate |
| $L$ | Packet length |
| $M$, $N$ | Number of senders, receivers |
| $K$, $I$ | Number of eavesdroppers, interference nodes |

### B. Contributions, Organization and Notations

This paper analyzes physical layer aspects of a blockchain-enabled FD-NOMA based vehicular network. The main contributions of the paper are

- We study a blockchain based vehicular network using FD-NOMA to ensure reliability in block addition. Physical layer aspects, i.e., SINR and secrecy rate, are analyzed for security and privacy of the proposed network. The percentage of success transmissions is evaluated in presence of jamming and eavesdropping attack.
- We propose an integrated approach of blockchain and PLS for ensuring both security and privacy. Simulation results with PLS show increase in goodput as compared to a blockchain system without PLS.
- We obtain the minimum allowable data rate in presence of multiple interference nodes and eavesdroppers. It is observed that 5G based V2X is required to provide sufficient data rate for security and privacy.

The rest of the paper is organized as follows. Section II analyzes a blockchain-enabled FD-NOMA based vehicular network. Results and conclusion are presented in Section III and Section IV respectively. Table II shows the key notations.

## II. Analysis of Blockchain-enabled FD-NOMA based Vehicular Network

### A. System Model

As shown in Fig. 1, all V2X nodes, i.e., vehicle, pedestrian, base station etc., are included in our FD-NOMA based V2X

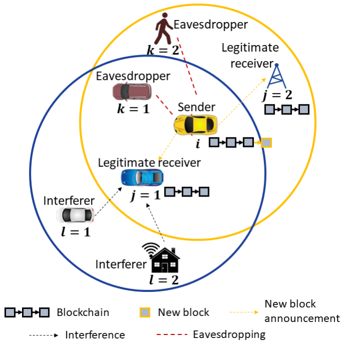


Fig. 1: The system model.

system and they can be categorized into one of the following: sender, legitimate receiver, interferer and eavesdropper. We assume urban and crowded environment, hence all communication channels are modeled by Rayleigh fading [20]. The channel matrix from $M$ sender nodes to $N$ receiver nodes in FD-NOMA based V2X systems is defined in [12] as

$$\mathbf{H} = \begin{bmatrix} h_{1,1} & h_{1,2} & ... & h_{1,M} \\ h_{2,1} & h_{2,2} & ... & h_{2,M} \\ . & . & . & . \\ . & . & . & . \\ h_{N,1} & h_{N,2} & ... & h_{N,M} \end{bmatrix}, \tag{1}$$

where $h_{j,i} = \sqrt{g_{j,i} s_{j,i}^{-\alpha}}$ is the channel coefficient between node $i$ and node $j$, $g_{j,i}$ is the channel gain following Rayleigh fading, $\alpha$ is the path loss exponent and $s_{j,i}$ is the instantaneous distance between node $i$ and node $j$ [5]. Assume that all channels are uncorrelated and have increasing order of channel coefficients, i.e. $|h_{j,1}| \leq |h_{j,2}| \leq, ...|h_{j,i}| \leq, ...|h_{j,M}| \, \forall j \, \epsilon \, [1, N]$, $i \, \epsilon \, [1, M]$ and vice-versa. In this case, co-channel interference of $j^{th}$ node is from $(j+1)^{th}$ to $M^{th}$ node. Other co-channel interference are nullified by SIC feature of NOMA [12].

Due to high mobility of nodes in a vehicular network, we take into account the uncertainty of nodes' positions. Therefore, $s_{j,i}$ is assumed as a random variable following exponential distribution. Exponential distribution has been shown as a suitable approximation to model traffic flow condition [21]-[22]. The Probability Density Function (PDF) of $s_{j,i}$ is $f(s_{j,i}) = \frac{1}{\bar{s}_{j,i}} e^{-\frac{s_{j,i}}{\bar{s}_{j,i}}}$, where $\bar{s}_{j,i}$ is the average distance between node $i$ and node $j$.

The performance of a blockchain-enabled wireless network is characterized by two important parameters: data rate and blockchain throughput. Data rate is defined as the amount of transmitted data in a unit time for a network, usually measured in bits per second (bps). Blockchain throughput is the number of blocks validated and generated in a unit time. It is measured in blocks per second (blocks/s). The relationship between data rate and blockchain throughput is defined in [16] as $R \geq \lambda \cdot L$, where $\lambda$ is the blockchain throughput, $R$ is the data rate and $L$ is the packet length of a block.

## B. SINR

When a signal is received by node $j$ from node $i$, the instantaneous SINR is defined in [12] as

$$\gamma_{j,i} = \frac{p_i |h_{j,i}|^2}{\sum_{l=j+1}^{M} p_l |h_{j,l}|_+^2 \eta p_j + p_n}, \tag{2}$$

where $\eta p_j$ is the self-interference by FD up-link, $\eta \epsilon \, [0, 1]$ is the coefficient of self-interference, $p_n$ is the noise power of Additive White Gaussian Noise (AWGN), $p_i$ and $p_l$ are the power of signal transmitted by node $i$ and interference node $l$ respectively. The received signal is subjected to only co-channel interference from neighbors of node $j$ after SIC.

In urban and crowded environment, the PDF of $\gamma_{j,i}$ is given in [12], [23] - [24] as $f(\gamma_{j,i}) = \frac{1}{\bar{\gamma}_{j,i}} e^{-\frac{\gamma_{j,i}}{\bar{\gamma}_{j,i}}}$, where $\bar{\gamma}_{j,i}$ is the average SINR. It depicts that $\gamma_{j,i}$ is a random variable following exponential distribution. As shown in (2), it depends on $h_{j,i}$, which is a function of $s_{j,i}^{-\alpha}$. Since $s_{j,i}$ is also an exponential variable, we present Lemma 1 and Theorem 1 to derive bounds of $\bar{\gamma}_{j,i}$ as functions of $s_{j,i}$ and $I^j$, i.e., the number of interference nodes to receiver $j$.

**Lemma 1:** $E\left(\frac{1}{s_{j,i}^{-\alpha}}\right) = \bar{s}_{j,i}^{\alpha} \left( \Gamma\left(\alpha{+}1, s_{min}/\bar{s}_{j,i}\right) {-} \Gamma\left(\alpha{+}1, s_{max}/\bar{s}_{j,i}\right) \right)$, where $s_{min}$ is the minimum $s_{j,i}$ and $s_{max}$ is the maximum distance up to which a signal can reach and $E(.)$ denotes expected value.

*Proof:* See Appendix A. □

**Theorem 1:** $\frac{1}{\left(I^j E(s_{j,i}^{-\alpha}) + n'\right) E\left(\frac{1}{s_{j,i}^{-\alpha}}\right)} \leq \bar{\gamma}_{j,i} \leq \frac{\bar{s}_{j,i}^{-\alpha}}{I^j s_{max}^{-\alpha} + n'}$, where $E\left(\frac{1}{s_{j,i}^{-\alpha}}\right)$ is defined in Lemma 1, $n' = \frac{\eta p_j + p_n}{pg}$ and $p = p_i = p_l$, $g = g_{j,i} = g_{l,i} \, \forall \, l \, \epsilon \, M$, without loss of generality.

*Proof:* See Appendix B. □

For a reliable message transmission and successful block generation, it is necessary that $\gamma_{j,i}$ exceeds a certain threshold. The probability that $\gamma_{j,i}$ is exceeds a threshold $\beta_1$ can be derived from its Cumulative Distributive Function (CDF), i.e.,

$$P(\gamma_{j,i} \geq \beta_1) = 1 {-} F_{\gamma_{j,i}}(\beta_1) = 1 {-} \int_0^{\beta_1} f(\gamma_{j,i}) d\gamma_{j,i} = e^{-\frac{\beta_1}{\bar{\gamma}_{j,i}}}. \tag{3}$$

Also, $e^{-\frac{\beta_1}{\bar{\gamma}_{j,i}^{LB}}} \leq P(\gamma_{j,i} \geq \beta_1) \leq e^{-\frac{\beta_1}{\bar{\gamma}_{j,i}^{UB}}}$, where $.^{LB}$ and $.^{UB}$ denote lower bound and upper bound respectively. In case of a jamming attack caused by interference, a block can only be generated if it is transmitted successfully to at least one legitimate receiver. Therefore, for a successful block announcement, it is must that $R \geq \frac{\lambda}{P(\gamma_{j,i} \geq \beta_1)^{UB}} \cdot L$.

## C. Secrecy Rate

If a signal from node $i$ is sent to a legitimate receiver node $j$ but a node $k$ attempts to receive the signal as an eavesdropper, the secrecy rate is defined in [26] as $C_{j,i} = [C_j - C_k]^+$, where $C_j = log_2(1{+}\gamma_{j,i})$, $C_k = \sum_{k=1}^{K} log_2(1{+}\gamma_{k,i})$, $K$ is the number of eavesdroppers present in the communication range of node $i$ and $[.]^+$ denotes $max(., 0)$. Using logarithmic property, i.e., $log(a) + log(b) = log(ab)$, $C_k$ can also be represented as $C_k = log_2 \phi$, where $\phi = (1 + \gamma_{1,i})(1 + \gamma_{2,i}).....(1 + \gamma_{K,i})$.

PLS ensures that a message is transmitted when secrecy rate is greater than a certain threshold $\beta_2$. Theorem 2 defines the probability of maintaining confidentiality through PLS.

**Theorem 2:**

$$P(C_{j,i} \geq \beta_2) = \begin{cases} \dfrac{\bar{\gamma}_{j,i} e^{\frac{1-2^{\beta_2}}{\bar{\gamma}_{j,i}}}}{2^{\beta_2}\bar{\gamma}_{k,i} + \bar{\gamma}_{j,i}}, & \text{if } K = 1, \\ \dfrac{\bar{\gamma}_{j,i}^2 e^{\frac{-2^{\beta_2}}{\bar{\gamma}_{j,i}}} E_1(\frac{vw}{u}) e^{\frac{vw}{u}}}{u}, & \text{if } K = 2, \end{cases}$$

where $u = 2^{\beta_2}\bar{\gamma}_{j,i}\bar{\gamma}_{k=1,i}\bar{\gamma}_{k=2,i}$, $v = \bar{\gamma}_{j,i} + 2^{\beta_2}\bar{\gamma}_{k=2,i}$, $w = v + 2^{\beta_2+1}\bar{\gamma}_{k=1,i}$ and $E_1(a) = \int_a^{\infty} \frac{e^{-z}}{z} dz$ is exponential integral. $P(C_{j,i} \geq \beta_2) \approx 0$ for $K > 2$.

*Proof:* See Appendix C. □

Theorem 2 shows that an FD-NOMA transmission without blockchain may not provide secrecy when $K > 2$. Therefore, privacy preserving measures such as encryption schemes and blockchain are therefore essential in such cases, where confidentiality cannot be protected by PLS alone. Using $E_1(z)e^z \leq log\big(1 + \frac{1}{z}\big)$ [25] and assuming $e^{\frac{1-2^{\beta_2}}{\bar{\gamma}_{j,i}}} \approx 1$, the upper bound of $P(C_{j,i} \geq \beta_2)$ can be defined as

$$P(C_{j,i} \geq \beta_2) \leq \begin{cases} \dfrac{\bar{\gamma}_{j,i}^{UB}}{2^{\beta_2}\bar{\gamma}_{1,i} + \bar{\gamma}_{j,i}^{UB}}, & \text{if } K = 1, \\ \dfrac{\bar{\gamma}_{j,i}^{2\ \ UB} log\big(1 + \frac{u'}{v'w'}\big)}{u'}, & \text{if } K = 2, \\ 0, & \text{otherwise}, \end{cases} \tag{4}$$

where $u' = 2^{\beta_2}\bar{\gamma}_{1,i}\bar{\gamma}_{2,i}$, $v' = \bar{\gamma}_{j,i}UB + 2^{\beta_2}\bar{\gamma}_{2,i}$ and $w' = v' + 2^{\beta_2+1}\bar{\gamma}_{1,i}$. In case of eavesdropping attack, the secrecy rate must be greater than $\beta_2$ for every receiver to protect confidentiality. Therefore, for protecting eavesdropping attack on physical layer, it is must that $R \geq \frac{\lambda}{\Pi_{j=1}^{N} P(C_{j,i} \geq \beta_2)^{UB}} \cdot L$.

### D. Goodput

To analyze the impact of PLS combined with blockchain, we define the term goodput as $R$ times the ratio of number of blocks successfully and secretly added into the blockchain to the total number of block generation attempts, i.e.,

$$Goodput = \frac{Number\, of\, blocks\, added\, to\, blockchain}{Total\, number\, of\, block\, generation\, attempts}, \tag{5}$$

where $Total\, number\, of\, block\, generation\, attempts$
$= Number\, of\, blocks\, added\, to\, blockchain$
$+ Number\, of\, blocks\, lost\, or\, eavesdropped$.

## III. Results and Discussion

In this section, we discuss simulation results compared with theoretical analysis presented in Section II. FD-NOMA based system is implemented in Matlab and Monte Carlo simulations are performed to analyze $\gamma_{j,i}$ and $C_{j,i}$. Additionally, the goodput of vehicular network is observed in OMNET++ integrated with Simulation of Urban Mobility (SUMO). The parameters used in simulations are listed in Table III.

TABLE III: Simulation Parameters.

| Parameters | Values | Parameters | Values |
|---|---|---|---|
| Iterations | $10^5$ | $\eta$ | 0.1 |
| $p$ | 20 dBm | $p_n$ | -104 dBm |
| $s_{max}$ | 400 m | $s_{min}$ | 10 m |
| $\beta_1$ | -15 dB | $\beta_2$ | 0.3 bits/sec/Hz |
| $\lambda$ | 1, 50 blocks | $L$ | 756 byts |
| $\alpha$ | -3 | $N$ | [2, 5] |
| $I^j$ | [1, 5] | $K$ | [1, 2] |

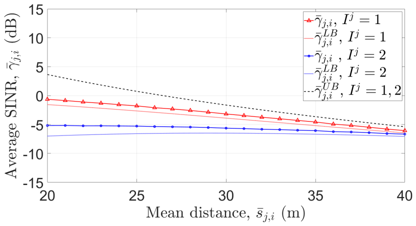
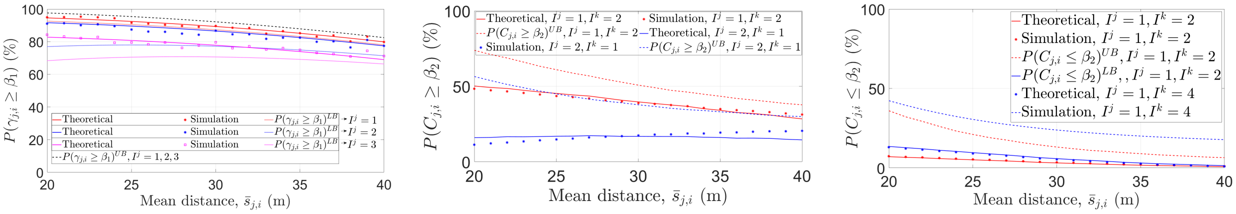


Fig. 2: $\bar{\gamma}_{j,i}$

Fig. 2 shows $\bar{\gamma}_{j,i}$ varying with respect to $\bar{s}_{j,i}$ at $I^j = 1$ and $I^j = 2$. The simulated $\bar{\gamma}_{j,i}$ lies within the bounds defined in Theorem 1, validating our analysis. It can be seen that $\bar{\gamma}_{j,i}$ falls with increasing $\bar{s}_{j,i}$. The dependence of $\bar{\gamma}_{j,i}$ on $\bar{s}_{j,i}$ is higher when $I^j = 1$ as compared to $I^j = 2$. It shows that $\bar{\gamma}_{j,i}$ can be enhanced by reducing $\bar{s}_{j,i}$ only when interference is low.

Fig. 3 shows $P(\gamma_{j,i} \geq \beta_1)$ and $P(C_{j,i} \geq \beta_2)$. The theoretical result of $P(\gamma_{j,i} \geq \beta_1)$ in Fig. 3 (a) is computed using (3). In simulation, $\gamma_{j,i} \geq \beta_1$ is counted as a successful transmission for each iteration. The percentage of successful transmissions is plotted as a simulated result in Fig. 3 (a). It can be seen in Fig. 3 (a) that $P(\gamma_{j,i} \geq \beta_1)$ falls with increasing $\bar{s}_{j,i}$ due to decreasing $\gamma_{j,i}$. $P(\gamma_{j,i} \geq \beta_1)$ is higher for less $I^j$, which depicts the effect of interference. High interference is considered as a collusion of attackers to hinder successful transmission. This is why a high $P(\gamma_{j,i} \geq \beta_1)$ is desired for a secure transmission. Fig. 3 (b) and (c) show $P(C_{j,i} \geq \beta_2)$ with $K = 1$ and $K = 2$, respectively. The theoretical result and upper bound are plotted using Theorem 2 and (4) respectively. Simulations show the percentage of iterations which resulted in $C_{j,i} \geq \beta_2$. As shown in Fig. 3 (b) and (c), $P(C_{j,i} \geq \beta_2)$ reduces with increasing $K$. Fig. 3 (c) shows that $P(C_{j,i} \geq \beta_2)$ is less than 50 % when $K = 2$ and $I^j = 1$ despite varying values of $I^k$. It reflects that maintaining secrecy is extremely challenging with large number of eavesdroppers. Therefore, cryptographically protected blockchain is an effective solution to ensure confidentiality of a transmission.

Fig. 4 shows percentage of success transmissions with respect to $\bar{s}_{j,i}$ in presence of jammers and eavesdroppers. A success transmission is counted if $\gamma_{j,i} \geq \beta_1$, with jammers only and also if $C_{j,i} \geq \beta_2$, when eavesdroppers are present. As shown in Fig. 4, success rate is higher with jammers only than with eavesdroppers. Specifically, when $K = 2$, the success rate is below 50% for every $\bar{s}_{j,i}$. As a PLS approach, a sender must estimate that $C_{j,i} \geq \beta_2$ to protect secrecy of a message. However, it is extremely challenging to attain $C_{j,i} \geq \beta_2$ in presence of large number of eavesdroppers. A cryptographically protected blockchain is an effective solution to ensure confidentiality of a transmission in such case. Therefore, a



(a) $P(\gamma_{j,i} \geq \beta_1)$

(b) $P(C_{j,i} \geq \beta_2)$ with $K = 1$

(c) $P(C_{j,i} \geq \beta_2)$ with $K = 2$

Fig. 3: $P(\gamma_{j,i} \geq \beta_1)$ and $P(C_{j,i} \geq \beta_2)$ with respect to $\bar{s}_{j,i}$.

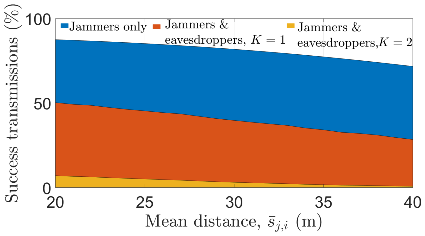
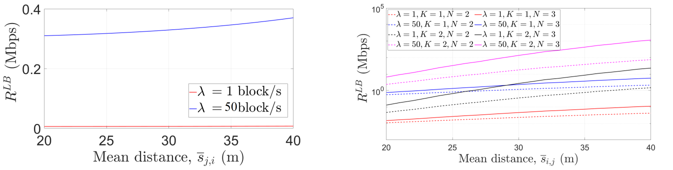


Fig. 4: Success transmissions in presence of jammers and eavesdroppers, $I^j = 2, I^k = 1$.



(a) against jamming attack, $I^j = 1$

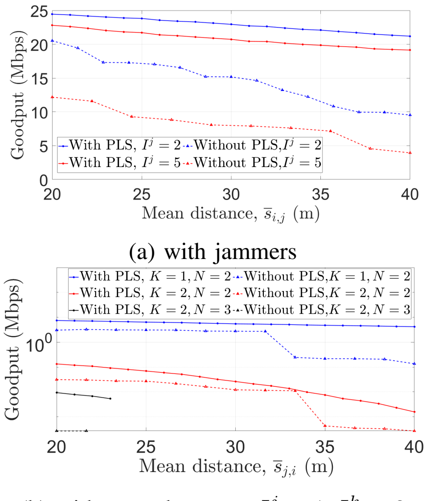
(b) against eavesdropping attack, $I^j = 1, I^k = 2$

Fig. 5: Minimum allowable $R$.

cross-layer approach combining both PLS and blockchain is promising to provide security against both attacks.

Fig. 5 shows the lower bound of $R$, i.e., minimum allowable $R$ sufficient to support both PLS and blockchain as a combined solution against jamming and eavesdropping. As shown in Fig. 5 (a), $R^{LB} < 0.5$ Mbps for both $\lambda = 1$ block /s and $\lambda = 50$ blocks/s, which shows that the proposed approach does not require a very high data rate to provide security against jamming attack. However, in Fig. 5 (b), $R^{LB}$ is rising with increase in $N$, $K$, $\lambda$ or $\bar{s}_{j,i}$. Specifically, for certain values of $\bar{s}_{j,i}$, when $N = 3$, it can be seen that $R^{LB} > 100$ Mbps. Since IEEE 802.11p supports $R$ ranging from 3 to 54 Mbps [27], it may not be feasible to implement a secure blockchain-enabled PLS solution when high blockchain throughput is required or large number of receivers are present. An integration of blockchain and PLS can be more effective with 5G or beyond 5G technologies which offer peak data rates in Gbps.

Fig. 6 shows comparison of goodput in a blockchain-based vehicular network, with and without PLS, simulated in OMNeT++ at $R = 27$ Mbps. Fig. 6 (a) depicts significant improvement in goodput by using PLS in presence of jammers. Goodput in presence of eavesdroppers is also improved, as shown in Fig. 6 (b). However, the goodput falls with increase in $\bar{s}_{j,i}$, $K$ or $N$. With $K = 2$ and $N = 3$, no block is successfully and secretly added into the blockchain after a certain $\bar{s}_{j,i}$. It shows that there is no sufficient $R$ available to support the integrated approach of blockchain and PLS. Nevertheless, strong cryptographic measures in blockchain can still protect confidentiality of eavesdropped blocks.



(a) with jammers

(b) with eavesdroppers, $I^j = 1, I^k = 2$

Fig. 6: Goodput in presence of jammers and eavesdroppers.

## IV. Conclusion

This paper has analyzed FD-NOMA based vehicular network which employs both PLS and blockchain to meet security and privacy requirements in presence of jammers and eavesdroppers. It can be concluded that the integration of PLS and blockchain can provide better goodput against both jamming and eavesdropping attacks. However, it requires high $R$ to support large number of legitimate receivers for protecting privacy in presence of eavesdroppers. DSRC based IEEE 802.11p communications may not provide sufficient $R$ for feasible integration of PLS and blockchain. Therefore, 5G based V2X is recommended for such applications.

## Appendix A

Let $X = s_{j,i}^{-\alpha}$, then the CDF of $X$ is $P(X \leq x) = P(s_{j,i}^{-\alpha} \leq x)$, which is equivalent to $P(s_{j,i} > x^{-\frac{1}{\alpha}}) = 1 - F_{s_{j,i}}(x^{-\frac{1}{\alpha}})$. Therefore, PDF of $X$ is

$$f_X(x) = \frac{1}{\alpha} x^{-\frac{1}{\alpha}-1} f_{s_{j,i}}(x^{-\frac{1}{\alpha}}) = \frac{1}{\bar{s}_{j,i}\alpha} x^{-\frac{1}{\alpha}-1} e^{-\frac{x^{-\frac{1}{\alpha}}}{\bar{s}_{j,i}}}. \quad (6)$$

Bringing (6) into $E(1/X) = \int_{-\infty}^{\infty} x^{-1} f(x) dx$ gives

$$\begin{aligned} E\Big(\frac{1}{s_{j,i}^{-\alpha}}\Big) &= \frac{1}{\bar{s}_{j,i}\alpha} \int_{s_{max}^{-\alpha}}^{s_{min}^{-\alpha}} x^{-\frac{1}{\alpha}-2} e^{-\frac{x^{-\frac{1}{\alpha}}}{\bar{s}_{j,i}}} dx, \\ &= \bar{s}_{j,i}^{\alpha}\Big(\Gamma(\alpha+1, \frac{s_{min}}{\bar{s}_{j,i}}) - \Gamma(\alpha+1, \frac{s_{max}}{\bar{s}_{j,i}})\Big). \end{aligned} \tag{7}$$

## Appendix B

Without the loss of generality, assuming $p = p_i = p_l$, $g = g_{j,i} = g_{l,i} \forall\, l \,\epsilon\, M$, (2) can be rewritten as $\gamma_{j,i} = \frac{s_{j,i}^{-\alpha}}{I^j s_{j,l}^{-\alpha} + n'}$ and $\frac{1}{\gamma_{j,i}} = I^j \frac{s_{j,l}^{-\alpha}}{s_{j,i}^{-\alpha}} + \frac{n'}{s_{j,i}^{-\alpha}}$. Therefore, $E\Big(\frac{1}{\gamma_{j,i}}\Big) = I^j E\Big(\frac{s_{j,l}^{-\alpha}}{s_{j,i}^{-\alpha}}\Big) + n' E\Big(\frac{1}{s_{j,i}^{-\alpha}}\Big)$. Let $E\Big(\frac{s_{j,l}^{-\alpha}}{s_{j,i}^{-\alpha}}\Big) = E\Big(\frac{Y}{X}\Big) = E(Y) \cdot \Big(\frac{1}{X}\Big)$, where $X = s_{j,i}^{-\alpha}$ and $Y = s_{j,l}^{-\alpha}$. Since both $s_{j,i}$ and $s_{j,l}$ represent distance between nodes, $E(Y) = E(X) = \frac{1}{\bar{s}_{j,i}\alpha} \int_{s_{max}^{-\alpha}}^{s_{min}^{-\alpha}} x^{-\frac{1}{\alpha}} e^{-\frac{x^{-\frac{1}{\alpha}}}{\bar{s}_{j,i}}} dx$. According to Jensen's inequality [28], $\frac{1}{E(\gamma_{j,i})} \le E\Big(\frac{1}{\gamma_{j,i}}\Big)$, which follows that $\bar{\gamma}_{j,i} \ge 1/E(\frac{1}{\gamma_{j,i}})$. Since $\gamma_{j,i}$ is directly proportional to $s_{j,l}$, $\bar{\gamma}_{j,i} \le \frac{\bar{s}_{j,i}^{-\alpha}}{I^j s_{max}^{-\alpha} + n'}$.

## Appendix C

$P(C_{j,i} \ge \beta_2)$ is given in [23] as $\int_{\gamma_{K,i}=0}^{\infty} \cdots \int_{\gamma_{1,i}=0}^{\infty} \int_{2^{\beta_2}\phi - 1}^{\infty} f(\gamma_{j,i}) f(\gamma_{1,i}) ... f(\gamma_{K,i}) d\gamma_{j,i} d\gamma_{1,i}.. ..d\gamma_{K,i}$. When $K = 1$, it reduces to

$$P(C_{j,i} \ge \beta_2) = \int_0^{\infty} \int_{2^{\beta_2}(1+\gamma_{1,i})-1}^{\infty} f(\gamma_{j,i}) f(\gamma_{1,i}) d\gamma_{j,i} d\gamma_{1,i}. \tag{8}$$

Using $\int_t^{\infty} \frac{1}{a} e^{-\frac{z}{a}} dz = e^{-\frac{t}{a}}$, (8) becomes

$$\frac{1}{\bar{\gamma}_{1,i}} \int_0^{\infty} e^{-\frac{2^{\beta_2}(1+\gamma_{1,i})-1}{\bar{\gamma}_{j,i}} - \frac{\gamma_{1,i}}{\bar{\gamma}_{1,i}}} d\gamma_{1,i} = \frac{\bar{\gamma}_{j,i} e^{\frac{1-2^{\beta_2}}{\bar{\gamma}_{j,i}}}}{2^{\beta_2}\bar{\gamma}_{1,i} + \bar{\gamma}_{j,i}}. \tag{9}$$

Similarly, $P(C_{j,i} \ge \beta_2)$ for $K = 2$ is

$$\begin{aligned} &\int_{\gamma_{2,i}=0}^{\infty} \frac{\bar{\gamma}_{j,i}}{2^{\beta_2}(1+\gamma_{2,i})\bar{\gamma}_{1,i} + \bar{\gamma}_{j,i}} e^{\frac{1-2^{\beta_2}(1+\gamma_{2,i})}{\bar{\gamma}_{j,i}}} f(\gamma_{2,i}) d\gamma_{2,i} \\ &= \frac{\bar{\gamma}_{j,i} e^{\frac{-2^{\beta_2}}{\bar{\gamma}_{j,i}}} E_1(\frac{vw}{u}) e^{\frac{vw}{u}}}{u/\bar{\gamma}_{j,i}}. \end{aligned} \tag{10}$$

As (10) involves exponential integral, obtaining a closed form equation of $P(C_{j,i} \ge \beta_2)$ for $K > 2$ is at least arduous, if not impossible [5], [12]. However, it can be seen that the resulting values of $u$, $v$ and $w$ for $K > 2$ are increased and lead to $P(C_{j,i} \ge \beta_2) \approx 0$.

## References

[1] Z. Lu, G. Qu and Z. Liu, "A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 760-776, Feb. 2019.

[2] B. Mokhtar and M. Azab, "Survey on Security Issues in Vehicular Ad Hoc Networks," *Alexandria Eng. J.*, vol. 54, pp. 1115-1126, Aug. 2015.

[3] A. Ilavendhan and K. Saruladha, "Comparative study of game theoretic approaches to mitigate network layer attacks in VANETs," *ICT Express*, vol. 4, no. 1, pp. 46-50, Jan. 2018.

[4] B. M. ElHalawany, A. A. A. El-Banna and K. Wu, "Physical-Layer Security and Privacy for Vehicle-to-Everything," *IEEE Commun. Mag.*, vol. 57, no. 10, pp. 84-90, Oct. 2019.

[5] A. U. Makarfi et al., "Toward Physical-Layer Security for Internet of Vehicles: Interference-Aware Modeling," *IEEE Internet Things J.,* vol. 8, no. 1, pp. 443-457, Jan. 2021.

[6] F. Ayaz, Z. Sheng, D. Tian, and V. Leung, "Blockchain-enabled security and privacy for Internet-of-Vehicles," in *Internet of Vehicles and its Applications in Autonomous Driving.* Cham, Switzerland: Springer, Sep. 2020.

[7] M. U. Aftab, M. Hussain, A. Lindgren and A. Ghafoor, "Towards A Distributed Ledger Based Verifiable Trusted Protocol For VANET," in *Proc. ICoDT2*, Islamabad, Pakistan, Jun. 2021, pp. 1-6.

[8] M. Baza et al., "Privacy-Preserving Blockchain-Based Energy Trading Schemes for Electric Vehicles," *IEEE Trans. Veh. Technol.*, vol. 70, no. 9, pp. 9369-9384, Sep. 2021.

[9] F. Ayaz, Z. Sheng, D. Tian and Y. L. Guan, "A Blockchain based Federated Learning for Message Dissemination in Vehicular Networks," *IEEE Trans. Veh. Technol.,* vol. 71, no. 2, pp. 1927 - 1940, Feb. 2022.

[10] F. Ayaz, Z. Sheng, D. Tian, G. Y. Liang, and V. Leung, "A voting blockchain based message dissemination in vehicular ad-hoc networks (VANETs)," in *Proc. IEEE Int. Conf. Commun.*, Dublin, Ireland, Jun. 2020, pp. 1–6.

[11] F. Ayaz, Z. Sheng, D. Tian and Y. L. Guan, "A Proof-of-Quality-Factor (PoQF)-Based Blockchain and Edge Computing for Vehicular Message Dissemination," *IEEE Internet Things J.,* vol. 8, no. 4, pp. 2468-2482, Feb. 2021.

[12] D. Zhang, Y. Liu, L. Dai, A. K. Bashir, A. Nallanathan and B. Shim, "Performance Analysis of FD-NOMA-Based Decentralized V2X Systems," *IEEE Trans. Commun.,* vol. 67, no. 7, pp. 5024-5036, Jul. 2019.

[13] Q. Chen, H. Jiang and G. Yu, "Service Oriented Resource Management in Spatial Reuse-Based C-V2X Networks," *IEEE Wireless Commun. Lett.,* vol. 9, no. 1, pp. 91-94, Jan. 2020.

[14] X. Yue, Y. Liu, S. Kang, A. Nallanathan, and Z. Ding, "Exploiting full/half-duplex user relaying in NOMA systems," *IEEE Trans. Commun.,* vol. 66, no. 2, pp. 560–575, Feb. 2018.

[15] C. Lai, R. Lu, D. Zheng and X. Shen, "Security and Privacy Challenges in 5G-Enabled Vehicular Networks," *IEEE Netw.,* vol. 34, no. 2, pp. 37-45, March/April 2020.

[16] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao, and M. A. Imran, "Blockchain-Enabled Wireless Internet of Things: Performance Analysis and Optimal Communication Node Deployment," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5791-5802, Jun. 2019.

[17] M. Brandenburger, C. Cachin, R. Kapitza and A. Sorniotti, "Trusted Computing Meets Blockchain: Rollback Attacks and a Solution for Hyperledger Fabric," in *Proc.38th Symposium on Reliable Distributed Systems,* Lyon, France, Oct. 2019, pp. 324-333.

[18] D. Yang, S. Yoo, I. Doh, and K. Chae, "Selective blockchain system for secure and efficient D2D communication," *Journal of Network and Computer Applications,* vol. 173, p.102817, Jan. 2021.

[19] Y. Qi, M.S. Hossain, J. Nie, and X. Li, "Privacy-preserving Blockchain-based Federated Learning for Traffic Flow Prediction," *Future Generation Computer Systems,* vol. 117, pp.328-337, Apr. 2021.

[20] N. Nguyen, T. Q. Duong, H. Q. Ngo, Z. Hadzi-Velkov and L. Shu, "Secure 5G Wireless Communications: A Joint Relay Selection and Wireless Power Transfer Approach," *IEEE Access,* vol. 4, pp. 3349-3359, Jun. 2016.

[21] A. May, *Traffic Flow Fundamentals*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1990.

[22] I. W. Ho, K. K. Leung and J. W. Polak, "Stochastic Model and Connectivity Dynamics for VANETs in Signalized Road Systems," *IEEE/ACM Trans. Netw.,* vol. 19, no. 1, pp. 195-208, Feb. 2011.

[23] V. U. Prabhu and M. R. D. Rodrigues, "On Wireless Channels With $M$-Antenna Eavesdroppers: Characterization of the Outage Probability and $\varepsilon$-Outage Secrecy Capacity," *IEEE Trans. Inf. Forensics Secur.,* vol. 6, no. 3, pp. 853-860, Sept. 2011.

[24] M. K. Simon and M. S. Alouini, *Digital Communication over Fading Channels: A Unified Approach to Performance Analysis.* Hoboken, NJ: Wiley, 2000.

[25] H. Alzer, "On some inequalities for the incomplete gamma function," *Mathematics of Computation,* vol. 66, no. 218, pp. 771–779, Apr. 1997.

[26] L. Wei, Y. Chen, D. Zheng and B. Jiao, "Secure performance analysis and optimization for FD-NOMA vehicular communications," *China Commun.,* vol. 17, no. 11, pp. 29-41, Nov. 2020.

[27] M. N. Tahir and M. Katz, "Performance evaluation of IEEE 802.11 p, LTE and 5G in connected vehicles for cooperative awareness," *Engineering Reports*, vol. e12467, Oct. 2021.

[28] R. Durrett, *Probability: theory and examples.* Cambridge University Press, 2020.