Spatial Filtering Approach for Security of Wireless Personal Area Networks

Halil Salih Orhan
Computer Engineering
Bogazici University
Istanbul, Turkey
halilsalihorhan@gmail.com

Abstaction – Wireless Personal Area Networks (WPANs) are used to connect devices in close proximity to a single user, but the transmitted data can be vulnerable to security threats. In this paper, we review the current state of security in WPANs and discuss the challenges of using cryptographic and trust-based algorithms, which can have vulnerabilities and incur additional power costs. We propose a distance-based spatial filtering security algorithm that uses signaling information to calculate the spatial positions of devices in a network and limits the actions of devices based on their positions. This approach improves the security and efficiency of WPANs and provides a solution to the challenges of using cryptographic and trust-based algorithms.

Keywords – spatial filtering, security of networks, WPAN

I. Introduction

Wireless Personal Area Networks (WPANs) are a type of wireless network that is used to connect devices in close proximity to a single user, typically within a few meters. These networks are used in a variety of applications, including wearable devices, home automation systems, and medical devices. However, the use of WPANs also raises concerns about the security of the transmitted data. In this paper, the current state of security in WPANs is reviewed and various threats and challenges that need to be addressed is discussed, then a distance-based spatial filtering security algorithm is suggested.

II. Background

A- Cryptographic techniques:

As stated in [2], AES is chosen to be the basic security approach for MAC sub layer in IEEE 802.15.4b standard. An AES system is a symmetric-key encryption by using a shared key between system ends. Yet, deciphering AES encrypted messages on a very low power and less computational devices, like most component of WPANs, is very hard to manage [3].

Despite the challenges of implementing AES on low-power devices, it is still widely used in WPANs due to its strong security and widespread adoption. For that reason, in most of the researches are focused on optimizing AES processers [2-3]. One approach is to use hardware accelerators, which are dedicated circuits designed specifically for the efficient execution of AES algorithms [4]. Another approach is to use software optimization techniques, such as parallelization and reduced instruction set computing [5], to improve the performance of AES on low-power devices.

Threshold cryptography is a type of cryptographic system that involves splitting a key into multiple pieces, known as "shares," and distributing them among different devices or participants. The key can only be reconstructed and used to decrypt a message when a sufficient number of shares are brought together. This approach has the advantage of being more secure, since an attacker would need to compromise a sufficient number of devices or participants in order to obtain the complete key. However, it can also be more complex and require more coordination among the devices or participants in order to use the key. The dynamic distributed key management method mentioned in [7] is a specific technique for managing and distributing the shares of a threshold key in a way that is flexible and can adapt to changes in the system, such as the addition or removal of devices or participants.

B- Trust-based techniques:

Due to the lack of central authority for authentication and authorization of WPANs, it is difficult to establish trust among devices in the network. To address this challenge, several trust-based techniques have been proposed for securing WPANs.

On this topic, different algorithms are suggested, to calculate trustworthiness of other devices and to decide whether to establish connection with them. However continuous calculation of trusts is power consuming.

For these challenges, [6] suggests sub-trust-networks by slicing networks and defining one device of each subnet as authority.

III. Definition Of Problem

The security of wireless personal area networks (WPANs) is an important concern, given the sensitive nature of the information that is often transmitted over these networks. Cryptographic and trust-based algorithms are commonly used to secure communication and establish trust among devices in WPANs. However, these algorithms are not perfect and can have vulnerabilities or weaknesses that can be exploited by attackers. This is a significant problem because it can compromise the security and integrity of the network and the information being transmitted, potentially leading to data breaches, unauthorized access, and other security incidents.

Additionally, the use of cryptographic and trust-based algorithms can incur an additional power cost, which can be a significant issue in WPANs that rely on battery-powered devices. This can reduce the efficiency and lifespan of these devices and may also limit the use of these algorithms in certain situations.

Overall, the challenges and implications of using cryptographic and trust-based algorithms in WPANs highlight the need for a solution that can address these problems and improve the security and efficiency of these networks.

IV. Explanation Of Technique

According to [1], we can use signaling information to calculate distances in connections, and by using this distance information to calculate the spatial position of all devices in a network. This is the key data that our technique will rely on.

We also know that some devices need proper positions to action. For instance, if a smartwatch is on the left arm, it should not be in action when it is positioned rightest part of spatial sphere; or a use of debit card can not be happened when it is in one's pocket or pack.

With position of devices and limitation of devices' actions, the network can flag this as a potential security breach and take appropriate action to protect the user's data. Overall, the use of signaling information to calculate the spatial positions of devices in a network can greatly improve the security of the network.

V. Pseudo Code

Inputs:
A: predefined accepted position areas of device's action;
R: predefined rejected position areas of device's action;
Output:
b: is action secure
Algorithm:
Step 1. p = Spatial Positioning (using algorithm in [1])
Step 2. If p is in R, return false
Step 3. If p is in A, return true
Step 4. return false

Fig. 1 Outline of the spatial filtering action validation algorithm

VI. Conclusion

In conclusion, the security of WPANs is a crucial concern due to the sensitive nature of the data transmitted over these networks. Cryptographic and trust-based algorithms are commonly used to secure communication and establish trust among devices, but these algorithms have vulnerabilities and can incur additional power costs. The proposed distance-based spatial filtering security algorithm addresses these issues by using signaling information to calculate the spatial positions of devices in a network and limiting the actions of devices based on their positions. This approach improves the security and efficiency of WPANs and provides a solution to the challenges and implications of using cryptographic and trust-based algorithms.

VII. References

[1] A. Kushki, K. N. Plataniotis and A. N. Venetsanopoulos, "Kernel-Based Positioning in Wireless Local Area Networks," in *IEEE Transactions on Mobile Computing*, vol. 6, no. 6, pp. 689-705, June 2007, doi: 10.1109/TMC.2007

[2] Y. Q. Zhong, J. M. Wang, Z. F. Zhao, D. Y. Yu and L. Li, "A Low-cost and High Efficiency Architecture of AES Crypto-engine," 2007 Second International Conference on Communications and Networking in China, 2007, pp. 308-312, doi: 10.1109/CHINACOM.2007.4469389.

[3] F. S. Hossain, M. L. Ali and M. A. Al Abedin Syed, "A very low power and high throughput AES processor," 14th International Conference on Computer and Information Technology (ICCIT 2011), 2011, pp. 339-343, doi: 10.1109/ICCITechn.2011.6164810.

[4] J. K. -T. Chang, S. Liu, J. -L. Gaudiot and C. Liu, "Hardware-assisted security mechanism: The acceleration of cryptographic operations with low hardware cost," International Performance Computing and Communications Conference, 2010, pp. 327-328, doi: 10.1109/PCCC.2010.5682293.

[5] T. Good and M. Benaissa, "Very small FPGA application-specific instruction processor for AES," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 53, no. 7, pp. 1477-1486, July 2006, doi: 10.1109/TCSI.2006.875179.

[6] Parvin, S., Gawanmeh, A., Venkatraman, S., Alwadi, A., Al-Karaki, J. N., & Yoo, P. D. (2021). A trust-based authentication framework for security of WPAN using network slicing. *International Journal of Electrical & Computer Engineering (2088-8708)*, *11*(2).

[7] Ji-eun Song, Byong-ho Chung and Kyo-il Chung, "A distributed certificate key management method in IEEE 802.15.3 WPAN environment," The 7th International Conference on Advanced Communication Technology, 2005, ICACT 2005., 2005, pp. 1019-1022, doi: 10.1109/ICACT.2005.246132.