Poster: Automatic Key Generation Using Motion Energy Harvesters

Qi Lin[1,3], Yesheng Cui[1], Shanqing Jiang[1], Tengyu Ma[1], Weitao Xu[2,3], Wen Hu[1,3]
[1]School of Computer Science and Engineering, University of New South Wales, Australia
Email: {qi.lin, yesheng.cui, shanqing.jiang, tengyu.ma}@student.unsw.edu.au {wenh}@cse.unsw.edu.au
[2]School of Information Technology and Electrical Engineering, University of Queensland, Australia
Email: {w.xu3}@uq.edu.au
[3]Data61 CSIRO, Australia

***Abstract*—Kinetic energy harvesters (KEH) or motion energy harvesters currently become an attractive trend as a self-sustainable power solution of Internet of Things (IoT) devices. As utilizing the ambient motion as the power source, KEH can be treated as a gait information carrier as well as a energy generator. This work focuses on exploiting gait information, carried by one type of KEH: piezoelectric energy harvesters (PEHs), to develop a communication key scheme. The key coding scheme is based on quantization of captured samples. The results show that the system can work in a narrowed experimental environment.**

I. Introduction

Facing the challenge of minimal maintenance and long operating life, future deployment of IoT devices will require self-sustainable power sources. With the development of ultra-low power electronics, low power sources can be now considered as possible future self-sustainable power sources. Among all these sources, KEH is an attractive direction as the ambient motion is the main source of energy harvesting. Human walking, as the main type of the ambient motion, contains a unique gait pattern for each person [1]. We can thereby assume that the power generated from the ambient motion can be more than just a power source, and also treated as a gait information carrier. By exploiting gait pattern, essential security functions of IoT devices such as wearer authentication, and communication key generation, etc., can be realized efficiently [2] [3] [4] [5].

This work prototypes a novel communication key system for IoT devices based on KEH signals as previous work focuses on accelerometers data. Among three mainstream types of KEH currently, PEH, which converts kinetic energy released from human motions into usable electrical energy, is used.

NDSS '16, 21-24 February 2016, San Diego, CA, USA
Copyright 2016 Internet Society, ISBN 1-891562-41-X
http://dx.doi.org/10.14722/ndss.2016.23xxx

II. Methodology

Assuming that all devices on body are legitimated, generated key based on PEH readings among all these legitimated device can match with each other, while any adversary device, which is not on body, cannot derive the correct key. Fig. 1 provides a brief overview on the key generation among legitimate IoT devices. Devices firstly collect PEH signals then generate keys based on collected signals. All keys on legitimated devices have the same bit extraction results and can match each other.

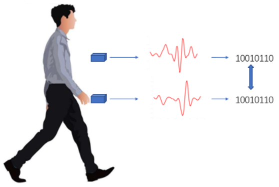


Fig. 1: Key Generation Scheme

A. Hardware Platform

Fig. 2 shows a developed hardware for the experiment. PEH used in the prototype device is PPA-1001 produced by MIDE Technology. Its resonant frequency is adjusted to be around 20Hz. The data logger is SensorTag produced by Texas Instruments [1]. An amplifying circuit is used to adjust the PEH signal to fit the ADC input range. The sampling rate of the data logger is set to be 64Hz. The accelerometer data is also captured by the Inertial measurement unit (IMU) in SensorTag for comparison.

B. Signal Preprocessing

Signal preprocessing on raw PEH data includes a temporal alignment process, a low pass filter, and a normalization process. An event-based approach is used for temporal alignment instead of explicit time synchronization. All testing devices are shaken simultaneously before they are distributed, and this shake event incurs a large impulse in the raw data which can be used for temporal alignment. The cutoff

[1] www.ti.com/sensortag

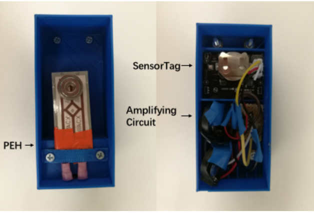


Fig. 2: Hardware

frequency for the low pass noise filter is selected to be 10 Hz as the frequency representing human motion is normally below this threshold [6]. The filtered data are then normalized to have zero-mean and the International System of Units.

C. Bit Extraction

The key generation process is based on a quantization process, where all samples are quantized to three categories: 0, 1, discarded. Samples that are not discarded are extracted to form the key. A moving window with no overlap is used to assist the bit extraction process. For all samples in one window, two thresholds based on statistics of all samples in this window are used for quantization.

$$t_+ = \mu + \alpha * \sigma, t_- = \mu - \alpha * \sigma \tag{1}$$

where μ is the mean, σ is the standard deviation in the window, and α is the evaluation parameter. The samples above the upper threshold are coded as “1” and those below the lower threshold as “0”. The samples in-between are considered as insignificant and discarded. The evaluation parameter α determines the threshold of samples considered to be significant.

III. Evaluation

In this stage, three evaluation metrics are of our interest: bit agreement rate, which evaluates the potential of agreeing generated keys from two devices; bit rate, which evaluates the time (or walking steps) required to generate valid keys; and entropy, which evaluates the potential of key decryption by attackers. The parameter α is used to balance the trade-off between bit agreement rate and bit rate, ranging from 0 to 1. Magnitude of accelerometer data is also evaluated for comparison.

The results are based on three datasets (average 10,000 samples for each dataset) from two participants. Legitimated devices are worn on the waist and chest on the same person and the adversary device is worn on the chest of another people. Fig. 3 and Fig. 4 show the relation between bit agreement rate and the evaluation parameter α based on PEH data and accelerometer data. Among legitimate devices, agreement rate increases as we narrow down the selection of significant samples and data from accelerometer perform better overall using this key scheme. On the other hand, agreement rate for adversary devices are between 45% and 50%. Increasing α makes adversary devices slightly harder to agree with each other. Considering only agreement rate, α is desired to be large for better performances but it trades off bit rate or time needed to generate key as shown in Fig. 5. Entropy of all results is above 0.97, safe from key decryption.

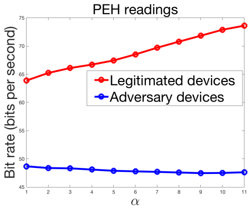


Fig. 3: Impact of α on agreement rate for PEH

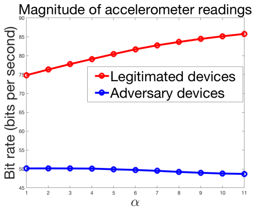


Fig. 4: Impact of α on agreement rate for accelerometer

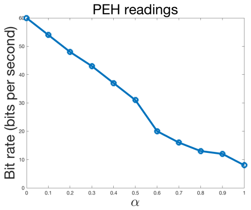


Fig. 5: Impact of α on bit rate

IV. Conclusion

In this work, we exploit the gait from KEH signals and propose a novel key generation scheme. The preliminary results show that the system can work in a narrowed experimental environment, but it still has room to improve.

References

[1] Mark S Nixon, Tieniu Tan, and Ramalingam Chellappa. *Human identification based on gait*, volume 4. Springer Science & Business Media, 2010.

[2] Weitao Xu, Girish Revadigar, Chengwen Luo, Neil Bergmann, and Wen Hu. Walkie-talkie: Motion-assisted automatic key generation for secure on-body device communication. In *2016 15th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, pages 1–12. IEEE, 2016.

[3] Weitao Xu, Guohao Lan, Qi Lin, Sara Khalifa, Neil Bergmann, Mahbub Hassan, and Wen Hu. Keh-gait: Towards a mobile healthcare user authentication system by kinetic energy harvesting. In *NDSS' 2017.*

[4] Weitao Xu, Chitra Javali, Girish Revadigar, Chengwen Luo, Neil Bergmann, and Wen Hu. Gait-key: A gait-based shared secret key generation protocol for wearable devices. *ACM Transactions on Sensor Networks (TOSN)*, 13, 2017.

[5] Weitao Xu, Yiran Shen, Neil Bergmann, and Wen Hu. Sensor-assisted face recognition system on smart glass via multi-view sparse representation classification. In *IPSN' 2016*, pages 1–12. IEEE, 2016.

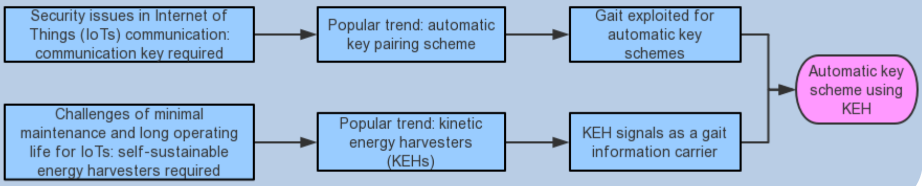
[6] Jonathan Lester, Blake Hannaford, and Gaetano Borriello. *“Are You with Me?” – Using Accelerometers to Determine If Two Devices Are Carried by the Same Person*, pages 33–50. Springer Berlin Heidelberg, Berlin, Heidelberg, 2004.

UNSW SYDNEY Australia's Global University

Automatic Key Generation Using Motion Energy Harvesters

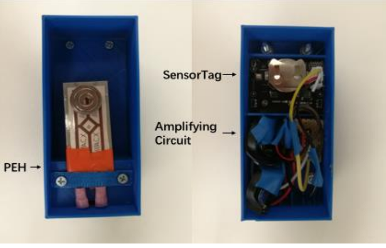
Qi Lin[1,3], Yesheng Cui[1], Shanqing Jiang[1], Tengyu Ma[1], Weitao Xu[2,3], Wen Hu[1,3]

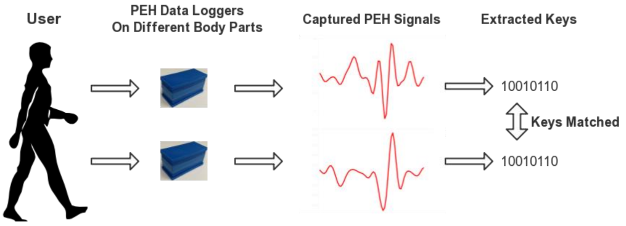
Motivation

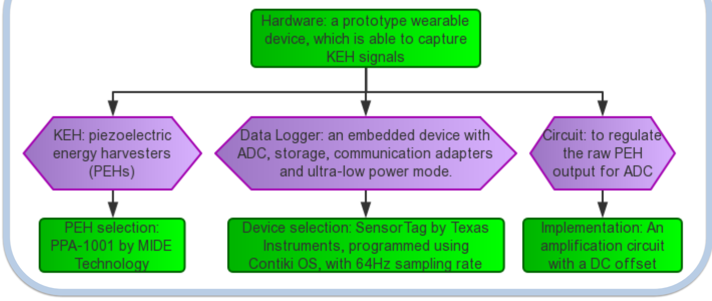

Security issues in Internet of Things (IoTs) communication: communication key required → Popular trend: automatic key pairing scheme → Gait exploited for automatic key schemes

Challenges of minimal maintenance and long operating life for IoTs: self-sustainable energy harvesters required → Popular trend: kinetic energy harvesters (KEHs) → KEH signals as a gait information carrier

→ Automatic key scheme using KEH





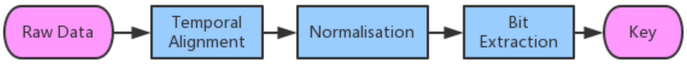

Hardware: a prototype wearable device, which is able to capture KEH signals

KEH: piezoelectric energy harvesters (PEHs) → PEH selection: PPA-1001 by MIDE Technology

Data Logger: an embedded device with ADC, storage, communication adapters and ultra-low power mode. → Device selection: SensorTag by Texas Instruments, programmed using Contiki OS, with 64Hz sampling rate

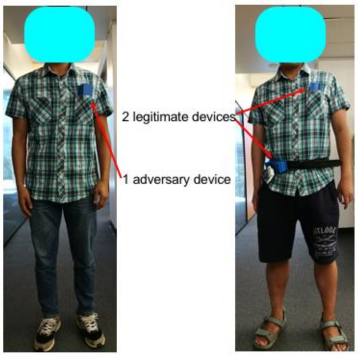
Circuit: to regulate the raw PEH output for ADC → Implementation: An amplification circuit with a DC offset

Key Generation Scheme


Raw Data → Temporal Alignment → Normalisation → Bit Extraction → Key

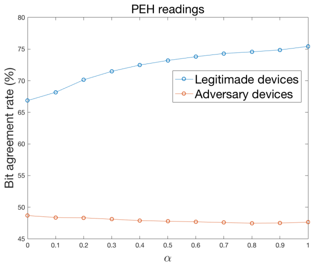
- Temporal alignment: find a global maximum corresponding to a shake event
- Normalisation: apply a 10Hz low pass filter to noise reduction, normalise the data to have zero-mean and internation system of units
- Bit extraction
  - Quantization

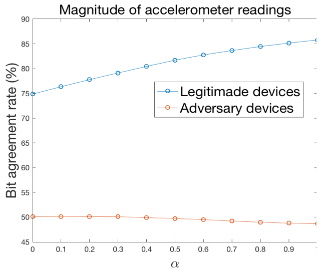
    $t_+ = \mu + \alpha * \sigma, t_- = \mu - \alpha * \sigma$
  - Reconciliation

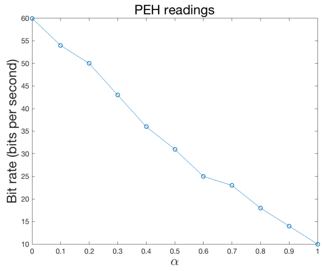


Evaluation

- Evaluation metrics:
  - Bit agreement rate
  - Bit rate
  - Entropy: it is always above 0.97 here
- Evaluation parameters:
  - α to balance the trade-off between bit agreement rate and bit rate;
  - Accelerometer data for comparison.







Author Information

[1] School of Computer Science and Engineering, University of New South Wales, Australia
Email: {qi.lin, yesheng.cui, shanqing.jiang, tengyu.ma} @student.unsw.edu.au {wenh} @cse.unsw.edu.au
[2] School of Information Technology and Electrical Engineering, University of Queensland, Australia
Email: {w.xu3} @uq.edu.au
[3] Data61 CSIRO, Australia