Personal and Ubiquitous Computing (2019) 23:583–594
https://doi.org/10.1007/s00779-019-01215-2

ORIGINAL ARTICLE

Research on reliability of Internet of Things RFID based on improved random hash protocol and cooperative game in low-carbon supply chain environment

Lijian Yu[1] · Yih-Chearng Shiue[1]

Received: 27 December 2018 / Accepted: 18 March 2019 / Published online: 13 April 2019

Abstract
With the maturity of RFID technology and the rapid development of mobile intelligent terminals, the Internet of Things (IOT) has attracted more and more attention and will become another revolution after the Internet. However, compared with traditional Internet applications, Internet of Things applications supported by RFID devices and intelligent terminals have more complex and serious security problems. For example, trust mechanism and malicious behavior detection have become the key issues to be solved in the construction of secure and trusted Internet of Things. The in-depth analysis and research of trust mechanism is of great significance to improve the security of the infrastructure of the Internet of Things and even the whole security system of the Internet of Things. Aiming at the relevant requirements of Internet of Things credibility in low-carbon supply chain environment, this paper proposes an improved random hash protocol and assistant game-based RFID credibility of Internet of Things. Combining with random oracle model security theory (ROM), experiments are carried out with data. A collaborative game method is proposed. Through collaboration with intra-agency nodes, inconsistent nodes and their observations are analyzed. Experiments show that simple game and cooperative game can effectively suppress malicious attacks in normal networks and malicious node–dominated networks, respectively. The protocol achieves the advantages of access authentication, anonymity security, anti-retransmit, anti-traceability, data accountability, time-scaling, and cost-effectiveness, and can effectively enhance the credibility of the Internet of Things in a low-carbon supply chain environment.

Keywords Cooperative game · Low-carbon supply chain environment · Random oracle model security theory · Improved random hash protocol · Malicious node–dominated attack model · Radio frequency identification

1 Introduction

With the acceleration of industrialization and urbanization, energy consumption and carbon emissions are rising rapidly [1]. Faced with the increasingly severe pressure of energy conservation and emission reduction at home and abroad, building an effective low-carbon supply chain has become an inevitable choice to achieve sustainable development and enhance comprehensive competitiveness [2–4]. Internet of Things technology is the use of radio frequency identification (RFID) sensors. Information equipment, such as Internet, connects all items involved in the supply chain and realizes intelligent omnidirectional positioning, tracking, and monitoring management of objects. It effectively reduces the cost of information transmission in the supply chain through digital material knowledge, improves efficiency and saves costs by means of extensive remote control, and makes use of intelligence. Management decision-making saves resources and energy consumption, thus becomes a strong support to promote the healthy development of low-carbon supply chain [5].

With the rapid popularization of RFID system, security issues will become more and more important. The research of security protection of RFID protocol depends on the research of security protection model of RFID. In recent years, some formal security frameworks have been proposed to evaluate the security and privacy of the system, but there is no absolutely correct and perfect security protection model to

✉ Lijian Yu
twncuyu@163.com

[1] Department of Business Administration, National Central University, Zhongli 320, Taiwan

prove the effectiveness of existing privacy protection schemes. The RFID security protection model used to analyze and prove the security of the RFID protocol can be divided into two categories: one is the RFID security protection model based on the oracle, that is, the attacker attacks the protocol by visiting the oracle to distinguish the privacy of the protocol. The other is a logic-based RFID security protection model, which uses mathematical symbols to formalize the protocol's communication process and the attacker's attack protocol process, so as to determine the protocol's security.

IBM, Intel, and Microsoft led more than 300 companies to establish international credibility organizations [6–8]. From a technical point of view, credibility aims to protect the information of designers and owners from being stolen or used by illegal users. Because of the difficulty of quantity processing and manual monitoring, the reliability of IOT has been paid more and more attention. According to the classification of IOT, IOT can be divided into perception layer, network layer, and application layer according to the technical framework. The perception layer mainly collects information of goods through RFID; the network layer mainly involves communication and interconnection fusion network. The application layer mainly integrates the Internet of Things and industry expertise [9]. The most critical of the three layers is the perception layer. Therefore, the core of the credibility of the Internet of Things in the low-carbon supply chain environment is to enhance the credibility of the RFID system in the perception layer [10–12].

This paper analyzes the existing problems of RFID security mechanism from physical mechanism and protocol mechanism, and designs an improved random hash lock protocol based on supply chain for RFID in order to improve the reliability of Internet of Things in supply chain environment.

Section 2 of this paper introduces reliability analysis of RFID system in supply chain environment, Section 3 of this paper introduces analysis of security mechanism of RFID system, Section 4 of this paper introduces RFID trustworthiness protocol based on supply chain, Section 5 of this paper introduces malicious behavior detection based on cooperative game, and Section 6 of this paper introduces experimental analysis and results.

2 Reliability analysis of RFID system in supply chain environment

The RFID system is mainly composed of tags, antennas, card readers, and back-end databases. Labels are composed of coupling coils and logic gates for data storage. They can be divided into active tags, passive tags, and semi-passive tags. Card readers are mainly used for reading and writing tags, and between tags are divided into forward and backward channels [13].

Internet of Things in supply chain environment Because the channel communication of the RFID system adopts the non-contact and exposed wireless channel, it is easy to threaten the reliability of the Internet of Things from the following aspects. Each node enterprise has its own RFID system, which reads the labels of upstream and downstream enterprises by card reader and obtains the detailed information of goods by combining with the back-end database. The system architecture is shown in Fig. 1.

First, interference rejection: Current RFID mainly uses low-frequency signals (13.56 MHz and 125 MHz) and high-frequency signals (433.56 MHz, 915 MHz, 2.45 GHz, and 5.8 GHz) [1], while strong interference between adjacent bands will result in confusion response of tags: write dormancy, identify errors, and other denial of service communication failures.

Second, stealing information: The RFID tag stores a large amount of item information. Illegal users can obtain commercial information such as items' price types and quantities by setting up related item list and stealing items' tag information from a long distance by means of large energy card reader and large size antenna.

Third, retransmit camouflage: Illegal users use devices to rewrite basic information of labels by stealing label responses and disguising them as legitimate labels to respond to inquiries from legitimate card readers, thereby tampering with basic data of items, or modify label security codes by interference of human signals, so that labels refuse legitimate card readers and interfere with supply chain Internet of Things services.

Fourth, location tracking: Illegal users can obtain dynamic data of tags by asking for tags many times with an unauthorized card reader, analyzing tag responses, and tracking items and business action paths under unauthorized circumstances.

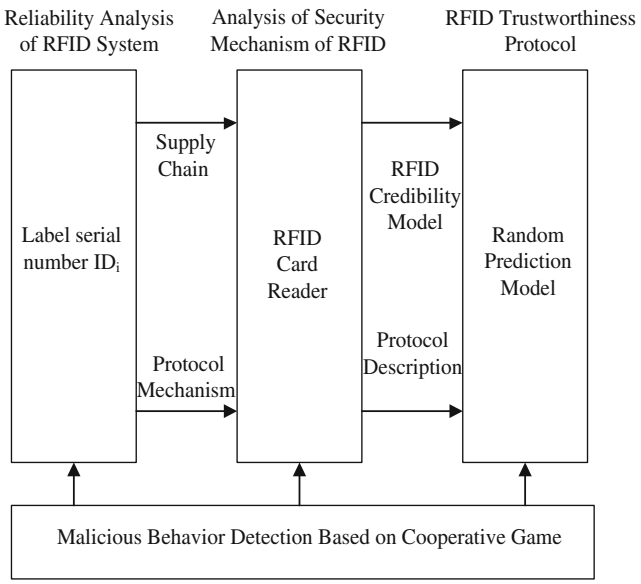

Fig. 1 The system architecture

Fifth, data tracking: After illegal users steal the label information of a link in the supply chain, they use data deductive tracking to infer other label information of the supply chain and obtain the data of the supply chain Internet of Things RFID system. In order to protect trade secrets and avoid conflicts of interest, node enterprises should transfer ownership after processing RFID tags; anonymous security can prevent information theft and rewriting camouflage through encryption system ID; and backtracking security can cutoff the forward and backward correlation of supply chain to prevent location and data tracking. In order to better deal with the above problems, the low-carbon supply chain environment requires that the RFID system meet the requirements of robust reliability, read-write authentication, and requirements of property, ownership transfer, anonymity security, backtracking security, etc. Among them, robust reliability ensures that the system can recover information flow by itself when communication protocol fails or frequency band is disturbed; read-write authentication requires that only legitimate authorized users can access label data; as a typical distributed loose structure, supply chain node enterprises cooperate.

3 Analysis of security mechanism of RFID system

Because of the cost factor, commercial RFID system must refine the physical circuit [14]. After satisfying the basic operation, only a small number of circuits serve for security and other purposes, and the use of complex encryption methods is limited by the very small size and weak power supply. According to the characteristics of the RFID system, the existing research mainly focuses on two aspects: physical and protocol mechanisms.

3.1 Physical mechanism

The physical mechanism mainly uses physical methods such as Ferrari shielding, active interference, and kill tag command. Ferrari shielding shields tags by blocking forward and backward communication for each item with a metal mesh cover, but this method obviously cannot be implemented for mass items in the supply chain. Users use signal devices to interfere with reading-protected labels, but this method may interfere with the operation of legitimate RFID systems while increasing costs. Kill label command sacrifices labels physically after the label information is read, but label traceability and low cost in low-carbon supply chain environment requirements make this method impossible to be widely used.

3.2 Protocol mechanism

Compared with physical security mechanism, software protocol mechanism is more suitable for the requirements of Internet of Things in low-carbon supply chain environment. It mainly uses cryptographic scheme and mechanism to design and create reliable protocols. The main protocol analysis is as follows.

(1) Two standard security protocol modes of ISO15693/IEC15693. Mode 1 sets 64-byte ID for non-collision avoidance and uses pseudo-random code generator to configure 32-byte feedback with unique random code for each tag. However, illegal users can use 32-byte linear feedback shifter or MAS Special decryption algorithms, such as crack random code traceable user label ID. Mode 2 uses slot mode or non-slot mode to equip the label with exclusive 64 bytes MFR label ID. According to the catalogue command requirements, the MFR label ID is fed back without access control, instead of illegal users. The basic principle of the two modes is that the reader transmits variable-length shielding information to respond to the corresponding tag while silently suppressing the non-corresponding tag. The illegal user can discover the response tag by double-shielding query of a single byte, increase query by 64 single byte, and steal the tag. Sign conflict avoids ID and controls MFR tag ID.
(2) Hash protocol. It is mainly divided into three protocols: Hash chain, hash lock, and random hash lock. Hash chain protocol requests authentication of tags and card readers by creating a certain number of hash functions. ID can be updated independently by using different responses. However, this protocol can only realize one-way identification of tags. It proves that once ID is intercepted, it is very vulnerable to retransmit camouflage attack, and each tag authentication requires several hash operations, which greatly increases the computational load and time cost. Hash lock uses one-way hash function to generate me taID to protect tag ID, but its metaID and ID cannot be dynamically refreshed. Random hash lock protocol adopts random number challenge response mechanism, but there are a lot of plaintext data communications between tag and card reader channel. On the one hand, it is vulnerable to data camouflage and tracking attack, on the other hand, it cannot be applied to the case of mass goods label in supply chain.
(3) Other protocols. The hash ID change protocol resists retransmit attacks by dynamically updating tag information with random numbers. But tags are not synchronized with the updating of back-end database information. If illegal users attack the upgraded back-end database, they can block the tag's back-end authentication. YA-TRAP resists tracing through monotonically

increasing timestamps, but it is easy. The improved YA-TRAP protocol and LPN protocol can identify tags by sharing key, and the key sharing cannot be guaranteed under the special interests of supply chain nodes.

The optimization objective with the greatest interval is used, that is, the distance between positive and negative sample data and the classification plane is the greatest. In protocol mechanism, finding the optimal hyperplane can be transformed into the optimization problem in formula (1):

$$\max \frac{1}{\|w\|} s.t. \quad y_i\left(w^T x_i + b\right) \geq 1, i = 1, 2, ..., n \tag{1}$$

This objective function represents a maximum of $\frac{1}{\|w\|}$ under $y_i(w^T x_i + b) \geq 1$, $i = 1, 2, ..., n$ constraints. Since maximization $\frac{1}{\|w\|}$ is equivalent to minimization $\frac{1}{2}\|w\|^2$, the objective function (11) can be transformed into formula (2) to facilitate solution:

$$\min \frac{1}{2}\|w\|^2 s.t. \quad y_i\left(w^T x_i + b\right) \geq 1, i = 1, 2, ..., n \tag{2}$$

The above discussion on protocol mechanism is based on the premise that the sample data is linearly separable. If the data is not completely linearly separable, that is to say, except for some interference noise points, it is basically linear separable, then protocol mechanism needs to introduce relaxation variable ζ. Relaxation variable ζ tolerates the presence of partial interference noise points. Therefore, the objective function (2) becomes formula (3):

$$\min \frac{1}{2}\|w\|^2 + C\sum_{i=1}^{n} \zeta_i s.t. \quad y_i\left(w^T x_i + b\right) \geq 1, \zeta \geq 0, i = 1, 2, ..., n \tag{3}$$

In summary, physical mechanism and protocol mechanism can guarantee security to some extent, but each has its own problems. Therefore, it is urgent to study a security protocol for RFID system to ensure the credibility of the Internet of Things in a low-carbon supply chain environment.

4 RFID trustworthiness protocol based on supply chain

Based on the analysis of the characteristics of the supply chain Internet of Things and the existing security mechanism of RFID, the reliability protocol of RFID based on the supply chain is designed by means of improved random hash lock protocol, and the reliability of the protocol is verified by data experiments combined with the security theory of random oracle model.

4.1 Supply chain–based RFID credibility model

Each node enterprise in the supply chain has its own RFID card reader and back-end database. Supply chain logistics contains *n* RFID tags. Because the reliability of RFID is mainly caused by the forward communication channel between tags and card reader, the enterprise card reader and back-end database are relatively safe due to the short communication distance. First, the model assumes that the illegal user can control all entity communications and can implement interference rejection, information stealing, retransmitting camouflage, location tracking, and data tracking by initiating inter-entity dialogues. The existing hash functions use block cipher hashing. Algorithms are constructed, and illegal users can also steal information by destroying hash functions through password attacks. Existing research shows that MD5, SHA, and other methods can be used to ensure the security of hash functions themselves, but there are various defects such as excessive hash diffusion. For this reason, based on the existing research results, this paper adopts the method of MD5, SHA, and other methods to ensure the security of hash functions. AES non-linear mapping method establishes hash function to ensure the security of the algorithm. According to the theory of random predictive model security, experimental data are setup to focus on channel transmission security.

4.2 Protocol description

(1) System settings: By default, when a supply chain node enterprise initially receives a tag (T_i, $1 < I < n$), the tag is in a secure mode state, and only the node enterprise has the right to modify the tag state. Ti contains the initial randomized identifier r_i and the tag serial number ID_i. Each record of TS in the back-end database corresponds to the randomized identifier of each tag. It also contains data information such as the initial bit length of the label, the indicator, and the flag bit.

(2) Protocol flow: The process of accessing tags by the t-th card reader is shown in Fig. 2.

Step 1: At the request of the reader, TS randomly generates the password RT and transmits it to the reader.

Step 2: The reader transmits RT to T_i and activates it.

Step 3: Ti combines TS and ID_i with its own state settings R_i, calculate hash ($ID_i \| r_i \| r_t$).

Step 4: Ti generates $s_i = r_i$ and updates the identifier to $ri + 1 = \text{hash}(ID_i \| r_i)$.

Step 5: Ti returns hash ($ID_i \| r_i \| r_t$) and Si to the card reader.

Step 6: The reader returns hash ($ID_i \| r_i \| r_t$) and S_i to TS.

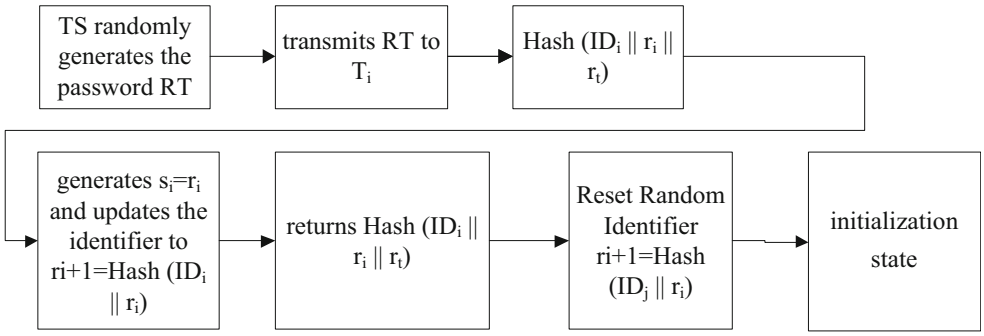

Fig. 2 Step of accessing tags

Step 7: According to s_i, TS detects whether ID_j exists in the data table, so that hash (ID_j || s_i || r_t) = hash (ID_i || r_i || r_t) is authenticated successfully if it exists, otherwise it fails.
Step 8: TS Reset Random Identifier ri + 1 = hash (ID_j || r_i), and new record RD_j corresponds to it. Re-send $r_i + 1$ to card reader and forward to T_i.
Step 9: T_i verifies whether hash (ID_j || r_i) = hash (ID_i || r_i) exists and the authentication is successful if it exists. Otherwise, $r_i + 1$ is replaced by S_i and R_I is restored to the initialization state.

$$Hash\left(ID_i \| r \| r_t\right) = \begin{cases} 0^\circ & if\ \max = \min \\ 60^\circ \times \frac{r_t - r_i}{\max - \min} + 0^\circ, & if\ \max = R\ and\ G\ G \geq B \\ 60^\circ \times \frac{r_t - r_i}{\max - \min} + 360^\circ, & f\ \max = R\ and\ G\ G < B \\ 60^\circ \times \frac{r_t - r_i}{\max - \min} + 120^\circ, & if\ \max = G \\ 60^\circ \times \frac{r_t - r_i}{\max - \min} + 240^\circ, & f\ \max = B \end{cases} \tag{4}$$

$$TS = \begin{cases} 0, & if\ \max = 0 \\ \frac{\max - \min}{\max} = 1 - \frac{\min}{\max}, & otherwise \end{cases} \tag{5}$$

In the formula, R, G, and B is RFID label; Max equals the largest in R, G, and B; and min is the smallest. The corresponding values in HSV space are H between 0 and 360°, S between 0 and 100%, V between 0 and max. With the above transformation formula, the RFID reader can be transformed to tag state.

5 Malicious behavior detection based on cooperative game

Malicious behavior detection is a feasible method to resist malicious node attacks. It is also the input of location privacy, trusted routing, and trust mechanism. It plays a very important role. However, in a dynamic environment, how to design a malicious behavior detection mechanism to accurately evaluate the credibility of nodes and reduce the frequency of malicious behavior will be a challenge [15].

We analyze the attack scenarios in which the attacker creates local advantages by deploying a large number of malicious nodes. Then, a simple game is constructed to judge the real events by the number of reported nodes, so that the Bayesian equilibrium can be achieved between normal nodes and malicious nodes. But in malicious node–dominated scenarios, the above equilibrium is broken. We then propose a cooperative game method to find all suspicious institutions and nodes, reducing the weight of forged reports, so as to achieve the goal: new Bayesian equilibrium.

5.1 Malicious node–dominated attack model

In a perceptual environment, multiple mechanisms {O_1, O_2,... O_j} deploy a certain number of RFID sensing nodes in a given region R. The nodes are connected to each other and can exchange information or relay data. Nodes of malicious organizations will take malicious actions against some characteristic data packets or interactive requests (such as publishing wrong topological information, discarding in routing, tampering with data packets, false positioning in LBS applications).

In order to reduce the impact of malicious events and the frequency of malicious attacks, nodes in the network (detection nodes) will monitor the surrounding phenomena, and according to the reports of neighbor nodes, analyze the possibility of malicious events, and decide whether to reduce the trust value of suspicious nodes. Attackers in the Internet of Things will perceive the current environment and predict the decision-making of detection nodes, and take malicious events or forged reports conditionally. Although the frequency of this kind of attack is lower than that of unconditional attack, it often has a high success rate and is more difficult to prevent. In local areas, malicious organizations can deploy a large number of nodes at very low cost to build their own local advantages, as shown in Fig. 3. In this scenario, the success rate of each attack execution is high, so the frequency of attacks also increases significantly.

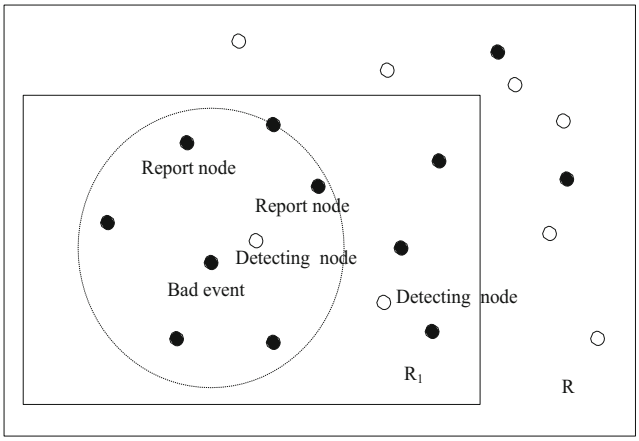

Fig. 3 Scenarios in which malicious nodes dominate

5.2 Attack suppression game method in normal networks

Behavior-based event deduction is faster and more general for generalized malicious events in perceptual networks. The main process is that ordinary perception nodes observe the surrounding phenomena, deduce the events that cause such phenomena through certain rules, so as to judge whether malicious events occur, and then update the trust value of the corresponding nodes. However, due to the dynamic nature of wireless networks and the limitations of node observation, single node inference is not reliable, so in our detection method, nodes refer to the inference results of other nodes. The specific steps of malicious event detection in perceptual environment are as follows:

Firstly, when the node R_0 detects the abnormal phenomenon e_i, the report E = {e_i, m (r_0, e_i), chk (r_0, {e_i, m (r_0, e_i)}, B (r_0, e_i), and B (r_0, e_i) are the confidence and uncertainty of event Key PR_0 signature name to ensure the integrity of the report.

After several iterations, the node r_n did not receive reports containing more nodes, forming a combined report E = {(r_j:{ei, m (rj, e_i), chk (r_j,{e_i, m (r_j, e_i)}, t, x)).

Finally, r_i parses the final report into r_j: {e_i, m (r_j, e_i)} according to the node partition. The most reported event E_{max} is:

$$e_{\max} = \operatorname{argmax}\left(\operatorname{count}\left(m\left(r_j, e_i\right)\right)\right) \tag{6}$$

When a malicious node r_m provides false reports, it will probably be rejected by r_n, and its credibility will be reduced. If an attacker repeats such behavior, his reputation value will soon be below a threshold, and he will be identified as a malicious node. Therefore, the method of judging events based on the number of reports is very effective.

5.3 Cooperative game method

To improve the simple game, a cooperative game method is proposed, which not only analyzes the behavior of nodes, but also focuses on the mechanism where the nodes are located. Despite the instability of nodes with short or few interactions, the institutions in which they are located are stable. If a malicious node has been identified before, then if it encounters the node of its organization again, these nodes may also take malicious actions. If the initial trust value and the weight of the report are reduced, the false report can be suppressed and the success rate of event detection can be improved. In the cooperative game, the main steps are as follows: firstly, updating the weights and priori properties of suspicious institutions and nodes to reduce the weights of suspicious reports when detecting events; secondly, adjusting the revenue function of detection nodes to improve the returns of reports with higher consistency with their own observations; thirdly, calculating the benefits of each strategy to select the best strategy; lastly, selecting the nodes with the same organization: share the deduction results, strengthen the positive feedback of trust, and reward and punish the relevant reporting nodes.

Let θ be "node normal" and report nodes r_{i1}, r_{i2},... r_{ir} property is θ, other report nodes r_{ir+1},..., *riw*. The nature of r_{iw} is $\neg\theta$. If the behavior a_1 is "the detection node considers the real event as an attack," then the nodes r_{j1}, r_{j2},..., *rjs* is the report of *rjs*. Because of the independence of nodes, the overall properties of reporting nodes are determined by the composite properties of most nodes (the number of nodes is greater than w/2). The prior probability p(θ) of reporting nodes is:

$$\begin{aligned} p(\theta) &= p(\theta(r_1, r_2, ..., r_w)) \\ &= \sum_{r>n/2} p(\theta(r_{i1}))p(\theta(r_{i2}))...p(\theta(r_{ir}))p(\theta(r_{ir+1}))...p(\theta(r_{iw})) \end{aligned} \tag{7}$$

When the detection node deduces the optimal strategy, the results are shared with the neighboring nodes of the same mechanism. When RN confirms the optimal strategy a2* = accept of most nodes in the organization for this event, it rewards the same reporting nodes as the overall report to increase their prior credibility:

$$p(\theta(r_i)) = p(\theta(r_i)) \cdot \text{award} \tag{8}$$

Table 1 Simulation argument setting

Area	1000 × 800 m^2	Node number	80	Communication distance	200 m
Proportion of mobile nodes	30%	Node speed	10 m/s	Time	200 s

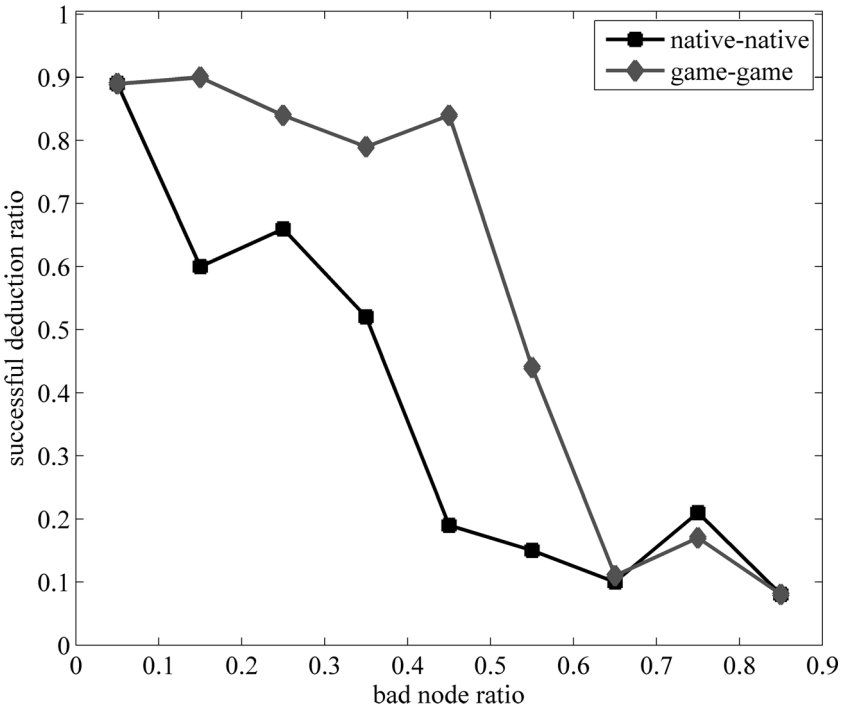

Fig. 4 Success rate of malicious behavior detection in normal scenarios

And punish the opposite node to reduce its transcendental credibility:

$$p(\theta(r_i)) = p(\theta(r_i)) \cdot \text{punish} \tag{9}$$

Conversely, when a2* = reject, the same is true for processing.

In order to prevent these nodes from being unavailable forever because of positive feedback, we stipulate that the trust value of nodes can be restored to a small value every other time [16]. In fact, the reputation of institutions in experiment has rebounded. That is because of the role of this mechanism.

6 Experimental analysis and results

The project team simulated and stored 900 tag data in SQL Server 2016. The experiment runs on a 6-core i7-8700

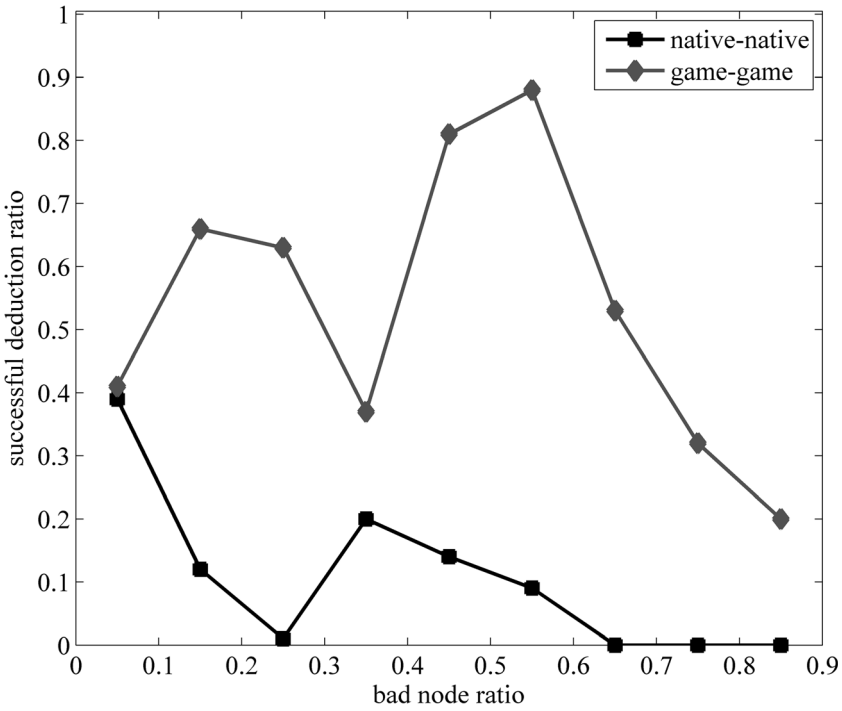

Fig. 5 Success rate of malicious behavior detection in abnormal scenarios

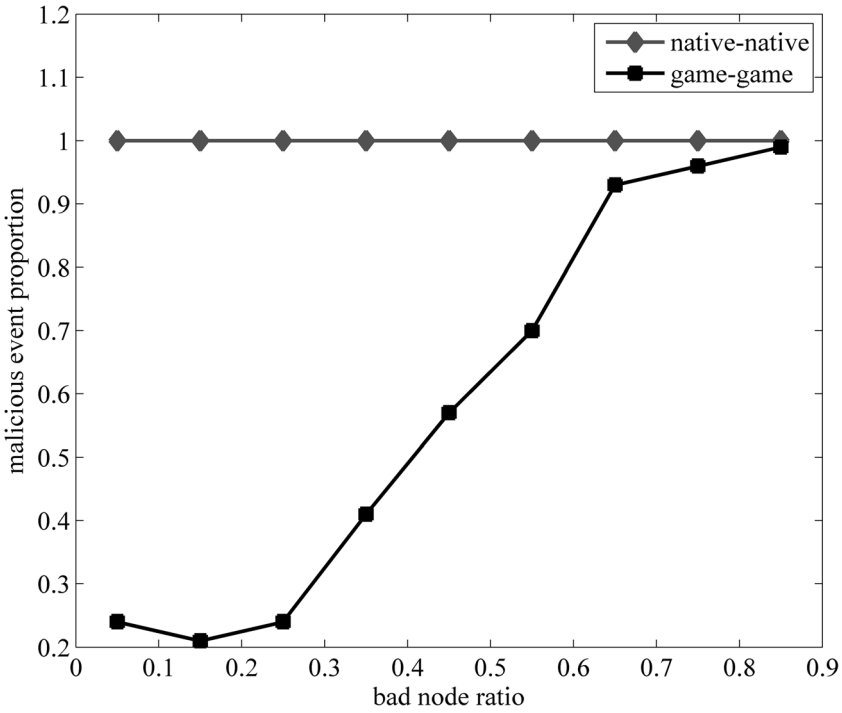

Fig. 6 Incidence of forged reports in normal scenarios

Windows 10 desktop computer with 2.0 GHz and 8 GB RAM. The algorithm uses open SSL and MATLAB libraries. The tag T_i was stored in TS format in the back-end database (ID = a, r_i = b, K = c), where a and B were initial assignments (random assignments 8 and 9); K was location index, and was not read. The simulation process TS generates random number RT = D (random assignment 36) to stimulate access to the 900th tag T_{900}. T_{900} calculates hash (8 || 9 || 36), $S_{900} = R_{900} = 8$, r_{901} = hash (8 || 9). From (hash (8 || 9 || 36), 9) to TS, TS searches for the existence of RD_{900} records based on $S_{900} = 9$: (8, 9, 0). If so, hash (ID || R_{900} || r_t) = hash (8 9 36) is calculated and is paired with the received hash values. By comparison, equality is validated. TS calculates $r_{901} = H$ (8 || 9) and builds RD_{901}: (ID = 8, r_{901} = hash (8 || 9), K = 901), then modifies RD_{901}: (ID = 8, $R_{900} = 9$, K = 901). If this communication ends, TS and T_{900} when communicating, RD_{901} will be queried according to $s_{901} = r_{901}$. At this time, the K of the record is 900, and RD_{901} will be used to cover RD_{900}. If this communication is

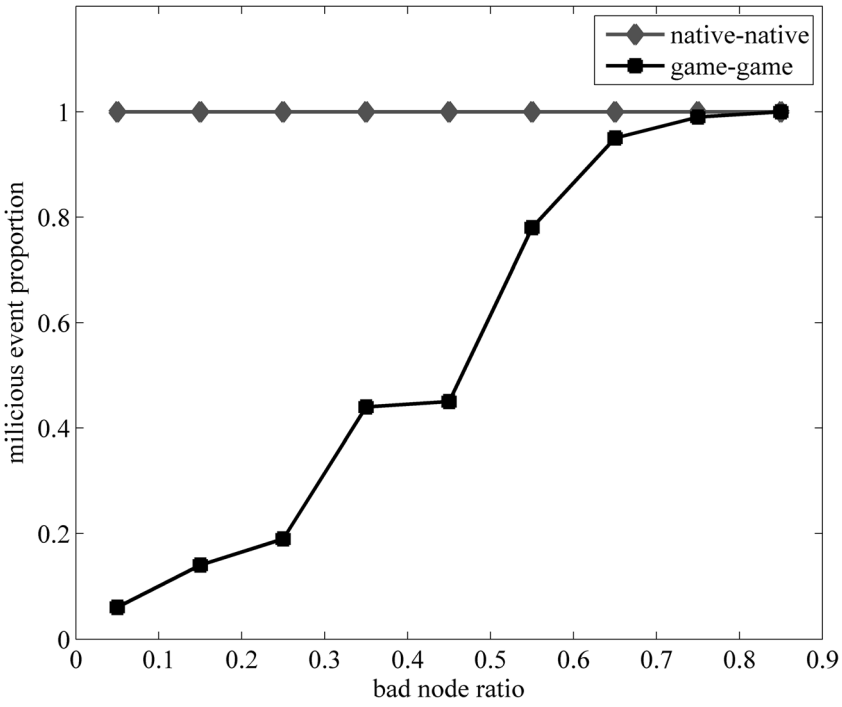

Fig. 7 Incidence of forgery reports in abnormal scenarios

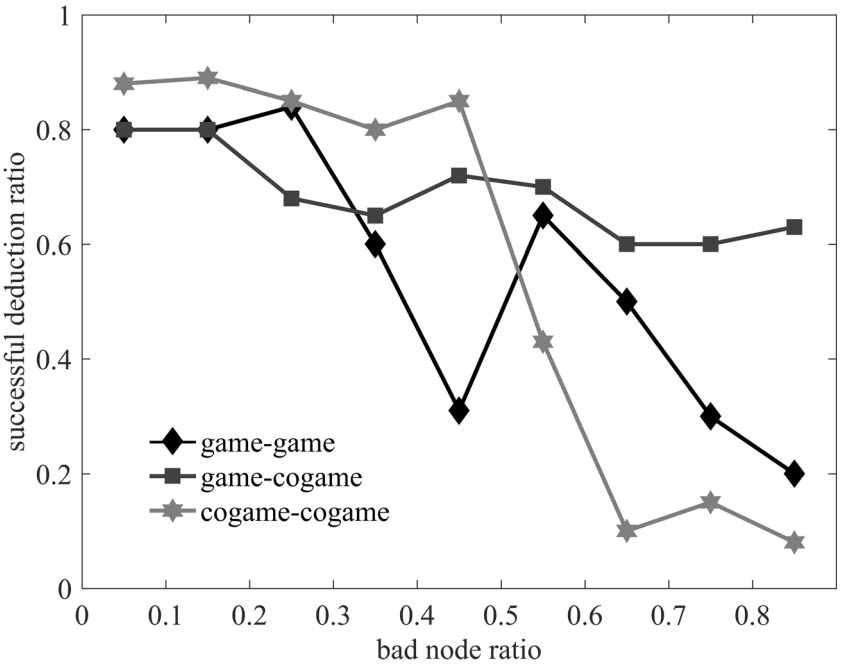

Fig. 8 Success rate of malicious behavior detection in normal scenarios

not passed, the T_{900} initialization identifier R_{900} will not be updated. When TS communicates with T_{900} again, RD_{900} will still be found, and modify RD_{901} according to K = 901.

6.1 Credibility analysis

6.1.1 Access authentication

Access authentication T_i initial state defaults to security mode, which only authorizes the supply chain node enterprise message authentication to access after success, effectively controlling the initial camouflage attack. When the reader requests T_i to read, it assumes that the illegal user has stolen r_t, but at this time, ID_i and r_i have not been transmitted through the channel, so they cannot steal r_{i+1}. The system will rewrite the identifier r_{i+1} only after locating the corresponding records in TS with the help of location index K. At this time, the probability of successful attack by illegal users is less than $1/2r_{i+1}$, which effectively guarantees the security of initial data query.

6.1.2 Anonymous security

In hash (x) = h, because of the unidirectional nature of hash function, it is impossible to use h to deduce X. Therefore, if

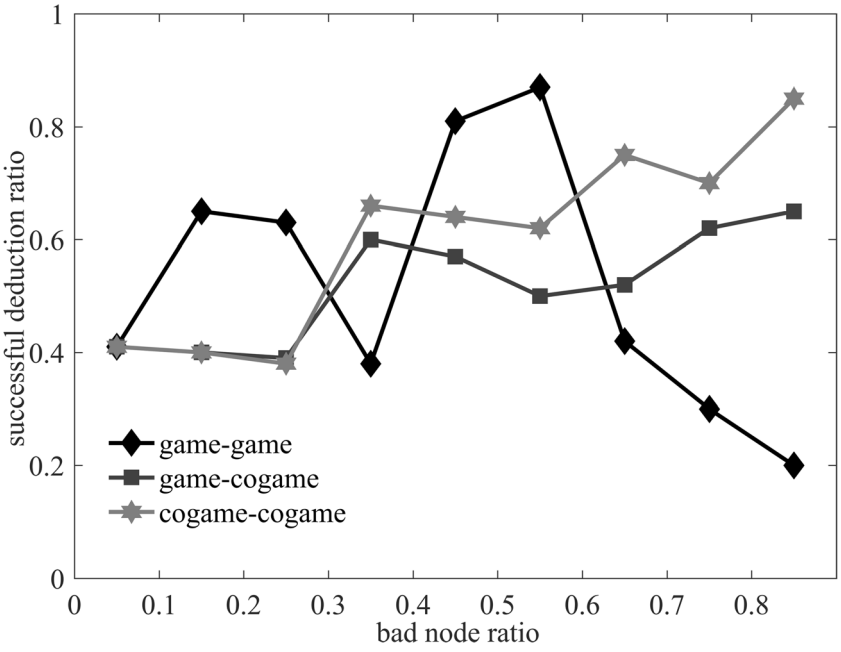

Fig. 9 Success rate of malicious behavior detection in abnormal scenarios

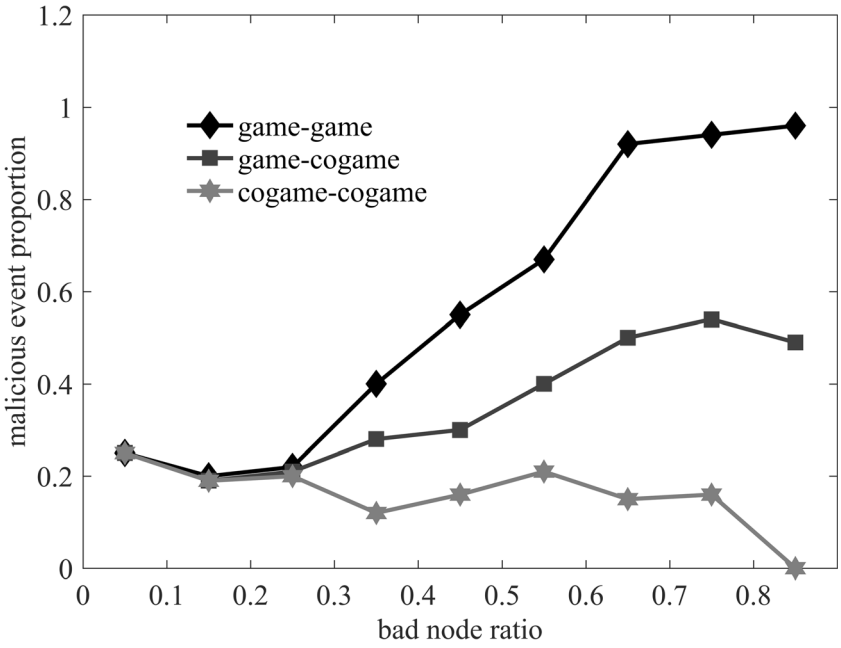

Fig. 10 Incidence of forged reports in normal scenarios

hash ($ID_i \| r_i$), hash ($ID_j \| r_t \| r_t$) equivalents are stolen; illegal users cannot deduce label ID and a random number.

6.1.3 Anti-retransmitting

The protocol dynamically refreshes the label ID in real time and updates each ID to exchange information. Even if the illegal user records the last ID passed, the ID cannot be validated by replaying the ID.

6.1.4 Anti-traceability

Because Ti has been updated before issuing hash ($ID_i \| r_i \| r_t$), it can effectively prevent illegal users from continually tracking an ID to obtain object location. Because the hash function based on AES can effectively shield the correlation information between r_i and r_{i+1}, even if illegal users use intermediate attack Ti and decode r_{i+1}, there is no such function. The method further obtains the historical data of r_i and guarantees the forward traceability of T_i.

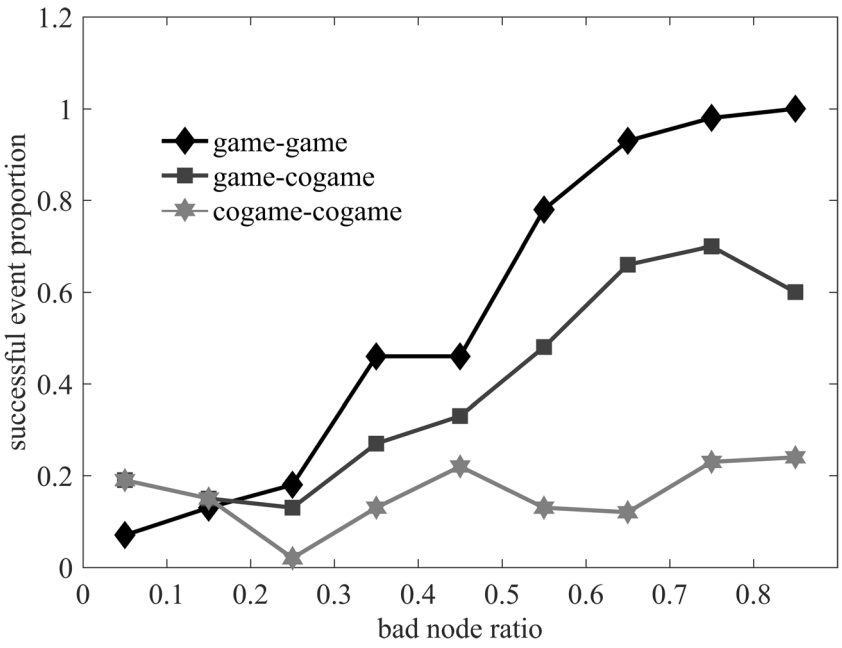

Fig. 11 Incidence of forgery reports in abnormal scenarios

6.1.5 Data accountability

Ideally, the back-end database TS holds all T_i information. When T_i is associated with the supply chain node enterprises asynchronously, T_i can be restored by K and S values, which effectively guarantees the consistency of TS and T_i data.

6.1.6 Reducing time and increasing efficiency

In this protocol, TS decodes ID according to r_i without exhaustive ID for hash function operation. When *n* Tis are stored in TS of supply chain node enterprises, using this protocol, each query of TS generates a random number, implements *n* searches and 2 hash function operations, while the relatively most efficient hash chain coordination is achieved. The protocol needs to implement 2n hash function operations, 2n searches, and comparisons. Therefore, this protocol effectively shortens the search time, reduces the computational load, and improves the comparative efficiency. With the increasing number of T_i items in the supply chain, the time required for protocol search calculation increases slowly, which is very suitable for the Internet of Things in the low-carbon supply chain environment. Massive commodity requirements.

6.1.7 Cost advantage

Data from Auto-ID Laboratory of MIT show that it takes about 0.02–0.04 KB gate circuit to implement single hash function operation, and 2.5–5 KB gate circuit for commercial RFID security purpose. This protocol only needs 0.04–0.10 KB gate circuit, which can easily adapt to existing hardware conditions. Moreover, the relatively complex computing processes such as generating random numbers are converted to TS, which effectively reduces the complexity of T_i and makes the tag have a good cost advantage in manufacturing and using.

6.2 Malicious behavior detection experiment

In the normal scenario, we compare the effect of using game and not using game to suppress attack [17]. Then, we verify the effect of using simple game to suppress attack in the scenario where malicious organizations dominate. Based on this, we compare the detection and suppression effects of attack using simple game and cooperative game. Finally, we verify the influence of inferential feedback between nodes on the game. The default parameters for the simulation are shown in Table 1.

Figures 4, 5, 6, and 7 show the incidence and success rate of malicious events in both normal and abnormal scenarios.

Because unconditional malicious nodes forge reports at any time, the incidence of malicious events is 100% in both scenarios. In simple game, malicious nodes forge reports only if and only if the neighboring nodes are dominant. Therefore, the number of forged reports increases approximately linearly with the number of malicious nodes in Figs. 5 and 7.

When there are 85% malicious nodes, the detection success rate of both methods is less than 25%. When malicious nodes in simple game behave normally, the success rate of normal scenarios is maintained at more than 75%, and the success rate of abnormal scenarios is maintained at more than 35%. It can be seen that, when the number of malicious nodes is small, malicious attacks cannot be suppressed even though they are easy to be detected, while simple game mechanism can not only detect and suppress malicious attacks [18]. When the number of normal nodes is equal to or greater than that of normal nodes, simple game is not suitable for malicious node–dominant scenarios. Then, we compare the success rate of event detection and the incidence of forgery reports in normal and abnormal scenarios. At this time, the detection nodes only infer events by the arithmetic average reported by each party.

It can be seen that when malicious nodes think that "detection nodes reject their own reports according to the optimal strategy," they will faithfully submit real reports, and both sides reach the dynamic Bayesian equilibrium. As a result, the incidence of malicious events in normal networks is greatly reduced, so simple game is very effective in ordinary networks where malicious nodes account for a small number (Figs. 8 and 9).

The experiment shows that the success rate of event detection is low when the detection report node uses simple game; especially when the malicious node reaches more than 90%, the detection success rate is not more than 25% and 35% in the two scenarios. When malicious organizations dominate (malicious nodes account for 70–90%), game-cogame relies on cooperative mechanism to make its detection success rate higher than game-game (51.5% and 18.2% higher in both scenarios). On the other hand, when malicious nodes are dominant, malicious nodes in cogame-cogame infer the strategy of detecting nodes. Therefore, the success rate of malicious behavior detection is higher, and the incidence of malicious events in cogame-cogame in Figs. 10 and 11 is less than the other two methods.

In the improved game method, the prior probability of nodes can be reflected by the credibility of institutions. Firstly, the reputation of institutions is long-term stable, which truly reflects the prior credibility of unknown nodes. Secondly, the behavior of a large number of nodes is quickly and directly fed back to the reputation of institutions, which solves the problem of trust initialization in dynamic environment. Furthermore, the prior probability of the nature of a single node is adjusted by the trust adjustment

factors of the node and its affiliated institutions, which reduces the weight of multiple collusion nodes and a single malicious node.

7 Conclusion

According to the characteristics of low-carbon supply chain environment Internet of Things, based on the analysis of the physical and protocol security mechanism of existing RFID systems, this paper designs an improved RFID protocol in low-carbon supply chain environment. According to the simulation data based on ROM model, the security protocol can effectively enhance the low-carbon supply chain. The next step is to design a general combined security model of the Internet of Things based on the requirements of low-carbon supply chain to further improve the self-security of hash function and enhance the credibility. This paper proposes a cooperative game method, which can effectively reduce the weight of malicious reports in the whole event report by cooperating with the nodes in the organization and analyzing the inconsistent nodes and their affiliated organizations. It can achieve a new Bayesian equilibrium and further suppress malicious attacks through feedback from the nodes. Experiments show that simple game and cooperative game can effectively suppress malicious attacks in normal networks and malicious node–dominated networks, respectively.

References

1. Rajaraman V (2017) Radio frequency identification. Resonance 22(6):549–575
2. Pescetto P, Pellegrino G (2018) Automatic tuning for sensorless commissioning of synchronous reluctance machines augmented with high frequency voltage injection. IEEE Trans Ind Appl 11(9):168–183
3. Purushothaman G, Prakash PR, Kothari S (2018) Investigation of multiple frequency recognition from single-channel steady-state visual evoked potential for efficient brain–computer interfaces application. Iet Sign Process 12(3):255–259
4. Hase A, Mishina H (2018) Identification and evaluation of wear phenomena under electric current by using an acoustic emission technique. Tribol Int 64:145–161
5. Hartcher KM, Hickey KA, Hemsworth PH, Cronin GM, Wilkinson SJ, Singh M (2016) Relationships between range access as monitored by radio frequency identification technology, fearfulness, and plumage damage in free-range laying hens. Animal 10(5):847–853
6. Bolaños F, Ledue JM, Murphy TH (2017) Cost effective raspberry pi-based radio frequency identification tagging of mice suitable for automated in vivo imaging. J Neurosci Methods 276:79–83
7. Dufour JC, Reynier P, Boudjema S, Soto Aladro A, Giorgi R, Brouqui P (2017) Evaluation of hand hygiene compliance and associated factors with a radio-frequency-identification-based real-time continuous automated monitoring system. J Hosp Infect 95(4):344–357
8. Barge P, Gay P, Merlino V et al (2017) Radio frequency identification technologies for livestock management. Can J Anim Sci 93(1): 23–33
9. Bachtobji S, Omri A, Bouallegue R, Raoof K (2018) Modelling and performance analysis of mmWaves and radio-frequency based 3D heterogeneous networks. IET Commun 12(3):290–296
10. Awan SA, Pan G, Taan LMA et al (2018) Radio-frequency transport electromagnetic properties of chemical vapour deposition graphene from direct current to 110 MHz. IET Circ Devices Syst 9(1):46–51
11. Li P, Lang Z, Zhao L et al (2018) System identification-based frequency domain feature extraction for defect detection and characterization. NDT&E Int 98:70–79
12. Kgwadi M, Rizwan M, Kutty AA et al (2016) Performance comparison of inkjet and thermal transfer printed passive ultra-high-frequency radio-frequency identification tags. IET Microwaves Antennas Propag 10(14):1507–1514
13. Mousavi N, Sharifkhani M, Jalali M (2016) Ultra-low power current mode all- MOS ASK demodulator for radio frequency identification applications. IET Circ Devices Syst 10(2):130–134
14. Rockelé M, Vasseur K, Mityashin A et al (2018) Integrated tin monoxide P-channel thin-film transistors for digital circuit applications. IEEE Trans Electron Devices 65(2):514–519
15. Hogan MT, Edge AC, Geach JE et al (2018) High radio-frequency properties and variability of brightest cluster galaxies. Mon Not R Astron Soc 453(2):1223–1240
16. Combs AW, Shiroma WA, Ohta AT (2018) Ferrofluidic actuation of liquid metal for radio-frequency applications. Electron Lett 54(3): 151–153
17. Fu S, Xu Z, Lu J et al (2018) Modulation format identification enabled by the digital frequency-offset loading technique for hitless coherent transceiver. Opt Express 26(6):755–769
18. Qian L, Zheng L, Shang Y, Zhang Y, Zhang Y (2018) Alzheimer's disease Neuroimaging Initiative. Intrinsic frequency specific brain networks for identification of MCI individuals using resting-state fMRI. Neurosci Lett 664:7–14