EMITTER International Journal of Engineering Technology
ISSN: 2443-1168, Vol. 8, No. 1, June 2020, pp. 140~160
DOI : 10.24003/emitter.v8i1.493

Higher Rate Secret Key Formation (HRKF) based on Physical Layer for Securing Vehicle-to-Vehicle Communication

Inka Trisna Dewi, Amang Sudarono, Prima Kristalina, Mike Yuliana

Electrical Engineering Department, Politeknik Elektronika Negeri Surabaya
E-mail: inkatrisnad@gmail.com, {amang,prima,mieke}@pens.ac.id

Received March 17, 2020; Revised April 23, 2020; Accepted May 10, 2020

Abstract

One effort to secure vehicle-to-vehicle (V2V) communication is to use a symmetrical cryptographic scheme that requires the distribution of shared secret keys. To reduce attacks on key distribution, physical layer-based key formation schemes that utilize the characteristics of wireless channels have been implemented. However, existing schemes still produce a low bit formation rate (BFR) even though they can reach a low bit error rate (BER). Note that V2V communication requires a scheme with high BFR in order to fulfill its main goal of improving road safety. In this research, we propose a higher rate secret key formation (HRKF) scheme using received signal strength (RSS) as a source of random information. The focus of this research is to produce keys with high BFR without compromising BER. To reduce bit mismatch, we propose a polynomial regression method that can increase channel reciprocity. We also propose a fixed threshold quantization (FTQ) method to maintain the number of bits so that the BFR increases. The test results show that the HRKF scheme can increase BFR from 40% up to 100% compared to existing research schemes. To ensure the key cannot be guessed by the attacker, the HRKF scheme succeeds in producing a key that meets the randomness of the NIST test.

Keywords: V2V security, RSS, polynomial regeression

1. INTRODUCTION

In the last decade, along with the development of communication and transportation technology, vehicles have been equipped with high-tech devices to communicate with each other. Vehicle-to-vehicle (V2V) communication utilizes an ad-hoc wireless network that allows vehicles to send various information on the road to other vehicles, such as traffic jams, warning of obstacles, or lane changes. Thus, V2V communication can improve driving safety and traffic flow efficiency to reduce the number of vehicle accidents [1]. Moreover, the vehicle can also send position and speed information at that time with a special purpose. An on-board unit (OBU), which

functions as a transmitter must be installed in each vehicle to send and receive messages from other vehicles. However, the development of communication on V2V increases the risk of vehicle attacks caused by data exchange via the internet and wireless networks [2]. One possible type of attack is eavesdropping, where the attacker listens secretly for information exchanged between authorized parties [3]. Furthermore, this information is used by unauthorized parties for personal gain that harms other vehicle users. Therefore, security issues in V2V technology are a big challenge for researchers. Various aspects of security that must be considered in V2V communication are ensuring the authenticity of information, maintaining the confidentiality of information, and knowing that information comes from the claimed source [3-5]. If these aspects cannot be met, the attacker can easily damage the main purpose of V2V technology.

To ensure the confidentiality of V2V communication, authorized parties must encrypt and decrypt messages, which are called cryptographic techniques [6]. Messages can be secured using asymmetric or symmetrical cryptographic schemes. Due to the need for complex mathematical operations and high computational time, asymmetric cryptographic schemes are not suitable for devices that have limited resources, such as on vehicular networks [7-9]. In contrast, symmetrical cryptographic schemes can be relied upon because of low computational time [9]. In this scheme, all authorized parties must obtain a distributed key before encrypting and decrypting messages. This makes symmetric cryptographic schemes vulnerable to key leaks, so communication between authorized parties has a high potential to be attacked. Recently, physical layer (PHY) characteristics are used as an alternative solution to establish secret keys on wireless networks [10-13]. PHY-based key formation scheme can overcome the problems of symmetric cryptographic schemes in terms of key distribution. It utilizes the properties of physical layer such as randomness and reciprocity of wireless channels to measure random information as a source of secret key formation. Randomness provides unexpected key characteristics, making it difficult for unauthorized parties to guess the key formed [13]. The principle of channel reciprocity is very important in key formation, where the random information obtained by the sender and receiver will be the same if they extract it within the coherent time [14]. There are several parameters that can be used as random information, such as received signal strength (RSS) [15-18], channel status information (CSI) [12, 19], and channel impulse response (CIR) [19]. The RSS-based key formation scheme can be easily implemented compared to the other two parameters because most existing wireless devices already provide RSS reading [20]. Therefore, RSS is widely used as information to generate PHY-based secret keys.

There are many researches about RSS-based secret key formation that are implemented in different scenarios. The method in this research produced a low bit error rate (BER) but still produced a low bit formation rate (BFR) [18, 21-23]. Bit error rate refers to the number of bit inequalities between the

sender and receiver of the entire key length. The bit formation speed is the total number of bits at the end of the key formation scheme for each RSS sample. They sacrifice a lot of bits that must be discarded to produce keys without errors. The secret key formation scheme that cannot reach high BFR is not suitable for V2V communication because there will be a delay in key formation. Two vehicles were out of range before successfully establish a shared secret key, causing a fatal error in road traffic. What's more, high mobility is the main feature of V2V where vehicles can move randomly so the challenge of establishment a key in V2V is to produce high BFR and zero BER using uncomplicated algorithms.

In this research, we propose a higher rate secret key formation (HRKF) scheme based received signal strength for V2V communication with a focus on increasing BFR without sacrificing BER. To provide confidentiality of data exchanged between vehicles, we use symmetric cryptography, AES-256, due to its low computational time [24]. The HRKF scheme consists of 4 main stages: channel characteristics measurement; reciprocal enhancement; quantization and encoding; and randomness extraction and key verification. We use the second order polynomial regression in the reciprocal enhancement stage to significantly increase the correlation between vehicles. This stage aims to reduce the BER of the key formed. A fixed threshold quantization (FTQ) method is designed to map RSS into four different levels. Then the quantized RSS is encoded into two-bits. This allows our scheme to establish secret keys with high BFR even in high mobility scenarios. In the second stage, we also adopt the level crossing algorithm as a first step to prevent successive 0 or 1 bits. Furthermore, this algorithm is able to eliminate all bit mismatches between authorized parties. Therefore, this scheme can produce zero BER without the bit error correction stage as in the existing schemes. Note that the bit error correction stage, commonly known as the information reconciliation stage requires the exchange of bit parity between authorized parties. Besides requiring a good network connection, the parity bit exchange stage is also vulnerable to eavesdropping. We evaluate the capabilities of the HRKF scheme by comparing it to the existing schemes in three metrics, namely BER, BFR, and randomness of the keys. The results of our research show that the proposed HRKF scheme outperforms the bit formation rate without any bit errors. All keys pass the NIST test to guarantee its randomness. Although it can produce high bit rates, this scheme does not require high computational time because it is designed for V2V communication.

The remainder of this paper is organized as follows. Section II reviews previous related research. Section III explains the originality of this research. Section IV explains in detail the proposed HRKF scheme and measurement scenarios. Section V analyzes the proposed scheme in three metrics and compares with other existing schemes. Finally, Section VI concludes this paper.

2. RELATED WORKS

There are several studies of key formation in wireless networks, mainly based on received signal strength. The purpose of their research is to get the best possible secret key that can be used for a secure communication process.

Aono et al. [25] proposed a quantization method that uses a threshold derived from the median of RSS measurements. This scheme produces a high BER. To overcome this problem, Mathur et al. [26] proposed a lossy-quantization method used in RSS-based secret key generation schemes. The proposed quantization method uses two thresholds and will discard the RSS value that is between the upper and lower threshold. In addition, this scheme proposes a level crossing algorithm that only retains one bit (0 or 1) of m-bits. If m-bits consist of different bits, they will be discarded. This scheme produces a low BER and high entropy so that it does not need the randomness extraction stage (known as the privacy amplification stage) anymore. But it produces a low BFR.

Jana et al. [27] utilize the mean and standard deviation of each RSS block as a quantization threshold. The proposed adaptive scheme uses two thresholds (q + and q-) and will convert RSS to 1 and 0 if it is above q + and below q- respectively. Otherwise, RSS measurements are discarded. This scheme can produce high BFR and entropy, but there is still a bit error even though it has passed the information reconciliation stage. The determination of the quantization threshold in [27] was developed by Ambekar et al. [6] to divide each RSS block into 4 levels. Each level is quantized into two bits based on gray code and no bits are discarded (lossless quantization). This scheme utilizes the average and variance of each RSS block as a threshold. The BFR of this scheme increases than the scheme [27], but the problem cannot reach 0-bit error.

The method of pre-processing before the quantization stage is equally important in key formation scheme. The author [28] proposed three pre-processing methods to improve reciprocal channels, namely minimization of norm l1, polynomial regression, and Kalman filter. As a result, the pre-processing stage can increase BFR and decrease BER. Mike et al. [21] proposed a secret key generation scheme by combining a modified Kalman filter and several quantization methods. This scheme divides the RSS measurement into several blocks to be processed using the Kalman filter. The test results show that the use of modified pre-processing can produce the same key bits without going through the information reconciliation stage. The combination of Kalman filter and adaptive quantization produces higher BFR and lower BER than other quantizations. However, the attacker also has a high BFR so it is possible to get the same key.

3. ORIGINALITY

We propose a higher rate secret key formation (HRKF) scheme to establish a secret key as security for V2V communication. The wireless channel information used is received signal strength (RSS) collected from a mobile

scenario at a frequency of 5.8 GHz. The HRKF scheme uses a combination of polynomial regression and fixed threshold quantization (FTQ) method to produce a secret key with a higher BFR than the existing scheme. The FTQ method is a modification of lossless quantization, where RSS data is divided into several blocks before being quantized and encoded into 2 binary bits. The combination of these two methods can establish a secret key formation scheme without an error correction stage. The secret key obtained has a high BFR and zero BER. Thus, this scheme can be applied to V2V communication given that V2V requires a non-complex scheme to obtain keys without delay. The proposed scheme will be compared with several studies, such as research [22] that use hybrid methods at the pre-processing stage, research [21] that use the Kalman filter and adaptive quantization, research [23] that use the Kalman filter and Modified Multibit (MMB) quantization, and research [18] that use the Kalman filter and Mathur quantization.

4. SYSTEM DESIGN

In this section, we briefly introduce the HRKF scheme model which consists of the attacker model, the system model, the key formation process of HRKF scheme, the message encryption-decryption process using AES-256 algorithm, and performance metrics.

4.1 Attacker Model

In this research, we have considered the 3-node model as shown in Figure 1. Alice and Bob acted as authorized vehicles while Eve acted as an unauthorized vehicle. Eve is a passive attacker in this scenario. He eavesdrops on all the information exchanged between Alice and Bob. It is assumed that Eve knows all the methods in the HRKF scheme used by Alice and Bob to establish a shared secret key.

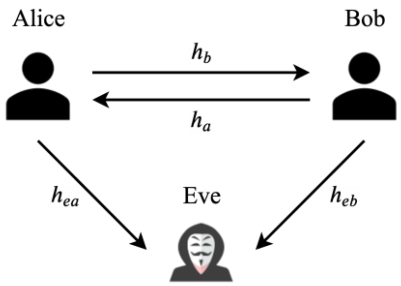

Figure 1. Attacker Model

With constant velocity, Alice and Bob carry out a measurement process to explore the characteristics of wireless channels in the form of RSS, h_b and h_a as a source of key formation. On the other hand, Eve followed the direction of the authorized vehicles to get RSS measurements from Alice, h_{ea} and Bob, h_{eb} by eavesdropping. The goal is to get an identical key, so Eve can leak the confidentiality of the message between Alice and Bob. The attacker, Eve also

assumed to be more than half the wavelength ($d > \lambda/2$) from the position of Alice and Bob. If the attacker is far from authorized parties, the RSS obtained cannot be used to generate an identical secret key because it is not correlated ($h_a \neq h_{ea}$ and $h_b \neq h_{eb}$) [14]. Meanwhile, RSS obtained by Alice and Bob will be highly correlated ($h_a \approx h_b$) if they carry out the measurements within the coherence time [28].

4.2 System Model

The HRKF scheme aims to establish shared secret keys by utilizing the characteristics of wireless channels. Reciprocity is a characteristic of wireless channels that is the principle of forming a secret key based on RSS. In this scheme, Alice and Bob cannot send and receive signals at the same time. Therefore, the channel characteristics obtained between authorized parties are not identical. In this condition, the principle of reciprocity must be fulfilled, so that Alice and Bob can make an identical secret key. To meet the principle of reciprocity, measurements are carried out within the coherence time (T_c). Coherence time is defined as the maximum time duration that the wireless channel response is stable. The Doppler effect can affect the coherence time because there are vehicles movement in V2V communication, where T_c is inversely proportional to the Doppler frequency (f_D). The vehicle velocity (v) of the authorized parties and carrier frequency (f_c) determines the value of f_D as given in Equations 1 and 2.

$$f_D = \frac{v}{\lambda} \tag{1}$$

$$\lambda = \frac{3x10^8\ m/s}{f_c} \tag{2}$$

Conversely, randomness can be fulfilled if the time interval of measurement exceeds the coherence time. The high randomness of channel characteristics makes it difficult for an attacker to get an identical key to authorized parties.

4.3 HRKF Scheme

The proposed HRKF scheme consists of four stages, including channel characteristics measurement, reciprocal enhancement, quantization and encoding, and randomness extraction and key verification. The sequence of the key formation stages is shown in Figure 2. The first stage is used to collect characteristics of wireless channels between authorized parties. In this scheme, channel characteristics are obtained from the signal sent by using the ping command. Alice sends a ping to Bob at time t, then Bob measures and stores the RSS received from Alice, expressed as h_b. At time t', Bob responds to Alice, then Alice measures and stores the RSS received from Bob, expressed as h_a. To ensure channel reciprocity, the value of $(t - t')$ must be less than the coherence time. Thus, Bob must respond as quickly as possible after receiving

a signal from Alice. Note that we cannot be sure Bob can respond quickly in coherence time. However, we can adjust the measurement time interval (T_m) that is smaller than the coherence time. Thus, the characteristics of wireless channels are highly correlated. The process of measuring wireless channel characteristics is carried out alternately. At the end of the channel characteristics measurement stage, Alice and Bob get several m RSS expressed in Equations 3 and 4.

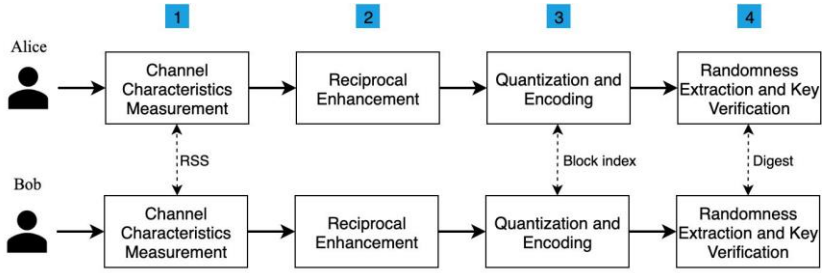

Figure 2. HRKF Scheme

$$h_a = [h_a(1), h_a(2), h_a(3), \dots, h_a(m)]^T \quad (3)$$

$$h_b = [h_b(1), h_b(2), h_b(3), \dots, h_b(m)]^T \quad (4)$$

Eve, who was on the same network as Alice and Bob, eavesdropped on the characteristics of the channels exchanged by the authorized parties. He can receive h_{ea} from Alice and h_{eb} from Bob without sending a ping command. If Alice and Bob get m RSS, then Eve also gets RSS in the same amount as shown in Equations 5 and 6. Because it is assumed that the distance of Eve is more than 1/2 wavelength, the channel information obtained does not correlate with authorized parties.

$$h_{ea} = [h_{ea}(1), h_{ea}(2), h_{ea}(3), \dots, h_{ea}(m)]^T \quad (5)$$

$$h_{eb} = [h_{eb}(1), h_{eb}(2), h_{eb}(3), \dots, h_{eb}(m)]^T \quad (6)$$

An illustration of the mechanism for measuring channel characteristics between Alice and Bob is shown in Figure 3.

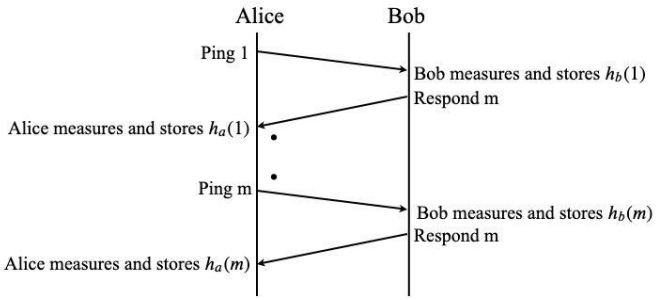

Figure 3. RSS Measurement between Alice and Bob

The second stage is reciprocal enhancement which aims to increase RSS correlation between Alice and Bob. We use the second order polyomial regression method. Second order polynomial Regression is known as quadratic for each block of RSS data as shown in Equation 7.

$$h_j = a_0 + a_1 x_j + a_2 {x_j}^2 \tag{7}$$

where h_j is the RSS data at time x_j with $j = (1, 2, 3, \dots, m)$. The polynomial regression Equation can be shown in Equation 8. We use the elimination method to get 3 unknown polynomial coefficients (a_0, a_1, a_2).

$$\begin{aligned} \sum h_j &= (a_0.m + a_1.\sum x_j + a_2.\sum {x_j}^2) \\ \sum x_j h_j &= (a_0.x_j + a_1.\sum {x_j}^2 + a_2.\sum {x_j}^3) \\ \sum {x_j}^2 h_j &= (a_0.{x_j}^2 + a_1.\sum {x_j}^3 + a_2.\sum {x_j}^4) \end{aligned} \tag{8}$$

The third stage is quantization and encoding using the fixed threshold quantization (FTQ) method. In this stage, RSS data is divided into 8 blocks where each block will be divided into 4 groups based on 3 certain thresholds. The threshold utilizes the mean and standard deviation of each RSS block, shown as Equation 9. The FTQ method is a modification of the MMB quantization method, but the threshold used is permanent in order to obtain a high BFR.

$$Q_u = \begin{cases} -\infty,\ \mu - 10 * \sigma & ; group\ 1 \\ \mu - 10 * \sigma,\ \mu & ; group\ 2 \\ \mu,\ \mu + 10 * \sigma & ; group\ 3 \\ \mu + 10 * \sigma, \infty & ; group\ 4 \end{cases} \tag{9}$$

Furthermore, RSS data in each group is encoded into 2 binary bits, group 1 = 10, group 2 = 01, group 3 = 11, and group 4 = 00. The quantization result using MMB quantization is K_u as shown in Equation 10, where m is the number of RSS channel characteristics. There are no wasted channel characteristics so the size of K_u is $2 \times m$.

$$K_u = [Q_u(1), Q_u(2), \dots, Q_u(m)]^T \tag{10}$$

Then, K_u sequences are divided into several blocks, each consisting of 3 binary bits to be processed using a level crossing algorithm. The purpose of this algorithm is to increase the randomness of the key bits generated from the quantization output. One block will be converted to single bit 0 or 1 if all three bits in the block are the same. Otherwise, the block will be discarded. In this condition, there is a block index exchange between two authorized parties. If Alice removes the x-block, Alice sends the index of block to Bob. Bob will also

delete his x-block. This also applies if Bob deletes the y-block and sends the block index to Alice. Alice will also delete her y-block. Thus, the level crossing algorithm can also reduce the value of BER.

The next stage is randomness extraction and verification. Key randomness is very important for cryptographic schemes so that the attacker cannot guess the key used to encrypt and decrypt messages easily. The key obtained as an output from the quantization stage does not fully meet the randomness requirements even though it has been processed using the Level Crossing algorithm. We use Universal Hash to increase the randomness of the key in order to meet the minimum entropy requirement, which is 0.01. The randomness level was tested using the National Institute of Standards and Technology (NIST) statistical tests. The output from Universal Hash is a number of 256-bit keys that have different entropy. Then a key that has the highest entropy is chosen as the secret key agreed by Alice and Bob. In this case, the key is called the best key.

The best key from Alice is not necessarily the same as Bob because the key that has the highest entropy in Alice is not necessarily the same as the key in Bob. Therefore, we use SHA-256 as verification to guarantee that the keys agreed between two authorized parties are the same. The verification process uses the digest of the best key to be exchanged so that the attacker does not know the actual best key. The best key between Alice and Bob is identical if the digest received is the same.

4.4 Encription and Decription Process

To secure secret messages on V2V communication you can use symmetric cryptography. We use a combination of AES-256 with SHA-256. An illustration of the message encryption and decryption process between Alice and Bob is shown in Figure 4. Alice uses the best key obtained to encrypt the original message into ciphertext. Furthermore, the ciphertext is processed using the SHA-256 function to provide higher security. The ciphertext is sent together with Alice's digest to Bob. To convince Bob that the sender is Alice, Bob must process the ciphertext that was received using SHA-256. If Bob's digest results are the same as Alice's digest, Bob decrypts the ciphertext using thes best key to produce the original message.

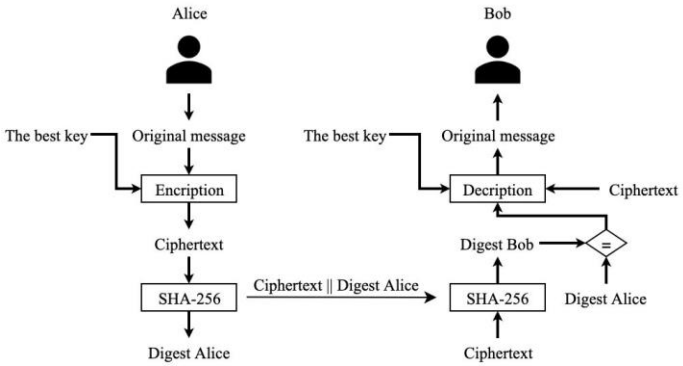

Figure 4. The process of Securing Messages using AES-256

4.5 Performance Metrics

There are five performance metrics to determine the performance of the HRKF scheme. The measurement position of each performance metric in the HRKF scheme is shown in Figure 5.

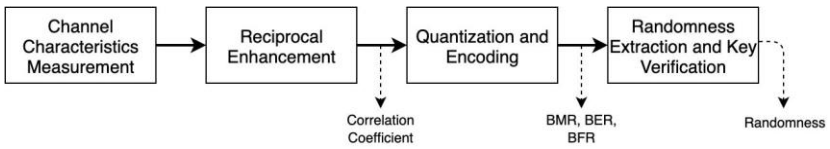

Figure 5. Position of Performance Metrics in the HRKF scheme

Performance metrics in this reseacrh include correlation coefficient of RSS measurement and RSS with high reciprocity, BMR, BER, BFR, and randomness. A detailed explanation of the five performance metrics are as follows:

1. Correlation coefficient

The correlation coefficient of RSS between Alice and Bob were tested to determine the effect of using the second order polynomial regression method at the pre-processing stage. An increase in the correlation coefficient of an authorized parties indicates the success of the method used in terms of increasing channel reciprocity. In order to have the possibility to get an identical key, the correlation coefficient must be getting closer to 1.

2. Bit Mismatch Rate (BMR)

BMR is a comparison of the number of mismatch bits between Alice and Bob with the total bits after the quantization and encoding stage using the FTQ method. This metric will affect the next stage in the HRKF scheme. If the BMR value is very high, many bits are discarded so that the number of bits produced is smaller.

3. Bit Error Rate (BER)

BER is a comparison of bit mismatches between Alice and Bob with the total bits produced after the level crossing process. This metric shows the success of the proposed FTQ method. The HRKF scheme does not use the error correction stage. Therefore, the BER must be equal to 0 before going through the randomness extraction and key verification stage.

4. Bit Formation Rate (BFR)

BFR is the total number of bits generated in each RSS sample after the level crossing process. The more random bits that are obtained, the more bits are wasted. This causes lower BFR. The more consecutive 1 or 0 bits, the higher the BFR. The higher BFR indicates that the method used is suitable for V2V communication scenarios.

5. Randomness

The randomness of the key was measured using the NIST test. In this case, we use 7 parameters on the NIST-test to test this metric. If each parameter value is more than 0.01, the secret key meets the randomness requirements.

5. EXPERIMENT AND ANALYSIS

This section describes two mechanisms including a description of the experiment and analysis of the HRKF scheme. We describe the devices and scenarios in the experiment implementation section. Meanwhile, the analysis section explains the performance evaluation of the HRKF scheme and comparison with other existing schemes.

5.1 Implementation of Experiment

To evaluate the HRKF scheme that we have proposed, we implemented using three Raspberry Pi 3 Model B devices with the specifications in Table 1. The wireless connectivity used is WiFi because of this research was implemented in V2V communication. Two Raspberry Pi became Alice and Bob as authorized parties, and the other Raspberry Pi became Eve as an eavesdropper. Each device is equipped with an 802.11ac wireless USB adapter with a frequency of 5.8 GHz to measure wireless channel characteristics. We conducted an HRKF scheme in an outdoor environment to support the V2V communication scenario.

Table 1. The Spesification of Raspberry Pi 3 Model B

Spesification	**Raspberry Pi 3 Model B**
Processor	Broadcom BCM2837 chipset
CPU	1.2 GHz Quad-Core ARM Cortex-A53 (64-bit)
Memory	1 GB LPDDR2
Operation System	Linux, Raspian, Windows 10
Storage	Micro SD port
Wireless Connectivity	802.11n wireless LAN (WiFi), Bluetooth 4.1, Bluetooth Low Energy (BLE)
Power	Micro USB 5V, 2.5 A

Figure 6. Measurement Scenario

In this research, we conducted several experiments on Suramadu Street, Surabaya. In Figure 6, Alice and Bob are placed 3 meters away and moving at the same constant velocity. The farther the distance between Alice and Bob will decrease the correlation coefficient of the measurement results so that the bit mismatch will increase. With a distance of 3 meters provides the most optimal measurement of the correlation coefficient. While Eve is behind Bob as far as 3 meters to eavesdrop on RSS from Alice and Bob. The velocity of Eve's vehicle follows the velocity of the authorized parties. Both authorized and unauthorized parties collected 2000 RSS data as a key formation source. There are 6 experiments with varying velocities and time intervals. Vehicle velocities are 40 km/hour, 50 km/hour, and 60 km/hour. The length of the track needed to get 2000 RSS data at each velocity are about 0.2 km, 0.15 km and 0.1 km, respectively. Due to the length of the track is not too long, we used a constant velocity. Based on the calculation of the Doppler effect, the coherence time for each speed is 4.7 ms, 3.7 ms, and 3.1 ms, respectively. In this experiment we measured with 2-time intervals, the first is less than coherence time and the second is more than coherence time for each velocity. The time intervals that are within the coherence time will fulfill the principle of channel reciprocity. While time intervals that are outside the coherence of time will fulfill the key randomness. Table 2 shows the various experiments conducted in this research.

Table 2. Research Experiment

Experiment	Vehicle's Velocity	Interval Time of Measurement	Additional Information
1	40 km/hour	3.5 ms	Less than T_c
2		10 ms	More than T_c
3	50 km/hour	2.5 ms	Less than T_c
4		7 ms	More than T_c
5	60 km/hour	2 ms	Less than T_c
6		5 ms	More than T_c

5.2 Experimental Result

This section explains the performance metrics results of the proposed scheme as well as comparisons with other existing schemes.

5.2.1 Correlation Coefficient

RSS measurement data between Alice and Bob have an initial correlation coefficient below 0.5 as shown in Table 3. Experiments with interval time less than coherence time have a higher correlation coefficient than experiments with interval time more than coherence time. This is because the measurement of RSS within the time interval allows RSS obtained by Alice and Bob to be similar, so it has a high correlation. Based on Table 3, experiment 1 has the highest correlation coefficient and experiment 6 has the lowest correlation coefficient. The lower the vehicle velocity, the higher the correlation

coefficient of RSS measurements, so Alice and Bob have the highest RSS correlation coefficient at velocity of 40 km/hour. Meanwhile, the correlation coefficient between Eve and the legitimate parties is close to 0 and there is also a negative correlation. The smaller the correlation coefficient, the more difficult it is to produce an identical secret key because the channel characteristics obtained are increasingly different.

The correlation coefficient between Alice and Bob has not been fulfilled for processing in the second stage. Therefore, we process RSS measurement data using polynomial regression to increase the correlation coefficient. The results of increasing the correlation coefficient are shown in Table 3. After the pre-process stage, Alice and Bob's correlation coefficient increased significantly to reach a correlation coefficient of 0.9, except in experiment 6. Experiment 2 has the highest correlation coefficient after the pre-processing stage, which is 0.99. The polynomial regression method is also used by Eve to increase the correlation coefficient obtained from authorized users. Based on Table 3, Eve can also increase the correlation coefficient in each experiment. But the correlation coefficient increases only on one side, so Eve is still difficult to obtain a key that is identical to the authorized parties.

Table 3. Measurement and Increased Correlation Coefficient

Experiment	Vehicle	Measurement Correlation Coefficient	Increased Correlation Coefficient
1	Alice and Bob Alice and Eve Bob and Eve	0.4891 -0.1081 0.2345	0.9206 -0.6260 0.7890
2	Alice and Bob Alice and Eve Bob and Eve	0.4297 0.2845 0.1566	0.9976 0.4387 0.7955
3	Alice and Bob Alice and Eve Bob and Eve	0.3396 0.0436 -0.3030	0.8856 0.4568 0.0324
4	Alice and Bob Alice and Eve Bob and Eve	0.2363 -0.1912 -0.3143	0.9620 -0.6246 -0.8841
5	Alice and Bob Alice and Eve Bob and Eve	0.2640 -0.1030 -0.4097	0.9851 0.0020 -0.5160
6	Alice and Bob Alice and Eve Bob and Eve	0.1797 -0.5030 0.0880	0.3465 -0.6711 0.1185

From all the results obtained it can be concluded that the polynomial regression method at the pre-process stage can increase the correlation

coefficient of Alice and Bob significantly more than 100%. Increasing the correlation coefficient has a large impact on the possibility of producing identical secret keys. Thus, the pre-process stage of the HRKF scheme can increase the channel reciprocity between Alice and Bob.

5.2.2 Bit Missmatch Rate (BMR)

The second stage is quantization and encoding, where the pre-processed RSS data is converted to binary bits. In this research, RSS data are divided into 8 blocks. We use the FTQ method on each RSS data block to divide into 4 groups. Each group is bounded by an upper and lower threshold based on averages and standard deviations. Furthermore, each RSS value is converted to 2-bits so that the total number of bits after the quantization and encoding process is 4000-bits for the whole experiment. The bits produced by Alice are not necessarily the same as the bits produced by Bob, although the correlation coefficient has been increased. This is because the RSS grouping on Alice's side is not the same as Bob's, so the encoding results will also be different. Table 4 shows the BMR values of all experiments in this research.

Table 4. Performance of HRKF Scheme in Terms of BMR

Experiment	Vehicle	BMR (%)
1	Alice and Bob Alice and Eve Bob and Eve	12.60 43.00 55.60
2	Alice and Bob Alice and Eve Bob and Eve	19.20 40.80 60.00
3	Alice and Bob Alice and Eve Bob and Eve	15.10 31.70 40.00
4	Alice and Bob Alice and Eve Bob and Eve	8.40 55.20 60.00
5	Alice and Bob Alice and Eve Bob and Eve	5.10 41.90 41.10
6	Alice and Bob Alice and Eve Bob and Eve	35.95 39.30 36.55

Based on Table 4, BMR between Alice and Bob in all experiments did not exceed 20%, except in experiment 6 which had the smallest correlation coefficient even after the pre-processing stage. Experiments that have the highest correlation coefficient do not guarantee to have the lowest bit mismatch. In Table 3, Alice and Bob have the highest correlation coefficient in

experiment 2, which is 0.99%. However, the lowest BMR between Alice and Bob was in experiment 5, which was 5.10%. On the other hand, BMR between Eve and authorized parties is between 30% to 60%. From these results it can be concluded that the attacker has a higher number of bit mismatches than the legitimate user, so Eve is difficult to make an identical key.

5.2.3 Bit Error Rate (BER) dan Bit Formation Rate (BFR)

The bits sequence produced by Alice and Bob still contains many consecutive 0 and 1 bits. Therefore, we use a level crossing algorithm to improve bit randomness. All bits are divided into several blocks, each block consisting of 3 bits. Blocks will be discarded if they contain 0 and 1 bits. Otherwise, each block will be converted to a single 1 or 0 bit. This algorithm can also reduce the number of bit mismatches after the quantization and encoding stages. The BER value between Alice and Bob is equal to 0% in all experiments. This is because there is an unused block index exchange between authorized parties. Therefore, the HRKF scheme does not require the bit error correction stage. On the other hand, Eve knows the block index exchanged between Alice and Bob so Eve also discards the block at that index. However, Eve does not send index blocks to authorized users so that the number of Eve bits after the crossing level process is not the same as the bits from authorized parties. Therefore, BER from Eve cannot be analyzed. Discarding blocks in the level crossing process causes the total number of final bits in the whole experiment is not the same. The fewer bits discarded, the more bits produced so that the BFR will also increase. Table 5 shows the BFR values for all experiments.

The highest BFR between Alice and Bob is in experiment 5, which is 80.00 bps and the lowest BFR is in experiment 6, which is 20.40 bps. These results are related to the BMR value, where experiment 5 has the lowest BMR value and experiment 6 has the highest BMR. But for other experiments the BMR value does not determine the value of the BFR. A low number of bit mismatches does not necessarily result in a high BFR, and vice versa. This result is caused by the level crossing algorithm that works based on blocks to increase bit randomness. Measurement time intervals also affect the BFR between Alice and Bob. Experiments carried out in coherence time have a higher BFR than trials with time intervals exceeding coherence time. This is caused by randomness in the experiment with the time interval below the coherence time is smaller than above the coherence time so that many bits are discarded during the process of level crossing.

Meanwhile, Eve has a smaller BFR than the authorized parties in all experiments. In fact, there are several experiments where BFR Eve is 0 bps which means there are no bits left. These results indicate that the total number of bits produced by Eve after the level crossing is very low due to block removal in this process. From the BFR results obtained, Eve could not produce an identical secret key because the required key size was 256-bits to encrypt and decrypt messages using AES-256. Thus, the HRKF scheme is secure from

passive attacks such as eavesdropping because the attacker is unsuccessful in establishing the same key despite knowing all the methods used by authorized parties.

Table 5. Performance of HRKF Scheme in terms of BFR

Experiment	Vehicle	BFR (bps)
1	Alice and Bob Alice and Eve Bob and Eve	51.26 0.00 0.00
2	Alice and Bob Alice and Eve Bob and Eve	21.50 0.00 0.00
3	Alice and Bob Alice and Eve Bob and Eve	58.10 2.84 1.51
4	Alice and Bob Alice and Eve Bob and Eve	45.05 2.15 3.90
5	Alice and Bob Alice and Eve Bob and Eve	80.00 0.00 0.00
6	Alice and Bob Alice and Eve Bob and Eve	20.40 0.00 4.15

5.2.4 Randomness

The last stage in the HRKF scheme is to increase the randomness of the bits resulting from the level crossing process with zero BER. We use the universal hash function to create several random 256-bit key candidates. Of the several key candidates obtained, one key was chosen with the highest approximate entropy to be the best key. The best key is then used by Alice and Bob as a shared secret key to carry out the cryptographic process while communicating on the road. Key randomness is very important because it minimizes the attacker to find out the pattern of the secret key. To ensure key randomness, we use 7 types of tests available on the NIST test. Explanation of the 7 parameters in Table 6 is as follows. The first test is the Approximate Entropy to determine the frequency of possible overlaps of all bit patterns in key sequences. The second test is Frequency to show the proportion of bits 0 and bit 1 in the key sequence. The third test is Block Frequency to determine the ratio of 1 for each block is half a block. The fourth and fifth tests are Forward and Reverse to compare the cumulative number of keys generated with the expected random cumulative number. Forward changes bit 0 to -1, and Reverse changes bit 1 to +1. The sixth test is Run to determine the oscillations of bits 0 or 1 in the key sequence too fast or slow. The final test is

the Longest Run to find out whether the length of 1 tested is consistent with the expected length of 1 from a random sequence.

Table 6. NIST Test Result

Type of Test	1	2	3	4	5	6
Approximate Entropy	0.636	0.714	0.747	0.810	0.622	0.622
Frequency	0.900	0.617	0.708	0.317	0.617	0.617
Block Frequency	0.582	0.582	0.893	0.344	0.582	0.582
Forward	0.746	0.906	0.746	0.338	0.804	0.804
Reverse	0.630	0.630	0.946	0.573	0.974	0.974
Run	0.212	0.814	0.208	0.754	0.790	0.790
Longest Run	0.230	0.648	0.200	0.478	0.357	0.357

The test results of all experiments are shown in Table 6. The best key in each experiment fulfills the randomness requirement with parameter values of more than 0.01 in all types of tests. These results indicate that the key established from the HRKF scheme can be used to secure V2V communication. Based on Table 6, experiments with interval times exceeding coherence time with the same speed have higher or at least equal approximate entropy than experiments with interval times less than coherence time.

5.2.4 Comparison with Other Schemes in Existing Research

In this research, we tested the value of BFR by comparing the performance of the HRKF scheme with several other key formation schemes, including scheme[22], scheme [21], scheme [23], and scheme [18]. The difference between the HRKF scheme and some comparison schemes is the method used for the pre-processing and quantization stages. For the pre-processing stage, scheme [22] uses the hybrid polynomial regression and Kalman filter while scheme [21], [23], and [18] use the Kalman filter with different parameters. For the quantization stage, scheme [22] and [23] use the MMB quantization method, scheme [21] uses the adaptive quantization method, and scheme [23] uses the Mathur quantization. Figure 7 shows the results of the BFR comparison of several schemes.

Overall, the HRKF scheme had the highest BFR in all trials compared to the existing scheme. The HRKF scheme can significantly increase BFR from 40% to more than 100%. The highest increase in BFR occurs when the HRKF scheme is compared with the study [18]. This is because the scheme [18] uses a single-bit quantization method that converts one RSS value into one bit and discards several bits that are between the threshold. This quantization method is commonly called lossy quantization which will affect the number of bits produced. Meanwhile, other comparison schemes use the lossless quantization method, no bits are discarded during the quantization process.

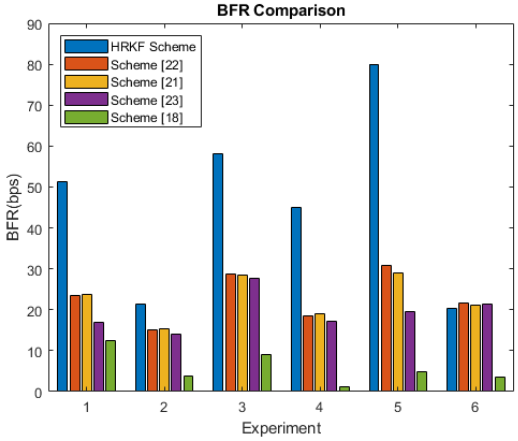

Figure 7. BFR Comparison of Several Schemes

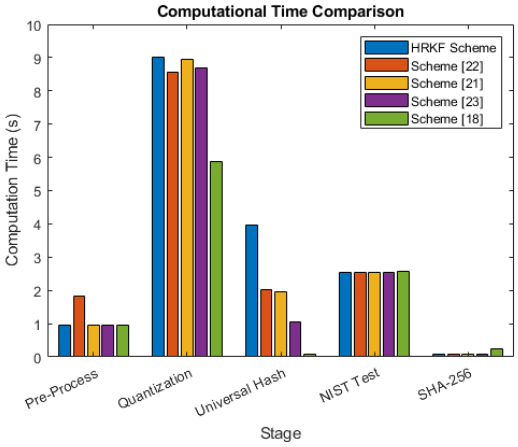

Figure 8. Computational Time Comparison of Several Schemes

Figure 8 shows the computational time comparison between the proposed scheme and the comparison schemes. The HRKF scheme requires a computational time of 16.5 seconds. Scheme [22] requires a computational time of 15 seconds, scheme [21] requires a computational time of 14.5 seconds, scheme [23] requires a computational time of 13.3 seconds, and scheme [18] requires a computational time of 9.7 seconds. In the pre-process stage, schemes that use the non-hybrid method have lower computational time than schemes that use the hybrid method. Therefore, scheme [22] has the highest computational time at the pre-process stage. At the quantization stage, the scheme [18] requires lower computational time than other schemes because it uses the single-bit quantization method, while other schemes use multi-bit. The proposed scheme requires the highest computational time at the Universal Hash stage. This is influenced by the number of bits produced (BFR). The greater the BFR, the longer the computation time because there is a multiplication of bits with a 256x256 hash table. In general, the proposed scheme requires higher computational time than existing researchs. However,

the proposed scheme has better performance in terms of BFR as well as providing high security guarantees from passive attacker.

5.2.5 Discussion

V2V communication security requires low computing time to achieve driving safety. One way to reduce the computing time of a secret key formation scheme is to replace the Universal Hash into Generic Hash Function that has no collison with high randomness rate satisfying NIST Test suite requirement.

6. CONCLUSION

In this research, we propose an effortless RSS-based secret key formation scheme (HRKF) to establish shared secret keys used in V2V communication. The purpose of the HRKF scheme is to produce keys with high BFRs and zero BER through non-complex schemes. To increase channel reciprocity, we use polynomial regression. At the quantization stage, we propose the FTQ method combined with a level crossing algorithm to reduce bit mismatch and minimize discarded bits. The experimental results show that the HRKF scheme can increase BFR by at least 40% and produce zero BER in all experiments. Furthermore, the best key obtained also fulfills the randomness requirements of the NIST test. The HRKF scheme can be proven to have high security from passive attacks because the attacker did not succeed in making one identical key.

Acknowledgements

The author would like to thank to Penelitian Dasar Unggulan Terapan (PDUPT), 2020 from Kementrian Riset, Teknologi dan Pendidikan Tinggi (Kemristekdikti) which have supported the funding of this research.

REFERENCES

[1] M.S. Sheikh, J. Liang, and W. Wang, **A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs)**, *Sensors*, vol. 19, pp. 1-40, 2019.

[2] H.P.D. Nguyen and R. Zoltan, **The Current Security Challenges of Vehicle Communication in the Future Transportation System**, *International Symposium on Intelligent Systems and Informatics*, pp. 161-165, 2018.

[3] R. Al-Mutiri, M. Al-Rodhaan, and Y. Tian, **Improving Vehicular Authentication in VANET using Cryptography**, *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 10, no. 1, pp. 248-255, 2018.

[4] M.S. Sheikh and J. Liang, **A Comprehensive Survey on VANET Security Services in Traffic Management System**, *Hindawi Wireless Communication and Mobile Computing*, vol. 2019, pp. 1-23, 2019.

[5] M.B Mansour, C. Salama, H.K. Mohamed, and S.A. Hammad, **VANET Security and Privacy – An Overview**, *International Journal of Network*

Security & Its Applications (IJNSA), vol. 10, no. 2, pp. 13-34, 2018.

[6] A. Ambekar, M. Hassan, and H.D. Schotten, **Improving Channel Reciprocity for Effective Key Management Systems**, *Conference Proceeding International Symposium Signal Systems Electronic*, pp. 1-4, 2012.

[7] R. Lin, L. Xu, H. Fang, and C. Huang, **Efficient Physical Layer Key Generation Technique in Wireless Communications**, *EURASIP Journal on Wireless Communications and Networking*, pp. 1-15, 2020.

[8] J. Zhang, T.Q. Duong, A. Marshall, and R. Woods, **Key Generation from Wireless Channels: A Review**, *IEEE Access*, vol. 4, pp. 614-626, 2016.

[9] A. Sudarsono, M. Yuliana, and P. Kristalina, **A Reciprocity Approach for Shared Secret Key Generation Extracted from Received Signal Strength in the Wireless Networks**, *International Electronics Symposium Engineering Technology and Applications (IES-ETA)*, pp. 170-175, 2018.

[10] O.A. Topal, G.K. Kurt, and B. Ozbek, **Key Error Rates in Physical Layer Key Generation: Theoritical Analysis and Measurement-Based Verification**, *IEEE Wireless Communications Letters*, vol. 6, no. 6, pp. 766-769, 2017.

[11] H. Fang, X. Wang, and L. Hanzo, **Learning-Aided Physical Layer Authentication as an Intelligent Process**, *IEEE Transactions on Communications*, vol. 67, no. 3, pp. 2260-2273, 2019.

[12] L. Cheng, L. Zhou, B. Seet, D. Ma, and J. Wei, **Efficient Physical-Layer Secret Key Generation and Authentication Schemes Based on Wireless Channel-Phase**, *Hindawi Mobile Information Systems*, vol. 2017, pp. 1-13, 2017.

[13] K. Moara-Nkwe, Q. Shi, G.M. Lee, and M.H. Eiza, **A Novel Physical Layer Secure Key Generation and Refreshment Scheme for Wireless Sensors Networks**, *IEEE Access*, vol. 4, pp. 1-15, 2016.

[14] M. Yuliana, Wirawan, and Suwadi, **An Efficient Key Generation for the Internet of Things Based Synchronized Quantization**, *Sensors*, vol. 19, pp. 1-25, 2019.

[15] D. Kreiser *et al*, **On Wireless Channel Parameters for Key Generation in Industrial Environments**, *IEEE Access*, vol. 5, pp. 79010-79025, 2017.

[16] X. Zhu, F. Xu, E. Novak, and C.C. Tan, **Using Wireless Link Dynamics to Extract a Secret Key in Vehicular Scenarios**, *IEEE Transactions on Mobile Computing*, pp. 1-14, 2017.

[17] M. Yuliana, Wirawan, and Suwadi, **Performance Evaluation of the Key Extraction Schemes in Wireless Indoor Environment**, *International Conference on Signals and Systems (ICSigSys)*, pp. 138-144, 2017.

[18] A. Sudarsono, M. Yuliana, P. Kristalina, and A.R. Barakbah, **An Implementation of Shared Key Generation Extracted from Received Signal Strength in Vehicular Ad-Hoc Communication**, *Sixth International Symposium on Computing and Networking (CANDAR)*, pp. 57-65, 2018.

[19] Y.E.H. Shehaded and D. Hogrefe, **A Survey on Secret Key Generation Mechanisms on the Physical Layer in Wireless Networks**, *Security and Communication Networks*, vol 8, pp. 332-341, 2015.
[20] X. Li, J. Liu, Q. Yao, and J. Ma, **Efficient and Consistent Key Extraction Based on Received Signal Strength for Vehicular Ad Hoc Networks**, *IEEE Access*, vol. 5, pp. 5281-5291, 2017.
[21] M. Yuliana, Wirawan, and Suwadi, **Performance Analysis of Loss Multilevel Quantization on the Secret Key Generation Scheme in Indoor Wireless Environment**, *International Journal on Advanced Science Engineering Information Technology*, vol. 9, no. 1, pp. 100-108, 2019.
[22] I.T. Dewi, A. Sudarsono, P. Kristalina, and M. Yuliana, **Reciprocity Enhancemenr in V2V Key Generation System by using HPK Method**, *International Electronic Symposium (IES)*, pp. 6-13, 2019.
[23] M. Yuliana, Wirawan, and Suwadi, **Performance Improvement of Secret Key Generation Scheme in Wireless Indoor Environment**, *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 9, no. 3, pp. 474-483, 2017.
[24] D.N. Purnamasari, A. Sudarsono, and P. Kristalina, **Medical Image Encryption Using Modified Identity Based Encryption**, *EMITTER International Journal of Engineering Technology*, vol. 7, no. 2, pp. 524-536, 2019.
[25] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, **Wireless Secret Key Generation Exploiting Reactance-Domain Scalar Response of Multipath Fading Channels**, *IEEE Transactions on Antennas and Propagation*, vol 53, no. 11, pp. 3776-3784, 2005.
[26] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, **Radio-telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel**, *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, pp. 128-139, 2008.
[27] S. Jana, S.N. Premnath, M. Clark, S.K. Kasera, N. Patwari, and S.V. Krishnamurthy, **On the Effectiveness os Secret Key Extraction from Wireless Signal Strength in Real Environments**, *Proceedings of the 15th ACM International Conference on Mobile Computing and Networking*, pp. 321-332, 2009.
[28] A. Ambekar and H.D. Schotten, **Enhancing Channel Reciprocity for Effective Key Management in Wireless Ad-hoc Networks**, *Conference Vehicular Technology (VTC Spring)*, 2014.