iARC: Secret Key Generation for Resource Constrained Devices by Inducing Artificial Randomness in the Channel

Girish Revadigar*†, Chitra Javali*†, Hassan Jameel Asghar †,
Kasper B. Rasmussen, and Sanjay Jha*
{girishr,chitraj,sanjay}@cse.unsw.edu.au; hassan.asghar@nicta.com.au;
kasper.rasmussen@cs.ox.ac.uk

*School of Computer Science & Engineering, UNSW Australia, Sydney, AUSTRALIA
†NICTA, Australian Technology Park, Sydney, AUSTRALIA
Dept. of Computer Science, University of Oxford, Oxford, UK

ABSTRACT

The existing secret key generation schemes for body-worn devices using wireless channel characteristics, e.g., received signal strength indicator (RSSI) are dependent on the node mobility and have very low bit rate. In this work, we propose a novel mobility independent RSSI based secret key generation protocol – iARC, which induces artificial randomness in the channel by employing dual antennas and dynamic frequency hopping effectively.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection—*Physical layer security*

Keywords

Wireless Body Area Networks, Physical Layer Security, Secret key generation

1. IARC

Prior schemes [2] dependent on body motion cannot be used in many real-time applications. In comparison with SeAK [1] proposed for initial trust establishment between a new device and an existing Wireless Body Area Network (WBAN), iARC can be employed by the body-worn devices for periodic key renewal even when the person is not in motion. We have validated our system using Opal and Iris motes operating in 2.4 GHz, and used TinyOS to program the devices. We have conducted extensive set of experiments to validate our protocol in different real-time environments.

1.1 Inducing artificial channel randomness

We assume that there is one Control Unit (CU) which acts as an aggregator for the sensor data, and one or more wearable sensor devices (D). The CU uses two antennas A1 and A2 having different features which are placed very close to each other. The CU employs a pseudo-random number generator (PRNG) to generate a random bit string $r \in \{0,1\}^{128}$ which is used for antenna selection. iARC employs frequency diversity along with random antenna switching to induce artificial channel randomness.

1.2 Secret key generation

The secret key generation process consists of the following steps: (1) Channel sampling, (2) Quantization and multiple bit assignment, and (3) Dynamic frequency hopping. In iARC, the total number of probes N required for key generation is divided into B number of multiple sub blocks of equal length and each sub block key k_{sb} is derived in a different channel. The final secret key K is obtained by the concatenation of all the sub block keys as shown by the following equation: $K = k_{sb1} \parallel k_{sb2} \parallel \cdots \parallel k_{sbB}$.

Channel sampling is the phase in which the CU and D exchange packets on a particular channel and record RSSI. *Quantization* is the process in which each RSSI sample is assigned an n bit code word. The CU and D decide *Dynamic channel hopping* pattern based on the lowest level of RSSI. The CU and D perform channel sampling, quantization and frequency hopping repeatedly until the total number of probes N required for key generation are exchanged.

2. RESULTS

iARC achieves bit rate of 800 bps with 100% bit agreement between the two legitimate body-worn devices, and generates a 128 bit key in 160 ms. The keys generated by iARC pass the NIST test with entropy ranging from 0.92 to 0.99.

3. REFERENCES

[1] C. Javali, G. Revadigar, L. Libman, and S. Jha. SeAK: Secure Authentication and Key Generation Protocol based on Dual Antennas for Wireless Body Area Networks. In *Proc. RFIDsec*, 2014.

[2] L. Shi, J. Yuan, S. Yu, and M. Li. ASK-BAN: Authenticated Secret Key Extraction Utilizing Channel Characteristics for Body Area Networks. In *Proc. ACM WiSec*, 2013.

ASIA CCS'15, April 14–17, 2015, Singapore, Singapore
ACM 978-1-4503-3245-3/15/04.
http://dx.doi.org/10.1145/2714576.2714644.