Non-Reciprocity Compensation Combined with Turbo Codes for Secret Key Generation in Vehicular Ad Hoc Social IoT Networks

Gregory Epiphaniou, *Member, IEEE* Petros Karadimas, *Member, IEEE* Dhouha Kbaier Ben Ismail, Haider Al-Khateeb, Ali Dehghantanha, *Senior Member, IEEE* Kim-Kwang Raymond Choo, *Senior Member, IEEE*

Abstract—The physical attributes of the dynamic vehicle-to-vehicle (V2V) propagation channel can be utilised for the generation of highly random and symmetric cryptographic keys. However, in a physical-layer key agreement scheme, non-reciprocity due to inherent channel noise and hardware impairments can propagate bit disagreements. This has to be addressed prior to the symmetric key generation which is inherently important in social Internet of Things (IoT) networks, including in adversarial settings (e.g. battlefields). In this paper, we parametrically incorporate temporal variability attributes, such as three-dimensional (3D) scattering and scatterers' mobility. Accordingly, this is the first work to incorporate such features into the key generation process by combining non-reciprocity compensation with turbo codes. Preliminary results indicate a significant improvement when using Turbo Codes in bit mismatch rate (BMR) and key generation rate (KGR) in comparison to sample indexing techniques.

Index Terms—Turbo codes, Social IoT Networks, Secret Bit Extraction, Key Generation Rate, Internet of Military Things, Internet of Battlefield Things.

1 Introduction

Conventional cryptographic solutions in wireless communications generate shared secrets using pre-computational techniques or asymmetric cryptographic protocols [1]. However, the challenges of generating such secret keys are compounded due to other competing requirements such as energy efficiency, and the need to minimize computational complexity and processing-communication overhead, particularly in autonomous communication of Internet of Things (IoT) nodes and social IoT networks [2]. In recent literature, there have been efforts to extend data sharing for different types of traffic in vehicle-to-vehicle (V2V) communications, in both civilian and military context (e.g. Internet of Military Things and Internet of Battlefield Things) [3]. Human social network infrastructures and subscription services are now available to sensors, where the establishment and exploitation of social relationships among them is completely transparent to the users or their owners [4], [5]. This necessitates the re-design of existing data networks, based on a new network paradigm to maximise security and reliability. However, these are challenging issues due to vehicle mobility in Vehicular Ad Hoc Networks (VANETs). Unsurprisingly, smart vehicles are the objects of SIoT interactions building relationships to enhance the driving knowledge and provide a wider range of the services to the drivers.

Existing cryptographic solutions are designed independently to the physical properties of the network in which they are applied. This has initiated research activities in the area of fast and efficient key generation algorithms based on physical layer characteristics, such as those based on broad Received Signal Strength (RSS) and frequency selectivity [6], [7], [8]. In these approaches, the wireless channel acts as a medium to increase key generation rate, cryptanalysis resilience, and quality of keys generated between end points due to the inherent stochastic nature of wireless propagation channels [9]. In addition, the ability to generate cryptographic keys using these approaches removes the reliance on higher-layer encryption protocols. These "channel-based key" extraction approaches seek to exploit the physical properties of wireless channels, such as reciprocity and temporal/spatial variability, in an attempt to provide the necessary randomness for symmetric key generation [10], [11].

In a typical VANET environment, the wireless links between nodes and co-existent adversaries experience uncorrelated channel attributes. Therefore, these channels can offer a certain degree of confidentiality during the key generation process between parties. Thus, this reduces computational complexity and eases key management. Secret key information is usually generated from one or more channel characteristics as part of the signal quantisation phase. However, the process to determine appropriate channel metrics to characterise a unique wireless channel still remains a challenging and complex domain of scientific inquiry [12], [13].

G. Epiphaniou is with the Wolverhampton Cyber Research Institute, School of Mathematics and Computer Science, University of Wolverhampton, UK (email:g.epiphaniou@wlv.ac.uk)
P. Karadimas is with the School of Engineering, University of Glasgow, Scotland, (e-mail:Petros.Karadimas@glasgow.ac.uk)
D. Kbaier and H. Al-Khateeb are with the School of Computer Science and Technology, University of Bedfordshire, UK (e-mail:Haider.Al-Khateeb@beds.ac.uk, dhouha.kbaier@beds.ac.uk)
A. Dehghantanha is the School of Computer Science and Engineering, The University of Salford, UK (e-mail: A.Dehghantanha@Salford.ac.uk)
K.-K. R. Choo, is with both Department of Information Systems and Cyber Security and Department of Electrical and Computer Engineering, University of Texas at San Antonio, San Antonio, TX 78249, USA (e-mail: raymond.choo@fulbrightmail.org)

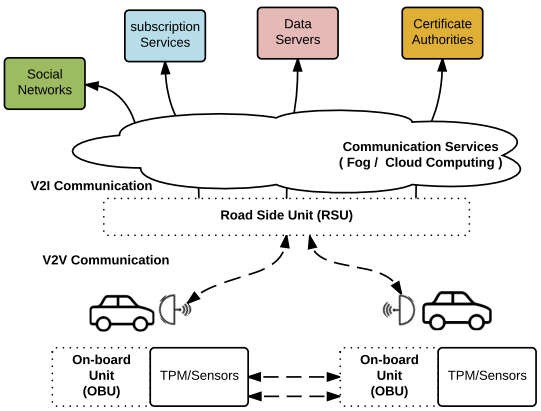

Fig. 1. Vehicular Networking Architecture

A trade-off also exists between quantisation performance and selection of thresholds with a direct impact (positive or negative) to the key generation rate. The unification of the shared secret key must also adhere to error correction principles and valid processes around privacy enhancement techniques in order to minimise information leakage during message exchanges. This process assures symmetric operation between peers and confidentiality by minimising information exchange during the process of correcting bit mismatch between transceivers. This is especially important in social IoT networks, due to the autonomous nature of the nodes exchanging private information.

This paper is the first attempt in the literature to incorporate all essential V2V communication characteristics, such as three-dimensional (3D) multipath propagation and surrounding scatterers' mobility (i.e. other vehicles), in the key generation process. Our key generation technique can be used to establish secure communication channels within ad hoc social vehicular networks. We employ the comprehensive parametric stochastic V2V channel model presented in [14] to synthetically generate the receiver's channel response (Bob's channel), where the transmitter's response arises after applying the non-reciprocity compensation technique presented in [15]. After the necessary thresholding is used to allocate bits according to designated signal levels, we apply turbo coding (TC) techniques for information reconciliation. At the time of this research, this is the first application of TC techniques in such a setting (V2V channels with parametric 3D multipath propagation and scatterers' mobility). We report significant improvement in certain key performance indicators (KPIs), in comparison to existing standard indexing technique described in [16]. To ensure a fair comparison, the particular indexing technique was again applied in conjunction with the non-reciprocity compensation technique in [15]. More specifically, the key generation rate (KGR) and bit mismatch rate (BMR) are significantly improved when combining both non-reciprocity compensation and TCs in our work.

The rest of this paper is structured as follows. Section 2 reviews existing works in secret key extraction focusing on error reconciliation techniques. In Section 3, we briefly present the performance metrics employed in similar works. In Section 4, we present the adopted key generation process by applying TCs and non-reciprocity compensation in V2V communication channels incorporating 3D multipath propagation and scatterers' mobility. A comparative summary is also presented. Finally, Section 5 concludes this paper.

2 Related Works

In VANETs (See Fig.1), nodes are distributed and self-organised with the majority of wireless communication carried out by on-board units (OBUs) integrated with additional services and processes running [17]. High mobility of these nodes and propagation mechanisms of vehicular channels render these environments susceptible to faster fading, multipath delay, path loss and increased Doppler frequency shift. These unique temporal and spatial properties can generate significant randomness in secret-bit extraction and key distribution because channel responses are reciprocal between two end points. Also, the prediction of randomness in these dynamic environments is more difficult than static ones due to the high entropy bits extracted in shorter time [18]. Different approaches have been published in secure key extraction protocols with different strengths and limitations with regards to entropy, secret bit extraction rate, key generation rate, number of nodes and threat models. For an exhaustive comparison of these protocols, readers are encouraged to see work in [19].

2.1 Challenges in secret key generation

The secret key information is usually generated from one or more channel characteristics as part of the signal quantisation phase, including fluctuations of signal amplitudes and channel phase [20], [21], [13]. A trade-off exists between quantisation performance and selection of thresholds with a direct impact (positive or negative) to the key generation rate, entropy and bit mismatch rate. These metrics can be affected by the time difference between channel estimates at Alice and Bob, channel decorrelation in time (channel coherence time), inherent communication noise and hardware impairments [22]. The unification of the shared secret key must also adhere to error correction principles and valid processes around privacy enhancement techniques in order to minimise information leakage during message exchanges. Specifically in V2V communications very high temporal variability takes place due to mobility of transmitter, receiver and surrounding scatterers [14], [23], [24]. Though disadvantageous for communication purposes, such temporal variability can be readily exploited in the key generation process. Signal strength variations due to dynamically changing environments have been leveraged in secret key extraction in [25], [26]. Authors have demonstrated certain degree of entropy in the key generation and exchange process under the assumption that an adversary has unbounded capacity to estimate RSS values of the packets transmitted. In [27], authors introduced a filtering technique promised to maintain entropy and improve signal correlation between communication parties by restricting bit generation only for the period of time that that high motion-related fluctuation is present. Movement characteristics and

their influence in RSS variation have also been exploited for key generation in [22], [28]. The correlation between the probing rate and key generation rate was observed in [29]. Authors introduced an adaptive probing scheme that dynamically changes the probing rate subject to channel-related parameters.

2.2 Secure key generation strategies

Authors in [30] positively correlate entropy of secret bits as a function of mobility with high secret-bit extraction rate. A single channel observation can lead to lower average number of secret bits generated whereas the authors in [31] model the upper bound of the average secret key extraction rate as a function of the signal bandwidth. Most of the approaches rely on the assumptions that Eve cannot jam the communication channel and is not close to either Alice or Bob.

Additional challenges have been recorded when RSS is used as a metric to be quantised [15]. Typical thresholds selected usually do not account for points in between them thus reducing the overall key quality or information available for the key generation process. In addition, RSS is usually extracted by a single frequency resulting in low bit generation rates. On the other hand, channel-phased quantisation presents several benefits as higher level of secrecy can be achieved by the uniform distribution of the phases on the channel taps and increase key generation rate by leveraging the whole channel impulse response (CIR) [19]. It is also noticed that a higher number of secret bits can be extracted that removes the need to estimate RSS over a certain time window. RSS-based approaches though do not require significant hardware modifications with better overall performance in respect to synchronisation errors. The CIR can be described as follows [9]

$$h(t) = \sum_{i=0}^{L-1} h_l \delta\left(t - t_l\right) \tag{1}$$

where $\delta(.)$ is the impulse delta function, L is the number of channel paths, h_l is the l-th path complex gain and t_l is the delay of the signal on the l-th path in the multipath channel. The multipath fading channel properties in frequency domain have also been investigated in the literature as an alternative way to achieve high entropy and key generation rate. Channel state information extracted from OFDM subcarriers has been also introduced in an attempt to reduce random noise and improve overall key generation rate [15]. Multiple thresholds are also used to further quantise these average values of channel response to generate a binary sequence. That bit sequence is then normalised through error reconciliation techniques to assure symmetric and identical bits within the key space. Although this approach is generic, applies more on static nodes and does not depend on mobility aspects making it suitable for wireless sensor networks. A further challenge would be the violation of orthogonality due to Doppler effect inherent in VANETs [32].

Authors in [15], argue that channel state information extracted within the coherence time of the channel could be non-reciprocal due to different electrical properties of wireless devices including antenna systems and RF front circuitry. This unavoidably prevents the extraction of symmetric cryptographic keys with low-bit mismatch rate. However, the channel response in different subcarriers should be different due to diversified frequencies. The location and time in which channel response measurements were taken for a specific subcarrier also differ which can be argued as a factor increasing key randomness. Authors in [33] added that channel information at the receiver can be modelled as a location-dependent variable with enough information entropy to be utilised in key generation. However, if channel response is measured in a short period of time highly correlated estimates are generated in both transmitters. A channel gain complement (CGC) algorithm was introduced in an attempt to reduce the disparity of channel responses [15]. The non-reciprocity components were identified with the use of probe packets for each subcarrier. Authors have recorded high bit mismatch rate when channel state information is quantised in the time domain compared to the frequency domain.

The randomness of signal envelope to share the secret key between two parties has also been examined where deep fades have been used to extract correlated bit strings based on a theoretical analysis and simulation results only [34], [22]*. Multiple antenna diversity has also been investigated for secret key extraction with limitations in the key generation rate [35]. Authors* have argued that the signal envelope can provide (to a pair of transceivers) enough entropy required to extract a cryptographic key for data exchange without the necessity to experience identical signal envelops between transceivers. Although focus on deep fades can partially overcome interference problems, however, the quality of the symmetric key and the key generation rate is low. Authors also limit their discussion on the secure ways that key verification information can be exchanged. They also hold assumptions that the size of the bit streams between the two transceivers are the same although calculated by different random sources. Also, work in [34] proved to be computationally expensive when it comes to key recovery phase that render the algorithm difficult to be implemented in V2V communications. Their fuzzy information reconciliation algorithm seems to remove these constraints but the outcome is reduced entropy in the overall quality of the key produced. Information reconciliation is the process of correcting mismatch bits of the quantisation phase by publicly exchanging information to be used for corrective actions [36].

Quantisation and thresholding are the most important processes in the key establishment process as they provide initial information based on channel characteristics. Also, these processes directly affect the bit mismatch probability due to non-fully reciprocal but highly correlated channel responses of Alice and Bob as a result of inherent communication noise and transceivers hardware impairments. The number of thresholds selected during quantisation also presents a tradeoff between key generation rate and random noise. Additional issues with fixed and multiple thresholds were also reported such as susceptibility to active attacks and discard of sampled values between thresholds respectively [9]. Protection against active attacks has been partially addressed in [6] with an Adaptive Secret bit Generation

(ASBG) scheme. In this approach sampled values were divided into blocks and each block has been independently quantised using its own thresholds based on its average and standard deviation. Although this work seem to improve overall key generation does not account for imperfect channel reciprocity.

Specifically in V2V communications very high temporal variability takes place due to the mobility of transmitter, receiver and surrounding scatterers. Though disadvantageous for communication purposes, such temporal variability can be readily exploited in the key generation process. Two different techniques have been introduced in [37] namely least square thresholding and neural network-based error reconciliation. Authors recorded an improvement in the detection of fades with smaller depth in environments with no deep fades (e.g., line-of-sight situations). The latter technique uses two similar bit strings to generate keys of arbitrary length known to both Alice and Bob. The security of this system is based on the assumption that Eve cannot adequately reverse the training process of the neural network. A low-cost approach with regards to channel sampling effort was introduced in [29]. The authors modelled mathematically an adaptive channel probing approach based on Lempel-Zin and proportional-Integral-Derivative (PID) controller. Adaptation of the probing rate showed improvements in both the key generation rate and efficiency of the probing process.

2.3 Privacy Amplification

The last step in the key generation process assumes that the information extraction about the shared key used should be computationally expensive to adversaries (privacy amplification). Most existing approaches focus on different threat models and assumptions around level of access to the channel. "Trapdoor" functions are used as a mean to assure certain level of authentication and integrity in this process [38]. These functions are also used as a mean to deduce the size of the final key and amplify any errors if hashing a reasonable copy of the key is attempted, to a degree that even an exhaustive search of the key space would be infeasible. This process is also used to account for any information exposed during error reconciliation phase and ensure that eavesdroppers do not gain significant advantage to the point where they are able to reconstruct a significant part of the key. In the next, we present an overview of the most important error correction codes that can be potentially used in the information reconciliation stage.

2.4 Error correction codes

Error reconciliation is the next step in the secret key generation process to correct miss-matched information due to imperfect reciprocity and random noise in the channel. Several error reconciliation algorithms have been introduced with different tradeoffs between communication and computational complexity and throughput error correction capabilities (e.g. Cascade and Winnow). The Cascade error reconciliation protocol assumes that two legitimate parties agree on a random permutation over a public channel [39]. This random permutation takes place over their shifted keys in an attempt to evenly distribute errors. Their shifted keys are then divided in blocks where each block does not present more than one error based on the error rate calculated [40].

Linear error correction codes known as Hamming codes have been also introduced in the literature [41]. In order for a sender to transmit a message with a Hamming code the dot product of a generator matrix and the message must be calculated (code word). The code word is then transmitted at the receiver who computes the product of the code word and the parity check matrix (syndrome). If the calculated syndrome at the receiver is a zero vector, the message was received without any errors. In Winnow protocol [42], the operation is much similar with Cascade. The protocol also suggests privacy maintenance throughout the whole reconciliation phase as a mean to protect information exposed during parity and syndrome exchanges.

Low Density Parity Codes (LDPC) are known for the low density of their parity check matrices which linearly increases the complexity of the decoding algorithm as the length of the message increases [43]. In LDPC codes the minimum distance (as in Hamming codes) and the decoding algorithm used are considered essential parameters to their performance. In their original form LDPC codes have fixed number of 1's in each column k and each row j along with the block n, known as (n,j,k) low density code. The original algorithm developed by Gallager to generate those LDPC matrices was deemed insufficient for large key spaces and limited to work only with regular codes (codes with fixed number of 1's in both columns and rows). LDPC can be more efficient than Cascade as they can become rate adaptive leading to more efficient interactive reconciliation protocols [44], [45].

The invention of turbo codes (TCs) [46] was a revival for the channel coding research community. Historical turbo codes, also sometimes called Parallel Concatenated Convolutional Codes (PCCCs), are based on a parallel concatenation of two Recursive Systematic Convolutional (RSC) codes separated by an interleaver. They are called "turbo" in reference to the analogy of their decoding principle with the turbo principle of a turbo compressed engine, which reuses the exhaust gas in order to improve efficiency.

The turbo decoding principle calls for an iterative algorithm involving two component decoders exchanging information in order to improve the error correction performance with the decoding iterations. This iterative decoding principle was soon applied to other concatenations of codes separated by interleavers, such as Serial Concatenated Convolutional Codes (SCCCs) [47], [48], sometimes called serial turbo codes, or concatenation of block codes, also named block turbo codes [49], [50]. The near-capacity performance of turbo codes and their suitability for practical implementation explain their adoption in various communication standards. In [51] the authors proposed utilizing Turbo codes for reconciliation purposes. Further investigation in [52] show that TCs are good candidates for reconciliation. The efficacy of TCs with regards to their error correction capabilities in various wireless communication standards is also recorded in [53]. Further work in [24] demonstrate the improved performance of TCs over Reed Solomon and CCs which are the de-facto error correction codes used in 802.11p vehicular networks. However, this work does not comprehensively incorporate physical propagation characteristics such as 3D

scattering and scatterers' mobility which is addressed in this work.

3 Performance Metrics

As VANETs are inherently rapidly time-varying due to multipath propagation, this work parametrically models and quantifies such temporal variability attributes and incorporates them into the key generation process. In addition, violation of reciprocity due to hardware impairments or other penalty factors will be compensated in the architectural design and implementation. The proposed algorithmic process will have to compensate for penalty factors influencing the coherence region. The necessity for this work stems from the research effort to further reduce bit mismatch rate while maintaining high key generation rate in practical VANET environments where mobility of the nodes and large network scale imposes unique security challenges. Three performance indicators namely, entropy, secret bit extraction rate and bit mismatch rate, are discussed. The later determines the rate at which the V2V channel is probed in order to secure highly uncorrelated successive samples. We thus present in the following the probing rate together with the three performance indicators.

3.1 Probing Rate

The probing rate for both Alice and Bob $F_P = f_{PA} = f_{PB}$ is considered the same for the purpose of channel estimates collection. To achieve uncorrelated successive channel probes, thus achieving highest entropy, successive probes have to be taken in different coherence regions. Thus, we must define $F_P \leq v_{max}$, where v_{max} is the maximum Doppler frequency shift [14]. Considering single bounce of multipath power onto mobile scatterers (e.g., other vehicles), it is defined as [14]

$$v_{max} = \frac{f_c}{c}\left(u_{Tmax} + u_{Rmax} + 2u_{Smax}\right) \tag{2}$$

where f_c is the carrier frequency, c the speed of light in free space and u_{Tmax}, u_{Rmax} and u_{Smax} the maximum velocities of transmitter, receiver and mobile scatterers, respectively. In order to maximise the bit extraction rate, we should investigate the feasibility of defining F_P as equal to v_{max}.

3.2 Entropy measures

The de-facto metric which quantifies the uncertainty is the entropy of the generated bit string. The higher the entropy the limited the ability to deduce a secret key established by Eve due to larger uncertainty introduced. Entropy per bit i is defined as [9]

$$H_i = -p_0 log_2 p_0 - (1-p_0) log_2 (1-p_0) \tag{3}$$

where p_0 the probability of having zero and $1 - p_0 = p_1$ the probability of having one. Ideally, we should have $p_0 = p_1 = 0.5$. For independent bit sequences, the total entropy is $H_{total} = \sum_{i=1}^{N} H_i$, where N is the total number of bits in a sequence [54]. In an ideal case, $H_{total} = N$ bits.

3.3 Secret bit extraction rate

The rate is measured in terms of the final secret-bits extracted after error reconciliation and privacy amplification. In practice the secret bit extraction rate depends on the probing rate from Alice and Bob and the number of secret bits per probing. The amount of secret bits extracted in a time varying channel is influenced by the thresholding. Considering 0s and 1s to be generated with equal probabilities (after proper thresholding) the secret bit extraction rate will be R_k [16]

$$R_k = 2 f_P p(A = 1, B = 1) \tag{4}$$

where $p(A = 1, B = 1)$ is the joint probability of having 1 simultaneously at Alice's and Bob's bit strings. However, in this paper we consider key generation rate as the number of symmetric keys produced per unit time.

3.4 Bit mismatch Rate

Usually BMR will be measured as a ratio of the number of bits that do not match between Alice and Bob to the number of bits extracted at the thresholding stage often used as a performance criterion for the quantisation process [9]. The BMR is measured immediately after the thresholding stage because a single mismatch in the bitstring can render the secret key unusable. Bit mismatch rate differs from the bit error rate in communication theory, which represents the number of bits received in error. The two reasons for bit mismatch are the unavoidable inherent noise in any wireless communication link and the violation of reciprocity due to hardware impairments. As violation of non-reciprocity is compensated we are left with the inherent noise as a unique problem. This noise will add uncertainty to the transmitted bit strings given the received bit strings. Ideally, both bit strings should have been identical. The bit mismatch probability can be described as follows [16]

$$P_N = 1 - (1 - p_e)^N \tag{5}$$

where p_e will be the probability of a single erroneous bit defined as [34]

$$p_e = P(B = 0 | A = 1) = \frac{P(B = 0, A = 1)}{P(A = 1)} \tag{6}$$

where $P(B = 0|A = 1)$ is the conditional probability of Bob's bit being 0 when Alice's is 1.

4 Non-reciprocity compensation and TC reconciliation in VANET

The key generation process presented in Fig. 2 considers for error reconciliation the method presented in [16] and for a first time TCs in a V2V environment. However, the input data in our case are generated synthetically in order to comply with V2V propagation settings.

4.1 V2V channel model

The synthetic simulated Bob's channel response is generated by employing the Monte Carlo simulation method [55]. For the V2V setting the theoretical channel model that needs to

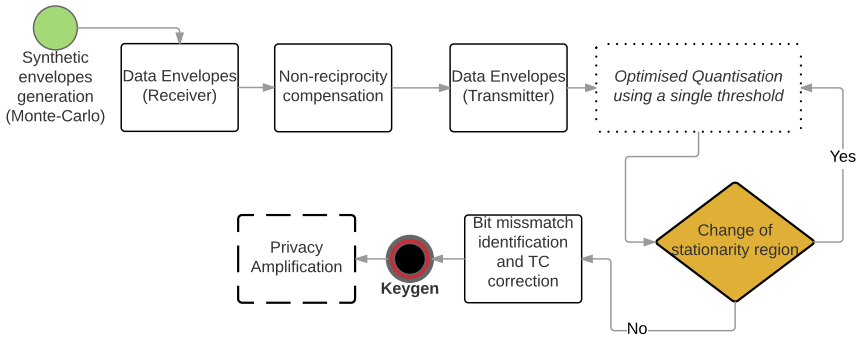

Fig. 2. Algorithmic process for combined TC and NR compensation

be simulated has been described in detail in [14]. Thus Bob's response in time domain is written as

$$G_B(t) = \sum_{l=1}^{L} |\alpha_l| exp(j\phi_l) exp(j2\pi u_l t) \tag{7}$$

The Doppler frequency u_l is determined by

$$u_l = v_{T,l} + u_{S,l} + u_{R,l} \tag{8}$$

where $u_{T,l}$, $u_{S,l}$ and $u_{R,l}$ are the contributions due to Tx mobility, scatterers' mobility and Rx mobility, respectively. The Doppler shift $u_{T(R),l}$ results from the departure (arrival) of the l^{th} multipath component from the mobile Tx (to the mobile Rx). It is defined as [14]

$$u_{T(R),l} = u_{T(R)max} cos\beta_{T(R),l} cos\alpha_{T(R),l} \tag{9}$$

where $u_{T(R)max} = v_{T(R)}/\lambda$, λ is the carrier wavelength, $u_{T(R)}$ the the Tx (Rx) velocity, $\alpha_{T(R),l}$ the azimuth angle of departure (AOD) (angle of arrival (AOA)) and $\beta_{T(R),l}$ the elevation AOD (AOA) with respect to the Tx (Rx) motion. $\alpha_{T(R),l}$ counts from the value $-\pi$ in the negative Y axis returning to the same point in the clockwise direction and $\beta_{T(R),l}$ is zero on the X-Y plane, $\pi/2$ on the positive Z axis and $-\pi/2$ on the negative Z axis. Considering interaction of the l^{th} multipath component with a single mobile scatterer, the Doppler shift $v_{S,l}$ will be [14]

$$u_{S,l} = (v_{S,l}/\lambda)(cos\alpha_{l,l} + cos\alpha_{2,l}) \tag{10}$$

where $v_{S,l}$ is the scatterer's velocity, $\alpha_{l,l}$ the AOA and $\alpha_{2,l}$ the AOD with respect to scatterer's motion.

The target is to appropriately model each factor affecting the V2V channel response namely $\{|\alpha_l|\}$, $\{u_l\}$, $\{\phi_l\}$. In this paper we consider a normalised (power equal to unity) Rayleigh V2V channel with partially uniform 3D scattering at both Alice's and Bob's sides with a Weibull distribution of the mobile scatterers' velocity. Rather than just a scenario for demonstration, the partially 3D uniform scattering can be further generalized to represent any multipath propagation scenario [56] whereas the Weibull distribution for the multipath power contributed by mobile scatterers has been proved a suitable modeling approach [57]. Thus the scatterers velocity, which in fact models the power contributed by mobile scatterers, is defined as

$$p_{u_s} = w u_S^{b-1} exp(-w u_S^b / b) \tag{11}$$

where $b \leq 1$ is the shape parameter and w the scale parameter. The amplitudes $|\alpha_l|$ are constant and phases ϕ_i are uniformly distributed in $[-\pi, \pi]$, i.e., $|\alpha_l| = \sqrt{2/L}$ and $\phi_l \sim U[-\pi, \pi]$ [55]. Each Doppler contribution of Eq. 7 has the following parameters need to be modelled: azimuth angle of departure (AOD), angle of arrival (AOA) $\alpha_{T(R),l} \sim U[A_{T(R)min}, A_{T(R)max}]$ elevation AOD (AOA) $\beta_{T(R),l} \sim U[B_{T(R)min}, B_{T(R)max}]$, AOA to mobile scatterer $\alpha_{1,l} \sim U[-\pi, \pi]$, AOD to mobile scatterer $\alpha_{2,l} \sim U[-\pi, \pi]$, power contributed by mobile scatterers $u_S \sim p_{u_s}(u_S)$. The symbolism $U[.,.]$ stands for the uniform distribution in the designated interval. This scenario can approximate an urban environment with other mobile vehicles and heavy scattering.

In order to simulate a purely diffuse Rayleigh environment we need at least seven sum of sinusoids such as those seen in Eq. (7) [58]. For simulation purposes, we define L=20. The sampling/probing rate $F_p = 1/T_{cmin}$ where $T_{cmin} = 1/v_{max} = \frac{c}{f_c}/(u_{Tmax} + u_{Rmax} + 2u_{Smax})$ is the minimum coherence in time and $u_{Tmax}, u_{Rmax}, u_{Smax}$ are the maximum Doppler shifts due to mobile transmitter, receiver, and scatterers respectively. In this way, we secure that the channel is mostly probed in different coherence regions, thus successive bits will be independent, resulting keys with maximum entropy. Considering the maximum velocity of transmitter, receiver and scatters to be 30m/s, frequency of operation $f_c = 6GHz$, the probing rate is calculated as $F_p = 2400$ samples per second. We can further reduce F_P, as $1/T_{cmin}$ is in fact its upper bound, however doing so, will reduce the key generation rate, resulting marginal improvement in the key entropy. The latter is just our perception and further research is required, however it goes beyond the scope of this article, which focuses on the applicability of TCs at the information reconciliation stage and potential performance improvement. A possible solution might be to adapt $F_P = 1/T_{cmin}$ to fit in changes of the coherence region due to variations in the propagation conditions (e.g., more intense scatterers' mobility, more directional propagation, etc).

4.2 Algorithmic Process

Alice's channel response would normally arise by similar channel probing rate in time instances such that hers and Bob's responses are taken within the same coherence region. However, to further improve performance, Alice's

response $G_A(t)$ will arise after applying the non-reciprocity compensation model presented in [15]. Thus considering M estimates within the same coherence region between Alice and Bob, their channel responses are related as [15]

$$G_A(t) - G_B(t) \sim N(0, \sigma^2) \tag{12}$$

The variance is estimated by the discrepancy of Alice's and Bob's estimates as follows

$$\sigma^2 = \frac{1}{M}\sum_{i=1}^{M}(G_{A,i}(t) - G_{B,i}(t) - \mu_t)^2 \tag{13}$$

where

$$\mu_t = \frac{1}{M}\sum_{i=1}^{M}(G_{A,i}(t) - G_{B,i}(t)) \tag{14}$$

This method was presented in [16] where Alice and Bob determine samples from channel estimates above and below an upper and lower threshold discarding those in between, i.e., lossy thresholding. We use this approach to compare it against our TC correction process presented in Figure 2. Those estimates are samples in a form of an excursion. The quantisation process creates segments of those samples (also referred as excursions) of succesive bit values of 1s and 0s. Each of those segments are created whenever a channel probe returns a reading that does not fall inside the thresholds. Alice selects a random set of these segments and sends to Bob the index of the channel estimate lying in the center of the segment defined as $i_{center} = \lfloor \frac{i_{start}+i_{end}}{2} \rfloor$ as a list L_a. The number of channel estimates are modelled in the simulation and the total size for each segment has been setup to $m = 5$ successive estimates that fall outside the thresholds (acceptable estimates). However, m is a configurable parameter of the algorithm that combined with the quantisation process affects the tradeoff between key generation rate and bit miss-match probability. Indeed a larger value of m reduces the number of secret bits that can be generated per second. Following implementation and testing in [16], we define $m = 5$. For each index from Alice, Bob checks his segments and verifies his samples centered around that index above or below the thresholds $q-$, $q+$ matched with Alice and generates a new list of those indices $L_b \leq L_a$. Bob sends L_b over to Alice. Both Alice and Bob quantise their channel estimates at each index of L_b in order to generate the bit-string. Thus, this method simultaneously accomplishes thresholding and information reconciliation.

4.3 Results and discussion

Part of the algorithmic operation is to develop an optimisation sub-routine to adaptively change the threshold as a function of the temporal variability of the channel. The optimisation routine will consider several attributes such as multi-clustered three dimensional scattering, specular-reflected multipath components, multiple bounces on mobile objects in dense propagation environments. Threshold selection has to be adopted dynamically to the temporal variations induced by the aforementioned effects. The thresholds should be refreshed after a specific amount of time over which the stationarity region has been crossed. We anticipate the refresh to take place every 10 coherence regions due to the inherent non-stationarity of the V2V channel [14]. An alternative way to refresh the thresholding process could be to consider a Doppler spectrum correlation criterion. More specifically, considering the normalised Doppler spectrum as a probability distribution of Doppler frequencies, the Doppler correlation coefficient will be defined as

$$\rho(X, Y) = \frac{cov(X, Y)}{\sigma_X \sigma_Y} \tag{15}$$

where $cov(X, Y)$ is the covariance of the X,Y normalised Doppler spectra and σ_X, σ_Y are the standard deviations of X, Y, respectively. When the correlation coefficient falls below a specified threshold (e.g.,) the quantisation and thresholding process will be refreshed. The first phase of the routine developed is the construction of the Synthetic data which will be generated via Monte Carlo simulation taking into account the number of multiple components, the sampling rate and total number of samples. In the next stage the probed received envelopes are generated considering an appropriately defined probing rate in order to maximize the entropy in the subsequent quantisation step. From the received data, the transmitted data are modelled by considering non-reciprocity compensation. At this stage a lossy quantisation process is preferred due to its computational simplicity. The target is to end up with a maximum secret bit extraction rate and entropy. For that purpose, in the following step several runs should take place considering the thresholds multiple pairs. A feasibility study of both lossless and lossy quantisation processes and their applicability in V-V scenarios is an area for further investigation. We consider the transmission scenario between Alice and Bob. The transmitter's samples are modelled by adopting a channel gain complement technique which compensates channel non-reciprocity. This is done by adding a zero mean Gaussian variability to the receivers samples. Thus, the input information sequence in the TC represents the generated key for Bob, while the output of the AWGN channel after turbo encoding designates the generated key for Alice. Then, turbo decoding is performed and the performance of the reconciliation method can be evaluated by measuring the Bit Error Rate and the key generation rate.

Bob's generated sequence after quantization is fed to the input of a TC. During this process a single threshold is adopted as a lossless quantisation scheme with the potential to substantially increase the key generation rate [34]. The threshold adopted in our work is static and equal to 1. However, an adaptive quantisation process related to the channel temporal variability that updates the threshold at each stage is currently investigated. Turbo decoding is then performed in order to generate a symmetric output, i.e. symmetric keys for Alice and Bob. Increasing the number of decoding iterations in TCs reduces the bit error rate, thus, improving the bit miss-match rate between Alice and Bob. Furthermore, it would result to an increased key generation rate at the expense of added computational complexity as part of the turbo decoding process. In our algorithm, TCs are simulated with a single iteration. Performance of the reconciliation method can be evaluated by measuring the BMR and to the Bit Error Rate (BER) in our case. The comparison is made against the sample indexing technique

TABLE 1
TC simulation results in secret key generation

Key Length (bits)	KGR (with TCs)	KGR (with Indexing [16])
128	35 keys/min	3 to 7 keys/min
256	17 keys/min	2 to 5 keys/min
512	8 keys/min	1 to 2 keys/min

TABLE 2
Comparison of BMR with existing RSS-Based approaches

Scheme	Design Approach	BMR
Patwari et al. [59]	RSS-based	0.482
Jana et al. [18]		$0 \sim 0.55$
Premnath et al. [6]		$0.02 \sim 0.24$
Croft et al. [60]		$0.01 \sim 0.07$
Zan et al. [7]		$0.005 \sim 0.02$
Mathur et al. [16]		0.22
Non-reciprocity compensation with TC (Our approach)		0.02

already applied in our algorithm as discussed in subsection 4.2. We measure the efficiency and efficacy of our algorithm against widely adopted metrics namely entropy, bit mismatch rate, probing rate and key generation rate. We calculated BMR for the indexing method by considering the discarded indexes after Alice's and Bob's channel probing. In Table 1 we compute the key generation rate for different key lengths. Compared to the samples' indexing method in [9], there was a significant improvement on both BMR and key generation rate. The simulated BER to generate a symmetric shared key between Alice and Bob after error reconciliation is estimated to only 0.0752 using TCs. Furthermore, the BMR with single thresholding is only 0.02 whereas the estimated BMR with the indexing technique is around 0.22 in both cases of static and mobile scatterers. The key generation rate was also reported high considering different key lengths requested. For instance, the secret key rate to generate the 128-bit symmetric key is 35 good keys per minute with TCs while it varies from 3 to 7 symmetric keys per minute with the indexing technique. As shown in Table 1, simulations proved similar improvements for different key lengths as part of the error reconciliation process. Satisfactory entropy values were obtained throughout all rounds of simulation during the key extraction process ranging from $0,85 \sim 0,97$ bits per sample. Note that the BMR with the indexing technique is nearly the same for different key lengths which is coherent with the uniform method used by the authors. In Table 2, we present a comparison between the BMR achieved in our approach with existing RSS-based approaches published in the literature.

5 Conclusion

We successfully combined non-reciprocity compensation and TCs for information reconciliation as the most important features in V2V communication including 3D scattering and scatterers' mobility. Findings from our evaluations indicated significant improvements were achieved in key generation rate with reduced BMR when TCs are employed against an existing indexing method. Our proposed technique can be used to secure communications between vehicular nodes in an ad hoc social IoT network, and this has applications in both civilian and adversarial / military context (e.g. Internet of Military and Battlefield Things).

Future studies include the investigation of TCs for error conciliation purposes especially in the context of social IoT networks. For example, we will focus on several parameters that affect performance of TCs such as component decoding algorithms, number of decoding iterations, generator polynomials, constraint lengths of the component encoders and the interleaver type. Increasing the number of iterations in the TC can significantly improve the BER, thus generating more symmetric keys. Furthermore, we are working towards the single thresholding process by creating a dynamic threshold that is updated according to the receiver's samples.

Acknowledgment

This work was partially funded by the Defence Science and Technology Laboratory (DSTL), under contract CDE 41130. Moreover, this work is partially supported by the European Council 268 International Incoming Fellowship (FP7-PEOPLE-2013-IIF) grant. The authors would also like to thank Mr George Samartzidis for his initial contribution in the algorithm development. The last author is funded by the Cloud Technology Endowed Professorship.

References

[1] K.-K. R. Choo, *Secure Key Establishment*, ser. Advances in Information Security. New York, NY, USA: Springer, 2009, vol. 41.

[2] M. J. B. Robshaw and O. Billet, Eds., *New Stream Cipher Designs - The eSTREAM Finalists*, ser. Lecture Notes in Computer Science. Springer, 2008, vol. 4986.

[3] C. Huang, R. Lu, and K.-K. R. Choo, "Vehicular fog computing: Architecture, use case and security and forensic challenges," *IEEE Communications Magazine*, 2017.

[4] S. Smaldone, L. Han, P. Shankar, and L. Iftode, "Roadspeak: Enabling voice chat on roadways using vehicular social networks," in *Proceedings of the 1st Workshop on Social Network Systems*, ser. SocialNets '08. New York, NY, USA: ACM, 2008, pp. 43–48. [Online]. Available: http://doi.acm.org/10.1145/1435497.1435505

[5] X. Hu, V. C. Leung, K. G. Li, E. Kong, H. Zhang, N. S. Surendrakumar, and P. TalebiFard, "Social drive: A crowdsourcing-based vehicular social networking system for green transportation," in *Proceedings of the Third ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, ser. DIVANet '13. New York, NY, USA: ACM, 2013, pp. 85–92. [Online]. Available: http://doi.acm.org/10.1145/2512921.2512924

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

[7] 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.

[8] Y. E. H. Shehadeh and D. Hogrefe, "A survey on secret key generation mechanisms on the physical layer in wireless networks," *Sec. and Commun. Netw.*, vol. 8, no. 2, pp. 332–341, Jan. 2015. [Online]. Available: http://dx.doi.org/10.1002/sec.973

[9] T. Wang, Y. Liu, and A. V. Vasilakos, "Survey on channel reciprocity based key establishment techniques for wireless systems," *Wireless Networks*, vol. 21, no. 6, pp. 1835–1846, 2015. [Online]. Available: http://dx.doi.org/10.1007/s11276-014-0841-8

[10] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *CoRR*, vol. abs/1011.3754, 2010. [Online]. Available: http://arxiv.org/abs/1011.3754

[11] Y. E. H. Shehadeh and D. Hogrefe, "A survey on secret key generation mechanisms on the physical layer in wireless networks," *Sec. and Commun. Netw.*, vol. 8, no. 2, pp. 332–341, Jan. 2015. [Online]. Available: http://dx.doi.org/10.1002/sec.973

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

[13] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 364–375, Sept 2007.

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

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

[16] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, *Secret Key Extraction from Level Crossings over Unauthenticated Wireless Channels*. Springer US, 2010, pp. 201–230. [Online]. Available: http://dx.doi.org/10.1007/978-1-4419-1385-2_9

[17] F. Qu, Z. Wu, F. Y. Wang, and W. Cho, "A security and privacy review of vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985–2996, Dec 2015.

[18] 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://doi.acm.org/10.1145/1614320.1614356

[19] A. Ghosal, S. Halder, and S. Chessa, "Secure key design approaches using entropy harvesting in wireless sensor network_ A survey," *Journal of Network and Computer Applications*, vol. 78, no. C, pp. 216–230, Jan. 2017.

[20] H. Koorapaty, A. A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Communications Letters*, vol. 4, no. 2, pp. 52–55, Feb. 2000. [Online]. Available: http://dx.doi.org/10.1109/4234.824754

[21] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[22] 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

[23] J. Almeida, M. Alam, J. Ferreira, and A. S. Oliveira, "Mitigating adjacent channel interference in vehicular communication systems," *Digital Communications and Networks*, vol. 2, no. 2, pp. 57 – 64, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2352864816300104

[24] G. Kiokes, G. Economakos, A. Amditis, and N. K. Uzunoglu, "A comparative study of ieee 802.11 p physical layer coding schemes and fpga implementation for inter vehicle communications," *Modern Traffic and Transportation Engineering Research*, vol. 2, no. 2, pp. 95–102, 2013.

[25] P. Barsocchi, S. Chessa, I. Martinovic, and G. Oligeri, "A cyber-physical approach to secret key generation in smart environments," *J. Ambient Intelligence and Humanized Computing*, vol. 4, no. 1, pp. 1–16, 2013. [Online]. Available: https://doi.org/10.1007/s12652-011-0051-5

[26] P. Barsocchi, G. Oligeri, and C. Soriente, "SHAKE: single hash key establishment for resource constrained devices," *Ad Hoc Networks*, vol. 11, no. 1, pp. 288–297, 2013. [Online]. Available: https://doi.org/10.1016/j.adhoc.2012.05.013

[27] S. T. Ali, V. Sivaraman, and D. Ostry, "Zero reconciliation secret key generation for body-worn health monitoring devices," in *Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WISEC '12. New York, NY, USA: ACM, 2012, pp. 39–50. [Online]. Available: http://doi.acm.org/10.1145/2185448.2185455

[28] J. Zhang, M. H. Firooz, N. Patwari, and S. K. Kasera, "Advancing wireless link signatures for location distinction," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, ser. MobiCom '08. New York, NY, USA: ACM, 2008, pp. 26–37. [Online]. Available: http://doi.acm.org/10.1145/1409944.1409949

[29] Y. Wei, K. Zeng, and P. Mohapatra, "Adaptive wireless channel probing for shared key generation," in *2011 Proceedings IEEE INFOCOM*, April 2011, pp. 2165–2173.

[30] Y. E. H. Shehadeh, O. Alfandi, and D. Hogrefe, "On improving the robustness of physical-layer key extraction mechanisms against delay and mobility," in *8th International Wireless Communications and Mobile Computing Conference, IWCMC 2012, Limassol, Cyprus, August 27-31, 2012*, 2012, pp. 1028–1033. [Online]. Available: http://dx.doi.org/10.1109/IWCMC.2012.6314347

[31] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *Trans. Info. For. Sec.*, vol. 2, no. 3, pp. 364–375, Sep. 2007. [Online]. Available: http://dx.doi.org/10.1109/TIFS.2007.902666

[32] T. Wang, J. G. Proakis, E. Masry, and J. R. Zeidler, "Performance degradation of ofdm systems due to doppler spreading," *IEEE Transactions on Wireless Communications*, vol. 5, no. 6, pp. 1422–1432, June 2006.

[33] M. Wilhelm, I. Martinovic, and J. B. Schmitt, "Secure key generation in sensor networks based on frequency-selective channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1779–1790, September 2013.

[34] 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

[35] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *Proceedings of the 29th Conference on Information Communications*, ser. INFOCOM'10. Piscataway, NJ, USA: IEEE Press, 2010, pp. 1837–1845. [Online]. Available: http://dl.acm.org/citation.cfm?id=1833515.1833766

[36] J. Wallace, R. Mehmood, R. Sharma, W. Henkel, O. Graur, N. Islam, and A. Filip, *Physical-Layer Key Generation andReconciliation*. Cham: Springer International Publishing, 2016, pp. 393–430. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-22440-4_17

[37] D. S. Karas, R. Schober, and G. K. Karagiannidis, "Channel level crossing-based security for communications over fading channels," *IET Information Security*, vol. 7, no. 3, pp. 221–229, Sep. 2013.

[38] 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

[39] G. Brassard and L. Salvail, "Secret-Key Reconciliation by Public Discussion," in *Eurocrypt '93*. Springer-Verlag, 1993, pp. 410–423. [Online]. Available: http://citeseer.ist.psu.edu/viewdoc/summary?doi=10.1.1.42.9686

[40] G. v. Assche, *Quantum Cryptography and Secret-Key Distillation*. New York, NY, USA: Cambridge University Press, 2012.

[41] T. K. Moon, *Error Correction Coding: Mathematical Methods and Algorithms*. Wiley-Interscience, 2005.

[42] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, and C. G. Peterson, "Fast, efficient error reconciliation for quantum cryptography," *Phys. Rev. A*, vol. 67, p. 052303, May 2003. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.67.052303

[43] R. G. Gallager, "Low-density parity-check codes," 1963.

[44] J. Martínez-Mateo, D. Elkouss, and V. Martin, "Blind reconciliation," *Quantum Information & Computation*, vol. 12, no. 9-10, pp. 791–812, 2012. [Online]. Available: http://www.rintonpress.com/xxqic12/qic-12-910/0791-0812.pdf

[45] J. Martnez-Mateo, D. Elkouss, and V. Martn, "Interactive reconciliation with low-density parity-check codes," in *2010 6th International Symposium on Turbo Codes Iterative Information Processing*, Sept 2010, pp. 270–274.

[46] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon

limit error-correcting coding and decoding: Turbo-codes," in *Proc. ICC'93, Geneva, Switzerland*, vol. 2, May 1993, pp. 1064–1070.
[47] S. Benedetto, D. Divsalar, G. Montorsi, and F. Pollara, "Serial concatenation of interleaved codes: Performance analysis, design, and iterative decoding," *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 909–926, May 1998.
[48] S. Benedetto and G. Montorsi, "Iterative decoding of serially concatenated convolutional codes," *Electronics letters*, vol. 32, no. 13, pp. 1186–1188, June 1996.
[49] ——, "Serial concatenation of block and convolutional codes," *Electronics Letters*, vol. 32, no. 10, pp. 887–888, May 1996.
[50] R. Pyndiah, "Near-optimum decoding of product codes: Block turbo codes," *IEEE Transactions on Communications*, vol. 46, no. 8, pp. 1003–1010, 1998.
[51] K. Nguyen, G. V. Assche, and N. J. Cerf, "Side-information coding with turbo codes and its application to quantum key distribution," *CoRR*, vol. cs.IT/0406001, 2004. [Online]. Available: http://arxiv.org/abs/cs.IT/0406001
[52] N. Benletaief, H. Rezig, and A. Bouallegue, "Toward efficient quantum key distribution reconciliation," *Journal of Quantum Information Science*, vol. 2014, 2014.
[53] E. Yeo and V. Anantharam, "Iterative decoder architectures," *IEEE Communications Magazine*, vol. 41, no. 8, pp. 132–140, Aug 2003.
[54] T. M. Cover and J. A. Thomas, *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience, 2006.
[55] P. Hoeher, "A statistical discrete-time model for the WSSUS multipath channel," *Vehicular Technology, IEEE Transactions on*, vol. 41, no. 4, pp. 461–468, 1992.
[56] P. Karadimas and J. Zhang, "A generalized analysis of three-dimensional anisotropic scattering in mobile wireless channels-part ii: Second-order statistical characterization." in *VTC Fall*. IEEE, 2012, pp. 1–5.
[57] P. Karadimas, E. D. Vagenas, and S. A. Kotsopoulos, "On the scatterers' mobility and second order statistics of narrowband fixed outdoor wireless channels," *IEEE Trans. Wireless Communications*, vol. 9, no. 7, pp. 2119–2124, 2010. [Online]. Available: http://dx.doi.org/10.1109/TWC.2010.07.080874
[58] M. Patzold, *Mobile Fading Channels*. New York, NY, USA: John Wiley & Sons, Inc., 2003.
[59] N. Patwari, J. Croft, S. Jana, and S. 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, 1 2010.
[60] 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: ACM, 2010, pp. 70–81. [Online]. Available: http://doi.acm.org/10.1145/1791212.1791222