Blockchain Based Secure Communication for IoT Devices in Smart Cities

Ramazan Yetis
National Defence University
Hezarfen Aeronautics and Space Technologies Institute
Istanbul, Turkey 34158
ryetis@hho.edu.tr

Ozgur Koray Sahingoz
Istanbul Kultur University
Computer Engineering Department
Istanbul, Turkey 34158
sahingoz@gmail.com

***Abstract*—In smart city technologies we have witnessed advanced technological improvements in small computing devices, which can be connected to the Internet and named as Internet of Thing (IoT) devices, and cooperatively working complex systems. With this increased use of new technologies, the security problem is becoming more and more important because complex systems lead to unpredictable security vulnerabilities, which result in financial and private information losses. As a recently emerged technology, Blockchain was emerged as an alternative solution to security breaches of a different application environment. In contrast to the central structure used by most systems, it is preferred especially in the area of security by its distributed structure and the cryptographic hash algorithm it uses.**

Today, structures such as Smart Home, Smart City, Smart Environment and Smart Agriculture, which are created by using IoT are seen as active research areas with more security shortages. The reason for the security weakness in these areas arises from the hardware restriction on the IoT devices used. In the proposed system, an authorization system for IoT devices has been tried to be set up by using the distributed node structure of Blockchain system and blocks kept in these nodes. UDP (User Datagram Protocol), which uses a simple communication model without establishing a connection to the minimum protocol mechanism for communication of nodes in the system, was preferred. The communication between the nodes has been encrypted using encryption methods, thus creating a secure environment.

Keywords-smart home; IoT; secure communication; blockchain; hashing

I. Introduction

In recent years, smart city technologies have gained an increasing demand not only from academics but also from industrial fields in the construction of urbanization projects, which are motivated by the governments. There is an increasing trend in the living of the urban areas, especially smart cities due to the benefits of economic development, capital and/or operational cost savings, resiliency for critical operations, enhanced services for residents, safety and security [1].

To accommodate this increasing demand on urbanization, authorities are turning to the Internet of Things (IoT) innovation to increase the quality of lives, decrease the cost of services, and improve communication models [2]. The potential of IoT technologies enables it to enter nearly every aspect of smart city applications such as public transportation, energy efficient buildings, public safety, etc.

According to the statistics of [3] the number of Internet of Thing (IoT) devices are increasing year by year in an exponential rate. Besides, it is easily foreseen that in the future use of IoT devices will be located exactly at the heart of the smart city solutions. Therefore, the related service qualities and security requirements of the IoT applications must be solved by the engineers.

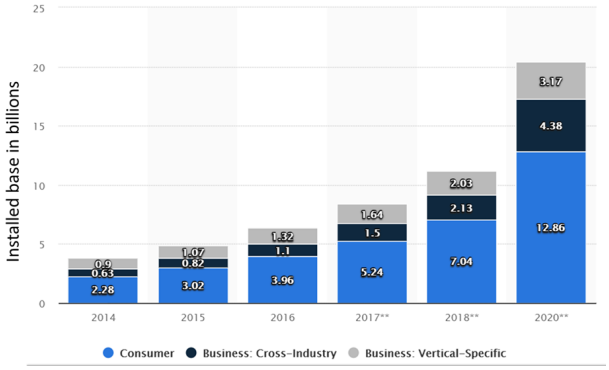

Fig. 1. Advantages of Smart Cities

Most of the IoT devices are used some messaging applications, which are widely used in the developing world, bring with its easy usage and features, as well as the central communication structure and security risks and suspicion of privacy. Because of these risks, the structures created by Blockchain technology, which has the distributed structure and can be approved by all the hosts in the network are more reliable.

A blockchain is an incremental record called blocks that are interconnected using cryptography. Each block contains an encryption frame of the previous block, a timestamp, and transaction data (usually shown as a Merkle tree root hash).

In general, in the Smart Home concept, in the event that the central router is attacked, the smart home and all the devices are broadly clarified for any attack. Malicious software such as trojans or backdoors can be placed on home computers, all network traffic can be monitored, and smart devices can be managed remotely. However, many of these smart devices can also be directly attacked without having to go through a router.

978-1-7281-1315-9/19/$31.00 ©2019 IEEE

Many smart devices are protected by default password and administrator credentials, and in some cases, they cannot be changed. In the smart home system, more nodes mean faster hacking. The simple or default passwords used in nodes can also be considered as openness.

The purpose of the proposed system is to create an authorization and secure messaging environment for IoTs with limited resources. Unlike the central structures used in smart home systems, the system is deployed in a distributed manner so that any node closes does not interfere with the system. The nodes recognize each other via the Blockchain and respond to received messages. The Blockchain structure, which is being implemented in many areas, can also be used in the security of the communication environment. In this project, a distributed structure was established, and the Blockchain structure was tried to be used for secure messaging.

The rest of the paper is organized as follows. In Section 2 the related works on the research area are listed and detailed. The methodology of the proposed system is detailed in Section 3. Experimental results are depicted in Section 4, and finally, conclusions and future works are drawn.

II. Related Work

In paper [4], authors proposed IoTChain, which is an architecture that combines OSCAR elements and the ACE authorization framework. The idea is to make the ACE authorization stage reliable and flexible. In [5], authors proposed a hybrid distributed architecture for a sustainable smart city network, focusing on limitations that provide low latency, reduce bandwidth usage and improve security and privacy and scalability. A memory-hardened PoW scheme was used in the proposed models to ensure security and confidentiality and to prevent tampering with attackers. In a similar study, Minoli et al. emphasized some IoT environments where Blocking Mechanisms (BCMs) play an important role and at the same time they pointed out that BCMs are only part of the IoTec solution (IoTec) [6]. In [7] authors introduced a relatively new blockchain technology to solve the communication problem between different types of machines in CPS. According to the principles of Blockchain technology, they designed a blockchain for secure M2M communication.

On the other hand, paper [8] proposed a real-time Blockchain-based incentive mechanism for Peer-to-Peer (P2P) applications that implement a crypto-currency, such as Bitcoin, to encourage users to collaborate. In [9], a detailed analysis of the role of blockchain in tracking sources of distrust in supply chains related to IoT devices is presented. The paper also examines how the blockchain may make it possible to contain an IoT security breach in a targeted manner after it has been discovered. At this front, it discusses and evaluates the initiatives of organizations, inter-organizational networks, and sectors.

In [10], papers discussed various possible security and privacy issues in IoT. These are defined based on observations in the IoT component interaction. Blockchain technology is defined as one of the solutions addressing problems and challenges in IoT. The paper describes the scope of blockchain integration with IoT. Besides, various possible applications of IoT with blockchain technologies have been highlighted. Finally, the difficulties in IoT with blockchain technology are also described. In the article [11], the authors of this article proposed a blockchain modification based on a floating genesis block, which makes it possible to solve problems caused by the unlimited growth of the blockchain and to implement safe routing protocols based on Blockchain technology. Secure routing enables the VANET / MANET network nodes to control the system as well as connect with the security services defined by the software.

In [12], they propose a method for sending secret messages over a blockchain that is considered a payment platform. Because of Blockchain's invariant nature, the sender has the ability to embed it. However, because everyone is free to pay in the chain, they apply these payments to a recipient to send encrypted messages. In the paper [13], they look more deeply at the technical building blocks of cyber threats to smart homes and define the basic classification criteria that help shape the attack scene. They do not claim that this taxonomy can be comprehensive. However, they can significantly highlight motivations, resources, vulnerabilities and their effects to identify and characterize current and potential future cyber threats in the smart home and help identify problem areas for their defense measures.

On the other site, some authors focused on setting up a publish-subscribe communication paradigm to set up a messaging paradigm between the IoT sensor nodes as seen in [14], [15]. In this mechanism there is not a great communication range of the nodes. Therefore they need to set up a hop-by-hop communication model for sending the related message to the target nodes. However, to set up a secure messaging, you need to use some additional encryption mechanisms.

Fig. 2. Smart City Environment and Components

In the paper [16], they present a smart city architecture by briefly introducing the building blocks (so-called planes), i.e., the application, communication, detection, data and security planes. Upon a brief introduction of the architectural building blocks, they move to their primary focus, which is the planes of perception, communication, and security. In the operation

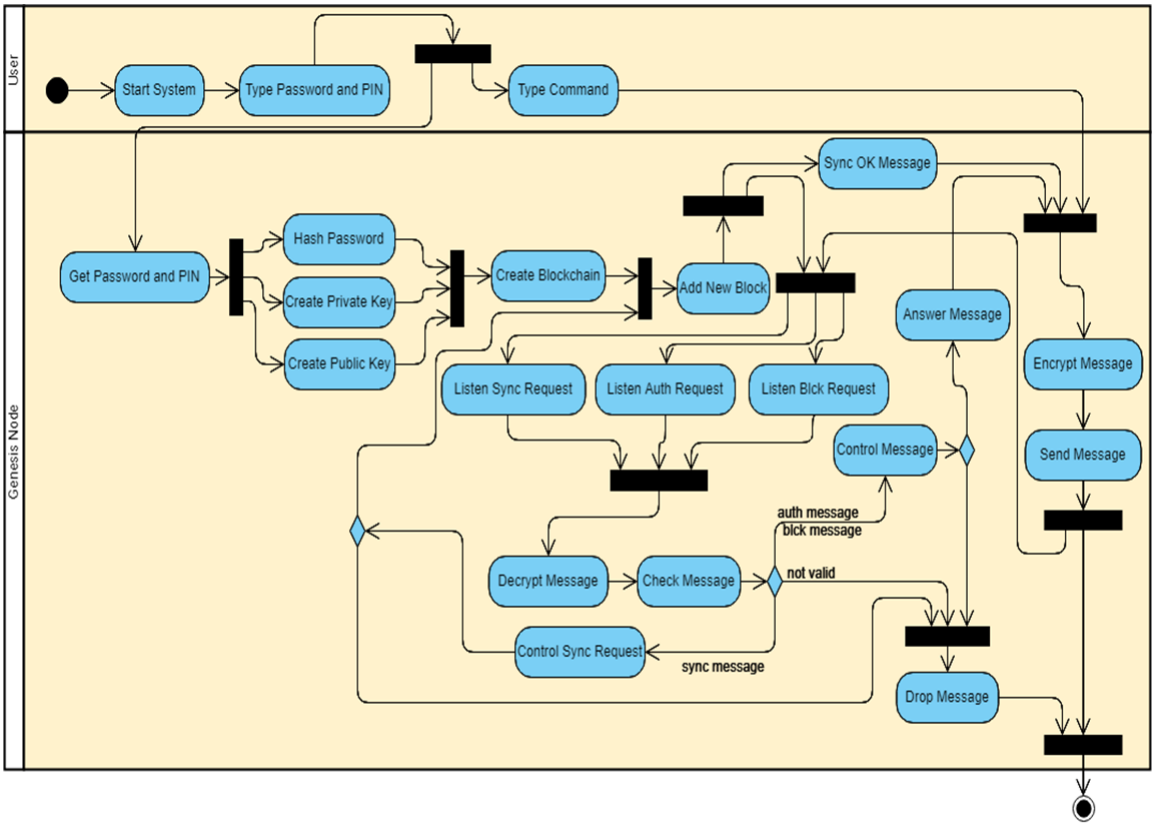

Fig. 3. Workflow of the system

of the sensor plane, they offer dedicated and non-specific detection paradigms for various smart city applications. They probe the types of sensors, the problems experienced by the relevant smart city applications, the existing solutions and the communication technologies used by the sensors.

III. Methodology

A. Workflow of the System

The activity diagram starts with the user running the system. After the system starts, the user determines the password and PIN. The system uses this password and PIN to generate the password hash summary, private key, and public key. Adds these parameters as the first node to the blockchain it creates. Because the previous node is not present when adding the first node, it creates the previous node hash with the genesis message it receives from the user. The system, which was started as the first node, starts listening to synchronization, authentication, block, and task requests. By decrypting the incoming synchronization request message, it adds the node information that it creates from the parameters in its content to the blockchain as the next block. Sends the synchronization request by encrypting the confirmation message to the sending node. Second, it receives the incoming authentication request and decrypts it by comparing the node ID sent with the node IDs in the blockchain. If the node ID is valid, it sends the confirmation message by encrypting it, if not, it drops the incoming request. By decrypting the confirmation message, the receiving node finally requests a block. Blocks the block message by decrypting the system message. If the block number of the system is large, the blocks are sent to the requesting node, if not, it requests blocks from the requesting node. The node that updates the block also starts to listen for synchronization, authentication, and block requests. The activity diagram is shown in Figure 3.

B. Implementation of the System

The proposal aims a Smart City environment as depicted in Figure 2. As can be seen from this environment there are lots of components in the Smart City Platforms such as education, smart health, public safety, gas/water detectors, smart parking, waste management, smart street lights, smart home, etc. All these components have some computing agents in them and depending on their creation aim; they need to communicate with other computing agents in the environment. This communication generally needs to be executed in an insecure medium such as wireless communication over the air. Therefore there is a need to set up a secure communication platform in a smart city environment.

Because it is set up on a distributed structure, there is no centralized server/authority/machine in the proposed system. The application was developed using the Python programming language. The Blockchains used by the system were created

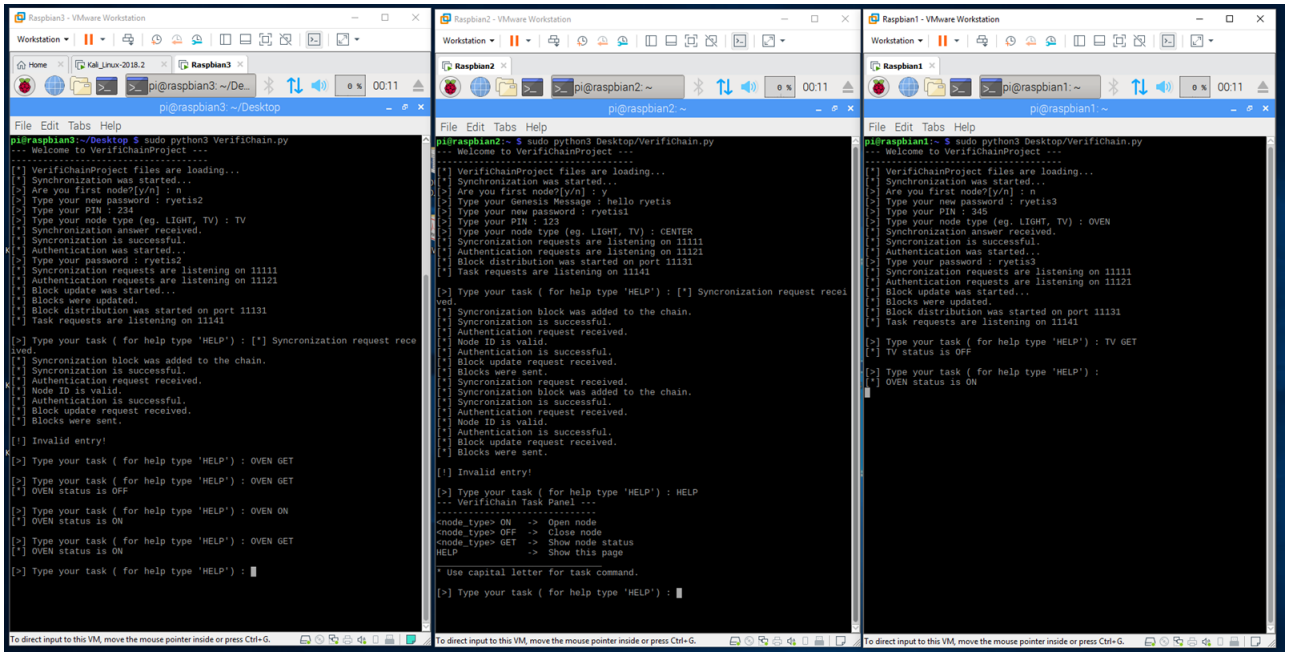

Fig. 4. System test on 3 nodes

using the JSON (JavaScript Object Notation) library. Using the Socket library, communication was made on the network using the UDP (User Datagram Protocol) protocol. The Vigenere cipher encryption method was used to encrypt messages in unsafe UDP-based communication. The SHA256 hash function is preferred to create a password, private key, and public key. Application 3 Raspbian (Debian based Linux System) operating system has been tested by running on the installed node.

C. Testing the System

The Raspbian Linux operating system, which is used as the node installed on the Vmware virtualization platform for the testing phase, started with three machines and the application file (VerifiChain.py) was uploaded.

The ”sudo python3 VerifiChain.py” command was entered by running the terminal on the nodes. This command is a general command used to run scripts written in the Python programming language. With this command, the application starts, and the application asks the user whether the first node is in the system. Because the Raspbian2 machine is the first node in the system, the user enters the ”y” for ”yes” response. Any subsequent nodes are included in the system by replying to this question, ”n”. After this response, the user is prompted to enter the password, PIN and node type. After the user enters this information, the first node completes the setup process and listens for the future requests and commands from the user. Other nodes first request synchronization from active nodes. Sends an authentication request after receiving the confirmation. The authenticated node finally requests blocks. It saves the blocks it receives from other nodes in its own blockchain and listens for future requests such as other nodes and commands from the user.

The node that receives the commands the user enters publishes the message to other nodes. The node that receives and is related with the command changes its state and sends information to the requesting node. All stages are shown in Figure 4.

IV. Experimental Results

When the results of the tested project are examined, it is seen that the ”nodechain.json” file created by the nodes is an empty list in the initial setup and synchronization phase. After the block update process after the authentication phase, as in Fig. 5, it is observed that the blocks from other nodes connected to the file are added. In the development phase of the project, the contents of the UDP packet, which is sent without encryption and is obtained by using the Wireshark program before the secure communication criteria are determined, is shown in Fig. 6. However, there is still some security vulnerability in the messaging paradigm of the components. They are sent without encryption. If some intruders want to sniff them and regenerate the same message again, they can easily accomplish this. In the third version of the project, it is aimed to use an encryption mechanism. The content of the UDP packet sent after the encryption as in Fig. 7.

As a result, it is seen that the system uses the blockchain structure, provides the confidentiality of network traffic which is an important criterion in secure communication, has authentication system and can be implemented to every system because it is coded with python.

V. Conclusions and Future Works

Considering the safety studies on IoT devices, many suggestions have been made. In this proposed project, the

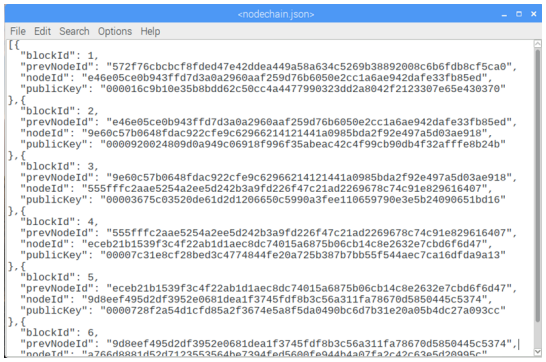

Fig. 5. nodechain.json file after blockchain update

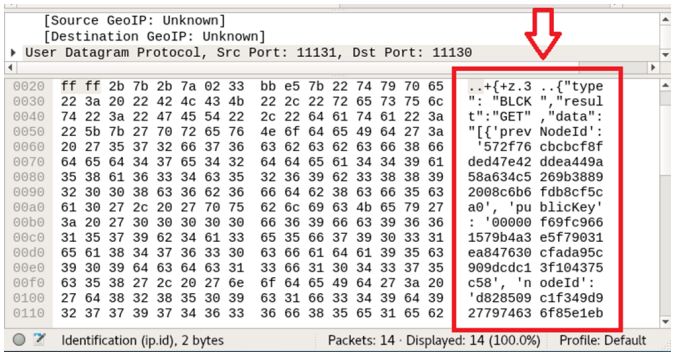

Fig. 6. UDP packet before encryption mechanism

authentication process was carried out by using the blockchain structure. Generally, since the IoT devices prefer the UDP protocol instead of the IP protocol, communication is provided in the proposed system using the UDP protocol. Unsafe UDP communication is considered, and the message content is encrypted by using Vigenere Cipher encryption method. This study shows that blockchain technology can be used for the security of IoT devices, and the authentication methods derived for the blockchain structure for communication security can be used to encrypt the messages used in communication. As a result of the tests carried out in the proposed project, some problems related to communication arising from the UDP protocol have been encountered. When any node used in the project was closed and reopened, it was seen that the blocks added to the blockchain of the other nodes were added to their blockchain as long as they were closed. It is considered that the proposed project could serve as an example for other projects that will use blockchain technology.

REFERENCES

[1] "Icma survey research: 2016 smart cities survey summary report," https://icma.org/documents/icma-survey-research-2016-smart-cities-survey-summary-report, accessed: 2019-01-05.

[2] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, "Security and privacy in smart cities: Challenges and opportunities," *IEEE Access*, vol. 6, pp. 46 134–46 145, 2018.

[3] "Smart cities - statistics & facts," https://www.statista.com/topics/4448/smart-city/, accessed: 2019-01-05.

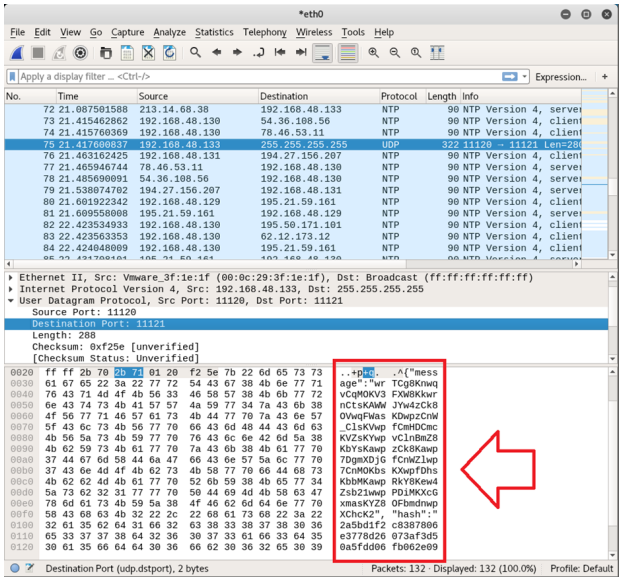

Fig. 7. UDP packet after encryption mechanism

[4] O. Alphand, M. Amoretti, T. Claeys, S. Dall 'asta, A. Duda, G. Ferrari, F. Rousseau, B. Tourancheau, L. Veltri, and F. Zanichelli, "IoTChain: A Blockchain Security Architecture for the Internet of Things," in *IEEE Wireless Communications and Networking Conference*, Barcelona, Spain, Apr. 2018.

[5] P. K. Sharma and J. H. Park, "Blockchain based hybrid network architecture for the smart city," *Future Generation Computer Systems*, vol. 86, pp. 650 – 655, 2018.

[6] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for iot security," *Internet of Things*, vol. 1-2, pp. 1 – 13, 2018.

[7] S. Yin, J. Bao, Y. Zhang, and X. Huang, "M2m security technology of cps based on blockchains," *Symmetry*, vol. 9, no. 9, 2017.

[8] Y. He, H. Li, X. Cheng, Y. Liu, C. Yang, and L. Sun, "A blockchain based truthful incentive mechanism for distributed p2p applications," *IEEE Access*, vol. 6, pp. 27 324–27 335, 2018.

[9] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications Policy*, vol. 41, no. 10, pp. 1027 – 1038, 2017, celebrating 40 Years of Telecommunications Policy A Retrospective and Prospective View.

[10] N. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in iot," *Procedia Computer Science*, vol. 132, pp. 1815 – 1823, 2018, international Conference on Computational Intelligence and Data Science.

[11] A. Busygin, M. Kalinin, and A. Konoplev, "Supporting connectivity of vanet/manet network nodes and elastic software-configurable security services using blockchain with floating genesis block," *SHS Web of Conferences*, vol. 44, p. 00020, 01 2018.

[12] J. Partala, "Provably secure covert communication on blockchain," *Cryptography*, vol. 2, no. 3, 2018.

[13] R. Heartfield, G. Loukas, S. Budimir, A. Bezemskij, J. R. Fontaine, A. Filippoupolitis, and E. Roesch, "A taxonomy of cyber-physical threats and impact in the smart home," *Computers & Security*, vol. 78, pp. 398 – 428, 2018.

[14] H. Cam, O. K. Sahingoz, and A. C. Sonmez, "Wireless sensor networks based on publish/subscribe messaging paradigms," in *Advances in Grid and Pervasive Computing*, J. Riekki, M. Ylianttila, and M. Guo, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 233–242.

[15] Y. Tekin and O. K. Sahingoz, "A publish/subscribe messaging system for wireless sensor networks," in *2016 Sixth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, July 2016, pp. 171–176.

[16] H. Habibzadeh, T. Soyata, B. Kantarci, A. Boukerche, and C. Kaptan, "Sensing, communication and security planes: A new challenge for a smart city system design," *Computer Networks*, vol. 144, pp. 163 – 200, 2018.