Poster Abstract: A Novel Modeling Involved Security Approach for LoRa Key Generation

Jiayao Gao
jiayao.gao@student.unsw.edu.au
The University of New South Wales

Weitao Xu
weitaoxu@cityu.edu.hk
City University of Hong Kong

Salil Kanhere
salil.kanhere@unsw.edu.au
The University of New South Wales

Sanjay Jha
sanjay.jha@unsw.edu.au
The University of New South Wales

Wen Hu
wen.hu@unsw.edu.au
The University of New South Wales

ABSTRACT

Taking the advantages of reciprocity and randomness of wireless fading channels, key generation via physical layer is attracting more attention. It becomes a remarkable solution for wireless communication in recent years. However, the feasibility under long-range and low data rate scenarios of narrow band low power wide area network (LPWAN) lacks proper studies. In this poster, we introduce a novel modeling method for Long Range Wide Area Network (LoRaWAN) key generation. The approach combines several signal processing techniques and using measured real-time Received Signal Strength Indicator (RSSI) to improve the applicability of key generation as well as increasing key generation rate (KGR) significantly.

CCS CONCEPTS

• **Networks** → **Mobile and wireless security**.

KEYWORDS

IoT, LoRa, LoRaWAN, wireless key generation

1 INTRODUCTION

Recently, LoRa, a novel wireless communication technology targeting the Internet of Things (IoT) device communication, has emerged. Its unique character of offering cost-effective connectivity to the low-power IoT devices and coverage over wide areas has attracted much attention. With the increasing deployment of LoRa in massive application domains, the security issue is becoming a real concern in this area.

Due to the broadcasting nature, transmissions via wireless communication can be received by any user, including the attacker. While considerable researches[6] have proved that the existing security approaches cannot be applied to IoT scenarios directly.

Key generation via the physical layer can achieve a reasonable security level with much less cost as a security solution for IoT[5]. It takes advantage of the reciprocity of the radio channel to obtain information that is both random and correlated among communication nodes. It needs less storage and computation power than asymmetric cryptographic solutions and mitigates the leakage risk of the pre-shared key.

However, when applying the key generation scheme to LoRa, the insufficient reciprocity due to low bandwidth and long packet airtime bring new challenges. The long distance communication is at the cost of low data rate, which results in decreased channel measurement reciprocity[4]. This directly leads to low KGR. Multiple-antenna[1] provides a way to solve the problem, but the high cost of modifying existing products makes it unscalable for more extensive deployment.

To address the above challenges, we introduce the modeling involved security approach for LoRa. We successfully verified the feasibility of using real time to generate keys and ran away from the limitation of the data rate. Compared to previous solutions, our method improves KGR by 6 times while achieving a similar key matching rate(KMR).

2 SYSTEM MODEL AND PROTOCOL DESIGN

There are mainly three steps, including sampling, signal processing, and key generation process. Fig. 1 shows the assumption model of the system.

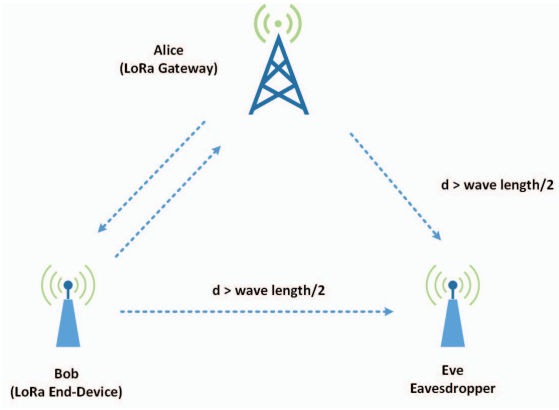

Figure 1: system model

2.1 Sampling

After inspecting the datasheet of the SX127x LoRa transceivers, we found that instead of PacketRssi ($RSSI_p$), which only provides one reading per packet and is used in most previous researches. Semtech provides users RegRssiValue ($RSSI_r$). $RSSI_r$ offers better linearity. More specifically, the sampling rate can be greatly increased[2]. Figure 2 shows the difference $RSSI_r$ and $RSSI_p$.

978-1-7281-5497-8/20/$31.00 ©2020 IEEE
DOI 10.1109/IPSN48710.2020.00-23

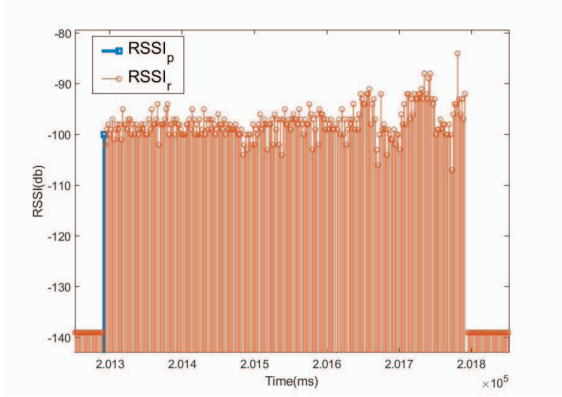

Figure 2: $RSSI_r$ **and** $RSSI_p$

2.2 Signal Processing

Signal processing is composed of two steps: modeling and curve fitting. According to experiments and previous research, the distribution of $RSSI_r$ will obey Rician distribution. A Rician fading distribution can be described by two parameters: K and Ω. After fitting the distribution of the RSSI in a specific period, it turns out that K and Ω form Alice and Bob are much closer than the eavesdropper Eve. After that, normalization is performed to the K and Ω and get Alice and Bob close enough for quantization. We note the set after normalization as K' and Ω'.

Then, we conducted a curve fitting to the points set K' and Ω'. We assume that $k_i'(\in K')$ and $\omega_i'(\in \Omega')$ will obey a linear function as follows.

$$\omega_i' = c_i * k_i' + d_i \tag{1}$$

The final coefficient set $C = \{c_1, c_2, ..., c_n\}$ and $D = \{d_1, d_2, ..., d_n\}$ will be used to compose the shared secret of the key generation process.

2.3 Key Generation

After the curve fitting, a set of random numbers $R = \{r_1, r_2, ...r_n\}$ and $-50 \leq r_i \leq 50$ will be generated by Alice (gateway) and sent to Bob. Alice and Bob can get similar results Z in equation (2), while Eve cannot.

$$Z = \{z_1, z_2, ...z_n\} \qquad z_i = c_i * r_i + d_i \tag{2}$$

We implement the multi-level quantization to z_i, and turn them into zero one key strings. The following equation shows how binary key is calculated when level = 4.

$$bk_i = \begin{cases} 00 & z_i \geq upperbound/2 \\ 01 & 0 \leq z_i < upperbound/2 \\ 10 & lowerbound/2 \leq z_i < 0 \\ 11 & z_i < lowerbound/2 \end{cases} \tag{3}$$

Due to noise, we often get $K_{Alice} \approx K_{Bob}$. We perform a Compressive Sensing (CS)-based reconciliation method [3] to reduce the bit mismatch rate. By exchanging the compressed samples from Bob to Alice, the CS-based reconciliation avoid Eve to recover the initial key even she can eavesdrop the transmitted message. message[4].

3 EVALUATION

Table 1: Experiment result

Test Name	Data rate	Matching Rate A-B	Key generation rate(bits/sec)
Modeling approach	High	100%	19.65
	Middle	99.59%	4.90
	Low	95.03%	4.84
LoRa-Key α = 0.8	High	74.48%	5.60
LoRa-Key α = 0.9	High	75.78%	4.54
LoRa-Key α = 1.0	High	94.53%	3.75

The preliminary result can be found in Table 1. The performance of the protocol surpasses the previous work in several aspects. The protocol is able to work under multiple data rates, while previous solution[4] works on solo data rates. Also, Different from [1] using special antennas, no special antennas is needed in the protocol proposed.

4 CONCLUSION

This poster proposes a novel modeling method for LoRa-based physical layer key generation. The method takes advantage of the $RSSI_r$ and uses the wireless channel model between two devices. With the features from the model and a series of randomly generated numbers, we generate the key based on wireless communication model and our method exceeds the pattern limit of the existing solution. Meanwhile, the KMR is reasonable, and KGR are also improved compared to previous work. Furthermore, our solution does not need any special antenna making the solution suitable for large scale deployment.

REFERENCES

[1] Henri Ruotsalainen, Junqing Zhang, and Stepan Grebeniuk. 2019. Experimental Investigation on Wireless Key Generation for Low Power Wide Area Networks. *IEEE Internet of Things Journal* (2019).
[2] Semtech. [n.d.]. SX1272 Datasheet. https://semtech.my.salesforce.com/sfc/p/#E0000000JelG/a/440000001NCE/v_VBhk1IolDgxwwnOpc_vTFxPfSEPQbuneK3mWsXlU
[3] Weitao Xu, Sanjay Jha, and Wen Hu. 2018. Exploring the Feasibility of Physical Layer Key Generation for LoRaWAN. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 231–236.
[4] Weitao Xu, Sanjay Jha, and Wen Hu. 2018. Lora-key: Secure key generation system for lora-based network. *IEEE Internet of Things Journal* (2018).
[5] Junqing Zhang, Trung Q Duong, Alan Marshall, and Roger Woods. 2016. Key generation from wireless channels: A review. *Ieee access* 4 (2016), 614–626.
[6] Kai Zhao and Lina Ge. 2013. A survey on the internet of things security. In *2013 Ninth international conference on computational intelligence and security*. IEEE, 663–667.