Demo

A Practical Secret Key Management for Multihop Drone Relay Systems based on Bluetooth Low Energy

Kai Li*

Ning Lu

Jingjing Zheng*

Pei Zhang

Wei Ni

Eduardo Tovar*

*CISTER Research Centre

CISTER-TR-210601

2021/07/06

A Practical Secret Key Management for Multihop Drone Relay Systems based on Bluetooth Low Energy

Kai Li*, Ning Lu, Jingjing Zheng*, Pei Zhang, Wei Ni, Eduardo Tovar*

*CISTER Research Centre

Polytechnic Institute of Porto (ISEP P.Porto)

Rua Dr. António Bernardino de Almeida, 431

4200-072 Porto

Portugal

Tel.: +351.22.8340509, Fax: +351.22.8321159

E-mail: kai@isep.ipp.pt, zheng@isep.ipp.pt, Wei.Ni@data61.csiro.au, emt@isep.ipp.pt

https://www.cister-labs.pt

Abstract

In this paper, we present a practical secret key management for data relay security of bluetooth-connected drones. Time-varying received signal strengths between the drones and the ground sensing nodes are quantized to generate the secret key pairs, where the quantization interval is adjusted to reduce the number of mismatched secret key bits. To validate the key management performance, a multihop aerial relay system testbed is developed based on the MX400 drone platform and the bluetooth low energy radio transceiver.

A Practical Secret Key Management for Multihop Drone Relay Systems based on Bluetooth Low Energy

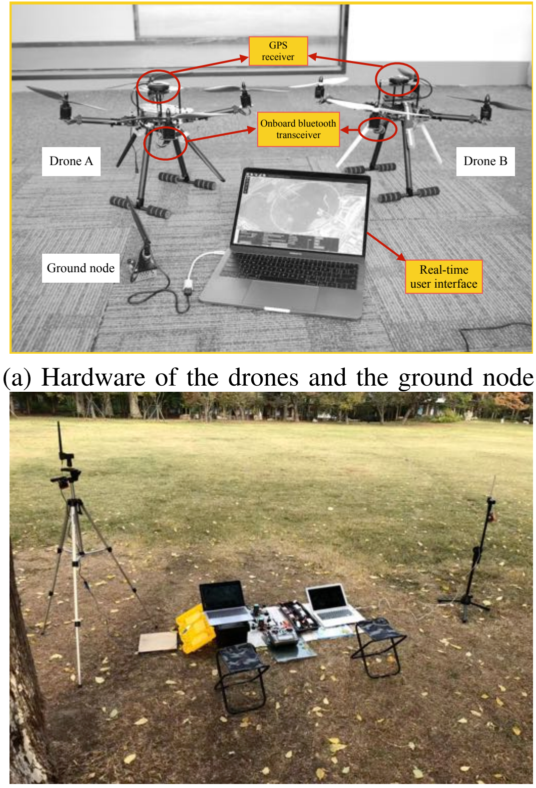
Kai Li*, Ning Lu[†], Jingjing Zheng*, Pei Zhang[‡], Wei Ni[§], and Eduardo Tovar*
*CISTER, Porto, Portugal.
Email: {kai, zheng, emt}@isep.ipp.pt.
[†]AirMind LLC., Shanghai, China.
Email: ning.roland@mindpx.net.
[‡]Electrical and Computer Engineering, University of Michigan, Ann Arbor, USA.
Email: peizhang@umich.edu.
[§]CSIRO, Sydney, Australia.
Email: wei.ni@data61.csiro.au.

***Abstract*—In this paper, we present a practical secret key management for data relay security of bluetooth-connected drones. Time-varying received signal strengths between the drones and the ground sensing nodes are quantized to generate the secret key pairs, where the quantization interval is adjusted to reduce the number of mismatched secret key bits. To validate the key management performance, a multihop aerial relay system testbed is developed based on the MX400 drone platform and the bluetooth low energy radio transceiver.**

***Index Terms*—Bluetooth low energy, Drones, Secret key, Communication channel, Testbed**

I. Introduction

In drones-aided relay networks, autonomous drones are employed as aerial relays to provide wireless connectivities between a ground data source node and a sink node [1]. Due to the broadcast nature of wireless channels, the communication between the drones and ground nodes in the aerial relay system is vulnerable to eavesdropping and replay attacks [2]. By eavesdropping the sensory data, adversaries can falsify the source data of the ground node or interpolate malicious data to abuse the flight trajectories of the drones [3]. Therefore, a secret key pair needs to be applied at the drones and the ground nodes for data encryption/decryption.



(a) Hardware of the drones and the ground node.

(b) Setup of the ground source node and the sink node.

Fig. 1: Hardware and experiment setup.

II. Channel-adapted key generation

In this paper, a long-distance bluetooth communication technique, Bluetooth Low Energy (BLE), *a.k.a.* Bluetooth 5.0, is considered [4]. We investigate a channel-adapted secret key management for communication security in the multihop aerial relay network, where two BLE-connected relaying drones are employed to hover over the ground nodes. Specifically, at the first hop, a secret key pair is generated at the ground source node to encrypt the source data which are sent to drone A. Similarly, another two pairs of secret keys are generated at the second hop (i.e., drone A and drone B) and the third hop (i.e., drone B and the data sink), respectively. A unanimous key pair needs to be generated at each hop so that the data can be successfully decoded by the receiver.

To generate the key pair, the drone or the ground device samples Received Signal Strength (RSS) of the channel.

978-1-6654-4108-7/21/$31.00 ©2021 IEEE

The RSS readings are quantized to a binary sequence, which is used as secret key bits. The number of quantization intervals can be predetermined [5]. In particular, upper bound and lower bound of each quantization interval can be recursively adjusted until a unanimous key pair is generated at the drone or the ground node in each hop. Due to motions of the drones, the temporal and spatial variations of the RSS randomize the generated key pairs, which enhances security of the channel-adapted key generation.

III. Testbed and Preliminary Results

A. *Testbed with BLE-connected drones*

Hardware of the testbed is depicted in Figure 1(a), where the drone is built based on the MX400 platform. The maximum transmit power of the BLE transceiver onboard the drone is up to 20.154 dBm, which leads to the BLE communication range of about 1 km [6]. Thanks to the long communication distance of the BLE transceiver, the channel-adapted key generation can be applied to most of aerial relay applications.

Figure 1(b) presents the experiment setup, where the BLE transceiver is connected to the ground source node and the sink node. The transmission of the data packet is initiated by the source node. Drone A and drone B patrol around the ground nodes along their predetermined trajectories. The trajectories are designed to prevent potential flight collisions.

B. *Number of mismatched key bits*

We conduct the experiments outdoor, where sensory data are generated by the source node, and relayed by the two drones to the sink node [7]. Figure 2 shows the number of mismatched key bits in the generated key pair, where the number of quantization intervals is set to 10, 20, or 30. The number of mismatched key bits increases with the growth of quantization intervals since the RSS readings can be quantized to the same interval with the small number of quantization intervals, which leads to the same key bits.

IV. Conclusions

This paper presented the multihop drone relay system, where the drones equipped with the BLE transceiver hover over the ground nodes. The channel-adapted secret key management is developed for communication security of the BLE-connected drones. The aerial relay testbed was built to evaluate the mismatched key bits in the generated key pair. Preliminary experimental results show that the mismatched key bits can be reduced by decreasing the number of quantization intervals.

Acknowledgements

This work was partially supported by National Funds through FCT/MCTES (Portuguese Foundation for Science and Technology), within the CISTER Research Unit (UIDP/UIDB/04234/2020); also by national funds through the FCT, under CMU Portugal partnership, within project CMU/TIC/0022/2019 (CRUAV).

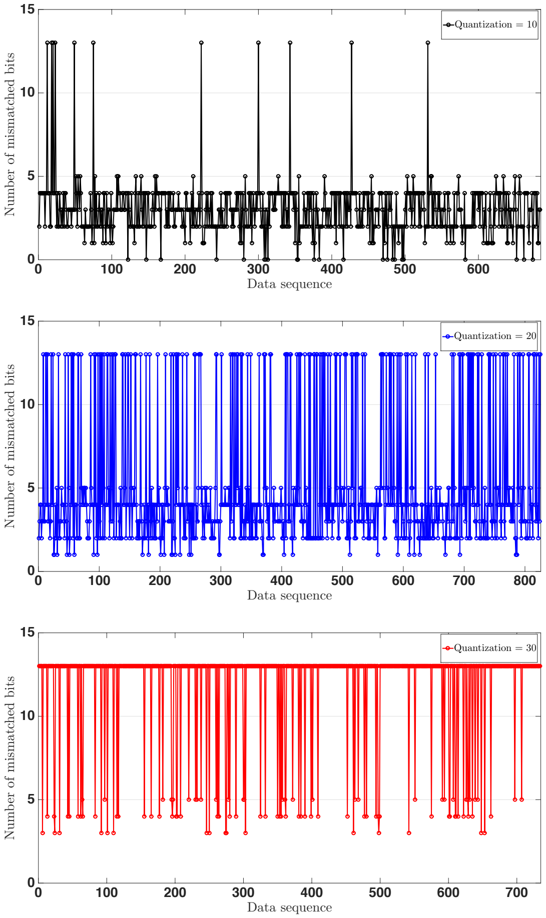


Fig. 2: Number of mismatched bits in regards to different number of quantization intervals.

References

[1] L. Bertizzolo, S. D'Oro, L. Ferranti, L. Bonati, E. Demirors, Z. Guan, T. Melodia, and S. Pudlewski, "Swarmcontrol: An automated distributed control framework for self-optimizing drone networks," in *INFOCOM*. IEEE, 2020, pp. 1768–1777.

[2] H. Guo, T. Liu, K.-S. Lui, C. Danilov, and K. Nahrstedt, "Secure broadcast protocol for unmanned aerial vehicle swarms," in *International Conference on Computer Communications and Networks (ICCCN)*. IEEE, 2020, pp. 1–9.

[3] Q. Wang, Z. Chen, W. Mei, and J. Fang, "Improving physical layer security using UAV-enabled mobile relaying," *IEEE Wireless Communications Letters*, vol. 6, no. 3, pp. 310–313, 2017.

[4] R. Heydon and N. Hunn, "Bluetooth low energy," *CSR Presentation, Bluetooth SIG*, 2012.

[5] K. Li, W. Ni, Y. Emami, Y. Shen, R. Severino, D. Pereira, and E. Tovar, "Design and implementation of secret key agreement for platoon-based vehicular cyber-physical systems," *ACM Transactions on Cyber-Physical Systems*, vol. 4, no. 2, pp. 1–20, 2019.

[6] K. Li, N. Lu, J. Zheng, P. Zhang, W. Ni, and E. Tovar, "Bloothair: A secure aerial relay system using bluetooth connected autonomous drones," *ACM Transactions on Cyber-Physical Systems*, vol. 5, no. 3, pp. 1–22, 2021.

[7] K. Li, N. Lu, P. Zhang, W. Ni, and E. Tovar, "Multi-drone assisted internet of things testbed based on bluetooth 5 communications," in *IPSN*. IEEE, 2020, pp. 345–346.