



Ben Ismail, D. K., Karadimas, P., Epiphaniou, G. and Al-Khateeb, H. M. (2019) Error Reconciliation with Turbo Codes for Secret Key Generation in Vehicular Ad Hoc Networks. In: Computing Conference 2018, London, UK, 10-12 Jul 2018, pp. 696-704. ISBN 9783030011765.

There may be differences between this version and the published version. You are advised to consult the publisher's version if you wish to cite from it.

<http://eprints.gla.ac.uk/189248/>

Deposited on: 1 July 2019

Error Reconciliation with Turbo Codes for Secret Key Generation in Vehicular Ad Hoc Networks

Dhouha Kbaier Ben Ismail¹, Petros Karadimas², Gregory Epiphaniou¹, and Haider Al-Khateeb¹

¹Cyber Research Institute, School of Mathematics and Computer Science, University of Wolverhampton, UK

²University of Glasgow, School of Engineering, Glasgow, Scotland

Abstract—We present an algorithm that allows two users to establish a symmetric cryptographic key by incorporating the most important features of the wireless channel in vehicle-to-vehicle (V2V) communication. The proposed model includes surrounding scatterers' mobility by considering other vehicles; it also includes three-dimensional (3D) multipath propagation. These temporal variability attributes are incorporated into the key generation process where non-reciprocity compensation is combined with turbo codes (TCs). For fair comparisons, the indexing technique is applied in conjunction with the non-reciprocity compensation technique. A series of simulations are run to calculate key performance indicators (KPIs). The entropy values were high throughout all rounds of simulation and estimated around 0.94 to 0.99 bits per sample. Furthermore, simulation results reveal a decrease in bit mismatch rate (BMR) and an increase key generation rate (KGR) when TCs are used. The estimated BMR is nearly the same for different key lengths, and it is estimated to only 0.02 with TCs, compared to 0.22 obtained with the indexing technique. Finally, the key generation rate was also reported high ranging from 35 to 39 for the 128-bit symmetric keys per minute with TCs, while it is ranging from 3 to 7 when compared with a sample indexing technique published in the public domain.

Keywords—bit mismatch rate, entropy, error reconciliation, key generation, quantization, scatterers' mobility, temporal variability, thresholding, turbo codes, VANET.

I. INTRODUCTION

TRADITIONAL wireless communications are vulnerable to man-in-the-middle attacks where certain aspects of confidentiality, integrity, and availability are violated. Conventional cryptographic solutions based predominantly on-stream ciphers generate shared secrets using pre-computational techniques or public key cryptography [1]. Aspects around centralised key management and computational complexity can render these solutions difficult to be often employed dependent on hardware configuration and requirements. Public key cryptography, in particular, has proved to increase computational complexity during secret key generation, especially for low-end energy efficient devices [2]. Research activities have initiated in the area of fast and efficient key generation algorithms via physical layer characteristics. Channel-based key extraction approaches try to exploit the physical properties of wireless channels such as reciprocity and temporal/spatial variability in an attempt to

provide the necessary randomness for the symmetric key creation [3], [4]. Indeed, the wireless channel acts a medium to increase key generation rate, cryptanalytic resistance, and quality of keys generated between end points due to the inherent stochastic nature of wireless propagation channels [5]. In a typical VANET environment where access to infrastructure is given (see Fig.1), the wireless links between nodes and co-existent adversaries experience uncorrelated channel attributes. Nodes are also distributed and self-organized with the majority of wireless communication carried out by on-board units (OBU) integrated with additional services and processes running [6]. Therefore, these channels in vehicular networks can offer some level of confidentiality during the key generation process between parties, which reduce the computational complexity and relax certain barriers related to key management requirements. Due to the mobility of nodes in VANETs, the network communication and topology is prone to constant changes acting almost like a random variable in time.

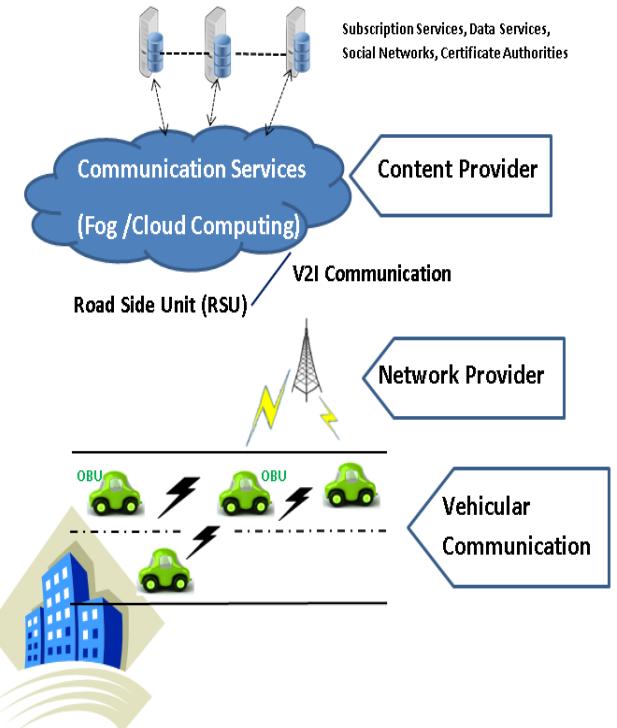


Fig. 1. Vehicular Networking Architecture.

In this paper, all the essential vehicle-to-vehicle (V2V) communication characteristics are incorporated in the key generation process such as surrounding scatterers' and three-dimensional (3D) multipath propagation. The receiver's channel response (Bob's channel) is synthetically generated by employing the comprehensive parametric stochastic V2V channel model presented in [7]. The transmitter's samples (Alice's channel) are modelled by adopting a channel gain complement technique which compensates channel non-reciprocity, inherent in any realistic wireless communication scenario [8]. Only samples above and below the thresholds imposed are allocated, then turbo coding (TC) technique is implemented for information reconciliation. For fair comparisons, the indexing technique described in [9] was applied in conjunction with the non-reciprocity compensation technique in [8]. Compared to the existing standard indexing technique, significant improvement in the key performance indicators (KPIs) is observed with TCs, namely for the key generation rate (KGR) and bit mismatch rate (BMR).

This paper is organised as follows. In Section II, the authors present their algorithm and the adopted V2V channel model. A Graphical User Interface (GUI) was designed to run the developed algorithm. Thus, simulations are run, and performance analysis is carried out in Section III. Several key performance indicators (KPIs) are employed. Finally, Section VI draws some conclusions.

II. PROPOSED ALGORITHM'S STRAWMAN

Fig. 2 presents the algorithm's strawman. First of all, synthetic data is generated for demonstration purposes by employing the Monte Carlo simulation method [10], [11]. The input parameters of the algorithm are provided by the inherent physical attributes of the dynamic V2V propagation channel introduced hereafter.

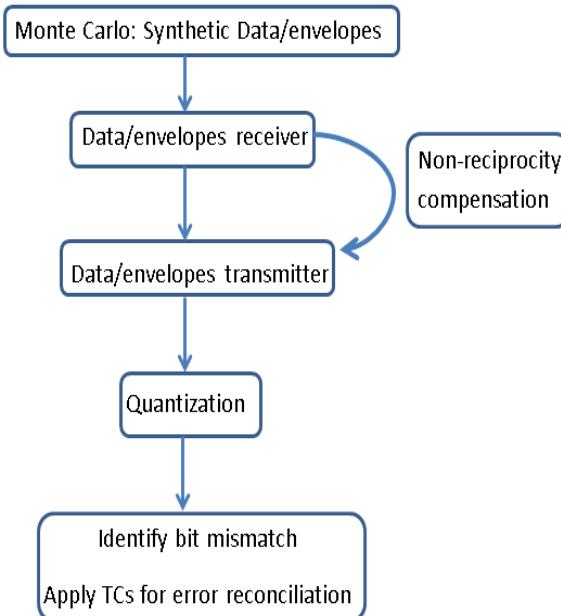


Fig. 2. Detailed architectural design.

A. V2V channel model

The adopted channel model is the comprehensive parametric stochastic V2V channel model presented in [7]. The channel may include a line-of-sight (LOS) path between the transmitter (T_x) and receiver (R_x), or it may be an obstructed, i.e., non-LOS (NLOS) link. The vehicles are in motion, and all are equipped with both T_x and R_x . In suburban areas, the density of vehicles would be smaller, with buildings set farther back from the street. Vehicle density will also affect the V2V channel characteristics. The frequency-time variant channel response is an ensemble of several frequency-time realisations. Furthermore, we consider 3D scattering at both the T_x and R_x . The existence of mobile scatterers between Alice and Bob is also modelled as a means of covering all the effects inducing temporal variability.

B. Receiver's samples

For simulation purposes, we use the theoretical channel model that has been previously described in [7]. The time-variant channel response (Bob's response in time domain) is expressed as

$$G_{Bob}(t) = \sum_{l=1}^L |a_l| \exp(j\varphi_l) \exp(j2\pi\nu_l t) \quad (\text{Eq. 1})$$

The Doppler frequency ν_l is determined by T_x mobility, scatterers' mobility and R_x mobility, respectively: $\nu_l = \nu_{T,l} + \nu_{S,l} + \nu_{R,l}$. Each l^{th} multipath component has its own Doppler shift resulting from the angle of departure (arrival) from the mobile T_x (to the mobile R_x). Details and calculations of the Doppler shift are available in [7].

C. Non-reciprocity compensation and Transmitter's Samples

To generate the transmitter's response $G_{Alice}(t)$ (Alice's channel estimates), the non-reciprocity compensation technique presented in [8] is applied. A channel gain complement technique is used to model the transmitter's samples. The adopted technique compensates channel non-reciprocity, inherent in any realistic wireless communication scenario. Thus, a zero-mean Gaussian noise variable is at any sample time to the receiver's samples $G_{Bob}(t)$ [9]:

$$G_{Alice}(t) - G_{Bob}(t) \sim N(0, \sigma^2) \quad (\text{Eq. 2})$$

The variance is estimated by the discrepancy of the transmitter and receiver samples [9].

D. Quantization and Thresholding

For simulation purposes, an upper and lower threshold are used in the model. After generating the receiver and transmitter's envelopes, Alice and Bob use their channel estimates to discard samples in between the thresholds while selecting only samples above and below the upper and lower threshold, i.e., lossy thresholding. Currently, the lossy quantization scheme from [9] is adopted:

$$Q(x) \begin{cases} 1, & \text{if } G > q_+ \\ 0, & \text{if } G < q_- \end{cases} \quad (\text{Eq. 3})$$

where G is the sample level and q_+ , q_- the upper and lower thresholds used to quantize the samples. We use this approach to compare it against our TC correction process presented in Figure 2.

E. Indexing technique

Alice and Bob exchange channel estimates to find samples above and below the thresholds imposed. Those estimates are samples in a form of an excursion for successive estimates (bit values of 0s and 1s) in half-duplex communication. Thus, Alice and Bob cannot probe the channel simultaneously. Segments of excursions are created whenever a channel estimate is discarded during the quantisation process. The indexing technique simultaneously accomplishes thresholding and information reconciliation. Indeed, a random set of these segments is exchanged between Alice and Bob. They check whether their segments match, and both quantise their channel estimates according to the final shared list.

F. Information reconciliation using Turbo Codes in VANET

In the early nineties, the invention of turbo codes (TCs) [12] was a revival for the channel coding research community. The turbo encoder is formed by the parallel concatenation of two Recursive Systematic Convolutional (RSC) codes separated by an interleaver or permutation. They are called "turbo" about the analogy of the use of feedback in the decoding process, like the turbo principle of a turbo-charged engine, which reuses the exhaust gas to improve efficiency. The turbo decoding principle calls for an iterative algorithm involving two component decoders, one decoder for each elementary encoder. Each decoder estimates the 'a posteriori probability' (APP) of each data bit. The APP's are used as a priori information by the other decoder. This exchange of information improves the error correction performance with a set number of iterations. Performance generally improves from iteration to iteration but follows a law of diminishing returns. The near-capacity performance of TCs and their suitability for practical implementation explain their adoption in various communication standards. In [13] the authors investigated TCs to be used for reconciliation. The study of TCs in [14] shows that they have a good potential for reconciliation purposes. The efficacy of TCs with regards to their error correction capabilities in various wireless communication standards is also recorded in [15]. The authors in [16] demonstrate the improved performance of TCs over the indexing technique in VANETs and incorporate, for the first time, physical propagation characteristics in their model. In our model, parameters such as 3D scattering and scatterers' mobility are also incorporated. In the next, simulations are run, and performance analysis is carried out.

III. SIMULATIONS RESULTS

The authors have designed a Graphical User Interface (GUI) to run the developed algorithm. The GUI is not fundamental to the core algorithmic operation and can be omitted in real-life implementations or fabricated products. An implementation of Alice's and Bob's samples is illustrated in Fig. 3.

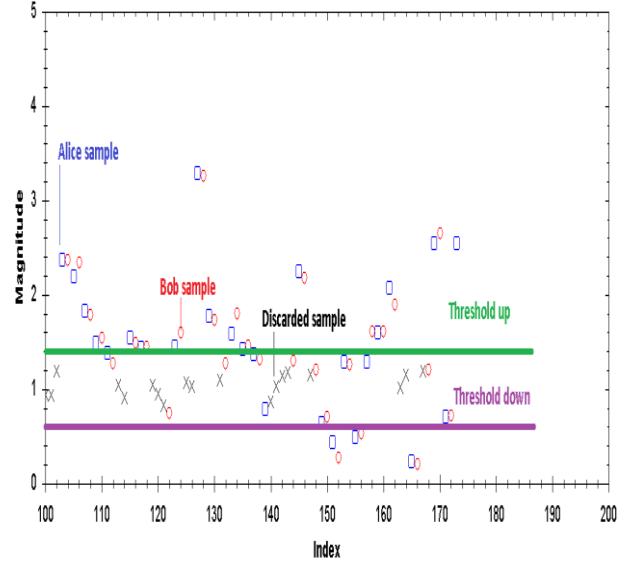


Fig. 3. Normal and discarded samples based on thresholding.

The thresholding scheme employed influences the number of samples discarded from both Alice and Bob. The GUI output also demonstrates the number of keys established during the simulation and the total time required to generate those keys.

A. Simulation results

Before defining the performance indicators, we first analyse the channel probing rate. It determines the rate at which the V2V channel is probed to secure highly uncorrelated successive samples. Thus, we have first appropriately defined the probing rate to maximise the entropy in the subsequent quantization step. To ensure the same number of channel estimates are collected for the transmitter and the receiver, the same probing rate is used for both Alice and Bob.

$$f_p = f_{p,Alice} = f_{p,Bob} \quad (\text{Eq. 4})$$

The core key performance indicators (KPIs) of interest in our protocol up to this stage are the entropy, the key generation rate (KGR), the randomness of the generated bits for symmetric keys and bit mismatch rate (BMR). The entropy is an important metric which quantifies the randomness of the generated bit string. A lack of entropy can have a negative impact on performance and security. Therefore, it is important to establish a secret key with high the entropy to restrain the ability of Eve to get that key. Usually, BMR is defined as the ratio of the number of bits that do not match between Alice

and Bob to the number of all the bits extracted from quantisation.

After the thresholding stage and appropriate quantisation, Bob's channel estimates are fed to the input of a TC. Contrary to the indexing technique where an upper and lower threshold are defined, and some bits are discarded; the quantisation scheme with TCs is lossless since a single threshold is adopted with the potential to substantial increase the key generation rate [17]. To generate symmetric keys for Alice and Bob, an iterative turbo decoding process is then performed to obtain a symmetric output. The BMR and the Bit Error Rate (BER) can be measured to evaluate the performance of the reconciliation method with TCs. Comparisons are made against the sample indexing technique already applied in our algorithm as discussed in subsection *III.E*. The discarded indexes after Alice and Bob have probed the channel are considered in calculating the BMR. Thus, the BMR is measured as a ratio of the number of bits that do not match between the transmitter and the emitter to the number of bits extracted by the adopted quantization process after appropriate thresholding.

TABLE I. SIMULATION RESULTS IN SECRET KEY GENERATION

	Indexing technique			Turbo Codes		
Key length (bits)	128	256	512	128	256	512
BMR	0.22			0.02		
Entropy (bits/sample)	0,85 to 0,97			0,94 to 0,99		
KGR (keys/min)	3 to 7	2 to 5	1 to 2	35 to 39	17 to 19	8 to 9

The key generation rate for different key lengths is computed in In Table I. Compared to the samples' indexing method in [9], there was a significant improvement on both BMR and key generation rate. While the estimated BMR with the indexing technique is around 0.22, the BMR with single thresholding is divided by ten and it is estimated to only 0.02. Note that the BMR with the indexing technique is nearly the same for different key lengths which is coherent with the uniform method used by authors and algorithm presented in [9]. Furthermore, we report the BER performance of the TC for the block size 5000 bits, at coding rate. Thus, the total number of samples is 10000 bits for both Alice and Bob. For a signal to noise ratio $SNR = 0.5 dB$, the simulated BER to generate a symmetric shared key between Alice and Bob after error reconciliation is estimated to only 6×10^{-2} for the 1st iteration using TCs while the BER is 3×10^{-4} for the 4th iteration (see Fig. 4). Also, the obtained key generation rate is considered high for different key lengths. For example, the secret key rate varies from 3 to 7 symmetric keys per minute with the indexing technique to generate the 128-bit symmetric key. When TCs are used for reconciliation purposes, the secret key rate depends on the number of decoding iterations and it is varying between 35 and 39 good keys per minute. Indeed, increasing the number of iterations in the TC can significantly improve the BER, thus generating more symmetric keys. However, a compromise should be found since this operation is computationally expensive and adds a delay in the process. In the simulations of Table I, the maximum number of turbo decoding iterations is set to 4 iterations. The simulations

results shown in Table I reveal similar improvements for different key lengths during the key extraction process. Finally, as part of the error reconciliation process, high entropy values are recorded throughout all rounds of simulation. Note that the higher the entropy, the limited the ability to deduce a secret key established by an adversary such as Eve.

In future studies, we would like to further investigate TCs for error conciliation purposes. To improve the KPI and particularly increase even more the KGR, performance of TCs used for reconciliation purposes is being investigated. We will focus on several parameters BER performance of TCs, such as number of decoding iterations but also decoding algorithms, generator polynomials, and the permutation used. Furthermore, we are working towards the single thresholding process by creating a dynamic threshold that is updated according to the receiver's samples.

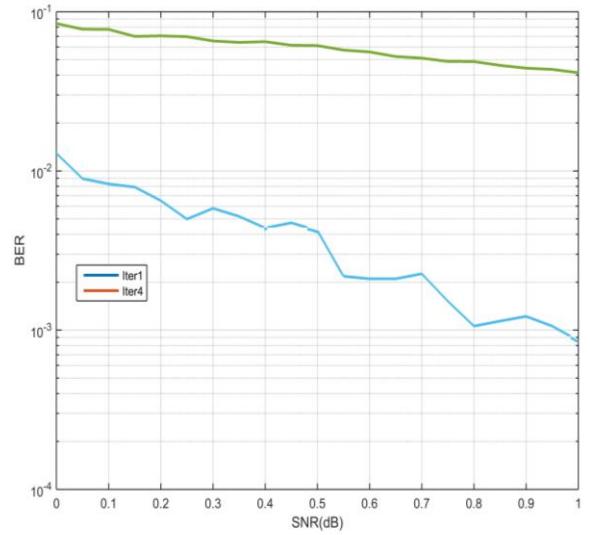


Fig. 4. BER performance of TC for a block length of 5000 bits. All simulations use the BCJR algorithm with 4 decoding iterations.

IV. CONCLUSION

We proposed an algorithm considering the most important features in V2V communication such as 3D multipath propagation and surrounding scatterers' mobility. Synthetic data were generated for the purpose of a demonstration by employing the Monte Carlo simulation method. Simulations were run successfully by combining non-reciprocity compensation with turbo codes. Compared with a sample indexing technique in the public domain, results have shown significant improvements for key generation rate and bit mismatch rate with high entropy values obtained throughout all rounds of simulation.

ACKNOWLEDGMENT

This work was partially funded by the Defense Science and Technology Laboratory (DSTL), under contract CDE 41130. The authors would also like to thank Mr George Samartzidis for his initial contribution in the algorithm development.

REFERENCES

1. M. J. B. Robshaw and O. Billet, Eds., New Stream Cipher Designs - TheeSTREAM Finalists, ser. Lecture Notes in Computer Science. Springer, 2008, vol. 4986.
2. N. K. Jha, A. Raghunathan, N. R. Potlapally, and S. Ravi, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols," *IEEE Transactions on Mobile Computing*, vol. 5, no. undefined, pp. 128–143, 2006.
3. A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of Physical layer security in multiuser wireless networks: A survey," *CoRR*, vol. abs/1011.3754, 2010.
4. Y. E. H. Shehadeh and D. Hogrefe, "A survey on secret key generation mechanisms on the physical layer in wireless networks," *Sec. and Commun. Netw.*, vol. 8, no. 2, pp. 332–341, Jan. 2015.
5. T. Wang, Y. Liu, and A. V. Vasilakos, "Survey on channel reciprocity based key establishment techniques for wireless systems," *Wireless Networks*, vol. 21, no. 6, pp. 1835–1846, 2015.
6. F. Qu, Z. Wu, F. Y. Wang, and W. Cho, "A security and privacy review of vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985–2996, Dec 2015.
7. P. Karadimas and D. W. Matolak, "Generic stochastic modeling of vehicle-to-vehicle wireless channels," *Vehicular Communications*, vol. 1, no. 4, pp. 153–167, 2014.
8. H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response." in *INFOCOM. IEEE*, 2013, pp. 3048–3056.
9. S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, *Secret Key Extraction from Level Crossings over Unauthenticated Wireless Channels*. Springer US, 2010, pp. 201–230.
10. P. Hirschhausen, L. Davis, D. Haley and k. Lever, "Identify key design parameters for Monte Carlo simulation of Doppler Spread channels," in *Communications Theory Workshop (AusCTW)*, Sydney, 2014.
11. P. Hoecher, "A statistical discrete-time model for the WSSUS multipath channel," *IEEE Transactions on vehicular technology*, vol. 41, no. 4, 1992.
12. C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes," in *Proc. ICC'93*, Geneva, Switzerland, vol. 2, May 1993, pp. 1064–1070.
13. K. Nguyen, G. V. Assche, and N. J. Cerf, "Side-information coding with turbo codes and its application to quantum key distribution," *CoRR*, vol. cs.IT/0406001, 2004.
14. N. Benlataief, H. Rezig, and A. Bouallegue, "Toward efficient quantum key distribution reconciliation," *Journal of Quantum Information Science*, vol. 2014, 2014.
15. E. Yeo and V. Anantharam, "Iterative decoder architectures," *IEEE Communications Magazine*, vol. 41, no. 8, pp. 132–140, Aug 2003.
16. Epiphaniou, G., Karadimas, P., Kbaier Ben Ismail, D., Al-Khateeb, H., Dehghanianha, A., Choo, K. K. R. "Non-Reciprocity Compensation Combined with Turbo Codes for Secret Key Generation in Vehicular Ad. Hoc. Social IoT Networks", *IEEE Internet of Things Journal*.
17. B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, ser. CCS '07. New York, NY, USA: ACM, 2007, pp. 401–410.