AI-based Enhancing of the Smart City Residents' Safety

Sabina Szymoniak
Czestochowa University of Technology
Czestochowa, Poland *sabina.szymoniak@icis.pcz.pl*

Mariusz Kubanek
Czestochowa University of Technology
Czestochowa, Poland *mariusz.kubanek@icis.pcz.pl*

Shalini Kesar
Southern Utah University
Cedar City, USA *kesar@suu.edu*

Abstract

Smart Cities are urban environments that use digital technology and data-driven solutions to improve citizens' efficiency, sustainability, and quality of life, especially using Artificial Intelligence to improve human lives. These methods can also help urban residents in dangerous situations by detecting dangerous situations and securing communication during emergency services notifications. In this paper, we present the security protocol that ensures secure communication during the notification of emergency services. This protocol is secure, lightweight, and scalable. We verified its security using an automated tool that did not detect a protocol attack.

Keywords: security, Smart City, Artificial Intelligence.

1. Introduction

Smart Cities (SCs) are urban environments that leverage digital technology and data-driven solutions to optimize citizens' efficiency, sustainability, and general quality of life. Also, they utilize Artificial Intelligence (AI) methods to analyze gathered data, enabling the devices to function autonomously or anticipate specific scenarios [14, 5].

Given the indispensability of smart devices in our daily lives, we have opted to utilize them to enhance security in SCs. This issue involves two research challenges and questions. The first is detecting dangerous situations (for example, fainting or fighting) in SC and notifying emergency services. The second challenge is securing communication during emergency services notifications to avoid cyber threats [5, 4]. This challenge is this paper's main theme.

This paper presents a security protocol that ensures secure communication. The protocol is part of a theoretical framework that utilizes a network of IoT devices to create an intelligent system that supports notification of emergency services using AI methods that enhance the detection and security of situations threatening SC residents' health and life. This paper's main contribution is the security protocol assumptions supported by the network and software assumptions of the proposed framework.

The rest of this paper is organized as follows. Section 2 will present related works and our motivations for taking up this research topic. Section 3 will present a security protocol. The last section includes our conclusions and plans for further work.

2. Related Works

Securing communication between devices is a critical and complex matter. Developing a communication security protocol necessitates carefully considering various elements, including cryptographic operations to enhance security, the specific problems that the solutions address, computational capabilities and device efficiency, and the network's architecture. We analysed existing solutions like [1, 2, 3, 7, 10, 8, 9, 6, 11, 13, 14].

Based on this, we recognized the need for the protocol to possess portability, security, and scalability. Also, the protocol's security should be directly linked to the confidentiality and integrity of the transmitted data and the authenticity and resilience against attacks. Additionally, we have come to understand that the scalability of a security protocol pertains to the computational resources required by both the device and the entire network to carry out its operations. So, we prepare a lightweight and secure security protocol to ensure SC communication as a part of the framework that supports notifying emergency services. Our solution uses efficient techniques such as hash functions, certificates, and pseudonymization.

3. Security Protocol for Emergency Services Notification

To better understand the protocol's operation in the context of the framework idea, Figure 1 shows communication flow in the proposed security protocol. In the subsequent subsections, we will describe each protocol's phase.

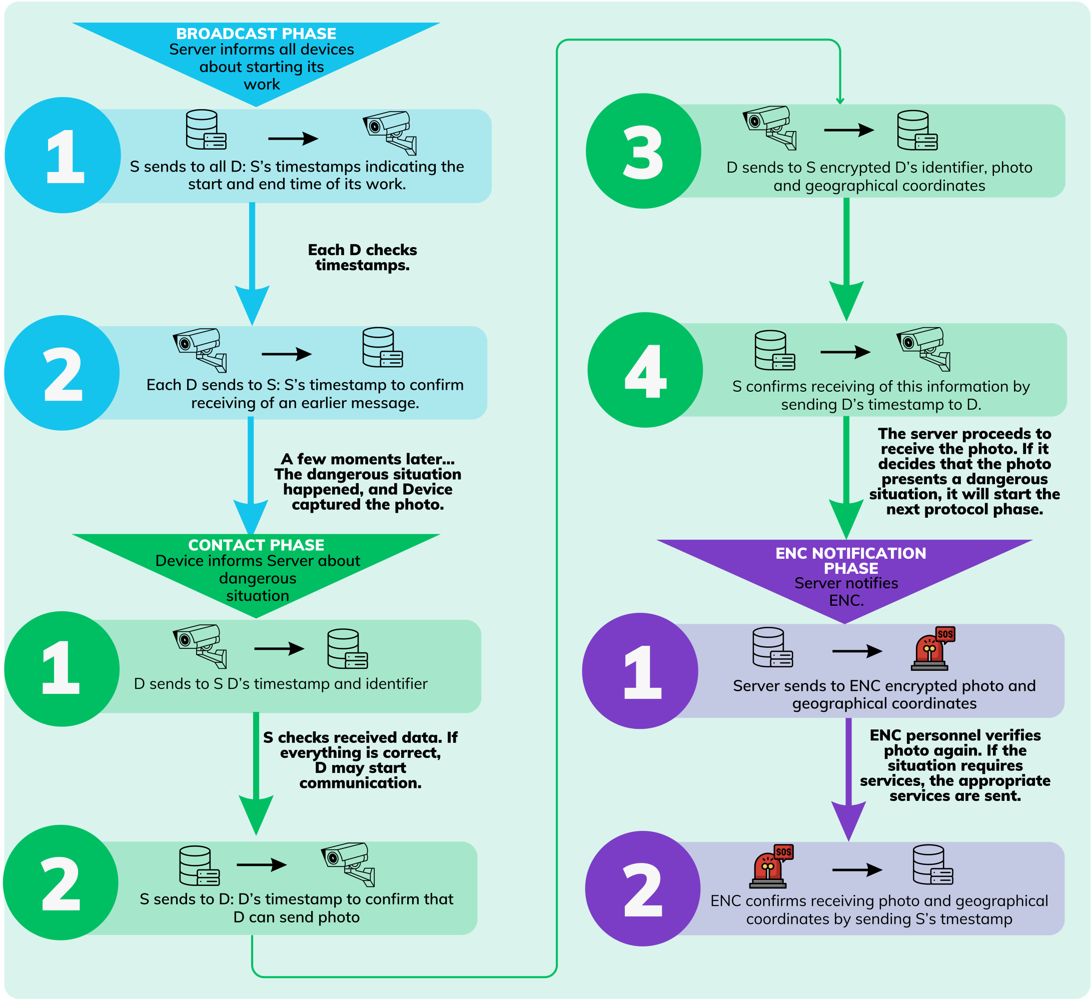
BROADCAST PHASE
Server informs all devices about starting its work
1
S sends to all D: S's timestamps indicating the start and end time of its work.
Each D checks timestamps.
2
Each D sends to S: S's timestamp to confirm receiving of an earlier message.
A few moments later... The dangerous situation happened, and Device captured the photo.
CONTACT PHASE
Device informs Server about dangerous situation
1
D sends to S D's timestamp and identifier
S checks received data. If everything is correct, D may start communication.
2
S sends to D: D's timestamp to confirm that D can send photo
3
D sends to S encrypted D's identifier, photo and geographical coordinates
4
S confirms receiving of this information by sending D's timestamp to D.
The server proceeds to receive the photo. If it decides that the photo presents a dangerous situation, it will start the next protocol phase.
ENC NOTIFICATION PHASE
Server notifies ENC.
1
SOS
Server sends to ENC encrypted photo and geographical coordinates
ENC personnel verifies photo again. If the situation requires services, the appropriate services are sent.
2
SOS
ENC confirms receiving photo and geographical coordinates by sending S's tmestamp

Fig. 1. Communication flow in proposed security protocol.

3.1. Protocol's broadcast phase

The broadcast phase informs IoT devices that the framework will commence operations. The operational time of the framework in an SC may vary depending on the prevailing circumstances, including the frequency and severity of threats and dangerous situations. It can operate for the entire day or a limited time, such as during nighttime. Additionally, the framework can oversee the entire city or selectively target specific sections inside the SC. Therefore, the trusted server must inform every device that the framework will commence its operations.

Here, the framework will carry out the broadcast phase of the protocols (in two steps). Initially, the trusted server transmits two timestamps to each device, specifying the framework's activity time to maintain the integrity of the timestamp value. As a response, each device shall transmit the timestamp to the server, indicating the beginning time. The messages in both steps are encrypted using a symmetric key shared between the device and the trusted server.

3.2. Protocol's contact phase

The contact phase initiates a linkage between the device and the trusted server. Initially, the device attempts to authenticate itself to the trusted server and provide a report regarding the potential occurrence of a hazardous circumstance. It transmits its identity and a freshly generated timestamp to the server. The trusted server verifies the device's identity by cross-referencing it with its database. Upon successful identity verification, the trusted server transmits the device's timestamp to indicate that communication is feasible, constituting the second stage. The messages in both steps are encrypted using a symmetric key shared between the device and the server. During the third step, the device transmits the recorded photograph, device identifier, and geographical coordinates to the trusted server. This message is encrypted using a symmetric key shared between the device and the trusted server. Furthermore, this identical key encrypts the photo file and the geographical coordinates to prevent cyberattacks. The trusted server verifies the message's receipt based on the device's timestamp. Next, the trusted server can analyze and authenticate the received photograph using AI methods and inform the ENC if required.

3.3. Protocol's ENC notification phase

If the trusted server chooses to inform the ENC, it will carry out the ENC notification phase of this protocol. Initially, the trusted server transmits the acquired photograph and the scenario's geographical coordinates to ENC. Both items are encrypted using a symmetric key shared between the ENC and the trusted server. Furthermore, the trusted server appends its timestamp to this message. During the second step, the ENC verifies the message's receipt and transmits the recently generated timestamp to the trusted server. Subsequently, the ENC personnel will examine the photograph and determine whether to dispatch rescue services to aid injured individuals or safeguard the vicinity.

3.4. Automated Security Analysis Results

We preliminarily investigated our protocol and checked its correctness and security using an automated verification method. We used a tool for automated verification mentioned in [12]. The tool did not find any attack on our protocol. The protocol's specification in Alice-Bob notation and test results are available at `https://github.com/spverification1/isd2024`.

4. Conclusions

In this paper, we presented the security protocol, which is the part of the framework that will enhance the detection and securing of situations that threaten the health and life of residents of a SC. We suggested the necessary phases of the security protocol (broadcast, contact, and

ENC notification). We performed preliminary protocol verification via methodology described in [12]. The tool did not find attacks for any protocol phase during these tests.

In future work, we will focus on the whole framework to ensure safe communication and notification of emergency services. We will continue testing our protocol and add the ability for regular smartphone users to appear, improving the protocol's complexity. Next, we will prepare the necessary software for all devices. We will also test the correctness of framework operations, during which the correctness of recognizing dangerous situations and communication using the proposed protocol will be checked.

References

[1] Akram, M. A., Ahmad, H., Mian, A. N., Jurcut, A. D., and Kumari, S.: Blockchain-based privacy-preserving authentication protocol for UAV networks. In: *Computer Networks* (2023), p. 109638.

[2] Attir, A., Naıt-Abdesselam, F., and Faraoun, K. M.: Lightweight anonymous and mutual authentication scheme for WBAN. In: *Computer Networks* (2023), p. 109625.

[3] Bagga, P., Sutrala, A. K., Das, A. K., and Vijayakumar, P.: Blockchain-based batch authentication protocol for Internet of Vehicles. In: *Journal of Systems Architecture* 113 (2021), p. 101877.

[4] Hussain, S. S., Farooq, S. M., and Ustun, T. S.: Analysis and implementation of message authentication code (MAC) algorithms for GOOSE message security. In: *IEEE Access* 7 (2019), pp. 80980–80984.

[5] Jia, X., Luo, M., Wang, H., Shen, J., and He, D.: A Blockchain-Assisted Privacy-Aware Authentication scheme for internet of medical things. In: *IEEE Internet of Things Journal* 9.21 (2022), pp. 21838–21850.

[6] Maes, R. and Verbauwhede, I.: Physically unclonable functions: A study on the state of the art and future research directions. In: *Towards Hardware-Intrinsic Security* (2010), pp. 3–37.

[7] Nita, S. L. and Mihailescu, M. I.: Elliptic Curve-Based Query Authentication Protocol for IoT Devices Aided by Blockchain. In: *Sensors* 23.3 (2023), p. 1371.

[8] Nyangaresi, V. O.: Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. In: *Ad Hoc Networks* 142 (2023), p. 103117.

[9] Park, Y., Ryu, D., Kwon, D., and Park, Y.: Provably secure mutual authentication and key agreement scheme using PUF in internet of drones deployments. In: *Sensors* 23.4 (2023), p. 2034.

[10] Pushpa, S. X. and Raja, S.: Elliptic curve cryptography based authentication protocol enabled with optimized neural network based DoS mitigation. In: *Wireless Personal Communications* 124.1 (2022), pp. 1–25.

[11] Sikarwar, H. and Das, D.: SMMAP: Secure MAC-based Mutual Authentication Protocol for IoV. In: *24th International Conference on Distributed Computing and Networking*. 2023, pp. 330–335.

[12] Szymoniak, S.: Security protocols analysis including various time parameters. In: *Mathematical Biosciences and Engineering* 18.2 (2021), pp. 1136–1153.

[13] Wu, T.-Y., Guo, X., Chen, Y.-C., Kumari, S., and Chen, C.-M.: SGXAP: SGX-Based Authentication Protocol in IoV-Enabled Fog Computing. In: *Symmetry* 14.7 (2022), p. 1393.

[14] Zhong, H., Gu, C., Zhang, Q., Cui, J., Gu, C., and He, D.: Conditional privacy-preserving message authentication scheme for cross-domain Industrial Internet of Things. In: *Ad Hoc Networks* (2023), p. 103137.