Future Generation of Communication and Internet of Things (FGCIOT)

Journal homepage: https://sanad.iau.ir/journal/fgciot/

PAPER TYPE (Research paper)

Secure protocol for communications in IoT-based wireless sensor networks using kerberos and elliptic curve cryptography

Atefeh Moradi[1], Mohammad Ahmadinia[1,*] ,Mohammad Hosein Davarpour[2]

[1] Department of Computer Engineering, Kerman Branch, Islamic Azad University, Kerman, Iran

[2] Department of Computer Engineering, Semnan Branch, Islamic Azad University, Semnan, Iran

Article Info

Article History:
Received: 15 October 2023
Revised 14 December 2023
Accepted 27 December 2023

Keywords:
Internet of Things, Wireless Sensor Network, Security, Kerberos, Elliptic Curve

*Corresponding Author's Email Address: ahmadinia@gmail.com

Abstract

The Internet of Things (IoT) is an emerging field of study and operation. IoT creates a structure for internet-connected devices. IoT-enabled systems are susceptible to various security and privacy attacks due to their inherently open nature. In IoT-enabled systems, multimedia information moves from one end to another, and computational complexity with constrained environments such as ad-hoc networks, mobile networks, etc., is crucial. Wireless Sensor Networks (WSNs) consist of a large number of sensor nodes, each with very limited computational power and storage capacity. Sensor nodes are typically installed for monitoring activities in unsupervised locations, controlled by one or more gateway nodes. Maintaining the confidentiality of information communication is one of the main challenges, and preserving the privacy of multimedia data from unauthorized access by attackers is a major issue for active WSNs with IoT. In this paper, to leverage the benefits of the Kerberos encryption protocol and reduce overhead for IoT-based wireless sensor networks, users are authenticated using the Kerberos protocol, and then sensor data is encrypted using elliptic curve encryption protocol. The proposed method enhances the security of wireless sensor network by combining Kerberos encryption and elliptic curve encryption techniques.

Introduction

Currently, the world is becoming smarter than ever with the use of IoT facilities that connect everything. The Internet of Things is an emerging field of research. IoT creates an ecosystem of interconnected devices connected to the internet. In this network, many network-based physical devices are authorized to create a wireless network for communication and data sharing among them. Nowadays, IoT networks have been widely studied in various applications such as agriculture for environmental monitoring, building and home automation for monitoring various electromechanical devices, healthcare for remote patient monitoring, transportation for smart traffic control, industry for monitoring machinery and environmental conditions, etc. Active IoT devices collect information and transmit it among other devices. However, IoT-enabled systems are exposed to various security and privacy attacks due to their open nature. In IoT-enabled systems, multimedia information moves from one end to the other, and computational complexity with limited environments like ad hoc networks, mobile networks, etc. is important. The rapid use of communication facilities in wireless multimedia sensor networks (WMSN) has increased the need for security assessments to protect various multimedia data during transmission. WMSN is an integral part of smart spaces and is used in various sensitive applications such as inactive infrared sensors, wireless surveillance sensor networks, audio and video sensors. There is much research on the use of IoT in multimedia transmission, which is related to service conditions and device configuration. The device's service status directly affects the performance of multimedia communications. After the request, the sensor node

Doi:

collects relevant multimedia information and then sends multimedia processing data to the user or gateway node. According to [5], in this research, it is considered that the sensor node directly transfers multimedia data to the gateway node. It is also assumed that IoT-enabled WSN in the proposed protocol is heterogeneous in nature, but maintaining the confidentiality of multimedia data is one of the main challenges, and preserving the privacy of multimedia data from unauthorized access by attackers is a big issue for active WSN with IOT. User authentication protocol by creating a session key is a comprehensive approach to solving the mentioned problems in IoT-enabled WSN. Additionally, the protocol can also provide secure communication in IoT-enabled cloud environments. Another challenge in IoT-enabled WSN is intrusion detection. In this paper, we propose a strong and efficient authentication protocol in IoT-enabled WSN to perform safe multimedia communications.

Kerberos is a network authentication protocol designed and implemented by MIT University to perform strong authentications in user-agent applications. An interesting point about Kerberos is that it is a three-headed dog that guards the gates of hell. Although the spelling is slightly different (Cerberus), the concept is the same. Kerberos has very high accuracy but has a lot of overhead. The main problem with conventional public key encryption systems is that to meet the security needs at a high level, the key size must be sufficiently large. This leads to reduced speed and increased bandwidth consumption. The solution is to use elliptic curve cryptography. Today, this encryption method is generally used in resource-constrained environments such as ad hoc wireless networks and mobile networks. There is a trend for traditional public key encryption systems to gradually replace with elliptic curve cryptography systems. As computational power increases, the key size of traditional systems needs to increase significantly.

In this paper, for the use of the advantages of the Kerberos encryption protocol and also to reduce the overhead for IoT-based wireless sensor networks, users are authenticated with the Kerberos protocol, and then sensor data is encrypted with elliptic curve cryptography protocol.

I. Related Works

Various efforts have been made to present security solutions in the Internet of Things. Lee et al. proposed an advanced security scheme based on mutual authentication and key agreement in IoT in 2013 [9]. Turkanoğlu and Holbl presented a new authentication protocol and key agreement scheme for heterogeneous sensor networks based on the Internet of Things in 2014 [10] and also pointed out that many security flaws in research protocols, such as theft attacks, accidental online attacks, insider attacks, user impersonation attacks, and smart card attacks, still exist. They also provided a better solution to maintain security in wireless sensor networks. In 2014, Turcanović et al. proposed user authentication and session key establishment protocols for heterogeneous WSNs using smart cards. They also applied the concept of IoT in WSNs. Their main research goal was to achieve lower energy consumption, low cost, computation, and mutual authentication. The Turcanovic et al. protocol authentication model restricts the role of a simple sensor node by allowing the user initially to communicate with a specific sensor node used to receive sensitive multimedia data [10]. Amin et al. also proposed an improved protocol for security vulnerability resistance in 2016[11]. Park et al. introduced a fingerprint-based solution. Fingerprint is a mature biometric technology and is widely used as an identity verification mechanism in our daily lives, such as mobile devices. In this work, a three-factor fingerprint-based user authentication ID is proposed for wireless sensor networks in IoT environments, where a fuzzy credentialing program is adopted to validate fingerprint information. The proposed method in this paper consists of four phases; sensor registration, user registration, login and authentication, and password change [12].

II. Proposed Method

In this section, the proposed method for enhancing the security of IoT-based wireless sensor network using elliptic curve cryptography (ECC) algorithm and Kerberos protocol is described in detail. The first step begins with deploying users, nodes, and base stations. Then, a request is made by the user to acquire the sensor node data. This request is transferred from the node to the base station. Upon user request, the authentication process begins using the Kerberos protocol. Kerberos, with its mechanism, has the capability to identify authorized users with high power. After user validation, the user can use the sensor node. To prevent eavesdropping and data theft on the sensor network by unknown individuals, the transmitted data in the wireless sensor network between nodes and the base station is encrypted using ECC. The process of exchanging information between the user, node, and base station continues until the end of user requests.

A. User Authentication with Kerberos

In this section, we examine the Kerberos encryption and authentication protocol for identifying the identity of users authorized to use the sensor node. Due to the large volume of information exchange, the Kerberos protocol is initially used in the process of user access to the base station and in other cases for encryption and recording information at the base station using ECC. The Kerberos algorithm is divided into five parts.

1. Kerberos identity authentication based on symmetric key encryption to authenticate entities.
2. Kerberos uses symmetric key encryption based on

RSA.

3. Kerberos Key Distribution Center (KDC) provides scalability.
4. Kerberos Ticket provides secure session key transfer.
5. The Kerberos Key Distribution Center distributes the session key to the user by sending it.
6. The Kerberos ticket restricts the use of cloud entity keys.

As stated, Kerberos uses symmetric key encryption based on RSA to authenticate entities. In symmetric key encryption, communicating entities use the same key for encryption and decryption. The basic mathematical relationship behind this process is as follows: In the first step, when a user requests access to a sensor node, the desired user is authenticated using RSA encryption algorithm. The keyword is a secret key shared between each specific security element and a central authentication authority (in the Kerberos protocol, KDC). Both entities and KDC must know the shared secret key before the actual Kerberos authentication process takes place. For security reasons, the Authentication Service (AS) never stores the plaintext keyword but keeps a version of its hash (the hash algorithm used in MD5). Cloud entity keys are generated as part of the domain registration process (for example, when the domain administrator registers a user and enters the password). Cloud entity keys are derived from the machine password when the machine administrator connects the machine to the domain and is automatically created. KDC is located at the base station in the proposed scheme.

B. Elliptic curve cryptography in the proposed method

Elliptic curve cryptography is one of the various types of public key cryptography.

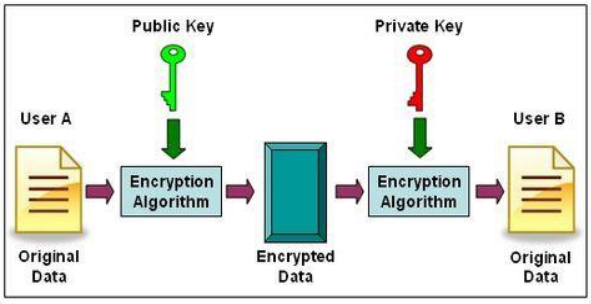

Fig. 1: Stages of Public and Private Key Encryption

Figure 1, shows two keys, a public key and a private key. These keys are used for encrypting and decrypting data. The characteristic of all public key encryption algorithms is that each of them has its unique trapdoor function. The trapdoor function is a function that is computable only in one way, or at least can be easily computed. After user authentication, access to the sensor node, including reading sensed information, using the processor and memory, etc., is confirmed. In this section, the method of inserting information in encrypted form on the sensor node using elliptic curve cryptography is explained. There is a trend for traditional public key encryption systems to gradually be replaced by elliptic curve cryptography systems. As computational power increases, the key size of traditional systems needs a significant increase [13]. Elliptic curves have been studied by mathematicians for hundreds of years. Elliptic curves have been used in various fields such as number theory, string theory, and elliptic curve cryptography. The elliptic curve E is defined over the real number R by a equation (1):

$$(x,y) \to (a_1^2 x + \frac{a_3}{a_1}, a_1^3 y + \frac{a_1^2 a_4 + a_3^2}{a_1^3})$$

$$\Rightarrow y^2 + xy = x^3 + ax^2 + b \qquad (1)$$

Elliptic curves are used to construct public key encryption systems. The private key d is randomly selected from the interval [1, n-1], where n is an integer. Then the public key Q is compared to dP, where P and Q are points on the elliptic curve. Like traditional cryptographic systems, once the key pair (d, Q) is created, various cryptographic systems such as signature, encryption/decryption, key management systems can be configured. The calculation of dP is shown as a numerical multiplication. This applies not only to calculating the public key but also to signing, encrypting, and key agreement in elliptic curve cryptography systems. With the shared key, information can be easily encrypted.

C. Steps of Method Execution

The steps of method execution are shown in the flowchart below. According to this figure, the first step begins with deploying users, nodes, and base stations. Then, a request is made by the user to acquire a sensor node. This request is transferred from the node to the base station. Upon user request, the authentication process begins using the Kerberos protocol. Kerberos, with its mechanism, has the capability to identify authorized users with high power. After user validation, the user can use the sensor node. To prevent eavesdropping and data theft on the sensor network by unknown individuals, the transmitted data in the wireless sensor network between nodes and the base station is encrypted using ECC. The process of exchanging information between the user, node, and base station continues until the end of user requests.

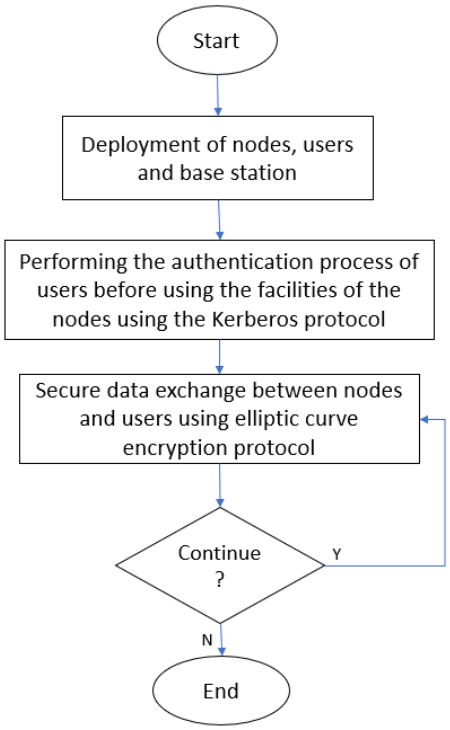

Fig. 2: Flow chart of proposed method

III. Evaluation of the Proposed Method

To evaluate the proposed method, it is necessary to use simulation software to implement the proposed scheme. For this purpose, MATLAB software is used. This software provides a suitable environment for performing mathematical operations, creating visual environments, and easy programming simultaneously.

A. Initial Settings

Before examining the simulation results, it is necessary to determine the number of sensor nodes and users, and then specify the positions of sensor nodes, users, and base stations. In addition to the mentioned items, the total number of user requests to access sensor nodes must also be determined from the beginning. To examine different scenarios and determine the efficiency of the proposed method under different conditions, the number and coordinates of sensor nodes and users, as well as the number of user requests to access sensor nodes, vary in multiple scenarios. The proposed method was evaluated on an Intel Core i7-4720HQ , 2.66GHz processor. The software used for evaluation is MATLAB R2015b.

Table 2: Simulation Settings Parameter Value

Parameter	Value
The dimensions network environment	50m & 50m
Coordinates of Base Station	Center of Environment
Number of Requests	200
Number of Users	15
Processor	CORE i7-4720HQ 2.66GHz
Number of Sensor Nodes	5
Software	MATLAB R2015b

B. Results

In this scenario, 15 users intend to use sensor nodes. The total number of requests is 200, each applied randomly by a user each time. An environment with dimensions of 50 meters by 50 meters is allocated for the random distribution of users and sensor nodes. Figure 3 illustrates the initial layout of wireless IoT sensor network components.

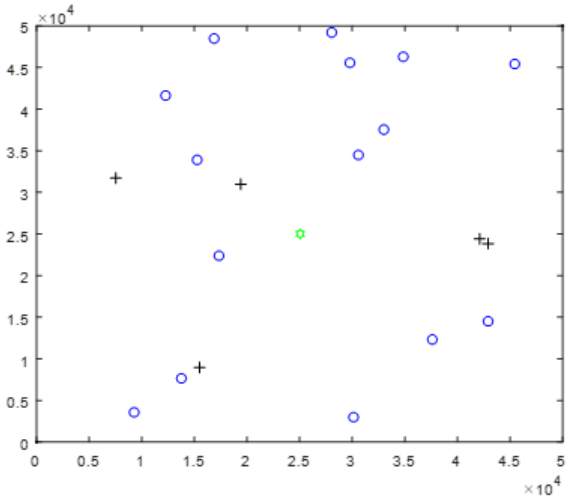

Fig. 3: Proposed Scenario Network Structure

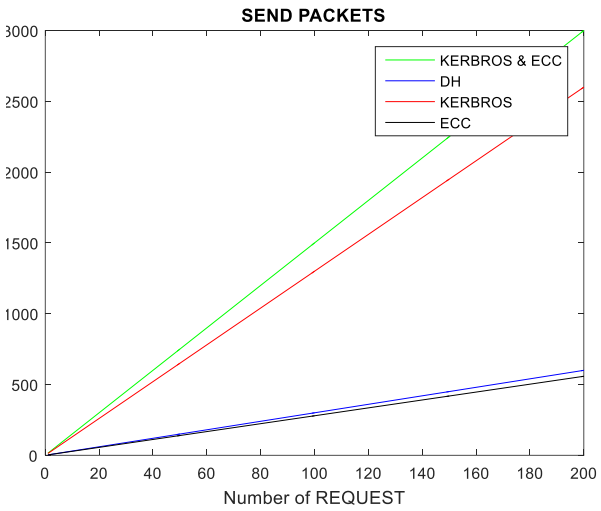

Fig. 4: compares the number of packets exchanged.

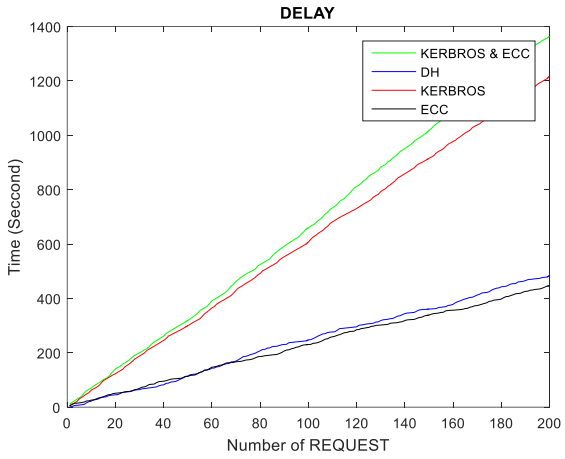

Fig. 5: Comparison of Request Execution Times

Figure 4 shows the number of packets exchanged to access sensor nodes by users. As evident in the figure, the Diffie-Hellman and Elliptic Curve methods require fewer packets due to their simple structures to access sensor nodes. However, the other two methods, due to the use of Kerberos and its complex security structure, require a considerable number of exchanged packets.

Figure 5 shows the delay created from the time the user creates a demand until the time the desired sensor nodes are accessed. As you can see in the figure, the delay created in the Kerberos and hybrid methods due to the use of a complex security structure is more than the Diffie-Hellman and elliptic curve methods. But there is not much difference between the combined method and Kerberos. So far, what is inferred is the superiority of the Diffie-Hellman method and the elliptic curve over the other two methods, but a very important criterion has not been investigated yet.

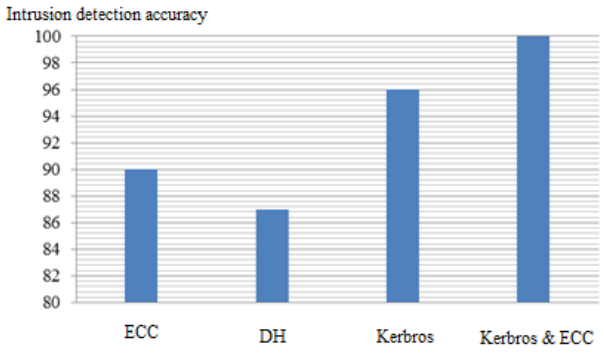

Fig. 6: Comparison of intrusion detection accuracy

Figure 6 shows the percentage of detected intrusions. Assuming the probability of a fake request to access the sensor nodes to the extent of 5% of all requests, this information is extracted from the simulation output. As you can see, the combined method has detected 100% of all the intrusions that occurred, while the Diffie-Hellman method and the elliptic curve have been able to detect only 85% and 90% of the intrusions, respectively. This number showed the ineffectiveness of Diffie-Hellman in the studied structure in the conditions where the information is critical. Although the Diffie-Hellman algorithm produces less delay and number of packets, it is not suitable for accessing the IoT-based wireless sensor network safely due to lack of accuracy in intrusion detection. The Kerberos method detects about 95% of all intrusions, and since there is not much difference in the delay and packets sent between it and the combined method, it can be said that the use of the combined method detects 100% of the intrusions. It is useful in accessing IoT sensor nodes.

Conclusion

In this paper, for the advantages of the kerberos encryption protocol and reducing the overhead for IoT-based wireless sensor networks, users are authenticated using the kerberos protocol, and then the sensor data is encrypted using the elliptic curve encryption protocol. Based on the simulation results, it can be said that the hybrid method identifies 100% of intrusions. Conversely, the Diffie-Hellman and elliptic curve methods, with lower accuracy, were able to detect intrusions to a lesser extent. This indicates the inefficiency of the Diffie-Hellman algorithm in the structure under investigation. Although the Diffie-Hellman algorithm generates fewer delays and packets, due to insufficient accuracy in intrusion detection, it is not suitable for secure access to IoT sensor nodes. The kerberos method identifies approximately 95% of intrusions, and since there is not much difference in delay and transmitted packets between it and the hybrid method, the use of the hybrid method, which identifies 100% of intrusions, is beneficial for accessing IoT sensor nodes.

References

[1] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78(2), 544-546.

[2] Wang, S. C., Tseng, S. C., Wang, S. S., & Yan, K. Q. (2017, April). Reaching Safety Vehicular Ad Hoc Network of IoT. In Asian Conference on Intelligent Information and Database Systems (pp. 289-298). Springer, Cham.

[3] Heydari, N., & Minaei-Bidgoli, B. (2017). Reduce Energy Consumption and Send Secure Data Wireless Multimedia Sensor Networks Using A Combination of Techniques For Multi-Layer Watermark And Deep Learning. International Journal of Computer Science and Network Security (IJCSNS), 17(2), 98.

[4] Jaladi, A. R., Khithani, K., Pawar, P., Malvi, K., & Sahoo, G. (2017). Environmental Monitoring Using Wireless Sensor Networks (WSN) based on IOT. International Research Journal of Engineering and Technology (IRJET) 4(1), 1371-1378.

[5] Mishra, D., Vijayakumar, P., Sureshkumar, V., Amin, R., Islam, S. H., & Gope, P. (2017). Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks. Multimedia Tools and Applications, 1-31.

[6] Roux, J., Alata, E., Auriol, G., Nicomette, V., & Kaâniche, M. (2017, September). Toward an Intrusion Detection Approach for IoT based on Radio Communications Profiling. In 13th European Dependable Computing Conference, 88-96.

[7] Kaur, M., Singh, T. P., & Singh, B. (2015). Modification in the Kerberos Assisted Authentication in Mobile Ad-hoc Networks to Prevent Black Hole Attack. International Journal of Computer Applications, 117(23), 49-58.

[8] Yadav, D., Malwe, D., Rao, K. S., Kumari, P., Yadav, P., & Deshmukh, P. (2017). Intensify the security of One Time Password using Elliptic Curve Cryptography with Fingerprint for E-commerce Application. International Journal of Engineering Science, 8(3), 54-80.

[9] Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 58(4), 431-440.

[10] Turkanović, M., Brumen, B., & Hölbl, M. (2014). A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. Ad Hoc Networks, 20, 96-112.

[11] Amin, R., & Biswas, G. P. (2016). A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. Ad Hoc Networks, 36, 58-80.

[12] Park, H. J. (2015). Enhanced User Authentication Scheme for Wireless Sensor Networks. International Journal of Security and Its Applications, 9(8), 367-374.

[13] Pan, W., Zheng, F., Zhao, Y., Zhu, W. T., & Jing, J. (2017). An Efficient Elliptic Curve Cryptography Signature Server With GPU Acceleration. IEEE Transactions on Information Forensics and Security, 12(1), 111-122.