A Study on Secure Key Generation Methods Based on Multimodal Attributes in Wireless Communications

Daewon Kim, Seungyong Yoon, Byoungkoo Kim, and Yousung Kang
Cyber Security Research Division
Electronics and Telecommunications Research Institute
Daejeon, Korea
{dwkim77, syyoon, bkkim05, youskang}@etri.re.kr

***Abstract*—Vulnerabilities in the wireless physical layer have exposed risks of eavesdropping and manipulation by external attackers. Conventional cryptographic techniques, which require high computational complexity, have been primarily designed for layers above the physical layer. To address the specific challenges inherent in wireless environments, this study investigates a real-time secure key generation method that leverages multimodal wireless attributes dynamically established between communication devices.**

Keywords—information security, physical layer security, wireless security, secure key generation

I. Introduction

The threats and challenges arising from the unique characteristics of wireless environments are becoming increasingly significant. Wireless communication, utilizing radio waves for transmission, is vulnerable to eavesdropping, replay attacks, and man-in-the-middle attacks. These vulnerabilities reveal limitations in physical authentication and data link layer security. The rapid proliferation of IoT devices and smart systems further exacerbates network vulnerabilities and risks, creating a demand for lightweight technologies to enable real-time secure communications.

Conventional cryptographic techniques, such as RSA, are computationally intensive, making them inefficient in resource-constrained environments like low-power IoT devices. The advancement of quantum computing poses a significant threat to existing public key-based cryptographic systems, thereby necessitating the development of novel security solutions. Static or repeatedly used keys are vulnerable to eavesdropping and key leakage, prompting the adoption of dynamic key generation methods to address these weaknesses.

To address the aforementioned challenges in wireless environments, various studies have explored alternative security approaches. PLS (physical layer security)[1, 2] is one of the representative research areas, with authentication techniques based on device characteristics[3-6] and channel characteristics[7-10]. In this paper, we propose a real-time secure key generation method that employs lightweight neural networks to process multimodal wireless features dynamically established between communicating devices. This approach aims to enhance the security of lightweight wireless devices.

II. Secure Key Generation Based on Multimodal Attributes in Wireless Communications

Figure 1 illustrates the technical process related to our study. It comprises wireless signal feature extraction, security credential generation, and physical layer cryptographic key management.

A. Wireless Signal Feature Extraction

This stage extracts multiple features from the communication signals exchanged between wireless devices A and B. By utilizing multimodal attributes derived from these features, it becomes more difficult for attackers to predict cryptographic keys, thereby defending against attacks such as eavesdropping and message tampering.

- Time-period Signal Acquisition

This module collects various raw data during the time period when pilot messages (e.g., "hello") are exchanged between wireless devices. The type of data collected depends on the device or sensor used, as well as the specific characteristics of the target signal. Examples of collected data include I/Q (in-phase/quadrature-phase) signals, RSSI (received signal strength indicator), timestamps, amplitude/phase information, channel power levels across various frequency bands, among others.

- Signal Feature Extraction

This process extracts meaningful information from the collected signal for specific purposes. Depending on the device's capabilities, the extracted features may include CIR (channel impulse response), CSI (channel state information), modulation schemes, frequency spectrum, clock offset, amplifier distortion, phase noise, signal delay, channel variability, I/Q imbalance, SNR (signal-to-noise ratio), and other relevant parameters.

B. Security Credential Generation

This stage generates security credentials based on wireless signal features extracted from communication devices. These credentials are derived from unique physical layer characteristics inherent to each device. They consist of a variety of wireless signal features, thereby making it difficult for adversaries to predict or reproduce them.

- Statistical Analysis

Statistical metrics such as mean, variance, skewness, kurtosis, co-occurrence matrices, and KLD (Kullback-Leibler Divergence) are analyzed to highlight the distinctive characteristics of the extracted features.

- Dimensionality Reduction

This step reconstructs the multidimensional and complex information obtained from extracted features and statistical metrics into simplified representations. Dimensionality reduction algorithms, such as t-SNE (t-distributed stochastic neighbor embedding) and UMAP(uniform manifold approximation and projection), can be applied to reduce the high-dimensional complexity of data. This process is essential for

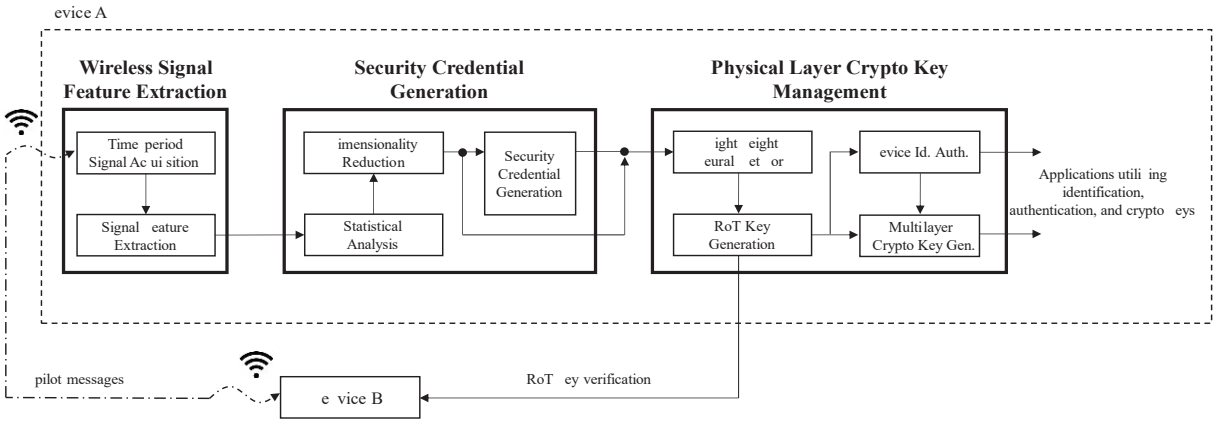

Fig. 1. System diagram for secure key generation based on multimodal wireless features.

lowering the complexity of security credential generation and supporting the operation of a lightweight neural network.

- Security Credential Generation

Using reduced-dimensional data, security credentials are generated to represent unique information shared between wireless communication devices.

C. Physical Layer Cryptographic Key Management

In this stage, the security credentials and reduced-dimensional data are fed into a lightweight neural network to generate a RoT (root of trust) key. This key can be used for device identification, authentication, and generation of cryptographic keys across multiple protocol layers.

- Lightweight Neural Network

The lightweight neural network integrates nonlinear and complex relationships that are challenging to design and implement using traditional analytical methods. It processes the security credentials and reduced-dimensional data to derive specific range values or unique identifiers. By leveraging multimodal features of wireless communication signals, this approach enhances resistance to adversarial prediction and exploitation.

- RoT Key Generation

This function refines the results predicted by the lightweight neural network to generate a key or a set of keys based on the desired length of the RoT key. Device A and B exchange their hashed RoT keys and compare the hash values. If the values do not match, the RoT key generation process restarts from the pilot message exchange stage.

- Device Identification and Authentication

If the RoT hash values match, the RoT key is utilized for managing device identification and authentication.

- Multilayer Cryptographic Key Generation

If the RoT hash values match, it is utilized to generate cryptographic keys that are applied across multiple protocol layers.

III. Conclusion

This paper studies a method for real-time security key generation by leveraging multimodal wireless characteristics dynamically formed between communication devices. The approach effectively mitigates vulnerabilities in the physical layer and supports device identification, authentication, and secure communication, particularly for lightweight and resource-constrained wireless devices.

Acknowledgment

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No. RS-2024-00360387, Development of core security technology utilizing multi-modal properties of wireless communication channels).

References

[1] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, et al, “Experimental study on key generation for physical layer security in wireless communications,” IEEE Access, vol. 4, pp. 4464-4477, Sep. 2016.

[2] N. Xie, Z. Li and H. Tan, "A survey of physical-layer authentication in wireless communications", IEEE Communications Surveys & Tutorials, vol. 23, no. 1, pp. 282-310, 2021.

[3] O. Ureten and N. Serinken, "Wireless security through RF fingerprinting", Can. J. Elect. Comput. Eng., vol. 32, no. 1, pp. 27-33, May 2007.

[4] C. Zhao, M. Huang, L. Huang, X. Du and M. Guizani, "A robust authentication scheme based on physical-layer phase noise fingerprint for emerging wireless networks", Comput. Netw., vol. 128, pp. 164-171, Dec. 2017.

[5] W. Hou, X. Wang, J. Y. Chouinard, and A. Refaey, “Physical layer authentication for mobile systems with time-varying carrier frequency offsets,” IEEE Trans. Commun., vol. 62, no. 5, pp. 1658-1667, May 2014.

[6] P. Hao, X. Wang and A. Behnad, "Performance enhancement of I/Q imbalance based wireless device authentication through collaboration of multiple receivers", Proc. Int. Conf. Commun. (ICC), pp. 939-944, 2014.

[7] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints", Proc. ACM Workshop Wireless Security (WiSec), pp. 43-52, 2006.

[8] J. K. Tugnait, "Wireless user authentication via comparison of power spectral densities", IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 1791-1802, Sep. 2013.

[9] J. Liu and X. Wang, "Physical layer authentication enhancement using two-dimensional channel quantization", IEEE Trans. Wireless Commun., vol. 15, no. 6, pp. 4171-4182, Jun. 2016.

[10] P. Baracca, N. Laurenti and S. Tomasin, "Physical layer authentication over MIMO fading wiretap channels", IEEE Trans. Wireless Commun., vol. 11, no. 7, pp. 2564-2573, Jul. 2012.