Adaptive and optimum secret key establishment for vehicular communications and sensing

***Abstract*—Confidentiality is a major concern in any wireless communication, especially so in vehicular networks where cyber-attacks easily evolve in the loss of human lives or assets. In these scenarios, the current proposed approach relies on public-key cryptography which, however, requires significant computational capabilities for the encryption/decryption process and large bandwidth for keys distribution. To overcome these limitations, physical-layer security has been proposed to provide confidentiality by exploiting the physical characteristics of the wireless medium. Nonetheless, the high dynamicity and heterogeneity of vehicular environments require the design of secure protocols that are able to self-configure and adapt to all conditions, free from any fixed choice of parameters. In this paper, we propose a secure scheme composed by a novel quantisation approach in which thresholds are analytically derived from the statistics of the channel, mathematically guaranteeing the robustness of the protocol. Moreover, we design an optimisation engine to continuously adapt the system to run in its optimal conditions. The performance of the proposed scheme is evaluated through extensive simulation in order to demonstrate its significant improvement to the existing approach.**

***Index Terms*—Physical layer security, Lossy quantisation, VANETs, Channel Reciprocity Adaptation, RSS**

I. Introduction

Wireless communication technologies provide the essential scalability required by the continuous increase of interconnected devices. In the case of Intelligent Transport Systems (ITS), electrical engineering together with computer science as well as, transport engineering and communication networks synergistically collaborate to improve transport safety and quality. ITS services span across different areas, as in the Advanced Traveller Information System, which provides drivers with real-time route information and the Advanced Transportation Management System that coordinates traffic control devices. Nonetheless, the most anticipated ITS applications arise from vehicle-infrastructure and vehicle-vehicle integrations. These applications rely on the collaboration between vehicles and road infrastructure and hence becomes the key factor in reducing the risk of accidents and environmental impact. A typical vehicle ad-hoc network (VANET) includes on-board units (OBUs) and road-side units (RSUs) which communicate through dedicated short-range communication (DSRC). Security is the first priority [1], [2] as the wireless medium opens up the possibility for unauthorised users to passively eavesdrop and/or to alter the transmissions [3]. Data confidentiality is traditionally provided by cryptographic mechanisms implemented in upper layers of the Open System Interconnection (OSI) model. Encryption approaches can be classified in two categories: symmetric (secret key) and asymmetric (public key) solutions [4].

The present security proposal is based on public-key infrastructure (PKI) to provide authentication, confidentiality, identity and non-repudiation. PKI cryptographic primitives are computationally complex and OBUs may still need hundreds of milliseconds to complete such operations, responsible for unacceptable delays when transmitting safety-related messages [5]. Furthermore, PKI is intrinsically a centralised approach where a trusted authority distributes and manages keys and certificates however, its adaptation to highly distributed and ad-hoc network rises scalability challenges [6]. On the other hand, symmetric cryptography is more power/computational efficient than PKI but its applications are drastically limited by the delicate tasks of distributing and storing the secret keys. Distribution usually requires a secondary secure channel which is hardly feasible, especially in VANETs due to their highly dynamic topology.

In these challenging scenarios, Physical Layer Security (PLS) has emerged as a technique to provide unconditionally secure communications by efficiently exploiting the wireless medium [7] as a shared source of randomness to extract symmetric keys. Randomness is a consequence of the unpredictability of the multipath phenomena [8], where the received wireless signal is altered by the superposition of different transmitted echoes, coming from different paths with different phases. Keys are generated through the quantisation of channel properties, which are considered stochastic processes, such as the Received Signal Strength (RSS) or the phase [9]. Keys distribution is avoided by channel reciprocity principle, which states that in sufficiently small-time intervals, referred to as coherence intervals, the Channel Impulse Response (CIR) is substantially constant [10]. This way, the communicating parties can probe the channel in an interleaved fashion, obtaining similar estimates inside the same intervals and therefore, generating the same keys. Nonetheless, estimates gathered by third entities are statistically uncorrelated due to spatial and time variability of multipath phenomena, leading to different useless keys and providing confidentiality to the communication.

In the PLS process, quantisation plays a crucial role since its performance greatly affects the overall system efficiency and robustness. Quantisation not only does it transform an analogous physical quantity in a stream of discrete numbers, but it also reduces differences among estimates taken by the legitimate parties, even in the same coherence interval. These variations are caused by hardware differences, asymmetric noise and mainly, by the half-duplex nature of wireless de-

vices, unable to receive and transmit at the same time [11]. All these effects are included in the term imperfect reciprocity. Even a single different bit makes the generated keys unusable, nullifying all efforts in the extraction process.

Another aspect to be taken into account is the entropy (H) of the extracted sequences, which measures their level of randomness [12]. The latter is a crucial property of cryptographic keys to remove possible statistical defects that could ease the attacks conducted by adversaries with active or passive presence to the channel [13].

What makes the design of PLS-protocols challenging, is the conflicting relationship among the throughput of the quantisation (bit-generation rate or BGR), the inevitable presence of erroneous bits (bit-mismatch rate or BMR) and the entropy of the resulting streams. In their attempt to optimise the corresponding proposed schemes, most literature sources address only a subset of the metrics introduced above, coming up with resulting in sub-optimal results [9].

Only few protocols in literature take the imperfect reciprocity into account [14], [15], [16] considered as a constant aspect of the environment. In other the studies [17], [18] non-reciprocity is simply ignored during quantisation and fully tackled in the error correction stage. Furthermore, to the best of our knowledge, there isn't a scheme which considers a continuously varying reciprocity due to changing environmental conditions and dynamic network topology. To fill these gaps, to the best of our knowledge, for the first time in the existing literature:

1) We prove the existence of optimal thresholding strategies within a two-level RSS-based quantisation block, which strike an optimal balance among the evaluation metrics (BGR, BMR and H). Moreover, thresholds are not fixed system parameters but continuously derived by the channel's statistics. Specifically, we introduce the use of the Cumulative Distribution Function (CDF) and Average Fade Duration (AFD) to mathematically create equiprobable regions. This way, our scheme outperforms the classical implementation proposed in [19], providing the minimum BMR, the maximum BGR and the maximum key entropy H.
2) We address the continuously varying reciprocity of the channel with the introduction of a novel Perturb & Observe algorithm. In a two-steps approach, we first unify BMR and BGR under a criterion named as secret-bit generation rate (SBGR) that accounts for the number of correct bits per channel sample hence, representing an efficient comparator for different quantisation schemes. Secondly, we design and develop the algorithm acting as a feedback in the key-extraction process. This algorithm is self-configurable and able to adapt to sharp changes in the channel and reciprocity parameters, while continuously observing the SBGR performance to adjust quantisation thresholds accordingly.

The remaining part of this paper is organised as follows: Section II reviews existing studies on PLS in vehicle-to-vehicle communication, focusing on RSS quantisation schemes. Section III introduces the V2V channel model and the quantisation performance metrics; Section IV explains the novel techniques of analytical thresholding, introducing and underlying the proposed optimisation algorithm. Section V compares and contrasts the simulations' results with the standard level-crossing method (hereinafter referred to as STD) [19]. Finally, Section VI draws the conclusions of the present piece of research.

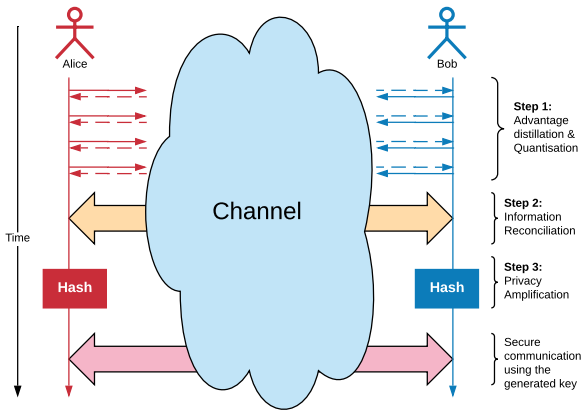

Fig. 1. PLS Key extraction process: Alice and Bob exchange probes in order to agree on a key.

II. Related Works

The research branch on PLS started with Wyner [20] who showed how it is possible to establish secure transmissions in scenarios where the eavesdropper (Eve) has a lower quality channel available than the communicating nodes (Alice and Bob). This difference of links' quality translates into a difference of channel capacities, referred to as secrecy capacity, which can be exploited to send private information. Maurer [21] and Ahlswede-Csiszar [22] demonstrated that confidentiality is also achievable when the attacker observes a higher quality link than the one available to authorised parties. Their technique is based on the extraction of a secret key over the public and insecure channel.

The key extraction process is shown in figure 1 and composed by three fundamental steps: advantage-distillation, information reconciliation and privacy amplification. In the first phase, legitimate parties probe the channel, in order to acquire a number of estimates proportional to the desired key-length. To collect correlated measurements, Alice and Bob must sense the medium inside the same coherence time, defined as the time period over which the channel impulse response is considered constant. Coherence time depends on the Doppler effects due to nodes mobility [8]. Extracted estimates are then converted into bit-streams through quantisation and sent to the information reconciliation phase. The latter has the duty to fix any bit disagreements with the aid of error correcting codes and public discussion through the insecure channel. A widely used technique is CASCADE [23] in which parties randomly

permute the sequences and recursively exchange parity check information. More sophisticated schemes are based on turbo codes [17] and low-density parity check (LDPC) [24] which both try to maximise reconciliation capabilities as well as, simultaneously minimise the leakage of information to the eavesdropper. Alice and Bob's sequences should now be identical, otherwise the entire extraction process is restarted. However, to use such strings as keys, the last step of privacy amplification strengthens them by improving their entropy, as for example with the application of universal hash functions and/or one-way functions [25].

This investigation focuses on the RSS quantisation for its ease of use and the immediate availability in all out-of-the-shelf wireless devices [26]. Furthermore, RSS greatly benefits from nodes' mobility, the main property of VANETs, generating keys at a fast rate and with high entropy. In their pioneer study [27], Tope et al. analysed the signal attenuation by collecting estimates of the envelope of received packets and storing them into arrays. By subtracting half of the latter from the other half, the scheme removed the path-loss contribution, which is correlated to distance and hence predicable. Two thresholds were used to drop estimates that have a high probability of being either foreseeable or converted to mismatching bits. Azimi-Sadjadi et al. [28] proposed the use of deep fades or local minima of the signal to improve keys agreement. Deep fades were detected by first quantising RSS estimates, using a single threshold and then by searching for runs of 1-bits of sufficient length. At this point, Alice can transmit the hash of the generated key to Bob, who compensates any disagreements by exploring a small search-space due to deep fades' statistical properties. Inspired by the previous idea, Mathur et al. [19] introduced a quantiser with two thresholds, whose distance is proportional to the standard deviation of an array of estimates. The quantisation bin between thresholds is referred to as censor or invalid region, where values are dropped because of their high probability of disagreement. Furthermore, only the estimates located inside sequences of sufficient excursions above or below the thresholds are considered to discard sharp changes in the signal amplitude. This constraint has been relaxed in a few derived works [17], [29], [30], where the increased error probability was counterbalanced by a more efficient reconciliation technique. Instead of using absolute thresholds, the research [31] proposed a differential approach where quantisation operates on the difference between two consecutive RSS values. This way, the scheme is able to provide better results, while being resistant to RSS-manipulation attacks. Since increasing the number of quantisation levels could have a negative impact on BMR, the study [32] introduced the use of vector quantisation to increase BGR. In the latter, RSS estimates are reused n times, where n is the dimension of the vector. While this approach could achieve better BGR without increasing BMR, it remains to investigate the security aspects related to the estimates' recycling. VANETs communication constraints have been considered in [33], where the authors designed a key-length optimisation algorithm. Starting from the characteristics of the specific scenario, such as the location of the parties and an estimate of the coherence time, the algorithm attempts to extract a key with as much robustness as possible.

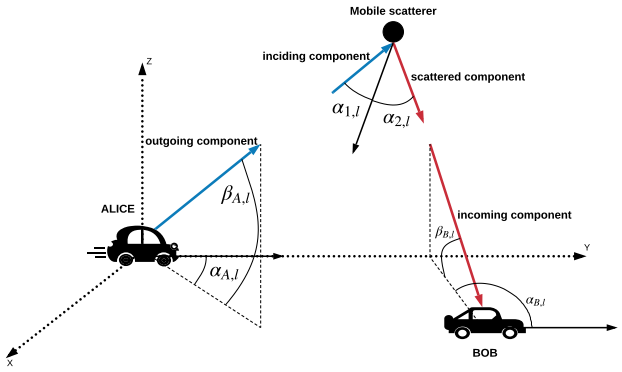

Fig. 2. V2V channel model: two vehicles are moving in a three-dimensional environment including mobile scatterers.

Only few protocols in literature take the imperfect reciprocity into account. Half-duplex limitations are addressed in [14], [15] by applying fractional interpolation in order to virtually measure estimates at the same time instants. Moreover, non-reciprocity due to hardware differences are removed with a ranking method in [16]. In [34] noise is reduced by smoothing the readings, using sliding windows whose weights are collaboratively generated by Alice and Bob.

III. Channel Model and Performance Metrics

The high dynamicity of VANETs constantly changes the physical characteristics of the wireless media. In fact, the multipath phenomena induce a time-variant impulse response, the receiver to collect a train of echoes of the transmitted message, which travels different paths and arrives at the destination with different delays and attenuation factors [8]. Just as the mobility of vehicles and intermediate objects appear to be unpredictable, so are the multipath effects on the received signals. In deterministic channel models, the propagation environment is recreated through ray-tracing techniques [35]. Nonetheless, a detailed description of both objects' specific coordinates and electrical characteristics is crucial to achieve accurate results, rendering this approach hardly generalisable to all possible operating conditions. On the other hand, stochastic models consider the wireless medium as a random process, whose statistics provide an inner sight of the channel properties [36]. Moreover, random approaches provide numerical stability and combine high performances and ease of implementation. For these reasons, in the current investigation we opted to use a generic stochastic model [37], which proved to be a complete, configurable and tuneable model for key-generation.

A. V2V generic stochastic model

Figure 2 shows the considered three-dimensional V2V scenario, where propagation's parameters and entities' locations are driven by a Monte Carlo process [38], [39]. Two vehicles,

Alice and Bob, are equipped with a single antenna and move at speeds $u_{A(B)}$. Alice's signals are received by Bob as the superposition of a number L of different echoes, unresolvable in delay. Each l-th multipath component reaches its destination with a specific complex amplitude a_l and phase ϕ_l caused by the different path it has travelled. To adequately approximate a trafficked urban scenario, we also considered the interaction with mobile scatterers moving at speed u_S [37].

In this environment, Alice's channel estimates G_A are generated by the following formula [37]:

$$G_A(t) = \sum_{l=1}^{L} |a_l| exp(j\phi_l) exp(j2\pi v_l t) \tag{1}$$

where t is the time and v_l the Doppler shift of the l-th multipath component. The latter is the sum of the contributions of the transmitter $v_{A,l}$, receiver $v_{B,l}$ and scatterers $v_{S,l}$, as follows:

$$v_l = v_{A,l} + v_{B,l} + v_{S,l} \tag{2}$$

$$v_{A(B),l} = v_{A(B)_{max}} \cos\alpha_{A(B),l} \cos\beta_{A(B),l} \tag{3}$$

$$v_{S,l} = v_{S_{Wb}} (\cos\alpha_{1,l} + \cos\alpha_{2,l}) \tag{4}$$

In the previous equations, $\alpha_{A(B),l}$ and $\beta_{A(B),l}$ are azimuth and elevation angles of departure (arrival) and $\alpha_{1,l}, \alpha_{2,l}$ correspond to the incoming and outcoming components at the mobile scatterer. Maximum Doppler shifts $v_{A(B)_{max}}$ arise from nodes' mobility, hence

$$v_{A(B)_{max}} = \frac{u_{A(B)_{max}}}{\lambda} = u_{A(B)_{max}} \cdot f_c/c \tag{5}$$

$$v_{S_{Wb}} = \frac{u_{S_{Wb}}}{\lambda} = u_{S_{Wb}} \cdot f_c/c \tag{6}$$

where $u_{A(B)_{max}}$ are the corresponding maximum velocities, λ is the carrier's wavelength at frequency f_c and c is the speed of light. The speed of mobile scatterers $v_{S_{Wb}}$ is randomised through a Weibull distribution, in order to adequately associate most multipath power contribution to static and slowly moving objects [37] thus,

$$p_{u_S}(u_{S_{Wb}}) = w_{Wb} u_{S_{max}}^{a_{Wb}^{-1}} \exp(-w_{Wb} u_{s_{max}}^{a_{Wb}} / a_{Wb}) \tag{7}$$

having scale w_{Wb} and shape a_{Wb}. Once we have Alice's estimates we need to properly generate the corresponding Bob's values in order to realistically simulate the effects of imperfect reciprocity. This loss of correlation is the direct consequence of slightly different channel state information (CSI) sensed by legitimate parties. According to the study [40], that difference is composed by a stable component and a noisy part, which are estimated after a non-reciprocity learning phase of M probes extracted from the same coherence intervals thus,

$$\mu_t = \frac{1}{M} \sum_{i=1}^{M} (G_{A,i}(t) - G_{B,i}(t)) \tag{8}$$

$$\sigma_C^2 = \frac{1}{M} \sum_{i=1}^{M} (G_{A,i}(t) - G_{B,i}(t) - \mu_t)^2 \tag{9}$$

The stable portion μ_t is removed by the Channel Gain Complement (CGC) method, leaving only the noisy component which is assumed to follow a zero-mean Gaussian distribution, thus $N(0, \sigma_C^2)$. Bob's values can now be obtained adding a normal random variable to Alice's estimates as follows: [40]:

$$G_B(t) = G_A(t) + N(0, \sigma_C^2) \tag{10}$$

The impact of the noisy component usually depends on the environmental conditions, which are dynamic and unpredictable, especially in VANETs. In this respect, our proposed algorithm aims to rapidly adapt quantisation thresholds to the available amount of channel reciprocity, modelled as a continuously changing standard deviation σ_C.

B. Key performance metrics

In order to compare the proposed algorithm to the other schemes in literature, it is necessary to introduce the performance metrics [41]. The quantisation performance is measured by the bit generation rate (BGR), which is the average number of bits that can be extracted per channel estimate or per unit time. The former definition is preferable, as it does not depend on the chosen probing rate. Thus

$$BGR = \frac{no.extracted\,bits}{no.channel\,samples} \tag{11}$$

Higher value of BGR indicates a faster production of bitstreams which, in turn, translates to keys being generated in less time and hence refreshed continuously.

Another relevant performance criterion is the bit-mismatch rate (BMR) defined as the ratio of the number of erroneous bits (i.e. they don't match between Alice and Bob) to the total amount of extracted bits

$$BMR = \frac{no.erroneous\,bits}{no.channel\,samples} \tag{12}$$

BMR determines the system resilience against noise and interferences, defined after the quantisation stage or after the information reconciliation. In the first case, BMR depends only on how the quantisation space is configured (as for example the number of thresholds). On the other hand, if BMR is defined after information reconciliation, it will also embrace the error-correcting capabilities of the protocol, having the unrecoverable bits at the numerator. As our thresholding optimisation engine aims to increase the number of valid keys, it is reasonable to define BMR after reconciliation, taking advantage of any implementation of the latter.

Considering that the extracted sequences will be treated as cryptographic keys, it is important they possess enough entropy, ideally close to 1, to maximise the uncertainty from an attacker's point of view. Entropy of bit i is measured by the following formula [17]:

$$H_i = -p_{0,i} \log p_{0,i} - (1 - p_{0,i}) \log(1 - p_{0,i}) \quad (13)$$

where $p_{0,i}$ is the posterior probability of bit i being 0. The maximum value of 1 indicates equal probability of having bits 1 or 0, i.e. $p_0 = 1 - p_0 = 0.5$. For independent bit-strings of length N, the total entropy is defined as $H_{total} = (\sum_{i=1}^{N} H_i)/N$. Entropy alone is not sufficient to prove the absence of statistical defects in the bit sequences. For example, they may contain long runs of the same bit and the repetition of sub-parts. For these reasons, in all our tests we also evaluate key robustness against the random-tests suite, provided by the National Institute of Standards and Technology (NIST) [13].

IV. Analytical Quantisation Thresholding

Our secret-key extraction algorithm follows from work introduced in [19], where legitimate nodes locally convert their RSS-estimates in bit-streams, prior to symmetric key generation. Channel probing is done in half-duplex mode, hence Alice and Bob extract samples from the same coherence intervals in an interleaved fashion. The inability to probe at the same time instants introduces a small, yet unpredictable variation in the channel response. The latter, together with other environmental factors, reduce the channel reciprocity as well as, increase the probability of extracting different key-candidates thus, they reduce the effectiveness of the extraction process. In order to reduce BMR, we apply a two-level "censor" quantisation function defined as follows:

$$Q(x) = \begin{cases} 1, & \text{if } x > q_+ \\ 0, & \text{if } x < q_- \\ \text{dropped} & \text{otherwise} \end{cases} \quad (14)$$

Estimates in the interval $q_- \leq x \leq q_+$ are dropped in accordance with their higher probability of being translated into different bits at both communication ends. On the other hand, the censor region has a direct impact of the throughput of the quantisation stage and its size should be set as the optimal trade-off between BMR and BGR metrics. In STD thresholds were originally computed using average and standard deviation of an array of samples $\underline{h}$, thus

$$q_\pm = average(\underline{h}) \pm \alpha_{STD} \cdot stdev(\underline{h}) \quad (15)$$

where parameter α_{STD} expresses the relationship between the censor region and how spread out the values are and is set empirically. To compare STD with our proposed methods we define a novel metric, namely the secret-bit generation rate (SBGR), as the ratio of the number of bits which are successfully used to compose keys to the total amount of channel samples that were used, thus

$$SBGR = \frac{no.keybits}{no.channel\ samples} \quad (16)$$

Remembering that BMR is defined after information reconciliation, the number of keybits corresponds to the amount of successfully generated bits after errors correction, which can be expressed as

$$no.keybits \leq no.samples \cdot BGR \cdot (1 - BMR) \quad (17)$$

where the less-than-equal symbol arises from the fact that a single erroneous bit eventually compromises an entire key. By merging equations 16 and 17

$$SBGR \leq BGR \cdot (1 - BMR) \quad (18)$$

Equation 18 elicits how the new metric embraces both the effects of BGR and BMR. Moreover, SBGR is evaluated after errors correction, making the optimisation engine capable of taking advantage of any existing or future reconciliation schemes. Figure 3 shows SBGR against different invalid region sizes modelled through the parameter α_{STD} in e.q. 15 and for different non-reciprocity settings, represented by standard deviation σ_C in e.q. 9. SBGR performance increases as channel non-reciprocity (σ_C) reduces. Simulation parameters are shown in table I.

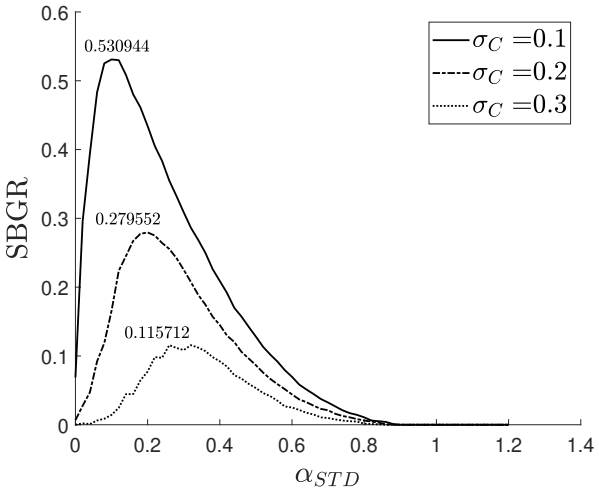

Fig. 3. SBGR against α_{STD} for different non-reciprocity factors in the standard censor approach.

Given the fact that all curves express a single (global) maximum, a Hill-climbing algorithm seems to be a simple, yet effective approach to locate the point with highest performance. The idea is to 'modulate' the quantisation thresholds, according to the resulting SBGR, in an attempt to identify the optimal set-point. However, as stated in the introduction, a high entropy H of the generated bit-streams is a mandatory requirement to guarantee the statistical robustness of the resulting symmetric keys. As this aspect is not covered by the definition of SBGR, we decided to mathematically relate the thresholds to ensure the maximum entropy.

A. CDF-based thresholding strategy

The first proposed strategy is based on the cumulative distribution function (CDF) $F_X(\cdot)$. In the case of two-level

quantisation, optimal key-entropy is guaranteed by forcing thresholds $q_{\pm}$ to generate equiprobable regions, thus

$$F_X(q_-) = Pr(-\infty < x \leq q_-) \\ = Pr(q_+ \leq x < +\infty) = 1 - F_X(q_+) \quad (19)$$

In the absence of a significant line-of-sight (LOS) component, Rayleigh distribution has proved to model channel propagation adequately [37]. Rayleigh's CDF is defined as follows:

$$F_X(x) = 1 - \exp(-\frac{x^2}{2\sigma^2}) \quad (20)$$

By merging 19-20

$$F_X(q_-) = 1 - \exp(-\frac{q_-^2}{2\sigma^2}) \\ = \exp(-\frac{q_+^2}{2\sigma^2}) = 1 - F_X(q_+) \quad (21)$$

where upper threshold q_+ can be derived by applying the logarithm to the reciprocal of the first side (due to the minus sign inside the second exponential) and extracting the square root, thus

$$q_+ = \sqrt{2}\sigma \sqrt{\log\left(\frac{1}{1 - \exp(-\frac{q_-^2}{2\sigma^2})}\right)} \quad (22)$$

B. ADF-based thresholding strategy

The second proposed method is based on the use of average fade duration (AFD), a second-order statistical parameter, which should better capture channel variabilities and simultaneously maintain a sufficient level of key robustness. AFD is defined as

$$T(z) = F_X(z)/N(z) \quad (23)$$

that is, the ratio between the cumulative distribution function $F_X(\cdot)$ and the level crossing rate (LCR) $N(\cdot)$. In Rayleigh environments LCR is expressed by the following formula [37]

$$N(z) = \sqrt{\frac{d_1}{2\pi}} \exp(-\frac{z^2}{2\sigma^2}) \frac{z}{\sigma^2} \quad (24)$$

where parameter d_1 depends on vehicles' speeds and multipath angular spread (see [37] for details). The core concept in this method is to ensure that when a signal crosses a threshold, it will remain in the corresponding region for the same (averaged) time duration. Mathematically,

$$T(q_-) = T^c(q_+) \quad (25)$$

where $T^c(z) = (1 - F_X(z))/N(z)$ is also commonly referred to as connection time. By merging equations 20, 23 and 25

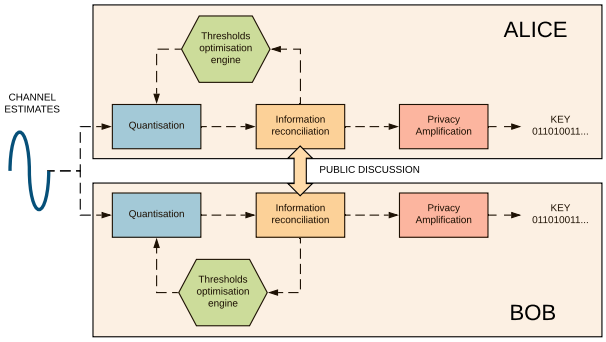

Fig. 4. Thresholds optimisation engine acts as a feedback in PLS key-generation process.

$$T(q_-) = \frac{1 - \exp(-\frac{q_-^2}{2\sigma^2})}{\sqrt{\frac{d_1}{2\pi}} \exp(-\frac{q_-^2}{2\sigma^2}) \frac{q_-}{\sigma^2}} \\ = \frac{\exp(-\frac{q_+^2}{2\sigma^2})}{\sqrt{\frac{d_1}{2\pi}} \exp(-\frac{q_+^2}{2\sigma^2}) \frac{q_+}{\sigma^2}} = T^c(q_+) \quad (26)$$

which, in turns, simplifies to

$$\frac{1 - \exp(-\frac{q_-^2}{2\sigma^2})}{\exp(-\frac{q_-^2}{2\sigma^2}) q_-} = \frac{1}{q_+} \quad (27)$$

Once again, the upper threshold q_+ can be derived from the lower one q_- as follows:

$$q_+ = \frac{q_-}{\exp(-\frac{q_-^2}{2\sigma^2}) - 1} \quad (28)$$

Whenever it is needed to adapt the quantisation thresholds, the two proposed strategies provide an analytic way to derive the invalid region's boundaries, enforcing maximum entropy as well as, preparing the ground for the upcoming SBGR optimisation block.

C. Thresholds Optimisation engine

In this section we introduce an optimisation algorithm in the standard process of key extraction to recognise the maximum SBGR performance of the system without relying on the choice of fixed quantisation parameters. Figure 4 shows that the novel block acts as feedback from the stage information reconciliation to adapt the quantisation parameters by continuously monitoring the output of the key-extraction process. Inside this block, a Perturb & Observe (PO) algorithm constantly alters the invalid region size and monitors the effects on the resulting SBGR. In doing so, PO can adapt to different scenarios, even within the ones with variable channel reciprocity, a common condition holding in VANETs. For the sake of simplicity, the algorithm perturbs the size of the censor region by a positive amount $\delta > 0$, acting on the lower

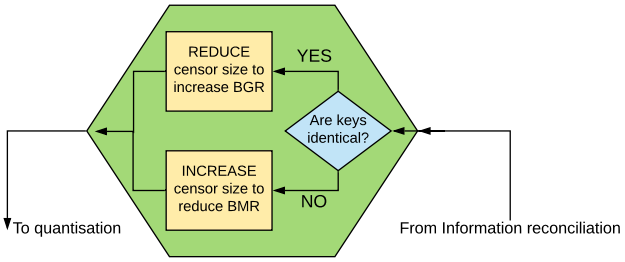

Fig. 5. A simplified view of the optimisation block: reconciliation outcome is used to adapt thresholds distance.

threshold q_- and leaving the corresponding upper threshold q_+ computed accordingly to the chosen strategy (CDF-based or AFD-based). Figure 5 shows the intuitive underlying idea: if the generated bitstreams are different after reconciliation, this indicates a decrease in channel reciprocity, which should be balanced by a larger censor region. On the other hand, matching keys suggest the possibility to reduce thresholds' distance further, thus, aiming for higher BGR.

The frequency with which the system should be perturbed must be carefully chosen: if thresholds are modulated too often, they can generate a significant oscillation around the optimal SBGR, preventing complete convergence. On the other hand, if the algorithm does not calibrate itself fast enough, it may not be able to reach optimality before the medium has moved to a different reciprocity condition. To strike a balance, it seems reasonable to perturb quantisation bins after a minimum number of events. More specifically, the algorithm waits for a number $INT_{SUCCESS}$ of successful keys before reducing the censor size and a number of INT_{FAIL} failed attempts before increasing it. Usually $INT_{FAIL} \leq INT_{SUCCESS}$ because it is safer to faster adapt to worse conditions than to improve already good ones.

Another improvement stems from the consideration that when the algorithm has successfully reached the optimal point, even the smallest positive and negative perturbance would possibly result in a waste of bits or the total rejection of the generated bitstreams. For that reason, the algorithm simultaneously quantifies the channel estimates against three pairs of thresholds $q_\pm^{(1)}, q_\pm^{(2)}, q_\pm^{(3)}$ whose lower parts are spaced by $\delta > 0$, thus

$$q_-^{(1)} = q_-^{(2)} + \delta \tag{29}$$

$$q_-^{(3)} = q_-^{(2)} - \delta \tag{30}$$

Considering that the formulae 22 and 28 are decreasing monotonic functions, the three regions are in the following order relation

$$(q_+^{(1)} - q_-^{(1)}) \leq (q_+^{(2)} - q_-^{(2)}) \leq (q_+^{(3} - q_-^{(3)}) \tag{31}$$

Recalling that smaller regions generate higher BGR as well as higher BMR, we will refer to those pairs hereafter as aggressive thresholds $q_\pm^{(1)}$, neutral thresholds $q_\pm^{(2)}$ and defensive thresholds $q_\pm^{(3)}$ which will be further evaluated in this specific order.

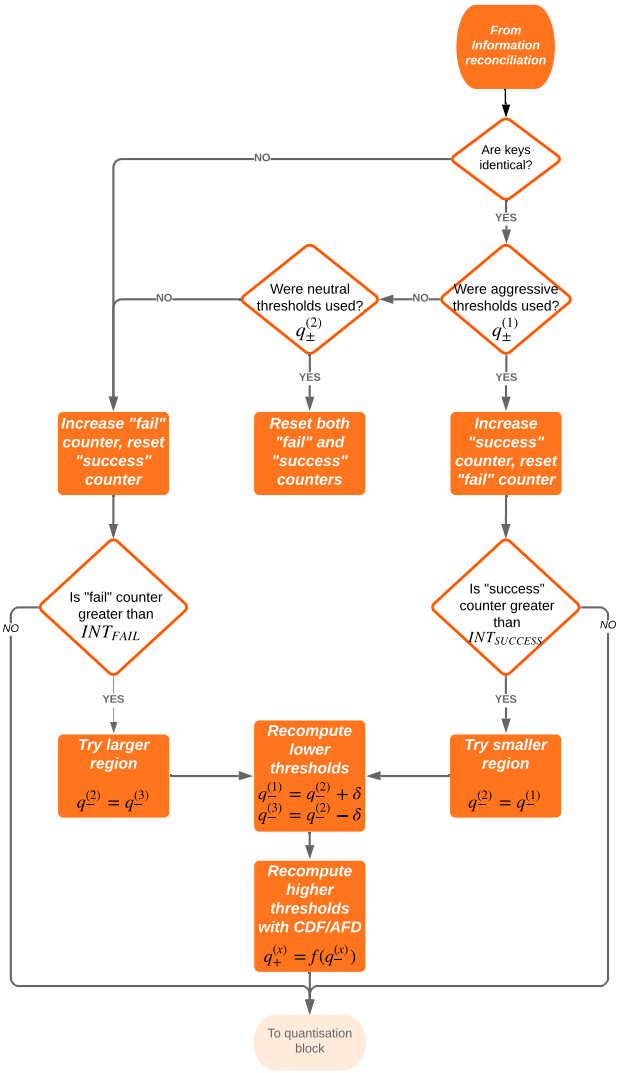

Fig. 6. Flowchart of PO algorithm where quantisation thresholds are adjusted to achieve the maximum key-generation rate.

Figure 6 shows the complete algorithm flowchart, which can be best explained by considering three possible conditions: firstly, the algorithm is using a censor region's size which is larger than the optimal one for the current reciprocity factor, dropping estimates that can be safely transformed into keybits. In that case it is highly probable that aggressive thresholds $q_\pm^{(1)}$ will be adequate to generate keys at a faster rate. If this condition is held for $INT_{SUCCESS}$ times, it is reasonable to consider these thresholds as neutral, assigning $q_\pm^{(2)} = q_\pm^{(1)}$ and recalculating the others according to formulae 29 and 30. Secondly, when the algorithm reaches the maximum and channel reciprocity is stable, it is more likely that neutral thresholds $q_\pm^{(2)}$ will be valid, leaving all parameters unchanged as in

TABLE I
SIMULATION PARAMETERS

Parameter	Value	Description
$DATASIZE$	50000	No. channel estimates
$RUNS$	120	No. test runs
L	20	No. multipaths components
$u_{A(B)_{max}}$	30 m/s	Vehicles max speeds
$u_{S_{max}}$	30 m/s	Scatterers max speed
$\alpha_{A(B),l}$	$\sim U[-\pi, +\pi]$	Azimuth angles
$\beta_{A(B),l}$	$\sim U[0, 1]$	Elevation angles
$\alpha_{1,l}, \alpha_{2,l}$	$\sim U[-\pi, +\pi]$	Scatterers angles
f_c	6 GHz	Carrier frequency
w_{Wb}	2.958	Weibull scale
a_{Wb}	0.428	Weibull shape

the previous attempt, thus avoiding oscillations. Finally, if we assume that the algorithm is using a smaller region concerning the current channel condition, only defensive thresholds are probably valid or else none, suggesting a shift $q_{\pm}^{(2)} = q_{\pm}^{(3)}$ after INT_{FAIL} occurrences.

V. SIMULATIONS

During our tests, every simulation included 50,000 channel estimates, repeated for 120 runs to stabilise the resulting statistics. Furthermore, the number of multipath components was $L = 20$ to recreate a pure diffuse Rayleigh environment, capable of modelling an urban scenario. Since estimates have to collected from uncorrelated different coherence region of duration T_{coh}, we use a fixed maximum probing rate $F_p = 1/T_{coh}$. Other relevant configuration settings are presented in table I.

In a first set of experiments we evaluated the performance of the new thresholding strategies. A standard two-level quantisation scheme [19] with CASCADE has been modified to analytically derive the thresholds using CDF and AFD-based formulae presented in section IV. Figures 7 and 8 show SBGR performances against censor size for different non-reciprocity configurations modelled by standard deviation σ_C. Results are shown in table II where both approaches outperform the standard one in all scenarios, especially with worse reciprocity. Performances are substantially equivalent, where CDF scores slightly better results in correspondence to $\sigma_C = 0.20$ and $\sigma_C = 0.30$, whilst AFD results superior in all other setups. The same table also illustrates how both analytical strategies are able to generate high entropy keys, even in low reciprocity environments ($\sigma_C = 0.30$), where STD fails to do so.

In the second set of experiments, correctness and performance of the Perturb-Observe algorithm have been evaluated through extensive simulation. As the baseline, we introduced a quantisation scheme, referred to as EX-SEARCH, where the thresholds are chosen directly from a lookup table. The latter has been created through exhaustive search, containing the optimal thresholds for various non-reciprocity settings in the range $\sigma_C \in [0.10, 0.30]$. Figure 9 shows PO algorithm's performance against EX-SEARCH. CDF and AFD configurations provide similar results, however, they both outperform EX-SEARCH, emphasising the superiority of our self-configurable

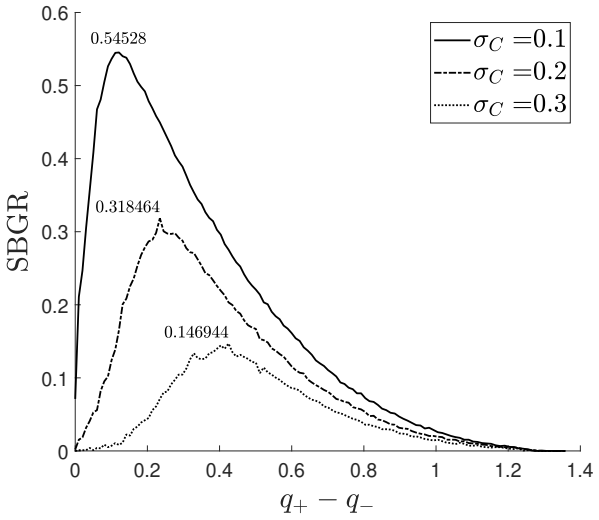

Fig. 7. CDF-thresholding strategy for different non-reciprocity factors.

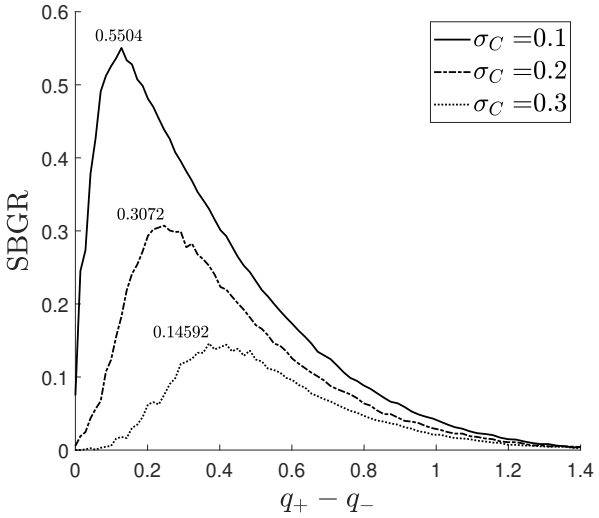

Fig. 8. AFD-thresholding strategy for different non-reciprocity factors.

approach. In fact, these better results are due to PO's ability to adapt and exploit the time intervals, where the random estimates temporally allow for a smaller censor size hence, a higher BGR.

In the last set of experiments, we applied NIST test suite [13] to the bit-streams generated by our algorithm in order to prove the absence of statistical defects. Each test returns a P-value indicating the strength of the evidence against the null hypothesis. More specifically, when the returned P-value is larger than the chosen significance level ($\alpha_{sig} = 0.01$), the sequence can be considered as random. Nonetheless, four tests, namely 'Binary Matrix Rank', 'Overlapping Template Matching', 'Maurers Universal' and 'Linear Complexity', require an extremely long streams, which cannot be provided by this specific simulator and hence they were excluded.

TABLE II
RESULTING SBGR AND ENTROPY OF STD, CDF AND AFD APPROACHES

σ_C	STD		CDF		AFD	
	SBGR	H	SBGR	H	SBGR	H
0.10	0.5309	0.9935	0.5453 (+2.71%)	0.9947	0.5504 (+3.76%)	0.9941
0.15	0.4122	0.9933	0.4188 (+1.60%)	0.9937	0.4270 (+3.59%)	0.9941
0.20	0.2796	0.9934	0.3185 (+13.91%)	0.9940	0.3072 (+9.87%)	0.9932
0.25	0.1946	0.9934	0.2068 (+6.27%)	0.9939	0.2140 (+9.97%)	0.9925
0.30	0.1157	0.5252	0.1469 (+26.97%)	0.9942	0.1423 (+22.99%)	0.9920

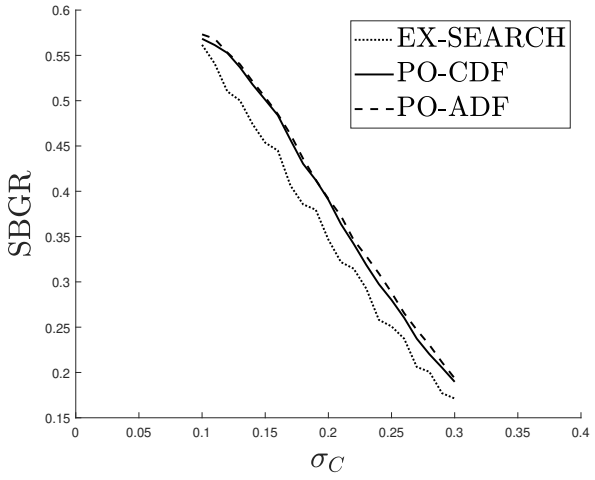

Fig. 9. Performance of Perturb-Observe algorithm compared to exhaustive search .

Table III shows the P-values of the different tests for different reciprocity conditions. CDF has occasionally failed the 'random excursions' tests in case of low channel reciprocity, whilst AFD proved to be always successful. Despite this, both techniques clearly proved to be able to generate random sequences, which can be safety used as cryptographic keys.

VI. CONCLUSIONS

In this paper, we proposed a new analytical method for the generation of quantisation thresholds in the Physical Layer Security extraction process from the channel RSS values. In contrast to the standard level-crossing approach, the presented CDF and AFD techniques guarantee the optimality of the entropy of the resulting keys. Additionally, using these methods we introduced a quantisation optimisation engine as a feedback block in the key generation process. The proposed PO algorithm changes the size of the invalid region and observes the results to identify the maximum point of the SBGR metric, which in turn simultaneously captures both the bit generation rate and the bit mismatch rate. Although the techniques discussed apply to different wireless propagation environments, the use of VANETs in an urban environment has been chosen as the use-case in this work. We implemented a three-dimensional stochastic model of a V2V channel, including the interaction between mobile scatterers as well as, first and second-order statistics.

The results obtained proved that the new approaches can better exploit channel randomness and generate a higher number of keys than the existing standard scheme. More importantly, the PO algorithm is capable of adapting to varying reciprocity conditions, which makes it independent of empirical choices of parameters that often do not behave well in scenarios not previously tested. Robustness of the generated keys was tested evaluating their respective Shannon entropies as well as, against the NIST tests suite. In both cases, the resulting sequences are considered as random thus, being resilient to statistical attacks.

Further research is recommended in the application of the PO algorithm to various deterministic channel models for VANETS in more specific environments. Moreover, it is desirable to investigate other error correction schemes, besides CASCADE, in order to evaluate their positive or negative impacts on SBGR and investigate further the evolution of the proposed adaptive algorithm.

REFERENCES

[1] L. Gafencu, L. Scripcariu, and I. Bogdan, "An overview of security aspects and solutions in vanets," in *2017 International Symposium on Signals, Circuits and Systems (ISSCS)*, 2017, pp. 1–4.

[2] 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://www.sciencedirect.com/science/article/pii/S2214209616301231

[3] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

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

[5] 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.

[6] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," *Computer Networks*, vol. 141, pp. 199 – 221, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128618301208

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

[8] A. Goldsmith, *Wireless Communications*. USA: Cambridge University Press, 2005.

[9] M. Bottarelli, G. Epiphaniou, D. K. B. Ismail, P. Karadimas, and H. Al-Khateeb, "Physical characteristics of wireless communication channels for secret key establishment: A survey of the research," *Computers & Security*, vol. 78, pp. 454 – 476, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404818300841

[10] 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.

TABLE III
RESULTS OF NIST TESTS ON THE PO ALGORITHM WITH CDF AND AFD THRESHOLDING STRATEGIES

Test (128-bit keys)	PO-CDF			PO-AFD		
	$\sigma_C = 0.10$	$\sigma_C = 0.20$	$\sigma_C = 0.30$	$\sigma_C = 0.10$	$\sigma_C = 0.20$	$\sigma_C = 0.30$
monobit	0.7798	0.0736	0.0292	0.4338	0.8230	0.1312
frequency	0.7328	0.5190	0.0336	0.8197	0.9705	0.4008
runs	0.9982	0.9374	0.1211	0.8096	0.3412	0.8604
longest run ones	0.0610	0.6601	0.9287	0.4793	0.6442	0.7589
dft	0.3049	0.7975	0.3049	0.7975	0.4416	0.6079
non overlapping template matching	0.9996	0.9931	0.8218	0.9935	0.9373	0.5865
serial	0.4731	0.5528	0.0321	0.2649	0.5620	0.2867
approximate entropy	0.5468	0.5719	0.0326	0.6215	0.8187	0.2970
cumulative sums	0.8982	0.0471	0.0113	0.5492	0.7797	0.1075
random excursions	0.0158	0.0001	0.0018	0.0238	0.0957	0.0445
random excursions variant	0.0514	0.0005	0.1597	0.0593	0.0156	0.1991

[11] IEEE Computer Society, "IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007)*, pp. 1–2793, 2012.

[12] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/j.1538-7305.1948.tb01338.x

[13] A. Rukhin, J. Sota, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications."

[14] 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, 2010.

[15] Hongbo Liu, Jie Yang, Yan Wang, and Yingying Chen, "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks," in *2012 Proceedings IEEE INFOCOM*, 2012, pp. 927–935.

[16] J. Croft, N. Patwari, and S. K. Kasera, "Robust uncorrelated bit extraction methodologies for wireless sensors," in *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks*, ser. IPSN '10. New York, NY, USA: Association for Computing Machinery, 2010, p. 70–81. [Online]. Available: https://doi.org/10.1145/1791212.1791222

[17] G. Epiphaniou, P. Karadimas, D. Kbaier Ben Ismail, H. Al-Khateeb, A. Dehghantanha, and K. R. Choo, "Nonreciprocity compensation combined with turbo codes for secret key generation in vehicular ad hoc social iot networks," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2496–2505, 2018.

[18] S. Baksi, J. Snoap, and D. C. Popescu, "Secret key generation using one-bit quantized channel state information," in *2017 IEEE Wireless Communications and Networking Conference (WCNC)*, 2017, pp. 1–6.

[19] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Securing Wireless Communications at the Physical Layer," pp. 201–230, 2009.

[20] A. D. Wyner, "The Wire-Tap Channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, oct 1975.

[21] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, may 1993.

[22] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, jul 1993.

[23] G. Brassard and L. Salvail, "Secret-Key Reconciliation by Public Discussion," in *Advances in Cryptology — EUROCRYPT '93*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 410–423.

[24] S. Baksi, J. Snoap, and D. C. Popescu, "Secret Key Generation Using One-Bit Quantized Channel State Information," in *2017 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, mar 2017, pp. 1–6.

[25] 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

[26] 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, p. 332–341, Jan. 2015. [Online]. Available: https://doi.org/10.1002/sec.973

[27] M. Tope and J. 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. IEEE, 2001, pp. 54–58.

[28] 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 - CCS '07*. New York, New York, USA: ACM Press, 2007, p. 401.

[29] M. Yuliana, Wirawan, and Suwadi, "Performance evaluation of the key extraction schemes in wireless indoor environment," in *2017 International Conference on Signals and Systems (ICSigSys)*. IEEE, may 2017, pp. 138–144.

[30] 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 - MobiCom '09*. New York, New York, USA: ACM Press, 2009, p. 321.

[31] 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.

[32] X. Li, J. Liu, Q. Yao, and J. Ma, "Efficient and Consistent Key Extraction Based on Received Signal Strength for Vehicular Ad Hoc Networks," *IEEE Access*, vol. 5, pp. 5281–5291, 2017.

[33] J. Wan, A. Lopez, and M. A. A. Faruque, "Physical Layer Key Generation: Securing Wireless Communication in Automotive Cyber-Physical Systems," *ACM Transactions on Cyber-Physical Systems*, vol. 3, no. 2, pp. 1–26, 2018.

[34] X. Zhu, F. Xu, E. Novak, C. C. Tan, Q. Li, and G. Chen, "Extracting Secret Key from Wireless Link Dynamics in Vehicular Environments," *2013 Proceedings IEEE INFOCOM*, pp. 2283–2291, 2013.

[35] J. Maurer, T. Fugen, T. Schafer, and W. Wiesbeck, "A new inter-vehicle communications (ivc) channel model," in *IEEE 60th Vehicular Technology Conference, 2004. VTC2004-Fall. 2004*, vol. 1, 2004, pp. 9–13 Vol. 1.

[36] G. Matz and F. Hlawatsch, "Chapter 1 - fundamentals of time-varying communication channels," in *Wireless Communications Over Rapidly Time-Varying Channels*, F. Hlawatsch and G. Matz, Eds. Oxford: Academic Press, 2011, pp. 1 – 63. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780123744838000017

[37] 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

[38] 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.

[39] 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.

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

[41] T. Wang, Y. Liu, and A. V. Vasilakos, "Survey on channel reciprocity based key establishment techniques for wireless systems," *Wirel. Netw.*, vol. 21, no. 6, p. 1835–1846, Aug. 2015. [Online]. Available: https://doi.org/10.1007/s11276-014-0841-8