IoT-Oriented Designated Verifier Signature Scheme

Min Li(✉)

School of Computer Engineering, Jingchu University of Technology, Jingmen 448000, Hubei, China
49035084@qq.com

Abstract. In order to reduce the computational cost of digital signature scheme in internet of things and improve the security of signature, based on analyzing the security requirement of Internet of things and SM2 Algorithm, a secure digital signature scheme in internet of things is proposed. The elliptic curve is used to construct the scheme, which improves the computing efficiency and meets the lightweight requirement in IoT environment. Specifies the verifier feature that meets the security requirements of a particular environment. The analysis shows that the scheme has the characteristics of message integrity, anti-repudiation, designated verification and anti-forgery.

Keywords: Internet of things · SM2 · Digital signature · Privacy protection

1 Introduction

IoT is a collection of interconnected objects, services, people, and devices that enable information exchange and data sharing in different domains. The Internet of things is used in many fields, such as transportation, agriculture, medicine, electricity, logistics, etc. The goal of building the Internet of things is to change the way people live their lives by enabling the smart devices around us to do the daily chores, such as smart homes, smart city, smart transportation. The Internet of things has many applications, from the personal environment to the Enterprise Environment [1]. In personal and social IoT applications, IoT users can interact with their environment and other users to build and maintain social relationships. In the transportation applications of the Internet of things, various smart cars, smart roads and smart traffic lights can improve traffic efficiency and safety. In the business and industry applications of the Internet of things, such as finance, banking, marketing, and so on, interactivity within and between organizations can be achieved. In recent years, due to the radio frequency identification (RFID) and wireless sensor network (WSN) technology progress, the rapid development of the Internet of things. Each device can be tagged with RFID, thus having a unique identity and being uniquely identified. With WSN, every "thing", that is, people, devices, etc., can be recognized wirelessly and communicate in the physical, network, and digital world. Although the Internet of things has brought convenience to people's life, similar to the

W. Li and D. Tang (Eds.): MOBILWARE 2020, LNICST 331, pp. 204–210, 2020.
https://doi.org/10.1007/978-3-030-62205-3_20

traditional Internet system, all kinds of security attacks come along, which seriously affect the development of the Internet of things and People's privacy security.

This paper first analyzes the security requirements of the Internet of things, then introduces the construction of SM2 digital signature scheme, then gives the concrete construction of the security digital signature scheme, and finally analyzes the security of the proposed scheme.

2 Premilaries

2.1 Security Requirements of IoT

The basic security goals of the Internet of things include confidentiality, integrity, and integrity in general network systems. However, due to the Heterogeneity of devices and the limitation of computing and communication resources, IoT has different security problems. The security challenges facing the Internet of things can be broadly divided into two categories: structural challenges and security challenges [2]. Structural challenges stem from the heterogeneity and ubiquity of the Internet of things itself, and security challenges are related to the principles and functions of the system, its basic goal is to construct the security network by the enforcement mechanism. Resolving structural challenges usually requires consideration of wireless communications, scalability, power and distribution, while resolving security challenges requires consideration of authentication, confidentiality, end-to-end security, integrity, etc., security mechanisms must be enforced throughout the life cycle of system development and operations [3]. Common security requirements include that all software running on IoT devices must be licensed, and that the network must authenticate IoT devices before they can be turned on to collect and send data; Due to the limited computing and storage resources of IoT devices, it is necessary to use a firewall network to filter packets directed to the device; updates and patches to IoT devices should be installed in a manner that does not increase the additional bandwidth consumption.

Overall, the security needs of the Internet of things include the following:

(1) confidentiality ensures that data is secure and available only to authorized users. In the Internet of things, users can be people, machines, services, internal objects (devices in the network) and external objects (devices outside the network). For example, you must ensure that the sensor does not disclose the data it collects to a nearby node [4]. Another confidentiality consideration is how to manage data, and it is important for IoT users to be aware that data management mechanisms are applied to process or people management to ensure that data is protected throughout the process [5].

(2) Integrity. Since the Internet of things is based on the exchange of data between many different devices, it is important to ensure that the data is accurate; that it comes from the right sender and that it is not tampered with or intentionally or unintentionally interfered with during transmission. Although data traffic can be managed by using firewalls and protocols, due to the limited computing and communication resources of IoT nodes, the security of endpoints cannot be guaranteed, so other mechanisms must be considered to achieve the integrity.

(3) Usability. The IoT vision is to connect as many smart devices as possible to make all the data available to IoT users at any time. However, data is not the only part of the Internet of things, and devices and related services must be and can be accessed whenever they are needed. Approaches that support usability may require both generic approaches such as fault tolerance and cryptology-based mechanisms.
(4) Authentication. Every object in IoT should be able to be recognized and identified by other objects, but the nature of IoT makes it challenging to identify and identify, which involves multiple types of entities such as devices, people, service providers, and so on. The design of the authentication mechanism needs to be compatible with all types of entities in heterogeneous systems. There is also a need to consider special scenarios where objects may need to interact with other entities that have not previously shared information [6].
(5) Lightweight. In addition to the usual security goals, considering that IoT nodes are usually resource constrained devices, lightweight is also a factor to consider when designing security mechanisms. Therefore, in the design and implementation of the corresponding encryption, authentication, integrity verification protocols or algorithms, it is not advisable to directly apply the traditional security schemes to the Internet of things.

2.2 SM2 Algorithm

SM2 [7] consists of three stages, including generation of keys, generation of signature,verification of signature:

Generation of keys:

(1) randomly selects d, $d \in [1, q-1]$;
(2) computes $P = dG$, set P as the public key, and d as the private key.

Generation of signature:

(3) the signer selects a random number $k \in [1, q-1]$, computes $kG = (x1, y1)$;
(4) computes $r = Hash(m) + x1 \bmod q$, where m is the message to be signed, Hash is a one-way function; if r = 0 or r + k = q, select another k.
(5) computes $s = (1+d)^{-1}(k - rd) \bmod q$; if s = 0, select another k; otherwise, take r, s as the signature.

Verification of signature:

(6) when the verifier receives m, r, s, checks $r, s \in [1, q-1]$, $r+s \neq q$; then computes

$$(x_1^1, y_1^1) = sG + (r+s)P$$

(7) computes $r^1 = Hash(m) + x_1^1 \bmod q$; checks r and r^1 is equal or not, if yes, accepts the signature; otherwise, reject the signature.

2.3 SM2 Based Signature for IoT

Suppose a node A in the Internet of things needs to sign message M and send it to another node B to verify. At the same time, the content of message M is sensitive information, so m cannot be disclosed to third parties. The transmission network is a non-secure network, so there may be various types of attackers in the transmission process. The system model of the scheme is shown in Fig. 1.

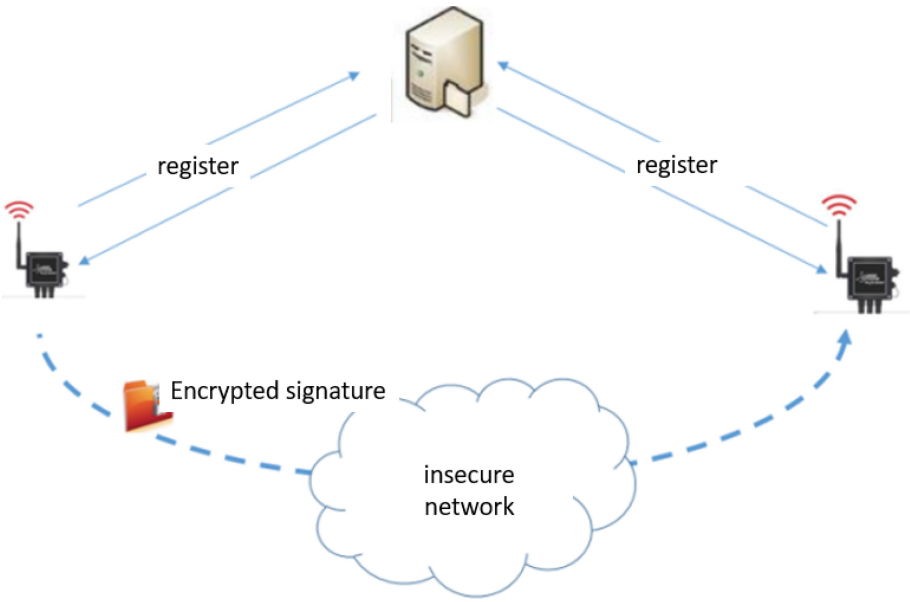

Fig. 1. The architecture of the scheme

In order to realize the signature that can protect the message content, this paper designs a digital signature scheme based on SM2. In the scheme, in addition to the IoT nodes, there is a trusted third party called as a key generation center KGC, which is responsible for registering and maintaining the public keys of each node, all nodes in the IoT join the system by first submitting the public key and other necessary information to the KGC for registration. The algorithm is constructed based on SM2 digital signature algorithm, so it is similar to SM2 digital signature algorithm, including system initialization, key generation, signature generation and signature verification, as follows:

(1) System initialization

Selects a big primer number p which is larger than 160 bits, then select a secure elliptic curve

$y = x^3 + ax + b(4a^3 + 27b^2 \neq 0 modp)$, chooses the basis G with the degree n. chooses a secure hash function H.

(2) Key generation

A randomly chooses $dA \in [1, q-1]$ as the private key then computes the public key $P_A = d_A G$; B randomly chooses $dB \in [1, q-1]$ as the private key then computes the public key $P_B = d_B G$. A afterwards and B register themselves in KGC.

(3) Signature generation

If the message to be signed is M, the sender A will sign it and send it to the designated verifier B. A randomly select $k \in [1, q-1]$,then compute

$$\begin{aligned} V &= kP_B = (x_1, y_1) \\ r &= H(m\|V) + x_1 \ mod \ q \\ s &= (1+d_A)^{-1}(k - rd_A) \ mod \ q \end{aligned}$$

and then the signature of the message m is $\sigma = \{r, s\}$, A sends $\{m, \sigma\}$ to B.

(4) Signature verification

As B receives $\{m, \sigma\}$, computes

$$V' = sd_B G + (r+s)d_B P_A = (x_1', y_1').$$

$$r' = H(m\|V') + x_1'$$

Checks r and r′ are equal or not. If yes, accepts the signature; otherwise, reject it.

3 Analysis

3.1 Correctness

Theorem 1. If the signature is not damaged during transmission, the verifier can accept the signature according the equation in the stage Signature verification.

Proof: Actually, the verifier can computes V′ as follows,

$$\begin{aligned} V' &= sd_B G + (r+s)d_B P_A \\ &= sP_B + sd_A P_B + rd_A P_B \\ &= (1+d_A)sP_B + rd_A P_B \\ &= (1+d_A)(1+d_A)^{-1}(k - rd_A)P_B + rd_A P_B \\ &= (k - rd_A)P_B + rd_A P_B \\ &= KP_B \end{aligned}$$

That is to say $V = V'$, then there exists $x_1' = x_1$, thus r and r ‘are equal, and the signature is valid.

3.2 Security

(1) Integrity

Because of the use of a secure hash function H in this scheme, if the message M is corrupted during encryption or during signature transfer, then verifier B does not compute the same as R, according to the Hash function, the resulting hash value must be different and the signature verification cannot pass. Therefore, the integrity of the scheme is guaranteed.

(2) Designated verifiability

According to the signature verification equation, no one other than designated verifier B can verify the validity of the signature because they do not have the private key of B. If the attacker attempts to push his private key through B's public key to complete the verification, he will face the problem of discrete logarithm. Therefore, the designated verifiability of this scheme is established.

(3) Non-repudiation

If A tries to deny its signature on M, because the scheme is constructed based on SM2 signature scheme, the scheme can satisfy the existence-unforgeable property, it is impossible for anyone but a to forge another message that is different from M and that is signed as. Therefore, A cannot disavow the signature it generated for M. Based on this, the scheme realizes the non-repudiation.

(4) Lightweight

The proposed signature scheme is constructed based on SM2 digital signature scheme, and SM2 digital signature scheme is implemented based on secure elliptic curve. As we all know, elliptic curve cryptography (ECC) has high computing efficiency. Using 160-bit key in ECC Algorithm, the security strength of 1024-bit key in RSA can be obtained. Therefore, the scheme is lightweight and suitable for the Internet of things environment.

4 Conclusion

Based on the analysis of the security requirements of Internet of things (IoT), this paper proposes a secure digital signature scheme based on SM2 algorithm considering the limited computing and communication resources and dynamic changes of nodes in IoT environment. The scheme uses a symmetric encryption algorithm with high efficiency and security to guarantee the confidentiality of the signature content. The signature based on SM2 ensures the scheme's high efficiency, this scheme is suitable for the security requirement of digital signature of sensitive content in internet of things.

Acknowledgment. This work was supported by the Research Fund Project of Jingchu university of technology (No. YB201808), the Special Funds of Jingchu University of Technology (No. QD201801), and the Outstanding Youth Science and Technology Innovation Team Project of Colleges and Universities in Hubei Province (No. T201923).

References

1. Samie, F., Bauer, L., Henkel, J.: IoT technologies for embedded computing: a survey. In: Proceedings of the Eleventh IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis, p. 8. ACM (2016)
2. Mahalle, P.N., Anggorojati, B., Prasad, N.R., Prasad, R.: Identity authentication and capability based access control (iacac) for the internet of things. J. Cyber Secur. Mob. **1**, 309–348 (2013)
3. Leo, M., Battisti, F., Carli, M., Neri, A.: A federated architecture approach for Internet of Things security. In: Euro Med Telco Conference (EMTC), pp. 1–5 (2014)
4. Farooq, M., Waseem, M., Khairi, A., Mazhar, S.: A critical analysis on the security concerns of internet of things (IoT). **111**(7), 1–6 (2015)
5. Khan, M.A., Salah, K., Salah, K.: IoT security: review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. **82**, 395–411 (2018)
6. Roman, R., Zhou, J., Lopez, J.: On the features and challenges of security and privacy in distributed internet of things. Comput. Netw. **57**, 2266–2279 (2013)
7. Ming, S., Ma, Y., Lin, J., et al.: SM2 elliptic curve threshold cryptographic algorithms. Chin. J. Cryptogr. **1**(2), 155–166 (2014)