An Adaptive Lossly Quantization Technique for Key Extraction Applied in Vehicular Communication

Ibraheem Abdelazeem Ibraheem Ali
Nanjing University of Science and Technology https://orcid.org/0000-0001-9607-1441
Zhang Weibin (13829668@qq.com)
Nanjing University of Science and Technology School of Electronic and Optical Engineering
Zhenping Zeng
Nanjing University of Science and Technology School of Electronic and Optical Engineering
Abdeldime mohamed saleh
Sudan Atomic Energy Commission

Research Article

Keywords: Vehicular Ad Hoc Networks, key Extraction, Mobile Ad hoc Networks, Quantization, RSS

Posted Date: July 13th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-671868/v1

An Adaptive Lossly Quantization Technique for Key Extraction Applied in Vehicular Communication

Ibraheem Abdelazeem[a], Weibin Zhang[a,*], Zeng Zhenping[a,*], Abdeldime M.S[b]

[a]*School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing,* 210094*, China*
[b]*Karary University, Khartoum,* 12304*, Sudan*

Abstract

Security in Vehicular Ad Hoc Network (VANET) is one of the major challenging topics and the secure key interchange between two legitimate vehicles is an important issue. The multi-environment of VANET has been exploited to extract the secret key and employed security services in VANET. However, it offered more excellence randomness owed to fading, noise multi-path, and velocity difference. Some of the factors like Bit-rate, complication and memory requests are reduced by using a process known as quantization. This paper proposes a new quantization method to extract the secret key for vehicular communications that uses a lossy quantizer in combination with information reconciliation and privacy amplification. Our work focuses on the quantization phase for the secret generation procedure. The comprehensive simulations display the propose method increases the zone and number of the quantization levels to utilize the maximum number of measurements to reduce reasonably the wasted measurements.

Keywords:

Vehicular Ad Hoc Networks, key Extraction, Mobile Ad hoc Networks, Quantization, RSS.

1. Introduction

Vehicular Ad Hoc Network (VANET) is a technology that collects the competencies of new wireless networks with vehicles. It supports various number of applications in the vehicular environment. It is a kind of Mobile Ad hoc Networks (MANETs) that uses vehicles as nodes. The key difference is that the mobile routers that structure the network are cars [1]. Recently, (VANETs) have developed and became very popular, because it has a great role in improving road safety, which is one of its most important goals, therefore, it has a significant impact on decreasing accidents and traffic congestions. Besides, it supports a wide range of applications, such as providing traffic management with real-time data for responding to road congestions [2]. Another advantage of VANET can

*Corresponding author.
Email addresses: ibrahem2k19@gmail.com (Ibraheem Abdelazeem), 13829668@qq.com (Weibin Zhang)

find a better path to access real-time data by saving fuel and time and has wonderful economic and safety benefits. Nevertheless, road safety is the primary goal of these networks [3]. VANET contains three main components namely, trusted authority, constant roadside unit (RSU), and on-board units (OBU) equipped on the moving vehicles. The vehicles are linked to each other (V2V) or with the Road Side Unit (V2R) by single hop or multiple protocols over the vehicle network of the contract [4].

Since accessing the medium in VANET is open, it is vulnerable to many attacks [32]. However, security is an important requirement in VANET. To protection VANET parts from attacks, many solutions have been proposed to afford security requirements against security attacks in VANETs. However, secret key distribution and the basic establishment between legitimate vehicles are the most significant part for all of them, and they are a common requirement and challenge to giving secure communication between vehicles [5–7]. Most of those solutions rely on cryptography and hash functions as a security technicality. Typically, asymmetric key cryptosystems, such as (Diffie-Hellman and RSA) are the most famous techniques for sharing a secret key in many communication systems. Owing to the problem of key distribution between the legitimate parties which face the hash functions and cryptography, particularly symmetric key cryptosystems, although it is the faster and reliable one between all cryptography systems [8]. Meanwhile one of the weaknesses of asymmetric key cryptosystems is spent on a great measure of computing resources, bandwidth, and capacity, which may be obtainable in many scenarios of VANET. Therefore, many researchers have supported to improve other methods [9–11]. Quantum cryptography is one of these efforts that utilize the Quantum concept rules for sharing a secret key. It has been attracted in numerous applications, but it is still in early stages and very costly [12].

The employment of the physical randomness inherent in mutual wireless communication channels is the next stage of the development for secret-key distribution. When using the physical layer (PHY) for secret key extraction, there are important properties of a radio signal that must be considered, which are: (the exchange of radio wave propagation, the chronological differences of the radio channel and the place alternatives) [13, 31]. There is strong relationship between Quantization schemes and the channel characteristics, used as sources of randomness for secret keys generation [14]. The most general channel factors used to estimate are Received Signal Strength (RSS), Channel Impulse Response (CIR) and phase. RSS is the most common method since its value is obtainable in all out of- the-shelf transceivers on a frame basis; therefore, reducing design and implementation costs. RSS values are linked with space, and the entropy is significantly affected [15]. by the movement of the

nodes and middle entities, revealing sensitiveness against prognostic and active attacks [16, 17]. In order to develop a secret key extraction approach suitable for VANET, we depend on the strengths of the technique of the current methods suitable for VANET that uses a lossy quantize in combination with information reconciliation and privacy amplification. In this paper, we took advantage of the randomness natural of the wireless channel to supply secrecy for the key interchange method by applying Received Signal Strength (RSS). The rest of the paper is organized as following. Section 2 presents the secret key extraction approach. Section 3 presents the Secret key extraction steps. Section 4 displays the simulation results and evaluation. Section 5 concludes the paper.

2. The SECRET KEY EXTRACTION APPROACH

We suppose that vehicles have a wireless channel to exchange messages, and they can register the RSS readings of the replaced messages. The two vehicles exchange some messages over the wireless channel and register the RSS readings of each message in order to extract a shared secret key between them. The third side cannot discover any information about the key. We reflect the passive attack sample, where the adversary knows about the method. The legitimate vehicles amount the differences of the wireless channel by transfer sensors to each other and computing the analytical RSS values to find a shared secret key. For identical readings, legitimate vehicles should perfectly amount RSS values at the same time [18–20]. While standard commercial wireless transceivers have one orientation and cannot send and receive signals at the same time, they should measurement the radio channel in one orientation at a time. However, as long as the time between two directional channel measurements is very short compared to the channel cohesion rate, we will get identical RSS estimates. The proposed method applied to extract the secret key between legitimate vehicles contains three main stages, as shown in Fig1.

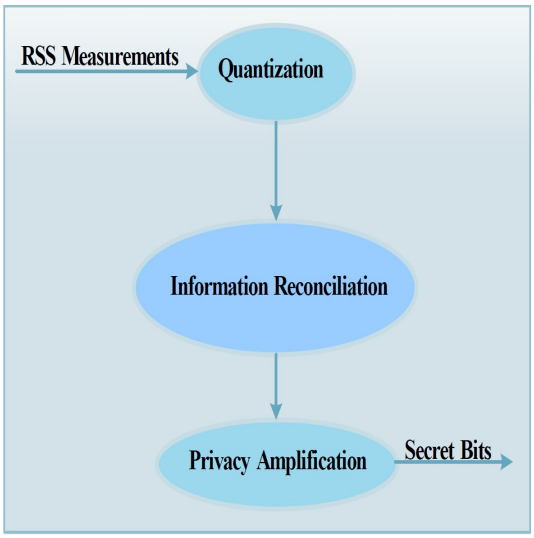

Fig. 1: The main stages of the extract secret key between legitimate vehicles.

3. KEY EXTRACTION STAGES

3.1. Quantization

Quantification is the process of determining a separate value from an area with potential values

for each derived sample. The number of potential values relies on the number of bits utilized to encode each sample [21]. In general, quantitative measurement is obtained founded on particular thresholds. Various options for thresholds and their number represent substantial variation between these quantities. Ordinarily, quantization methods are classified into two main classes which are namely: the lossless and lossy (scalar quantization and vector quantization). The previous generates a great rate production bit current though it does not drop any bits. Nevertheless, employ privacy amplification to raise the uncertainty related by the bits [22].

As several packets are exchanged between two legitimate vehicles, each of them gathers a time sequence of measured RSS. Then, each node quantizes its time series to generate an initial secret bit sequence The proposed quantize takings of the RSS measurements and regulates them into block of size N_P and computes thresholds. One of the legitimate vehicles starts the key extraction procedure. The sender saves indexed transmission probes to the receiver vehicle, which directly responds to receiving through acknowledgments (ACKs). The probes and ACKs are made as short as possible to be exchanged within the coherence time since this will decrease the Information Reconciliation load [23]. Legitimate vehicles reflect the block of serial measurements of the size N_P. The volume of N_P depends on the wanted key size. The RSS reading of received packets and their indexes are register by both sender and receiver.

Currently, quantization approaches utilizing a higher and a lower threshold drop on all the patterns which lay among these thresholds [24]. There are many of the RSS reading information which are dropped, as shown on Fig. 2. These dropped patterns are damage of useful information that can be applied by legitimate vehicles to create secret bits and also product in passive employment and depletion of resources the wireless channel because additional probes are required to be replaced.

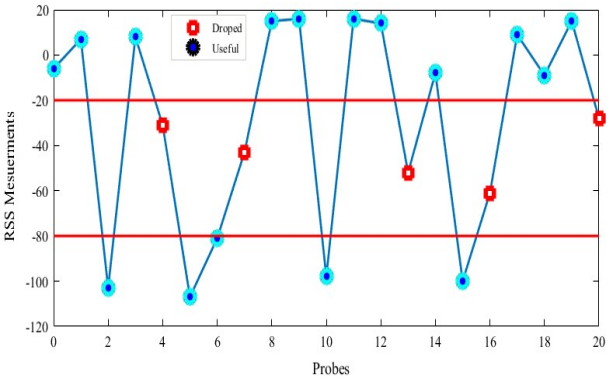

Fig. 2: Two quantization levels using higher and lower threshold drops.

We assume the distance between two vehicles Initiator and Responder(I,R) is D_{IR}, the distance between Initiator and adversary (I,E) is D_{IE}, and the distance between responder and adversary(R,E) is D_{RE} as depicted in Fig. 3, and that the recorded reading of (I,R, E) are respectively represented by

$$D_I = [a_1, a_2, a_3, \dots a_{N_P}] \tag{1}$$

$$D_R = [a_1, a_2, a_3, \dots a_{N_P}] \tag{2}$$

$$D_E = [a_1, a_2, a_3, \dots a_{N_P}] \tag{3}$$

The measurements collected by content the con-

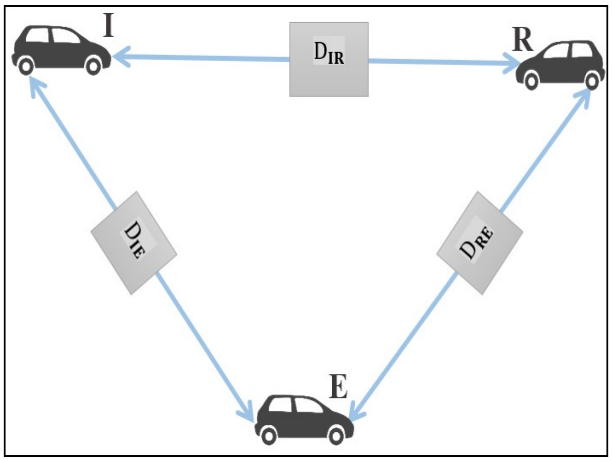

Fig. 3: System model for a secret key generation system.

dition of Eq.4 for probes transfer by (P) during coherence time (C_T).

$$r_a \begin{bmatrix} = r_b \\ \neq r_e, if D_{AE} > p, D_{BE} > p \end{bmatrix} \tag{4}$$

Thus, one obtains

$$\mu = \frac{1}{N_P} \sum_{1}^{N_P} D_I \tag{5}$$

where μ is the average of the random RSS readings, N_P is the number of probes, while D_I is the set of RSS readings from the initial side (I).

$$q_1 = \frac{1}{2} (\mu + \max(D_I)) \tag{6}$$

where q_1 is the first quantization level, as shown in Fig. 4

$$q_4 = \frac{1}{2} (\mu + \min(D_I)) \tag{7}$$

The legitimate vehicles generate their initial bit

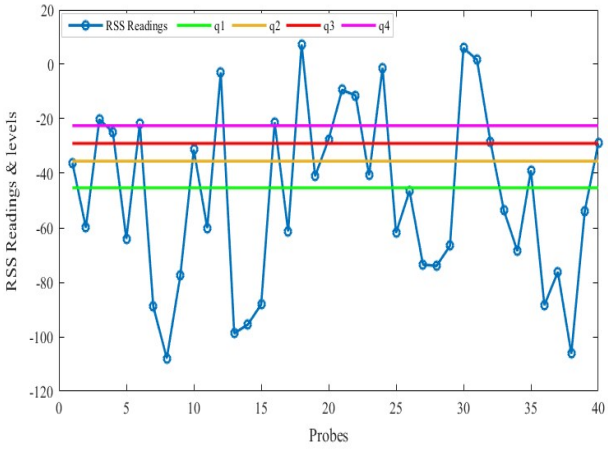

Fig. 4: The quantization levels in the proposed approach.

streams by extracting two bits for each RSS dimension, conditional on the level intermission in which the RSS dimension leaves and rendering to the quantization rules explained in Table 1. The

Table 1: Quantization Rules

bits	*measurement*(r)
00	$r \leq q_1$
01	$q_1 < r \leq q_2$
10	$q_3 \leq r < q_4$
11	$r > q_4$

purpose is to extract a key without a large number of drop information, in additional high entropy, high bit rate, and sensible randomness. Due to the coherence time being too short, the goal is to reduce the lasted measurements as possible to use the most number of measurements. To realize this, we increase the number of samples and adjust the array of quantization levels to adapt to the normal distribution of the readings [5]. Using the above

method for finding $\widehat{q_2}$, $\widehat{q_3}$ values may cause many drops. Therefore, to adjust the levels and reduce the number of drop readings, we use two methods. Firstly, by using level adjustment values α_1, α_2 for finding q_2, q_3 as follow:

$$\hat{q}_2 = \frac{1}{2}(\alpha_1 \mu + \mathrm{q}_1) \tag{8}$$

$$\hat{q}_3 = \frac{1}{2}(\alpha_2 \mu + \mathrm{q}_4) \tag{9}$$

where $0 < \alpha_1, \alpha_2 < 1$.

Secondly, by adjusting the levels using the normal distribution of the readings between q_1, μ and the average of the drops limit as,

$$\mu_1 = \frac{1}{2}\left(q_2 + q_3\right) \tag{10}$$

$$\mu_2 = \frac{1}{2}\left(\hat{q}_2 + \mu_1\right) \tag{11}$$

Thus,

$$q_2 = Rand\left[\mu_1 \;\; \mu_2\right] \tag{12}$$

Similarly,

$$\mu_3 = \frac{1}{2}\left(\hat{q}_3 + \mu_1\right) \tag{13}$$

$$q_3 = Rand\left[\mu_1 \;\; \mu_3\right] \tag{14}$$

The quantization levels in our approach will follow the normal distribution of the measurement readings and the fine adjustment of q_2 and q_3 will decrease the number of drop readings, while the average RSS value is dropped out of the RSS measured because it can be a predictable function of space, as shown in Fig. 5

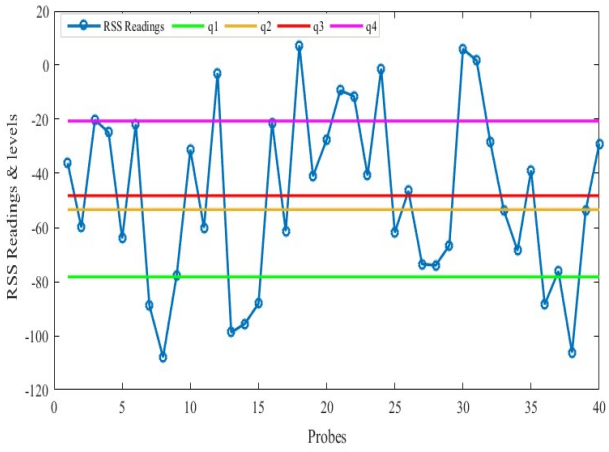

Fig. 5: The normal distribution approach of the quantization levels.

3.2. Information Reconciliation

In this stage, after quantization, due to noise and interference, wireless hardware conditions and half-duplex natures of the channel, arise the variances in between bit streams of legitimates vehicles. The information reconciliation technique used to decide upon the same key to proper mismatch bits without any need to exchange some information on the channel that can be utilized by the attacker to detect the extracted secret bits [25]. The existing solutions used for information reconciliation are either error adjustment codes or some communicating information reconciliation procedures. In this study, we applied Cascade [26], which is a two-method information reconciliation protocol. Employing the Cascade approach, one side provides the bitstream randomly, splits it into small blocks and sends variation and consistency information of each block to the other side. While other side offers his bits stream, gaps it into small blocks, computes, and

checks if the equality of the blocks correspond or not. For each block whose equality does not correspond, the other side implements a double search to discover whether a small number of bits in the block can be altered to create the block corresponds to the equality information. These stages are repeated many times pending on the chance of attainment becomes upper than a required threshold. The bit streams are missed, and the key extraction method is resumed by measuring new RSS rates. Since the information reconciliation is a probabilistic method, it sometimes may fail [27]. Hence, correct selection to the number of passes and the block size significantly decreases the failure probability.

3.3. Privacy Amplification

Privacy amplification is a necessary stage in post-processing, which is used to extract the final secret keys from the identical altered keys between legitimate vehicles [28]. The vehicle needs to probe the channel just once through its coherence time in order to find independent channel measurements. In VANET, it is very hard to approximation the coherence time of a channel, owing to mobility and the incidence of random movements produced by entities in the environment [29]. Consequently, in the tested RSS data, a bit and the sequential bit are possibly connected since the two consistent RSS measurements happening within the same coherence period. We need another technicality to decrease the connection between subsequent bits, although our quantization method usages dissimilar bit symbol for each interpretation rendering to its position inside the quantization levels, thus that the lastly extracted key from the bit stream is really strong. Privacy amplification alleviates problems that may occur during the information reconciliation stage. Such as remove or alteration portions of the bit stream, and an adversary cannot use this information to deduction parts of the extracted key. Moreover, the created bits could have some successive connected bits and have a small entropy rate [7].

Firstly, in order to raise the randomness and mix of the extracted bits, we use a double arrangement of Markov chain to solve the dependency problem in the quantized bits and to alter the bit stream series [20]. The number of states equal $[s_0, s_1, s_2, s_3]$ by four subs-sequences consistent to a special Markov case, because we have used binary order Markov chain. Every bit in the stream is changed by new bits (C_{bs}), which depend on the previous binary bits (P_{bs}) in the streaming series and the present value (C_{bs}) of the envisioned bit. That is meant by three bits rendering to its present value, and it is previous binary bits, the value of (N_{bs}) is envisioned show in Table 2.

Secondly, to find the stable length and low output from lengthier input streams, and to gain a high entropy rate, the legitimate vehicles use a global hash function. Most of the general methods used for privacy amplification are founded on the left-over hash lemma, as a well-known technique to ex-

Table 2: Two Order MARKOV Chain According to the Status of the Previous Bits to Get the New Bit

State	(P_{bs})	(C_{bs})	(N_{bs})
s_0	00	0	000
	00	1	001
s_1	01	0	010
	01	1	011
s_2	10	0	100
	10	1	101
s_3	11	0	110
	11	1	111

tract randomness from inadequate random sources [28]. Each legitimate vehicles get the last secret key bits of size(m)through calculating the hash value $h_{P,Q}(x)$, giving to Eq.15.

$$h_{P,Q}(x) = (P_x + Q) \bmod ((P_m) \bmod (m)) \quad (15)$$

4. SIMULATION AND RESULTS

4.1. Simulation and Arrangements

There are some assumptions we have to make. Before implementing our Mat lab program, we have to explain the communication environments of two moving vehicles in city situations. Initially, we cautious the requirement of IEEE802.11p for communication among vehicles. Then, we utilized a Rayleigh fading channel plus additive Gaussian noise to signify the communication channel conduct [30]. We used dissimilar values of rapidity ranged from 20 to 60 km/h for each vehicle. Utilizing these locations, we sent numerous probes that have randomly created contents plus preambles among the two vehicles, through a rate of 160 probes per second. In the simulation program, we mounted and path the worth of the coherence time. We sent the probes and logged the RSS values using two styles. One during the coherence time and the other after we finished the coherence time.

We reflect measurements for ten tracks over dissimilar molds, making ten datasets, these readings are for the establishment of the secret key, which profits through a few seconds during the transmission process. Additionally, we record these readings along with their consistent mode (drop and useful) and directories to create more analysis on them, in order to evaluate the offered approach and compare it with other alternatives and examine its suitability for vehicular networks. Each of our RSS measurements is quantized to produce one or more bits depending on the quantization scheme and forms the basis for key extraction. We used these datasets as an input to the quantization procedure, for each run of the program. We implement a Mat lab function to achieve the quantization method rendering to the quantization rules and utilizing the above registered RSS values [31]. It excerpts bits from the un-dropped reading and computes the total of extracted bits as well as the amount of drop RSS reading for each quantization technique. We applied the created bits streams of the two vehicles to evaluate the mismatch bits rate, secret bit rate, and the initial entropy rate. The mismatch rate is the ratio of the number of bits that do not match between legitimate vehicles to the number of bits

extracted from RSS quantization, while secret bit rate is the rate number of secret bits extracted per composed measurements [6, 23].

4.2. SIMULATION RESULTS AND EVALUATION

The major issue of the security of the proposed method is those measurements which are composed by legitimate vehicles and the adversary are completely different and random and linked to their locations. We recorded the RSS measurements at three sides within the coherence time of the channel. From the composed reading, we detected that, the measurements at any two sides are nearly similar, while they are significantly different in the third side (adversary vehicle), as shown in Fig. 6.

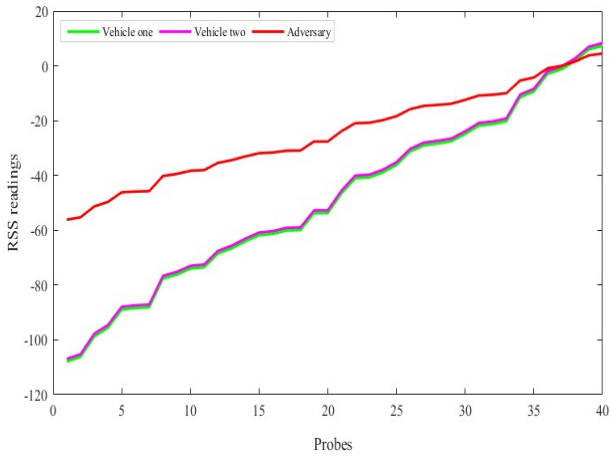

Fig. 6: The RSS reading of the signal between legitimate vehicles and the third adversary vehicle.

to IEEE 802.11p, the multipath, noise, and distance between two vehicles, as well as the inflection method, greatly effects RSS readings. The impact of quantization level on the amount of dropped RSS values, we noted the number of droops in quantization levels with adjustment. Besides, when we make the normal distribution of the measurement readings and the fine adjustment of the measurement readings and the fine adjustment of q_2 and q_3 we reduce the number of the drop readings as shown in Fig. 7. Moreover, we entered ten various datasets and quantize them utilizing two, four levels without adjustment with our quantization method. Then we calculated the secret bit rate and drop ratio, as shown in Fig. 8 and Fig. 9, The evaluations of these simulations are plain from those figures that the drop ratio of the proposed quantization outperformed than others, as well as the secret bit rate is very high.

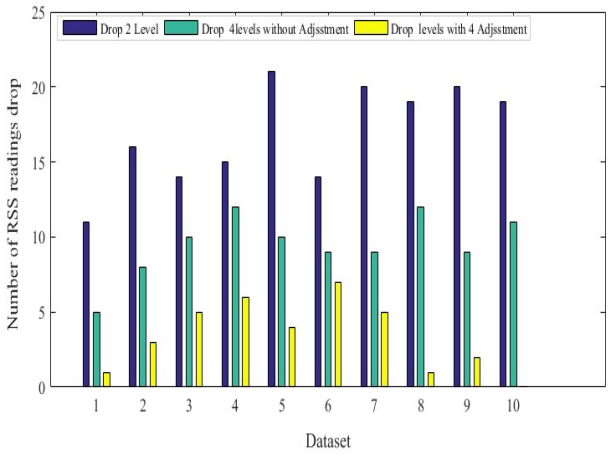

Fig. 7: The impact of quantization levels on the number of dropped measurements.

5. Conclusion

Vehicular Ad Hoc Networks (VANETs) have great advantages and various goals on the road to

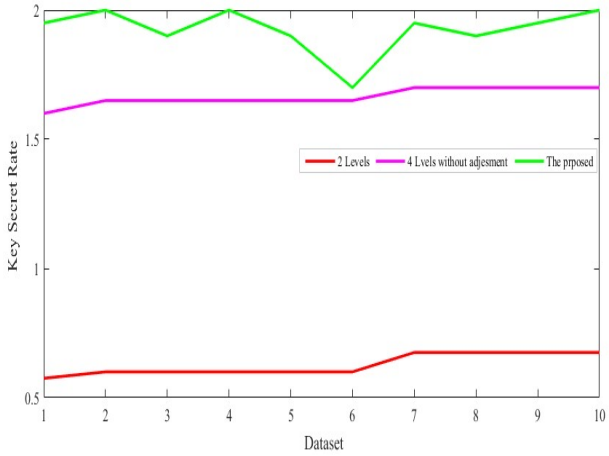

Fig. 8: The secret bit rate of ten datasets using two levels, four levels, and the proposed quantization.

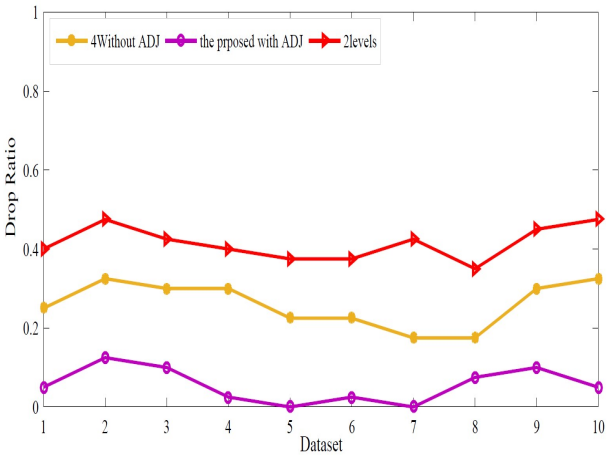

Fig. 9: The drop ratio of ten datasets using two levels, four levels, and the proposed quantization.

raise efficiency and human safety by different applications. All of these advantages will increase security threats and confidentiality problems if security attacks are not completely studied and evaluated. This paper offered a quantization method to extract a secret key by taking advantage of the randomness nature of the wireless channel and to exploit the special properties of VANET. The results that we obtained show that the proposed technique has a high bit rate and entropy rate, besides, the secret bit rate being very high, which reduced the wasted measurements and it can be effectively useful as part of numerous security schemes to offer security services for the VANETs scenarios.

6. Acknowledgment

This work is supported by National Natural Science Foundation of China under Grant 71971116.

7. REFERENCES

[1] Rewashed, Z.Y. and S.M. Mahmud, Communications in vehicular networks. Mobile Ad-Hoc Networks: Applications, Cap, 2011. 2: p. 20.

[2] Mansour, M., et al., VANET Security and Privacy - An Overview. International Journal of Network Security and Its Applications, 2018. 10: p. 13-34..

[3] Lai, L., et al., Key generation from wireless channels, in Physical Layer Security in Wireless Communications. 2013, Citeseer. p. 47-92.

[4] Ahmed, W. and M. Elhadef. Securing Intelligent Vehicular Ad Hoc Networks: A Survey. 2018. Singapore: Springer Singapore.

[5] Abdelgader, A.M.S. and L. Wu. A Secret Key Extraction Technique Applied in Vehicular Networks. in 2014 IEEE 17th International Conference on Computational Science and Engineering. 2014.

[6] Chen, L. and T. Jiang. Key Generation Rate in the Full Duplex Relay Wireless Communication Network. in Communications, Signal Processing, and Systems. 2018. Singapore: Springer Singapore.

[7] Premnath, S.N., et al., Secret Key Extraction from Wireless Signal Strength in Real Environments. IEEE Transactions on Mobile Computing, 2013. 12(5): p. 917-930.

[8] Ahmed, W. and M. Elhadef. Securing Intelligent Vehicu-

lar Ad Hoc Networks: A Survey. in Advances in Computer Science and Ubiquitous Computing. 2018. Singapore: Springer Singapore.

[9] Al-Khalil, A.B., A. Al-Sherbaz, and S. Turner, Enhancing the Physical Layer in V2V Communication Using OFDM MIMO Techniques. architecture, 2013. 1: p. 10.

[10] Brassard, G. and L. Salvail. Secret-Key Reconciliation by Public Discussion. 1994. Berlin, Heidelberg: Springer Berlin Heidelberg.

[11] Ever, Y.K., Secure-Anonymous User Authentication Scheme for e-Healthcare Application Using Wireless Medical Sensor Networks. IEEE Systems Journal, 2019. 13(1): p. 456-467.

[12] Hasrouny, H., et al., VANet security challenges and solutions: A survey. Vehicular Communications, 2017. 7: p. 7-20.

[13] Mukherjee, A., et al., Principles of physical layer security in multiuser wireless networks: A survey. IEEE Communications Surveys and Tutorials, 2014. 16(3): p. 1550-1573.

[14] Bottarelli, M., et al., Physical characteristics of wireless communication channels for secret key establishment: A survey of the research. Computers and Security, 2018. 78: p. 454-476.

[15] Sampath, V., S. Karthik, and R. Sabitha. "Position-Based Adaptive Clustering Model (PACM) for Efficient Data Caching in Vehicular Named Data Networks (VNDN)." Wireless Personal Communications 117.4 (2021): 2955-2971.

[16] Zhang, J., S.K. Kasera, and N. Patwari, Mobility assisted secret key generation using wireless link signatures, in Proceedings of the 29th conference on Information communications. 2010, IEEE Press: San Diego, California, USA. p. 261-265.

[17] Mathur, S., et al., Radio-telepathy: extracting a secret key from an unauthenticated wireless channel, in Proceedings of the 14th ACM international conference on Mobile computing and networking. 2008, ACM: San Francisco, California, USA. p. 128-139.

[18] Li, X., et al., Efficient and Consistent Key Extraction Based on Received Signal Strength for Vehicular Ad Hoc Networks. IEEE Access, 2017. 5: p. 5281-5291.

[19] Cunha, F., et al., Data communication in VANETs: Protocols, applications and challenges. Ad Hoc Networks, 2016. 44: p. 90-103.

[20] Sun, X., et al. Improved Generation Efficiency for Key Extracting from Wireless Channels. in 2011 IEEE International Conference on Communications (ICC). 2011.

[21] Bottarelli, M., et al. Quantisation feasibility and performance of RSS-based secret key extraction in VANETs. in 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). 2018.

[22] Bennett, C.H., et al., Experimental quantum cryptography. Journal of Cryptology, 1992. 5(1): p. 3-28.

[23] Wang, X., et al., High-speed Implementation of Length-compatible Privacy Amplification in Continuous-variable Quantum Key Distribution. IEEE Photonics Journal, 2018. PP: p. 1-1.

[24] Ismail, D.K.B., et al. Optimizing Turbo Codes for Secret Key Generation in Vehicular Ad Hoc Networks. in Smart Technologies and Innovation for a Sustainable Future. 2019. Cham: Springer International Publishing.

[25] Badawy, A., et al., Unleashing the secure potential of the wireless physical layer: Secret key generation methods. Physical Communication, 2016. 19: p. 1-10.

[26] Moara-Nkwe, K., et al., A novel physical layer secure key generation and refreshment scheme for wireless sensor networks. IEEE Access, 2018. 6: p. 11374-11387.

[27] Johnson, J.S., et al., An analysis of error reconciliation protocols used in Quantum Key Distribution systems. The Journal of Defense Modeling and Simulation, 2013. 12(3): p. 217-227.

[28] Cencioni, P. and R. Di Pietro, A mechanism to enforce privacy in vehicle-to-infrastructure communication. Computer Communications, 2008. 31(12): p. 2790-2802.

[29] Mailloux, L.O., et al., Modeling decoy state Quantum Key Distribution systems. The Journal of Defense Modeling and Simulation, 2015. 12(4): p. 489-506.

[30] Jiang, D. and L. Delgrossi. IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments. in VTC Spring 2008 - IEEE Vehicular Technology Conference. 2008.

[31] Kaemarungsi, K. and P. Krishnamurthy, Analysis of WLAN's received signal strength indication for indoor location fingerprinting. Pervasive and Mobile Computing, 2012. 8(2): p. 292-316.

[32] Ibraheem, Ibraheem Abdelazeem, et al. "Analysis of Possible Security Attacks and Security Challenges Facing Vehicular-Ad Hoc Networks." transportation 9.10 (2019): 11.

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- Creditauthorstatement.docx
- Declarationofinterests.docx