A Noise-Shaped Signaling Method for Vehicle-to-Everything Security based on Channel State Information

Dongryul Park [1], Seongho Woo [1], Sungryul Huh [1] , Seungyoung Ahn [1]

1) CCS Graduate School of Mobility, Korea Advanced Institute of Science and Technology (KAIST), Daejeon 34141, South Korea
E-mail: dongryulpark@kaist.ac.kr

ABSTRACT: This paper presents a method to improve the Vehicle-to-Everything (V2X) security. With recent development of communication technology and traffic applications, V2X is recently commercialized and has been growing as a fundamental system for future applications. Because of the high mobility of the vehicles, V2X requires a low latency and high-reliability. However, previous security methods demand a large computational burden and generate high latency owing to complex operations and long additional data bits for ensuing security. We propose a noise-shaped signaling method that provides high-level security with low latency for reliable V2X communication. The proposed method encrypts original data symbols to noise-like symbols by applying a noise envelope that consists of Chaotic Random Magnitude Sequence (CRMS) and Chaotic Random Phase Sequences (CRPS). The proposed method does not demand additional data bits, generate delay and degrade error rate because the method only uses simple procedure with automatically manipulated sequences for data encryption. We analyze our method in depth using extensive simulations and various viewpoints such as error rate. After these analyses, we confirm that the noise-shaped signaling method is high-level of secure method with a low latency for V2X communication.

KEY WORDS: Cryptography, Dedicated Short Range Communication (DSRC), Vehicular Ad-Hoc Network (VANET), Vehicle-to-Everything (V2X)

1. INTRODUCTION

Vehicular communication is a promising technology that increases road safety and traffic efficiency [1]. With the recent advances in various technologies such as such as autonomous driving and Intelligent Transportation System (ITS), vehicular communication systems have shown tremendous growth and attract worldwide interest. Recently, vehicular communication develops into Vehicle-to-Everything (V2X), which considers not only vehicle drivers, but also other vehicle-related components. The Dedicated Short-Range Communication (DSRC) protocol is the representative protocol used for V2X; IEEE 802.11p and IEEE 1609.2 are adopted for physical layer and security service, respectively. With the deployment of DSRC, the protocol has been validated and matured through various standards, research, and tests over the past two decades [2].

Although wireless communication technology brings many advantages, security threats have to be considered because of the broadcasting nature for a wide range service and for large numbers of users. Especially for V2X, to construct the communication network dynamically, the DSRC protocol designates vehicles and infrastructures as communication nodes. During communications among nodes, malicious users may be selected as an important network element, and those users are able to paralyze the network. Moreover, various attacks such as eavesdropping and Sybil can cause more serious accidents [3]. Thus, a method higher level of security method is essential to enable reliable vehicular communications.

To address such security threats, we propose a noise-shaped signaling method in the physical layer using channel state information (CSI). The proposed method provides high-level security performance and a low latency for reliable vehicular communication. Our method modifies conventionally modulated symbols to a severely noisy symbols by multiplying a noise envelope. The noise envelope, a key item to modify the symbols, consists of Chaotic Random Magnitude Sequence (CRMS) and Chaotic Random Phase Sequence (CRPS). The CRMS and CRPS simplify the sequence sharing method and guarantee a high level of security performance by using the characteristics of chaotic sequence such as non-periodicity, disorder, and sensitivity to the initial and control values. The CRMS, which can degrade

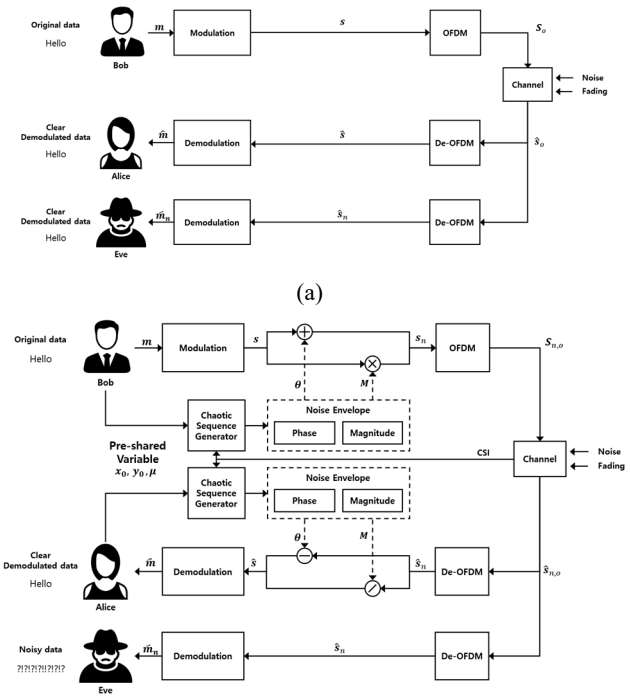


Fig. 1 Overall block diagram of systems: (a) Conventional, (b) With proposed noise-shaped signaling method.

communication performance, are automatically determined by CSI. In addition, the method operates with only simple processes and does not use additional data bits. To demonstrate the performance of the proposed method, we analyze proposed method in Vehicle-to-Vehicle (V2V) environments with performance metrics of the packet error rate.

This paper is organized as follows. The proposed method is presented in Section 2. Section 3 introduces the simulation setups and the results used to verify the proposed method.

2. PROPOSED NOISE-SHAPED SIGNALING METHOD

System block diagram is shown in Fig. 1. Conventional system is denoted in Fig. 1 (a). The conventional system does not have any physical layer security system, all user (include attacker) can easily steal the signals. On the other hand, the proposed method protects the signal by multiplying CRMS, CRPS which make the signal similar to noise. An overview of the proposed method is as follows.

1) Sender (Bob): Bob selects pre-shared variables and shares with the intended receiver. Afterward, the message bits m are modulated into symbols S, and the symbols are modified to noise-shaped signal S_n. The noise envelope is generated using pre-shared variables. The noise-shaped signal is created by multiplying the noise envelope to original symbols S and protects the message by changing the original mapping symbols into severe fading noise symbols. After

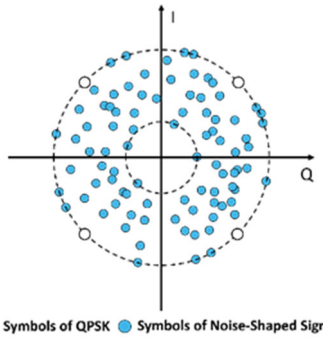


Fig. 1 Overall block diagram of systems: (a) Conventional, (b) With proposed noise-shaped signaling method.

the Orthogonal Frequency Division Multiplexing (OFDM) modulation, the radio signal $S_{n,o}$ is generated by splitting noise-shaped signal S_n into each subcarrier and send through the channel.

2) Intended receiver (Alice): Alice captures the transmitted radio signal as $\widehat{S_{n,o}}$ with channel noise and obtains noise-shaped signal $\widehat{S_n}$ through OFDM demodulation. Alice can recover the symbol $\hat{S}$ by eliminating the noise envelope from $\widehat{S_n}$ and can decode the message bit. Because Alice has the pre-shared variables, the noise envelope used to encrypt the data can be reconstructed

3) Attacker (Eve): Eve can also capture the transmitted signal $\widehat{S_{n,o}}$ that passes through the channel and can restore $\widehat{S_n}$. However, Eve cannot eliminate the noise envelope that the intentionally multiplied signal at the transmitter. Because Eve does not have the pre-shared variables, Eve cannot reconstruct the noise envelope. Thus, Eve unable to recover the original mapping symbols and recognizes the captured signal as a signal with intense fading noise.

The proposed method adds a noise-shaped signaling process between modulation/demodulation and OFDM/de-OFDM in the transmitter and receiver. In the process, the same noise envelope is generated by pre-shared variables (x_0, y_0, μ) in both transmitter and receiver. x_0, y_0, μ are the initial and control values used to generate chaotic random sequences. Details about the variables are described in subsections 2.1 and 2.2. Fig. 2 shows the effect of the noise envelope when the original modulation scheme is Quadrature Phase Shift Keying (QPSK). The constellation shape of the original symbols is changed to a ring shape constellation that resembles a heavily faded signal. Then each symbol, consisting of the noise-shaped signal, is encrypted and protected because the original mapping point is altered by a noise envelope which is only shared with Bob and Alice. Moreover, leakage of the modulation scheme can be prevented since the discrete

characteristics of the conventional modulation scheme are disappeared. The proposed noise-shaped method consists of following two steps. First, the Mag_{min} required for generating the noise envelope is decided based on CSI. And the pre-shared variables are shared with Alice. Second, the proposed method is applied to the original signal by multiplying the noise envelope constructed by Mag_{min} and pre-shared variables.

2.1. Chaotic Random Sequence

The noise envelope consists of CRMS and CRPS. Both sequences are based on a chaotic map that has the characteristic of A chaotic dynamic system. A chaotic dynamic system has fine properties for security such as aperiodic variation, irregularities, and sensitive to the initial values and control parameters [4]. Owing to these properties, the behavior of the system cannot be predicted and resembles noise. Moreover, the exact same random sequence is possible to restore using the identical initial value because the chaotic dynamic system is a deterministic system. In this paper, we use the 2D Logistic-Adjusted-Sine-Map (LASM) to generate the CRMS and CRPS [5]. The LASM is formulated in (1).

$$\begin{cases} x_{k+1} = \sin(\pi\mu(y_k + 3)x_k(1 - x_k)) \\ y_{k+1} = \sin(\pi\mu(x_{k+1} + 3)y_k(1 - y_k)) \end{cases} \quad (1)$$

The x_k and y_k is the sequence value at a certain index k. The sequence consisting of x_k is expressed as $\boldsymbol{X}$ using the vector expression method, and the sequence consisting of y_k is also expressed as $\boldsymbol{Y}$. The μ is the control parameter that regulates the chaotic behavior of LASM. The $x_{k+1}$and y_{k+1} are created using the previous value. Thus, the initial values x_0, y_0 must be given before the sequence generation process. The distribution of an example sequence is shown in Fig. 4. $\boldsymbol{X}$ and $\boldsymbol{Y}$ are randomly distributed in [0, 1].

2.2. Generating Noise Envelope and Noise Shaped-signal

In order to create the noise-like effect, the original chaotic sequences $\boldsymbol{X}$ and $\boldsymbol{Y}$ are generated as same length of the originally mapped symbols and used to generate CRMS, M_k, and CRPS, θ_k, using (2).

$$\begin{cases} M_k = (1 - Mag_{min}) \cdot x_k + Mag_{min} \\ \theta_k = 2\pi \cdot y_k \end{cases} \quad (2)$$

Mag_{min} defines the low boundary of the CRMS. Through the (2), the range of x_k is adjusted to [Mag_{min},1] and turned into CRMS. If CRMS is greater than 1, a signal with greater energy than the original signal is generated. A larger energy signal makes the distinction between signal and noise clearer; therefore, we set the upper bound to 1 for making the signal similar to noise. And if CRMS is close to 0 in other words the Mag_{min} are seriously low, the energy of signal is reduced relatively original signal. The small

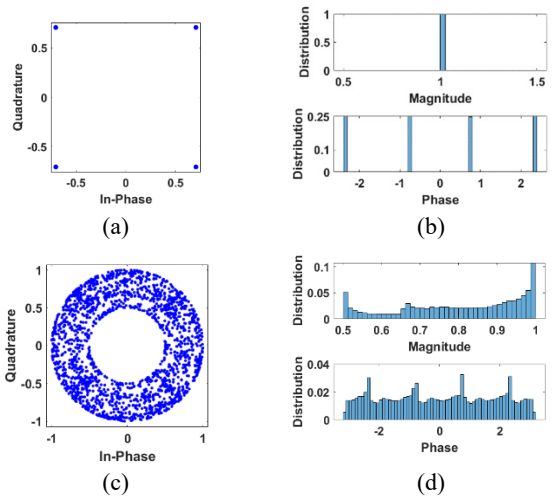


Fig. 3 Constellation and histogram: (a) Conventional symbols, (b) Conventional histogram, (c) Noise-shaped signal symbols, (d) Noise-shaped signal histogram.

energy signal easily influenced by channel noise and degrade the BER performance. Therefore, we select the Mag_{min} based on CSI to maintain the original signal energy and BER performance. Also, the CRPS is generated by changing the range of y_k to [0, 2π], as shown in the (2). When the CRMS is multiplied by the existing symbol, the symbol energies are decreased, and the position of the symbol is located at a point closer to the origin of the complex plane. The modified symbols are encrypted because symbols do not follow the conventional mapping rules. In addition, each symbol energy has a large variation similar to a signal with severe fading noise. Then, the CRPS encrypts the symbol mapping by rotating the symbols. However, as the symbol energy decreases due to the effect of CRMS, the modified symbols react sensitively to noise, and a higher error rate can occur. Thus, we adaptively control Mag_{min} by using CSI. If channel response has positive response, we set the Mag_{min} at low value according to CSI value. And, if channel response has negative response, we do not modify the Mag_{min} and set to 1 for no signal energy degradation.

The noise envelope consists of $\boldsymbol{N}$ number of noised symbols,

The noise-shaped signal $\boldsymbol{S}_n$is expressed by (3)

$$\begin{aligned} \mathbf{S_n} &= [S_{n,0}, S_{n,1}, S_{n,2}, \ldots, S_{n,N-2}, S_{n,N-1}] \\ S_{n,k} &= S_k \cdot M_k \cdot \exp(j\theta_k) \end{aligned} \quad (3)$$

The noise envelope consists of $\underline{N}$ number of noised symbols, and $\underline{N}$ represents the number of symbols transmitted in the packet. The k represents the index of a certain symbol. M_k and θ_k are components of the noise envelope and mean CRMS and CRPS value in specific index k. Each noised symbol $S_{n,k}$ is generated by multiplying the noise envelope to the original mapping symbol S_k. The noise envelope acts like a multiplicative factor of the fading channel and changes the symbol into severe fading noise.

Table 1 V2X Simulation parameters

Parameter	Value
Modulation	QPSK
Coding rate	1/2
Data rate [Mbps]	6
Subcarriers (Pilot, Null)	64 (4, 12)
Propagation channel model	TDL
Environment	Urban LOS , Urban NLOS, Highway NLOS

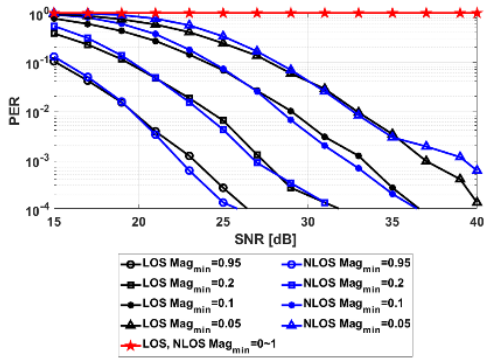
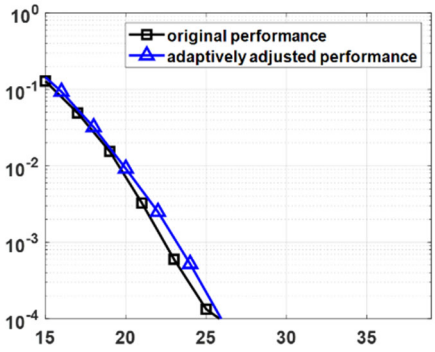


Fig. 4 PER performance according to SNR w/o adaptive Mag_{min} control.

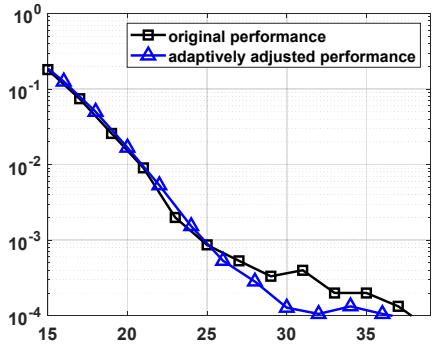
3. Evaluation

In this section, we present the result of simulation-based experiments to assess the proposed noise-shaped signaling method. Fig. 3 show the changes of the symbol when the proposed method is applied to QPSK symbols. Fig. 3(a) show the constellation of the conventional modulation scheme, and Fig. 3(c) represent the constellation of the proposed noise-shaped signaling method. The symbols are transformed into severely faded symbols because the magnitude and phase are modified according to the noise envelope. Also, the randomized behaviors of the magnitude and phase are confirmed by the histograms shown in Fig. 3(b), (d). Consequently, the mapping rules of the modulation scheme, with discrete features, are eliminated and the attacker cannot estimate the modulation of the original signal.

We present the results of simulations of the proposed method in realistic V2V channel environment. The simulation configurations are shown in Table 1. The overall simulation complies with the 802.11p standard that defines the physical layer of the DSRC protocol and uses the Tapped Delay Line (TDL) model to consider the special channel characteristic of V2V. Unlike existing path loss or statistical models, the TDL model is configured by the impulse response of each tap by considering channels as various taps. The TDL model can provide realistic communication environments to simulate because each small taps reflect fading and the multi-path signals due to the high speed of a vehicle and surrounding obstacles [6, 7].



(a)



(b)

Fig. 5 PER performance according to adaptive Mag_{min} control (a) urban NLOS, (b)highway NLOS.

Fig. 4 shows the PER performance of the proposed method. In all scenarios, Alice has a PER converged in low error rate, whereas Eve always has PER of 1 that is the maximum PER. Through these results, we confirm that Eve cannot interpret the message in any case, which indicates that the proposed noise-shape signaling has a high level of security functionality. By converging PER of Alice, we confirm that our method can be used in real V2X communication. In addition, the BER increases with lowering Mag_{min} which means a reduction of average symbol energy because we do not adjust Mag_{min} based on CSI channel conditions in this case.

To alleviate this performance degradation, we use the CSI based control method. Fig. 5 shows the PER performance with adaptive Mag_{min} control based on CSI. The PER has no significant fluctuation compare with original system that are not apply the proposed system. As a consequence, the proposed method can use any performance degradation with high level of security functionality.

4. CONCLUSION

In this paper, we propose a noise-shaped signaling method, which is applied at the physical layer, to improve the security of V2X communication system. Our method enhances security performance using a simple process that modifies the originally mapped symbols to a noise-like symbols. The effect of the noise

envelope consisting of CRMS and CRPM is analyzed in depth. From these evaluations, the proposed method is suitable for the V2X environment because the method does not require additional elements and does not cause latency of communication. In addition, even if the modulation scheme is leaked, interpretation of the signal is impossible due to characteristics of the noise envelopes that only can be restored with exactly same pre-shared variables. Thus, we conclude the proposed method is well suitable for the V2X communication system.

REFERENCES

(1) K. Sjoberg, P. Andres, T. Buburuzan, and A. Brakemeier, “Cooperative intelligent transport systems in europe: Current deployment status and outlook,” IEEE Vehicular Technology Magazine, vol. 12, no. 2, pp. 89–97, Jun. 2017.

(2) X. Zhao, S. Jing, F. Hui, R. Liu, and A. J. Khattak, “Dsrc-based rear-end collision warning system–an error-component safety distance model and field test,” Transportation Research Part C: Emerging Technologies, vol. 107, pp. 92–104, Oct. 2019.

(3) A. Ghosal and M. Conti, “Security issues and challenges in v2x: A survey,” Computer Networks, vol. 169, p. 107093, Mar. 2020

(4) L. Xu, Z. Li, J. Li, and W. Hua, “A novel bit-level image encryption algorithm based on chaotic maps,” Optics and Lasers in Engineering, vol. 78, pp. 17–25, Mar. 2016.

(5) Z. Hua and Y. Zhou, “Image encryption using 2d logistic-adjusted-sine map,” Information Sciences, vol. 339, pp. 237–253, Apr. 2016.

(6) Intelligent Transport Systems (ITS); Access Layer; Part 1: Channel Models for the 5, 9 GHz Frequency Band, document TR 103 257-1, ETSI, Valbonne, France, May 2019.

(7) P. Alexander, D. Haley, and A. Grant, ‘‘Cooperative intelligent transport systems: 5.9-GHz field trials,’’ Proc. IEEE, vol. 99, no. 7, pp. 1213–1235, Jul. 2011