Sensors & Transducers, Vol. 160, Issue 12, December 2013, pp. 570-577

www.sensorsportal.com

Sensors & Transducers

© 2013 by IFSA

http://www.sensorsportal.com

A Design of Solving the Security Problem of Internet of Things Based on Ellipse Curve Algorithm

Wu Mingxin

Higher Education Research Institute Beijing University of Aeronautics and Astronautics, Beijing 100191, China

Received: 9 November 2013 /Accepted: 22 November 2013 /Published: 30 December 2013

Abstract: In response to the increasingly serious security issues of internet, especially the safety threats existed in ONS query which is the EPCglobal network issues. In order to meet the stability and efficiency of things of internet we proposed a method of resolving EPCglobal network security issues based on elliptic curve encryption algorithm. It including the elliptic curve encryption algorithm application into ONS query, and DNSSec applied into it. The entire protocol has fully take advantage of the security and efficiency of elliptic curve algorithm. Finally, we showed the experiment data proposed that the protocol is feasible. *Copyright © 2013 IFSA.*

Keywords: Things of internet, Security, Ellipse curve algorithm.

1. Introduction

Compared with the Internet, the main achievements of internet of things including the communication between things, person and things, and the communication object expanded to items. According to different functions, Internet of things architecture can be divided into three levels, the bottom is used to collect information on the perception layer, middle layer is the data transmission network layer, and the top layer is the application/middleware layer. As the security of internet of things overall demand is the combination of physical security, security information collection, information transmission security, and integrated information processing security, safety is the ultimate goal is to ensure the confidentiality, integrity, authenticity and freshness of data. Therefore, in this paper we analyze the key techniques of each layer based on the corresponding security model combined with DCM (device, connect, manage) of internet of things. In Fig. 1 shows the security hierarchy of internet of things.

Physical security layer: to ensure that information node of internet of things do not been acquisition, control and destruction. Information collection security layers: the information collected to prevent eavesdropping, tampering, forgery and replay attacks, mainly related to sensor technology and RFID security. In the hierarchical model of internet of things, the physical layer of security and information security layer corresponds to the perceived layer security. Information transmission security layer: data transfer process to ensure information confidentiality, integrity, authenticity and freshness, mainly the telecommunication network security, which corresponds to the network layer security. Information processing security layer: to ensure the privacy and storage security of information, mainly individual privacy protection and middleware security, corresponding IOT application layer security [1, 2].

Article number P_1658

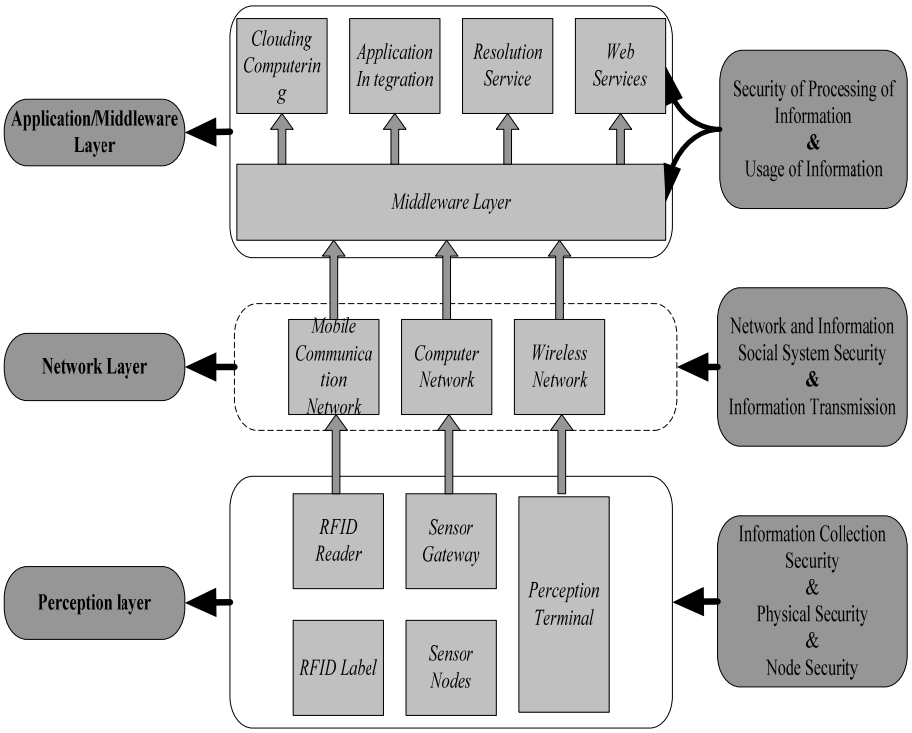

Fig. 1. Structure of Security Hierarchy of Things of Internet.

2. Security Current Situation of Internet of Things

2.1. Information Collection Security of Internet of Things

Information gathering is the function of IOT perception layer. Things should be achieved by IOT perception layer including information collection, capture and object recognition. Perception layer extending key technologies include sensors, RFID, self-organizing network, short-range wireless communications, low-power routing. Perception / extension layer mainly for security issues related to data and information on the confidentiality, integrity, availability requirements, mainly related to RFID, sensor technology security issue [2-4].

2.1.1. RFID/EPC Security Issues

RFID (radio frequency identification) is commonly known as electronic labels. Electronic Product Code (EPC) is used to uniquely identify an item code. EPC RFID-based system is the information and networking applications in the traditional products of the logistics industry and the specific implementation, EPC system components shown in Fig. 2. In networking systems reader received from the electronic tag of the carrier information and the received signal is demodulated and decoded, its information will be sent to the computer system in the savant middleware software for processing, and sends them to the communication network, and then the communication network through the name of the object name solver (ONS) to find the items of information stored in the location specified by the ONS to savant system stores the information about the article servers, and get the information about this item in the document.

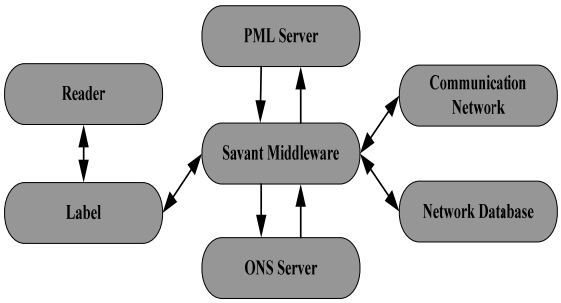

Fig. 2. RFID/EPC System Architecture.

Tag access defects. User (legitimate and unauthorized users) can take advantage of a legitimate reader or a self-configuring reader to communicate directly with the tag read, tag tampering even delete the stored data. Meanwhile, support for EPCglobal standards allow only written once, but will support other standards such as ISO RFID tags was able to repeatedly write (or re-programmed). Function in multiple writes to RFID applications bring convenience, but also bring greater security risks. In the absence of adequate protection of trusted security policy, the tag data security,

availability, integrity, availability, authenticity is not guaranteed.

Mobile RFID security: Mobile RFID systems is smart mobile devices which use implantable RFID reader chip, and get the information on the label, and through the mobile network access back-end database, access to relevant information, the common application is mobile payment. In the mobile RFID network security problems existed mainly are counterfeiting and unauthorized services. Firstly, in mobile RFID network, there is no fixed physical connection between the reader and the background data. When transmit their identity information through RF channel, an attacker intercepts a status message, you can use this identity information to impersonate the legitimate reading writer's identity. Secondly, by copying others reader information, you can replace several consumer. In addition, as the cost of replication attacks realization is not high, and without any other conditions, it has become the most commonly used means of an attacker. Finally, the mobile RFID network also exist non-authorized service, denial and denial of service attacks [3, 5].

2.1.2. Sensing Technology and Networking Security

In IOT, the use of RFID tags are static properties of the object's identity, while sensing technology is used to identify the dynamic properties of an object, which constitutes a prerequisite for the object perception. From the network hierarchy structure, the existing network technology sensor network security problem as shown in Table 1.

Table 1. Security Issues of Sensor Network.

Level	Received Attack
Physical Layer	Physical Destruction, Channel Blocking
Link Layer	Make Collision Attack, Link Layer Blocking
Network Layer	Routing Attacks, Wormhole Attacks, Witch Attacks
Application Layer	Desynchronized, Denial of Service Flow

2.1.3. IOT Terminal Security

Front-end is responsible for the perception of things to collect real-time data, the data is uploaded to the network data processing centers, data processing centers to process data or making available the information generated to the user or interlocks. The perception is that these information terminal or decisions rendering device. Common terminals include PC, PDA, mobile phone and so on. The main problems of existing terminal includes a terminal sensitive information leakage, tampering, SIM/UIM card information disclosure, copying, air interface information leakage, tampering, terminal viruses and other issues. The common security measures are authentication, data access control, channel encryption, one-way data filtering and strong auditing [6].

2.2. Information Transmission Security of Internet of Things

Information transmission security of IOT mainly involved network layer security and network layer's main function are the transmission of information and communication. Network layer can rely on the public telecommunications network and the internet. You can also rely on industry communications network, while also relying on public and private networks, such as relying on public network access layer. Wherein the network currently involved in a wireless communication network, including WLAN, WPAN, the next generation mobile communication networks and networks. Currently the network layer most significant problem is to solve existing address space shortage, the best way is to use the current IPv6 technology, which uses 128-bit address length and the adoption of the IPSec protocol, the IP layer packet on the safety of high-intensity processing, providing data source address validation, connectionless data integrity, data confidentiality, anti-replay and limited traffic encryption and other security services, and enhance network security.

2.3. Information Process Security of Internet of Things

Information processing security is mainly reflected in IOT application/middleware layer, wherein the middleware layer and network layer mainly IOT interface between application services and capabilities calls, including an analysis of the enterprise integration, sharing, intelligent processing, management, etc., embodied as a series of obligations supported platforms, management platform, information processing platform, intelligent computing platforms, middleware platforms. Application layer mainly contains a variety of applications, such as monitoring services, smart grid, industrial control, green agriculture, smart home, environmental monitoring and so on.

3. EPCglobal Internet Framework

3.1. Standard EPCglobal System

EPCglobal Network includes three main components of the system levels, as shown in Fig. 3, including: EPC coding system, radio frequency identification systems, information network system. Information network system includes EPC

middleware, application layer events (ALE, Application Level Event), EPC Information Services, and the ONS. EPC middleware so that users can customize according to some application requirements and integrate the different functions of EPC middleware components; ALE layer for processing applications related events; EPCIS processed information stored EPC middleware, and query-related information; ONS, similar to the domain Name Server (DNS), where information can be used to point to a storage device EPC middleware information EPCIS these are EPC system software support system [4-7].

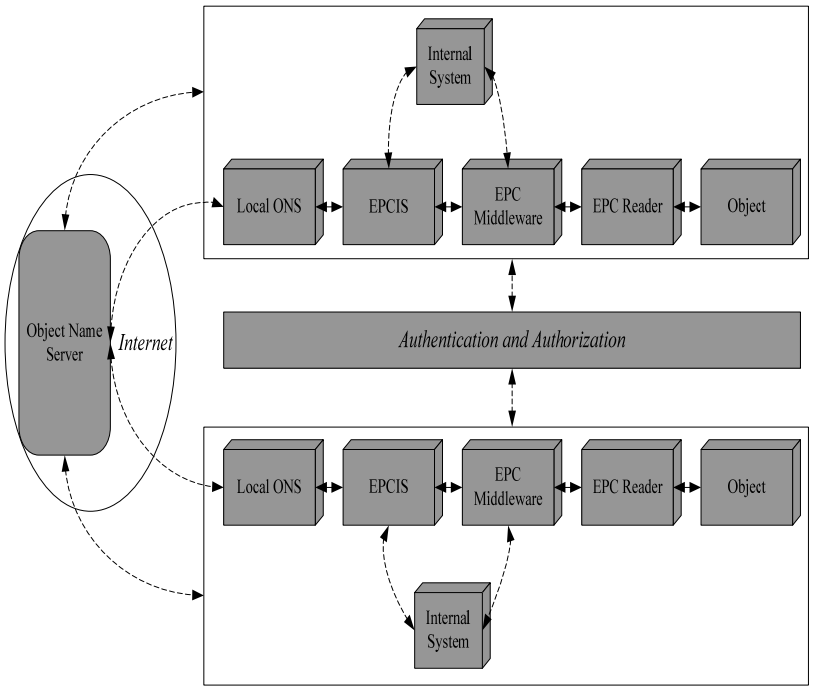

Fig. 3. EPCglobal Network Architecture.

3.2. EPC Coding System

EPC code is an important part of the system of EPC, which is the entity and entities related information coding, through a unified, standardized coding to create a universal information exchange language. It also is a new generation of Global Identification of the coding system, and is the expansion of the existing coding system. EPC objective is to provide a unique identity to everything, so as to through the computer network to identify and access a single target object, as in the Internet using the IP address to identify and communicate [5, 7].

3.2.1. EPC Coding Rules

EPC is only tag information stored in the RF and has been supported by UCC and EAN who are two major international standards supervisory. The basic rules including: 1) Uniqueness, the difference of the current widely used EAN/UCC code is which provides a unique identification of the physical object. In other words, an EPC code is just assigned to an item. The same size with the same kind of product corresponds to a product code, the same kinds of products with different specifications corresponding to different product code. Depending on the product properties, such as weight, packaging, size, color, shape to give different product codes. To ensure that uniquely identifies the entity object implementation, EPCglobal take the following basic steps: sufficient coding capacity, EPC must have large enough address space to identify all of these objects; forever, product code once assigned, which will no longer be changed; simple, EPC encoding is simple while providing uniquely identifies of the entity object; scalability, EPC address space is scalable, with sufficient redundancy to ensure that the EPC system upgrades and sustainability; confidentiality and security, with security and encryption technology combined, EPC encoding a high degree of confidentiality and security.

3.2.2. EPC Coding Structure

EPC code is generated by a version number plus another three pieces of data (the order of the domain name, object class, serial number) consisting of a set

of numbers, as shown in Table 3. The version number is used to identify the version of EPC code sequence, which makes the subsequent code segment can have different lengths; domain management is described in the manufacturer of the EPC-related information.

Table 2. The status of EPCglobal System.

Activity Type	Standards	State
EPC Physical Object Exchange	UHF Class0 Gen1	Replaced by Class1 Gen2
	UHF Class1 Gen1	Replaced by Class1 Gen2
	Class1 Gen1	Not Approved
	Class1 Gen2	Approved
	Class 1 Gen2 RFID Spec	Not Approved
	EPC Label Standard	Approved
	900 MHz Class0	Not Approved
	13.56 MHz ISM	Not Approved
	860-930 MHz Class1	Not Approved
EPC Basic Infrastructure	EPCglobal	Not Approved
	Application Activities Protocol	Approved
	Reader Protocol	Being Development
	Reader Management Spec	Being Development
	Tag Data Resolution Protocol	Being Development
EPC Data Exchange	EPCIS Data Protocol	Being Development
	EPCIS Search Interface Protocol	Not Approved
	Object Name Operational Protocol	Not Approved
	EPCIS Data Gain Interface Protocol	Approved
	EPCIS Foundation Protocol	Not Approved
	User Authentication Protocol	Not Approved

Table 3. EPC Coding Structure.

Coding Program	Coding Type	Version	Domain Management	Object Class	Serial Number
EPC-64	I type	2	21	17	24
	II type	2	15	13	34
	III type	2	26	12	23
EPC-96	I type	8	28	13	23
EPC-256	I type	8	32	56	160
	II type	8	64	56	128
	III type	8	128	56	64

3.2.3. EPC Encoding Type

Currently, EPC code has three kinds 64, 96 and 256 bits. To ensure that all items have an EPC code and carrier label costs as low as possible so that it is recommended to use 96 bits type, so that their number may be provides unique identification to 268 million companies, and each manufacturer can have 6,000,000 object types and each object type can have 68 billion serial number, which have a very good enough to the future of the world.

4. Ellipse Curve Coding Algorithm

According to an elliptic curve point doubling formulas, in finite fields GF (q), suppose $P=(x,y)$, $2P=(x_1,y_1)$, and $x_1=(x+\frac{y}{x})^2+(x+\frac{y}{x})+a$, $y_1=x^2+(x+\frac{y}{x})x_1+x_1$. The reference [7] supposed that 4P, 8P, 16P can be directly calculated for solving 2mP when $m\geq 1$. Based on reference [4] we can know $4P=(x_2,y_2)$, $x_2=\frac{\zeta^2+(\delta\gamma)\zeta}{(\delta\gamma)^2}+a$, $y_2=\frac{\zeta(\delta\gamma)x_2+(\delta)^2}{(\delta\gamma)^2}+x_2$, $\gamma=x^2$, $\eta=\gamma+y$, $\delta=\eta^2+\eta x+a\gamma$, $\xi=\eta x+\gamma$, $\zeta=\delta(\delta+\xi)+\gamma^2$. As can be seen from these expressions, although the direct calculation of 4P will consume much more 9 times compared to first count 2P and then count 2*2P, it need less inversion time. Since an inversion time is usually more than 9 multiplications of the time, so this can effectively reduce the operation time.

Reference [8] made an expansion, we can know $x_k=(x_{k-1}+\frac{y_{k-1}}{x_{k-1}})^2+(x_{k-1}+\frac{y_{k-1}}{x_{k-1}})+a$, $y^2{}_{k-1}=x^2{}_{k-1}+(x_{k-1}+\frac{y_{k-1}}{x_{k-1}})x_k+x_k$, $x_k=\frac{a_k}{c_k}+a$, $y_k=\frac{b_k}{c_k}+x_k$. Based on these expression we can get $c_k=\delta^2$, $a_k=\gamma^2+\sigma\gamma$, $b_k=a^4{}_{k-1}+\sigma\gamma x_k$, $\sigma=a_{k-1}c_{k-1}$, $\gamma=a^2{}_{k-1}+b_{k-1}c_{k-1}$, $a_0=x$, $b_0=y$, $c_0=1$.

By comparison of the table 4, it can be seen that the improved algorithm from reference [5] has a fast replacing the square or multiplication, thus reducing the amount of calculation, to speed up the operation speed. Improved performance of the algorithm with the index s increases, respectively.

Table 4. Comparison between two algorithms.

	4P		8P		16P		2^sP	
	Algorithm 1	**Algorithm 2**	**Algorithm 1**	**Algorithm 2**	**Algorithm 1**	**Algorithm 2**	**Algorithm 1**	**Algorithm 2**
Multiplication	8	4	12	6	16	8	4 s	2 s
Square	8	4	12	6	16	8	4 s	2 s
Inverse	1	2	1	3	1	4	1	s
Total Time (μs)	501.05	488.62	710.24	720.24	920.49	977.24	169.16 s	243.31 s
Saving Rate	-2.4 %		1.3 %		5.8 %		30.5 %	

5. Security Protocol Design of EPCglobal Net

5.1. Design Refer to Network Security and Efficiency of EPCglobal

EPCglobal Network security problems exist mainly in the ONS and the client application to communicate the existence of security risks and the ONS internal security. ONS inquiry procedure shown in Fig. 2, in which (1)/(6) is the client application and the ONS for information exchange, the client application that generates queries sent to the ONS, the ONS further queries related EPCIS address information back to the client. (2)/(3) is the ONS and DNS (Domain Name System) for information exchange, mainly due to the IOT networks rely on the Internet, ONS first check whether there is a local EPC code corresponding to the EPCIS address information. If YES, that is immediately returned EPCIS address as in step (6); if not, the search for the appropriate DNS root ONS address and return it to the sub-ONS. (4)/(5) is the sub-ONS and the information exchange between the root ONS. (7) is a client application to get after the address on the EPCIS visit and other services [8, 11].

This shows that the query process will has ONS information hijack. First, ONS and the client application requests and responses returned when the data is easy to be hijacked, some sensitive information is leaked, seen from Fig. 4, the first of which (1)/(6) steps are involved; these leakage of information may be altered and re-send the entire system error. Again if the attacker gained an EPC tag, you can disguise the identity of the way through, from the ONS query detailed information of this product, leading to more sensitive information being leaked. While in ONS also need to ensure that ONS sub-server and root server communication security and credibility.

Also, because the characteristics of things of internet, often the client program in a shorter period of time has a large number of queries, each encryption will bring a huge propagation delay information which will lead to the exchange efficiency and storage efficiency greatly reduced, so we need to provide a kind of efficient and secure protocols.

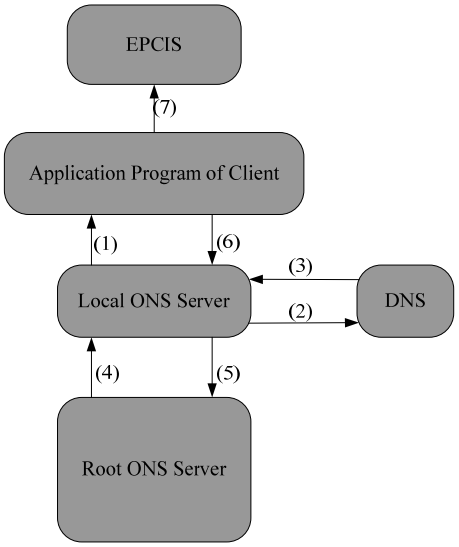

Fig. 4. Interact Procedure of ONS and Client Application Program.

This paper presents an algorithm based on elliptic curve cryptography options for resolving things EPCglobal network security and efficiency issues, and further for the ONS, applied ONS application interaction with the client in order to prevent the part may be subject to security threats. System design includes: a client application and the communication protocol between ONS. The agreement using the elliptic curve encryption algorithm security, and multiple handshake agreement, the agreement mainly for the system shown in Fig. 2 (1)/(6) the steps to avoid an attacker could intercept ONS client applications communicate with the data, including EPC code and other sensitive information; Meanwhile, the agreement contains ONS for client authentication process, elliptic curve encryption algorithm is randomly generated integer ONS calculated, and the client is also used in the encryption process random number is encrypted using a disposable set aside, the encryption key is not the same each time. These mechanisms prevent an attacker using information obtained illegally disguised attack. Prevent an attacker using camouflage to disguise the identity spoofing ONS, thereby performing inquiry service. Furthermore, the agreement contains the client for each of a complete verification of successful communication, as well as information on access authentication, the correctness

of the corporate identity. Overall system design, including Secure Sockets Layer Security protocol tunneling protocol, when there is no error, the error can not be decrypted if the key client encrypted data, the client ID error, the client exits and other incidents, the state machine automatically enters the initial state, which is waiting for a connection state. This effectively avoids the attacker can tamper with the intercepted message and send, or a DoS (denial of service) attacks leading to the ONS client application interacts with an error, to avoid loss of business information exchange. In addition, as elliptic curve encryption algorithm reduces processing overhead, with storage efficiency, computational efficiency and communication bandwidth savings and other advantages, and the agreement will be the client application requests bulk operations to address efficiency issues [10-12].

5.2. Communication Protocol between Safely Client and ONS Combined with ECC Algorithm

In this paper, based on elliptic curve encryption algorithm to solve the EPCglobal network security design is mainly used in the ONS and the client application interaction. The process is shown in Fig. 5, the specific protocol steps are as follows: 1) a client application generates query request, the request contains the ID of the client application and sends ONS. 2) ONS according to the acquired client application ID number, according to the ID in the back-end database, select the finite field GF (p) on an elliptic curve E: $y^2 = x^2 + ax + b$, $a, b \in GF(p)$, integer p indicates the characteristics of finite fields GF(p), and $g \in GF(p)$ indicates a point. Each parameter should meet: $p > 2^{160}$, $4a^2 + 27b^2 (\text{mod } p) \neq 0$. These parameters should be negotiated in advance with the client and announce in the document of parameters from elliptic curve. 3) ONS select a random integer x as the private key in [1, P-1], and obtained public key X=xg based on base point. ONS will set X to the client application. 4) Query messages contain sensitive information such as EPC code, commonly used EPC encode as 64/96 or 256 bits. Code EPC can get the M and the ID number should be placed in the header of information. The EPC code query batch connected with ID number, and then M will be embedded into the elliptic curve point P. 5) Client random select integer yg, and P+yX in [1,P-1], then sent yg and P+yX. 6) ONS receives information from client application, and it will be decrypted using the private key x, namely $(P + yX) - xyg = P + yxg - xyg = P$. If we get P, through conversion can get M. Because the client application ID number digits are known, can be directly obtained client application ID number and EPC code and other sensitive information, and you can get the comparison between ID number and the previous. 7) ONS sent the client ID number and query results into the user. Query results, address information of EPCIS, will be introduced DNSSec for data management or ensuring security. 8) Clients will verify the ID number with received ID number, if they are match very well which means that they have receive their expected results, else discarded [12-15].

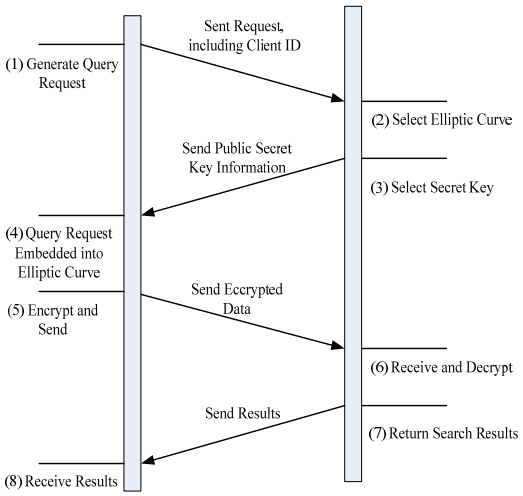

Fig. 5. Specific Flow of Security Program.

5.3. Combination of DNSSec into ONS

DNSSec is a security mechanism, the main context contains: key distribution and management, original data authentication and integrity verification, transmission and the requested authentication. Most of these services can prevent security threats against DNS. Because the hierarchy structure is very similar with ONS, so in DNS security problems also exist in the ONS.

Use DNSSec security mechanism, relying on elliptic curve encryption algorithm to be included in the EPCIS ONS address information and EPC information to create cryptographic signature. Cryptographic signature by calculating the hash function to provide data integrity in ONS, then protect the hash number. The use of private/public key pairs in elliptic curve encryption algorithm to encapsulate hash number, and then you can get the hash number with public key. If the hash value matches the calculated number, it indicates that the data is complete. In the internal ONS, it need to assure that the security and credibility between sub-server and root server when communication. From DNSSec mechanism, you can see that when the local ONS can not query the relevant records, it will send a query to the root ONS, then according to the relevant ONS address and access rights to access relevant ONS. The key of the mechanism is to access all relevant ONS must undergo root ONS, which will provide query address for relevant ONS.

6. Experiment and Analysis

In this experiment, suppose EPC coding of client application is EPC-64I type, namely 64bit. Suppose the client ID is 4bit. Algorithm programming tools is Java JDK 1.6. The experiment data is shown in Table 5. Encrypted information time overhead is 0.472 s, decryption time is 0.488 s. Such as increasing the amount of data processed, that is to handle 105 EPC data request at same time, the encryption of the entire process time overhead is 3.314 s, decryption time is 3.340 s. This experiment is completed in an ordinary PC, complete, and if the hardware conditions further improved, this program will greatly enhance the efficiency of the design.

Table 5. Experiment Data.

EPC Code/Per	Plaintext Length	Secret Key Length	Encryption time	Decryption time
1	68	128	0.472	0.488
10^5	6400004	128	3.814	3.340

7. Conclusion

In this paper, IOT network security issues, and network encryption protocols are facing high demand, is designed based on elliptic curve encryption algorithm to solve the EPCglobal Network security agreement, the agreement using the elliptic curve encryption algorithm safety and efficiency to meet the security and other safety equipment tamper-proof performance. The design is to get some things networking applications and want to get from the application of the system of security and efficiency of the system more effective improvements.

References

[1]. Rolf H. Weber, Internet of things – new security and privacy challenges, *Computer Law & Security Review*, Vol. 26, No. 1, 2010, pp. 23-30.

[2]. O. Gunther, Security challenges of the EPCglobal net-work Benjamin Fabian, *Communications of the ACM*, Vol. 7, Issue 52, 2009, pp. 121-125.

[3]. Ping Yu, Research on network privacy security based on model, *Journal of Chongqing Vocational Technical Institute*, No. 19, 2010, pp. 91-92.

[4]. Wang Yong Chao, Wei Wei, Lu Dong Ming, Wireless sensor network security review, *Computer Era*, No. 12, 2008, pp. 15-19.

[5]. Jiangyong Yao, Weiming Lang, et al., RFID standard of EPCglobal, *Logistics Technology*, No. 7, 2006, pp. 27-32.

[6]. Chen Xiang, Zhuang Yi, Wu Xuecheng, Research on ECC and application model of ECC to PKI, *Computer Technology and Development*, Vol. 16, No. 3, 2006, pp. 129-131.

[7]. J. Guajardjo, C. Paar, Efficient algorithms for elliptic curve cryptosystems, in *Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques*, Konstanz, Germany, May 11-15, 1997, Lecture Notes in Computer Science, *Springer-Verlag*, 1997, pp. 342-356.

[8]. Li Zhan, An improved algorithm elliptic curve cryptography, *Electronic Science and Technology*, No. 7, 2004, pp. 31-33.

[9]. Zhou Guo Xiang, Zhang Qing Sheng, ECC was applied on study of PKI, *Hefei University of Technology (Natural Science Edition)*, Vol. 26, Issue 6, 2003, pp. 101-107.

[10]. Hou Ai-Qin, Gao Bao-Jian, Xin Xiao-Long, An improved algorithm and its implementation for the embedding of plain text into elliptic curve, *Computer Applications and Software*, Vol. 25, Issue 7, 2008, pp. 63-65.

[11]. Xie Jian-Quan, A fast calculating method for large datamode power, *Information Security and Communications Privacy,* No. 8, 2006, pp. 21-27.

[12]. Wu Ming Hu, Zhang Yu, Opportunities and challenges introduced by things of internet, *Information Technology*, No. 5, 2010, pp. 97-99.

[13]. Hu Xiang Dong, IOT research and development review, *Digital Communications*, No. 2, 2010, pp. 19-23.

[14]. D. Chakrabarti, S. Maitra, B. Roy, A key pre-distribution scheme for wireless sensor networks: merging blocks in combinatorial design, *Journal of Information Security*, Vol. 5, Issue 2, 2006, pp. 105-114.

[15]. Lang Wei Ming, Wang Feng Dong, RFID Related Standards, *China Ratio*, Vol. 22, Issue 6, 2005, pp. 23-26.

2013 Copyright ©, International Frequency Sensor Association (IFSA). All rights reserved.
(http://www.sensorsportal.com)