On the security of UWB secret key generation methods against deterministic channel prediction attacks

S.Tmar-Ben Hamida*, J-B.Pierrot*, B.Denis*, C.Castelluccia†, B.Uguen‡
*CEA-LETI, Minatec Campus, 17 rue des Martyrs 38054 Grenoble, France
Email: [sana.ben-hamida, jean-benoit.pierrot, benoit.denis]@cea.fr
†INRIA Rhône-Alpes, 655 Av de l´Europe, Montbonnot, 38334 Saint Ismier Cedex, France
Email: claude.castelluccia@inria.fr
‡IETR-UMR 6164, Université de Rennes 1, 263 Av du Général Leclerc, 35042 Rennes, France
Email: bernard.uguen@insa-rennes.fr

Abstract—**Generating secret keys in mobile wireless networks is considered a challenging problem where a key management infrastructure is not always available. Recent security methods have shown that secret keys can be generated using Ultra Wide Band (UWB) channels. These solutions rely on relevant channel properties such as reciprocity and spatial decorrelation. Accordingly, the radio channel responses can be used as common information to derive secret keys shared by legitimate parties. However, novel studies in the field of UWB channel prediction have demonstrated that channel profiles could be reliably inferred using for instance Ray-Tracing tools. This paper explores this technique to perform attacks and to evaluate the security of UWB secret key generation methods. The main observation here is that it is difficult for a third party to obtain the exact channel responses; thus to retrieve the secret keys. The robustness of UWB key generation methods then depends on the complexity for attackers to describe precisely the physical environment and on the post processing methods to agree on the same key (i.e., quantization, erroneous bits detection, etc.).**

I. Introduction

Securing a wireless network is a challenging problem due to the shared broadcast medium that makes it easy to eavesdrop on communication, record and modify transmitted packets by adversaries. Conventional symmetric cryptography is required to establish communication confidentiality. Therefore, a trusted party must be developed to generate and share secret keys. However, such conditions are not usually available for dynamic wireless networks.

Novel security methods [1], [2], [3] and [4] propose to use Ultra Wide Band (UWB) channel features to derive secret keys. These solutions rely on the *reciprocity* principle that states that: in the absence of interferences and non-symmetric components, both the emitter and the receiver experience the same channel response (CR) [5]. This shared information can be used to generate a secret key. In addition, the channel profile *decorrelates rapidly in space* in multipath radio environments. In fact, for a given emitter, waveforms travel differently from one receiver location to another. As a result, an eavesdropper cannot obtain the same CR and thereafter will be unable to extract the shared key, which guarantees its secrecy.

However, in spite of favourable UWB properties, radio CRs can be inferred using existing simulation tools. In the field of radio propagation prediction, significant advances have indeed been achieved for the last past years, and more particularly regarding the site-specific deterministic Ray-Tracing methods [6]. Recent results show that these simulators allow to generate realistic received multipath profiles, which are resulting from superposed 'rays' (e.g., [7], [8], [9] and [10]). The crucial information required for these tools are: the transmitter and receiver positions, the waveform feeding the transmit antenna, the antenna angular radiation pattern and the description of the operating environment (e.g. electromagnetic characteristics of surrounding materials, building geometry, etc.).

To the best of our knowledge, Ray-Tracing (RT) based attacks have not been considered previously to show the channel based encryption key strength. The aim of this paper is to test the security of secret key generation method based on UWB channel responses against channel prediction attacks. Two scenarios are considered. First, the attacker tries to derive the emitter-receiver channel responses assuming a known receiver location. The second scenario consists in performing a brute-force attack to determine the most likely receiver location through cross-correlation. For the legitimate parties, we use real UWB channel measurements to generate secret keys. The resulting information is then compared to the attacker keys, which are obtained by simulation using the RT channel prediction tool.

This paper is organized as follows: Section II presents the principle of secret key generation based on radio channel characteristics. Section III outlines the principle of UWB site-specific deterministic Ray-Tracing methods. Section IV describes the adversary's scenarios using this technique and discusses the simulation results, followed by the conclusion.

II. Secret key derivation based on UWB channel response

The concept for building secret keys from UWB channel responses ([1], [2], [3] and [4]) exploits special properties of

978-1-4673-1881-5/12/$31.00 ©2012 IEEE

the wireless channel such as: *the reciprocity* and *the spatial decorrelation*. Electromagnetic theory indicates that in the absence of non-symmetric components, the radio channel responses between any two endpoints are reciprocal during the coherence time and decorrelate rapidly in space [5]. As a consequence, the underlying channel responses can be used as common sources to generate secret keys. These properties have been validated for the UWB communications in a typical indoor environment (e.g. [11], [12]).

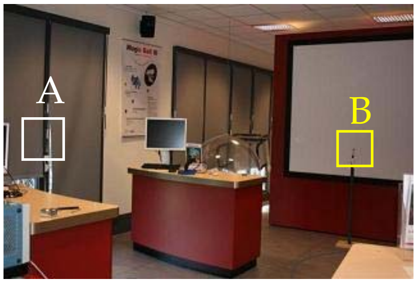


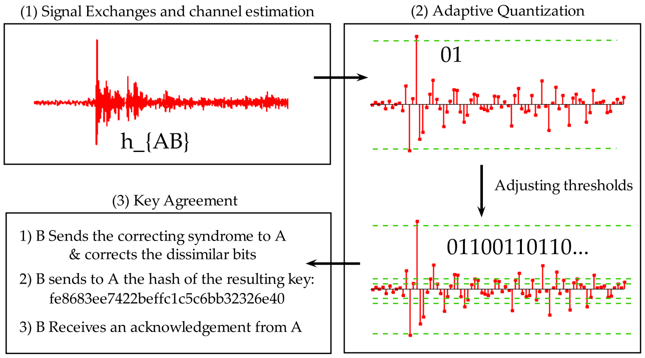
Fig. 1. The indoor environment considered for UWB channel measurements. A is the emitter while B is the receiver.

Suppose two parties A and B want to establish a secret communication without the help of a key management authority, as shown in figure 1. These nodes must perform three main stages to obtain correlated information and to confirm the same secret key, as summarized in figure 2:

Phase 1- The communicating nodes A and B exchange a known shape pulse $s(t)$. During this operation, the environment must be quasi-stationary (movements should be minimized). Next, the channel responses are estimated by A and B: $\hat{h}_{BA}(t) = h_{BA}(t) + n_A(t)$ and $\hat{h}_{AB}(t) = h_{AB}(t) + n_B(t)$ respectively where $\hat{h}_{BA}(t)$ and $\hat{h}_{AB}(t)$ are the estimates of the channel responses $h_{BA}(t)$ and $h_{AB}(t)$. The noise signals $n_A(t)$ and $n_B(t)$ refer to the errors in the estimates, which can be considered as zero-mean Gaussian noises. The true channel responses are assumed to be similar due to the reciprocity hypothesis (i.e. $h_{BA}(t) \equiv h_{AB}(t)$).

Phase 2- The channel estimations are translated to binary vectors using an adaptive quantization algorithm [4]. This method has the advantages to create sufficiently long secret keys with a high key agreement ratio between authorized users while reducing the revealed information to the attacker.

Phase 3- The resulting binary vectors may present some errors due to the measurement noise. Therefore, each node proceeds by correcting the dissimilar bits using an algebraic coding method (e.g. the Reed Solomon code [13]). Then, a hash is generated to check for agreement between nodes. Finally, if a positive acknowledgement has been received a secure communication can be initiated using the shared key. In contrast, if the nodes do not agree on the same key, the previous steps are repeated.


(1) Signal Exchanges and channel estimation
h_{AB}
(2) Adaptive Quantization
01
Adjusting thresholds
01100110110...
(3) Key Agreement

1) B Sends the correcting syndrome to A & corrects the dissimilar bits

2) B sends to A the hash of the resulting key: fe8683ee7422beffc1c5c6bb32326e40

3) B Receives an acknowledgement from A

Fig. 2. Different steps of secret key generation based on channel measurements. In (1), a signal s(t) is received by node B. Then, the latter estimates the channel response h_{AB} which is converted to binary vector using a quantization algorithm (2). Finally, the resulting sequence is corrected and verified to agree on the same secret key (3).

III. Ray Tracing Concept

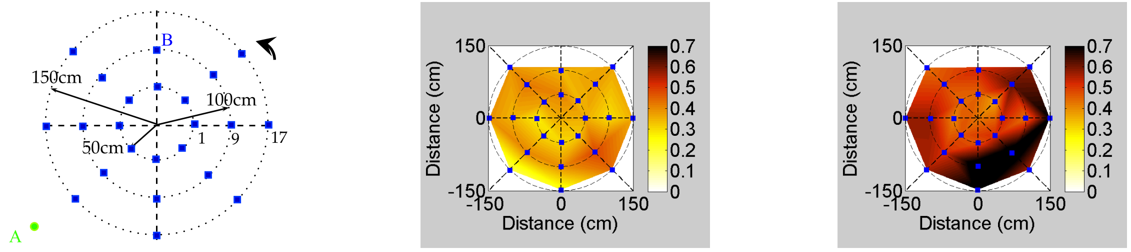
Several site-specific deterministic tools, such as Ray-Tracing simulators, have been recently developed. The major goal of these techniques is to offer an accurate knowledge of the radio channel propagation (e.g. coverage prediction or radio planning). The main objective of this paper is to use a RT simulator in the security context. Specifically, we test the robustness of the secret key generation method described in section II against channel prediction attacks.

A Ray-Tracing simulator is generally used to generate realistic received multipath profiles resulting from superposed 'rays' [7], [8], [9] and [10]. The channel simulation requires to consider the transmitter and receiver positions, the waveform feeding the transmit antenna, the antenna radiation pattern and the description of the operating environment (e.g. electromagnetic characteristics of surrounding materials, building/room geometry, etc.). The main idea is to calculate the received signal as the sum of all the significant rays associated with each source in the environment [14]:

$$\begin{aligned} r(t) &= \sum_{k=1}^{N_l} r^{(k)}(t) + n(t) \\ &= \sum_{k=1}^{N_l} \sum_{j=1}^{N_{ray}(k)} s^{(k)}(t) * h_j^{(k)}(t) + n(t) \end{aligned}$$

where N_l is the number of considered links, $N_{ray}(k)$ is the number of significant rays propagating between the source k and the receiver, $s^{(k)}(t)$ is the emitted sequence, $h_j^{(k)}$ is the impulse response of the j_{th} ray, which includes the propagation delays and $n(t)$ represents the receiver noise. It has been shown that some uncertainty can be observed due to fading and to the unpredicted device orientation.

In this paper, we explore this technique to predict the channel responses for different receiver's locations in an indoor environment and verify whether the attacker can easily 'guess' the secret keys.



(a) (b) (c)

Fig. 3. (a) The grid for the receiver B locations (in this example, A is the emitter which is kept stationary and B is a moving receiver) the distance separating the two transmitters varies between 2m and 7m (b) Cross-Correlation Coefficients (the whole channel impulse responses for the attacker and legitimate parties (c) Cross-Correlation Coefficients for the 30 significant paths

IV. Ray-Tracing based attacks

The crucial insight that allows to generate secret keys from channel randomness is that the radio channel is unique and only shared by the two legitimate nodes. This property offers the possibility to compute and agree on a secret key. As already seen in section III, recent experimental studies on the UWB Ray-tracing simulations have revealed that deterministic prediction tools can rather reliably predict the received channel profile [6]. In this part, we focus on the consequences of using such techniques by an adversary to derive the shared key.

We consider a system with an emitter (A) and a receiver (B) in a typical indoor office environment, which is relatively wide and comprises different reflectors (metallic objects, glass...), as shown in figure 1. In our adversary model we assume that the attacker Eve E knows the secret key extraction algorithm and can listen to the communication between A and B to eavesdrop the exchanged correction messages. We also assume that E has a knowledge of the building's layout, the different transmitter and receiver locations, the emitted waveform and the antenna characteristics. As described in the following sections, the attacker tests two scenarios to infer the channel responses using the UWB Ray-Tracing tool [9] and then generates the secret key. For each scenario, two comparative steps will be considered. First, we examine the similarity between the attacker and the legitimate receiver channel responses (CR) using the cross-correlation and the mutual information (MI) measures. We then observe the similarity between the resulting binary sequences extracted from the channel responses.

A. First Scenario

We assume that the system is composed by an emitter A and a mobile receiver B which moves in the emitter vicinity on a circular grid, as shown in figure 3a. A campaign of measurements has been performed to collect real UWB channel responses for a typical indoor environment. We invite the interested reader to refer to [11] for a description of the measurement setup.

At each location of B, the impulse channel response between A and B was estimated. In total, 23 channel responses, corresponding to 23 arbitrary locations of B, have been estimated. Furthermore, at each location of B, nodes A and B extract a secret key using the algorithm described in section II. The goal of the attacker is to derive the emitter-receiver channel responses at the receiver locations. We suppose that the adversary has the possibility to guess the correct emitter and receiver coordinates (using for instance ultrasonic technique). Then, he simulates the UWB radio responses at these locations using the Ray-Tracing channel prediction tool.

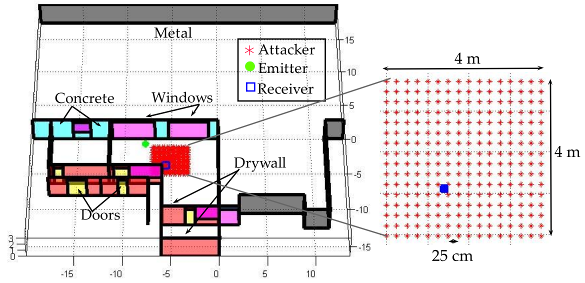


Fig. 4. Showroom layout for Ray-Tracing channel prediction showing the attacker, receiver and emitter locations. The attacker moves on a 16 by 16 grid. The distance between the close points (in row or in column) of the grid is 25 cm. In total, radio channel responses are inferred at 256 different points

Step 1: Similarity between different channel responses We compute the mutual information [15] which is a practical measure to show the mutual dependence of the attacker and legitimate parties' channel responses. Figure 5 gives the mutual information $I(A, B)$ between A and B estimates ($\hat{h}_{BA}$ and $\hat{h}_{AB}$) and the information that can be learned by the adversary about the receiver's measurements, denoted by $I(B, E)$. The expression $I(x, y)$ refers to the mutual information between measurements of users x and y. As we can see, the MI between the adversary and the receiver is smaller than that between the emitter and the receiver and very close to zero, indicating that the attacker cannot retrieve significant information about the legitimate parties' channels. Then, we compute the cross-correlation which is a similarity measure of the adversary and the receiver waveforms. Figure 3b displays the channel responses correlation between the CRs estimated by the attacker and the CRs computed by A and B. The correlation coefficients are small for most tested locations. In fact, the maximum correlation coefficient is equal to 0.45. This shows that the estimated channel responses are different from the actual ones, and cannot easily be exploited by the attacker to retrieve the secret key. However, when we only consider the 30 most significant paths of the CRs computed by A and B, the correlation coefficients become much higher (up to 0.7), as shown in figure 3c. That means that the Ray-Tracing tool can predict finely the most significant rays. This result can be explained by the fact that the 3-D environment description used by the Ray-Tracing tool only considers large objects and just ignores some others (e.g. desks, chairs, cabinet, personnel computers, etc.) in the surrounding. In addition, the simulation tool cannot take into account low signal contributions resulted from multiple diffractions.

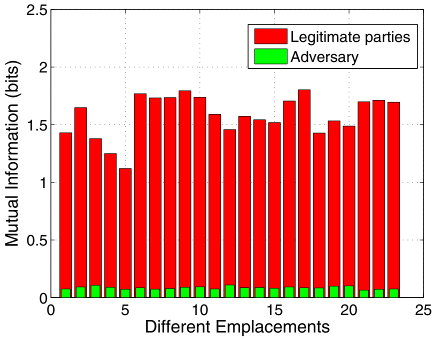


Fig. 5. The mutual information between A-B and E-B

Step 2: Similarity between binary sequences After the channel estimation process, the attacker executes the secret key generation algorithm described in section II and produces a set of candidate secret keys. Figure 6 displays the sizes of the derived (by A and B) and the simulated (by the adversary) binary vectors for the different 23 locations. It shows that due to the lack of multipath diversity, the attacker cannot generate large binary vectors to retrieve the shared key. On average, the attacker generates 20% of secret binary vectors that only 6% are common to the actual keys generated by A and B.

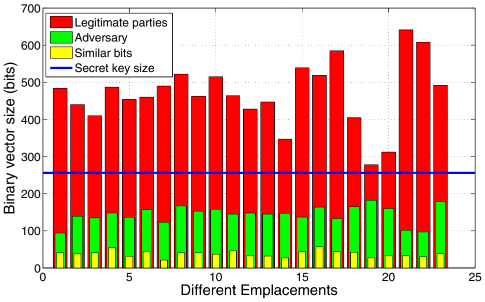


Fig. 6. The size of binary vectors at different locations for the first scenario

B. Second Scenario

We now focus on testing a brute-force attack by collecting channel responses at different locations. In this scenario, we assume that the attacker knows the emitter's (A) location. However, as opposed to the previous scenario, it is assumed that the adversary does not know the exact location coordinates of B but only knows that he is somewhere on $4m * 4m$ grid. To retrieve the key, the adversary decomposed the grid into 256 points. As shown in figure 4, the distance between points (in row or in column) of the grid is 25 cm. He then estimates for each of these points the CR using the Ray-Tracing tool.

Step 1: Similarity between different channel responses Figure 7 shows the correlation between the actual channel response computed by B (at coordinates $x_B = -5.6$, $y_B = -3.9$) and the normalized predicted channel responses at the 256 different points of the grid. As shown, the correlation coefficients are small (the maximum coefficient is equal to 0.44). This result indicates that the simulated channel responses are uncorrelated with the actual one, shared by A and B. It is notable that this difference is principally due to the presence of scatterers which are not considered in the 3-D environment description used by the Ray-Tracing tool and its incapability to consider for example multiple diffractions. As in the previous scenario, we then consider the 30 most significant paths at the legitimate parties' channel response, and recomputed the 256 correlation coefficients. This results in higher correlation coefficients (up to 0.7), as shown in figure 8, which means that the adversary shares some common paths with the legitimate user. Consequently, some bits of the shared key may be guessed by the attacker (as it will be discussed in step 2 of this scenario). Due to the space editorial constraint, the plot for the mutual information is not presented. It is notable that these results are similar to the previous scenario and that the mutual information $I(E, B)$ is smaller than $I(A, B)$ and very close to zero, demonstrating that the attacker is unable to obtain significant information about A and B channel responses.

Step 2: Similarity between binary sequences After the channel estimation and prediction steps, the different parties apply the key generation algorithm as described in section II. Figure 9 displays the binary sequences size generated by the attacker. These results show that the attacker can only generate small binary vectors, and only recover a small number of the key bits (less than 40 bits), contrary to legitimate parties which agree on a 256 bits key. These common bits are not enough to recover the whole shared secret key even the attacker performs a brute-force attack. This is due to the fact that he may not guess the exact position of the extracted bits and which one are similar to the legitimate parties.

The described tests indicate that the key generation algorithm based on the UWB channel responses is resilient to an attacker using the Ray-Tracing channel prediction tool. It has been shown that Eve cannot infer the exact channel responses and thus retrieve the shared key. Despite the success on extracting a small number of common bits, it is difficult to guess the total secret key.

V. Conclusion

In this paper we have introduced novel attack scenarios based on the UWB Ray-tracing channel prediction tool for retrieving the shared secret keys in a typical indoor environment. The proposed attacks are very complex to perform since they require an important amount of information such as the emitted waveform, the emitter's antenna pattern, the environment layout, the transmitters' locations, etc. Our work demonstrates that the exhaustive UWB radio channel responses cannot be inferred by a third party (especially less significant paths) and, then it is impossible to recover the shared secret keys. The robustness of the novel key generation methods relies on the complexity to reproduce precisely the indoor environment and on the post processing phases (i.e. the quantization and key agreement). However, it is important to recognize that research on the UWB Ray-Tracing simulations are expanding greatly advances and that using the UWB channel as a common to generate secret keys can be perilous, especially for narrower bandwidth applications.

Acknowledgement

The research leading to these results was partly funded from the French National Research Agency under grant agreement ANR-VERSO-ARESA2. The authors extend their thanks to Dr. Vincenzo Latosa, for technical discussions they had regarding this work.

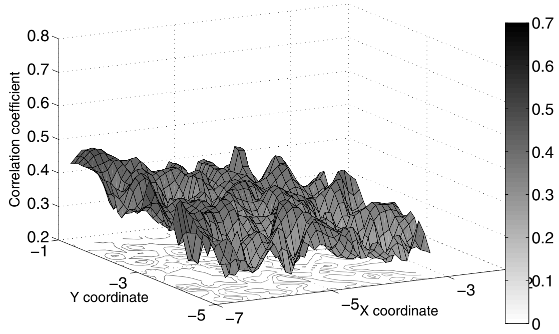


Fig. 7. Cross-Correlation between the CR measured at the actual receiver location ($x_B = -5.6$, $y_B = -3.9$) and the CR simulated through Ray-Tracing (we consider the whole channel impulse responses)

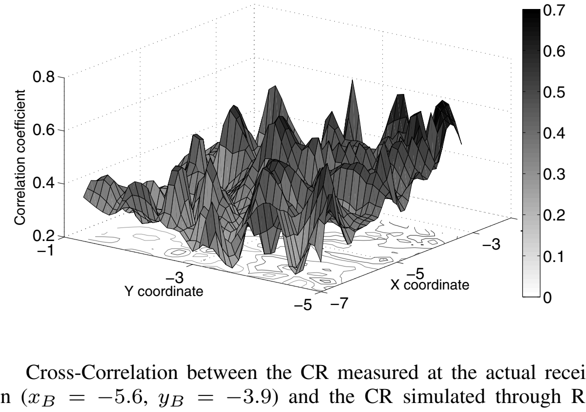


Fig. 8. Cross-Correlation between the CR measured at the actual receiver location ($x_B = -5.6$, $y_B = -3.9$) and the CR simulated through Ray-Tracing (we consider the 30 most significant multipath components)

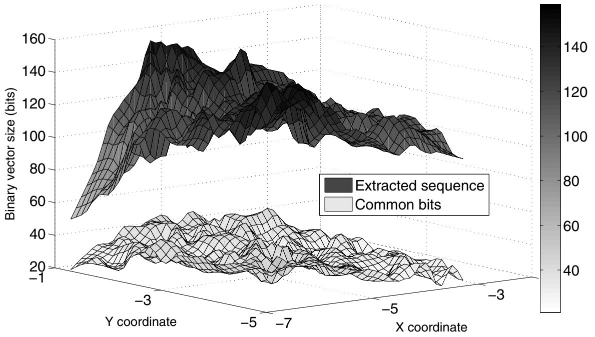


Fig. 9. The size of the extracted binary vectors for the adversary node and the number of common bits with the legitimate parties data

References

[1] R. Wilson, D. Tse, R. A. Scholtz, and L. Fellow, "Channel identification: Secret sharing using reciprocity in UWB channels," *IEEE Transactions on Information Forensics and Security*, pp. 364–375, 2007.

[2] A. Kitaura, T. Sumi, T. Tango, H. Iwai, and H. Sasaoka, "A private key sharing scheme based on multipath time delay in UWB systems," in *International Conference on Communication Technology, 2006. ICCT '06.*, 2006, pp. 1 –4.

[3] M. G. Madiseh, M. L. McGuire, S. S. Neville, L. Cai, and M. Horie, "Secret key generation and agreement in UWB communication channels," in *IEEE Global Telecommunications Conference*, 2008, pp. 1–5.

[4] S. Tmar-Ben Hamida, J.-B. Pierrot, and C. Castelluccia, "An adaptive quantization algorithm for secret key generation using radio channel measurements," in *Proceedings of the 3rd international conference on New technologies, mobility and security*, 2009, pp. 59–63.

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

[6] M. Raspopoulos, S. Stavrou, B. Uguen, R. Burghelea, M. Garca, T. Pedersen, G. Steinbck, B.-H. Fleury, B. Denis, J. Youssef, Y. Lostanlen, and A. lvarez, "Modelling of the channel and its variability (final report)," Delivrable D4.5 of the EU-funded WHERE project (ICT FP7 217033), Tech. Rep., May 2010.

[7] F. Tchoffo Talom, "Modélisation déterministe du canal de propagation indoor dans un contexte Ultra Wide Band, (in French)," Ph.D. dissertation, INSA de Rennes, October 2005.

[8] M. Hassan-ali and K. Pahlavan, "A new statistical model for site-specific indoor radio propagation prediction based on geometric optics and geometric probability," *IEEE Transactions on Wireless Communications*, vol. 1, pp. 112–124, 2002.

[9] R. Qiu, "A study of the ultra-wideband wireless propagation channel and optimum UWB receiver design," *IEEE Journal on Selected Areas in Communications*, vol. 20, no. 9, pp. 1628 – 1637, Dec. 2002.

[10] F. Tchoffo-Talom, B. Uguen, E. Plouhinec, and G. Chassay, "A site-specific tool for UWB channel modeling," in *in Proc. IEEE Joint UWBST04 and IWUWBS04,*, May 2004, pp. 61 – 65.

[11] S. Tmar-Ben Hamida, J.-B. Pierrot, and C. Castelluccia, "Empirical analysis of UWB channel characteristics for secret key generation in indoor environments," in *IEEE 21st Inter. Symposium on Personal Indoor and Mobile Radio Communications*, 2010, pp. 1984 –1989.

[12] M. G. Madiseh, S. He, M. L. McGuire, S. W. Neville, and X. Dong, "Verification of secret key generation from UWB channel observations," in *IEEE International Conference on Communications, 2009. ICC '09*, Jun. 2009, pp. 1–5.

[13] I. S. Reed and G. Solomon, "Polynomial Codes Over Certain Finite Fields," *Journal of the Society for Industrial and Applied Mathematics*, vol. 8, no. 2, pp. 300–304, 1960.

[14] B. Uguen, E. Plouhinec, Y. Lostanlen, and G. Chassay, "A deterministic ultra wideband channel modeling," in *Ultra Wideband Systems and Technologies, 2002. Digest of Papers. 2002 IEEE Conference on*, 2002.

[15] T. M. Cover and J. A. Thomas, *Elements of information theory*. Wiley-Interscience, 1991.