Hindawi
Journal of Electrical and Computer Engineering
Volume 2017, Article ID 1360289, 11 pages
https://doi.org/10.1155/2017/1360289

Research Article

Health Monitoring System for Nursing Homes with Lightweight Security and Privacy Protection

Yu'e Jiang[1,2] and Jiaxiang Liu[2]

[1]*School of Computer and Information and the University Key Laboratory of Intelligent Perception and Computing of Anhui Province, Anqing Normal University, Anqing 246011, China*
[2]*School of Computer and Information, Anqing Normal University, Anqing 246011, China*

Correspondence should be addressed to Yu'e Jiang; wsxiaoe@163.com

Received 9 November 2016; Revised 21 December 2016; Accepted 23 January 2017; Published 7 March 2017

Academic Editor: Liangmin Wang

With the rapid growth of aged population in China, it is urgent to design a safe and effective monitoring system for the nursing homes. An optimized scheme and high performance security and privacy protection for monitoring system have already become the focus studied especially. So this paper proposed a health monitoring system with lightweight security and privacy protection for nursing homes. Dual-band RFID, virtual routing location algorithm, and diet and exercise data collection based on RFID were adopted to obtain the location and health information. And that fused a mobile authentication protocol based on Hash function to realize security access and privacy protection, which can improve security and reduce the complexity of calculation and the implementation cost compared with the typical authentication protocols. The experiment results show that the ratio of relative network delay is below 35%. The system has strong real-time, high security, more comprehensive data, and lower cost of computation and communication. It can satisfy the requirements of health monitoring for nursing homes.

1. Introduction

It is estimated that China will enter the aging society. How to provide more comprehensive pension services becomes more and more urgent. As families and community can only provide limited elderly services, a tendency to meet the rocketing demands is to promote healthy monitoring system for nursing homes. As environment in nursing homes is complex, managers cannot focus on every one of the elderly people. So the challenge is to provide location service and health service in the event of dangerous conditions [1–5]. With the rapid development of monitoring technology, RFID get more attention due to its advantage, such as unique identification, moveable identification, multitargets identification, and good environmental adaptability. In a word, a safe and effective monitoring system based on RFID for the nursing homes will be required urgently.

Existing monitoring systems based on RFID usually lack an optimized scheme of data collection and privacy protection. For example, in the aspect of data collection, some are operating in a single frequency band, transmitting collection-data via line, even short of effective location algorithm and health data collection. As we known, there are obvious disadvantages in wireline monitoring system, such as routing restriction, the lack of flexibility, and high-cost. In terms of operation of frequency, RFID systems can be divided into four categories: low frequency (LF), high frequency (HF), ultra-frequency (UHF), and microwave, which have different properties. Due to low power, strong penetrating in RFID LF system, moveable identification, and multitargets identification in other RFID systems, how to realize the combination of the two advantages is a worthy topic [6–10]. Findings indicated that healthy diet and sufficient and regular exercises not only contribute to reduce and resist chronic diseases, but also promote physical and psychological health of elderly people. So to establish a system that can gather diet and exercise information and do some

statistical analysis for residents in nursing homes is of great signification. Manual entry and a survey are applied for data collection in traditional method, which still have some problems and drawbacks: low-efficiency, poor data quality, and less data quantity [11–14]. In another aspect of privacy protection, security and privacy threats exist in the monitoring system for nursing homes based on RFID, in which personal information, recording information in daily life, and personal property information are prone to attacks such as replay attacks, counterfeit attacks, and tracking attacks. It is urgent to establish policies and standards for avoiding security issues, especially the encryption algorithm based on Hash function. Presently, there are Hash-Lock protocol, Randomized Hash-Lock protocol, and Hash-Chain protocol. However these have some flaws and fail to solve the security problems [15–20].

This paper adopts a RFID system with dual-band, in which low frequency is used to activate the passive tag and the HF is used for communicating. A simple algorithm named virtual routing location algorithm is introduced to realize area location. It effectively uses RFID and ZigBee technology to establish an expanded RFID wireless network for collecting location data. A method of diet and exercise data acquirement based on RFID technology is also proposed later. At the same time, the system effectively integrates a lightweight RFID authentication protocol based on Hash function to achieve secure access and privacy protection. This protocol is effective against counterfeiting, tracking, and replay attacks and realizes the interaction between tag, reader, and back-end server. These works show that the new system overcomes the security leaks and has the merits of an optimized scheme of data collection, low communication and computation complexity, and so on.

The rest of this paper can be outlined as follows. Section 2 describes the architecture of the system, along with main modules, which is divided into vertical and horizontal aspects: function module and security and privacy protection module. Section 3 discusses the key technology in the function module, such as area location and data collection based on RFID. Section 4 designs a kind of lightweight RFID authentication protocol based on Hash function from the vertical aspect. Section 5 sets up experimentation environment and the network latency is tested, along with related work. Finally, in Section 6 we summarize our discussion.

2. System Description

The section mainly focuses on two aspects as follows: on the one hand, the architecture of this system is proposed, and the frequency selectivity of the RFID system, workflow, and communication mode are described in detail. On the other hand, the more detailed function requirements are analyzed from vertical and horizontal aspects. In the vertical aspect, the system is divided into monitoring subsystem and service subsystem. Security and privacy are discussed from the horizontal aspect. Security mode is embedded into every subsystem, such that a unified secure design makes sure that the monitoring system runs well.

2.1. Architecture. This system conforms to the IOT concept, which contains three layers, the perceptual layer, the network layer, and the application layer [3, 7]. The perceptual layer is at the most front-end of information collection and includes location nodes, other data collection nodes, sticking tags, and RFID wristbands. Then the information collected is uploaded to the back-end serve by ZigBee network with tree topology in the network layer. Finally, the system uses .NET+MYSQL technologies to realize the development of the whole system, including monitoring subsystem, service subsystem, and web service. Its design architecture is shown in Figure 1.

According to different requirements, we choose two kinds of nodes for data collection. Location node is designed to collect the location information, and the collection node is for another data collection. Each node communicates with CC2530 module by RS485 bus. Then ZigBee network formed by CC2530 modules will transmit the whole data to the back-end server.

Every location node and RFID wristbands work together in two phases: activation phase and communication phase. 125 KHz band is selected to activate passive part in a RFID wristband, and 433 MHz band is for communication between one node and the active part of a wristband. Compared with a single frequency band, the Dual-band RFID system combines the advantage of low frequency and high frequency effectively: low power and strong penetrating in LF system, moveable identification, and multitargets identification in HF system. According to the structure of antenna in a location node, it can also be divided into single-channel mode and dual-channel mode, which suit for different areas to be located. Every collection node mainly communicates with sticking tags, which follows the EPC standards. Desktop RFID reader with 433 MHz frequency band is selected for collection node to collect diet data, part of exercise data, and other service data.

In the system, tags or wristbands, any one of RFID reader, and back-end service are connected with each other by wireless network: RFID or ZigBee. This quite suits the monitoring system, but it also brings a problem. The wireless channel is prone to attacks such as replay attack, counterfeit attack, and tracking attack. So security and privacy should be paid adequate attention.

2.2. Function Module. The monitoring system mainly contains monitoring subsystem and service subsystem according to the actual function from the vertical aspect. Each subsystem combines with RFID wristbands to realize all-around automatically monitoring management. Security and privacy are designed to resist attacks from the horizontal aspect. The detailed functions are shown in Figure 2.

Monitoring subsystem offers a safe and secure environment for the nursing homes residents. All residents in the nursing homes wear RFID wristbands that can help the staff monitor their locations. So, when dangers occur, the staff can quickly locate and provide appropriate help [5–7]. The specific function is analyzed as follows.

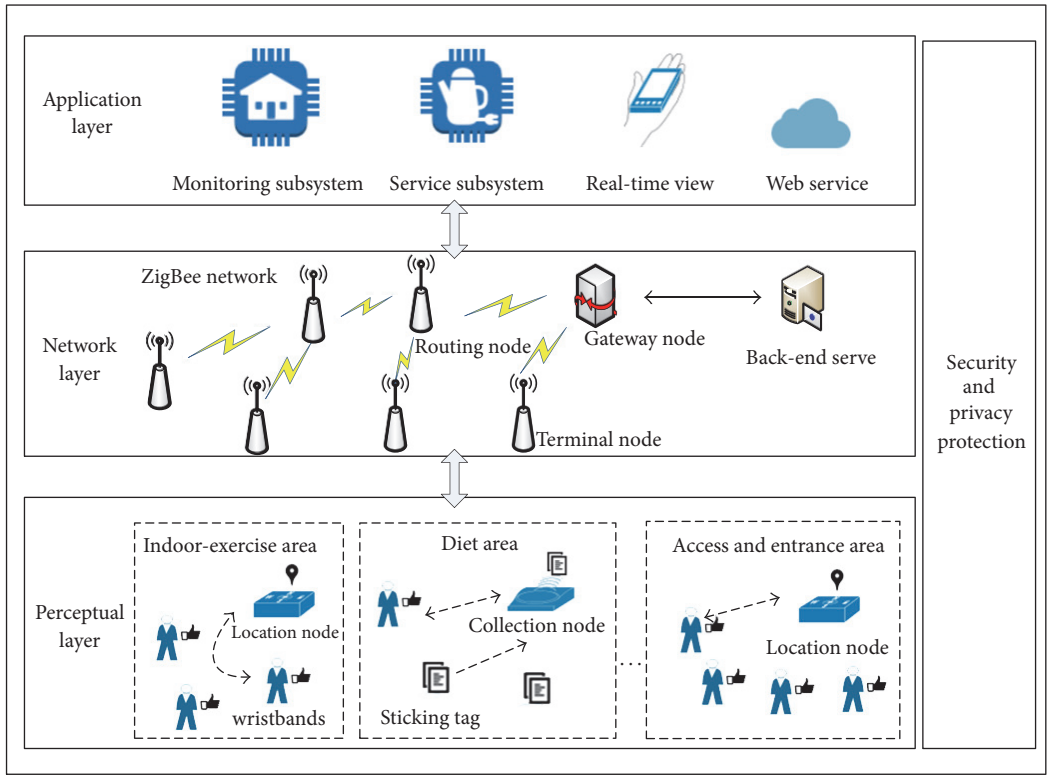


Figure 1: The overall architecture.

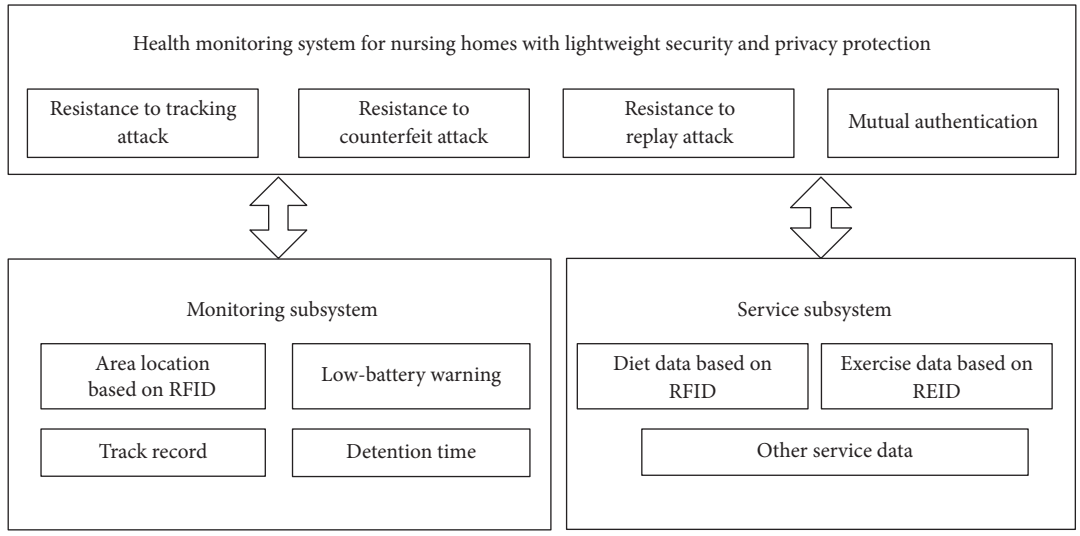


Figure 2: Function diagram.

(1) Area location: this module is mainly used for location Query for the residents wearing RFID wristbands. Or use the module to achieve a certain period of time statistics.

(2) Low-battery warning: the module can monitor the consuming situation of battery for the RFID wristbands. A warning signal is transmitted to the staff when the battery capacity is below the threshold.

(3) Detection time: calculate the detection time in some dangerous and privacy areas, such as bathrooms and toilets. For example, a resident wearing a RFID wristband stays in these areas longer than normal; it is very likely that an emergency has happened.

(4) Track record: record the daily activities of the residents wearing the RFID wristbands, and then provide the information for health assessment or other requirements.

Service subsystem is designed to offer health service and others and collect diet and exercise data which partly reflects the health of residents in the nursing homes. Concrete analysis is as follows.

(1) Diet data based on RFID: the diet data for every resident in the nursing homes are collected by the collection node, tricking tags, and RFID wristband. The back-end serve will record the data and compare with the standard.

(2) Exercise data based on RFID: the exercise data comes from three kinds of activities: the usage of athletic facilities, the usage of indoor recreational area, and outdoor-activities. All the exercise data and diet data are supported to help professionals to access health status for every resident in nursing homes.

(3) Other service data: the module is for other data services: querying relational information for every resident, sending blessing on holiday, reminding the resident to take medicine, and so on.

Security and privacy are designed to defend all the subsystems from threats. It can be detailed as follows.

(1) Resistance to Counterfeit Attacks. It prevents attackers from counterfeit RFID tags or readers, illegal access to personal information of the resident, guardian information and sensitive data, and so on.

(2) Resistance to Tracking Attacks. It prevents attackers from gaining traces of activity by tracking location information, threatening their person and property.

(3) Resistance to Replay Attacks. In an extreme case, the attacker may obtain relevant information. It prevents it from being reproduced by using this information, thereby illegally passing the authentication

(4) Mutual Authentication. It aims to achieve the tag, reader, and the back-end server mutual authentication between the three.

Security design will be embedded above the various subfunctional modules and unified security design to ensure that all functional modules are safe. The next step will be a detailed analysis of key technologies and the authentication protocol in the security module.

3. Key Technologies

As mentioned, the system is divided into monitoring subsystem and service subsystem from the vertical aspect. The area location module is very important and supports the other modules. And that diet data and exercise data are the important parts of service subsystem. So in this section we will focus on the key technologies on these modules: area location, diet data, and exercise data collection.

3.1. Area Location Based on RFID. According to the structure characteristics of the monitoring area in nursing homes, it can be divided into different areas, such as indoor gymnasium area, diet area, indoor-recreation area, and access and entrance area. The system is designed to provide a more flexible, easily configurable deployment model. So we can deploy the location node according to actual size of areas to be monitored and other requirements. The actual physical location is known when the location node has been deployed. In this section we will talk about the process of data acquisition of one location node and the location algorithm.

The location nodes mainly work together with RFID wristbands; then the workflow of one single location node and RFID wristband is shown in Figure 3.

The process of data acquisition consists of two phases: namely, activate phase and communication phase. In the trigger phase, the location node sets control parameters and initiates readers at first. Then the RFID reader (location node) will scan RFID tags (RFID wristbands) in its coverage area. Finally, when the searched tag ID matches the ID stored in memory, the communication can begin. In the communication phase, the RFID reader starts to receive data after authenticating successfully. If the data is a distress signal or warning signal, then give priority to transmit; otherwise transmit the location data in the order queue.

The location data mainly contains location array, which comes from the virtual routing location algorithm. In the following parts, we will simply describe the basic concepts about the algorithm. The algorithm uses ZigBee and RFID technology to form the RFID wireless network; the coverage is far away. As we known, the read-write distance of RFID reader is relatively close. So we assume that the tag to be located has the same physical location with the RFID reader. As the resident wearing RFID wristband moves in the RFID wireless network, the wristband will transmit a location array to back-end server. The principle of the algorithm is shown in Figure 4.

Assuming that the coordinates of all readers are already known, then the coordinate of the tag can be gotten by the algorithm. As shown in Figure 4, the solid line is the actual route the tag selected and the dotted line is the virtual route, which is calculated by the algorithm. For example, the actual route of the tag can be the same as the virtual route as shown below:

$$(0,0) \longrightarrow (1,1) \longrightarrow (1,2) \longrightarrow (1,3) \longrightarrow (1,4) \longrightarrow (2,4) \longrightarrow (3,3) \longrightarrow (4,2) \longrightarrow (3,1) \longrightarrow (3,0) \quad (1)$$

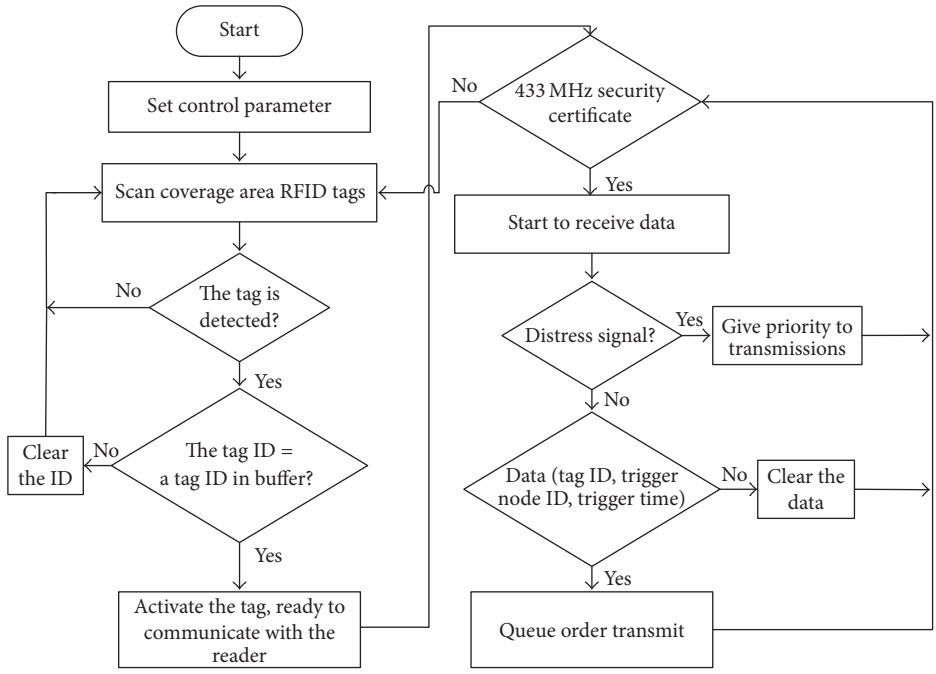


Figure 3: Workflow for one location node.

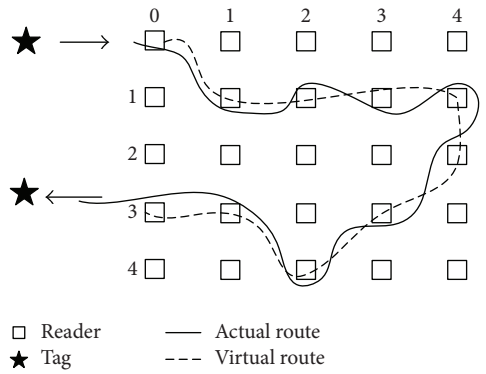


Figure 4: Schematic diagram of the algorithm.

A location array is chosen to realize the progress of the algorithm. It contains three parameters: the ID of the tag, the reading time, and the ID of the reader. The following formula can be used.

$$\left\langle T_i, t_j, R_k \right\rangle = \left\langle \text{tag } j, \text{time } j, \text{reader } k \right\rangle. \quad (2)$$

As shown is formula (2), the location array is expressed by $\langle T_i, t_j, R_k \rangle$; T_i is the ID of the ith tag. R_k is the ID of the kth reader. And t_j is the time when the kth RFID reader starts to communicate with the ith tag. Location arrays are firstly categorized according to T_i and then according to t_j. Finally, we can get the coordinate of kth RFID reader as the coordinate of ith tag at the time of t_j. The algorithm is simple and effective, fully in line with the needs of area location for the nursing homes.

3.2. Health Data Based on RFID. In this section we will build a module to collect diet and exercise data automatically based on RFID and do some statistical analysis. Diet and exercise data is usually very complex, but there still has certain regularity and periodicity for collective life environment in nursing homes. Based on this application background, a simplified model for diet and exercise data collection is designed as follows.

Diet area is divided into selection-area and settlement-area. In selection-area, plates and bowls sticking with tags establish the one-to-one relationship between each tag and the food in its plate or bowl. The settlement-area mainly contains RFID readers and displays. With the help of sticking tags, RFID readers, and wristbands, the subsystem can realize settlement and diet data collection quickly and automatically. Next, we will introduce the progress of data analysis in the

Table 1: Exercise data based on RFID.

Categories	Indoor-entertainment	Outdoor-activities	Athletic facilities
Methods	Accumulate the continuous time by indoor-RFID readers	Accumulate the continuous time by entrance-RFID readers	Accumulate the exercise time on athletic facilities by RFID readers
Time (hours/day)	T_1	T_2	T_3
The weight	w_1	w_2	w_3

back-end server. Five categories of the essential nutrients in body are chosen as the main parameters to analyze, which are proteins, fats, carbohydrates and trace elements, vitamins, and minerals. Based on a nutrient criterion proposed by China and the special requirements for the elderly, a daily meal nutrition supplement standards are designed. Compared with the standards, the system will judge whether the daily diet is reasonable and then put forward some suggestions. Finally, a mathematical model is built to detail the progress. Let the amount of common food in nursing homes as i. k take 1 to 5, respectively, as protein, fat, vitamins, energy, minerals, and inorganic salts. a_{ki} is the value of kth nutrient in ith food, and $\{a_{ik}\} \in A$; u_{ik} is the value of daily intake of kth nutrient in ith food, and $\{u_{ik}\} \in B$. $u_{ik} = 1$; the formula indicates that the kth nutrient contained in the ith food is ingested. The daily intake of nutrients is shown in formula (3).

$$Y = A * U = \begin{pmatrix} a_{11} & \cdots & a_{1i} \\ \vdots & \ddots & \vdots \\ a_{k1} & \cdots & a_{ki} \end{pmatrix} \begin{pmatrix} u_{11} & \cdots & u_{1k} \\ \vdots & \ddots & \vdots \\ u_{i1} & \cdots & u_{ik} \end{pmatrix} = \begin{pmatrix} y_{11} & \cdots & y_{1i} \\ \vdots & \ddots & \vdots \\ y_{k1} & \cdots & y_{ki} \end{pmatrix}. \quad (3)$$

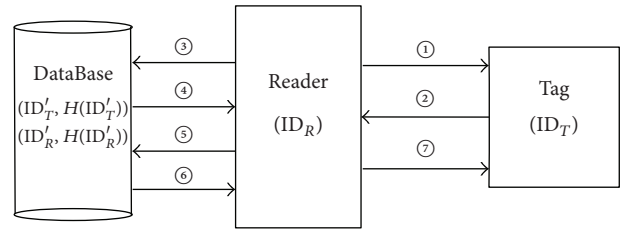
Y is the daily intake of nutrients, y_{ki} express the kth nutrient intake from the ith food. Add the elements in the same column for array Y, and get a new array $V = (v_1, v_2, \ldots, v_k)$; v_k is the kth nutrient you has been absorbed. $M = (m_1, m_2, \ldots, m_k)$ is the standard value of nutrients. Comparing the V with M, a result that whether you get the sufficient nutrients or not will be offered to the residents and staff.

The system classifies exercises as indoor-entertainment, outdoor-activities, and exercise on athletic facilities. Formula (4) as below is used to calculate the amount of exercises daily simplify.

$$S = \sum_{i=1}^{n} (T_i * w_i). \quad (4)$$

As shown in formula (4), $n = 3$, $i = \{1, 2, 3\}$ represent indoor-entertainment, outdoor-activities, and exercise on athletic facilities, respectively. w_i is the weight value of the amount of the whole exercises. The sum amount of ith exercises daily is T_i, and the sum of all kinds of exercise is calculated by formula (4), noted by S. The specific progress of calculation is shown in Table 1.

According to the health status of the elderly and special needs, daily exercise standards are designed when the elderly checked in the nursing home. And the standard for comparison, to determine the amount of the daily exercise, is appropriate or not.



① Reader ⟶ Tag: Query, r_R
② Tag ⟶ DataBase: M_1, M_2, M_3, r_T
③ Reader ⟶ DataBase: Query
④ DataBase ⟶ Reader: r_D
⑤ Reader ⟶ DataBase: M_2, M_3, M_4, r_T, r_R
⑥ DataBase ⟶ Reader: M'_3, M'_4
⑦ Reader ⟶ Tag: M'_3

Figure 5: The authentication flow of the protocol.

4. Security and Privacy

As before, security and privacy are very important for the wireless system, and security mode is embedded into every subsystem. So a mobile authentication protocol based on Hash function is designed in this section. The procedure and implementation of the protocol are discussed as follows.

4.1. Proposed Protocol. Based on a one-way Hash function, this paper proposed a mutual authentication for information protection. It is depicted in Figure 5. The symbols in the protocol are described as follows: $H(x)$ is the Hash function of x. ID_T is the identification number of the tag and is stored in the tag. ID_R is the identification number of the RFID reader and is stored in the reader. $(ID'_R, H(ID'_R))$ and $(ID'_T, H(ID'_T))$ are stored in the DataBase. The authentication flow of the protocol is shown in Figure 5.

(1) The RFID reader generates a random number r_R and sends $(Query, r_R)$ to the tag.

Table 2: Protocol performance analysis.

Performance actor	Hash-Lock	Radom Hash-Lock	Hash-Chain	The proposed protocol
Computational complexity				
Tag	$1H$	$1H + 1R$	$2H$	$3H + 1R$
Reader	—	$(\sum(n/2))\,H$	—	$4H + 1R$
DataBase	—	—	$(\sum(n/2))\,H$	$4H + 1R$
Security performance				
Resistance to counterfeiting attacks	×	×	×	√
Resistance to tracking attacks	×	×	√	√
Resistance to replay attacks	×	×	×	√
Two-way authentication	×	×	√	√

(2) The tag receives the data, generates a random number r_T, and then uses the received number and calculates $M_1 = H(r_R \parallel r_T)$, $M_2 = H(\mathrm{ID}_T) \oplus M_1$, and $M_3 = H(\mathrm{ID}_T \parallel r_R \parallel r_T)$. M_3 is stored in the tag and (M_1, M_2, M_3, r_T) are sent to the reader.

(3) Using the received random number r_T and its generated random number r_R, the reader calculates $M_1' = H(r_R \parallel r_T)$. Then it makes a judge whether M_1' is equal to the received variable M_1. if $M_1' = M_1$, the tag is authenticated. And then Query is sent to the DataBase.

(4) After receiving the Query, the DataBase generates a random number r_D and sends it to the reader.

(5) Using the received r_D and its own numbers r_R and ID_R, the reader calculates the following numbers: $M_4 = H(\mathrm{ID}_R) \oplus H(r_R \parallel r_D)$ and $M_5 = H(\mathrm{ID}_R \parallel r_R \parallel r_D)$. M_5 is stored in the reader and $(M_2, M_3, M_4, r_T, r_R)$ are sent to the DataBase.

(6) When the DataBase receives the data, it will carry on the following three steps. The first step is to authenticate the reader: it calculates $H''(\mathrm{ID}_R) = M_4 \oplus H(r_R \parallel r_D)$ to meet the requirement of $(\mathrm{ID}_R', H(\mathrm{ID}_R'))$, which are stored in the DataBase. And if $H''(\mathrm{ID}_R) = H(\mathrm{ID}_R')$, the reader is authenticated. In the second step, it calculates $H''(\mathrm{ID}_T) = M_2 \oplus H(r_R \parallel r_T)$. If $H''(\mathrm{ID}_T) = H(\mathrm{ID}_T')$, the tag is authenticated. The third step calculates $M_5' = H(\mathrm{ID}_R' \parallel r_D \parallel r_R)$ and $M_3' = H(\mathrm{ID}_T' \parallel r_T \parallel r_R)$ and sends (M_3', M_5') to the reader.

(7) The reader compares the received data M_5' with the data M_5, which is stored earlier. If $M_5' = M_5$, then the reader authenticates the DataBase and sends M_3' to the tag.

(8) The tag receives the data M_3' and compares it to the data M_3 which is stored in tag earlier. If $M_3' = M_3$, then the tag authenticates both the Reader and the DataBase.

4.2. Protocol Performance Analysis. The following will analyze security performances of the proposed protocol from four aspects.

(1) Resistance to Counterfeiting Attacks. The protocol can effectively exploit the one-way of Hash function. The attackers cannot analyze the identification numbers of the tag or the reader by intercepting data. So the system has the ability to resist counterfeiting attacks.

(2) Resistance to Tracking Attacks. The tag, the reader, and the DataBase will generate random numbers; the response data are changing in each certification process. So attackers are unable to obtain location information, thus avoiding tracking attacks.

(3) Resistance to Replay Attacks. The random numbers of the tag, the reader, and the DataBase are changed during each authentication process, so that the previous authentication information cannot be used to complete the replay attacks.

(4) Two-Way Authentication. Firstly, the reader authenticates the tag by judging whether $M_1' = M_1$. Then the DateBase verifies the security of the tag and the reader by the received $(M_2, M_3, M_4, r_T, r_R)$. Finally, the reader authenticates the DataBase by the formula $M_5' = M_5$. And the tag verifies that the formula $M_3' = M_3$ is true and authenticates the Reader and the DataBase.

On the basis of security considerations, the protocol proposed also effectively reduces the calculation of the tag, reducing tag costs and the use of energy consumption, as shown in Table 2. In Table 2, H is the Hash function, R is the random function, n is the total number of tags, and "—" is not Hash function, random function, and so on [18–20].

As shown in Table 2, this authentication protocol fully considers the new problems brought by the wireless transmission of the mobile RFID system compared with the classical protocol. The proposed protocol balances the computational protocol at the tag, the reader, and the DataBase while providing strong security which can resist various types of attacks, obtain dual-authentication, and decrease computational complexity. All these performances make the proposed the system be appropriate for the nursing homes usage.

5. Performance Testing and Related Work

The following will analyze the performance and related work to verify the feasibility and superiority of the system. Firstly,

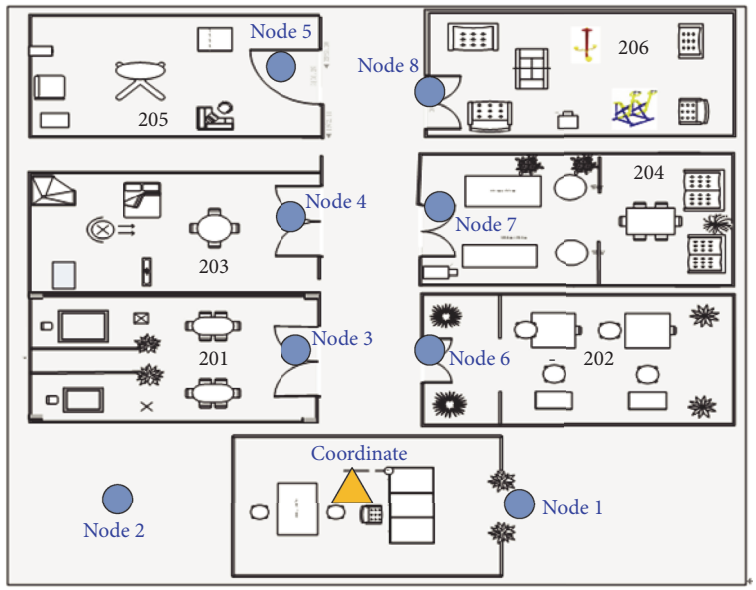


Figure 6: Location nodes layout diagram.

we will build the test environment, testing the system's network delay characteristics and then analyze the related work of the system and compare it with the common monitoring system.

5.1. Performance Testing. Because the indoor layout of the nursing home is similar to the laboratory, we choose the second floor laboratory to carry out system testing. The monitoring rooms are divided into 201 room, 202 room, 203 room, 204 room, 205 room, 206 room, the lobby, and server room, as shown in Figure 6.

As shown in Figure 6, the RFID node 1 and node 2 are located in the lobby area. The node 3 is arranged at the entrance of the room 201. Moreover, node 4 is located at the 203 entrance of the room 203, node 5 at the room 205, node 8 at the room 206, node 7 at the room 204, and node 6 at the room 202. The coordinate node is arranged at the server room and connected with the back-end server. The distance between the location nodes is 6–8 meters, and the nodes that are far away from the server communicate with their nearest nodes as the parent node. We use packet sniffer and hardware timers to test the system. Assume that the data acquisition interval is 5 s and 100 times for each node during the test. The average network delay for each node is shown in Figure 7.

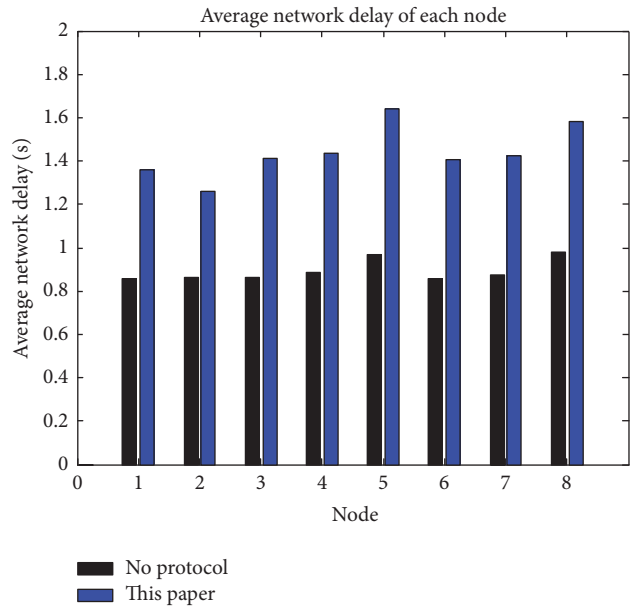


Figure 7: The average network delay of each node.

From Figure 7, we can see that the network latency of nodes 1, 2, 3, and 6 is close to each other. In the network topology, these nodes are single-hop nodes, and the actual physical location is closer to the coordinator node. Node 4 and node 7 are close to each other. In the network topology, they are two-hop nodes. Node 5 and node 8 are three-hop nodes and the network delay is relatively large. Therefore, the system topology design has some impact on the network delay, but overall, adding a security authentication protocol increases the system's average network latency. [19, 20] and the simulation show that the implementation of the protocol time is about 500–550 ms, but many monitoring systems data acquisition time is about 5–60 s. So here 5 s is chosen as the sampling interval; we discuss the relative network latency and the average network delay divided by the sampling interval, as shown in Figure 8.

Figure 8 shows that, compared with the sampling interval, the relative network delay for the proposed system with lightweight security and privacy protocol is less than 35%, so the authentication protocol does not affect the system real-time data collection but can greatly improve system security and privacy.

Table 3: Week of diet data from a tester.

Data/appliance	Week of diet data from a tester				
	Protein (g)	Fat (g)	Vitamins (mg)	Minerals and inorganic salts (mg)	Energy (KJ)
02/10/2016 (Sun)	73.1	23.7	81.32	5828	6307.5
03/10/2016 (Mon)	76.1	45.5	130.75	6273.33	6953.81
04/10/2106 (Tue)	95.2	60.3	86.3	7832.85	7200.67
05/10/2016 (Wed)	107.5	71.8	84.08	7409.73	9790.56
06/10/2016 (Thu)	87.1	45	89.35	6899.35	7284.34
07/10/2016 (Fri)	92.8	63.7	113.55	7541.83	8037.46
08/10/2016 (Sat)	66.1	29.6	46.36	5282.9	5514.51
Mean	85.41	48.51	90.24	6724	7298.4
Reference value	65~75	25	130.5~131.4	6530	7100~9200
Conclusion	High	High	Low	High	Normal

Table 4: Week of exercise data from a tester.

Data/appliance	Week of exercise data from a tester				
	Indoor-entertainment ($w_1 = 0.2$)	Outdoor-activities ($w_2 = 0.35$)	Athletic facilities ($w_3 = 0.45$)	Sum (hour)	Reference value (hour)
02/10/2016 (Sun)	2 hours	0.5 hour	0.3 hour	0.71	0.6~1
03/10/2016 (Mon)	3 hours	0.8 hour	0.2 hour	0.97	
04/10/2106 (Tue)	2.5 hours	1 hour	0.2 hour	0.94	
05/10/2016 (Wed)	4 hours	0.1 hour	0 hours	0.835	
06/10/2016 (Thu)	3.6 hours	0.3 hour	0.3 hour	0.96	
07/10/2016 (Fri)	2.8 hours	0.4 hour	0.1 hour	0.745	
08/10/2016 (Sat)	3.6 hours	0.3 hour	0.3 hour	0.96	

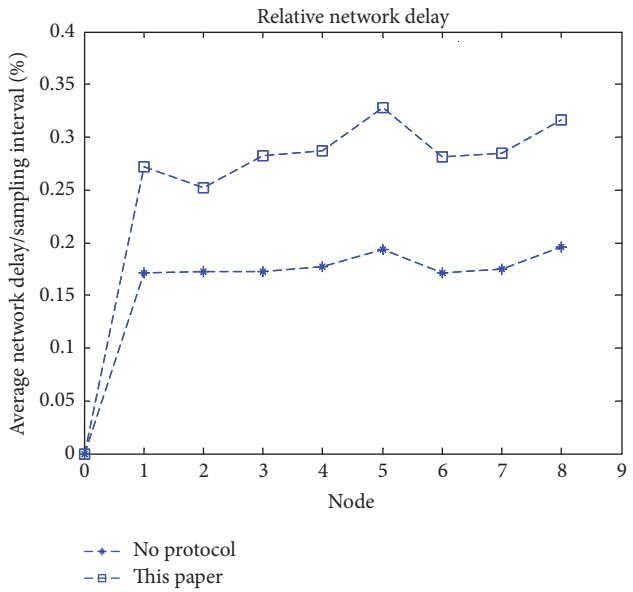


Figure 8: Relative network delay.

In the experimental environment, we collected a week of diet and exercise data from a tester, as shown in Tables 3 and 4.

In Table 3 the reference value comes from daily intake of dietary nutrient values for Chinese residents aged 60 years and over. The nursing home provides a basic diet menu similar to the one provided each week, which facilitates the collection of diet data. In Table 4 the reference value can be adjusted according to the previous exercise and health status. We can see that week of diet and exercise data have certain regularity and periodicity to reflect the elderly's diet and exercise status, which can monitor the health of the elderly.

5.2. Related Work. There are a lot of monitoring systems, but few ones are in line with the needs of nursing homes in all aspects. Reference [21] introduces a remote monitoring system for the tower clusters, which focuses on industrial data transmission and is not suitable for the elderly monitoring. In [22], a remote monitoring system based on intelligent fiber structure is proposed. The system uses the liquid core optical fiber structure based on ARM and GPRS to communicate. The cost is high and cannot be applied to the nursing home monitoring system. References [23, 25] all use video for data acquisition. Reference [23] uses the pyroelectric infrared sensor and the video monitor to carry on the multitarget tracking. But its calculation and communication complexity are high, and the data acquisition is not comprehensive. In [24], a wireless network life-monitoring system for the nursing home is proposed, which uses the wireless sensor

Table 5: Comparison of related system performance.

Monitoring systems	System performance					Main technical shortcomings
	Real-time	Data comprehensiveness	Security and privacy	Computational and communication costs	Suitable for nursing homes	
Reference [21]	Medium	Industrial data	Low	medium	No	Lack of security
Reference [22]	Medium	Industrial data	Low	High	No	Communication costs are high
Reference [23]	High	Location data	Medium	High	Yes	Lack of security Computational costs are high Data are not comprehensive
Reference [24]	Medium	Health data	Low	Low	Yes	Data are not comprehensive
The system proposed	High	Comprehensive data	High	Low	Yes	No

network to collect the basic health data but lacks the consideration of security and privacy protection. Specific analysis and comparison are shown in Table 5.

Compared with the monitoring system shown in Table 5, the system has four characteristics: high real-time monitoring, small network delay; comprehensive data collection, involving location information, diet, and exercise data collection; security and privacy protection mechanism embedded in the module design; the use of lightweight mobile security architecture, computing, and low communication cost.

6. Conclusion

According to the characteristics and needs of the nursing home, this paper designed a health monitoring system with lightweight security and privacy protection, which is focused on vertical and horizontal aspects: health data collection and security and privacy protection. From the vertical aspect, RFID dual-frequency band, virtual route location algorithm, and diet and exercise data acquisition based on RFID are adopted in the health data collection. From the horizontal aspect, a lightweight RFID authentication protocol based on Hash function is embedded into each collection module, which has high security and low computation cost. Through the performance analysis and testing, we can see that the system has characteristics of high security, high real-time, and high data comprehensive and low computational and communication complexity and fully meets the needs of health monitoring system for the nursing homes.

Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was supported in part by Educational Commission of Anhui Province under Grant 2015jyxm237 and in part by the Foundation of University Research and Innovation Platform Team for Intelligent Perception and Computing of Anhui Province.

References

[1] M. H. Y. Shum, V. W. Q. Lou, K. Z. J. He, C. C. H. Chen, and J. Wang, "The 'Leap Forward' in nursing home development in Urban China: future policy directions," *Journal of the American Medical Directors Association*, vol. 16, no. 9, pp. 784–789, 2015.

[2] N. Kumar, K. Kaur, S. C. Misra, and R. Iqbal, "An intelligent RFID-enabled authentication scheme for healthcare applications in vehicular mobile cloud," *Peer-to-Peer Networking and Applications*, vol. 9, no. 5, pp. 824–840, 2016.

[3] N. K. Suryadevara and S. C. Mukhopadhyay, "Wireless sensor network based home monitoring system for wellness determination of elderly," *IEEE Sensors Journal*, vol. 12, no. 6, pp. 1965–1972, 2012.

[4] J. E. Morley, G. Caplan, M. Cesari et al., "International survey of nursing home research priorities," *Journal of the American Medical Directors Association*, vol. 15, no. 5, pp. 309–312, 2014.

[5] J. E. Morley, "Under nutrition: a major problem in nursing homes," *Synthetic Communications*, vol. 44, no. 8, pp. 1019–1042, 2014.

[6] H. Makimura, K. Watanabe, H. Igarashi, and H. Waki, "Monitoring system of railway using passive RFID in UHF band," *IEEJ Transactions on Electronics, Information and Systems*, vol. 132, no. 5, pp. 691–696, 2012.

[7] L. M. Wang and S. M. Xiong, *Introduction to the Internet of Things Engineering*, Tsinghua University Press, Beijing, China, 2011.

[8] J. C. Chen and T. J. Collins, "Creation of a RFID based real time tracking (R-RTT) system for small healthcare clinics," *Journal of Medical Systems*, vol. 36, no. 6, pp. 3851–3860, 2012.

[9] N. Li and B. Becerik-Gerber, "Performance-based evaluation of RFID-based indoor location sensing solutions for the built environment," *Advanced Engineering Informatics*, vol. 25, no. 3, pp. 535–546, 2011.

[10] K. Liu and Z. C. Ji, "Research on RFID reader network tracking algorithm," *Computer Engineering*, vol. 38, no. 18, pp. 248–250, 2012.

[11] M. Arebey, M. A. Hannan, H. Basri, R. A. Begum, and H. Abdullah, "Solid waste monitoring system integration based on RFID, GPS and camera," in *Proceedings of the International Conference on Intelligent and Advanced Systems (ICIAS '10)*, pp. 1–5, June 2010.

[12] Y. Tao, X. Zhou, Y. Ma, and F. Zhao, "Mobile mutual authentication protocol based on hash function," *Journal of Computer Applications*, vol. 36, no. 3, pp. 657–660, 2016.

[13] S.-J. Zhou, W.-Q. Zhang, and J.-Q. Luo, "Survey of privacy of radio frequency identification technology," *Journal of Software*, vol. 26, no. 4, pp. 960–976, 2015.

[14] A. Wickramasinghe, D. C. Ranasinghe, C. Fumeaux, K. D. Hill, and R. Visvanathan, "Sequence learning with passive RFID sensors for real time bed-egress recognition in older people," *IEEE Journal of Biomedical and Health Informatics*, p. 1, 2016.

[15] B. Fabian, T. Ermakova, and C. Muller, "SHARDIS: a privacy-enhanced discovery service for RFID-based product information," *IEEE Transactions on Industrial Informatics*, vol. 8, no. 3, pp. 707–718, 2012.

[16] X. L. Liu, H. Qi, Q. K. Li et al., "Efficient detection of cloned attacks for large-scale RFID systems," in *Algorithms and Architectures for Parallel Processing*, vol. 8630 of *Lecture Notes in Computer Science*, pp. 85–99, Springer International Publishing, Berlin, Germany, 2014.

[17] A. Arbit, Y. Oren, and A. Wool, "A secure supply-chain RFID system that respects your privacy," *IEEE Pervasive Computing*, vol. 13, no. 2, pp. 52–60, 2014.

[18] H. Jannati and B. Bahrak, "Security analysis of an RFID tag search protocol," *Information Processing Letters*, vol. 116, no. 10, pp. 618–622, 2016.

[19] X. Y. Wang, F. X. Jing, and Y. Q. Wang, "An improved hash-based RFID security authentication algorithm," *Journal of Shangdong University*, vol. 49, no. 9, pp. 154–159, 2014.

[20] D.-Z. Sun and J.-D. Zhong, "A hash-based RFID security protocol for strong privacy protection," *IEEE Transactions on Consumer Electronics*, vol. 58, no. 4, pp. 1246–1252, 2012.

[21] H. M. Zheng, Y. J. Wang, K. Chen, and J. T. Zhang, "Design of wireless remote security monitoring system for tower crane fleet," *Journal of Electronic Measurement and Instrumentation*, vol. 28, no. 5, pp. 520–527, 2014.

[22] L. Shen, Z. Zhao, and X. Yu, "Design of remote monitoring internet of things system for new optical fiber smart structure," *Journal of Nanjing University of Aeronautics and Astronautics*, vol. 3, no. 47, pp. 453–458, 2015.

[23] F.-M. Li, N. Jiang, J. Xiong, and J.-Y. Zhang, "Multi-object tracking scheme with pyroelectric infrared sensor and video camera coordination," *Acta Electronica Sinica*, vol. 42, no. 4, pp. 672–678, 2014.

[24] Y.-J. Chang, C.-H. Chen, L.-F. Lin, R.-P. Han, W.-T. Huang, and G.-C. Lee, "Wireless sensor networks for vital signs monitoring: application in a nursing home," *International Journal of Distributed Sensor Networks*, vol. 2012, Article ID 685107, 12 pages, 2012.

[25] G.-X. Han and C.-R. Li, "Improvement on moving object tracking method for network video surveillance," *Journal on Communications*, vol. 35, pp. 160–164, 2014.