Reliable Information Transmission Mechanism Research of the Internet of Things Sensing Layer based on the Digital Signature

Zenghui Zhao

Xi'an Peihua University, Shaanxi Xi'an,china

296883619@qq.com

Key words: Internet of Things; Security Level Agreements; Digital Signature; Sensing layer

Abstract. With the rapid development of information technology and network communication technology, Internet of Things technology to flourish, in the Internet of Things environment, not only contains the past network environment components, but also joined the intelligent object, it will form hundreds of millions of data , These huge amount of data will result in a huge computing cost. In this paper, we use the concept of security level protocol to reduce the cost of computing, and propose a lightweight security mechanism based on the concept of digital signature between the mediation layer and the perceptual layer. Through the intermediary layer, The identity of a verifiable and non-repudiation, thereby enhancing the security of things.

1 Introduction

The Internet of Things refers to the network of interconnections between objects and objects. The method of interconnection is to install sensors or RFID tags on the carrier so that the communication technology supports the transmission of sensed information between carriers, or even an automatic control device. The function of intelligent automatic control and response of objects can be further realized through the intelligent function interface or cloud computing technology, which can be used as an advanced remote monitoring, interpretation of massive information analysis and other application functions [1]. The network based on object communication is called the Internet of Things, but the object information must also be backed up by people in order to serve the purpose of the service. In the past, some scholars have conducted relevant research on the deep heterogeneity of the Internet of Things intermediaries and the unknown topology architecture [2].

In order to improve the identification between the sensing layer and the mediation layer, this study added a mechanism of digital signatures to provide authentication and non-repudiation of identity so that the services at the application layer are transparent. The intermediary layer can learn the identity of the perceptual layer entity object, and the perceptual layer entity object accurately transmits the data via the mediation layer to the service that issues the demand. In this study, a coverage rate extending from a regular hexagon is proposed centered on the Sink Node, which receives the data transmission from the sensing node and divides the security level agreement within the coverage of the regular hexagon to reduce the risk of data theft and the computational cost of data encryption technology [3].

2 Three-tier Internet of Things architecture model

The IoT topology architecture defined in this study is mainly responsible for gathering the requirements of cloud service providers from the nodes of each region. Each region has different sensing nodes for services. Each network service will correspond to one or more sensing layers. The topology of the device. The definition of the mediation layer in this study is to be responsible for data authentication and processing of the cloud port, and to manage the storage of keys and signatures for each sensing node through the mediation layer[4].

The three-tiered IoT architecture proposed by this study consists of an application layer, a middleware layer, and a perception layer. The application layer is a diversified network service, which includes currently existing network services and network services extended from smart objects of the Internet of Things. Between the two tiers, information transmission and data authentication and processing are performed through the intermediary layer, and data is authenticated by the equipment and service monitoring agent and certification center. The certification history and signatures will be recorded in the information log. When successful data is authenticated by Event Identification, Communication Management, Policy Management, and Remote Management, the data is processed by the Intermediary [5].

3 Internet of Things Awareness Layer Security Level Agreement

This study uses the concept of a regular hexagonal coverage area to plan mechanisms that are appropriate to the perception level security level agreement. Hexagon coverage is often used in wireless network environments such as fourth-generation mobile communications, LTE and WiMax. The hexagon is a concept that extends from a circle, so the distance between each diagonal of the hexagon and the center is equal.

This study establishes a security level agreement that is suitable for the perception layer of the Internet of Things in the coverage of regular hexagons. In order to reduce the load of the center point Sink Node and the encryption calculation time is too long, a three-phase security level protocol is divided. In the initial definition, the size of six isosceles triangles connected from the center point to the outermost 1/3 of the connected length is the coverage of Level 1, and Level 2 is the length of 2/3. The size of the six triangles, Level 3 is the size of the entire regular hexagon, as shown in Figure 1.

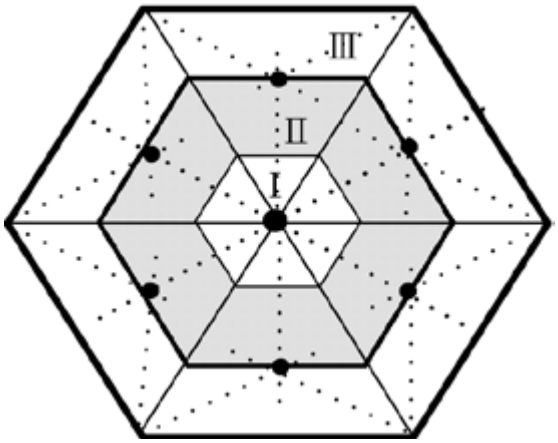

Figure 1 Three-phase security level agreement

The Level 1 security level protocol is the closest to the center point, and the number of sensing nodes

covered under normal conditions is the smallest, and the Sink Node bit is within the range of Level 1, so the sensing node within the Level 1 range is closest to the Sink Node. The encryption and decryption technology needed does not need to be too complicated. Therefore, this study uses the hash function h(.) for sensing nodes in the Level 1 range to encrypt the data that needs to be transmitted.

Level 2 covers more sensing nodes than Level 1, and is farther away from Sink Node than Leve1. Therefore, establishing a Level 2 security level protocol requires Sink Node to generate between Level 1 and Level 2. The key of the sensing node. When each sensing node in Level 2 transfers data to the Sink Node, it must use the key generated by the Sink Node in addition to the data to perform h(QM). Therefore, the final transmitted encryption result is.

Level 3 covers the widest range, that is, the number of sensing nodes between Level 3 and Level 2 is the most. Because of the large amount of data, it will consume a considerable amount of computational cost when performing encryption, so it is not appropriate to use complex data for data encryption. Encryption technology. However, if you use an encryption technology that is too simple, the data may be stolen or tampered with when it is passed to the Sink Node.

Therefore, this study calculates the center of gravity of each isosceles triangle from the total coverage of the Sink Node as a multi-Mobile Agent Node (multi-MAN). The multi-MAN is responsible for receiving data from each sensing node in the range of Level 3 covered by the isosceles triangle. Each multi-MAN will have the key generated by the Sink Node and then pass the encrypted data to the Sink Node. Finally, the Sink Node will integrate the received data and send it to the mediation layer for data authentication and processing.

4 Workflow of lightweight security mechanisms

In this study, between the sensory layer and the mediation layer, the digital signature is used to obtain the identity information of the sensing nodes in the perceptual layer to ensure the reliability of the data. Therefore, third-party arbitration methods within digital signatures are used to perform data transmission between the source and target sides through third-party authentication for the intermediary.

4.1 Generation of KSNi, MW, KSNi and KAC

In the framework of this study, the perception layer must perform identity verification via the mediation layer. A conference key KSNi, MW, KSNi, and MW are dynamically generated between the form and the MW, and the XMM is converted between the KMM and the KMM. This session key mainly establishes a communication channel between the SN and the MW. The OM transmitted by the SN will encrypt the information through the conference key. Because the KSNi of the SN may have the risk of being cracked, adding the conference key during the transmission mainly improves the security during the transmission of the SN and MW.

First, the DSM 4 starts calculating the secret key rDMA(SNi) and the private key rDMA(AC) of each area SNi, and loads the sensing node SNi and the authentication node AC, respectively, to form KSNi and KAC.

4.2 Certification stage

$$SN_i \to DSMA : OM \| E\left(K_{SNi},,[\ ]\right)$$

$$DSMA \to AC : E\left(K_{AC},\left[SN_i \| OM \| E\left(K_{SNi,MW}\right),\left[SN_i \| h\left(OM\right)\right] \| TS\right]\right)$$

Sink Node SNThe data collected by i will be converted into a fixed-length information digest h(OM) via the hash function algorithm h(.), encrypted with the private

key KSNi of SNi and KSNi, MW that SNi and SNi co-owned by the intermediaries MW. The signatures are formed and transmitted to the device and service monitoring agent DSMA and authentication node AC in the mediation layer for authentication and program processing. SNi has KSNi derived from DSMA, so DSMA first performs the first stage of KSNi and KSNi, MW certification, confirming the identity of SNi. After the DSMA sends the verified information to the AC, the AC obtains the plaintext of the SN. via the KAC generated from the DSMA, and the signature E (KSNi, (KSNi, MW), [SN||h(OM)]) and The timestamp is stored in the information log, and the plaintext data is processed by the intermediaries' programs.

There are two scenarios for the certification process proposed in this study. Figure 2 shows the data authentication process proposed by the Institute:

(1) The service provider or DSMA sends probe information to collect data.

a. When the service provider needs to sense the data of the layer device, it will send notification information to SNi via the DSMA. In the notification information, DSMA is written into the service provider's requirement SRy. KSNi is the private key generated by DSMA to SNi. It replaces the original KSNi and the private key KMW of the intermediaries, and mainly performs XOR with the original KSNi of SNi. Generate a conference key.

b. The DSMA will periodically request that each zone SNi transmit data. Therefore, the DSMA sends a request for probe information. The private key KMW of the mediation layer is written in the message, and the original KSNi of SNi is XORed to generate the conference key.

(2) After SNi has collected the original data, it forms a fixed-length message digest with h(.), and returns the conference key KSNi, MW after SN authentication and KSNi and XOR to DSMA.

(3) The DSNA uses the private key KAC of the AC to encrypt the data encrypted by the SNi again, and transmits the DSN-certified KSNi, KSNi, MW, and timestamp TS to the AC.

(4) AC compares KAC, KSNi, and KSNi. Whether the MW is correct. If it is correct, then the signature from SNi via DSNA to AC is stored in the information log.

(5) The information of the AC private key update is returned, and the private key of the SNi and the AC is updated synchronously.

Continuing the need for SN to send data actively, in addition to periodically collecting data from the sensing layer in the Internet of Things environment, sensing devices in the sensing layer have intelligent functions. When unreasonable data occurs, they must be transmitted immediately. Intermediary data analysis and processing.

(6) The urgency data collected by SNi must be immediately certified by the DSMA and transmitted to the service provider.

(7) SNi actively sends encrypted data transmission requirements SNi, areq to DSMA.

(8) After the DSMA determines the identity of SNi, it returns the new KSNi and the private key KMW of the intermediaries.

(9) After SNi has collected the original data, it forms a fixed-length message digest with h(.), and returns the conference key KSNi, MW after SNi authentication and KSNi and XOR to DSMA.

(10) DSNA encrypts the encrypted data of SNi again with AC private key KAC, and transmits the DSNA-certified KSNi and KSNi, MW and timestamp TS to AC.

(11) The AC matches KAC, KSNi, and KSNi. Whether the MW is correct. If it is correct, the signature from SNi to the AC through the DSNA is stored in the information log.

(12) The AC private key update information is returned, and the private keys of SNi and AC are updated synchronously.

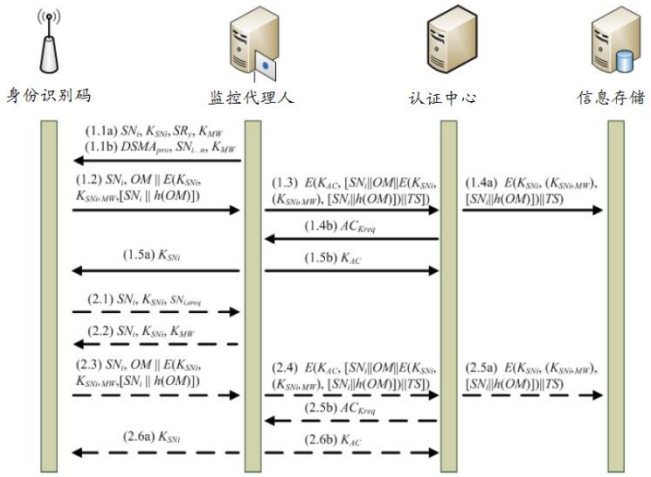

Figure 2 Data Authentication Process

5 Conclusion

Because there are tens of thousands of smart objects in the Internet of Things environment, there may be a huge amount of data. In order to enable service providers and demanders to ensure secure data transmission in the Internet of Things environment, encryption technology is used to preserve data integrity, but when each data must be encrypted securely, It will cause the computing cost of the perception layer of the Internet of Things to increase, and cause the Sink Node itself to load too much. Therefore, this study proposes a security-level protocol based on a regular hexagon in the perception layer of the Internet of Things. Through the three-phase security level protocol, the amount of data in the Internet of Things environment is shared, and the encryption technology is simplified by using different attributes of each stage. To reduce the computational cost of the sensing layer and still have relative security protection.

References

[1] Ian H. Witten, Radford M. Neal. Arithmetic coding for data compression[J]. Communications of the ACM, 2015,48(6):32-37.

[2] Chun-Ta Li, Min-Shiang Hwang. A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks[J]. Computer Communications, 2013, 86(12):29-33.

[3] Gongjun Yan, Stephan Olariu,Michele C. Weigle. Providing VANET security through active position detection[J]. Computer Communications, 2015, 28(12):48-35.

[4] Peng Ning, Wenliang Du, Maxim. Securing vehicular ad hoc networks[J]. Journal of Computer Security, 2012, 75 (1):19-23.

[5] Ahmed Helmy, Saurabh Garg. CARD: A Contact-based Architecture for Resource Discovery in Wireless Ad Hoc Networks[J]. Mobile Networks and Applications, 2015, 47(1):29-36.