DOI: 10.3969/j. issn. 1673-5188. 2013. 03. 003
http://www.cnki.net/kcms/detail/34.1294.TN.20130911.1354.001.html, published online September 11, 2013

Methodologies of Secret-Key Agreement Using Wireless Channel Characteristics

Syed Taha Ali and Vijay Sivaraman
(School of Electrical Engineering and Telecommunications, University of New South Wales, NSW 2052, Australia)

Abstract

In this article, we give an overview of current research on shared secret-key agreement between two parties. This agreement is based on radio wireless channel characteristics. We discuss the advantages of this approach over traditional cryptographic mechanisms and present the theoretical background of this approach. We then give a detailed description of the key-agreement process and the threat model, and we summarize the typical performance metrics for shared secret-key agreement. There are four processes in shared secret-key agreement: sampling, quantization, information reconciliation, and privacy amplification. We classify prior and current research in this area according to innovation on these four processes. We conclude with a discussion of existing challenges and directions for future work.

Keywords

physical-layer security; secret key generation

1 Introduction

The Diffie-Hellman key exchange protocol is the de facto mechanism for cryptographic secret-key agreement [1]. Relying on the intractability of the discrete logarithm problem, two parties with no prior knowledge of each other are able to exchange public messages over an insecure communications channel and arrive at a shared secret key that is safe from an eavesdropper and that can be used for encrypting communications between themselves. Research interest has recently revived an alternative approach to secret-key agreement. Two parties (Alice and Bob) who are communicating using radios can exploit unique spatio-temporal properties of the wireless channel between them to generate a shared secret. Due to the highly unpredictable and symmetric nature of multipath propagation, the wireless channel that Alice and Bob share is unique to them. It is reciprocal and cannot be deduced in detail by an eavesdropper (Eve). The wireless channel is also highly sensitive to motion and changes in the environment, and variations can be quantized independently by Alice and Bob to yield a shared secret key that Eve has no access to.

This approach has several advantages. First, security implemented at higher layers in the protocol stack can be undermined at the lower layers, and an argument has been made that security should be implemented at multiple layers, if possible. An early research effort in this domain [2] strongly emphasized that physical layer security can complement existing cryptographic solutions and help build systems that are more secure overall. The physical layer has, thus far, mostly been neglected in the stack. This is unfortunate because the physical wireless link can be a rich source of randomness, (due to signal noise and highly sensitive channel states). The physical wireless link is also a means of deriving shared secrets because of the high correlation in channel characteristics at two ends of a link. These advantages can be easily harnessed because most radios today already have hardware support for performing basic channel estimates, such as measuring radio signal strength.

Second, prevailing cryptographic techniques are based on difficult number theory problems, i.e. these techniques rely on certain assumptions about the adversary´s computing power. In contrast, physical layer approaches offer information-theoretic security, also referred to as unconditional security. Even with unlimited computing power, advances in number theory, and the advent of quantum computing, an adversary still cannot break information-theoretic schemes.

Third, traditional cryptographic mechanisms can be resource-intensive and impractical to implement in hardware. This is especially critical for newly emerging computing paradigms, such as Smart Dust, RFID chips, body area networks, and the Internet of Things, which are all based on miniaturized, resource-constrained wireless devices. Devices such as wireless sensors are not typically equipped with secure clocks or powerful pseudorandom number generators, in which case

the Diffie–Hellman key exchange may not lead to truly random keys. Furthermore, research indicates that the Diffie–Hellman key exchange is not very practical to execute on sensor devices [3].

Secret–key agreement using wireless channel characteristics is essentially a four–step process. Alice and Bob first sample the wireless channel to obtain correlated estimates of the channel state. They individually quantize these estimates to yield closely matching bit sequences, or bitstrings. This is followed by an information reconciliation process in which Alice and Bob identify and correct mismatching bits in their bitstrings. Then, there is a privacy amplification step in which a transform operation is used to minimize Eve´s knowledge of the shared bitstring. The result is a secret key shared by Alice and Bob that they can use to encrypt communications between themselves. Research in this domain has mostly focused on innovating at different steps of the key–agreement process, and this technique has been validated using different wireless technologies and in various environments.

In section 2, we briefly introduce secret–key agreement using wireless channel characteristics. We discuss the threat model, and we summarize the performance metrics most commonly used. In section 3, we give an overview of existing research in this domain, categorized as per the four steps of the process, i.e. sampling, quantization, information reconciliation, and privacy amplification. In section 4, we discuss alternative methods of using the wireless channel for secret–key agreement. We also discuss potential attacks in this space and outline possible directions for future work. Section 5 concludes the paper.

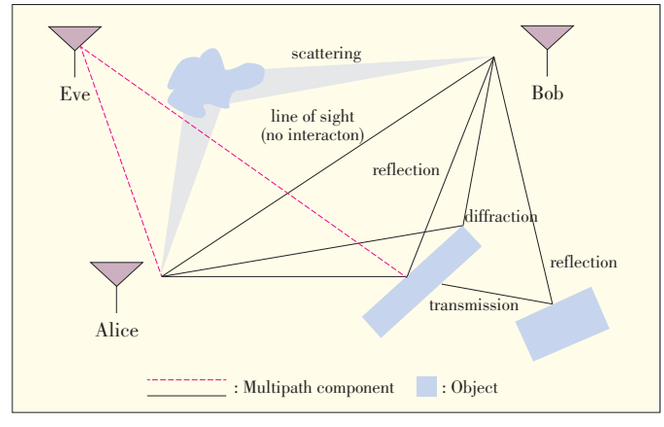
2 Basic Principles

The groundwork for physical layer security was laid in 1975, when Wyner introduced the classic wiretap model [4] and demonstrated that two parties (Alice and Bob) could communicate securely without a shared secret key and assuming that the illegal channel that Eve uses for eavesdropping is a noisier version of the legitimate Alice–Bob channel. The trick here is for Alice and Bob to use sufficiently large code words to encode their messages and to prevent Eve from successfully deciphering the noisier version of data that she receives. In the early nineties, Maurer [5], [6] proved that Alice and Bob could communicate securely with even fewer restrictions. Even if Eve has access to a less noisy channel than the Alice–Bob channel, Alice and Bob can still agree on a shared secret key if they generated correlated random sequences and then harmonized their observations by exchanging public messages on an error–free channel. The process could be devised using obfuscation techniques so that even if Eve were to access these public messages, her knowledge of the shared secret would still be negligible.

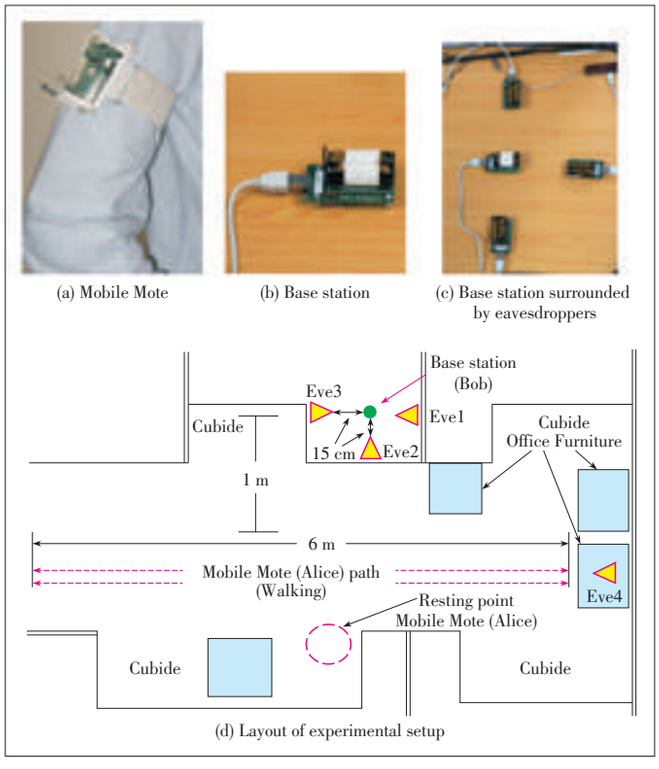
The concept of two parties generating correlated random sequences, perfected via public discussion and obfuscated from third parties, is very applicable to the wireless medium. The wireless channel has an intrinsic symmetry because of the reciprocity of electromagnetic propagation. If Alice and Bob were to transmit identical signals to each other, using identical transceivers and antennas and in the absence of interference and noise, they would receive perfectly identical signals. Radio signals take multiple paths from the source to the destination where, depending on the particular path, they undergo reflection, diffraction, and scattering. The signals also experience different amounts of delay, attenuation, and phase distortion. Alice and Bob can both therefore measure a set of parameters defined by the cumulative effects of all these paths on the signal at their ends. In ideal conditions, these measurements agree.

If Alice and Bob collect a time series of these channel state measurements over a period of sufficient variation, the channel state profile (or envelope) can be directly quantized into a shared secret key that is unique to their positions in that particular environment at that point in time. If Eve is located more than one radio wavelength away from either Alice or Bob, she will be limited to measuring an entirely different channel and will not be able to deduce the legitimate channel spectra or the shared secret. This concept, is shown in **Fig. 1** and described by a Jake uniform scattering model [7], which is well–known in the field. According to this model, there is a rapid decorrelation in the signal over a distance of approximately half a wavelength, and for a separation of one to two wavelengths or more, the signals can be assumed to be independent. In the 2.4 GHz range, our threat model would require Eve to be situated 6.25 cm or more away from Alice and Bob.

Fig. 2 shows an indoor office environment at the Faculty of Electrical Engineering, University of New South Wales. A base station (Bob) communicates with a wearable mobile device (Alice) walking along the path illustrated. Multiple stationary eavesdroppers (Eve 1 and Eve 4) are in close to the base station, separated by a distance of 15 cm on either side. Alice and Bob send messages at a rate of 1 packet per second, sampling



▲**Figure 1. Multipath propagation in indoor setting.**



▲ **Figure 2. Mobile node, base station, and experimental layout for indoor environment.**

the channel in succession, and all parties record the received signal strength indication (RSSI) as an estimation of the channel state. **Fig. 3** shows the channel state measured over a one minute interval. Alice and Bob are in very good agreement with slight discrepancies with regard to the channel profile. Furthermore, the eavesdroppers drop a large number of packets and are unable to replicate the channel profile in significant detail. This confirms that Alice and Bob can use these measurements to generate shared secret keys.

In practice, all parties experience low-amplitude asymmetric components in their channel measurements because of factors such as random noise, transceiver differences, interference, motion, or sampling delay (caused by half-duplex radios). Quantizing these channel estimations may therefore result in discrepancies in the generated bit sequence. Information-reconciliation protocols are used to resolve these disagreements. In these protocols, Alice and Bob publicly exchange data about their bit sequences (through, for example, parity checks) to identify and correct mismatching bits. This is followed by a privacy amplification step, which eliminates the partial information that Eve has deduced about the shared secret. This step usually involves a transformation operation, such as using a hash function.

Typically, key agreement, secret bit generation rate, entropy, and implementation costs and overheads are the performance metrics used to measure the efficiency of wireless channel-based key agreement.

Key agreement is the fraction of matching bits in the sequences generated by Alice and Bob. Ideally, this should be 100%, and whatever mismatches occur (due to practical considerations) are resolved using information reconciliation. Very high agreement rates, i.e. greater than 99% , have been achieved in the literature [8]. Eavesdroppers, on the other hand, should match in about 50% of the bits they generate by listening to the Alice-Bob transmissions. The probability of eavesdroppers guessing the right bit is equivalent to a fair coin toss, i.e. there is no advantage at all.

The secret bit generation rate is the average number of usable secret key bits extracted from the wireless channel per unit time. This value depends on various factors, such as the channel sampling rate, quantization parameters, deployment scenario, and channel variability. Bit generation rates in the literature range from 1 bit/s [2] to 40 bits/s [9].

Entropy is a measure of the uncertainty or inherent randomness in the generated bits. Typically, the entropy of a random variable X over a set of n symbols x_1, x_2,..., x_n is given by

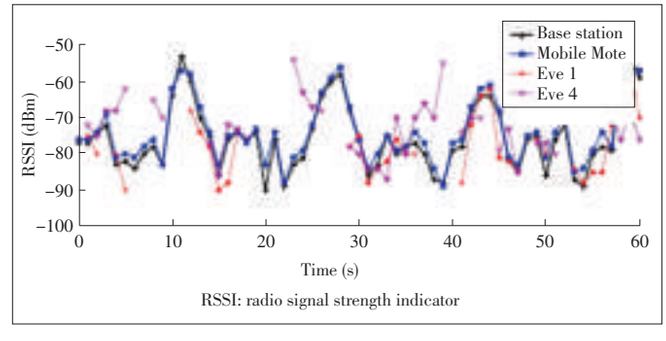
$$H(X) = -\sum_{i=1}^{n} p(x_i)\log_2 p(x_i) \quad (1)$$

where $p(x_i)$ is the probability of the occurrence of symbol x_i. For binary symbols, a value close to 1 indicates high entropy. In the literature, the NIST test suite [10] is typically used to validate the entropy for the generated bits.

Implementation cost and overheads depend on the particular mechanism used to generate bits. Whereas this technique has been demonstrated to work with off-the-shelf hardware, in instances such as that in [11], specialized hardware is required. Furthermore, information reconciliation mechanisms, such as Cascade, require storage and repeated manipulation of large arrays of data. Large-scale data transmission involves significant processing costs [12], which is a serious consideration for resource-constrained devices, such as wireless sensors.

3 Process

In this section, we describe current research on shared se-

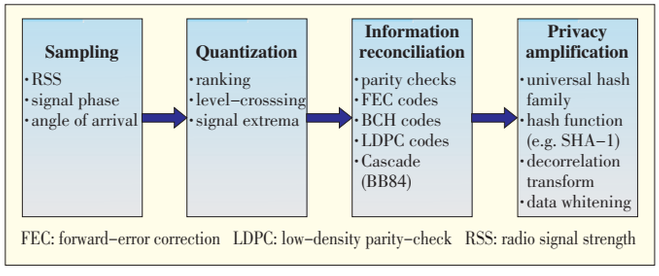


▲ **Figure 3. Measurements comparing RSSI in an indoor office environment.**

cret key agreement using the wireless channel. A pictorial summary is shown in **Fig. 4**.

3.1 Channel Sampling

Various wireless channel characteristics have been investi-



▲**Figure 4. Classification of methodologies for secret-key agreement.**

gated in the literature. Radio signal strength (RSS), discussed in [2], [13] and [14], is the most popular characteristic because it already exists in most off-the-shelf radios. Schemes using signal phase [15], angle of arrival [11], and deep fades [16] have also been successfully used for secret-key agreement.

It is imperative that there is sufficient fluctuation in the channel over a period of time so that the generated key has acceptable entropy. This can be a problem in static deployments, and motion on the part of Alice or Bob has been recommended in several research efforts [13], [17]. An alternative approach to generating signal variation in a static setting is channel-hopping. The wireless channel is also frequency-sensitive, so channel characteristics can be measured over a range of frequencies to generate a shared secret [14].

Non-identical hardware may result in Alice and Bob having different channel state measurements. Experiments performed by Jana et al. [13] have shown that heterogeneous hardware may result in a consistent value offset at the two ends, and the resulting channel profile is relatively consistent for Alice and Bob. For this reason, instead of encoding absolute channel measurements, the profile or envelope is quantized to produce secret-key bit sequences.

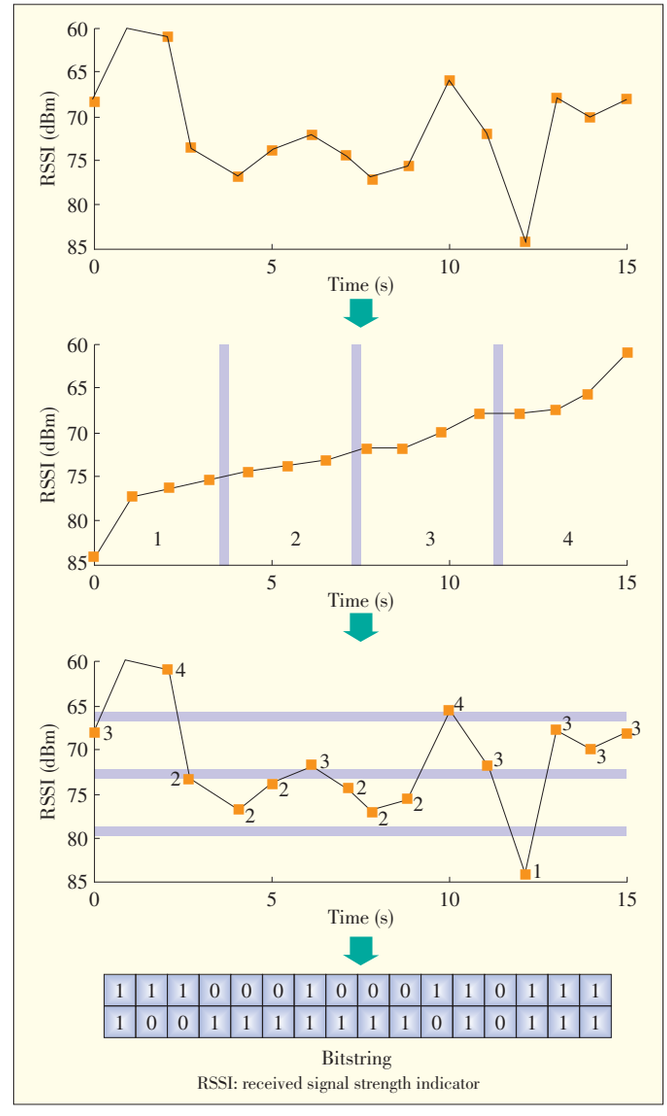
3.2 Quantization

Quantization is the process by which the sampled channel estimates are mapped to a specific bit sequence. Common approaches to quantizing the channel profile include ranking, level crossing, and using signal extrema. Rank quantization involves "bucketizing" the channel estimates in a manner that ensures an equally probable bit distribution. The buckets can be assigned single or multiple bits, and in the case of the latter, Gray coding is used to demarcate adjacent buckets. Gray coding is a binary numbering system where successive values differ in only one bit. It is used instead of binary coding so that discrepancies in measurements, which may cause a value to be assigned to a different bucket between Alice and Bob, will at most lead to a disagreement in only one bit. This process is shown in **Fig. 5**. Rank quantization is performed in [17] and [9].

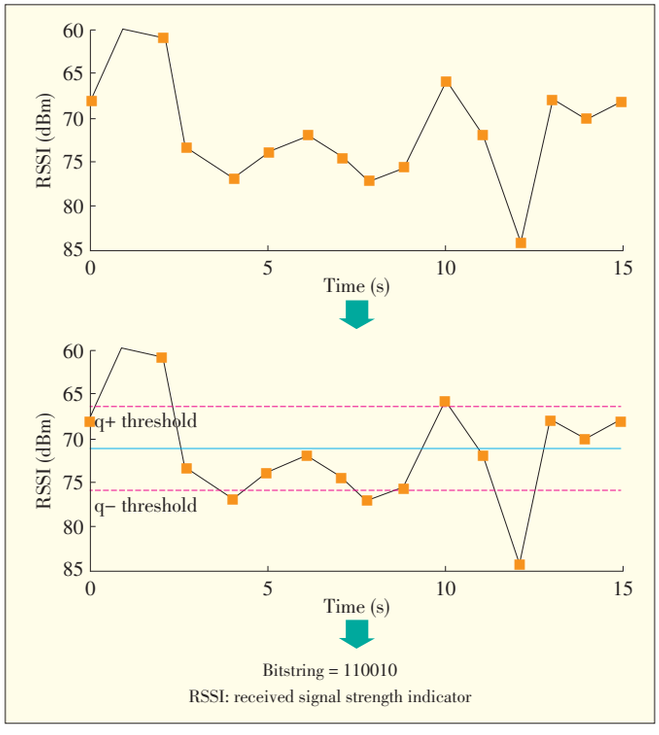
The level-crossing technique involves superimposing certain thresholds onto the channel profile and assigning bit values whenever a threshold is crossed. Variations on this basic concept have been developed to suit application requirements. For example, Mathur et al. [2] propose a quantizer (**Fig. 6**) that uses a moving window in which each block is assigned two threshold values:

$$q+ = \mu + \alpha.\sigma$$
$$q- = \mu - \alpha.\sigma \quad (2)$$

where μ is the mean, σ is the standard deviation, and $\alpha \geq 0$ is an adjustable parameter. If an RSSI reading within a window is greater than $q+$, it is encoded as 1. If an RSSI reading within a window is less than $q-$, it is encoded as 0. The thresholds de-



▲**Figure 5. Rank quantization.**



▲Figure 6. Level–crossing quantization.

fine a censor zone, and values lying within this zone are discarded. This concept is similar to a guard band. The rationale for discarding such values is to filter out random noise effects or asymmetric components that are typically low–amplitude and liable to cause bit disagreement between the two parties.

3.3 Information Reconciliation

Much of the research on information reconciliation has been done in the context of quantum cryptography. Discrepancies in the bitstrings generated over the quantum channel occur because of eavesdropping or imperfections in the transmission media. Researchers have sought secure and efficient mechanisms to reconcile these bitstrings. Information reconciliation attempts a form of error correction using the public channel. To reconcile their bit sequences, Alice and Bob exchange metadata (usually parity information) to identify mismatching bits. At the same time, they simultaneously try to minimize the potential leakage of information to an eavesdropper. If mismatching bits are identified, they are either discarded or corrected. This concept is similar to the cyclic redundancy check used to detect data corruption and is also probabilistic, which means only a specific class of errors can be handled. Various error–correction codes, including BCH [11] and LDPC [18], have been used for reconciliation.

Cascade [19] is the most popular information–reconciliation protocol and works iteratively in an interactive manner. Alice permutes her bit sequence randomly, divides it into blocks, computes the parity on each block, and sends the permutation and parity information to Bob, who then performs the same process at his end. If parity does not match for certain blocks, Bob performs a binary search to identify the minimum number of bits that he can change to match the parity check. This process is then repeated multiple times with different permutations of the bit sequence to identify which bits need to be corrected. The probability of success can be fine–tuned by specifying an adequate block size and the number of passes of the protocol.

3.4 Privacy Amplification

Privacy amplification is necessary because successive wireless channel estimates may be correlated in time, and this leads to predictability in portions of the bit sequence. Privacy amplification is also necessary because the information reconciliation process may reveal some information about the sequence to eavesdroppers. To effectively decorrelate successive bits in the sequence and nullify any knowledge an eavesdropper may have about parts of the key, an obfuscation operation is performed. Typically, Alice and Bob use universal hash functions chosen from a public set of such functions. This results in smaller, fixed–size bit sequences that can be used as a secret key.

4 Future Directions

In this section, we briefly discuss a few promising directions for future work in secret–key agreement using wireless channel characteristics.

Several research efforts have already resulted in proof–of–concepts for wireless–channel–based secret–key agreement in different environments. Jana et al. [13] investigated the efficacy of this approach in buildings, cafeterias, and tunnels as well as on a lawn or road. The authors also investigated the efficacy of this approach for various modes of activity, such as a sitting, walking, or riding a bike. Wilhelm et al. [14] characterize the channel frequency response for static configurations. In [8], we adapted this mechanism for wearable health monitoring devices and presented experimental results.

However, significant work still needs to be done before secret–key agreement using wireless channel characteristics can actually be deployed in everyday, usable technology. Thus far, research on this technique has mostly relied on offline analysis of trace data, and there is a lack of actual prototype solutions implemented on user platforms, such as mobile phones and sensor devices. Running these solutions on user devices would require significant engineering and optimization, which has yet to be done.

Furthermore, wireless channel–based attacks have only just begun to be examined seriously. An early attack, also called a predictable channel attack, was described by Jana et al. in [13]. The authors demonstrated that, in a stationary environment, an attacker may be able to cause predictable variations in RSS by repeatedly blocking the line of sight between Alice

and Bob. Likewise, Mathur et al. [2] discuss an attack where Eve might spoof Alice and Bob. The authors show how that can be detected easily using RSS authenticators. These attacks are relatively simple and can be easily avoided by taking a few precautions. However, some very recent research indicates that multiple eavesdroppers might be able to collude to obtain a greater portion of the quantized bit sequence, even up to approximately 70% agreement with Alice and Bob. This is a serious concern. Such attacks, detailed in [20] and [21], are ad hoc in nature and have so far only been experimentally demonstrated. We suggest there needs to be a thorough inquiry into the theoretical basis for such attacks before solutions can be sought. There also needs to be corresponding research on adequate privacy amplification mechanisms in this domain. So far, this area has been neglected.

5 Conclusion

In this paper, we have briefly introduced current research on wireless channel-based secret-key agreement. We have highlighted the advantages of and challenges related to this technique. We have provided the requisite theoretical background and elaborated on the component processes, sampling, quantization, information reconciliation, and privacy amplification of this technique. We have also summarized certain challenges in this domain, such as the urgent need for practical implementations and the lack of comprehensive theory on threats and attacks. We believe there is great potential for wireless-channel-based secret-key agreement, especially with the advent of new resource-constrained computing paradigms, such as body area networks, mobile computing, and the internet of things.

References

[1] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.
[2] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret Key from an unauthenticated wireless channel," In *ACM MobiCom*, San Francisco, CA, 2008, pp. 128–129.
[3] E. Blass and M. Zitterbart, "Efficient implementation of elliptic curve cryptography for wireless sensor networks," University at Karlsruhe, Tech. Rep., 2005.
[4] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[5] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
[6] U. M. Maurer, "Perfect cryptographic security from partially independent channels," in *Proc. STOC'91*, New Orleans, pp. 561–571.
[7] W. C. Jakes, *Microwave Mobile Communications*, New York: Wiley, 1974.
[8] S. T. Ali, V. Sivaraman, and D. Ostry, "Zero reconciliation secret key generation for body-worn health monitoring devices," in *Proc. WISEC'12*, Tucson, USA, pp. 39–50.
[9] J. Croft, N. Patwari, and S. Kasera, "Robust uncorrelated bit extraction methodologies for wireless sensors," in *Proc. IPSN'10*, Stockholm, Sweden, pp. 70–81.
[10] L. E. Bassham III, et al., "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST, Tech. Rep. SP 800-22 Rev. 1a., 2001.
[11] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Transactions on Antennas and Propagation*, vol. 53, no. 11, pp. 3776–3784, Nov. 2005.
[12] P. Bellot and M. Dang, "BB84 implementation and computer reality," *IEEE RIVF*, Da Nang, Jul. 2009, pp. 1–8.
[13] S. Jana, S. N. Premnath, M. Clark, S. Kasera, N. Patwari, and S. Krishnamurthy, "On the effectiveness of secret key extraction using wireless signal strength in real environments," *ACM MobiCom*, Beijing, 2009, pp. 321–332.
[14] M. Wilhelm, I. Martinovic, and J. B. Schmitt, "Secret keys from entangled sensor motes: implementation and analysis," *ACM WiSec*, Hoboken, NJ, 2010, pp. 139–144.
[15] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Transactions on Communications*, vol. 43, no. 1, pp. 3–6, 1995.
[16] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," *ACM CCS*, Alexandria, USA, 2007, pp. 401–410.
[17] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High rate uncorrelated bit extraction for shared key generation from channel measurements," *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 17–30, 2010.
[18] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240–254, 2010.
[19] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Proc. EUROCRYPT'93*, Lofthus, Norway, pp. 410–423.
[20] M. Edman, A. Kiayias, and B. Yener, "On passive inference attacks against physical-layer key extraction?" in *Proc. EUROSEC'11*, Salzburg, Austria, article no. 8.
[21] S. Eberz, M. Strohmeier, M. Wilhelm, and I. Martinovic, "A practical man-in-the-middle attack on signal-based key generation protocols," *Computer Science*, vol. 7459, pp. 235–252, 2012.

Manuscript received: July 11, 2013

Biographies

Syed Taha Ali (taha@unsw.edu.au) received his BSc.(Eng) degree from the GIK Institute of Engineering Sciences and Technology, Pakistan, in 2002. He received his MSc from the University of New South Wales, Australia, in 2006. He recently concluded his PhD degree at UNSW, writing a thesis on developing novel security mechanisms for body sensor networks. His research interests include wireless sensor networks, network mobility, software defined networks, and applied network security. His work has appeared at ACM WiSec, IEEE SECON, IEEE BodyNets and IEEE TrustCom. He has been published in journals such as *IEEE Transactions on Mobile Computing* and *Elsevier Future Generation Computer Systems*. He is currently working as a postdoctoral researcher in the School of Electrical Engineering, UNSW.

Vijay Sivaraman (vijay@unsw.edu.au) (M '94) received his BTech. degree from the Indian Institute of Technology, Delhi, in 1994. He received his MS degree from North Carolina State University in 1996. He received his PhD degree from the University of California, Los Angeles, in 2000. He has worked at Bell-Labs and at a Silicon Valley start-up, where he was involved in manufacturing optical switch routers. He is currently an associate professor in the School of Electrical Engineering and Telecommunications, UNSW, and a visiting researcher at the CSIRO ICT Centre. He has considerable experience working with network routing protocols and QoS mechanisms and has initiated and led projects on optical networking, energy-efficient networks, power optimization and security protocols for wearable devices, and sensor networks for air pollution monitoring. His work has appeared at conferences such as IEEE INFOCOM and ACM CoNEXT and has been published in prestigious journals such as *IEEE/ACM Transactions on Networking*, *IEEE Journal of Selected Areas in Communication*, and *IEEE Transactions on Image Processing*.