Quantisation feasibility and performance of RSS-based secret key extraction in VANETs

Quantisation feasibility and performance of RSS-based secret key extraction in VANETs

Mirko Bottarelli*, Gregory Epiphaniou†, Dhouha Kbaier Ben Ismsail†,
Petros Karadimas‡ and Haider Al-Khateeb†
*Institute for Research in Applicable Computing (IRAC), University of Bedfordshire, Bedfordshire, UK
†Wolverhampton Cyber Research Institute (WCRI), University of Wolverhampton, UK
‡School of Engineering, University of Glasgow, Scotland
Email: *mirko.bottarelli@study.beds.ac.uk, †g.epiphaniou@wlv.ac.uk, †d.Kbaier@wlv.ac.uk, †H.Al-Khateeb@wlv.ac.uk,
‡Petros.Karadimas@glasgow.ac.uk

***Abstract*—Vehicular Ad Hoc Networks (VANETs) has emerged as a unique implementation of Mobile Ad Hoc Networks (MANETs). These networks promise to increase road safety and improve the driving experience by exploiting recent advances in wireless technologies for both intra-vehicle and inter-vehicle communications. Physical layer security is a promising alternative approach to secure communication in VANETs where physical and applications' constraints encourage the use of lightweight and fast cryptographic algorithms. Our work focuses on the quantisation stage of the secret generation process, by reviewing existing schemes in the public domain and associated performance metrics. Evaluations are done through simulation with the aid of a wireless channel model which includes three-dimensional scattering and scatterers' mobility. Preliminary findings show that RSS-based algorithms do not perform efficiently in the proposed vehicular stochastic wireless model. Hence they are not able to satisfy the typical low latency required in safety-related broadcasting messaging. We conclude that more research is desirable to design protocols capable of taking advantage from the nodes' high-mobility and the consequent variability of both coherence intervals and level crossing rates, to further improve secret bit extraction throughput.**

***Index Terms*—Physical layer security, Secret bit extraction, Key Generation Rate, Vehicle Ad-hoc Networks**

I. Introduction

ROAD-safety plays a key role in all societies, especially in developing countries where the transport system is continuously changing to support expanding cities. In low and medium income countries Global Health Observatory (WHO) anticipated that by 2017 the vast majority of people will be living in urban areas, pushing towards a rapid yet disorganised increase in transport infrastructures often resulting in a drastic reduction of road-users safety [1]. For example, in Brazil, about 30.000 people die in road accidents every year where in South Africa the incidence of this event happening is even higher. Most of these accidents could have been avoided if the driver had been alerted in time [2]. Intelligent Transport System (ITS), born from the synergy among transport engineering, informatics, electronics and communication networks, aims to simultaneously increase transport-safety, quality and efficiency and decrease environmental impact. Furthermore, these objectives are not entirely disjunct, but often causally interconnected and interrelated, as in the reduction of road accidents which would imply a subsequent decrease in traffic-jams and hence a reduction of pollution from fumes [3].

A fundamental concept underlying ITS is the interconnection and communication of both transport entities and road-side infrastructures through Vehicle Ad-hoc Networks (VANETs), where nodes collaborate to spread vital messages, navigation-related information, internet access and other infotainment data. The large variety of applications and services, the high number of user and the heterogeneous set of circulating data render the VANETs possible and desirable targets of many attacks, encouraging the design of architectures imbued of security considerations [4] [5] [6].

The establishment of secure communications requires, among other properties, the presence of an authentication mechanism, with which nodes could identify themselves as vehicles or road-side units. The integrity of the messages needs to be maintained through all the transmission life-cycle against voluntary (made by unauthorised entities) or involuntary alterations (deterioration), guaranteeing the validity of their contents, which must not be available or disclosed to illegitimate parties, preserving confidentiality.

The realisation of a complete security scheme, which fulfils the specific requirements of VANETs, is still under investigation by researchers. Currently proposed approaches rely on the use of public key infrastructure (PKI) where RSA and Diffie-Hellman schemes are the typical choices. These, however, require a significant amount of channel capacity and computational capabilities which may not be available in VANETs, which significantly reduce the overall network performance. On the other hand, symmetric cryptography achieves high security together with high-speed processing and ease of implementation [7]. Unfortunately, the fundamental task of sharing the secret key between the legitimate parties must be addressed, eventually worsened by the continuously connecting-disconnecting nature of this kind of networks.

Surprisingly, the wireless medium provides a unique source of randomness that can be 'digested' to generate secure keys. The wireless signal is often subjected to intense reflection and diffraction that creates multipath propagation phenomena [8], [9], [10]. Changes in the transmitters and receivers' positions and velocity of intermediate objects significantly influence the

resulting signal, due to the sum of different phases coming from different paths.

Even if multipath variability is considered as a stochastic process, the channel reciprocity principle [11] guarantees that its effects are almost identical for both communicating parties, a correlation which rapidly vanishes with time and at a distance in the order of half a wavelength [12]. Physical layer (PHY) security protocols simultaneously exploit such a correlation and time-spatial variabilities to extract and share secure keys with low computational complexity, low bandwidth usage and provide unconditionally secure communications [13].

VANETs expose a continuously changing nature which constitutes a fertile ground for physical layer security protocols. However, despite the high number of schemes available in the literature, their application in real-world scenarios is limited. In [14] researchers adapt accordingly their previously proposed physical-layer-security scheme [15] and offer two different algorithms for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications, based on reciprocity and diversity theorems, respectively. They do not seem to consider the challenging time constraints of VANETs applications, which are further analysed in [16]. Researchers also propose to use slow fading (i.e., log-normal-modelled spatial variations) along with fast fading (i.e., Rayleigh-modelled temporal variations) when the transmitter and receiver's speed difference is negligible.

None of the previous schemes considers the presence and the possible interactions among vehicles and intermediate objects. Work in [17] incorporates three-dimensional scattering and scatterers' mobility to obtain a more realistic system model and corresponding simulation [18]. The application of a non-reciprocity compensation technique in conjunction with an information reconciliation phase based on turbo codes, record a significant improvement in both key generation rate and bit mismatch rate (defined in Section 3). Besides the improvements towards more accurate VANETs models, previous schemes rely on a standard lossy quantisation approach, where the choice of the thresholds is made in a context-unaware way.

This work compares and contrasts existing quantisation schemes for secret key generation when applied in vehicular networks. Performances are evaluated through extensive simulations in a stochastic wireless model which includes three-dimensional scattering and scatterers' mobility [18], in order to analyse the feasibility of physical security protocols in a urban high-trafficked scenarios.

The paper is structured with introduction above followed by Section 2 which gives a brief overview of VANETs' security constraints and reviews existing literature on physical secret key generation focusing on quantisation aspects. Section 3 introduces the fundamental performance metrics to be used in our work. Section 4 presents the V-V channel model, its simulation parameters and analyses the results. Finally, Section 5 concludes this paper.

II. Related Works

Vehicle Ad-hoc Networks (VANETs) are a subclass of Mobile Ad-hoc Networks (MANETs) in which vehicles and road infrastructures collaborate through dedicated short-range communications (DSRC). Two types of radio apparatus represent the node in a VANET: vehicles' on-board-units (OBUs) and road-side units (RSUs). Besides supplying the ability to connect to the wireless medium, OBUs and RSUs also have to implement several aspects regarding security. These aspects include protection of sensible data, drivers' identity and vehicles' kinematic data in tamper-proof devices (TPDs) and providing fundamental cryptographic abilities through mixed hardware and software trusted platform modules (TPMs) [6].

Even if the term ad-hoc usually refers to networks with specialised unicast routing algorithms, in the specific case of VANETs, the "ad-hoc" concept assumes a broader sense which indicates a decentralised network, built on no pre-existing infrastructures with routing determined only by the current connectivity and topology. Furthermore, broadcasting techniques are more suitable for critical messages, which are emitted in a periodic or event-driven fashion in safety-related applications [19] to reduce accidents, as the implementation of the cooperative forward collision warning.

The absence of a central coordinator and the necessity of broadcasting both justify the creation of a control channel (CC), as well as the rising importance of PHY/MAC layers. The current focus is on the IEEE 802.11 family of standards in which the American Society for Testing and Materials (ASTM) and IEEE modified the WLAN IEEE 802.11a standard obtaining the new IEEE 802.11p (WAVE) to support vehicular wireless communications and Intelligent Transport System's services. This new standard is based on orthogonal frequency division multiplexing (OFDM), a CSMA-based scheme and a bandwidth of 10MHz (down from 20MHz of IEEE 802.11a) centred at 5.9GHz, resulting in a channel capacity in the range 3-27 Mb/s [20].

In [21] scientists analyse how different factors concur on the probability of receiving packets and state that it is better to renounce high-speed data rates, to maximise the packet-capture capabilities. A MAC layer based on enhanced distributed channel access (EDCA) has been proposed to increase reception probabilities of high-priority packets. However, the current standard IEEE 802.11p seems to be quite limited for the ITS services to rely upon. For a full survey on VANETs challenges and vulnerabilities, the reader is encouraged to refer to [6] [22] [5].

Besides the limited data-rate, the main characteristic of VANETs is their high mobility and continuously changing topology due to the random speed of nodes and their frequent disconnection. Volatile and short-life communications harden the task of securing the wireless link and simultaneously dispatching alert messages in the pre-established delay. For instance, safety-related messages require a minimum transmission frequency of 10Hz with a maximum latency of 100ms [23]. Furthermore, in [24] authors analyse the relationship

between data-packet sizes and communication efficiency in VANETs, concluding that small packets achieve better transmission rate.

Security approaches have to take into account previous constraints, aiming to design light-weighted protocols with both low transmission overhead and high-speed processing. A viable path consists of the use of symmetric cryptography together with a PHY key generation scheme, providing both faster encryption-decryption and a continuous refreshment of secret keys which need not be exchanged.

A. The secret key generation process

In its simplest form, in physical layer security, the secret key is generated through a three-step process: advantage distillation, information reconciliation and privacy amplification.

The first block [25], [26] extracts mutual information between legitimate parties Alice and Bob through an interleaved exchange of probes. The duration of the probing phase is proportional to the desired key length, while the probing frequency depends on the dynamic characteristics of the channel.

To collect correlated estimates Alice and Bob must collect their measurements inside the coherence time T_c of the channel that represents the time duration over which the channel impulse response is considered as not changing. In wireless medium the coherence time is strictly connected to Doppler effects due to nodes' movements [27]. Specifically, the coherence interval is the time domain dual of the maximum Doppler frequency f_m, hence $T_c \approx 1/f_m$. A fast probing rate will quickly result in redundant estimates which are not suitable for the generation of a key and must be re-sampled to extract a distinct measurement for each coherence time.

Even at the fastest probing frequency, the half-duplex limitation of the wireless channel does not allow nodes to acquire beacons simultaneously, and the positive delay induces (small) asymmetries at the received signals triggered by the white nature of the noise. In a very few cases, these asymmetries are addressed by preventive and compensation techniques such as an interpolation based on Cubic Farrow filters [28] [29] or an application of low pass filters [30] [31] [32] [33]. However, in the vast majority of protocols, differences due imperfect reciprocity are left untouched until the information reconciliation step, explained hereafter.

The core of the distillation stage is the quantisation step where channel's estimates are converted into binary strings. Quantisation plays a primary role in the entire extraction process because its output has the potential of becoming a shared secret key and its performance dramatically influences the overall efficiency of the protocol and its applicability in real-world scenarios. Unfortunately, every quantisation scheme should be designed by considering three contrasting metrics, which are the Bit Mismatch Rate (BMR), the Bit Generation Rate (BGR) and key robustness, in the challenging effort to simultaneously minimise the first one, while increasing as much as possible the others.

Quantisation schemes are said to be lossless if they can generate at least one bit for each estimate, for example using a single threshold. On the other hand, conversion algorithms may choose to drop values to both decreases the disagreement probability as well as maximise the generated sequence entropy, referred to as lossy or censor schemes.

Following quantisation, bit-streams enter into an information reconciliation block which has the duty of compensating imperfect reciprocity and correcting any key disagreement between communicating nodes. Its implementation varies from error correction codes to fuzzy information reconciliation techniques [34] with the aid of a public channel. A widely used approach, called $CASCADE$, was proposed in [35] in which disagreements are resolved through iterative parity-based correction codes calculated on randomly permuted bit sequences. Other works tried to both improve reconciliation capabilities and reduce the information leakage during the public discussion [36] [37].

After the information reconciliation step, Alice and Bob's bit-streams should be identical otherwise the key generation process is restarted. These sequences, however, are not yet ready to be used as a key because they still contain information used in their creation. The step of privacy amplification sacrifice part of the key to elevating its entropy, as in the application of a universal hash function [38].

B. Quantisation schemes

Quantisation schemes are strongly linked to the channel characteristics, used as sources of randomness for secret keys generation. Received Signal Strength (RSS), Channel Impulse Response (CIR) and phase are the most popular channel parameters used in estimates. More precisely, RSS is the most common approach because its value is available in all out-of-the-shelf transceivers on a frame basis hence, dramatically reducing design and implementation costs. Unfortunately, RSS values are correlated with distance, and the entropy is greatly influenced by the mobility of the nodes and intermediate objects, exposing vulnerabilities against predictive and active attacks.

Phase [39] [40] and CIR-based approaches [41] [31] [36] are more resilient to incursions, and able to generate long secret keys depending on the uniformly distributed nature of the former, as well as the CSI details were given by the latter. However, phase and CIR protocols require complex hardware capabilities which reduce their possible application scenarios.

Following from the fact that the wireless signal behaves independently in different antennas, in Multiple Input Multiple Output (MIMO) scenarios the amount of mutual information is greater than the one in single antenna single frequency protocols. Therefore it allows improved performance in the secret key extraction rate [42] [43].

In VANETs, the high-mobility of nodes and the continuous changing of the complex topology make up for RSS vulnerabilities stated above, especially in a highly-trafficked urban scenario where multi-path effects dominate the more predictable line-of-sight component. Following this consideration and the fact that the vast majority of out-of-the-shelf transmitters have only one available antenna, the present work

will focus on the most representative Single Input Single Output (SISO) RSS schemes in the literature.

A first technique was presented by Tope et al. [44] based on the evaluation of signal attenuation caused by multipath channels extracted from the envelope of received packets. Let X_k for $k = 0, 1...N-1$ be the array of envelope samples and Δ_k the sequence obtained by subtracting half values from the other half. The quantisation function drops the estimates that lie outside the two fixed thresholds γ_l, γ_h to avoid measurements with a high probability of disagreement ($\Delta_k < \gamma_l$) or easily predictable ($\Delta_k > \gamma_h$).

To improve bit agreement rate, in [32] scientists propose the use of a single threshold to detect deep fades, i.e. local minima of the wireless signal. An improvement of this work has been proposed in [41] where Mathur et al. give a detailed analysis of quantisation parameters. The lossy quantisation is based on two thresholds q_+, q_- calculated using average and standard deviations of estimates, which are previously removed of slowly changing RSS variations by subtracting a running average.

Both communicating parties search their estimates for all excursions above q_+ and below q_- that last at least for $m > 0$ time slots and agree with the counterpart on a list of corresponding indices which will be used for the final key extraction. Thresholds levels and minimum excursion parameter m should be chosen accordingly considering the expected probability of key disagreement, as well as the key generation rate.

In [45] Jana et al. improve the previous scheme introducing an algorithm named Adaptive Secret Bit Generation (ASBG) where thresholds are dynamic and locally calculated in every block of estimates of a configurable size. Multi-level quantisation is applied to all measurements. However, the number of bits per estimate N is severely constrained by noise. In [46], authors improved further their analysis exploring the key generation possibilities offered by multiple input multiple output (MIMO) contexts.

In [47] researchers introduce a lossless quantisation scheme employing a least-square polynomial curve as the threshold and a neural-network-based information reconciliation. Simulations suggest that even a small polynomial's degree lead to high-level crossing rate (LCR) in both Richian and Rayleigh fading models.

A first attempt to mitigate imperfect reciprocity is introduced with HRUBE [29] which interpolates channel measurements to consider them as retrieved at the same time instant. Furthermore, the algorithm uses Karhunen-Loève Transform (KLT) to obtain vectors with uncorrelated components. The adaptive ranking-based uncorrelated bit extraction protocol (ARUBE) has been proposed in [48] as an improvement over HRUBE, based on a ranking method which both makes the scheme independent of the specific fading distribution and normalises the scale of signal powers due to different hardware characteristics.

Fading trends as quantisation input are evaluated in [28] where the assumption is that legitimate parties are more likely to agree on positive or negative RSS trends instead of absolute values. Trends are directly converted into bit-streams using their variations' polarity while other estimates are quantised through a standard multi-level scheme.

In [37] Aono et al. make use of an electronically steerable parasitic array radiator (ESPAR) antenna to create artificial randomness of channel's measurements. Sequences of estimates contain $K + \alpha$ items, where K is the desired key length and α addresses imperfect reciprocity. Disagreement is reduced by considering sub-sequences composed of highest and lowest values which are then losslessly quantised using the median value as the unique threshold. An improvement of this scheme is shown in [49] with the application of an RSS-interleaving technique which randomises and strengthens the keys.

A modified version of Mathur et al. lossy scheme is proposed in [17] where m consecutive excursions need not be on the same side (either below the lower threshold or above higher threshold). Despite being more influenced by sharp magnitude changes, resulting bit-streams are the direct concatenation of whole quantised excursions instead of considering only the exchanged indices, as in the inspiring protocol.

III. Quantisation performance metrics

The quantisation schemes in literature are evaluated under many performance metrics, for example, the ease of implementation translates in a reduction of deployment costs, while the scalability of the protocol determines to what extent the algorithm is adaptable to a larger group of nodes. However, the fundamental metrics are the randomness or the entropy of the key, the bit generation rate (BGR) and the bit mismatch rate (BMR).

A. Randomness or entropy of the key

Similar to any conventional cryptographic method, in physical layer security algorithms the key must not have any statistical defects in order to maximise the uncertainty from eavesdropper's point of view. Given a key of length N, the associated entropy is defined as follows:

$$H = \sum_{i=0}^{N} -p_{0,i} log p_{0,i} - (1 - p_{0,i}) log(1 - p_{0,i})$$

where $p_{0,i}$ is the probability of bit i being 0.

Therefore, the key must expose properties that a truly random sequence would probably exhibit as expressed in [50]. Even if there are infinite statistic properties of random sequences, a finite subset of fifteen tests is provided by the National Institute of Standards and Technology (NIST) [51]. That aims to verify different aspects, such as the frequency of 0s and 1s, the frequency of longer runs, periodic features, etc. Some tests require a certain sequence of the length outside the magnitude of a key generation system, so they are merely avoided. In the key generation process, there is a privacy amplification stage whose objective is to improve key randomness.

B. Bit mismatch rate

The bit mismatch rate (BMR) is an evaluation parameter strictly correlated to the quantisation step (for example to the number of its levels), and it is defined as the ratio of mismatch bits between Alice and Bob to the total number of quantised bits. Low levels of BMR confirm the resilience of the quantisation scheme against the noise and the asymmetric differences of the channel. On the contrary, high BMRs could significantly influence the overall performance of the systems since a single uncorrectable bit may force the rejection of the entire sequence and the restart of the full process. In the case of group key extraction, the total BMR could be either defined as the average or the maximum BMR from all nodes' pairs.

C. Bit generation rate

The bit generation rate (BGR) is defined as the number of secret bits generated per unit time. This metric embraces all the phases of the extraction process. Hence, it acts as a global performance indicator. Unfortunately, BGR often depends on environmental characteristics, such as nodes' movements and multipath richness. Higher values of BGR indicate the faster ability of two nodes of generating a key of the desired length, therefore improving the efficiency and the security of the communication.

IV. Simulation parameters and results

The first step in creating a realistic simulation for V2x environments rely on the choice of a channel model capable of capturing relevant propagation properties [18], and composed of a discrete set of time-varying and frequency-selective channel taps. These correspond to resolvable delay paths distributed according to specific delay and Doppler spectrum [52].

Channel taps are generated as a sum of sinusoids, i.e. multipaths echoes unresolvable in delay, whose frequencies and phases are chosen in a deterministic or random fashion. In the former, sinusoids' weights are calculated in a bottom-up reproducible, yet complex manner, while in the latter, they are the output of a Monte Carlo process, piloted by the interested Doppler probability density function [53]. The random approach provides numerical stability, easy of implementation and fast computational processing. Therefore, it seems to be the natural choice in designing accurate, yet straightforward systems [54].

According to [18], the frequency-time variant channel response is

$$G(f,t) = \sum_{l=1}^{L} |\alpha_l| exp(j\phi_l) exp(j2\pi v_l t) exp(-j2\pi f \tau_l)$$

where L is the number of multipath components, each-one having a the complex amplitude $|\alpha_l|exp(j\phi_l)$ where $|\alpha_l|$ is the magnitude with random phase ϕ_l, a delay τ_l and Doppler frequency v_l.

Considering narrowband frequency-invariant V-V channel with three-dimensional scattering at both communicating nodes, the previous equation can be simplified as

$$G_N(t) = G(0,t) = \sum_{l=1}^{L} |\alpha_l| exp(j\phi_l) exp(j2\pi v_l t)$$

where the Doppler contributions of transmitter $v_{T,l}$, receiver $v_{R,l}$ and scatterers $v_{S,l}$ add up, thus

$$v_l = v_{T,l} + v_{S,l} + v_{R,l}$$

obtained by the trigonometric projection of their maximum values $v_{T(R)max}, v_{Smax}$ in respect to azimuth angles $\alpha_{T(R),l}$ and elevations $\beta_{T(R),l}$ of both departure (AOD) and arrival (AOA) of the corresponding multipath echo [18]. Scatterers are modelled by directly manipulating AOA and AOD angles α_1, α_2 of the impacting multipath component, to avoid the inaccuracies emerging from unrealistic randomisation of scatterers' directions of movement.

As stated in [17], previously introduced parameters are appropriately chosen to recreate a Rayleigh-modelled environment suitable for urban scenarios with heavy scatterers' influence. As an improvement, the introduction of a line-of-sight component and the consequential rise of Rician fading have to be investigated in future efforts, making the model also adequate for rural and high-ways backgrounds.

The number of multipath components is $L = 20$ and their complex amplitudes have a constant magnitude $|\alpha_l| = \sqrt{2/L}$ and a uniformly distributed phase $\phi_l \sim U[-\pi, \pi]$ as suggests in [54]. Furthermore, angles of departure (AOD) and arrival (AOA) are uniformly distributed, thus

$$\alpha_{T(R),l} \sim U[A_{T(R)min}, A_{T(R)max}]$$

$$\beta_{T(R),l} \sim U[B_{T(R)min}, B_{T(R)max}]$$

$$\alpha_1, \alpha_2 \sim U[-\pi, \pi]$$

Scatterers' speed is randomised following a Weibull distribution which has been proved to model multipath power contribution of mobile scatterers [55] adequately.

Probing rate $F_p = 1/T_{coh}$ is set to the maximum possible frequency achievable without introducing statistical defects in the generated streams, which means estimates have to be collected from uncorrelated different coherence regions of duration T_{coh} defined as

$$T_{coh} = \frac{c}{f_c(v_{Tmax} + v_{Rmax} + 2v_{Smax})}$$

Considering $v_{Tmax} = v_{Rmax} = v_{Smax} = 30m/s$ the maximum probing rate is $F_p = 2400Hz$.

A. Results

Simulations are composed of several runs of 10.000 estimates to stabilise the evaluation metrics. Without considering any correcting codes at this stage, lossless quantisation schemes such as [49] seem not to able to generate zero-disagreement bit-streams. A standard lossy quantisation scheme defines two thresholds q_-, q_+ and a quantisation function $Q(\cdot)$

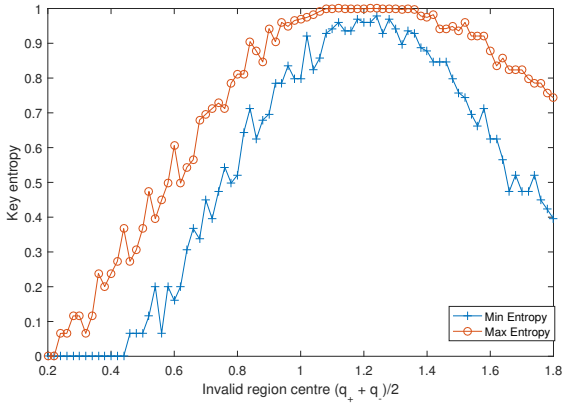

Fig. 1. Key entropies of differently positioned invalid regions.

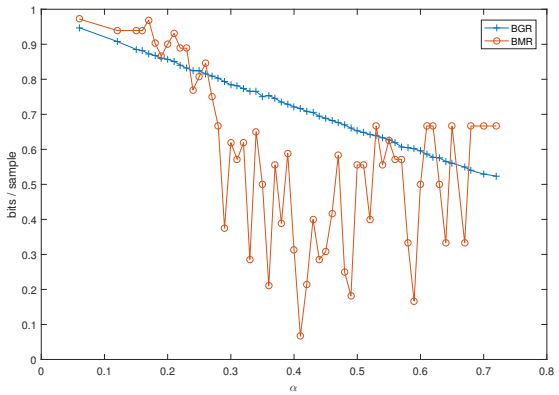

Fig. 2. BGR and BMR behaviours for different α values.

$$Q(x) = \begin{cases} 1, & \text{if } x > q_+ \\ 0, & \text{if } x < q_- \\ \text{dropped} & \text{otherwise} \end{cases}$$

Considering a fixed invalid region with size $q_+ - q_- = 0.4$, figure 1 reveals that key entropy assumes maximum values (~ 0.95) when thresholds are centred on Rayleigh distribution mean $(q_+ + q_-)/2 = \sigma\sqrt{\frac{\pi}{2}} \sim 1.2533$ where $\sigma = 1$ is the scale parameter. In these conditions, the commonly used Mathur et al. scheme [41] achieves a bit generation rate of approximately ~ 0.2 bits/sample whilst the recent scheme [17] records ~ 0.76 bits/sample, however, higher results > 0.8 are achievable sacrificing key robustness. Unsurprisingly, a wider invalid region implies a reduction of both BMR and BGR, justified by the smaller probability of bit disagreement and the increased number of dropped values, respectively.

Thresholds can be statistically computed by means of average μ and standard deviation σ, as follows

$$q_+ = \mu(\hat{\underline{h}}) + \alpha \cdot \sigma(\hat{\underline{h}})$$

$$q_- = \mu(\hat{\underline{h}}) - \alpha \cdot \sigma(\hat{\underline{h}})$$

where $\hat{\underline{h}}$ is the array of estimates. Thresholds are refreshed every $|\hat{\underline{h}}| = 10$ coherence intervals in response to the unpredictable stationarity region of VANETs [18]. Parameter α determines the influence of standard deviations in computing thresholds' distance: lower α values increase BGR but also increase BMR. Evaluations showed an optimal value $\alpha = 0.3$ (see figure 2) achieving a throughput of ~ 0.85 bits / sample, a small yet significant improvement over the previous fixed thresholding strategy. However, considering a key length of 128bits and transmission rate of 300 packets per second [24], the examined protocols can generate a shared secret key in about a second, which is insufficient for the low latency required in safety-related VANETs applications.

V. Conclusions

We have introduced vehicular communication properties and security constraints and analysed the possible solution offered by the physical layer key generation approach. RSS-based schemes are attractive due to their ease of implementation on off-of-shelf devices and because key entropy is highly correlated to wireless nodes mobility, which is the fundamental characteristic of VANETs.

Extensive simulations have been evaluated to test the most representative protocols against a stochastic V-V channel model which consider three dimensional scattering and scatters mobility. Besides the increasing performances of recent protocols, they still need to improve bit generation rate to provide a sufficiently fast key agreement for low-latency safety-related services and keep an high level of entropy to guarantee statistical resilience.

Future studies should investigate in depth the possibility of creating a quantisation scheme which better suits the referenced stochastic V-V model and its peculiar properties, for example by adapting the probing rate, the number and the tolerances of quantisation bins, in response to sharp changes in channel variability caused by transmitter, receiver and scatterers mobility.

References

[1] GIZ, "Urban Road Safety," *Sustainable Transport: A Sourcebook for Policy-makers in Developing Cities*, 2017.

[2] M. Vanderschuren, "Safety improvements through Intelligent Transport Systems: A South African case study based on microscopic simulation modelling," *Accident Analysis and Prevention*, vol. 40, no. 2, pp. 807–817, 2008.

[3] S. Grant-Muller and M. Usher, "Intelligent Transport Systems: The propensity for environmental and economic benefits," *Technological Forecasting and Social Change*, vol. 82, no. 1, pp. 149–166, 2014. [Online]. Available: http://dx.doi.org/10.1016/j.techfore.2013.06.010

[4] L. P. Gafencu, L. Scripcariu, and I. Bogdan, "An overview of security aspects and solutions in VANETs," in *ISSCS 2017 - International Symposium on Signals, Circuits and Systems*, 2017.

[5] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Vehicular Communications*, vol. 7, pp. 7–20, 2017. [Online]. Available: http://dx.doi.org/10.1016/j.vehcom.2017.01.002

[6] M. Raya, P. Papadimitratos, and J.-p. Hubaux, "SECURING VEHICULAR COMMUNICATIONS," *IEEE Wireless Communications*, vol. 13, no. 5, pp. 8–15, oct 2006. [Online]. Available: http://ieeexplore.ieee.org/document/4015703/

[7] A. Menezes, P. van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography," vol. 19964964, 1996. [Online]. Available: http://www.crcnetbase.com/doi/book/10.1201/9781439821916

[8] A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu, "Cryptographic Key Agreement for Mobile Radio," *Digital Signal Processing*, vol. 6, no. 4, pp. 207–212, 1996.

[9] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[10] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," *IEEE International Symposium on Information Theory - Proceedings*, pp. 2593–2597, 2006.

[11] G. S. Smith, "A direct derivation of a single-antenna reciprocity relation for the time domain," *IEEE Transactions on Antennas and Propagation*, vol. 52, no. 6, pp. 1568–1577, 2004.

[12] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy," *Proceedings of the 14th ACM international conference on Mobile computing and networking - MobiCom '08*, p. 128, 2008. [Online]. Available: http://portal.acm.org/citation.cfm?doid=1409944.1409960

[13] C. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal, Vol 28, pp. 656–715*, Oktober 1949.

[14] B. Zan, M. Gruteser, and F. Hu, "Key agreement algorithms for vehicular communication networks based on reciprocity and diversity theorems," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 8, pp. 4020–4027, 2013.

[15] ——, "Improving robustness of key extraction from wireless channels with differential techniques," *2012 International Conference on Computing, Networking and Communications, ICNC'12*, pp. 980–984, 2012.

[16] M. Syvanen, J. Wan, A. B. Lopez, and M. A. Al Faruque, "Exploiting Wireless Channel Randomness to Generate Keys for Automotive Cyber-Physical System Security," in *2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems, ICCPS 2016 - Proceedings*, vol. 13, no. 2, Vienna, Austria, jan 2016, pp. 13:1—-13:10.

[17] G. Epiphaniou, P. Karadimas, D. K. B. Ismail, H. Al-Khateeb, A. Dehghantanha, and K. K. R. Choo, "Non-Reciprocity Compensation Combined with Turbo Codes for Secret Key Generation in Vehicular Ad Hoc Social IoT Networks," *IEEE Internet of Things Journal*, no. October, 2017.

[18] P. Karadimas and D. Matolak, "Generic stochastic modeling of vehicle-to-vehicle wireless channels," *Vehicular Communications*, vol. 1, no. 4, pp. 153–167, 2014. [Online]. Available: http://dx.doi.org/10.1016/j.vehcom.2014.08.001

[19] VSC-A Consortium, "Vehicle Safety Communications Applications (VSC-A) Project Final Report," *Security*, no. September, 2011.

[20] X. Ma, X. Chen, P. Hightower, M. Abdul-hak, N. Al-Holou, U. Mohammad, K. Sjöberg-Bilstrup, E. Uhlemann, E. G. Strom, A. M. S. Abdelgader, W. Lenan, S. M. Nazir, and R. Rastogi, "The Physical Layer of the IEEE 802 . 11p WAVE Communication Standard : The Specifications and Challenges," *Electric Vehicles - Modelling and Simulations*, vol. II, no. 3, pp. 1–5, 2014.

[21] M. Torrent Moreno, D. Jiang, and H. Hartenstein, "Broadcast Reception Rates and Effects of Priority Access in 802.11-Based Vehicular Ad-Hoc Networks," *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks (VANET 2004)*, pp. 10–18, 2004. [Online]. Available: http://portal.acm.org/citation.cfm?id=1023878

[22] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, 2014.

[23] E. C. Eze, S. J. Zhang, E. J. Liu, and J. C. Eze, "Advances in vehicular ad-hoc networks (VANETs): Challenges and road-map for future development," *International Journal of Automation and Computing*, vol. 13, no. 1, pp. 1–18, 2016.

[24] C.-K. Park, K.-H. Cho, M.-W. Ryu, and S.-H. Cha, "Measuring the Performance of Packet Size and Data Rate for Vehicular Ad Hoc Networks," *2013 International Conference on Information Science and Applications (ICISA)*, pp. 1–2, 2013. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6579370

[25] C. Cachin and U. M. Maurer, "Linking information reconciliation and privacy amplification," *Journal of Cryptology*, vol. 10, no. 2, pp. 97–110, 1997. [Online]. Available: http://dx.doi.org/10.1007/s001459900023

[26] U. Maurer, "Secret key agreement by public discussion," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993, preliminary version: [**?**].

[27] T. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2001.

[28] H. Liu, J. Yang, Y. Wang, and Y. Chen, "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks," in *2012 Proceedings IEEE INFOCOM*, March 2012, pp. 927–935.

[29] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 17–30, Jan 2010.

[30] S. T. Ali, V. Sivaraman, and D. Ostry, "Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices," *IEEE Transactions on Mobile Computing*, vol. 13, no. 12, pp. 2763–2776, 2014.

[31] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *2013 Proceedings IEEE INFOCOM*, April 2013, pp. 3048–3056.

[32] 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. [Online]. Available: http://doi.acm.org/10.1145/1315245.1315295

[33] A. Junqing Zhang; Roger Woods; Marshall, "AN EFFECTIVE KEY GENERATION SYSTEM USING IMPROVED CHANNEL Junqing Zhang Roger Woods Trung Q . Duong ECIT , Queen ' s University Belfast Department of Electrical Engineering and Electronics , University of Liverpool Email : Alan.Marshall@liverpool.ac.uk," pp. 1727–1731, 2015.

[34] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, Mar. 2008. [Online]. Available: http://dx.doi.org/10.1137/060651380

[35] G. Brassard and L. Salvail, *Secret-Key Reconciliation by Public Discussion*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 410–423.

[36] J. Zhang, S. K. Kasera, and N. Patwari, "Mobility assisted secret key generation using wireless link signatures," in *Proceedings of the 29th Conference on Information Communications*, ser. INFOCOM'10. Piscataway, NJ, USA: IEEE Press, 2010, pp. 261–265. [Online]. Available: http://dl.acm.org/citation.cfm?id=1833515.1833568

[37] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Transactions on Antennas and Propagation*, vol. 53, no. 11, pp. 3776–3784, Nov 2005.

[38] R. Impagliazzo, L. A. Levin, and M. Luby, "Pseudo-random generation from one-way functions," in *Proceedings of the Twenty-first Annual ACM Symposium on Theory of Computing*, ser. STOC '89. New York, NY, USA: ACM, 1989, pp. 12–24. [Online]. Available: http://doi.acm.org/10.1145/73007.73009

[39] Y. E. H. Shehadeh and D. Hogrefe, "An optimal guard-intervals based mechanism for key generation from multipath wireless channels," in *2011 4th IFIP International Conference on New Technologies, Mobility and Security*, Feb 2011, pp. 1–5.

[40] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *2011 Proceedings IEEE INFOCOM*, April 2011, pp. 1422–1430.

[41] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, ser. MobiCom '08. New York, NY, USA: ACM, 2008, pp. 128–139. [Online]. Available: http://doi.acm.org/10.1145/1409944.1409960

[42] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *2010 Proceedings IEEE INFOCOM*, March 2010, pp. 1–9.

[43] A. Kitaura, H. Iwai, and H. Sasaoka, "A scheme of secret key agreement based on received signal strength variation by antenna switching in land mobile radio," *International Conference on Advanced Communication Technology, ICACT*, vol. 3, pp. 1763–1767, 2007.

[44] M. A. Tope and J. C. McEachen, "Unconditionally secure communications over fading channels," in *2001 MILCOM Proceedings Communications for Network-Centric Operations: Creating the Information Force (Cat. No.01CH37277)*, vol. 1, 2001, pp. 54–58 vol.1.

[45] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proceedings of the 15th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '09. New York, NY, USA: ACM, 2009, pp. 321–332. [Online]. Available: http://0-doi.acm.org.brum.beds.ac.uk/10.1145/1614320.1614356

[46] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Transactions on Mobile Computing*, vol. 12, no. 5, pp. 917–930, May 2013.

[47] D. S. Karas, G. K. Karagiannidis, and R. Schobert, "Neural Network Based PRY-Layer Key Exchange," pp. 1233–1238, 2011.

[48] J. Croft, N. Patwari, and S. K. Kasera, "Robust uncorrelated bit extraction methodologies for wireless sensors," *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks - IPSN '10*, p. 70, 2010. [Online]. Available: http://portal.acm.org/citation.cfm?doid=1791212.1791222

[49] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Transactions on Antennas and Propagation*, vol. 53, no. 11, pp. 3776–3784, 2005.

[50] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, *Handbook of Applied Cryptography*, 1st ed. Boca Raton, FL, USA: CRC Press, Inc., 1996.

[51] L. E. Bassham, III, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, N. A. Heckert, J. F. Dray, and S. Vo, "Sp 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications," Gaithersburg, MD, United States, Tech. Rep., 2010.

[52] J. G. Proakis, *Digital Communications*. McGraw-Hill, 1995.

[53] P. Hirschausen, L. M. Davis, D. Haley, K. Lever, L. Davis, D. Haley, and K. Lever, "Identifying Key Design Parameters for Monte Carlo Simulation of Doppler Spread Channels," pp. 33–38, 2014.

[54] P. Hoeher, "A Statistical Discrete-Time Model for the WSSUS Multipath Channel," *IEEE Transactions on Vehicular Technology*, vol. 41, no. 4, pp. 461–468, 1992.

[55] P. Karadimas, E. D. Vagenas, and S. A. Kotsopoulos, "On the scatterers' mobility and second order statistics of narrowband fixed outdoor wireless channels," *IEEE Transactions on Wireless Communications*, vol. 9, no. 7, pp. 2119–2124, 2010.