Secret Keys from Entangled Sensor Motes: Implementation and Analysis

Matthias Wilhelm, Ivan Martinovic[*], and Jens B. Schmitt
TU Kaiserslautern
Distributed Computer Systems Lab
67653 Kaiserslautern, Germany
{wilhelm,martinovic,jschmitt}@cs.uni-kl.de

ABSTRACT

Key management in wireless sensor networks does not only face typical, but also several new challenges. The scale, resource limitations, and new threats such as node capture and compromise necessitate the use of an on-line key generation, where secret keys are generated by the nodes themselves. However, the cost of such schemes is high since their secrecy is based on computational complexity. Recently, several research contributions justified that the wireless channel itself can be used to generate *information-theoretic* secure keys between two parties. By exchanging sampling messages during movement, a bit string can be derived that is only known to the involved entities. Yet, movement is not the only possibility to generate randomness. The channel response is also strongly dependent on the frequency of the transmitted signal. In our work, we introduce a protocol for key generation based on the *frequency-selectivity* of channel fading. The great practical advantage of this approach is that we do not rely on node movement as the source of randomness. Thus, the frequent case of a sensor network with static motes is supported. Furthermore, the error correction property of the proposed protocol mitigates the effects of measurement errors and other temporal effects, giving rise to a key agreement rate of over 97%. We show the applicability of our protocol by implementing it on MICAz motes, and evaluate its robustness and secrecy through experiments and analysis.

Categories and Subject Descriptors

C.2.1 [**Computer Communication Networks**]: Distributed networks, Wireless communication

General Terms

Security, Algorithms, Measurement

1. INTRODUCTION

Securing wireless sensor networks (WSNs) has been one of the main wireless network research areas in recent years. Especially key generation and key management, which are at the heart of any security design, pose new challenges because of the low computational capabilities of wireless motes, their limited battery lifetime, and the broadcast nature of wireless communication. Given these peculiarities, a large number of key management protocols for WSNs has been proposed, often fine-tuned between different performance vs. security trade-offs and adapted for specific WSN scenarios and their applications (for a general overview see, e.g., [3, 15]). However, most of these protocols follow a conventional cryptographic approach, where the secret is based either on pre-distributed keys or public-key schemes assuming more performance capable devices that are able to generate and distribute the keys. Although there have been efforts to adapt public key cryptographic protocols to the world of WSNs (e.g., TinyECC [6]), these adaptations usually have a significant complexity and memory footprint as well as a high energy consumption (for energy analysis of public key schemes, see, e.g., [13]).

Recently, there have been research contributions that follow an alternative path to key generation using an information-theoretic approach to derive secrets from unauthenticated broadcast channels. Informally, the general idea is similar to the quantum world, in which the laws of quantum mechanics ensure that two spatially separated particles experience highly correlated quantum states (called "quantum entanglement"). Measuring the quantum properties of one particle discloses the knowledge of another. However, in contrast to the mystical quantum nature, contributions on key generation using wireless channel are concerned with conventional physical signal propagation and, to some extent, its reciprocal behavior. Specifically, recent results described by Mathur et al. [7] and Azimi-Sadjadi et al. [2] justify that the unpredictable multipath propagation and the resulting fading behavior of wireless channel can be used to extract shared secret material. Simply by exchanging messages that serve to sample the signal propagation behavior, both transmitters can establish mutual secret information, while an eavesdropper who also receives these messages still remains completely ignorant. Since the secrecy of the extracted information is not based on computational complexity as common to conventional public key cryptography, these protocols are especially valuable to computationally limited wireless devices. Yet, existing solutions require that the wireless devices move at certain speeds to produce enough unpre-

[*]The work in this paper was partially funded by the Carl-Zeiss Foundation.

WiSec'10, March 22–24, 2010, Hoboken, New Jersey, USA.
Copyright 2010 ACM 978-1-60558-923-7/10/03 ...$10.00.

dictability in their signals. Thus, the most prevalent applications of WSNs which are based on static wireless motes makes these protocols inapplicable. This brings us to the contribution of this work, which abstains from this limitation and provides a novel key generation protocol for static WSNs.

2. CONCEPT

In this section, we introduce the concept of key generation using the frequency-selectivity of wireless channels. As we base the secrecy of our protocol on our ability to extract secrets at two different locations, we require two things from the wireless channel: strongly correlated information between the two parties and high unpredictability of the generated keying material for adversaries. Our results in [14] show that two parties experience strong correlation in their measured values (the so-called channel reciprocity), so we will focus on security aspects in this paper.

2.1 Security Considerations

The unpredictability of the channel state is the most important aspect when considering the wireless channel as the source of randomness, as it directly affects the provided secrecy. In the related work [7, 2], the *spatial* selectivity of the wireless channel due to movement was used to generate secret bits. In this work, we show that the frequency-selectivity of multipath fading is a viable alternative to generate secret information using the wireless channel.

In general, wireless signals are not traveling on a single path from a sender to a receiver, but arrive from several directions at the receiver, i.e., the signal exhibits multipath propagation characteristics. Each path is affected by different attenuations and phase shifts, and the resulting signal at the receiver is a combination of all signal paths by wave interference, resulting in a channel response depending on many variables. A small variation in phase, e.g., by using a different carrier frequency, leads to unpredictable changes in the signal strength, even when signal paths are unchanged. This behavior is captured by the impulse response of the wireless channel, considering L signal paths

$$h(\tau) = \sum_{l=1}^{L} \alpha_l e^{j\phi_l} \delta(\tau - \tau_l),$$

with different values of each path for the amplitude α_l, phase shift ϕ_l and delay τ_l, acting as random variables on each impulse δ. Because of phase shifts, interference effects can lead to signal cancellation or amplification, depending on the relative phase shifts.

To show the magnitude of these effects, we conducted an experiment to evaluate the selectivity of the channel both with respect to position and carrier frequency. Figure 1 shows the uncertainty of an adversary even if the positions of Alice and Bob are known up to a few centimeters. Each barplot represents the received signal strength measurements on 16 channels in the 2.4 GHz range available on the MICAz platform. The sensor mote acting as Alice was placed in a fixed position on a desk, Bob was placed in an adjacent room, such that both were separated by a wall, and the channel response was sampled from 12 positions on a 10 cm radius around Bob's initial position. The results show that the multipath effects are strong, and even if an attacker has knowledge of the environment and the positions of Alice and Bob; the channel behavior is unpredictable. More quantitative results are presented in Section 4.2.

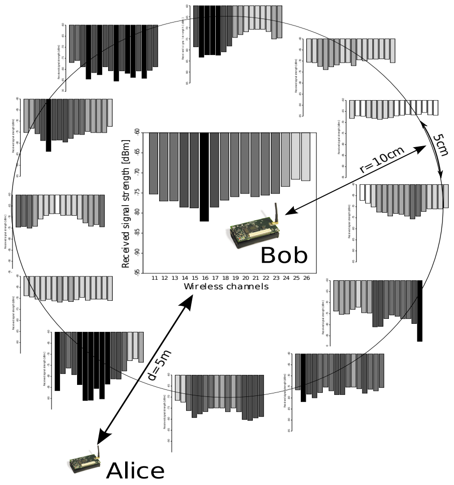

Figure 1: Spatial and frequency selectivity of the wireless channel. Even with shifts of 5 cm, the measured signal prints are significantly different for each position.

2.2 System Model

We are interested in the *amount* of uncertainty that an adversary experiences. Information theory introduces the notion of (Shannon) entropy to quantify the average amount of information of a discrete random variable, making it suitable for capturing the amount of uncertainty an attacker experiences. In this section, we derive a stochastic model of the system enabling us to evaluate the secrecy of the proposed protocol based on signal strength distributions of real-world measurements.

2.2.1 Secrets from the Wireless Channel

The state of the wireless channel for a specified frequency at a certain point in time is captured by the *discrete* random variable C, that is, we assume that only finite precision can be achieved in channel state acquisition. Possible sources for this variable are, for example, the complex impulse response of the channel, or as in our case, the received signal strength. The outcome of C is stable during channel coherence time, which depends on the speed of movement. In static scenarios on which we focus, this time is very long, enabling us to take several samples and use mean values as outcomes of C.

Both Alice and Bob have access to the wireless channel and can exchange sampling messages. Each can monitor one of the random variables

$$\begin{aligned} X_{Alice} &= C_{Alice} + N_{Alice} \\ X_{Bob} &= C_{Bob} + N_{Bob}, \end{aligned}$$

with C_x being the measured channel state at the respective position and N_x being random variables representing the noise processes that introduce errors in the channel state estimations. With the help of channel reciprocity we can assume that $C_{Alice} = C_{Bob} = C$, i.e., both parties experience the same channel properties in their exchanged sampling messages. The mutual information that the channel provides is described by

$$I(X_{Alice}, X_{Bob}) = H(X_{Alice}) - H(X_{Alice} \mid X_{Bob}) \leq H(C).$$

The conditional entropy $H(X_{Alice} \mid X_{Bob})$ is zero if the channel is noiseless, and the amount of shared information which Alice and Bob gain from monitoring the wireless channel is quantified by the entropy $H(C)$ of the channel state variable, given by

$$H(C) = -\sum_{c \in \mathcal{C}} p(c) \log p(c),$$

where $p(c)$ denotes the probability mass function of c and $\mathcal{C}$ is the support of the random variable C. This also represents the maximum attainable mutual information from the wireless channel [8]. An experimental evaluation of the magnitude of measurement errors and the effects on secrecy is given in Section 5, as we aim to quantify the amount of secrecy using the propagation properties of realistic wireless channels.

2.2.2 *Multiple Channels*

In this work, we consider the random vector $\mathbf{C} = (C_1, \ldots, C_n)$, measured on n different frequencies to increase the amount of shared information between Alice and Bob. This approach allows to support static networks. Alice measures $\mathbf{X}_{Alice} = (X^{(1)}_{Alice}, \ldots, X^{(n)}_{Alice})$ and Bob measures $\mathbf{X}_{Bob}$, which both can be used to obtain the mutual information

$$I(\mathbf{X}_{Alice}, \mathbf{X}_{Bob}) = H(\mathbf{X}_{Alice}) - H(\mathbf{X}_{Alice} \mid \mathbf{X}_{Bob}) \leq H(\mathbf{C}),$$

assuming reciprocity on all channels and $H(\mathbf{C})$ being the *joint* entropy over all channels, given by

$$H(\mathbf{C}) = -\sum_{c_j \in \mathcal{C}_i} p(c_1, \ldots c_n) \log p(c_1, \ldots, c_n).$$

If the elements in the random vector are independent, then the amount of uncertainty can directly be evaluated using the entropy values from individual channels, $H(\mathbf{C}) = \sum_{i=1}^{n} H(C_i)$. This value represents the upper bound of joint entropy, as dependencies between the variables enable predictions and reduce the overall uncertainty of Eve. However, wireless channels experience correlated fading if the distance between the center frequencies is smaller than the coherence bandwidth. Therefore, we must analyze the dependency structure to evaluate the amount of uncertainty, i.e., the secrecy of keys generated by the presented protocol.

3. KEY GENERATION PROTOCOL

In this section, we present a key generation protocol suitable even for limited hardware capabilities by using a performance-aware design, specifically with WSNs in mind.

We conduct measurements by sampling RSS values on a set of n different frequencies $\mathcal{F} = \{f_1, \ldots, f_n\}$ (also referred to as *channels*). The number of samples taken is k, i.e., for each channel f_i we collect a set of measurements $\{m_i\} = \{m_i^{(1)}, \ldots, m_i^{(k)}\}$. To increase the error tolerance of our scheme, we calculate the mean value $\mu_i = \frac{1}{k}\sum_{j=1}^{k} m_i^{(j)}$ of these RSS samples. We view this mean as the random variable C_i, which is distributed depending on the characteristics of wireless propagation, e.g., following the commonly assumed Rayleigh or Ricean distributions. The means of all n channels are combined to a random vector $\mathbf{C} = (C_1, \ldots, C_n)$. A realization, the outcome of our measurements is $\mu = (\mu_1, \ldots, \mu_n)$, with $\mu_i \in \mathcal{M} = [\mu_{min}, \mu_{max}]$, the range of mean values that can be measured by the hardware platform. We associate $\mathcal{M}$ with the distance function $dis : \mathcal{M} \times \mathcal{M} \to \mathbb{R}^+$ defined as $dis(\mu, \mu') := |\mu - \mu'|$, which is the difference in dB in our case.

3.1 Robustness Considerations

In order to achieve a high success rate in the key generation, we require a mechanism that ensures equality of the measurements of Alice and Bob. To this end, we introduce a multilevel quantization scheme on the measured signal strength values.

We choose K quantization levels, and each of these levels is identified by the binary string p. For simplicity of analysis, the chosen levels have an equal distance. The choice of K is critical for the security of the proposed key generation protocol. The higher the number of levels, the more information can be extracted from the state of the wireless channel, however, the required precision in the measurements equally increases, as the distance d between the values is decreasing. We denote this set of quantization levels as $\mathcal{C}_t = \{c_1, \ldots, c_K\}$, the bijective mapping to the binary representation as $bin : \mathcal{C}_t \to \{0,1\}^p$, which represents the quantized values. The tolerance of this scheme is given by $t = \frac{d}{2}$, i.e., the proposed quantization algorithm is able to repair deviations up to this value. Thus, we can trade robustness and secrecy by choosing a set $\mathcal{C}_t$ with a suitable parameter $t \in \mathbb{R}$ that is able to correct errors in measurements given $dis(\mu, \mu') < t$. The process of quantization of μ to c is denoted as

$$enc_t(\mu) = \arg\min_{c \in \mathcal{C}} dis(\mu, c).$$

3.2 Protocol Phases

The complete protocol is shown in Figure 2. We used a straightforward protocol for the ease of presentation of the protocol evaluation, but we also experimented with several protocol optimizations that can further increase the robustness and secrecy of the protocol.

3.2.1 *Sampling Phase*

In this initial phase, Alice and Bob exchange sampling messages on the set of available wireless channels. For each of the n frequencies in $\mathcal{F}$, Alice and Bob exchange k messages and each one stores a set of measured RSS values $\{m_i\}$ or $\{m'_i\}$, respectively. Alice initiates the message exchanges, Bob answers incoming sampling messages as fast as possible for a maximum of channel reciprocity. Due to constraints of the wireless hardware, the samples must be collected in an interleaved manner, such that the state of the wireless channel can change slightly, contributing to the noise terms N_{Alice} and N_{Bob}. However, by using several sampling messages per channel, the effects of such short term deviations can be mitigated. The mean values $\mu_i = \frac{1}{k}\sum_{j=1}^{k} m_i^{(j)}$ are then generated by Alice, while Bob proceeds similarly with μ'_i. Thus, after finalization of the sampling phase, both Alice and Bob possess the vectors of channel state information μ and μ' that capture the fading behavior of the wireless channel.

3.2.2 *Key Generation Phase*

The gathered mean values μ and μ' contain secret information that can be used as secret keys, but after the sampling phase these vectors are unlikely to agree. The *key generation phase* uses information reconciliation based on a multilevel quantization to produce a bit string that is equal

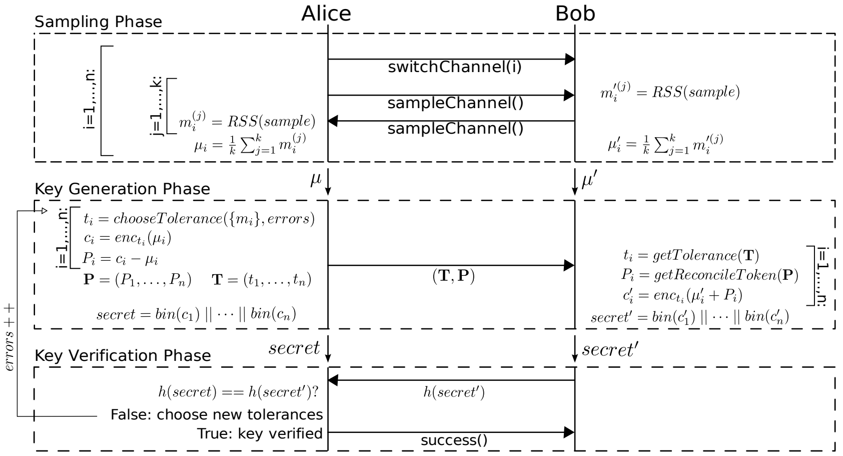
Alice
Bob
Sampling Phase
i=1,...,n:
j=1,...,k:
switchChannel(i)
sampleChannel()
sampleChannel()
$m_i^{(j)} = RSS(sample)$
$\mu_i = \frac{1}{k}\sum_{j=1}^{k} m_i^{(j)}$
$m_i'^{(j)} = RSS(sample)$
$\mu_i' = \frac{1}{k}\sum_{j=1}^{k} m_i'^{(j)}$
μ
μ'
Key Generation Phase
$t_i = chooseTolerance(\{m_i\}, errors)$
$c_i = enc_{t_i}(\mu_i)$
$P_i = c_i - \mu_i$
$\mathbf{P} = (P_1, \ldots, P_n)$
$\mathbf{T} = (t_1, \ldots, t_n)$
$secret = bin(c_1) \mid\mid \cdots \mid\mid bin(c_n)$
$(\mathbf{T}, \mathbf{P})$
$t_i = getTolerance(\mathbf{T})$
$P_i = getReconcileToken(\mathbf{P})$
$c_i' = enc_{t_i}(\mu_i' + P_i)$
$secret' = bin(c_1') \mid\mid \cdots \mid\mid bin(c_n')$
$errors++$
$secret$
$secret'$
Key Verification Phase
$h(secret) == h(secret')?$
$h(secret')$
False: choose new tolerances
True: key verified
success()

Figure 2: Key generation protocol. The proposed key generation protocol operates in three phases. In the *sampling phase*, the channel state is acquired, and due to the reciprocity of the wireless channel state information strongly correlated measurements are collected by the two legitimate parties in the protocol. In the *key generation phase*, these deviations are corrected, resulting in a secret bit string that is guaranteed to be equal if the experienced deviations are bounded and a suitable quantization is used. The *key verification phase* ensures correct key agreement.

on both sides, without discarding shared bits or revealing information to eavesdroppers. Alice chooses a set of tolerance values $\mathbf{T} = (t_1, \ldots, t_n)$ based on the variance of the RSS values $\{m_i\}$ and the number of experienced verification errors from possible previous runs. We used the same tolerance value $t_i = 1$ for all channels as the basis for our experiments and analysis, which combines a high rate of successful key agreements and good secrecy, as shown experimentally with our implementation. However, the choice of tolerance values strongly influences the robustness and secrecy trade-off, and considering optimization at this point is useful.

Alice chooses tolerance values by using the the appropriate quantization function enc_{t_i} on her mean values μ_i to generate the values c_i for each channel. She also generates the vector of public reconciliation strings $\mathbf{P} = (P_1, \ldots, P_n)$ by calculating $P_i = c_i - \mu_i$ to aid Bob in his error correction and to ensure matching secrets. He can generate his quantized vector by calculating $c_i' = enc_{t_i}(\mu_i + P_i)$. Both parties now have sufficient information to generate their candidate secrets $secret$ and $secret'$.

3.2.3 Key Verification Phase

Finally, both parties proceed to verify if the secret keys are generated successfully, i.e., if a mutual secret is established. After Bob has finished his computations, he sends the hash value $h(secret')$ of his secret string to Alice. She ensures successful key generation by comparing Bob's value to her secret string. If the hash values do not match, Alice can retry the key generation by increasing the error count and choosing new tolerance values in the key generation phase; new sampling of the wireless channel is not necessary. The approach used in our implementation uses a tolerance increase of 0.5 dB on each channel. However, our implementation on MICAz sensor motes presented in the next section shows that with a tolerance $t = 1$, key agreement was reached in 90.5% of the cases on the first try.

After the finalization of this step, both Alice and Bob share a secret string that can be used to support security services.

4. IMPLEMENTATION AND ANALYSIS

After the definition of the key generation protocol, the next interesting aspect is how this protocol performs in real-world environments, and how large the achievable secrecy and robustness is given realistic propagation properties. With several experiments, these properties are explored in detail in this section. We also show that the concept is applicable on resource-constrained devices under realistic properties of the wireless channel. The first part is focused on the robustness and performance of the protocol, and in the second part the secrecy is quantified empirically using the notion of information entropy. These insights are used as a basis and justification for the analytical model developed in the next section.

4.1 WSN Testbed and Methodology

Several different scenarios were considered to evaluate the impact of positioning to secrecy and robustness. A large meeting room was used for experiments, where the sensor motes always maintained a line of sight connection, and several smaller office rooms were used to quantify the impact of shadowing objects and walls. For each of these scenarios, 250 positions were considered, and the distance was kept constantly at 2.5 meters to avoid the influence of path loss effects. In long-term and mobile scenarios, these rooms and the connecting corridors were used, and 1000 additional positions were tested with mixed distances and obstacles. We used $k = 16$ samples on each channel, collected on $n = 16$ channels.

4.2 Protocol Robustness and Security Analysis

The success ratio of the protocol can be directly controlled by the tolerance values used, as larger tolerance values are able to correct stronger deviations. With a tolerance of 1 dB, 90.5% of the key agreements are successful on the first run. This value is increased to 98.3% with a tolerance of 2 dB. The empirical cumulative distribution function (ECDF) for the successful key generations of all experiments is shown in Figure 3. The majority of deviations are below 2 dB, and only a small number of extreme outliers were measured. As

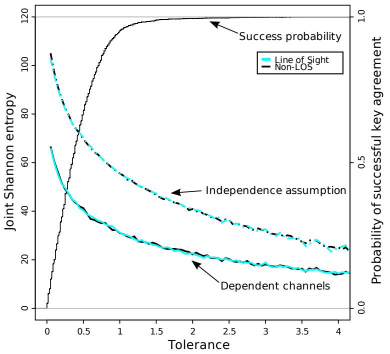

Figure 3: Results for the implementation on MICAz sensor motes. The amount of secrecy under different dependence assumptions is shown, with the corresponding success probabilities of key agreement.

the chosen tolerance value also has an impact on the secrecy of the resulting bit string, a careful trade-off between secrecy and robustness must be found.

The secrecy analysis focuses on the distribution of codewords, especially on the entropy that the distributions offer. The evaluation of the entropy for single channels is straightforward: we use the empirical distribution to calculate $H(C_i)$ for each of the n channels individually, using the relative frequencies as the estimations of codeword probabilities. This analysis results in 3.5 bit of entropy available from each channel channel for a tolerance value of $t = 1$, a value of $t = 0.5$ results in an increase to 4.38 bit. The joint entropy under this assumption of independence is the sum of the channels' entropy values. The resulting entropy values are shown in Figure 3.

The entropy of dependent channels is hard to quantify considering unknown dependencies in the variables. The Shannon entropy operates on the knowledge of the underlying distributions, which are unknown in our case, and a precise estimate of these distributions, i.e., a large number of observations, is necessary to estimate the entropy accurately. This becomes increasingly difficult when considering multivariate distributions, as the number of observations needed increases rapidly. Yet, several analytical tools are available to estimate the joint entropy from empirical data [12, 10]. The approach in this work is based on construction complexity, which uses insights from the theory of data compression to find the shortest representation of the channel codewords, which also results in a maximum entropy. As a result, using this method we were able to capture the dependencies between channels in the empirical data without explicitly knowing them. In Section 4.3, we use them for the verification of the derived stochastic model.

A comparison of different results is shown in Figure 3. With a tolerance value of $t = 1$, the entropy under independence assumption is 56 bit for both LOS and non-LOS connections. When considering the dependencies in the measurements, 31 bit of entropy can be achieved with the limited number of channels and precision that the wireless sensor mote hardware offers. Lower tolerance values can be used to increase secrecy. For example, a tolerance value of 0.4, which results in a 50% chance of key agreement, offers 45 bit under dependent channels. The hardware capabilities are the most limiting factor in the proposed key generation protocol. Therefore, in the next section we analyze the amount of secrecy if current technology limitations are lifted.

4.3 Analyzing Dependent Wireless Channels

The experimental analysis shows that the dependencies between channels have considerable influence on the overall secrecy of the proposed protocol. In this section, we develop a stochastic model that makes these dependencies explicit and enables us to analyze the protocol and predict ways to increase the achieved secrecy, such as the impact of increasing the number of available channels or a larger spacing between center frequencies. To derive a realistic model of dependent wireless channels, we start with fitting and validating the distribution of single channel measurements and then extending it to a multivariate case, which describes the dependency structure of wireless channels. The model is validated by comparing the resulting entropy values with our empirical results.

Frequently used distributions for large-scale models of wireless channels are Rayleigh, Ricean, or Log-Normal [9] depending on the properties of the respective propagation environment. Also, in scenarios common to WLANs and WSNs, where distances between transceivers are short, the empirical data can be estimated by the Normal distribution [11, 5, 1]. To find an adequate distribution, we collected 4000 RSS sample means for each of the LOS and non-LOS scenarios, where every RSS mean was calculated over 16 measurements, estimating the distribution parameters using Maximum Likelihood Estimation (MLE). Additionally, we tested the normality of the sampled data using the probability plot correlation coefficient test for normality (PPCC), which is based on checking for linearity between the theoretical quantiles and the sample data [4]. In fact, the goodness of fit test confirms that the assumption of the Normal distribution (correlation coefficient = 0.992) can be accepted with an even higher confidence than the corresponding Rayleigh distribution (correlation coefficient = 0.967). In this case, the multivariate Normal distribution can be used to describe the complex dependency structures of wireless channels by directly estimating the covariance matrix from the empirical data.

Hence, to analyze the dependencies of the joint distribution over all 16 wireless channels, especially with respect to joint entropy, we model the signal strength values of different channels using a single multivariate Normal distribution. The distribution parameter estimation is straightforward: the vector of mean values μ, which is in case of the Normal distribution already the MLE for the population mean, and for the covariance matrix Σ we used the MLE method:

$$\hat{\Sigma} = \frac{1}{n-1} \sum_{i=1}^{n} (X_i - \overline{X})(X_i - \overline{X})^T.$$

Finally, we validated the multivariate channel dependency model against our empirical data by using the same error correction mechanism (described in Section 4) to generate codewords and to compare the Shannon entropy of the empirical data with the results of the model. The results of this evaluation are given in Figure 4, which shows the resulting entropy values for the non-LOS data applying the same analysis methods used in the experimental analysis. The LOS experiment is omitted as the behavior is similar. The model captures the dependency structure well, resulting in a similar progression of the curve for the existing toler-

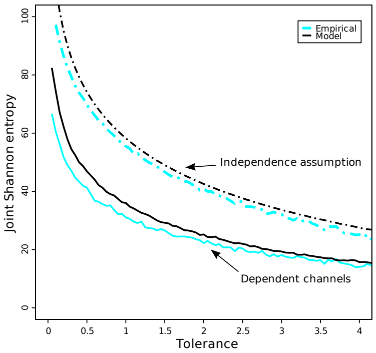

Figure 4: Comparison of discrete entropy values based on RSS values generated using the stochastic model derived in Section 4.3.

ance values, although the entropy is slightly overestimated by the model.

Using the model, we can estimate the amount of entropy if additional resources are available, such as a higher number of channels or a larger spacing between channels. Due to space limitations, we omit the extrapolation procedure and only pointing out some results. Adding a new channel that can be probed increases the amount of secret bits by 4.02. For example, if the number of channels of the present IEEE 802.15.4 is set to 40, this protocols can generate up to 160 bit secret keys in static scenarios. Additionally, the model allows to analyze larger channel spacing, which decreases the dependency across channels. For example, the additional gain if the channels are spaced 10 MHz apart, instead of the 5 MHz spacing in our experiments, yields a 4.25 bit increase.

Our model shows that there are several ways to increase the secrecy of the proposed protocol. With measurements of higher precision it is possible to generate more bits on each channel, but as this increases the hardware costs, it is advisable to rather use a larger number of channels, or a larger channel spacing.

5. CONCLUSION

Taking advantage of the unpredictable nature of wireless communication, two transmitters can generate a shared secret without exchanging any information other than frames used merely for measuring the received signal strength. Most importantly, any other transmitter that is positioned only a few centimeters away remains ignorant of the generated secret. While such an approach for generating secret keys has already been addressed, existing contributions require movement as the main generator of secret material. Valuable to mobile networks, such solutions however are not applicable to the majority of WSN applications based on static sensor motes. The main focus of this work was to overcome this limitation.

We started by introducing a system model based on real-world measurements using IEEE 802.15.4 technology, and describing building blocks of the novel key generation protocol. To demonstrate its applicability, the protocol was implemented and evaluated using MICAz sensor motes. Experiments show that the protocol is able to successfully generate keys in over 95% of the cases, irrespective of the scenario. By using only a very limited number of wireless channels, the proposed protocol can already provide secrets up to 60 bit, depending on the wireless channel behavior. In addition, the derived stochastic model verified our experimental data and provided insights on how to increase the number of generated secret bits. Finally, even if only a small number of wireless channels is available, the introduced protocol can be applied to various applications, e.g., as a part of device-pairing schemes to establish an authenticated channel, or as a source of fresh randomness for initial key deployments.

6. REFERENCES

[1] C. H. Foh A. Bose. A practical path loss model for indoor WiFi positioning enhancement. In *International Conference on Information, Communications & Signal Processing*, pages 1–5, 2007.

[2] Babak Azimi-Sadjadi, Aggelos Kiayias, Alejandra Mercado, and Bulent Yener. Robust Key Generation from Signal Envelopes in Wireless Networks. In *CCS '07: Proceedings of the 14th ACM Conference on Computer and Communications Security*, pages 401–410, New York, NY, USA, 2007. ACM.

[3] S. A. Camtepe and B. Yener. Key Distribution Mechanisms for Wireless Sensor Networks: a Survey, 2005. Technical Report TR-05-07 Renesselaer Polytechnic Institute, Computer Science Department, March 2005.

[4] James J. Filliben. The probability plot correlation coefficient test for normality. *Technometrics*, 17(1):111–117, 1975.

[5] K. Kaemarungsi and P. Krishnamurthy. Modeling of indoor positioning systems based on location fingerprinting. In *Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, volume 2, pages 1012–1022, March 2004.

[6] A. Liu and P. Ning. TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks. In *Information Processing in Sensor Networks, 2008. IPSN'08. International Conference on*, pages 245–256, 2008.

[7] Suhas Mathur, Wade Trappe, Narayan Mandayam, Chunxuan Ye, and Alex Reznik. Radio-telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel. In *MobiCom '08: Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, pages 128–139, New York, NY, USA, 2008. ACM.

[8] Ueli Maurer, Renato Renner, and Stefan Wolf. Unbreakable keys from random noise. In P. Tuyls, B. Skoric, and T. Kevenaar, editors, *Security with Noisy Data*, pages 21–44. Springer-Verlag, 2007.

[9] Theodore Rappaport. *Wireless Communications: Principles and Practice.* Prentice Hall PTR, 2001.

[10] Thomas Schürmann and Peter Grassberger. Entropy estimation of symbol sequences. *CHAOS*, 6:414, 1996.

[11] Yong Sheng, Keren Tan, Guanling Chen, David Kotz, and Andrew Campbell. Detecting 802.11 MAC layer spoofing using received signal strength. In *Proceedings of the 27th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, pages 1768–1776, April 2008.

[12] Ulrich Speidel, Mark Titchener, and Jia Yang. How well do practical information measures estimate the Shannon entropy? In *Proc. of the Fifth International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP 2006)*, pages 861–865. IEEE, 2006.

[13] Arvinderpal Wander, Nils Gura, Hans Eberle, Vipul Gupta, and Sheueling Chang Shantz. Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks. In *Proceedings of the third annual IEEE International Conference on Pervasive Computing and Communications (PerCom '05)*, pages 324–328, March 2005.

[14] Matthias Wilhelm, Ivan Martinovic, and Jens B. Schmitt. On Key Agreement in Wireless Sensor Networks based on Radio Transmission Properties. In *Proceedings of the 5th Annual Workshop on Secure Network Protocols (NPSec)*, pages 37–42, Princeton, New Jersey, USA, October 2009. IEEE Computer Society.

[15] Y. Xiao, V.K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway. A Survey of Key Management Schemes in Wireless Sensor Networks. *Computer communications*, 30(11-12):2314–2341, 2007.