ISSN 2278-8808
SJIF 2013 = 4.194
An International Peer Reviewed
SCHOLARLY RESEARCH JOURNAL
FOR INTERDISCIPLINARY STUDIES

SECURE PACKETS IN WIRELESS SENSOR NETWORKS BASED ON FREQUENCY-SELECTIVE CHANNELS

J.Thirumaran , Ph.D[*].

[*]Dean-Academic,
Rathinam College of Arts & Science,
Coimbatore.

S. Raja[**]

[**]Asst. Professor,
Department of Computer Science,
Rathinam College of Arts & Science,
Coimbatore.

Abstract

***W**ireless sensor network faces several unique challenges. The scale, resource limitations, and new threats such as node capture suggest the use of in-network key generation. The wireless channel itself can be used to generate information theoretic secure keys. By exchanging sampling messages during device movement, a bit string is derived known only to the two involved entities. Yet, movement is not the only option to generate randomness: the channel response strongly depends on the signal frequency as well. In this work, we introduce a key generation protocol based on the frequency-selectivity of multipath fading channels. We discuss in this paper how to secure packets in wireless networks.*

***Keywords**: secured packet, wireless sensor network, key generation protocol*

Introduction

Key distribution and key management face many challenges in wireless sensor networks (WSNs), mainly because of the low computational capabilities of sensor motes, their limited battery lifetime, and the lack of a private communication channel because of broadcast signal propagation. In the face of these constraints an abundance of key management protocols for WSNs has been proposed, often finely tuned for different performance and security trade-offs, and adapted to limited WSN scenarios and applications. there have been several research contributions that follow an alternative path towards key generation by using an information-theoretic approach to derive secrets from unauthenticated broadcast channels. Justify that the unpredictable multipath propagation and the resulting fading behavior of wireless channels can be used to extract shared secret keys even in the presence of eavesdroppers. Yet, existing key generation protocols require that the wireless devices move randomly to produce changing signal propagation properties and thus sufficient unpredictability in their signals. Therefore, the most prevalent indoor applications of WSNs based on static sensor devices make these protocols inapplicable. So while resource-limited devices would benefit strongly from the current information-theoretic advances in physical layer key generation, existing protocols require the availability of sufficient hardware resources and rely on mobile computing scenarios.

Secure Data Generation:

We introduce the concept of key generation using the frequency-selectivity of wireless channels with multipath fading. The successful execution of this protocol depends on the ability to extract secrets at two separated positions. We require two things from the wireless channel: (i) strongly correlated information between the two legitimate parties and (ii) a high degree of uncertainty for adversaries.

Mutually Shared Keys by Channel Reciprocity:

The principle of channel reciprocity states that two receivers experience the same channel properties when their role as sender and receiver is exchanged, given that the time interval is shorter than the coherence time of the channel. The measurements are strongly correlated but not identical because of measurement errors caused by noise in the hardware and by radio interference. This imperfect reciprocity directly influences the reliability of the proposed key generation protocol because it leads to possible disagreement in the generated bit strings.

Secure Keys by Multipath Fading Channels:

the spatial selectivity of the wireless channel due to movement is used to generate secret bits. A change in position results in changing paths that the signal travels on, which in turn interfere at the receiver and influence the observed signal strengths. In this work, we augment this finding and show that the frequency selectivity of multipath fading is a viable extension to generate secret information with both a higher rate and without the requirement for node movement. Multipath fading: When considering indoor signal propagation, we observe that the signal exhibits multipath propagation characteristics. Each path is affected by different signal attenuation and phase shifts, and the resulting signal at the receiver is a superposition of all signal paths.

Strength and behavior in wireless channels:

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 our key generation scheme, enabling us to evaluate the strength of the generated keys with measurements in realistic scenarios. Subsequently, we perform an experimental study to capture the signal behavior in realistic wireless channels. This allows quantifying the amount of uncertainty that the attacker experiences; we quantify its expected uncertainty with the entropy of the signal strength distributions of the channel.

Channel Model and Key Generation:

We formalize the key generation process as follows: 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 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.

Performance in real-world environments:

We present our key generation protocol that is suitable even for limited hardware capabilities by using a performance aware design, specifically with WSNs in mind. After the definition of the key generation protocol, the next goal is to evaluate the performance in real-world environments and to quantify the achievable security and robustness given realistic propagation properties. We also show that the concept is applicable on resource-constrained devices under realistic channel properties. The first part is focused on the robustness and performance of the protocol, and in the second part the security is quantified empirically using the notion of information entropy.

Methodology Experiments in wireless networks:

The experiments were conducted over several days on a university floor, an indoor setting across several rooms. During the measurements, several wireless LAN access points were operating concurrently in the 2.4 GHz band; thus the experiments were performed in a real-world environment with unpredictable factors. The environment contained concrete walls as well as office furniture made of various materials. In this setting, several scenarios are considered to evaluate the impact of positioning on security and robustness. A large meeting room is used for experiments where the devices constantly maintain a line of sight connection, and several smaller office rooms are used to quantify the impact of shadowing objects and walls. In contrast to previous sections, we now develop a stochastic model that makes these dependencies explicit and enables us to analyze and predict ways to increase the achievable security. We start with fitting and validating the distribution of single channel measurements and then extending it to the multivariate case that captures the dependencies between channels. The model is validated by comparing the resulting entropy values with our empirical results. First, we consider the effects of the determinant on the security given a larger number of channels (while keeping the spacing between channels constant). To this end, we extrapolate the covariance matrix and evaluate the effect on the determinant. Two different prediction methods are used; one that extrapolates directly and another that also simulates the effect of larger spacing between center frequencies and then extrapolates the matrix.

Signal strength based approaches: Several research groups applied the concept to wireless communication systems to generate secret keys from signal propagation properties, providing insights into the feasibility and reliability in realistic settings. The randomness of the received signal strength that is generated by movement as a source for correlated information, the so-called "radio-telepathy." The authors employ a level-crossing algorithm with two thresholds to turn signal strength values into bit strings. For information reconciliation, both parties detect mutual threshold excursions by exchanging suitable candidate regions in the sequence. In contrast to our work, their solution requires movement as a generator of randomness and thus it is not applicable in resource-constrained static networks. The problem of resource-constrained devices has also inspired research in the same direction as this article. Consider movement-based key generation protocols for WSN. It provides a similar study for body area networks. However, both works do not consider the use of multiple channels to support static networks. Our preliminary results outline the protocol implementation and some experimental results. Here, we present new experimental results, and a detailed analytical model that captures the interdependencies between channels. As subsequent work, other authors applied our approach of exploiting frequency selective channels in the context of body area networks. It analyzes the security of physical layer key generation protocols under a sophisticated active adversary. They show that during the channel sampling phase, the adversary can identify opportunities to jam and inject messages that result in symmetric, yet predictable quantization's. As a result, a significant part of the generated secret key may be disclosed to the adversary. That paper indicates that there is a need for a better understanding of active adversaries against key generation protocols, and the development of methods to detect and mitigate such attacks.

Conclusion:

Secure packet and distribution poses one of the main security challenges in wireless networks, especially in computationally limited WSNs. Taking advantage of physical properties of signal propagation, mutual secrets between wireless transmitters can be derived with greatly reduced computational complexity. Although this approach for securing wireless networks has been recently addressed by others, these protocols require continuous movement as a randomness source. Although valuable to mobile networks, such solutions are not applicable to the majority of WSN applications, which are based on static devices.

References

A. Liu and P. Ning, "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks," in Proc. 7th Int'l Conf. Inf. Processing Sensor Net., IPSN 2008, Apr. 2008, pp. 245–256.

A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," CoRR, vol. arXiv:1011.3754v1, pp. 1–13, Nov. 2010.

A. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in Proc. 3rd IEEE Int'l Conf. Pervasive Computer Communication., Per Com 2005, Mar. 2005, pp. 324–328.

B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in Proc. 14th ACM Conf. Comput. Commun. Security, CCS 2007. ACM, Oct. 2007, pp. 401–410.

C. Chen and M. A. Jensen, “Secret key establishment using temporally and spatially correlated wireless channel coefficients,” IEEE Trans. Mobile Comput., vol. 10, no. 2, pp. 205–215, Feb. 2011.

P. Szczechowiak, L. Oliveira, M. Scott, M. Collier, and R. Dahab, “NanoECC: Testing the limits of elliptic curve cryptography in sensor networks,” in Wireless Sensor Net., ser. LNCS. Springer, Jan. 2008,vol. 4913, pp. 305–320.

R. Wilson, D. Tse, and R. A. Scholtz, “Channel Identification: Secret sharing using reciprocity in ultrawideband channels,” IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 364–375, Sep. 2007.

S. A. Çamtepe and B. Yener, “Key distribution mechanisms for wireless sensor networks: a survey,” Computer Science Department, Rensselaer Polytechnic Institute, Troy, NY, USA, Technical Report TR-05-07, 2005.

S. Kullback and R. A. Leibler, “On information and sufficiency,” Ann. Math. Statist., vol. 22, no. 1, pp. 79–86, Mar. 1951.

S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, “Radiotelepathy: Extracting a secret key from an unauthenticated wireless channel,” in Proc. 14th ACM Int’l Conf. Mobile Comput. Netw., MobiCom 2008. ACM, Sep. 2008, pp. 128–139.

S. T.-B. Hamida, J.-B. Pierrot, B. Denis, C. Castelluccia, and B. Uguen, “On the security of UWB secret key generation methods against deterministic channel prediction attacks,” in Proc. 2012 IEEE 76th Vehicular Technol. Conf., VTC2012-Fall, Sep. 2012, pp. 1–5.

T. Rappaport, Wireless Communications: Principles and Practice, 2nd ed. Upper Saddle River, NJ, USA: Prentice Hall, Dec. 2001.

U. Maurer, R. Renner, and S. Wolf, “Unbreakable keys from random noise,” in Security with Noisy Data, 1st ed., P. Tuyls, B. Škoric, and T. Kevenaar, Eds. Springer, 2007, pp. 21–44.

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 Communication., vol. 30, no. 11–12, pp. 2314–2341, Sep. 2007.