Research Article

Adaptive Sensing Private Property Protection Protocol Based on Cloud

Kai Fan,1 Wei Wang,1 Hui Li,1 and Yintang Yang2

1State Key Laboratory of Integrated Service Networks, Xidian University, Xi’an 710071, China
2Key Laboratory of Ministry of Education for Wide Band-Gap Semiconductor Materials and Devices, Xidian University, Xi’an 710071, China

Correspondence should be addressed to Kai Fan; kfan@mail.xidian.edu.cn

Received 15 May 2015; Accepted 6 September 2015

Academic Editor: Jianping He

Copyright © 2015 Kai Fan et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Private property refers to something carrying private information, or expensive items; these items are very important for companies or individuals. The proposed private property protection system uses adaptive sensing technology to protect private materials in real time. In this paper, we propose an adaptive sensing private property authentication scheme which can be applied in the cloud computing. Considering a relatively safe room with a remote reader, there are several valuable items in the room. Each item is labeled with a unique tamper-evident adaptive sensor and the reader can simultaneously read a plurality of sensors. Encrypted information of items, sensors, and readers is stored in the cloud. The reader reads sensors and uploads the collected data to the cloud for further processing in real time. The proposed scheme is under the cloud environment to protect the user privacy and prevent synchronized attacks. Compared with some traditional schemes, our scheme is economical, practical, and easy to be expanded. Furthermore, it pays attention to privacy protection with real-time monitoring.

1. Introduction

Nowadays the network information developed well enough, and the requirement of property security has also been raised to a new level. Personal privacy is usually under a great threat, especially private valuable property, such as antiques, gold, jewelry, and, many well-known pictures. Under normal conditions, valuable private property may be managed by insurance company, as a result, the user information leaks easily. Considering a situation where customers want to keep security of private property but do not want more persons to know, first, insurance company managers cannot access the private property easily, because many items are easy to damage, but when something abnormal occurs, the manager can locate sensor accurately [1]. Secondly, even though many hackers have attacked the management system, they cannot obtain any useful information. Although the RFID system has wide prospect, it has to face huge challenges because of potential security risks, privacy problems, and efficiency because of its restrictions on processing, storage, and power in RFID tags [2]. WSANs contain static sensors that are energy-constrained and actors that cannot communicate with each other directly. These unique characteristics make the data dissemination problem in WSANs extremely challenging [3]. By analyzing the above reasons, adaptive sensing technique and cryptography are the key techniques in private property protection system. Sensing technology is safer and has more economic means of monitoring; it is more reliable than the traditional access control and authorization technology [4].

Due to the rapid development of wireless communication and hardware device technology, Wireless Sensor Networks (WSNs) are expected to be widely applied in security areas such as intrusion detection, border surveillance, and fire detection [5]. Because the sensors are mobile devices, they may encounter various issues when providing ongoing services. For instance, they may suddenly disconnect from the network, since the mobile devices carried by people could change their point of attachment very frequently. That may cause significant packet loss and degrade the quality-of-experience (QoE) of consumers [6]. The scheme we propose
uses adaptive sensor to collect information; it can prevent forgery and has a higher transmission speed than a bar code and a two-dimensional code. Also, it can operate stably at the condition of low temperature, high temperature, and humidity [7]. The tamper-evident adaptive sensors embedded in the valuables are not easily found by the illegal user, so they will not affect the appearance of goods and does not harm the customer’s property. But how do we deploy them? The first approach, namely, random deployment, assumes that sensors are abundant and randomly distributed. Clearly, the random deployment may result in suboptimal network topology and thus degrades the barrier coverage performance [8]. Therefore, it is of great interest to deploy as few sensors as possible while ensuring the desirable performance.

The other fundamental question is how to deploy readers in a network to ensure that the WISP (wireless identification and sensing platform) tags can receive harvest sufficient energy for continuous operation. Point provisioning uses the least number of readers to ensure that a static tag placed in any position of the network will receive sufficient energy. Path provisioning exploits the potential mobility of tags (e.g., those carried by human users) to further reduce the number of readers necessary: mobile tags can harvest excess energy in power-rich regions and store it for later use in power-deficient regions [9]. By exploiting the physical characteristics of wireless sensor, point provisioning can greatly reduce the number of readers compared with those assuming traditional coverage models. Reader placed in the room reads adaptive sensors in real time. The reader cannot read sensor information correctly when the sensor is opened or the property was taken from within the read range. Then, the clouds will give alarm information to the security guards. If additional items will be placed in the room, just store items information in the clouds. If the client took the item away, simply delete the corresponding records from the cloud information. Since this system is long-term real-time monitoring, which would generate a lot of data, the system also has to process data with a high speed. So it is not suitable to use the backend server to store and process data locally.

Cloud computing has brought a new round of information revolution; the technology which combines traditional adaptive sensing with cloud computing is promising. Because the cloud itself is open, the cloud security is a serious problem. Adaptive sensing technology can adaptively change sensing time and sensing frequency without affecting the sensing quality; the benefits of this technology are that we can reduce power consumption and facilitate the coordination between the sensors [10]. Adaptive sensing technology has been applied to government departments, military, and financial protection, but there will be privacy and security issues while using this technology [11]. The scenario in this paper is assumed for the security of companies, customers, and items information which is required to be absolutely private. While traditional safety protection is mostly done manually, it is inefficient and unsafe. We can use the bar code and two-dimensional code technology to protect the valuables, but bar codes and two-dimensional codes are easy to fake and are fragile. In addition, when many bar codes are present simultaneously, there is too much interference between the multiple bar codes, especially in the case where the multiple bar codes are overlapped [12].

We move data storage and processing from the traditional backend servers to the cloud. By using the new technique, only legitimate users know the account name and password, so they can manipulate the data, no matter when and where customers are; they can obtain the adaptive sensing information as long as the readers which can be fixed or mobile are connected to the network. [13].

The rest of the paper is structured as follows. In Section 2, including the review content, we also detail the reasons that current adaptive sensor authentication schemes are incapable to work in cloud-based scenarios and provide primary requirements to design a cloud-based adaptive sensing authentication scheme. The scheme is proposed in Section 3. It applies a global EHT (encrypted hashtable), mobile reader, or fixed reader, and the first adaptive sensing authentication protocol against database keepers is proposed in detail. In Section 4, we provide the analysis and evaluation of our scheme. We give our conclusions and the following work in Section 5.

2. Related Work

2.1. Cloud Computing. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal protection effort or service provider interaction. Many services are migrating to the cloud for its better scalability, cost efficiency, and other benefits. Cloud computing also offers an appropriate environment for deploying evacuation services [14]. Cloud computing is a new computing model which comes from distributed computing, parallel computing, virtualization technology, and other computer technologies and it has many advantages such as large-scale computation and data storage, virtualization, high expansibility, high reliability, and low price service [15].

Cloud computing has three service models including Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), and Cloud Infrastructure as a Service (IaaS); Cloud computing has four deployment models including Private Cloud, Community Cloud, Public Cloud, and Hybrid Cloud. Key enabling technologies include the following: (1) fast wide-area networks, (2) powerful, inexpensive server computers, and (3) high-performance virtualization for commodity hardware. The security problem of cloud computing is very important and it can prevent the rapid development of cloud computing. Single security method cannot solve the cloud computing security problem and many traditional and new technologies and strategies must be used together for protecting the total cloud computing system [16].

2.2. Adaptive Sensor. Adaptive sensor is a wireless automatic identification technology. Unlike traditional static sensors, adaptive sensors have locomotion and are thus able to autonomously improve network performance by adjusting
their initial status to desired ones [17]. Compared to other existing wireless technologies, it has some advantages such as strong adaptability, low power consumption, high sensitivity, strong storage and data processing capabilities, and stable performance [18]. Sensors can recognize specific target via wireless signal; it does not need the establishment of mechanical or optical contact between recognition system and a specific target. The technology has been widely used in Internet of Things (IoT), health care, logistics protection, environmental monitoring, military, and food security [9]. In the IoT systems, physical things in our environment and people will be connected anywhere and anytime via any service. These connections can be made with intelligent sensors, GPS, adaptive sensing systems or any sensing devices which can exchange data between two objects [19]. The ubiquitous availability of devices such as smartphones, tablets, and other portable devices enables the collection of massive amounts of distributed data from the daily lives of citizens. These types of emerging mobile networks can provide new forms of valuable information that are currently not available on this scale via any traditional data collection methods [20].

Adaptive sensing system is usually protected by authentication and encryption in terms of privacy and safety. If the two parties are not certified before beginning a communication, the system will be likely attacked by some ways such as interception, counterfeiting, replay, denial of service, and desynchronization.

Traditional adaptive sensing system has two typical ways which are as shown in Figures 1 and 2.

The architecture consists of sensor, reader, and the backend server [21]. Reader delivers the message from the sensor to the backend server in this architecture, and sensor is certificated through the background database. Because it is special cable connection between the reader and the server, the channel is considered to be safe. When designing authentication protocol, the security of the frontend communication between adaptive sensor and the reader needs to be considered; however, the backend security issues do not need to be considered. But the weakness of the architecture is that the reader uses a special cable network, which limits the reader’s mobility. In addition, a backend server’s storage and computing power are limited, so the presence of large amounts of data is likely to lead to system crash.

The model in Figure 2 can be used offline via mobile reader to authenticate the adaptive sensor [21]. The system consists of adaptive sensor, reader, and CA and is divided into two phases: initialization and certification. In the initialization phase, reader downloads AL (access list) from CA through secure channel, and then the reader becomes a portable device, which can have the ability of offline authentication. During authentication phase, the reader sends RID to sensor, waiting for the sensor response $H(RID, Kt)$ to reader. In order to gain legal SID, reader exhaustively tries to match the $H(RID, Kt)$ in AL.

In recent years, some authentication schemes for adaptive sensing system are put forward, but the common weakness is that the data between these protocols is plaintext form, it is easy to expose sensors and readers information, and an attacker can track sensor. It is extremely dangerous for the security system, because the attacker is likely to implement the theft once determining the item information. At present, most authentications cannot resist synchronization attacks, which is a fatal flaw in the real-time monitoring system. As a result, the previous authentication cannot be directly applied to the scenario.

2.3. Requirements of Cloud-Based Adaptive Sensing. Cloud has a capacity of powerful computing and storage and can allocate storage space dynamically. In addition, robustness is an important reason for its popularity, so this system makes use of these advantages. The private property protection system consists of sensor, reader, and cloud, the cloud instead of the traditional server to store data and query record. It is necessary to consider the security of communication between
3. The Adaptive Sensing Private Property Protection Protocol Based on Cloud

As it is shown in Table 1, the sensor and the reader identity information is processed by one-way hash function instead of plaintext form. In this case, we can protect the reader and adaptive sensor privacy from leaking to untrusted cloud. We introduce adaptive sensor and reader privacy, authentication protocol against untrusted database.

3.1. Notations and Assumptions. Notations in this paper are listed in Notations section. Reasonable assumptions are listed as follows:

(i) Adaptive sensors are with middleweight computing capacity of XOR, PRNG, and hashing processes.

(ii) Readers are with middleweight computing capacity of XOR, PRNG, and hashing processes.

(iii) The frontend communications between sensors and readers are on public radio channels. Attackers are able to eavesdrop, manipulate, delete, and replay frontend messages.

(iv) Cloud obtains computing capacity of XOR, PRNG, hashing processes, and symmetric encryption and decryption. The cloud provider as the database keeper is not trusted. It may be malicious or vulnerable.

3.2. Encrypted Hash Table. Encrypted hash table is used in the scheme that can prevent the private information of customers from leaking to the cloud; it can also promise client’s anonymous access. The structure of encrypted hash table is shown in Table 1; NUM denotes the current maximum number of sessions between the reader and the sensor, after the session between reader and sensor is completed successfully, the value of NUM will be plus one. The index \(H(RID \ || \ SID \ || \ NUM)\) is unique because the number of NUM changes constantly, according to the characteristics of one-way hash function, an attacker cannot forge the index value.

\[ E((RID \ || \ SID \ || \ NUM \ || \ Data) \oplus \ RID) \]

can be obtained through searching the index value \(H(RID \ || \ SID \ || \ NUM)\); it is cipher text using algorithm selected by the cloud. The scheme of encryption and decryption is accomplished by the cloud. This greatly reduces the burden of the reader and adaptive sensors. Even if the cloud can decrypt the data using its algorithm, the result of decrypted data is still the XOR operation. The cloud cannot have the most important data, so it is unable to obtain relevant information. Data domain stores some application data, such as the position of the sensor, item type, storage time, and access time; all these
Figure 4: The adaptive sensing private property protection protocol based on cloud.

The proposed protocol is as follows. The 1st step of the proposed protocol is for the reader to obtain $N$ and $S$. The reader initiated inquiry signal “query,” between the sensor and the reader by using the flags bit. An adaptive sensor queries flag bit before it communicates with reader; if Flag = 0, NUM will use $N$ in the communication; if Flag = 1, NUM will use $N + 1$ in the communication. The scheme is different from the conventional backend server authentication scheme. The traditional authentication scheme assumes that the communication between reader and the backend server is secure. However, the cloud acts as the backend server in the scheme. The traditional security authentication protocol is not applicable in this situation because the cloud is not entirely credible [18]. So we propose a new protocol for the private property protection scheme using the adaptive sensor under a cloud environment.

The proposed protocol is as follows. The 1st step of the proposed protocol is for the reader to obtain $N$ and $S$. The reader initiated inquiry signal “query,”...
Table 2: Performance comparison.

| Authentication protocols | Mutual authentication | Confidentiality | Complete anonymity | Anticounterfeit | Antireplay | Against synchronization attack | Anti-dos attack | Revocation |
|--------------------------|-----------------------|-----------------|-------------------|----------------|-----------|-------------------------------|----------------|-----------|
| Chien protocol           | ✓                     | ✗               | ✗                 | ✓              | ✓         | ✗                            | ✗              | ✓         |
| Tan protocol             | ✗                     | ✓               | ✗                 | ✓              | ✗         | ✗                            | ✗              | ✗         |
| Proposed protocol        | ✓                     | ✓               | ✓                 | ✓              | ✓         | ✓                            | ✓              | ✓         |

$H(R \parallel S \parallel N)$; as the authentication request of adaptive sensor is sent to the reader, reader retrieves the record through $H(R \parallel S \parallel N)$; then, the cloud decrypts $E((R \parallel S \parallel N) \oplus R)$, so we can get $(R \parallel S \parallel N) \oplus R$. At the same time, cloud will generate a random number $N_c$ as a challenge to the reader sent together with $(R \parallel S \parallel N) \oplus R$. In order to obtain $R, S, N_c$, reader operates as $(R \parallel S \parallel N) \oplus R \oplus R$ and checks the integrity by verifying $R$.

The 2nd step is to authenticate the adaptive sensor. The reader generates a random number $N_c$ as a challenge to the adaptive sensor. The sensor calculates $H(R \parallel S \parallel N_c)$ as a response and a random nonce $N_c$ as its challenge to the reader. The reader verifies the response, if valid, and the 3rd step is started; otherwise, the protocol is terminated.

The 3rd step is to check the synchronization of $N$ between the sensor and the EHT. In addition, reader must respond to the challenge of cloud. The reader calculates $(R \parallel S \parallel N_c) \oplus R \oplus N_c$, as a response to the cloud. If valid, the reader tries to read the next record indexed by $H(R \parallel S \parallel (N+1))$ from the EHT and check the integrity. If there is a valid record, it means that the sensor and the cloud have desynchronized. The reader continues trying to read the $(N+2)$th record indexed by $H(R \parallel S \parallel (N+2))$ and so on, until finding the last valid record, assuming its $N$ is $M$.

The 4th step is to update the adaptive sensor and response to the challenge of sensor. The reader calculates $H(R \parallel S \parallel N_c)$ and then operates $H(R \parallel S \parallel N_c) \oplus M' \oplus N_c$ as a simple encryption, which is sent to the sensor with $H(R \parallel S \parallel M')$ which is also to be verified by the sensor. If valid, then $N = M' + 1$.

The 5th step is to confirm the adaptive sensor update successfully. Adaptive sensor sends $H(R \parallel S \parallel M' \oplus R)$ to the reader. If the reader cannot receive a response signal within the fixed time, the reader sends update information to sensor again. If the received message $M' \oplus H(R \parallel S \parallel M') \oplus H(R \parallel S \parallel N_c)$ is not equal to zero, the reader also sends updating information to sensor again. If sensor receives resend updating information, the sensors repeat the operation of the last step, the reader always waiting for the response from the adaptive sensor until the reader confirms that the sensor updates successfully.

The 6th step is to update the cloud EHT. The cloud writes $E((R \parallel S \parallel M') \oplus R)$ together with the index $H(R \parallel S \parallel M')$ into the EHT, where $M' = M + 1$.

The 7th step is to confirm the cloud updates successfully. A message of $H(R \parallel S \parallel M' \oplus (R \parallel S \parallel M') \oplus R$ is sent back to the reader from the cloud to confirm the updating is successful. The session between sensor and reader is successful, so the flag bit $\text{Flag} = 1$; until now the authentication protocol is terminated.

4. Analysis and Evaluation

The proposed protocol is analyzed and evaluated in this section.

4.1. Security and Privacy

In this section, we compare with two classical authentication schemes. One is backend-server-based scheme of Chien and Chen [24]. The other one is the first server-less authentication protocol proposed by Padmanabhi and Shanmugapriya [25]. These two protocols are very typical; this has attracted much attention. Comparison in performance is listed in Table 2.

Mutual authentication typically means that a sensor authenticates a reader while the reader authenticates the sensor. In addition, mutual authentication is also considered between the reader and the cloud in our protocol. It is useful for access control of sensors. The server-less protocol [26] only achieves unilateral authentication. The protocol [24] achieves mutual authentication which is essential for a protocol, but it lacks mobility. It is feasible for attackers to pretend to be an authorized reader successfully sending fake messages without mutual authentication [25, 27].

The proposed authentication protocol can protect against synchronization attack. It is vital to the protocols applied to real-time monitoring system. In particular, the system is based on cloud. It is clever to use “Flag” which is very convenient to determine the state whether it is of desynchronization or not. In our protocol, the step of confirmation is indispensable after the sensor or the cloud updates. We also add a delay judging device in protocol innovatively when we confirm the success of update. To the best of our knowledge, the proposed protocol is invulnerable to all existing types of desynchronization attacks. The protocol [20] is put forward in a typical scheme which can protect against desynchronization. But it has two fatal mistakes; the first is that mutual authentication is absent between the reader and the untrusted cloud; this will be directly related to the synchronization problem. Because the reader is always giving a wrong $H(R \parallel T \parallel S)$, the cloud cannot find $H(R \parallel T \parallel S)$ in EHT; the cloud will consider the communication with tags has lost synchronization. In fact, it is possible that the communication between the tag and cloud works normally. The second one is that the protocol [21] updates EHT first before the tag; the practice will directly lead to the increase
of computation. If tag cannot update successfully, it will spend a lot of time when the reader searches in EHT. The problem of desynchronization is easy to be ignored in many protocols; the protocol [24] has been proven to be vulnerable to desynchronization attacks.

Anti-dos attack is also indispensable in an adaptive sensing private property protection system. In the information processing system based on the cloud, the cloud is usually an important target in the anti-dos attack [28]. In our proposed authentication protocol, $H(R \| S \| N)$ as the authentication request of adaptive sensor is sent to the reader and retrieves the record through $H(R \| S \| N)$, and then cloud decrypts $E((R \| S \| N) \oplus R)$. If attacker counterfeits an $S$ and generates a wrong $H(R \| S \| N)$, the alarm system will initiate immediately. The reader finds out the wrong number of $S$ and terminates the service for attacker. In the meantime, the service to legitimate users will be normal. From the above analysis, the data of attackers cannot be processed further; thus, the system will run normally; the condition that legitimate users cannot access will not occur.

Database security is a crucial but widely neglected issue in current adaptive sensor researches [29]. The issue is about how to keep privacy of sensors/readers even if the database keeper is malicious. In the proposed cloud-based protocol, data in the EHT is either encrypted or hashed, and the cloud is malicious, even if the decryption is executed by the cloud but the data is the result of XOR. The frontend communications between sensors and readers are composed of random challenges and hashing function. The use of challenge-response technology provides the frontend communications with freshness, defending against replaying attacks. The hashing functions are used in order to protect the privacy of RID, SID, and NUM, defending against eavesdropping and manipulating. The EHT is composed of hashed and encrypted data, unfeasible to be eavesdropped on or manipulated. The database security in the protocol [24] entirely depends on the assumed-trustworthy and assumed-invulnerable backend server. Although an AL is partly hashed in the server-less protocol [26], the SID field is stored in plaintext form. Once the reader which is with AL is stolen, attackers are able to trace all sensors listed in the AL.

4.2. Complexity and Authentication Mode. The least numbers of calculation between complete sessions are listed in Table 3. We compare with two classical authentication schemes again. The operation of encryption and decryption usually requires a lot of computing resources. The scheme of encryption and decryption is accomplished by the cloud. This greatly reduces the burden of the reader and adaptive sensors. The scalability of this scheme is also very attractive. In the proposed protocol, $H(R \| S \| N)$ is an index sent to a reader. The reader can therefore read the matched record from the EHT only one time using accurate index, so the complexity of the proposed scheme is only $O(1)$ which means better scalability than most current adaptive sensor authentication protocols. Both protocols [24, 26] depend on a brute-force search through the database or the AL to find a legal SID; it makes the computational complexity $O(N)$, where $N$ denotes the number of sensors. It means these protocols are not well scalable in a large-scale application with a huge number of sensors in real-time system. In addition, CRC is not needed in our proposed protocol, but the numbers of hashing, pseudorandom, and XOR are more than other protocols.

Offline authentication is to authenticate sensors with an offline reader without connecting to a backend database. The proposed protocol [26] is specially designed for offline authentication; meanwhile, the protocol [24] based on a database in a backend server and the proposed protocol based on the EHT in the cloud cannot work in offline scenarios.

The developments of pervasive computing and mobile networking, however, make offline scenarios less and less. Pervasive authentication will allow reader authenticates sensors wherever and whenever the reader is and the users login the sensing system with constant user names. The proposed protocol that utilizes cloud computing is unrelated to the user’s reader. It is only related to the user’s identity (RID); therefore, it is ubiquitous. The protocol, like most backend-server-based protocols, depends on private intranet connections to the database [26]. Lacking of mobility makes the backend-server-based protocols unsuitable to the requirement of pervasive authentication. The protocol replaces the backend database with an AL downloaded into a specific reader [26]. It is not allowed that a legal user uses another reader’s device to identify sensors if the original reader storing the AL is missing. It indicates that the server-less authentication is not ubiquitous too.

According to the above comparisons, we evaluate the proposed cloud-based adaptive sensing authentication scheme as follows. Compared to the classical authentication schemes, the proposed scheme’s advantages lie in the following: (1) the pay-on demand resource deployment greatly meets the requirements of large enterprises; it is cost-efficient; (2) the cloud-based adaptive sensing authentication is offered as a pervasive and customized service unrelated to device, location, or time; (3) the proposed protocol is about cloud as owner. However, the proposed scheme has higher requirements for application conditions than the traditional

| Authentication protocols | Search complexity | Number of hashing processes | Pseudorandom number generation | Number of XOR | CRC | Number of encryption and decryption processes |
|--------------------------|-------------------|----------------------------|------------------------------|---------------|-----|-----------------------------------------------|
| Chien protocol           | $O(N)$            | 0                          | 2                            | 3             | Yes | 0                                             |
| Tan protocol             | $O(N)$            | 1                          | 0                            | 0             | No  | 0                                             |
| Proposed protocol        | $O(1)$            | 6                          | 3                            | 7             | No  | 2                                             |

Table 3: Calculated comparison.
schemes. Cloud is required to support symmetric encryption algorithm like AES or DES. The requirement is higher than other protocols, but it is easy to achieve in cloud [30].

5. Conclusions

In this paper, a novel authentication protocol is proposed and used properly in cloud-based adaptive sensor private property protection system. The reader reads sensors and uploads the collected data to the cloud for further processing in real time. The cloud will give alert with a simple LED warning device if the sensor works abnormally; it will present alarm information to the administrator to make protective measures quickly as long as the system does not work properly and then decrypts data to determine abnormal adaptive sensor, the staff immediately open the antitheft door to ensure the security of customers’ property. The cloud is employed in the new property protection protocol; this is an innovation but also a challenge. Private property should be protected from being known by others, so the SID and the RID must appear in encrypted form; in this way, privacy of the SID and the RID can be protected. There is no need to worry about leakage of information to the cloud. In the protocol, many valuable advantages are available, such as the authentication between sensors and readers being mutual and having the ability to resist synchronized attack. Because data storage and query and data encryption and decryption are performed in the cloud, the system does not support offline authentication. Accurate index \( H(R \parallel S \parallel N) \) is used for searching in cloud; data can be obtained without the need of traversing the entire hashing table, so computational complexity is \( O(1) \), which means when the number of users is large, the scalability of the system is better than current authentication protocol.

The key points of our work in the future are as follows: (1) designing a lightweight authentication protocol; (2) stating how to protect the system from attacking caused by malicious cloud and malicious sensor in a perfect way; (3) proving the safety of the authentication protocol.

Notations

- \( \text{RID, R:} \) Denotes the identity of an adaptive sensing reader
- \( \text{SID, S:} \) Denotes the identity of an adaptive sensor
- \( \text{NUM, N:} \) Numbers of authentication sessions between a reader and an adaptive sensor, which starts from zero
- \( \text{M:} \) Denotes the last number of sessions (the maximum NUM) between a reader and an adaptive sensor
- \( \text{Data:} \) Denotes any data relevant to a session about the user, the reader, and the adaptive sensor
- \( N_c: \) Denotes a random number generated by cloud
- \( \text{PRNG():} \) Denotes the PRNG (pseudorandom noise generation) function
- \( H(): \) Denotes a secure one-way hash function
- \( E(): \) Denotes an encryption function by using a symmetric algorithm
- \( D(): \) Denotes an decryption function by using a symmetric algorithm
- \( \oplus: \) Denotes the bitwise XOR operation
- \( \|: \) Denotes the concatenation operation
- \( \text{Flag:} \) Denotes the last session success or failure.

Conflict of Interests

The authors declare that they have no conflict of interests.

Acknowledgments

This work has been financially supported by the National Natural Science Foundation of China (no. 61303216 and no. 61373172), the China Postdoctoral Science Foundation funded project (no. 2013M542328), and the National 111 Program of China B08038.

References

[1] Z. Zhu, A. M.-C. So, and Y. Ye, “Universal rigidity: towards accurate and efficient localization of wireless networks,” in Proceedings of the IEEE INFOCOM, pp. 1–9, San Diego, Calif, USA, March 2010.
[2] K. Fan, Y. Gong, C. Liang, H. Li, and Y. Yang, “Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G,” Security and Communication Networks, 2015.
[3] S. He, X. Li, J. Chen, P. Cheng, Y. Sun, and D. Simplot-Ryl, “EMD: energy-efficient p2p message dissemination in delay-tolerant wireless sensor and actor networks,” IEEE Journal on Selected Areas in Communications, vol. 31, no. 9, pp. 75–84, 2013.
[4] Y. M. Huang, M. Y. Hsieh, H. C. Chao, S. H. Hung, and J. H. Park, “Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks,” IEEE Journal on Selected Areas in Communications, vol. 27, no. 4, pp. 400–411, 2009.
[5] J. Chen, J. Li, and T. H. Lai, “Energy-efficient intrusion detection with a barrier of probabilistic sensors: global and local,” IEEE Transactions on Wireless Communications, vol. 12, no. 9, pp. 4742–4755, 2013.
[6] M. Dong, T. Kimata, K. Sugiuira, and K. Zettsu, “Quality-of-experience (QoE) in emerging mobile social networks,” IEICE Transactions on Information and Systems, vol. 97, no. 10, pp. 2606–2612, 2014.
[7] C.-L. Fok, G.-C. Roman, and C. Lu, “Agilla: a mobile agent middleware for self-adaptive wireless sensor networks,” ACM Transactions on Autonomous and Adaptive Systems, vol. 4, no. 3, article 16, 2009.
[8] S. He, X. Gong, J. Zhang, J. Chen, and Y. Sun, “Curve-based deployment for barrier coverage in wireless sensor networks,” IEEE Transactions on Wireless Communications, vol. 13, no. 2, pp. 724–735, 2014.
[9] S. He, J. Chen, F. Jiang, D. K. Y. Yau, G. Xing, and Y. Sun, “Energy provisioning in wireless rechargeable sensor networks,” IEEE Transactions on Mobile Computing, vol. 12, no. 10, pp. 1931–1942, 2013.
[10] P. L. Shrestha, M. Hempel, S. M. Rakshit, Y. Qian, and H. Sharif, “Analysis of energy usage in adaptive sensor networks,” in Proceedings of the IEEE 79th IEEE Vehicular Technology Conference (VTC ’14), pp. 1–5, IEEE, Seoul, Republic of Korea, May 2014.
[11] L. Gheorghe, R. Rughinis, and N. Tapus, “Adaptive security framework for wireless sensor networks,” in Proceedings of the 4th International Conference on Intelligent Networking and Collaborative Systems (INCoS ’12), pp. 636–641, Bucharest, Romania, September 2012.
[12] D.-T. Tran and S. J. Hong, “RFID anti-counterfeiting for retailing systems,” Journal of Applied Mathematics and Physics, vol. 3, no. 1, pp. 1–9, 2015.
[13] R. Paoli, F. J. Fernández-Luque, G. Doménech, F. Martinez, J. Zapata, and R. Ruiz, “A system for ubiquitous fall monitoring at home via a wireless sensor network and a wearable mote,” Expert Systems with Applications, vol. 39, no. 5, pp. 5566–5575, 2012.
[14] M. Dong, H. Li, K. Ota, L. T. Yang, and H. Zhu, “Multicloud-based evacuation services for emergency management,” IEEE Cloud Computing, vol. 1, no. 4, pp. 50–59, 2014.
[15] Z. Wei, Y. Zhang, and J. Yang, “Private assets protection system based on RFID and cloud computing,” in Proceedings of the International Conference on Electronics, Communications and Networks (CECNet ’13), pp. 196–198, Xiaming, China, November 2013.
[16] W. Liu, “Research on cloud computing security problem and strategy,” in Proceedings of the 2nd International Conference on Consumer Electronics, Communications and Networks, pp. 1216–1219, Yichang, China, April 2012.
[17] S. He, J. Chen, X. Li, X. S. Shen, and Y. Sun, “Mobility and intruder prior information improving the barrier coverage of sparse sensor networks,” IEEE Transactions on Mobile Computing, vol. 13, no. 6, pp. 1268–1282, 2014.
[18] G. Anastasi, M. Conti, M. Di Francesco, and A. Passarella, “Energy conservation in wireless sensor networks: a survey,” Ad Hoc Networks, vol. 7, no. 3, pp. 537–568, 2009.
[19] L. Yang, P. Yu, W. Bailing et al., “Hash-based RFID mutual authentication protocol,” International Journal of Security & Its Applications, vol. 7, no. 3, pp. 183–194, 2013.
[20] M. Dong, X. Liu, Z. Qian, A. Liu, and T. Wang, “QoE-ensured price competition model for emerging mobile networks,” IEEE Wireless Communications, vol. 22, no. 4, pp. 50–57, 2015.
[21] W. Xie, L. Xie, C. Zhang, Q. Zhang, and C. Tang, “Cloud-based RFID authentication,” in Proceedings of the IEEE International Conference on RFID (RFID ’13), pp. 168–175, IEEE, Penang, Malaysia, May 2013.
[22] K. Fan, J. Li, H. Li, X. Liang, X. S. Shen, and Y. Yang, “RSEL: revocable secure efficient lightweight RFID authentication scheme,” Concurrency and Computation: Practice and Experience, vol. 26, no. 5, pp. 1084–1096, 2014.
[23] H. Lim, J.-H. Kang, M.-G. Lee et al., “The design of multi-hop routing with asset monitoring application using wireless sensor networks,” in Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, vol. 2, pp. 256–261, IEEE, Taichung, Taiwan, June 2006.
[24] H.-Y. Chien and C.-H. Chen, “Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards,” Computer Standards and Interfaces, vol. 29, no. 2, pp. 254–259, 2007.
[25] D. G. Padmavathi and M. Shanmugapriya, “A survey of attacks, security mechanisms and challenges in wireless sensor networks,” International Journal of Computer Science and Information Security, vol. 4, no. 1-2, pp. 1–9, 2009.
[26] C. C. Tan, B. Sheng, and Q. Li, “Secure and serverless RFID authentication and search protocols,” IEEE Transactions on Wireless Communications, vol. 7, no. 4, pp. 1400–1407, 2008.
[27] Y. Yu, K. Li, W. Zhou, and P. Li, “Trust mechanisms in wireless sensor networks: attack analysis and countermeasures,” Journal of Network and Computer Applications, vol. 35, no. 3, pp. 867–880, 2012.
[28] K. Pelechiris, M. Iliofotou, and S. V. Krishnamurthy, “Denial of service attacks in wireless networks: the case of jammers,” IEEE Communications Surveys & Tutorials, vol. 13, no. 2, pp. 245–257, 2011.
[29] S. Zihao and L. Shufen, “Security threats and security policy in wireless sensor networks,” Advances in Information Sciences and Service Sciences, vol. 4, no. 10, pp. 166–173, 2012.
[30] G. Han, J. Jiang, L. Shu, J. Niu, and H.-C. Chao, “Management and applications of trust in wireless sensor networks: a survey,” Journal of Computer and System Sciences, vol. 80, no. 3, pp. 602–617, 2014.