Wireless Netw
DOI 10.1007/s11276-014-0841-8

Survey on channel reciprocity based key establishment techniques for wireless systems

Tao Wang · Yao Liu · Athanasios V. Vasilakos

Abstract Channel reciprocity based key establishment techniques have attracted more and more attention from the wireless security research community for its easy implementation, low computational requirement, and small energy consumption. The basic idea of these techniques is to establish a shared key by utilizing the wireless channel reciprocity, i.e., the transmitter and receiver of one wireless link can observe the same channel simultaneously. In this survey, we reviewed different types of existing techniques based on (1) how they quantize the wireless channel reciprocity into binary bits to form a secret key; (2) how they handle communication errors to achieve the key agreement between the transmitter and the receiver; and (3) the feasibility and security issues related to these techniques. This survey attempts to summarize the emerging research on channel reciprocity based key establishment, which may provide insights for us to identify wireless security problems and propose comprehensive defenses.

Keywords Key establishment · Wireless channel · Network security · Authentication

T. Wang · Y. Liu (✉)
Department of Computer Science and Engineering, University of South Florida, Tampa, FL, USA
e-mail: yliu@cse.usf.edu

T. Wang
e-mail: taow@mail.usf.edu

A. V. Vasilakos
University of Western Macedonia, Kozani, Greece
e-mail: vasilako@ath.forthnet.gr

1 Introduction

Wireless devices have been widely used due to its remarkable evolvement in the past 2 decades. Unlike traditional communication, a wireless device can communicate with any other device within its power range. This makes wireless communication vulnerable to potential attacks, because any devices within the power range of a wireless transmitter can receive the signal from this transmitter through the open public air. Therefore, eavesdropping becomes one of the major secure problems to wireless systems. Intuitively, the communicators would like to share a common secret key, so that their conversation can be encrypted against eavesdroppers.

Traditional approaches to generate shared secret keys are mainly based on key pre-distribution schemes and public key cryptography. In the former, a centralized trusted third party generates, maintains, and distributes shared keys to communicators. However, such a scheme introduces a high key management complexity for large scale wireless networks, which usually involve a large size of key pool and require intensive key distribution to support the key establishment between every pair of nodes.

On the other hand, public key cryptographic approaches to generate secret keys normally require the communication entities to be equipped with desired computing chips or modules, and they have been long regarded as expensive in terms of computational complexity. For example, Diffie–Hellman algorithms [1], the most popular cryptographic tools to establish a shared secret key between two parties, require exponential operations on large numbers. Thus, they are not suitable for establishing the secret key among low-end wireless devices (e.g., wireless sensor nodes) that are of limited battery lifetime and computational capability.

Published online: 13 January 2015

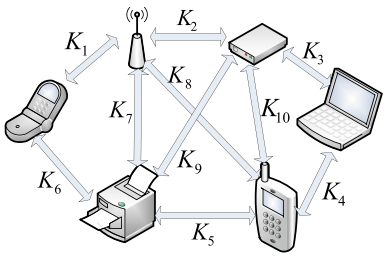


Fig. 1 A scenario of wireless key establishment

Recently, researchers have started to explore alternative key establishment techniques that are efficient and unique for wireless systems. There is an increasing concern about achieving fast and efficient key establishment via exploiting physical layer characteristics of wireless channels. The basic idea is to use the wireless channel reciprocity, which means that the receiver and the transmitter of one wireless link observe the same channel simultaneously. The reciprocity property of wireless channels allows two legitimate devices to establish a shared key. As a scenario illustrated in Fig. 1, wireless devices that are connected by the same wireless link can observe the same channel and establish a shared key. Due to the spatial uncorrelation of wireless channels, for two transmitters at different locations, the channels observed by the same receiver are different. Thus, the key established between a pair of wireless devices is confidential to a third un-colocated party. Past measurement results show that a distance of half a wavelength between the third party and the communicators can cause a mismatch about 50 % between the channels observed by the third-party and legitimate communication parties [2].

Such techniques have formed a fruitful area, and they overcome the drawbacks of traditional key establishment approaches due to its reduced computational effort and relaxed key management requirement. In what follows, we give the taxonomy of these techniques and discuss the open research issues. First, we described the techniques that have been proposed to use different channel metrics to establish the secret key [2–5]. Second, we showed the schemes on how to achieve the key agreement between the transmitter and the receiver [6, 7]. Finally, we talked about the feasibility, security and new emerging techniques of key establishment Schemes [8–11].

1.1 Basics of shared key generation

In general, a shared key is a binary bit sequence that is only known to the transmitter and the receiver. They use the shared key to encrypt and decrypt transmitted information to secure their communication. In channel reciprocity based key establishment, a shared key is generated from one or more channel characteristics, such as signal frequency-phase, received signal strength (RSS), and channel impulse response (CIR).

It normally takes three steps to implement a channel reciprocity based key establishment, and they are *quantization*, *reconciliation*, and *privacy amplification*. In quantization, the transmitter and receiver first sample the transmitted signal at a certain frequency, then both of them quantize the sampled signal based on particular thresholds to generate initial binary bit sequences. Due to imperfect reciprocity and random noise, the bit sequence generated at the transmitter and the receiver from quantization may not be exactly the same. Hence, reconciliation schemes will be applied to deal with these mismatch bits. The objective of reconciliation is to correct or delete these mismatch bits using minimum channel information. After reconciliation, the transmitter and the receiver then perform privacy amplification to avoid a malicious adversary deducing the secret bit sequence. In this survey, we will classify the existing approaches on wireless channel reciprocity based key establishment into three categories based on the following critical aspects:

1. *Quantization* quantization is the most important part of the shared key establishment, because it provides initial information of the wireless channel. All the remaining steps expect an efficient and precise quantization output. The essential challenge of quantization is how to determine channel metrics that can fully characterize a unique wireless channel. Recent studies (e.g., [12–15]) show that the selection of channel metrics has a direct impact on the performance of quantization, and there exist appropriate channel metrics (e.g., RSS, CIR, and frequency-phase information) that can describe a particular wireless channel and achieve a desired performance. Note that a good quantization performance also depends on the choice of quantization thresholds. A single threshold will lead a low generation rate while multi-level thresholds are susceptible to the random noise. In this survey, we will take a review on the wireless channel reciprocity based key establishment techniques that differ each other in terms of the selection of quantization channel metrics and thresholds.
2. *Reconciliation and privacy amplification* As we mentioned earlier, information reconciliation and privacy amplification are two indispensable components of the wireless key establishment. We combine them in one category because they are closely correlated to generate a shared secret key from the wireless channel. In reconciliation, devices need to exchange some channel information to correct mismatch bits. Thus, the goal of reconciliation is to minimize the channel information

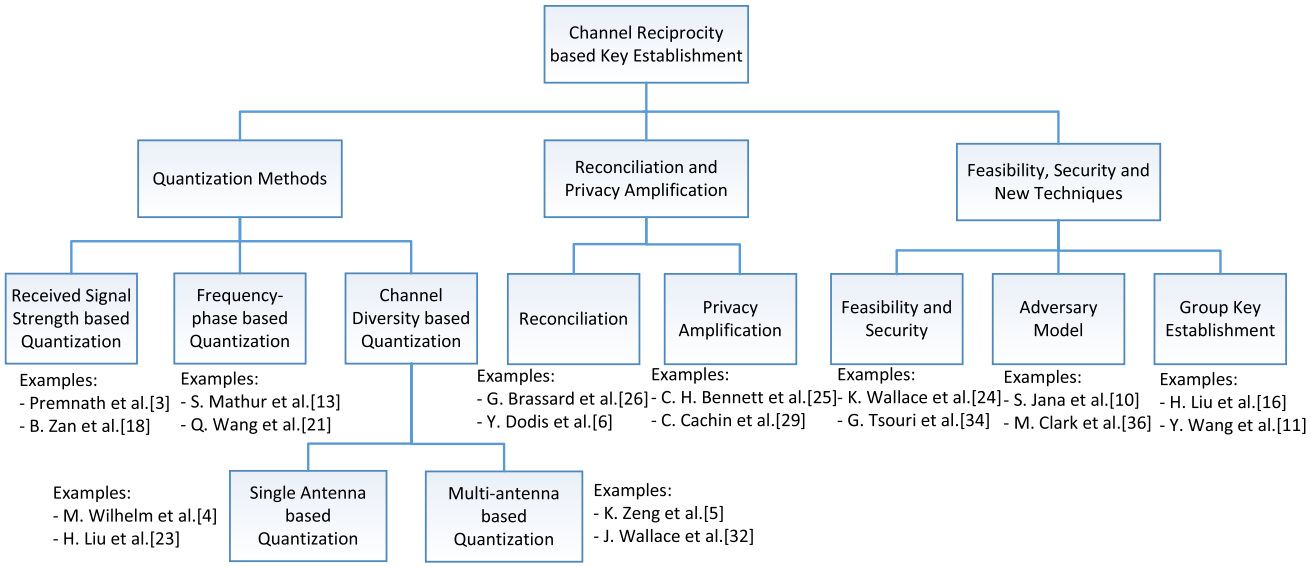


Fig. 2 The taxonomy of wireless key establishment techniques

exchanged between the communicators, so that the chance of information leakage can be reduced. Similarly, privacy amplification aims at "amplifying" the difficulty of an eavesdropper to deduce the shared secret based on the channel information exchanged in reconciliation. In this survey, we will discuss the existing methods that concern these two steps, and examine how both steps collaborate with each other to achieve an adequate key generation rate with minimum information leakage.

3. *Feasibility and security* Since many schemes have been proposed to achieve wireless channel reciprocity based key establishment, it is essential to analyze the feasibility of them when they are used in a practical scenario. We would like to evaluate their performance under different situations and to investigate the certain requirements they should satisfy to guarantee the generation of secret keys. On the other hand, using wireless channel reciprocity information to establish a shared secret key is still a developing field, and multiple attacks against such techniques have been discovered. For example, an eavesdropper may launch proximity attack (e.g., [2]), in which the eavesdropper infers the secret key established between the target communicators through physically approaching to the communicators or predicting the channel characteristics between them. In this survey, we will take a look at the threats and vulnerabilities of channel reciprocity based key establishment, and the corresponding countermeasures. Figure 2 gives a summary of these key establishment techniques.

The remaining sections are organized as follows. The next section describes the common metrics that evaluate the key establishment techniques. Section 3 discusses the quantization methods in previous work. Section 4 presents the existing approaches on reconciliation and privacy amplification. Section 5 talks about the feasibility, security and emerging new techniques of wireless key extraction. Section 6 concludes this survey.

2 Evaluation metrics

To facilitate the discussion of key establishment techniques, we describe the following important terms that are frequently used to assess the performance of these techniques.

2.1 Entropy

Entropy refers to the uncertainty associated with a random variable. It is used to evaluate the security strength of the shared secret key. Normally, a higher entropy means a larger uncertainty of a random variable. Thus, an eavesdropper can hardly deduce a secret key of a high entropy. The definition of entropy is as follows:

$$H_i = -p_0 \log p_0 - (1 - p_0) \log(1 - p_0)$$

and

$$H_{total} = \sum_{i=0}^{N} H_i,$$

where N represents the total length of the secret key, and p_0 denotes the posterior probability when the bit is 0 from the eavesdropper knowledge.

2.2 Bit mismatch rate

Bit mismatch rate is the difference between the initial bit sequences obtained by the transmitter and the receiver. It is the ratio of the number of mismatch bits to the total number of bits output by the quantization. It is a parameter to evaluate the performance of the quantization. A large bit mismatch rate indicates that the quantization method is more susceptible to random channel noise and the imperfect reciprocity.

2.3 Key generation rate

key generation rate is defined as the number of secret keys generated per unit time. This term is crucial to describe the overall performance of secret key establishment techniques. With a high generation rate, two wireless devices can establish a shared secret key in a short time, thereby achieving a high communication efficiency.

3 Quantization methods

Quantization is the first step of wireless key establishment. The initial idea of quantization is using thresholds to quantize the sample values into binary bits based on certain channel metrics. To give a better review of quantization, we describe an example that uses RSS to achieve the quantization. Each point on Fig. 3 is a sample value and the quantizer has two fixed thresholds (0.3 and 0.7). The sample value will be encoded as 1, when it is larger than the high threshold 0.7, or encoded as 0, when it is smaller than the low threshold 0.3. Other values between the two thresholds will be dropped.

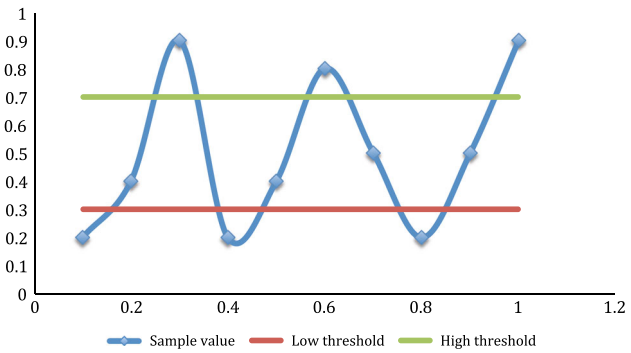


Fig. 3 RSS based quantization

Current research focuses on how to identify and utilize appropriate channel metrics to improve the entropy and the efficiency of the quantization. We classify these quantization methods into three categories based on the channel metrics they select. In general, RSS, CIR, and frequency-phase information are used as channel metrics for the purpose of quantization.

3.1 Received signal strength (RSS) based quantization method

Received signal strength is the most widely used channel metric in quantization, because the amplitude of a received signal is easy to measure and is varying from different channels [3, 16–18]. The basic idea of RSS based quantization is illustrated in Fig. 3. As discussed above, the quantizer uses two fixed thresholds to encode sample values into a binary sequence.

However, using fixed thresholds makes the quantization susceptible to the varying environment and active attacks, where adversary tries to decrease or increase the RSS by inserting or moving the intermediate objects between the transmitter and the receiver. Further, the method fails to exploit the sampled values between thresholds. These values may provide additional information to generate the secret key. Aware of these drawbacks, several adaptive approaches are proposed to improve the performance of quantization.

In order to eliminate the impact of predictable component related to distance and overcome active attack, in [3] the authors propose a method named Adaptive Secret Bit Generation (ASBG). The quantizer divides the sampled values into blocks and each block has its own thresholds based on its average and standard deviation. So each block will do quantization independently and this makes the ASBG adaptive to varying environment. In addition, the size of each block is configurable, so the communicators may choose proper size to accommodate different wireless channels.

Although ASBG solves the active attack issues by adapting the threshold based on the current environment, the quantization is still suffering from the impact of random channel noise. The sample values between the two thresholds are not exploited either. To reduce the effect of random noise and extract more secret bits, the authors of [18] propose to generate a secret key using the relative difference between sample values. In this method, the quantizer performs the local average over every D sample values to eliminate the short-term fluctuation caused by the random noise, and it chooses the certain length of uncorrelated samples as the window size to quantize the sample values. Unlike ASBG, this approach doesn't use the absolute signal amplitude, instead the quantizer determines

the output based on the relative signal amplitude difference. In addition, it enforces more thresholds to further increase the amount of secret bits.

The scheme proposed in [18] gives us another angle to do the quantization and it makes an efficient utilization of the sampled values. In addition, it mitigates the impact of random noise. However, we still expect a fast key generation rate. Also, none of the previous schemes take the imperfect reciprocity into consideration. The imperfect channel reciprocity is mainly caused by half-duplex property of a practical wireless system. To further improve the key generation rate and to deal with the imperfect reciprocity, in [16] the researchers combine the two previous schemes and uses both local average and individual sampled values to perform the quantization. This approach applies a new scheme of interpolation on the top of sample values to offset the asymmetry between the transmitter and receiver in their sampling rate. After sampling, the quantizer uses multiple thresholds to quantize the sample values and a single threshold to quantize the local average, because the quantization of local average and sample values are two independent procedures. The technique proposed in [18] can get more uncorrelated bits in a short time, and thus it achieves a larger entropy and a higher generation rate.

3.2 Frequency-phase based quantization method

Because RSS is a distance related parameter, the RSS based quantization techniques do not work well for wireless networks that consist of static nodes. In such networks, wireless channels remain unchanged due to the lack of the mobility. To establish the shared secret key in static wireless networks, new methods (e.g., [2, 19–21]) have been proposed based on the channel frequency-phase information, which is uncorrelated with the distance between communicators.

A basic prototype design of frequency-phase based quantization is proposed in [2]. The proposed approach obtains the channel frequency-phase information by collecting consecutive estimates of the channel frequency phase, and then it uses multiple thresholds to map each collected phase into particular binary bits. Because the channel frequency-phase is not correlated with the transmission distance, the method in [2] can establish a secret key with high randomness. Later, the authors of [21] propose an enhanced method that exploits uniform distributed frequency-phase information of a narrow band multipath fading models to establish the secret key.

Such a method uses a time-slotted round-trip protocol to establish the pairwise key. Both the transmitter and receiver independently choose random frequency-phases that are uniformly distributed in a certain interval. Then, they transmit and receive signals in different time slot. After phase estimation, the frequency-phase information will not only correlate with the channel characteristics but it is also related to the initial choices made by the communicators. Finally, the method applies multiple thresholds to quantize each estimated frequency-phase.

In practice, the observed frequency-phase is usually divided into several regions for quantization, and wrong decisions can be made if the estimated frequency-phases are close to the region boundaries. Thus, the authors of [22] propose a guard-interval based scheme to reduce the error rate in the region boundaries. The sampling procedure is the same as the previous frequency-phase based quantization methods (e.g., [2, 19–21]). After the frequency-phase sampling, the quantizer determines the quantization thresholds and chooses a guard interval. The estimated frequency-phases that fall in this guard interval are discarded to reduce the bit error rate. The technical challenge is how to choose a proper guard interval. A large interval leads to a low key generation rate while a small interval causes a high bit error rate. To deal with this challenge, in [22] it creates a bit disagreement function that establishes the relationship between the guard interval, the quantization level, and the signal-to-noise ratio, and then finds the optimal guard interval that balances the key generation rate and the bit error rate.

3.3 Channel diversity based quantization method

Both RSS and frequency-phase based methods generate the secret key from a single frequency with a single antenna. They quantize one sample value at a time, and thus can only provide coarse-grain information of the wireless channel. This means that the key generation rate is still quite limited. Although multiple thresholds can increase the key generation rate of secret bits, the improvement is restricted because using too many thresholds may make the quantization susceptible to random channel noise. Hence, it is highly desirable to find a new way to improve the key generation rate and key entropy.

It has been long observed that a wireless signal sent by the transmitter usually propagates to the receiver in the air along multiple pathes due to reflection, diffraction, and scattering. Thus, people have proposed to exploit the multipath feature of wireless signals to significantly increase the key generation rate. In what follows, we discuss these approaches.

3.3.1 Single antenna based quantization

Intuitively, since a wireless channel can be modeled as a multipath-fading channel, we can use the channel state information to further increase the amount of secret bits

generated during a short time. The *channel impulse response*, a metric to depict the multipath channel state, can be represent as follows:

$$h(t) = \sum_{l=0}^{L-1} h_l \delta(t - \tau_l),$$

where δ is the unit impulse function, L is the number of channel paths, h_l denotes the l-th path complex gain, and τ_l represents the delay of the signal traveling on the l-th path. Herein, each channel tap (i.e., a multiple path) is regarded as independent from each other. Thus, the receiver can quantize each tap separately and combine the output to achieve a high key generation rate. Channel estimation based quantization normally estimates the multipath channel, and then quantizes each channel tap into channel impulse response. In the following, we give a detail review of these methods.

Wireless channels are usually frequency selective. Thus, a small change of frequency will cause an unpredictable variation in signal strength. Towards this observation, in [4] the authors introduce a scheme that exploits the frequency diversity to generate secret keys. This scheme measures the RSS values from a set of different channel frequencies. For each frequency, it samples the channel impulse response several times and calculates the average to reduce the influence of random noise. Then, quantizer applies multiple thresholds to quantize the average of the sampled channel impulse responses into a binary bit sequence. The advantage of such a scheme is that it doesn't depend on the movement of the wireless nodes and is capable of supporting the wireless sensor networks that usually consist of static nodes, like wireless sensor network.

The method proposed in [4] uses the frequency diversity to achieve a significant speed-up of the key generation rate. However, the values sampled from different frequencies may interfere each other. Consequently, these values are indeed correlated and result in a reduced key generation security. To solve this problem, the Orthogonal Frequency Division Multiplexing (OFDM) can be applied to minimize the frequency interference. OFDM modulates the data stream into multiple subcarriers with different frequencies that are orthogonal to each other, and it enables a simple equalizer to easily estimate the channel taps in the frequency domain. The following two quantization schemes are based on OFDM.

In [22] the authors propose a scheme to achieve the secret key establishment by quantizing each tap gain of an OFDM system. It first estimates the channel impulse response in the frequency domain, and then transfers the estimated channel impulse response into the time domain by applying Fourier Transformation. The proposed method quantizes sampled channel impulse responses based on the frequency-phase instead of the amplitude, because the amplitude of each tap gain may provide information for an adversary to deduce the secret key (e.g. the amplitude of the first arrival signal is the largest). Finally, it applies a guard-interval based method to map the frequency-phases into binary bits.

Due to the adoption of OFDM, the method proposed in [22] can generate secret keys at a fast rate without introducing the interference. But it doesn't take non-reciprocity factors (e.g. antenna gain and RF front attenuation) into consideration when estimate the channel. These factors cause the asymmetry between the transmitter and the receiver and may increase the bit mismatch rate. As an enhancement, in [23] the researchers propose a scheme to eliminate the non-reciprocity factors by applying the channel gain complement (CGC) algorithm. The CGC algorithm estimates the channel impulse response based on certain collected wireless signals to eliminate the non-reciprocity factors. After estimating the reciprocity factors, this scheme quantizes the channel impulse response of each subcarrier frequency in the frequency domain. The detailed quantization procedure is similar to [22].

3.3.2 Multi-antenna based quantization

Besides using a single antenna with different frequencies to estimate the channel and generate the shared key, some studies explore the possibility of using multiple antennas to achieve an improved performance in key generation(e.g., [5, 24]). Wireless signals normally experience various channel effect between different antennas, so the schemes can yield more secret bits per unit time than single antenna single frequency based quantization.

In [5], the authors propose a Multiple Antenna Key Generator (MAKG) protocol to exploit the spatial diversity in a real wireless environment. The protocol makes the maximum utilization of the multi-antenna diversity. In the sampling step, it collects the channel state information for each pair of antennas. Suppose each node has N antennas. After the channel estimation, each node can get N^2 channel state information per sample interval. This means that a long secret key with rich entropy can be generated. The remaining steps are similar to the RSS-based quantization methods. The quantizer applies multiple quantization thresholds to convert the collected channel state information into binary bits.

Unlike [5], in [24] it proposes a frequency-phase based quantization scheme that explores the diversity of a Multiple-input and Multiple-output (MIMO) system. The quantization of each channel is exactly the same as what described in [22], where a guard interval is placed to avoid

Table 1 Comparison of different quantization methods

	RSS based quantization	Frequency-phase based quantization	Channel diversity based quantization	
			Single antenna based quantization	Multi-antenna based quantization
Feasibility	Easy to implement	Frequency-phase estimation is not trivial	Need to send multiple frequencies	Need extra hardware
Entropy	Low, distance-related parameter	High, hard to predict	High, multiple frequencies	High, multiple antennas
Mismatch bits	Use average value to reduce the impact from the channel noise	Use guard interval to decrease the bit mismatch rate	NA	NA
Key generation rate	Low, single frequency single antenna	Low, single frequency single antenna	High, multiple frequencies	High, multiple antennas

bit errors. Similar to [5], for a M-input and M-output MIMO system, M^2 channels can be estimated to gather a large number of binary bits and increase the entropy of the final secret key.

3.4 Summary and open research issues

Table 1 shows the summary of these quantization methods. The RSS based quantization methods are easy to implement, but they are predictable since RSS values are closely related to the distance between the transmitter and the receiver. To increase the security, frequency-phase based quantization methods have been proposed to generate the secret keys by exploiting the frequency-phase information that is normally independent from the distance. However, the implementation of such methods are non-trivial since the estimation of the frequency-phase is not easy. Recently, researchers proposed to explore the multipath channel diversity to achieve a high key generation rate, and they demonstrated that such approaches can significantly boost the key generation rate. We foresee that this research trend will continue to generate more efficient quantization algorithms that exploit the channel diversity for shared key establishment.

However, the performance of current quantization techniques is still limited by certain issues. The first issue is channel asymmetry. Since the transmitter and the receiver observe different channels due to imperfect reciprocity and random noise, the bit sequences generated by them will always have a certain amount of mismatch bits using current quantization methods. Normally, for the same channel the longer the bit sequences are, the more the mismatch bits will occur in these sequences. Second, Current techniques highly depend on a fast changing environment to ensure a quick key generation rate. In a static situation, the channel changes so slowly that the schemes can hardly obtain enough uncorrelated bits in a short time. Several schemes have been proposed to address this issue. However, the key generation rate is still low and accordingly the security of the schemes is reduced. We expect that in the future the quantization methods could be improved to eliminate the impact caused by the channel asymmetry. Thus, the bit sequences generated by the quantization methods can be used as the secret key directly. Further, we also hope that the future quantization methods can be applied to explore the channel in a static situation and guarantee a fast key generation rate.

4 Reconciliation and privacy amplification

According to the channel reciprocity property, the transmitter and the receiver should observe the same quantization output. However, due to imperfect reciprocity and random noise, there may exist a small number of mismatch bits between two outputs. Thus, reconciliation and privacy amplification are applied to achieve an identical final secret key.

Reconciliation is the process of finding and correcting mismatch bits of the quantization outputs generated at the transmitter and the receiver. As shown in Fig. 4, during the reconciliation, the bit correcting information is exchanged through the public channel, and thus an eavesdropper may learn part of the secret key by wiretapping the channel

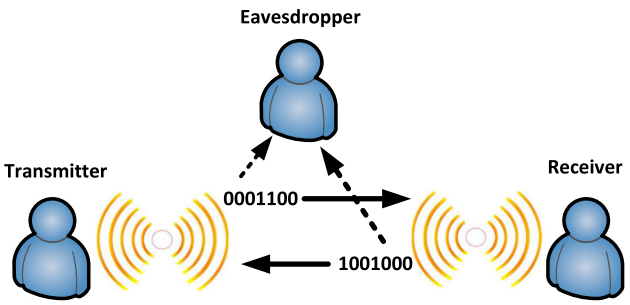


Fig. 4 Eavesdropping during the information reconciliation

communication. Privacy amplification is then launched to eliminate the use of the bit correcting information in the final key generation. In this section, we will review the existing approaches on reconciliation and privacy amplification.

4.1 Reconciliation

Reconciliation is applied to correct the mismatch bits between the transmitter and the receiver through public channels. Since the transmitter and the receiver must share certain information to achieve the agreement on the bit sequences, the critical problem of reconciliation is how to correct these mismatch bits with a minimum amount of exchanged information.

Based on the intuition that the error correction codes can identify and correct the bit errors, the authors of [6] propose a simple reconciliation scheme that applies a $[n, k, 2t + 1]$ error-correction code to correct the mismatch bits, where n is the length of codeword, k is the length of the code, and t is the maximum number of bit errors that the code can correct. However, as pointed out in [25], the efficiency of this approach drops dramatically with the increasing of the key size.

In [25], the authors propose a practical way to achieve reconciliation. Prior to the key establishment, both the transmitter and the receiver agree on a random permutation that permutes their quantization outputs. Such a permutation enables the communicators to randomize the positions of mismatch bits. Then, the transmitter and the receiver further divide their permutation results into multiple blocks. The size of a block should be carefully chosen so that the expected number of mismatch bits in each block is less than or equal to 1. The transmitter and the receiver then exchange and compare their block parity. If the parity is the same, then they reach the agreement on the corresponding block. Otherwise, they use the binary search to correct the mismatch bits. The approach proposed in [25] is a typical way to achieve the reconciliation and it discloses only a small amount of bits quantized from the wireless channel.

An alternative reconciliation scheme is further proposed in [26] to achieve an improved performance as compared to [25]. This approach uses several passes to correct the mismatch bits. The operation of each pass is the same as that described in [25]. However, different passes use different block sizes and permutations. Another difference between [25] and [26] is that the former discards the last bit of each block to prevent the adversary deducing the parity of this block, whereas the latter doesn't discard any bits so that it can correct more mismatch bits.

All of the approaches mentioned above focus on the reconciliation of binary random variables. They pay less attention to nonbinary random variables. In [27], it investigates the reconciliation approaches targeting nonbinary random variables. In [27], the transmitter and the receiver encode the quantization output, which is modeled as Gaussian random variables, into n-bit codewords. They then add parity bits to the encoding result and further convert the encoding result into low-density parity-check (LDPC) codes. With the LDPC codes, the transmitter and receiver can compare their parity bits, correct the mismatch portion, and decode the exact Gaussian random variables into binary bits that will construct the shared secret key.

4.2 Privacy amplification

After reconciliation, the transmitter and the receiver can eliminate mismatch bits and reach the agreement on the shared secret key. However, as mentioned earlier, this step inevitably discloses a small amount of information about the shared key. To enhance the security and amplify the difficulty for the attacker to guess the shared key, privacy amplification approaches (e.g., [7, 28, 29]) have been therefore proposed, and they achieve this goal by slightly reducing the length of the secret key.

Privacy amplification was first introduced in [7], which designs amplification protocols based on different eavesdropper models. The authors assume that the transmitter and the receiver can communicate through both public and private channels, and they take three eavesdropper models into consideration. In the first model, the eavesdropper can get the complete access to the public channel, and the amount of bit errors introduced by the private channel is small. In the second model, the eavesdropper not only gets complete access of public channel but it also obtains partial information from the private channel. Similar to the first model, the second model assumes that the amount of bit errors caused by the private channel is small. In the third model, the eavesdropper can wiretap the public channel and part of the private channel. Moreover, the private channel is highly unreliable and the data transmitted through the private channel may be tampered arbitrarily.

To deal with these eavesdropper models, the paper relies on the construction of a function $g : (0, 1)^n \rightarrow (0, 1)^r$, which can eradicate the leaking information on both the public and private channels by shrinking the final shared key size from n bit to r bit, where $r < n$. In [29], it proposes an efficient implementation of such a function. In [29], the function g is generated based on a publicly known set of universal hush functions (e.g., [30]) that map a n-bit input to a r-bit output. Further, the authors of [28] give a comprehensive theoretical analysis of the feasibility of achieving an efficient privacy amplification, and it discusses the practical implementation of universal hashing functions as well.

4.3 Summary and open research issues

Reconciliation and privacy amplification are always combined to gain the key agreement between the transmitter and the receiver, and to reduce the chance for an adversary to infer the final secret key. In reconciliation, the key agreement is achieved by sharing some bit mismatch information through the public channel. While privacy amplification eliminates such shared information to prevent an eavesdropper learning the secret key. Because reconciliation and privacy amplification are still within the scope of information theory. Their practical implication on real-world wireless communication systems are still unknown and under-explored. It would be desirable for researchers to integrate the existing theoretical results on reconciliation and privacy amplification into a practical wireless system, and reveal the implementation feasibility and the actual performance of them. Besides, since reconciliation and privacy amplification require Alice and Bob to exchange massages over the public channel, the sensitive information may be disclosed. Researchers may explore the other opportunities to deal with the mismatch bits (e.g. auto-correct code or perfect channel symmetry).

5 Feasibility, security and new techniques of key extraction

In this section, we will present three key factors that substantially affect the feasibility and security of key extraction: channel reciprocity, spacial decorrelation, and key extraction rate. In addition, we will discuss adversary models with strong capabilities and corresponding countermeasures, and also describe a recent emerging scheme, called group key extraction.

5.1 Feasibility and security of wireless key extraction

The work in [8] and [31] theoretically analyze the secret key generation based on the correlated randomness of wireless channel. The paper shows that two parties can achieve a secret key agreement in the scenario, where the signal is transmitted through the public area in the presence of a third party, who is the eavesdropper. It was shown that channel reciprocity and spacial decorrelation are two essential components to establish a secure transmission for this scenario. In the following, we summarize the research on the feasibility of using these two properties for key establishment.

First, channel reciprocity is a fundamental property for the transmitter and receiver to establish a shared key. The work in [23] gives an analysis on why and how to get the initial secret keys with this property. Assuming that channel estimations for the transmitter and the receiver are $H(a)$ and $H(b)$, it shows that if they obtain $H(a)$ and $H(b)$ within a short time duration, the channel reciprocity will ensure a high correlation between $H(a)$ and $H(b)$, which means an increasing in $H(a)$ will result in an increasing in $H(b)$, and vice versa. Thus, the two parties can use the high correlated channel estimation to achieve the initial secret key.

Second, wireless channels are spatially correlated. Therefore, we may extracted correlated keys from correlated channels. It is essential to ensure channels between different transmitter-receiver pairs are independent of each other with spacial decorrelation. For a security perspective, secret keys related to different channels should be distinct with high probability, which means that eavesdropper should keep a certain distance from both receiver and transmitter to ensure a uncorrelated link. Recently, the work in [2] and [32] focuses on investigating the impact of the eavesdropper's distance to the receiver. In [32], a function of the distance between the eavesdropper and the receiver was constructed to evaluate the ratio of susceptible secret bits to the total secret bits based on a variety of factors, such as the presence of line of sight (LoS), number of multipath and number of antennas. Experiments were used in [2] to evaluate the eavesdropper's capability of deducing the key as a function of its distance from the receiver. The measurements show that a distance of half a wavelength will result in a 50 % mismatch of secret keys between the eavesdropper and the receiver, based on which the threshold of the distance can be obtained to guarantee the complete secrecy of generated keys.

In addition to channel reciprocity and spacial decorrelation, key generation rate is very important to the security strength of secret keys. In practical, a fast key generating rate is required to build a fast and secure link between the transmitter and the receiver. However, wireless channel status is not only spatially-correlated but also temporally-correlated. As a result, frequent key extraction from the same wireless channel unavoidably leads to the correlation between consequent extracted keys, thereby degrading the security that those keys can provide. The work in [9, 33] and [34] studied this fundamental limits on secrecy capacity and energy per bit in key agreement. In [34], an information-theoretical approach is used to evaluate the the secrecy capacity of keys. It shows that the achievable key generation rate largely relies on the channel conditions. Specifically, the capacity of channel between the transmitter and the receiver must be larger than the capacity between the eavesdropper and the transmitter to ensure a secure transmission. In [33], the minimum energy requirement per bit was studied for a reliable key generation rate under low SNR. The minimum energy requirement of generating a fixed length secret key was evaluated

as a function of error probability during the key establishment. It was shown that under certain conditions, a proper key generation rate can be achieved with high security strength.

5.2 Adversary models against key establishment

The adversaries against key establishment are usually assumed to have limited capabilities: although they can listen to all the communication through the public channel, they can neither be too close to the transmitter and the receiver, nor jam or modify the communication between the transmitter and the receiver. However, recent analysis has shown that prior assumption is not necessarily valid [10, 35]. In the following, we summarize recently proposed adversary models against wireless key establishment.

In [16], the paper presents a passive adversary called stalker, which can follow the trajectory of either the transmitter or the receiver, and gain the communication between them. The stalker always keeps a certain distance from the transmitter or the receiver to prevent exposing itself. Because of this, even though the stalker can trace the trajectory of either transmitter or receiver, it cannot obtain the same channel estimation and thus fails to extract the identical secret key. The measurements in [16] also show that the mismatch bit probability between the stalker and either the transmitter or the receiver is much higher than that between the transmitter and the receiver.

The work in [10] proposes an attack model in RSS based key establishment, which may happen when both of the receiver and transmitter are stationary or move slowly. In this case, the adversary uses planned movement to make the desired and predictable change in channel measurements between the transmitter and the receiver. To deal with the attack, the paper proposes to estimate channel with channel state information (CSI) at each subcarrier. It shows that different subcarriers do not experience the same trend like RSS does. Hence, when the attacker manages to change the environment, it is still hard for it to predict the fluctuation of CSI at each subcarrier.

The adversary model in [36] assumes that the attacker can either manipulate the environment or predict the effect of environments on the wireless channel. It was pointed out in [36] that a typical key extraction protocol will fail to defend against this powerful adversary. To combat such an adversary, the paper proposes an improved key extraction protocol, which consists of entropy harvesting and entropy Management. In entropy harvesting, a key is extracted repeatedly instead of refreshed only when needed. All the updated keys are placed into a key pool. In entropy management, the state of each key is maintained to guarantee that a key with strong security will be selected to secure an authorized connection. As we can see, more sophisticated key establishment schemes are vital to handle more powerful attacks to ensure strong security, reliability and robustness for key extraction.

5.3 Group key establishment

In general, wireless key establishment is used to build a secure connection between two parties. However, in a broadcast or multicast scenario, it is necessary to establish a collaborative key among a group of wireless devices. Key establishment concerning the shared group key is discussed in [11] and [16]. In a group key establishment scheme, each node keeps a matrix, which includes the values measured from all its channels to its neighbors. Two group key establishment schemes are proposed in [16] for two different scenarios.

- If every wireless node is within each other's communication range, a star-based key establishment protocol is designed to obtain the secret key. In particular, each device within a group needs to estimate the channel between a randomly selected device and the central device. Based on the same channel estimation, the devices will be able to share the secret key.
- If not every device is in each others's range, a chain-based key establishment protocol is used to establish the secret key, which involves relay nodes to obtain the shared key. In this protocol, each device within a group needs to estimate the same channel between two certain devices. And channel information will be transmitted to each device through relay nodes, thus allowing the group to share the same secret key.

The star-based and chain-based protocols can be used at one-hop and multi-hop network scenarios respectively, for proper group key establishment.

5.4 Summary and open research issues

Wireless channels exhibit various properties, including channel reciprocity, spatial and temporal uncorrelations. The channel reciprocity is the foundation for the transmitter and the receiver to generate a common secret key from the wireless channel, and the security of the established key is guaranteed by the varying channel. Yet, spatial and temporal correlations have adverse effects on the performance and security of key establishment. As discussed earlier, more strong adversary models have been proposed to attack existing key establishment protocols from different aspects. In the future, channel reciprocity based key establishment schemes can further exploit the channel randomness to yield more uncorrelated bits. In addition, predictable components of the channel (e.g. received signal strength, the value related to the distance)

should be addressed to avoid the leakage of the key. Finally, techniques such as friendly jamming can also be introduced to assist these schemes to keep the channel information away from the eavesdroppers. Therefore, we can expect more sophisticated schemes and countermeasures will be designed with the increased capability of adversaries.

6 Conclusion

In this survey, we reviewed the existing research effort on the channel reciprocity based key establishment from three perspectives. First, we discussed the different types of quantization techniques, which convert the unique wireless channel features into binary bits. Second, we described the main reconciliation and privacy amplification techniques, which enable the establishment of a shared secret key in the presence of eavesdroppers. Third, we discussed the feasibility, security issues, and emerging techniques in this research field.

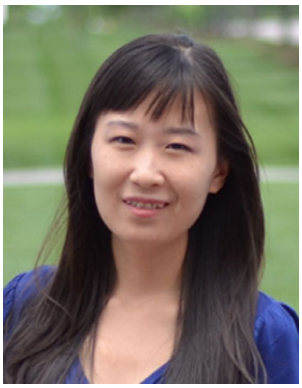
Using wireless channel characteristics to establish a shared secret key is becoming a proliferate area for its high reliability, easy implementation, and low energy consumption. However, the key generation rate is relatively low in some special scenarios like a static wireless enviorment. In addition, the mismatch bits introduced by channel asymmetry are still an issue that should be solved. Further, adversaries are evolving with stronger ability and higher stealthiness, and they raise a big security concern for wireless key establishment techniques. Consequently, seeking more sophisticated key generation protocols is still necessary and challenging in the future.

References

1. Chang, R. Y., Lin, S. J., & Chung, W. H. (2013). Diffie–Hellman key distribution in wireless multi-way relay networks. In *Proceedings of signal and information processing association annual summit and conference* (pp. 1–4).
2. Mathur, S., Miller, R., Varshavsky, A., Trappe, W., & Mandayam, N. (2011). Proximate: Proximity-based secure pairing using ambient wireless signals. In *Proceedings of ACM Mobisys*, New York, NY, USA.
3. Premnath, S. N., Jana, S., Croft, J., Gowda, P. L., Clark, M., & Kasera, S. K., et al. (2013). Secret key extraction from wireless signal strength in real environments. *IEEE Transaction on Mobile Computing*, *12*(5), 917–930. doi:10.1109/TMC.2012.63.
4. Wilhelm, M., Martinovic, I., & Schmitt, J. B. (2010). Secret keys from entangled sensor motes: Implementation and analysis. In *Proceedings of ACM WiSec* (pp. 139–144)
5. Zeng, K., Wu, D., Chan, A., & Mohapatra, P. (2010). Exploiting multiple-antenna diversity for shared secret key generation in wireless networks. In *Proceedings of IEEE INFOCOM* (pp. 1–9). doi:10.1109/INFCOM.2010.5462004.
6. Dodis, Y., Ostrovsky, R., Reyzin, L., & Smith, A. (2008). Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM Journal on Computing*, *38*(1), 97–139. doi:10.1137/060651380.
7. Bennett, C. H., Brassard, G., & Robert, J. M. (1988). Privacy amplification by public discussion. *SIAM Journal on Computing*, *17*(2), 210–229.
8. Maurer, U. (1993). Secret key agreement by public discussion from common information. *IEEE Transaction on Information Theory*, *39*(3), 733–742.
9. Chou, T. H., Draper, S., & Sayeed, A. (2012). Key generation using external source excitation: Capacity, reliability, and secrecy exponent. *IEEE Transaction on Information Theory*, *58*(4), 2455–2474.
10. Jana, S., Premnath, S. N., Clark, M., Kasera, S. K., Patwari, N., & Krishnamurthy, S. V. (2009). On the effectiveness of secret key extraction from wireless signal strength in real environments. In *Proceedings of ACM Mobicom* (pp. 321–332).
11. Wang, Y., Damodaran, D., & Le, P. D. (2006). Efficient group key management in wireless networks. In *Proceedings of information technology: New generations (ITNG)* (pp. 432–439).
12. Liu, Y., Draper, S., & Sayeed, A. (2012). Exploiting channel diversity in secret key generation from multipath fading randomness. *IEEE Transaction on Information Forensics and Security*, *7*(5), 1484–1497. doi:10.1109/TIFS.2012.2206385.
13. Mathur, S., Trappe, W., Mandayam, N., Ye, C., & Reznik, A. (2008). Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel. In *Proceedings of MobiCom* (pp. 128–139).
14. Ali, S., Sivaraman, V., & Ostry, D. (2010). Secret key generation rate versus reconciliation cost using wireless channel characteristics in body area networks. In *Proceedings of IEEE/IFIP EUC* (pp. 644–650).
15. Zhu, X., Xu, F., Novak, E., Tan, C., Li, Q., & Chen, G. (2013). Extracting secret key from wireless link dynamics in vehicular environments. In *Proceedings of IEEE INFOCOM* (pp. 2283–2291).
16. Liu, H., Yang, J., Wang, Y., & Chen, Y. (2012). Collaborative secret key extraction leveraging received signal strength in mobile wireless networks. In *Proceedings of IEEE INFOCOM* (pp. 927–935).
17. Patwari, N., Croft, J., Jana, S., & Kasera, S. (2010). High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. *IEEE Transaction on Mobile Computing*, *9*(1), 17–30.
18. Zan, B., Gruteser, M., & Hu, F. (2012). Improving robustness of key extraction from wireless channels with differential techniques. In *Proceedings of IEEE ICNC* (pp. 980–984).
19. El Hajj Shehadeh, Y., Alfandi, O., & Hogrefe, D. (2012). On improving the robustness of physical-layer key extraction mechanisms against delay and mobility. In *Proceedings of IEEE IWCMC* (pp. 1028–1033).
20. Sayeed, A., & Perrig, A. (2008). Secure wireless communications: Secret keys through multipath. In *Proceedings of IEEE ICASSP* (pp. 3013–3016).
21. Wang, Q., Su, H., Ren, K., & Kim, K. (2011). Fast and scalable secret key generation exploiting channel phase randomness in wireless networks. In *Proceedings of IEEE INFOCOM* (pp. 1422–1430) . doi:10.1109/INFCOM.2011.5934929.
22. El Hajj Shehadeh, Y., & Hogrefe, D. (2011). An optimal guard-intervals based mechanism for key generation from multipath wireless channels. In *Proceedings of IFIP NTMS* (pp. 1–5). doi:10.1109/NTMS.2011.5720584.
23. Liu, H., Wang, Y., Yang, J., & Chen, Y. (2013). Fast and practical secret key extraction by exploiting channel response. In

Proceedings of IEEE INFOCOM (pp. 3048–3056). doi:10.1109/INFCOM.2013.6567117.
24. Wallace, J., Chen, C., & Jensen, M. (2009). Key generation exploiting mimo channel evolution: Algorithms and theoretical limits. In *Proceedings of EuCAP* (pp. 1499–1503).
25. Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., & Smolin, J. (1992). Experimental quantum cryptography. *Journal of Cryptology*, *5*(1), 3–28.
26. Brassard, G., & Salvail, L. (1994). Secret-key reconciliation by public discussion. In *Workshop on the theory and application of cryptographic techniques on advances in cryptology*.
27. Bloch, M., Barros, J., Rodrigues, M. R. D., & McLaughlin, S. (2008). Wireless information-theoretic security. *IEEE Transaction on Information Theory*, *54*(6), 2515–2534.
28. Bennett, C., Brassard, G., Crepeau, C., & Maurer, U. (1995). Generalized privacy amplification. *IEEE Transaction on Information Theory*, *41*(6), 1915–1923.
29. Cachin, C., & Maurer, U. M. (1997). Linking information reconciliation and privacy amplification. *Journal of Cryptology*, *10*(2), 97–110.
30. Carter, J. L., & Wegman, M. N. (1977). Universal classes of hash functions (extended abstract). In *Proceedings of the ACM symposium on theory of computing*, pp. 106–112 (1977).
31. Ahlswede, R., & Csiszar, I. (1993). Common randomness in information theory and cryptography. I: Secret sharing. *IEEE Transaction on Information Theory*, *39*(4), 1121–1132.
32. Wallace, J., & Sharma, R. (2010). Automatic secret keys from reciprocal mimo wireless channels: Measurement and analysis. *IEEE Transaction on Information Forensics and Security*, *5*(3), 381–392.
33. Chou, T. H., Sayeed, A., & Draper, S. (2009). Minimum energy per bit for secret key acquisition over multipath wireless channels. In *Proceedings of IEEE ISIT* (pp. 2296–2300).
34. Tsouri, G., & Wagner, D. (2013). Threshold constraints on symmetric key extraction from rician fading estimates. *IEEE. Transaction on Mobile Computing*, *12*(12), 2496–2506.
35. Döttling, N., Lazich, D., Müller-Quade, J., & Almeida, A. (2011). *Vulnerabilities of wireless key exchange based on channel reciprocity*. Berlin: Springer.
36. Clark, M. (2012). Robust wireless channel based secret key extraction. In *Proceedings of IEEE Milcom* (pp. 1–6).

Tao Wang is a currently a Ph.D. student in the Department of Computer Science and Engineering, University of South Florida, Tampa, FL. His research interests include wireless network and mobile security, cyber-physical system security.



Yao Liu received the Ph.D. degree in Computer Science from North Carolina State University in 2012. She is now an assistant professor at the Department of Computer Science and Engineering, University of South Florida, Tampa, FL. Dr. Liu's research is related to computer and network security, with an emphasis on designing and implementing defense approaches that protect emerging wireless technologies from being undermined by adversaries. Her research interest also lies in the security of cyber-physical systems, especially in smart grid security. Dr. Liu's research work has appeared in premier journals and conferences including ACM Transactions on Information and Systems Security, IEEE Symposium on Security and Privacy (IEEE S&P), ACM Conference on Computer and Communications Security (CCS), and IEEE International Conference on Computer Communications (INFOCOM). She was the recipient of Best Paper Award for the 7th IEEE International Conference on Mobile Ad-hoc and Sensor Systems.

Athanasios V. Vasilakos breceived the Ph.D. degree in computer engineering from the University of Patras, Patras, Greece, in 1988. He is currently Professor at the Department of Computer and Telecommunications Engineering, University of Western Macedonia, Kozani, Greece, and visiting Professor at the Graduate Program of the Department of Electrical and Computer Engineering, National Technical University of Athens (NTUA), Athens, Greece. He has authored or coauthored over 200 technical papers in major international journals and conferences. He is author/coauthor of five books and 20 book chapters in the areas of communications. Dr. Vasilakos served as General Chair, Technical Program Committee (TPC) Chair, and Symposium Chair for many international conferences. He served or is serving as an Editor or/and Guest Editor for many technical journals, i.e., the IEEE Transactions on Network and Service Management, the IEEE Transactions on System, Man, and Cybernetics-Part B: Cybernetics, the IEEE Transactions on Information Technology in Biomedicine, and the IEEE Journal on Selected Areas in Communications. He is the founding Editor-in-Chief of the International Journal of Adaptive and Autonomous Communications Systems (IJAACS, http://www.inderscience.com/ijaacs) and the International Journal of Arts and Technology (IJART, http://www.inderscience.com/ijart). He is Chairman of the European Alliance for Innovation.