RESEARCH ARTICLE

ScienceAsia 40S (2014): **16–21**

doi: 10.2306/scienceasia1513-1874.2014.40S.016

Enhancing data credibility by a lightweight security mechanism underlying the framework of the internet of things

Shu-Ching Wang[a], Ching-Wei Chen[a], Shun-Sheng Wang[b,*], Kuo-Qin Yan[c]

[a] Department of Information Management, Chaoyang University of Technology, Taiwan
[b] Department of Industrial Engineering and Management, Chaoyang University of Technology, Taiwan
[c] Department of Business Administration, Chaoyang University of Technology, Taiwan

*Corresponding author, e-mail: sswang@cyut.edu.tw

Received 13 Feb 2014
Accepted 9 Jun 2014

ABSTRACT: Currently, information technology is developing rapidly, and has resulted in vigorous development of the IPv6. The new concept of the future network is applied to smart objects which have sensing, networking and computing abilities, and the ability to transfer data between the objects; the novel network environment is called the internet of things (IoT). In addition to the past components of the network environment, there are also smart objects in the IoT. Hence there are hundreds of millions of bits in the data of the IoT. Studies on the middleware layer in the IoT have not discussed data insecurity issues. Thus the digital signature is used to establish a lightweight security mechanism between the application and the perception layer. Through the framework of the middleware layer, the identity of the application and the perception layer will have a verification and non-repudiation, and the security of the IoT can be obtained.

KEYWORDS: IoT, digital signature, middleware layer

INTRODUCTION

The internet of things (IoT) refers to uniquely identifiable things (objects) and their virtual representations in an internet-like structure. The term internet of things was first used by Baumgarten in 1999[1]. The concept of the IoT first became popular through the related applications. Radio-frequency identification (RFID) is often seen as a prerequisite for the IoT. If all objects and people in daily life were equipped with radio tags, they could be identified and inventoried by computers (European Commission). However, unique identification of things may be achieved as well through other means, such as barcodes or 2D-codes. IoT can apply the RFID to the internet architecture, and the communication can be achieved from Peer-to-Peer (P2P) extended to Machine-to-Machine (M2M). The report of the International Telecommunications Union (ITU) in 2005 stated that the IoT will connect the world's objects in both sensory and intelligent manner[2]. In the future world, any objects can be connected by the IoT, and be directly subject to communication at anytime and anywhere. The ITU has described the IoT from four dimensions: item identification (tagging things), sensors and wireless sensor networks (sensing things), embedded systems (thinking things) and nanotechnology (shrinking things). There are many aspects in the IoT, including ICT (information, communication and technology) and related applications. However, the challenges of IoT are the same as those in a network environment containing: cloud computing, distributed computing, wireless networks, wireless sensor networks and radio frequency technology[1,3]. IoT is a service-oriented architecture; there are more smart objects than the existing internet, hence the IoT will form a more complex entity subject to a deluge of data[4–6]. The data of sensing tags in the IoT constitute micro data; an actuator can quickly read and identify the data derived from the tags. However, if the data experience malicious interception or tampering, it will require a considerable degree of security in the IoT[7]. In addition, the privacy, identity management, security and access control between the sensors and applications in the IoT must be considered[4]. Through the framework of middleware (MW) layer, the identity of the application and the lightweight security between the middleware layer and the perception layer, the perception layer will require verification and non-repudiation, so that the availability and reliability of the IoT can be obtained and maintained.

Internet of things

Over the past 50 years, the internet has exponentially grown from a small research network, comprising only a few nodes, to a worldwide pervasive network that services more than a billion users. The miniaturization and cost reduction of electronic devices further expand the internet into a new dimension: to smart objects, i.e., everyday physical things that are enhanced by a small electronic device to provide local intelligence and connectivity to the cyberspace established by the internet. The small electronic device, a computational component that is attached to a physical thing, bridges the gap between the physical world and the information world. A smart object is thus a cyber-physical system or an embedded system, consisting of a thing (the physical entity) and a component (the computer) that processes the sensor data and supports a wireless communication linked to the internet[8]. The novelty of the IoT is not in the functional capability of a smart object, as many embedded systems are connected to the internet, but in the expected size of billions or even trillions of smart objects that bring about novel technical and social issues that are related to size. Some examples of these issues are authentic identification of a smart object, autonomic management and self-organization of networks of smart objects, diagnostics and maintenance, context awareness and goal-oriented behaviour, and intrusion of privacy[8]. The IoT is a novel paradigm that is rapidly gaining ground in the scenario of modern wireless telecommunications. The basic concept is the pervasive presence around us of a variety of things or objects, such as RFID, tags, sensors, actuators, mobile phones, etc., which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbours to reach common goals[9]. Unquestionably, the main strength of the IoT idea is the huge impact it will have on several aspects of everyday-life and behaviour of potential users. From the point of view of a private user, the most obvious effects of the IoT introduction will be visible in both the work and domestic fields. Several industrial, standardization and research bodies are currently involved in the development of solutions to fulfil the highlighted technological requirements[10]. This survey provides a picture of the current state of the art concerning the IoT. More specifically, the IoT has three functions[11].

(i) The IoT can provide the readers with a description of the different visions of the internet of things paradigm generated by different scientific communities.

(ii) The IoT can review the enabling technologies and illustrate the major benefits of the diffusion of this paradigm in everyday life.

(iii) The IoT can offer analysis of the major research issues the scientific community still has to face with.

Digital signature

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document[12]. A valid digital signature gives a recipient reason to believe that the message was created by a known sender such that they cannot deny sending it (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering[13]. Digital signatures are often used to implement electronic signatures, a broader term that refers to any electronic data that carry the intent of a signature, albeit not all electronic signatures use digital signatures[14]. An encryption method is used in digital signatures, publicly revealing that an encryption key does not reveal the corresponding decryption key[1]. This has two important consequences: (1) Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only they can decipher the message, since only they know the corresponding decryption key. (2) A message can be signed using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of their signature. This has obvious applications in electronic mail and electronic fund transfer systems[12]. Digital signatures employ a type of asymmetric cryptography. For messages sent through a non-secure channel, a properly implemented digital signature assures the receiver that the message was sent by the claimed sender[15]. Digital signatures are equivalent to traditional handwritten signatures in many respects, but properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes in the sense used here are cryptographically-based, and must be implemented properly to be effective[15]. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim that they did not sign a message, while also claiming that their private key remains secret; furthermore, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature remains valid. Digitally signed messages may be anything that can be represented as a bitstring; examples include electronic mail, contracts, or a message sent via some other cryptographic protocol. A digital signature scheme typically consists of three algorithms[15]:

(i) A key generation algorithm selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.

(ii) A signing algorithm is given a message and a private key then produces a signature.

(iii) A signature-verifying algorithm given a message, public key and a signature, either accepts or rejects the message's claim to authenticity.

Two main properties of digital signature are required[13]. First, a signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key. By using the digital signature, the authentication, integrity and non-repudiation of data can be ensured.

Wireless sensor networks

Wireless sensor networks (WSNs) comprise many spatially distributed small autonomous devices under cooperatively monitoring environmental conditions and sending the collected data to a command centre. This small device, called a sensor node, consists of sensor, wireless communication device, small micro-controller and energy source[16]. The WSNs are the important components of perception layers under the IoT, being responsible for regional collecting and monitoring of data. In the past, the WSNs have been used in both military and civilian applications, such as battlefield surveillance, habitat monitoring, healthcare and traffic control. Since WSNs are based on the wireless networks, they are prone to malicious attacks on different types of data transmission, or on small devices, such as impersonating, masquerading, or interception for misleading purposes. Recently, the issues of security in the field of the WSNs have been widely discussed. A number of researchers have investigated key management schemes and divided them into different categories[1,17,18], some studies on the three categories are based on the encryption techniques and the key establishment mechanism[16]. The three encryption techniques are symmetric, asymmetric, and hybrid. The symmetric-key schemes are widely used, as they entail relatively less computation complexity. On the other hand, the asymmetric schemes can provide much stronger security strength, but are considered too computationally expensive, related to the required high calculation and storage capacity for small devices. This study uses the arbitrated schemes that belong to symmetric-key schemes to solve this problem. Arbitrated schemes of key distributions and key establishment are based on a trusted entity, including a master key based pre-distribution scheme[19], base station participation[20]and a trusted third node-based scheme[21]. In a master key-based pre-distribution scheme, a master key is pre-distributed and stored to each sensor in the network. A pairwise key can be established by using this master key and a random number exchanged between each sensor. This scheme has infinite scalability, and each sensor needs very little memory. But the drawback is that, if the master key is compromised, all the pairwise keys are exposed[19]. An improved scheme has the master key erased after the pairwise keys are established[22]. In a base station participation process, each sensor has a share key with the base station; when two sensors need a pairwise key, the base station must send the pairwise key encrypted as the shared keys. This scheme has perfect resilience, but does not have good scalability[20]. In a trusted third node-based scheme, the key establishment between two sensor nodes is based on the common trust of a third node[21].

THREE-LAYER FRAMEWORK OF THE IoT

This study defines the topology of the IoT: the sink node (SN) of each region is responsible for the collecting requirement for the cloud service providers and deals with the sense devices of different services; thus each service provider may correspond to multi topology architecture. The middleware layer is defined as authenticating and processing of the cloud data, manages the private key of the sensors, and stores the signature of authenticate completion (Fig. 1). In this study, a three-layer framework of IoT is proposed, including the application layer, middleware layer and the perception layer. The proposed framework is shown in Fig. 2. The application layer can provide a wide range of network services, such as today's internet services and the services of networked smart objects. The middleware layer performs information transmission, processing and authentication of data between the perception layer and the application layer. The middleware layer entails two parts of the processing: Data Authentication and Data Processing. This study mainly discusses Data Authentication. Data Authentication involves three components: Devices and Services Monitoring Agent (DSMA), Authenti-

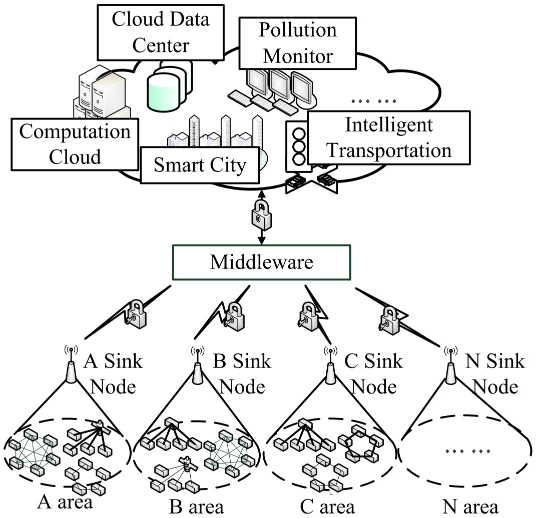

Fig. 1 The topology architecture of the IoT.

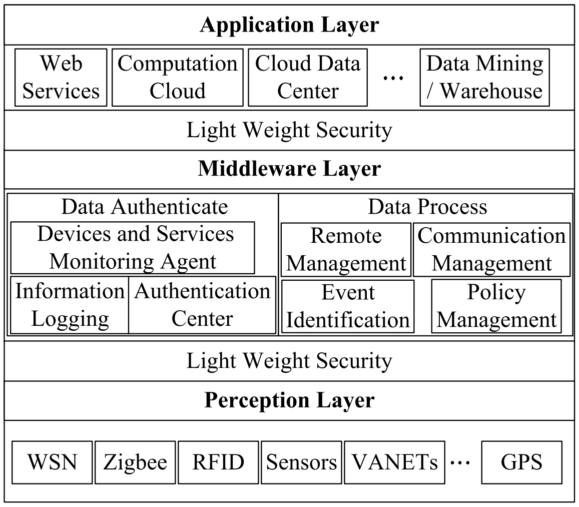

Fig. 2 The three-layer framework of the IoT.

cation Centre (AC) and Information Logging (IL). Through the devices and Services Monitoring Agent and the Authentication Centre, data are authenticated, with the signature stored in the Information Logging. The data are authenticated successfully via the Event Identification, the Communication Management, the Policy Management and the Remote Management, and completed by the middleware layer that uses a lightweight security mechanism to send data for the service providers between the application layer and the middleware layer.

Many scholars have discussed the lightweight security issues for the cloud computing environment. In this study, for the environment, the lightweight security of the cloud may be applied between the application layer and the middleware layer; thus the focus is on a proposed lightweight security mechanism between the middleware layer and the perception layer in the IoT environment.

THE OPERATION FLOW OF LIGHTWEIGHT SECURITY MECHANISMS

This study applied the concept of the digital signature to ensure the reliability of data, by using the third-party arbitration approach, with the middleware layer as third-party authentication to ensure data transmission between the source and destination.

Generated $K_{\mathrm{SN}_i,\mathrm{MW}}$, K_{SN_i} and K_{AC}

In the framework of this study, the perception layer must make identity authentication through the middleware (MW) layer. Let SN_i be the sink node (SN) identifier i where $i \geqslant 0$. Between the SN_i and MW a session key $K_{\mathrm{SN}_i,\mathrm{MW}}$ will be generated. $K_{\mathrm{SN}_i,\mathrm{MW}}$ is generated by K_{SN_i} and K_{MW}, converted to XOR. The session key function is building a secure communication channel for SN_i and MW because K_{SNi} may face the risk of being compromised. In the transmission process, the session key enhances the security of transmission for SN_i and MW. The devices and services monitoring agent (DSMA) starts to calculate the private key for SN_i of every area and the authentication centre (AC); via generated random value of function, using the private key of DSMA, $r_{\mathrm{DSMA}(\cdot)}$, it generates K_{SN_i} and K_{AC}, finally loading to the sensor node and authentication centre, respectively.

Authenticate phase

SN_i→DSMA:$E\big(K_{\mathrm{SN}i}, K_{\mathrm{SN}i,\mathrm{MW}}, [\mathrm{SN}_i, h(\mathrm{OM})]\big)$

DSMA→AC:$E\big(K_{\mathrm{AC}},$

$[E(K_{\mathrm{SN}_i}, K_{\mathrm{SN}_i,\mathrm{MW}}, [\mathrm{SN}_i, h(\mathrm{OM})]), \mathrm{TS}]\big)$

SN_i collected the original message (OM) through the hash function $h(\cdot)$ to be converted to a fixed-length message digest h(OM). It then used the private key of SN_i, K_{SN_i}, and session key $K_{\mathrm{SN}_i,\mathrm{MW}}$ to encrypt a signature that was transferred to DSMA of MW and AC performed authentication. DSMA executed authentication of the first phase K_{SN_i} and $K_{\mathrm{SN}_i,\mathrm{MW}}$, verifying the identity of SN_i. Then DSMA sends that verified message to AC; AC used K_{AC} obtain the plaintext of SN_i, and stores the signature $E\big(K_{\mathrm{SN}_i}, K_{\mathrm{SN}_i,\mathrm{MW}}, [\mathrm{SN}_i, h(\mathrm{OM})]\big)$ and the timestamp (TS) in the information logging (IL). The plaintext data are delivered to the subroutine of the MW layer that processes the data.

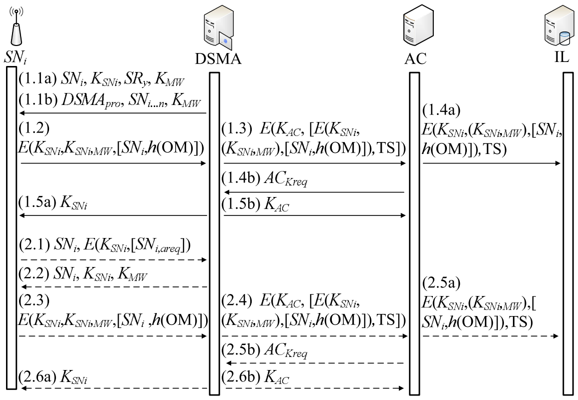
SN_i
DSMA
AC
IL
(1.1a) SN_i, K_{SNi}, SR_y, K_{MW}
(1.1b) $DSMA_{pro}$, $SN_{i...n}$, K_{MW}
(1.2) $E(K_{SNi},K_{SNi,MW},[SN_i,h(\mathrm{OM})])$
(1.3) $E(K_{AC}, [E(K_{SNi}, (K_{SNi,MW}),[SN_i,h(\mathrm{OM})]),\mathrm{TS}])$
(1.4a) $E(K_{SNi},(K_{SNi,MW}),[SN_i, h(\mathrm{OM})]),\mathrm{TS})$
(1.4b) AC_{Kreq}
(1.5a) K_{SNi}
(1.5b) K_{AC}
(2.1) SN_i, $E(K_{SNi},[SN_{i,areq}])$
(2.2) SN_i, K_{SNi}, K_{MW}
(2.3) $E(K_{SNi},K_{SNi,MW},[SN_i ,h(\mathrm{OM})])$
(2.4) $E(K_{AC}, [E(K_{SNi}, (K_{SNi,MW}),[SN_i,h(\mathrm{OM})]),\mathrm{TS}])$
(2.5a) $E(K_{SNi},(K_{SNi,MW}),[SN_i,h(\mathrm{OM})]),\mathrm{TS})$
(2.5b) AC_{Kreq}
(2.6a) K_{SNi}
(2.6b) K_{AC}

Fig. 3 Process of the data authentication.

Process of authentication

The authentication process has two scenarios: (1) the service provider or DSMA sends out a probe message to collect data, (2) SN_i collects urgent data that must be immediately undergo DSMA authentication and be transmitted to the service provider. (1.1a) When the service providers need the data of devices from the perception layer, a notification message via DSMA can be sent to SN_i, DSMA provides the requirements to the service provider y sends out requirements for the data collection SR_y in the notification message. K_{SN_i} is a new private key generated via DSMA that replaces the original K_{SN_i}. Furthermore, the session key $K_{\mathrm{SN}_i,\mathrm{MW}}$ is generated via K_{MW} and the original K_{SN_i} is converted to XOR. (1.1b) DSMA requests the regional SN_i to send the data periodically. Thus DSMA sends a probe message to ask SN_i to transfer the data, $\mathrm{DSMA}_{\mathrm{pro}}$; DSMA writes K_{MW} into the notification message, and the session key $K_{\mathrm{SN}_i,\mathrm{MW}}$ is generated via K_{MW} and original K_{SN_i} converted to XOR. (1.2) After SN_i collects OM which, through the hash function, is converted to a fixed-length message digest $h(\mathrm{OM})$, and returns an authenticated K_{SN_i} and $K_{\mathrm{SN}_i,\mathrm{MW}}$ is sent to DSMA. (1.3) DSMA uses K_{AC} to encrypt data of SN_i again and send authenticated K_{SN_i}, $K_{\mathrm{SN}_i,\mathrm{MW}}$ and TS to AC. (1.4a) AC will match K_{AC}, K_{SN_i} and $K_{\mathrm{SN}_i,\mathrm{MW}}$; if correct, then it stores the signature $E\big(K_{\mathrm{SN}_i}, K_{\mathrm{SN}_i,\mathrm{MW}}, [\mathrm{SN}_i, h(\mathrm{OM})]\big)$ and the TS in the IL. And (1.4b) returns an updated message for the AC private key, $\mathrm{AC}_{\mathrm{Kreq}}$. Finally (1.5a) and (1.5b) will be updated private keys with SN_i and AC (Fig. 3). SN_i active sends out the requirements for transferring the data. In addition to periodic collected data under the IoT environment, when the sensor device discovers unreasonable data, they are immediately transferred for analysis and processing by the middleware layer. (2.1) SN_i active sends out the requirements for transferring the data $\mathrm{SN}_{i,\mathrm{areq}}$ to DSMA with K_{SN_i}. (2.2) DSMA authenticates the identity of SN_i; if the identity is correct, it then returns a new K_{SN_i} and K_{MW}. The subsequent authentication process of (2.3) to (2.6) and (1.2) to (1.5) is the same (Fig. 3).

CONCLUSIONS

This study proposed architecture for arbitrated digital signature with symmetric encryption to transfer data between the perception layer and the middleware layer. The private keys of SN_i and AC use DSMA to generate, and add $K_{\mathrm{SN}_i,\mathrm{MW}}$ to ensure the integrity of data, verifiability of identity and non-repudiation. The transmission generates the signature and the timestamp that are then stored in the information logging of the middleware layer in order to prove the trustworthiness of the data. Since this study only proposes a lightweight security mechanism between the perception layer and the middleware layer, in future work, we will analyse and discuss the security issues between the application layer and middleware according to the existing lightweight security mechanisms for cloud computing, and propose improved methods and applications for the IoT environment.

Acknowledgements: This work was supported in part by the Taiwan National Science Council under Grants NSC101-2221-E-324-032, NSC101-2221-E-324-034 and NSC102-2221-E-324-008.

REFERENCES

1. Sarma AC, Girão J (2009) Identities in the future Internet of Things. *Wireless Pers Comm* **49**, 353–63.
2. International Telecommunications Union (2005) *ITU Internet Reports 2005: The Internet of Things - Executive Summary*. ITU, Geneva.
3. Perrig A, Szewczyk R, Tygar JD, Wen V, Culler DE (2002) SPINS: Security protocols for sensor networks. *Wireless Netw* **8**, 521–34.
4. Lee H, Kim YH, Lim J (2007) Classification of key management schemes for wireless sensor networks. In: *Advances in Web and Network Technologies, and Information Management*, pp 664–73.
5. Sarma SE, Weis SA, Engels DW (2003) RFID systems and security and privacy implications. In: Kaliski BS, Koç ÇK, Paar C (eds) *Cryptographic Hardware and Embedded Systems - CHES 2002*, pp 454–69.
6. Zhou Q, Zhang J (2011) Research prospect of Internet of Things geography. In: *19th International Conference on Geoinformatics*, pp 1–5.
7. Teixeira T, Hachem S, Issarny V, Georgantas N (2011) Service oriented middleware for the Internet of Things:

a perspective. In: *Towards a Service-Based Internet*, pp 220–9.

8. Kopetz H (2011) *Real-Time Systems: Design Principles for Distributed Embedded Applications*, 2nd edn, Springer US.
9. Giusto D, Iera A, Morabito G, Atzori L (2010) *The Internet of Things. 20th Tyrrhenian Workshop on Digital Communications*, pp v–xviii.
10. Wang B (2009) Review on internet of things. *J Electron Meas Instrum* **23**, 1–7.
11. Luigi A, Antonio I, Giacomo M (2010) The Internet of Things: a survey. *Comput Netw* **54**, 2787–805.
12. Rivest RL, Shamir A, Adleman L (1978) A method for obtaining digital signatures and public-key cryptosystems. *Comm ACM* **21**, 120–6.
13. Pointcheval D, Stern J (2000) Security arguments for digital signatures and blind signatures. *J Cryptol* **13**, 361–96.
14. Mao W (2004) *Modern Cryptography: Theory and Practice*. Prentice Hall PTR.
15. Merkle RC (1988) A digital signature based on a conventional encryption function. In: *Advances in Cryptology - CRYPTO '87*, pp 369–78.
16. Zhang J, Varadharajan V (2010) Wireless sensor network key management survey and taxonomy. *J Netw Comput Appl* **33**, 63–75.
17. Ren X, Yu H (2006) Security mechanisms for wireless sensor networks. *Int J Comput Sci Netw Secur* **6**, 155–61.
18. Sun D, He B (2006) Review of key management mechanisms in wireless sensor networks. *Acta Automat Sin* **32**, 900–6.
19. Chan H, Perrig A (2005) PIKE: Peer intermediaries for key establishment in sensor networks. In: *IEEE INFOCOM 2005 - IEEE International Conference on Computer Communications*, no. 1, pp 524–35.
20. Coetzee L, Eksteen J (2011) The internet of things - promise for the future? An introduction. In: Cunningham P, Cunningham M (eds) *IST-Africa 2011 Conference Proceedings*, pp 286–94.
21. Yang X, Li Z, Geng Z, Zhang H (2012) A multi-layer security model for Internet of Things. In: *Internet of Things*, pp 388–93.
22. Zhu S, Setia S, Jajodia S (2003) LEAP: Efficient security mechanisms for large-scale distributed sensor networks. In: *Proceedings of the 10th ACM Conference on Computer and Communications Security*, pp 62–72.