International Journal on
Advanced Science
Engineering
Information Technology

Vol.10 (2020) No. 6
ISSN: 2088-5334

MAPI: Key Generation Scheme for Security in V2V Communication Environment based RSS

Inka Trisna Dewi[a,1], Amang Sudarsono[a,2], Prima Kristalina[a,3], Mike Yuliana[a,4]

[a] *Department. of Electrical Engineering, Politeknik Elektronika Negeri Surabaya, Surabaya 60111, Indonesia*
E-mail: [1]inkatrisnad@gmail.com; [2]amang@pens.ac.id; [3]prima@pens.ac.id; [4]mieke@pens.ac.id

***Abstract*—Vehicular ad-hoc network is an exciting study that aims to improve driver safety in driving. Vehicle-to-vehicle (V2V) is communications between vehicles that occurs on a VANET using wireless channels. This channel allows vehicles to share personal or safety information with other vehicles. Vehicle communication is potentially vulnerable to adversaries' security attacks that can harm the driver and other legitimate users. Therefore, it requires a high-security system. This research proposes a new scheme, namely the MAPI (Mike-Amang-Prima-Inka), as a modified secret key generation scheme obtained from received signal strength (RSS) values. Our research focuses on obtaining a symmetric key that has a high key formation speed (KFS) with a low-key discrepancy level (KDL), while still thinking about the randomness and ensure safety from passive attackers. In the pre-processing, we use a combination of Kalman Filter and Polynomial Regression by modifying the parameters to produce the best performance. We also modified the grey code in the Modified Multibit (MMB) Quantization method to reduce the quantization bit mismatch. Our approach to the MAPI scheme can assign symmetric keys with better performance than existing schemes, increasing KFS and decreasing KDL up to 100%. Moreover, the scheme can generate a symmetric key that deals with NIST's statistical tests.**

***Keywords*— vehicle-to-vehicle; secret key generation scheme; modified pre-processing method; modified quantization method.**

I. Introduction

In recent years, the vehicle ad-hoc network (VANET) is one of the most promising researches along with the development of the vehicle industry and wireless communication technology. VANET is part of a mobile ad-hoc network (MANET), which refers to an ad-hoc network that provides communication over a wireless network [1]. There are 2 kinds of communication on VANET, such as Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) communications. RSU (Road-Side Unit) is used for infrastructure modules installed along the side of the road, while OBU (On-Board Unit) is a module installed in vehicles [2]. Vehicles exchange messages directly without an intermediary entity due to V2V communication used dedicated short-range communication (DSRC) standard at a frequency of 5.9 GHz [3]. The main application of V2V communication is for safety rides, such as preventing vehicle clashes, obstacle warnings, lane change warnings, and others. by exchanging information with other vehicles [4].

This technology is susceptible to various security attacks, such as falsifying road congestion messages, giving false warnings, delays messages, attacker monitors important data exchanged between authorized parties, attacks network accessibility, and others. Therefore, high-security systems are an essential concern for secure V2V communication. Some security requirements include availability, message authentication and integrity, the confidentiality of the message content, non-repudiation, and privacy protection [5].

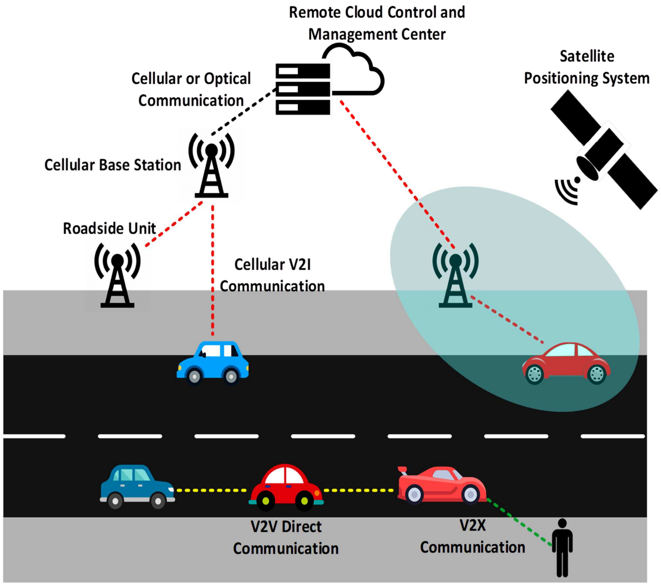
Remote Cloud Control and Management Center
Satellite Positioning System
Cellular or Optical Communication
Cellular Base Station
Roadside Unit
Cellular V2I Communication
V2V Direct Communication
V2X Communication

Fig. 1 DSRC-based communications [4]

A classic cryptographic scheme can be used to meet the security of V2V communication. The scheme depends on the key used by two legitimate parties that will communicate. It can be divided into two; asymmetric cryptographic schemes and symmetric cryptographic schemes [6]. Asymmetric cryptographic schemes use a different personal key and the same universal key, while symmetric cryptographic schemes use the same symmetric key. These classic cryptographic schemes are vulnerable to attacks because it requires symmetric key distribution between legitimate users. Also, asymmetric schemes require an infrastructure of key management to be secured to disseminate universal key, and most algorithms consume much computational time [7]. The main challenge in-vehicle networks are high mobility, so it requires less-complex algorithms for security. Also, key management needs to be explicitly handled because the algorithm used in security depends on the key [8].

The secret key generation (SKG) scheme is the solution to deal with these problems. The SKG used the characteristics of wireless channels that are unpredictable and random [9], 10]. The fundamental of channel reciprocity is used to show the similarity of channel characteristics of the sender and receiver if the measurement is in the coherence time [11]. There are several parameters for obtaining information from a wireless network channel: received signal strength (RSS) [12], [13], channel status information (CSI) [14], and channel impulse response (CIR) [15]. CIS and CIR are parameters provided by multipath wireless channels. These parameters have three main advantages; uniform distribution of the channel phase to increase critical confidentiality, a higher secret key generation rate, and automatic key extraction [15]. However, most wireless devices need modification to display all channel information, requiring a lot of effort and difficulty [16]. Many studies use RSS-based approaches as parameters of wireless channels to produce secret keys in Physical Layer Security (PLS) [17]. We used RSS as a parameter because of not requiring hardware modification. Also, RSS-based schemes are more reliable in synchronization [18]. RSS is obtained from the average of signals strength received by each legitimate user for a certain period.

There are three performance evaluations in the SKG scheme, namely key discrepancy level (KDL), key formation speed (KFS), and randomness. The trade-off that must be dealt with is that increasing KFS will result in high KDL, and a decrease in KDL will be followed by a low in KFS. RSS-based key generation schemes have low key formation speed (KFS). The smaller the KFS value, the more challenging it is to produce symmetric keys because the cryptographic scheme requires a particular key length, such as AES, requiring a minimum key length of 128 bits. Several studies have modified the conventional SKG scheme by adding a signal pre-processing stage to increase wireless channels' reciprocity [16], [21]. Scheme [16], [20] discards the information reconciliation stage for security reasons. There are two methods of quantization, namely lossless quantization and lossy quantization. The lossy quantization method removes some of the bits extracted from the RSS measurement that does not meet the specified threshold. Therefore, it has a low KFS. In comparison, lossless quantization does not discard any bits, so it has a high KFS.

In this paper, we propose the MAPI scheme as an RSS-based secret key generation scheme. The scheme can improve key symmetrical generation performance compared to other existing schemes in the V2V communication environment. This study indicates that the MAPI scheme can increase the correlation of legitimate users up to 0.99. In terms of KFS and KDL, this scheme can also increase KFS significantly more than 100% and reduce KDL up to 100% compared to the existing scheme. Decreasing the KDL can improve the probability of generating a symmetrical key.

II. Material and Method

This section describes the implementation, the proposed system design, and the performance parameter of the MAPI scheme. The implementation section describes the measurement scenario in V2V communication and the device's specifications when measuring. The system design shows the stages used to generate the symmetric secret key and the MAPI scheme algorithm. The performance parameters are used to show the success of the system being built.

A. Implementation and Experimental Environment

The proposed secret key generation system is implemented on 3 Raspberry Pi 3 (Model B) with Raspbian as the OS. Raspbian is a Linux version explicitly built for the Raspberry Pi. Two devices become Alice and Bob as legitimate users, and the remaining device becomes a non-legitimate user, namely Eve. The high-level programming languages used are Python 3.6 for processing data and C language for NIST Test. Channel characteristics measurement in the V2V environment used an 802.11ac wireless USB adapter that operates at a frequency of 5.8 GHz. It is used to send ICMP packets and measure RSS values between Alice and Bob. Fig. 2 and Fig. 3 shows the devices used in this system.

Fig. 2 Raspberry Pi 3 (Model B)

Fig. 3 Wireless USB adapter 802.11ac

Raspberry 1 (Alice) and Raspberry 2 (Bob) are two legitimate vehicles that create an ad-hoc wireless network to communicate peer-to-peer. Raspberry 3 (Eve) is a non-legitimate vehicle as a passive attacker that intercepts communication between them to get RSS. Therefore, Eve has the potential to generate identical keys with legitimate users. In this scenario, Alice became the initiator, and Bob became the responder. Alice transmits PING with a specific time interval (T_m), then Bob collects RSS measurements based on PING by Alice. Bob 3 meters away from Alice sends RESPOND after a delay (τ), then Alice collects RSS measurement based on RESPOND by Bob. The mechanism of RSS measurements is shown in Fig. 4. In this measurement, we collected 2000 RSS data in Suramadu Street, Surabaya, as shown in Fig. 5.

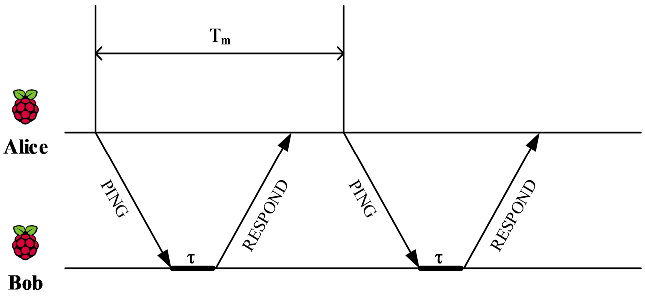

Fig. 4 Mechanism of RSS collection between legitimate users

In this research, there are two measurement conditions, i.e., quiet and crowded conditions, as shown in Table 1 and Table 2. Quiet conditions are expressed as scenario A1 to scenario F1, and crowded conditions are expressed as scenario A2 to scenario F2. We assume the condition is quiet when the volume of the vehicle is low, so there are no obstacles between Alice and Bob. At the same time, the condition is crowded when the volume of vehicles is high. The speed variations of users are 40 km/h, 50 km/h, and 60 km/h. Each speed has two-timed intervals, above and below the coherence time.

TABLE I
QUIET MEASUREMENT CONDITION

Scenario	Quiet Condition	
	Velocity	Interval time
A1	40 km/h	3.5 ms
B1		10 ms
C1	50 km/h	2.5 ms
D1		7 ms
E1	60 km/h	2 ms
F1		5 ms

TABLE II
CROWDED MEASUREMENT CONDITION

Scenario	Crowded Condition	
	Velocity	Interval time
A2	40 km/h	3.5 ms
B2		10 ms
C2	50 km/h	2.5 ms
D2		7 ms
E2	60 km/h	2 ms
F2		5 ms

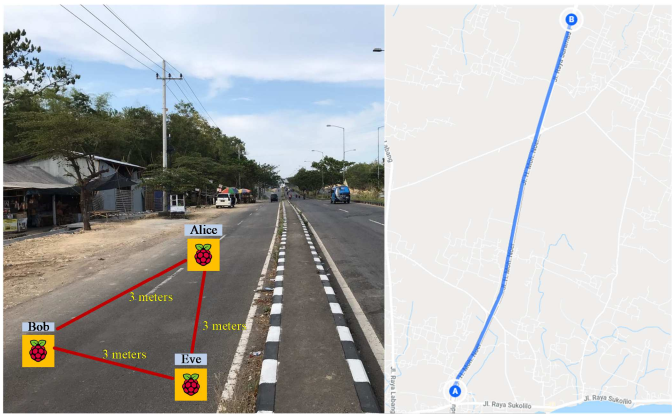

Fig. 5 Measurement route of scenarios

B. *Proposed System Design*

The MAPI scheme consists of four stages to produce symmetric secret key: channel examining, signal pre-processing, quantization, and the last is privacy amplification. The MHPK (modified hybrid Polynomial Regression and Kalman Filter) method is used at the signal pre-processing stage adopted from a previous study [19]. At the second stage, the method used is Dual-Bit Quantization [17] as modified from MMB Quantization combined with a Sequential Bit Remover Technique [19]. The Universal Hash and SHA-256 functions are used at the privacy amplification stage to increase security and key verification between Alice and Bob, respectively. We explain in detail each stage of the proposed MAPI scheme, as shown in Fig. 6.

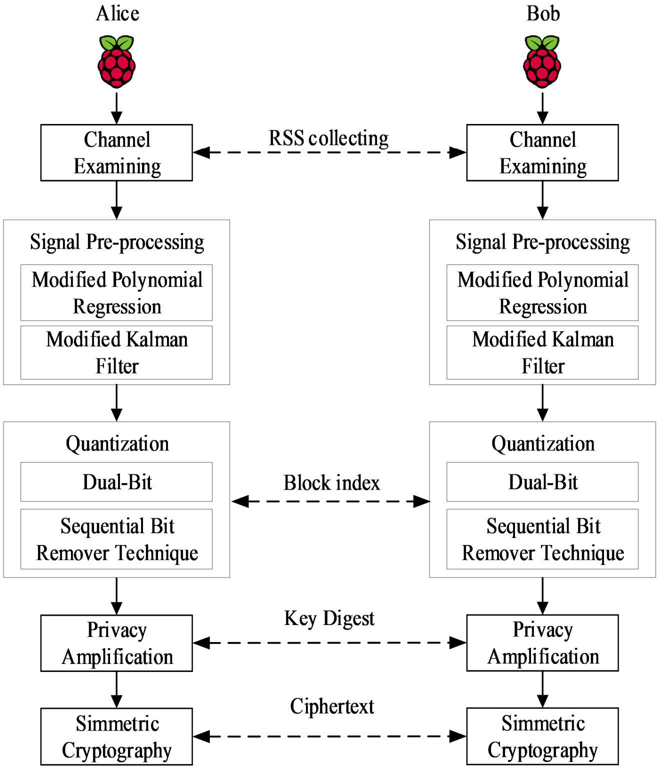

Fig. 6 Proposed MAPI scheme

1) Channel Examining: Channel examining is the first stage in the MAPI scheme to collect randomness from wireless channel characteristics reciprocally to get the RSS values. We captured RSS values between legitimate vehicles by utilizing PING commands that use the ICMP protocol at certain time intervals [21]. We used the V2V environment communication scenario between Alice and Bob as a legitimate vehicle and Eve as an eavesdropper vehicle. Alice and Bob perform channel examining to obtain RSS measurement values with varying vehicle speeds and ping intervals. Meanwhile, Eve tries to capture the legitimate user RSS to generate a key that is identical to them. The scenario design in this paper is shown in Figs. 7.

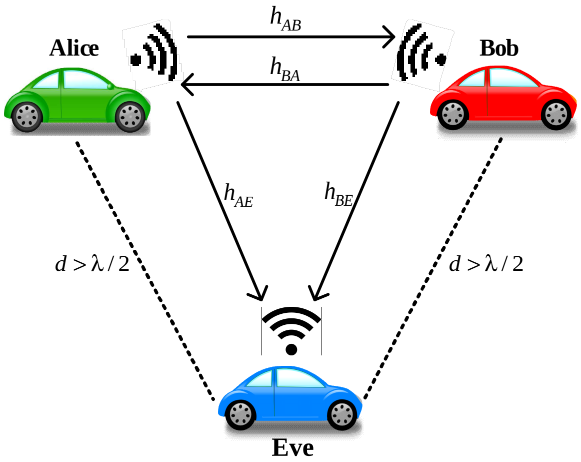

Fig. 7 Scenario design

To produce a similar RSS between two legitimate users, the calculation of the time interval (T_m) in the channel examining is based on coherence time (T_c). The coherence time is inverse to the maximum Doppler frequency (f_d), as shown in Equation (1) [14]. In Equation (2), v is the vehicle speeds of Alice and Bob. In Equation (3), c = 3 x $10^{8,}$ and f_c is the frequency used in V2V communication (5.8 GHz). Therefore, based on the variation in speed, the coherence time values are 4.7 ms, 3.7 ms, and 3.1 ms, respectively.

$$T_c = \frac{1}{f_d} \tag{1}$$

$$f_d = \frac{v}{\lambda} \tag{2}$$

$$\lambda = \frac{c}{f_c} \tag{3}$$

Based on the scenario in Fig. 7, it is assumed that the information channel measured by Alice from Bob is h_{BA} and that measured by Bob from Alice is h_{AB}. Eve tapped Alice and Bob's measurements until she obtained an information channel from Alice (h_{AE}) and from Bob (h_{BE}). After the channel examining stage, the legitimate and non-legitimate user will get a set of RSS values represented in Equations (4), (5), (6), and (7). The principle of wireless channels reciprocity shows that legitimate users will have a high correlation if the measurements are conducted in coherence time, so $h_{AB} \approx h_{BA}$ [16]. Due to the Eve distance is more than $\frac{1}{2}$of the wavelength (λ/2) from Alice and Bob, so it is hard for Eve to produce an identical key because it does not correlate with Alice and Bob [16].

$$h_{AB} = [h_{AB}(1), h_{AB}(2), \dots, h_{AB}(n)] \tag{4}$$

$$h_{BA} = [h_{BA}(1), h_{BA}(2), \dots, h_{BA}(n)] \tag{5}$$

$$h_{AE} = [h_{AE}(1), h_{AE}(2), \dots, h_{AE}(n)] \tag{6}$$

$$h_{BE} = [h_{BE}(1), h_{BE}(2), \dots, h_{BE}(n)] \tag{7}$$

2) Signal Pre-processing: The purpose of this second stage is to increase the RSS correlation coefficient that has been measured by Alice and Bob. We use MHPK method to improve channels reciprocity. It is assumed that Eve also used the same algorithm as legitimate users. In the Polynomial Regression, RSS data measurements are then divided into N blocks as Equation (8). In this case, we divide the RSS data into 20 data blocks.

$$h_y = \left[h_y(1)^T \; h_y(2)^T \; \dots \; h_y(N)^T\right] \tag{8}$$

$$h_i = a_0 + a_1 x_i + a_2 {x_i}^2 \tag{9}$$

$$\begin{bmatrix} M & \sum x_i & \sum {x_i}^2 \\ \sum x_i & \sum {x_i}^2 & \sum {x_i}^3 \\ \sum {x_i}^2 & \sum {x_i}^3 & \sum {x_i}^4 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} \sum h_i \\ \sum x_i h_i \\ \sum {x_i}^2 h_i \end{bmatrix} \tag{10}$$

Each block contains several M RSS data, where subscript y is replaced by BA for Alice, AB for Bob, AE and BE for Eve. In this paper, we model each block of RSS measurement data using the 2nd order polynomial as shown in Equation (9), where h_i is the RSS data at the time x_i with $i = (1,2,3,\dots,M)$. Furthermore, the usual equation of Polynomial in the form of a matrix is shown in Equation (10). Finally, RSS data estimation can be obtained based on Equation (9) by obtaining three unknown polynomial coefficients in Equation (10).

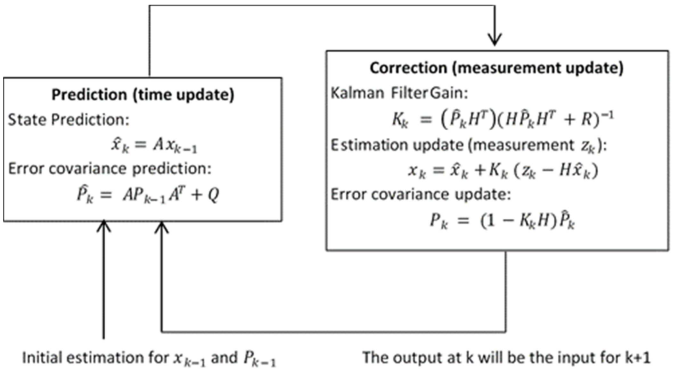
Prediction (time update)
State Prediction:
$\hat{x}_k = A x_{k-1}$
Error covariance prediction:
$\hat{P}_k = A P_{k-1} A^T + Q$
Correction (measurement update)
Kalman Filter Gain:
$K_k = (\hat{P}_k H^T)(H \hat{P}_k H^T + R)^{-1}$
Estimation update (measurement z_k):
$x_k = \hat{x}_k + K_k (z_k - H \hat{x}_k)$
Error covariance update:
$P_k = (1 - K_k H) \hat{P}_k$
Initial estimation for x_{k-1} and P_{k-1}
The output at k will be the input for k+1

Fig. 8 Kalman Filter process [18]

RSS estimation from Polynomial Regression is processed using the Kalman Filter method on each data block (the same as Polynomial Regression). Kalman Filter works recursively by using a priori and a posteriori estimates to get RSS prediction values. The initial estimation of RSS is conducted by the time update equation, while the measurement update equation performs the correction of the prediction. Kalman Filter process is described in Fig. 8.

The input of time update equation is a priori estimation (x_{k-1}), a priori covariance error (P_{k-1}), and a covariance noise process (Q). The input of the measurement update is a posteriori estimation ($\hat{x}_k$), a posteriori covariance error (P_k), Kalman gain (K_k), covariance noise measurement (R), and

RSS data from the previous Polynomial Regression process (z_k). Also, A and H are the measurement status at the time of prediction and correction, respectively. We initialize some Kalman Filter parameters, such as A = 0.1, H = 0, R = 0.25, and Q = 0.12. These parameters can provide the best configuration in the proposed scheme.

3) Quantization: After obtaining RSS data with a high correlation, the data is converted to bit form at this stage. The MAPI scheme used the Dual-Bit Quantization method [17] as a lossless quantization. In this case, RSS data are divided into 20 blocks, then quantized based on the threshold at each level as below:

- Level 1 : $[-\infty,\ \mu - \alpha * \sigma]$ = 00
- Level 2 : $[\ \mu - \alpha * \sigma,\ \mu]$ = 10
- Level 3 : $[\ \mu,\ \mu + \alpha * \sigma\ ]$ = 01
- Level 4 : $[\ \mu + \alpha * \sigma,\ \infty]$ = 11

The level is determined based on the average of each block μ, the standard deviation of each block σ, and the constant α, which is 5. RSS data are converted into two binary bits until the total of bits is twice as the RSS data because there are no bits removed. Dual-Bit Quantization method can increase the KFS value, but the randomness has not been fulfilled. We use the Sequential Bit Remover Technique to increase bit randomness. We divided the bits into several blocks; there are 3 bits in one block. If three sequential bits in a block are equal, then the block is converted to a bit "1" or "0". Otherwise, if there are different bits in a block, then the block is removed. There are bit indexes exchange which is discarded between Alice and Bob, so this technique can also reduce bit errors. Therefore, the output bit has a low KDL value. However, this exchange process cannot be imitated by eavesdroppers.

4) Privacy Amplification: The quantization output's initial key bits have not met the NIST Test randomness requirements. The Universal Hash function is used to increase the initial key bits [19]. This stage produces some keys with high entropy. Legitimate users use the key with the highest entropy as the symmetrical secret key. Keys that are approved by legitimate users are verified using SHA-256 function to ensure keys are identical. This verification process requires the exchange of key digest so that the eavesdropper cannot obtain the actual key. If Alice's key digest is the same as Bob's key digest, then the agreed key can be used as a secret key for the cryptosystem. Otherwise, this means there is still a mismatch of the remaining bits.

5) Symmetric Cryptography: After Alice and Bob successfully verify the agreed key, then the symmetric key is used to send a secure important message. We use AES-256 in this stage as symmetrical cryptography, which requires one symmetrical secret key between legitimate users. Besides that, the SHA-256 function is used again to send ciphertext from Alice to Bob, so it is not misused by third parties [18].

C. Performance Parameter

The MAPI scheme is designed to create symmetric secret keys for encryption and decryption. Thus, the scheme can be evaluated in 3 essential parameters: key disagreement rate (KDL), key generation rate (KFS), and randomness. The explanation of these parameters is as follows.

1) KDL: In this experiment, we evaluated two types of KDL parameters, namely KDL_M and KDL_L. KDL_M shows the discrepancy bit between two users to the total of bits generated after Dual-Bit Quantization process. KDL_L shows the discrepancy bit between two users to the total number of bits generated after Sequential Bit Remover process. The KDL parameters of all users are expressed as a percentage. If the KDL value is getting lower, then the legitimate users are easier to create an identical secret key.

2) KFS: KFS is the number of bits generated per second. In general, KFS parameters are evaluated after the quantization process. However, in this experiment, we evaluated KFS after the Sequential Bit Remover process because Dual-Bit Quantization is a lossless quantization that produces the same total number of bits. Therefore, it cannot be compared. The KFS parameter between Alice-Bob, Eve-Alice, and Eve-Bob are expressed as bit per second (bps).

3) Randomness: The NIST Test used the p-value as a key randomness level reference. The secret key is entirely random if the p-value is equal to 1. The p-value parameter ranges from 0.001 until 0.1. The p-value chosen is 0.01 for cryptographic applications. If p-value > 0.01, the secret key bit passes the randomness requirement.

III. Results and Discussion

We conduct tests in the V2V environment to find out the performance of the MAPI scheme and analyze it with another existing scheme.

A. Channel Examining

We collect the RSS values between two legitimate users in this stage. The initial correlation coefficients for each scenario in two different traffic conditions can be seen in Table 3 and Table 4.

TABLE III
Correlation Coefficient of Measurement in Quiet Condition

Scenario	**Correlation Coefficient**		
	Alice - Bob	**Eve - Alice**	**Eve - Bob**
A1	0.83	-0.52	-0.45
B1	0.78	-0.07	-0.02
C1	0.58	0.19	0.27
D1	0.35	-0.06	0.26
E1	0.70	0.16	2.37
F1	0.64	0.07	-0.28

TABLE IV
Correlation Coefficient of Measurement in Crowded Condition

Scenario	**Correlation Coefficient**		
	Alice - Bob	**Eve - Alice**	**Eve - Bob**
A2	0.49	-0.11	0.23
B2	0.43	0.28	0.16
C2	0.34	0.04	-0.30
D2	0.24	-0.19	-0.31
E2	0.27	-0.10	-0.40
F2	0.18	-0.50	0.09

In this research, Alice and Bob's coefficient correlation value is higher than the value between Eve and legitimate users. These results make eavesdropper challenging to generate an identical key. The highest correlation coefficient value between legitimate users in quiet and crowded conditions is scenario A1 and scenario A2. The measurement results show that the RSS data between Alice and Bob in quiet conditions is more similar than in crowded conditions; consequently, the correlation coefficient value in scenario A1 is higher than scenario A2. This result is because the volume of vehicles in crowded conditions is higher than in quiet conditions, causing a response delay at the time of measurement.

Analysis of Alice and Bob's correlation value is obtained by dividing the RSS data into 20 blocks. The test results show that in scenario A2, there are nine blocks with negative correlation values, and there is one block with correlation values of more than 0.5. In scenario A1 there are five blocks with negative correlation values, and there are two blocks with correlation values of more than 0.5. Measurement scenarios with time intervals below coherence time have a higher correlation than time intervals above coherence time. However, this causes a low randomness level because of the RSS similarity is very high.

B. *Improved Correlation using MHPK Method*

We use MHPK method to increase reciprocity between legitimate users. Table 5 and Table 6 show the correlation coefficients of the MHPK method performance in two conditions. This method can significantly enhance the correlation of legitimate users up to 0.99 in all scenarios. However, it does not significantly increase the correlation of Eve with legitimate users. Thus, our pre-processing method can maintain the security factor by ensuring that non-legitimate users cannot generate secret keys identical to legitimate users. The average correlation coefficient in quiet conditions does not significantly differ with crowded conditions because each RSS data block has a high correlation after the pre-processing stage.

TABLE V
IMPROVED CORRELATION COEFFICIENT IN QUIET CONDITION USING MHPK METHOD

Scenario	Correlation Coefficient		
	Alice - Bob	Eve - Alice	Eve - Bob
A1	0.99	-0.66	-0.92
B1	0.99	0.57	0.43
C1	0.99	-0.96	0.35
D1	0.99	-0.78	-0.97
E1	0.99	0.07	0.87
F1	0.99	0.19	-0.90

TABLE VI
IMPROVED CORRELATION COEFFICIENT IN CROWDED CONDITION USING MHPK METHOD

Scenario	Correlation Coefficient		
	Alice - Bob	Eve - Alice	Eve - Bob
A2	0.99	-0.61	0.78
B2	0.99	-0.71	-0.96
C2	0.99	0.26	-0.17
D2	0.99	0.68	0.77
E2	0.99	-0.95	-0.99
F2	0.99	-0.99	0.77

C. *Quantization Measurement*

RSS data that has been pre-processed is quantized using the proposed Dual-Bit Quantization. The quantization process converts RSS data into two bits without discarding any bits, so this process produces 4000 bits. Therefore, the KFS parameters cannot be compared after the quantization process. The evaluation parameter that can be compared is bit mismatch (KDL_M) between the users, as shown in Table 7 and Table 8.

TABLE VII
MAPI SCHEME PERFORMANCE IN TERM OF KDL_M IN QUIET CONDITION

Scenario	KDL_M (%)		
	Alice - Bob	Eve - Alice	Eve - Bob
A1	0.05	24.90	25.45
B1	0.00	22.60	23.20
C1	0.30	25.20	24.15
D1	0.10	24.75	24.85
E1	1.05	26.45	23.25
F1	0.30	24.45	25.75

TABLE VIII
MAPI SCHEME PERFORMANCE IN TERM OF KDL_M IN CROWDED CONDITION

Scenario	KDL_M (%)		
	Alice - Bob	Eve - Alice	Eve - Bob
A2	0.25	24.35	24.75
B2	0.20	24.90	24.70
C2	0.10	23.95	24.35
D2	0.05	23.00	23.70
E2	0.05	25.20	25.20
F2	0.30	25.25	23.95

Table 7 shows that the average KDL_M of legitimate users in the quiet condition is 0.3%. The non-legitimate user average is 24.73% and 24.44% for Eve with Alice and Eve with Bob, respectively. The results show that the KDL_M Eve value is very high compared to legitimate users because the RSS correlation is very low even after the pre-processing stage. A high KDL_M value indicates many error bits between the bits produced by Eve and legitimate users, making it difficult for Eve to get identical vital bits. Table 8 shows that the average KDL_M of legitimate users in the crowded condition is 0.16%. In comparison, the non-legitimate user has a higher average KDL_M, which is 24.44% for Eve with Alice and Eve with Bob. These results are the same as the quiet condition where Eve is challenging to produce the same key as legitimate users because it has a high KDL_M value.

The lowest KDL_M between Alice and Bob in quiet conditions is 0% (scenario B1). Whereas in crowded conditions, scenarios D2 and E2 have the lowest KDL_M with a value of 0.05%. There are several scenarios where the KDL_M of legitimate users in quiet conditions is higher than crowded conditions at the same speed and interval. This result shows that the quiet condition does not guarantee to have a lower bit mismatch than the crowded condition due to the pre-processing stage before quantization.

The bits produced from the quantization process have low randomness. Sequential Bit Remover Technique is used to increase the randomness of key bits between legitimate users. This algorithm can reduce the KDL_L of Alice and Bob's to 0% in all scenarios, both quiet and crowded conditions. This case means there are no bit errors, so there is a high probability of generating the same secret key. The block index removed by Alice will also be removed by Bob, and vice versa. It is assumed that Eve knows the indexes being exchanged, and Eve will discard them too. However, Eve did not send the index block that was discarded to Alice or Bob. Thus, the number of bits from Eve after the Sequential Bit Remover process is different from the legitimate user. Therefore, in this paper, the KDLL of Eve was not analyzed.

The highest KFS between Alice and Bob in quiet conditions is 43.64 bps (scenario E1). Whereas in crowded conditions is 44.02 bps (scenario E2). It can be seen that the highest KFS of Alice and Bob has the same speed and time interval in quiet and crowded conditions. The higher the vehicle speed, the higher the KFS. Scenarios with time intervals above coherence time have smaller KFS values than those below coherence time. Based on Table 9 and Table 10, the KFS value of Eve is much smaller than the KFS of Alice and Bob. In almost all scenarios, Eve has a KFS value of 0 bps, which means all bits are discarded in the Level Crossing process. In this paper, the required secret key size is 256 bits for the symmetric cryptography process, which is AES-256. So, Eve cannot generate a secret key because the resulting key bits are insufficient. Therefore, the MAPI scheme can generate secure secret keys.

TABLE IX
MAPI SCHEME PERFORMANCE IN TERM OF KFS IN QUIET CONDITION

Scenario	KFS (bps)		
	Alice - Bob	Eve - Alice	Eve - Bob
A1	35.32	0.31	2.19
B1	21.60	2.64	1.89
C1	40.26	0	2.48
D1	26.08	0	0
E1	43.64	0	5.88
F1	32.30	1.92	0

TABLE X
MAPI SCHEME PERFORMANCE IN TERM OF KFS IN CROWDED CONDITION

Scenario	KFS (bps)		
	Alice - Bob	Eve - Alice	Eve - Bob
A2	35.16	0	0
B2	21.22	0	0
C2	41.27	2.50	2.50
D2	25.85	2.52	1.60
E2	44.02	0	0
F2	31.20	0	1.92

D. *Performance Comparison of MAPI Scheme and Other Existing Schemes*

TABLE XI
COMPARISON OF KDL$_M$ IN QUIET CONDITION

Scenario	KDL$_M$ (%)				
	MAPI	Scheme [19]	Scheme [20]	Scheme [17]	Scheme [21]
A1	0.05	0.2	0.22	1.18	0.21
B1	0	0.5	0.25	2.48	4.44
C1	0.3	0.5	0.25	2.17	23.54
D1	0.1	0.2	0.25	5.03	33.36
E1	1.05	0.57	0.53	3.52	23.98
F1	0.3	0.58	0.15	4	22.67

Some comparison schemes to evaluate the performance of the MAPI scheme [17], [19]–[21]. All of the comparison schemes use the pre-process before the quantization stage and are implemented on devices that support IoT technology.

It is assumed that all comparison schemes use the Level Crossing algorithm to improve randomness and use the same privacy amplification function as the MAPI scheme. Thus, the difference between the comparison scheme with the MAPI scheme is the pre-process and quantization methods used. In this case, the parameters being compared are KDL$_M$, KDL$_L$, and KFS of legitimate users.

TABLE XII
COMPARISON OF KDL$_M$ IN CROWDED CONDITION

Scenario	KDL$_M$ (%)				
	MAPI	Scheme [19]	Scheme [20]	Scheme [17]	Scheme [21]
A2	0.25	1.06	0.83	5.33	19.26
B2	0.2	0.15	0.2	3.28	20.06
C2	0.1	0.2	0.3	5.05	17.23
D2	0.05	0.15	0.18	2.85	48.98
E2	0.05	0.05	0.18	5.25	51.22
F2	0.3	0.55	0.25	3.38	40.11

Scheme [19] used the HPK method in the signal pre-processing stage and MMB Quantization at the quantization stage. This scheme does not divide the RSS data into several blocks before the pre-processing stage. Scheme [20] used Kalman Filter, and Adaptive Quantization at the pre-process and the quantization stages. Before the first stage, RSS data are divided into several blocks, each containing 50 data. Similar to MMB Quantization, the type of quantization used in the scheme [20] is multibit quantization with different quantization levels thresholds. Scheme [17] used Kalman Filter, and MMB Quantization at the pre-process and quantization stages. Before the first stage, RSS data is divided into several blocks, each containing 20 data. Unlike other schemes, scheme [21] usedthe single-bit quantization method, Mathur Quantization. The quantization method converts RSS data into 1 bit and discards some data that does not meet the upper and lower threshold. At the pre-processing stage, this scheme used the Kalman Filter method.

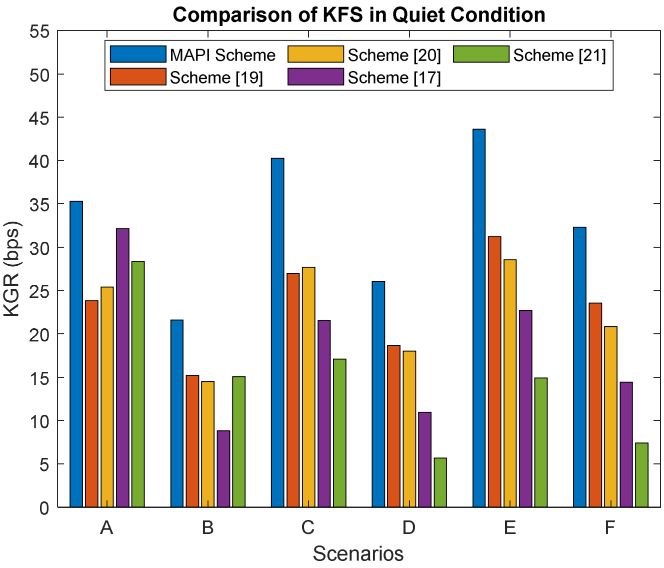

Fig. 9 KFS comparison of legitimate users in quiet condition

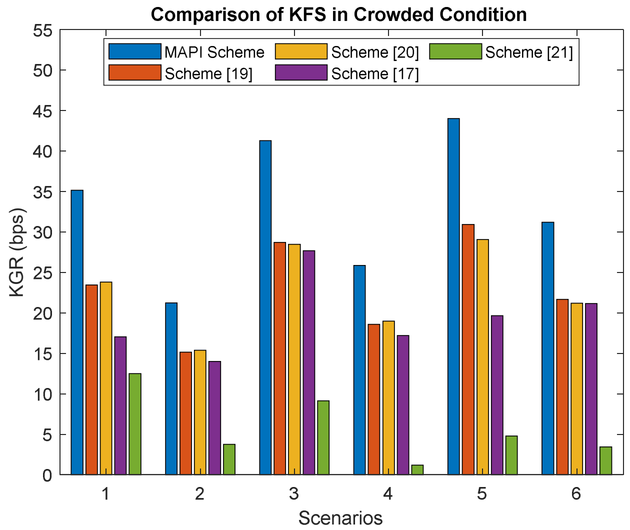

Fig. 10 KFS comparison of legitimate users in the crowded condition

Table 11 and Table 12 show that the MAPI scheme has a smaller KDLM value in most of the scenarios than the other schemes. The smaller the KDL_M value, the higher the possibility to generate a symmetric secret key. The measurement results show that the MAPI scheme can reduce KDL_M values up to 100% compared to the existing schemes in almost all scenarios. The average value of KDL_M in the quiet condition of the scheme [19] is 0.42%, in the scheme [20] is 0.275%, in the scheme [17] is 3.06%, and in the scheme [21] is 18%. For all measurement scenarios, the proposed MAPI scheme has the smallest average KDL_M value compared to other comparison schemes. The MAPI scheme can significantly reduce the KDL_M values in quiet condition up to 28.57%, 9.09%, 90.20%, and 98.33% from the schemes [19], [20], [17], and [21], respectively.

Based on Table 12, the average value of KDL_M in crowded conditions of the scheme [19] is 0.36%, in the scheme [20] is 0.32%, in the scheme [17] is 4.19% and in the scheme [21] is 32.81%. The MAPI scheme can significantly reduce the KDL_M values in crowded condition up to 56.02%, 51.03%, 96.22%, and 99.52% from the schemes [19], [20], [17], and [21], respectively.

All the comparison schemes above have a KDL_L value of 0% after Level Crossing process. The results will affect the KFS value of the key bits generated because this algorithm discards 3 bits if the three are not the same and if the converted bits between legitimate users are not equal. Therefore, if the quantization method is single-bit, the KFS value is low because Level Crossing can cause the number of bits to decrease.

Fig. 9 and Fig.10 show KFS's comparison from legitimate users between MAPI schemes and other existing schemes in quiet conditions and crowded conditions. In all scenarios, the MAPI scheme has the highest KFS value compared to other schemes. Meanwhile, in almost all scenarios, the scheme [21] has the smallest KFS value caused by using the single-bit quantization method so that there is a bit removal during the quantization process. Therefore, the scheme [21] is less efficient when applied to V2V communication systems.

In a quiet condition, the MAPI scheme can increase the KFS value between legitimate users up to 42.88%, 47.5%, 80.20%, and more than 100% from the schemes [19], [20], [17] and [21], respectively. Whereas in crowded conditions, MAPI scheme can increase the KFS value of legitimate users up to 43.57% of the scheme [19], 45.21% of the scheme [20], 69.89% of the scheme [17], and more than 100% of the scheme [21]. In general, the average value of KFS in quiet conditions is higher than in crowded conditions.

E. *NIST-Test Measurement*

In the NIST Test, there are seven tests conducted to ensure the randomness level of the secret key, such as:

- The approximate entropy tests
- The frequency (mono bit) test
- The frequency test within a block
- The cumulative sums test (forward)
- The cumulative sums test (reverse)
- The run tests
- The longest-run-of-ones in a block test.

TABLE XIII
PERFORMANCE OF NIST TEST IN QUIET CONDITION

Test	Scenario					
	A1	**B1**	**C1**	**D1**	**E1**	**F1**
1	0.640	0.826	0.794	0.113	0.737	0.254
2	1.000	0.104	0.211	0.061	0.803	0.261
3	0.344	0.275	0.328	0.031	0.844	0.344
4	0.520	0.183	0.301	0.049	0.804	0.208
5	0.520	0.140	0.379	0.057	0.573	0.470
6	0.382	0.425	0.634	0.121	0.210	0.741
7	0.713	0.285	0.497	0.584	0.716	0.781

TABLE XIV
PERFORMANCE OF NIST TEST IN CROWDED CONDITION

Test	Scenario					
	A2	**B2**	**C2**	**D2**	**E2**	**F2**
1	0.872	0.651	0.719	0.640	0.720	0.794
2	0.532	0.532	0.532	1.000	0.532	0.211
3	0.215	0.582	0.785	0.344	0.785	0.328
4	0.804	0.422	0.746	0.520	0.746	0.301
5	0.301	0.687	0.858	0.520	0.858	0.379
6	0.270	0.548	0.220	0.382	0.220	0.634
7	0.68	0.760	0.474	0.713	0.474	0.497

The MAPI scheme produces two keys that can be used for cryptography. Table 13 and Table 14 shows the results of the NIST Test. The secret key obtained meets the randomness for all types of tests (ρ exceeds 0.01). Scenario A2 produces a key with the highest level of randomness because it has the highest entropy value. The frequency test (mono bit) shows the proportion of bits 1 and 0. If the test results are equal to one, then the distribution of bits 1 and 0 is the same, as in scenario A1 and scenario D2. Scenario E1 produces a key with a proportion of bit 1 that is close to half a block because it has the highest frequency test within a block. Cumulative sums (forward) tests change 0 to -1, and cumulative sums (reverse) tests change 1 to +1 compared to the number of cumulative keys produced with the expected. Scenario F1 has the highest run test results that show the key oscillations faster than other scenarios. The longest-run-of-ones in a block test show that the key in scenario B2 has a length of 1 that is more invariant length than the expected length.

IV. Conclusion

This paper proposes a modified secret key generation scheme, i.e. the MAPI scheme. The resulting key is extracted from RSS in V2V communication in two conditions, quiet and crowded. The results show that the MHPK method can enhance the correlation coefficient between legitimate users until 0.99. Furthermore, the combination of Dual-Bit Quantization and Sequential Bit Remover Technique can eliminate the information reconciliation stage because it can remove all bit errors (KDL_L = 0%) while still producing a high KFS of up to 33 bps in both quiet and crowded conditions. The test results also showed that Eve could not generate an identical key at the final stage even though she used the same method. Moreover, the symmetric secret-key generated passes the randomness test on the NIST Test. The MAPI scheme has a better performance than other existing schemes that also adopt the pre-processing stage in terms of KDL and KFS values.

Further study is recommended to include improving secret key generation schemes' performance by proposing non-hybrid pre-processing methods and new multi-bit quantization methods. The combination of both is expected to eliminate the function of the Sequential Bit remover Technique. Thus, keys can be generated without requiring a long computing time.

Acknowledgment

This paper is funded Applied Leading Basic Research scheme by 2019 from the Ministry of Research, Technology and Higher Education of the Republic of Indonesia.

References

[1] T. Limbasiya and D. Das, “Secure Message Transmission Algorithm for Vehicle to Vehicle (V2V) Communication,” *IEEE Reg. 10 Annu. Int. Conf. Proceedings/TENCON*, pp. 2507-2512, 2017.

[2] K. Orkun and V. Erol, “Network Security Issues and Solutions on Vehicular Communication Systems,” *Preprints*, 2017.

[3] H. Xu, M. Zeng, W. Hu, and J. Wang, “Authentication-Based Vehicle-to-Vehicle Secure Communication for VANETs,” *Journal of Hindawi Mobile Information Systems*, vol. 19, pp. 1–9, 2019.

[4] F. Arena, G. Pau, “An Overview of Vehicular Communications,” *Future Internet*, vol. 11, pp 1-12, 2019.

[5] M. B. Mansour, C. Salama, H. K. Mohamed, and S. A. Hammad, “VANET Security and Privacy – An Overview,” *Int. J. of Netw. Secur. Its Appl.*, vol. 10, no. 2, pp. 13-34, 2018.

[6] W. Stallings, “Cryptography and Network Security: Principles and Practice,” 6th ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2013.

[7] 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.

[8] R. Mishra, A. Singh, and R. Kumar, “VANET Security: Issues, Challenges and Solutions,” *Int. Conf. Elec. Electron. Optim. Tech. ICEEOT*, pp. 1050–1055, 2016.

[9] K. Moara-Nkwe, Q. Shi, G. M. Lee, and M. H. Eiza, “A Novel Physical Layer Secure Key Generation and Refreshment Scheme for Wireless Sensor Networks,” *IEEE Access*, vol. 6, pp. 11374–11387, 2018.

[10] L. Sun, Q. Du, “A. Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions,” *Entropy*, pp. 1-21, 2018.

[11] M. Yuliana, Wirawan, and Suwandi, “An Efficient Key Generation for the Internet of Things Based Synchronized Quantization,” *Sensors*, vol. 19, pp. 1–25, 2019.

[12] D. Kreiser *et al.*, “On Wireless Channel Parameters for Key Generation in Industrial Environments,” *IEEE Access*, vol. 6, pp. 79010-79025, 2018.

[13] M. Yuliana, Wirawan, and Suwadi. “Performance Evaluation of the Key Extraction Schemes in Wireless Indoor Environment,” *Proc. – Int. Conf. Signals Syst. ICSigSys 2017*, pp. 138–144, 2017.

[14] L. Cheng, L. Zhou, B.C. Seet, W. Li, D. Ma, and J. Wei, “Efficient Physical-Layer Secret Key Generation and Authentication Schemes Based on Wireless Channel-Phase,” *Journal of Hindawi Mobile Information Systems*, vol. 2017, pp. 1–13, 2017.

[15] Y.E.H. Shehadeh 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.

[16] M. Yuliana, Wirawan, and Suwandi, “A Simple Secret Key Generation by Using a Combination of Pre-Processing Method with a Multilevel Quantization”, *Entropy*, vol 21, no.2, pp. 1-25, 2019.

[17] M. Yuliana, Wirawan, and Suwadi, “Performance Improvement of Secret Key Generation Scheme in Wireless Indoor Environment,” *Int. J. Commun. Networks Inf. Secur.*, vol. 9, no. 3, pp. 474-483, 2017.

[18] A. Sudarsono, M. Yuliana, and P. Kristalina, “A Reciprocity Approach for Shared Secret Key Generation Extracted from Received Signal Strength in The Wireless Networks,” *2018 Int. Electron. Symp. Eng. Technol. Appl. IES-ETA 2018 – Proc.*, pp. 170-175, 2019.

[19] I. T. Dewi, A. Sudarsono, P. Kristalina, M. Yuliana, “Reciprocity Enhancement in V2V Key Generation System by using HPK Method,” *IES 2019 – Int. Electron. Symp. Role Techno-Intelligence Creat. An Open Energy Syst. Towar. Energy Democr. Proc.*, pp. 6-13, 2019.

[20] M. Yuliana, Wirawan, and Suwadi, “Performance Analysis of Loss Multilevel Quantization on the Secret Key Generation Scheme in Indoor Wireless Environment,” *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 9, no. 1, pp. 100-108, 2019.

[21] 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,” *Proc. – 2018 6th Int. Symp. Comput. Networking, CANDAR 2018*, pp. 57-65, 2018.