International Journal of Smart Home
Vol. 9, No. 11, (2015), pp. 187-196
http://dx.doi.org/10.14257/ijsh.2015.9.11.20

Food Security Sensor Management Based on RIHA

Zhehui Xiao[1], Dekui Li[2*], Chinling Chen[3] and Jinlong Zhang[1]

[1]School of Management, Huazhong University of Science and Technology, Wuhan, 430074, China
[2]Liaocheng University, Shandong, 430065, China
[3]College of Management, Chaoyang University of Technology, Taiwan
JerryinKorea@gmail.com

Abstract

The coming of information age makes the integrated electronic food security sensor management in industrial field face new challenges. This paper takes the security management food security sensor management of food industry the industrial area as the researching object, discussing the architecture of ASAAC standard food security sensor management, by means of a RSSI-based Information Hiding Algorithm (RIHA) analysis method, it puts forward ideas of assessment on the food security sensor management safety. And uses RSSI (Received Signal Strength Indication) as hidden information carrier and designs. It does not affect original data or bring additional communication cost. The simulation results show that RIHA has high hidden information transmission accuracy without bringing additional communication energy consumption.

***Keywords**: Food security sensor management; RIHA; hidden information transmission*

1. Introduction

The architecture of software can be defined as IMA (Integrated Modular Avionics) in food safety electronic food security sensor management, which can provide a uniform requirement for the design and development of the software framework of the core processing food security sensor management [1]. The software framework of ASAAC standard food security sensor management is based on the architecture of the layered software, the structure of this layered food security sensor management consists of three layers, including application layer (AL), operating food security sensor management layer (OSL) and module of supporting layer (MSL) [2]. Application layer defines the function application as well as the management application. The function application is usually so-called application task; application management is the implementation of the food security sensor management management which is closely related to the application [3]. The operating food security sensor management layer defines three parts, namely, the operating food security sensor management, general management food security sensor management (GSM) and running blueprint [4]. General management food security sensor management includes health monitoring, fault management, configuration management and security management; operating blueprint contains all the information of the configuration and the core part of management food security sensor management. Module supporting layer defines the basic drive management of the low-level hardware resources. The interface between the application layer and operating food security sensor management layer is APOS, while the interface between the operating food security sensor management layer and supporting layer is MOS. These interfaces make the three levels be independently separated with each other [5, 6].

2. The Architecture Component of Food Security Sensor Management Software

The software architecture of ASAAC standard food security sensor management defines a set of components and interfaces, moreover, the interface of software can be divided into two categories, namely, direct interface and logical interface [7]. In the direct interface, it defines the application layer and the interface of operating food security sensor management layer (APOS), module support layer / module operating food security sensor management layer (MOS), food security sensor management management (SMBP) / interface of blueprint as well as food security sensor management management / interface of operating food security sensor management (SMOS), totally four kinds of interfaces [8]. While in the logic interface, it defines four kinds of interface, namely, the logic interface of the operating food security sensor management (OLI), the logic interface of general food security sensor management management (GLI), the logic interface of food security sensor management management (SMLI) as well as the logic interface of module (MLI). The architecture model of ASAAC software in detail can be shown in Figure 1:

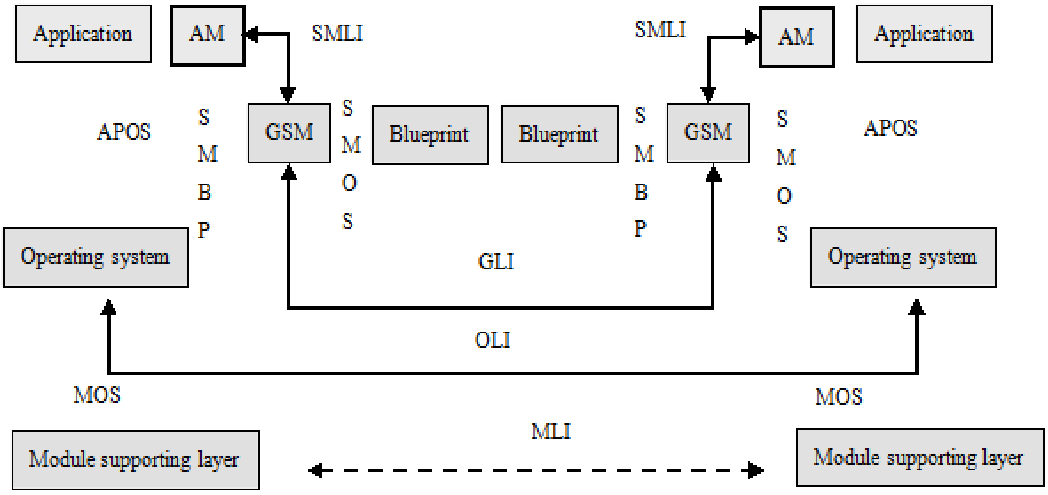


Figure 1. The Architecture Module of Software Food Security Sensor Management

Application management (AM): it can be responsible for non-standard food security sensor management management, implementing mission, management mode, the interface between AM and GSM is the logic interface for the food security sensor management management;

Operating food security sensor management (OS): it is a specific section that can offer OSL function, which also can control the real-time behavior of the processing unit as well as its related components;

General food security sensor management management (GSM): it is responsible for the core processing management, which can be including four parts: health monitoring (HM), (FM) fault management, configuration management (CM) and safety management (SM);

Running blueprint (RTBP): it contains the information of the configuration and management at the core process on the host computer (such as: processing description, routing information, fault management, *etc.*,);

Module of supporting layer (MSL): it encapsulates the underlying hardware details, which can provide methods of the universal, independent access to the underlying resources;

The interface from application to the operating food security sensor management (APOS): the separated aircraft depends on software named as AL, as well as the independent software of aircraft named as OSL. Its purpose is to provide a standard OS service interface for the AL process, which can improve the re-usability and portability of the application software;

The interface from module support to operating food security sensor management (MOS): in order to divide the OSL and hardware, it needs software called MSL[9]. Its purpose is to provide a transparent interface for operating food security sensor management which can independently adjust the function of hardware[10]. Thus, MOS allows the same OSL software reside in the specific CFM, regardless of the underlying hardware;

The interface from safety management to the blueprint (SMBP): the interface between GSM and the blueprint is encapsulated in OSL, which can allow and the implementation and structure of blueprint is non - standard, but it should be the interface from the defined blueprint to the standard interface of GSM;

The interface from food security sensor management management to the operating food security sensor management (SMOS): it is packaged in OSL, which can describe the services for GSM offered by the operating food security sensor management;

The logic interface of operating food security sensor management (OLI): it describes the process with two examples of OS, as well as the usage of VC communication;

The logic interface of GSM (GLI): it describes mutual communication between two examples of GSM, moreover, the internal communication between GSM is hierarchical;

The logic interface of food security sensor management management (SMLI): it describes communication protocol between AM and GSM based on VC. AM and GSM must be cooperated with each other, with the help of SMLI for communication and synchronization;

The logic interface of module (MLI): it defines the interface between the modules and the food security sensor management structure of the interface to meet the demand of interoperability.

3. Food Security Sensor Management

Food security sensor management management is a whole management food security sensor management from the flight of the aircraft to landing stage, which is composed of two parts, namely, the application management of application layer that is located in ASAAC model of the three layer stack (TLS), as well as the general food security sensor management management GSM of the operating food security sensor management layer. Its main tasks can be included: the initialization of controlling food security sensor management, reconfiguration, power off; authentication, filtering, fault locating; providing related security services.

3.1 The Main Functions of Each Management Level of the Food Security Sensor Management

AC. AC is a single entity of the food security sensor management management, which is responsible for controlling and monitoring the entire integrated modular food safety electronic food security sensor management (IMA), as well as responsible for loading the food security sensor management data (both task data and safety data); AC is responsible for the initialization of food security sensor management security. Before the operation of the food security sensor management, AC is responsible for the initialization of IA and RE, AC can receive the initialization security request and key request of IA and RE.

IA. IA is a logical group of comprehensive application. This group is a dynamic group, which can be generated dynamically according to the need of the task; each IA can control one or more RE; the internal of IA may be organized as a hierarchical layer, such as: a comprehensive district may be included one or more levels of IA, in this case, IA in the lower layer must control one or more PE; the food safety electric food security sensor management can be designed a food security sensor management without including IA level, in this case, it can exist one AC and one or more RE.

RE. RE is the lowest layer, which is responsible for dealing with a single PE; it can receive the security information of initialization from CM, at the same time, it can send the initialization security request and key request to the upper layer.

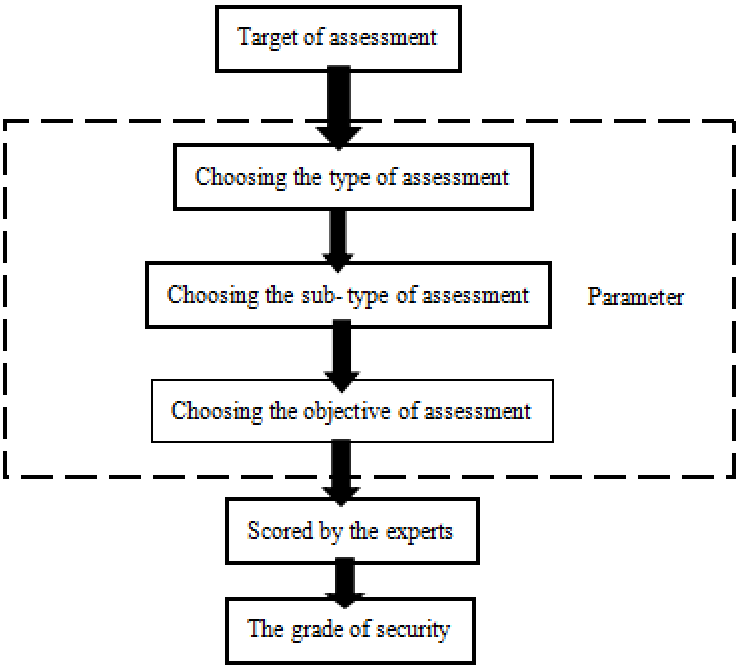

Target of assessment
Choosing the type of assessment
Choosing the sub-type of assessment
Parameter
Choosing the objective of assessment
Scored by the experts
The grade of security

Figure 2. The Model Diagram of Security Assessment

3.2. RSSI Based Information Hiding

In this section, we introduce the characteristics of RSSI first, and analyze the feasibility of taking it as hidden information carrier. Then we design the RSSI based information hiding algorithm which is called RIHA, and analyze its performance in theory.

3.2.1. Feasibility Analysis: In resource constrained sensor networks, gathering RSSI value is "free lunch", because it neither adds communication overhead nor increases network burden. It is widely used in node location, target tracking, protocol design and so on.

Although RSSI changes with environment, a large number of studies show that the variation has certain regularity. Generally log distance path loss model is used to describe wireless signal propagation energy variation in wireless sensor networks:

$$RSSI(d) = P_T - P_L(d_0) - 10\eta \log_{10}\frac{d}{d_0} + X_\sigma \tag{1}$$

In which, P_T is the emission energy, $P_L(d_0)$ is the path loss of propagation unit distance d_0. The unit of energy is dBm, the unit of distance is m. η is the path attenuation index, its value between 2 and 5. Random Gauss function $X_\sigma = N(0,\sigma^2)$ represent the uncertainty of RSSI, σ between 4 and 10, its value depends on the actual environment.

RSSI relates to initial transmit power and path loss, path loss can be computed out when the environment and distance is known. Thus the initial transmit power is the main factor of RSSI. Existing sensor nodes can set different transmit power to meet different application requirements. Adjusting node's transmit power could obtain corresponding RSSI that provides the feasibility of information hiding. The sending node uses different transmit power to deliver hidden information, and the receiving node restores the hidden information from received RSSI value.

As RSSI varies with spatial and temporal, taking it as hidden information carrier is undetectable. This method does not require complex computation, does not change original data, does not affect communication process, and does not bring additional energy consumption. It is very suitable for source limited wireless sensor networks. It not only can be used in hidden information transfer and extract, but also can be used in network data integrity protection, security transmission check and *etc*.

3.2.2. Algorithm Design: In order to improve the discrimination and reduce the fluctuation impact of RSSI, RIHA uses the maximum transmit power behalf of 1, and the minimum transmit power behalf of 0. RIHA sets the upper and lower limit values of RSSI, if sampled RSSI value greater than the upper limit value represents the hidden information is 1, if it less than the lower limit value represents the hidden information is 0.

Before hidden information transmission, coding rules should be determined. Coding rules are set before node deployment, and be used after deployment. In order to improve network security, the base station changes the coding rules by broadcasting periodically. Thus, hidden information cannot be obtained without coding rules, which improves network security greatly.

RIHA can be divided into three steps: establish hidden information transmission link; transmit hidden information; release hidden information transmission link.

The First Step: establish hidden information transmission link.

Sensor nodes select transmit power randomly to send routine data when there is no hidden information to be sent. A node with hidden information to be transmitted is called source node. The source node sends a link establish request information according to the decided rule, for example, the sequence of "maximum power - minimum power" repeats n times. Then it sends the hidden information receiving node's ID according to the encoding rule.

The node receives the link establish request information, for example, received information's RSSI with the sequence of "larger than the upper limit - less than the lower limit" repeated n times. Then it judges whether to receive the hidden information according to the node ID received subsequently. The receiver will work normally when the received node ID neither matches its ID nor in its routing table. The receiver will become destination node when the received node ID matches its ID or in its routing table. The destination node sends a confirmation message to the source node in accordance with the decided rule. The hidden information transmission link is established. If the hidden information transmits through multi hop routing, repeat above steps until the integral information transmission path is established.

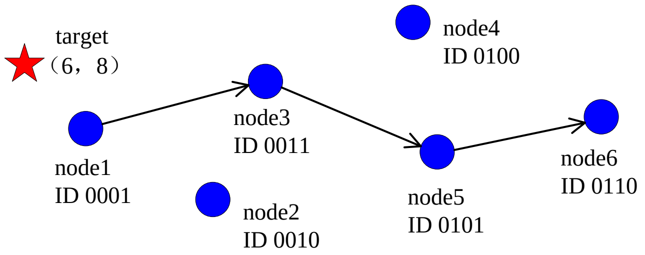


Figure 3. RSSI based Information Hiding

In order to explain RIHA better, take figure 3 for example. The decided rule is 8421 code, nodes are used to collect temperature, humidity information, and transmit suspicious target position with covert. Node 1 (ID code 0001) finds the suspicious target, it has to send the target's position (6, 8) (coordinate code 01101000) to node 6 (ID code 0110).

Node 1 sends n times of temperature and humidity information with the sequence of "maximum power - minimum power". Then it sends temperature and humidity information with the sequence of "minimum power - maximum power - maximum power - minimum power" in accordance with node 6's ID code "0110". Node 2 receives this information, "0110" does not match its ID and not in its routing table, it does not do any treatment. Node 3 finds that the ID in its routing table. It sends confirm information to node 1 and establishes transmission link. Then, node 3, node 5 and node 6 establish the transmission link in the same way.

The Second Step: transmit hidden information.

After the transmission link is established, the source node begins to send hidden information in accordance with the determinate coding rule. The destination node decodes hidden information according to the coding rule. If the hidden information transmits through multi-hops routing, intermediate forwarding nodes do not decode the information. They only determine the information transmit power, and send message with the same transmit power until the information is transferred to the destination node or base station.

However, RSSI is fluctuating due to interference and other reasons, especially in the disrupting situation like battlefield. And packet loss also brings hidden information decode error. Redundant information is used to improve the reliability of hidden information transmission. The source node sends information with the transmit power correspond to the hidden information repeatedly, rather than each hidden information's transmit power used only once. The number of repetition depends on the environment and packet loss rate. The destination node uses filtering algorithm to dispose received RSSI, checks received information integrity and corrects error to get more accurate and effective information.

Still using the example of figure 1, the transmit power of each hidden information is used 3 times. That is to say node 1 sets different transmit power in accordance with the sequence of "000 111 111 000 111 000 000 000" to send temperature and humidity information. Node 3 does not decode the hidden information, it judges the transmit power and sends message to Node 5 with the same transmit power. In the same way, Node 5 forward information to Node 6. Node 6 uses filtering algorithm to handle received RSSI value, such as average filtering and so on, then it could get the position of target.

The Third Step: release hidden information transmission link.

The source node sends link release request information according to the decided rule when the hidden information transmission complete. For example, it sends m regular data with the sequence of "maximum power - minimum power - minimum power". The destination node receives link release request information, and sends a confirmation according to the determined rule. The information transmission link is released, and the hidden information transmission process complete.

When the data transmission is complete, node 1 sends temperature, humidity information m times with the sequence of "maximum power - minimum power - minimum power". Node 3 sends a confirmation message to node 1. It sends temperature, humidity n time with the sequence of "maximum power - minimum power - minimum power", and gets the confirmation of node 5. In the same way, Node 5 obtains node 6's confirmation. The transmission process of hidden information is over.

In many applications, networks transmit hidden information all the time which does not need to establish and release the transmission link frequently. In this case, the first step runs only one time after network deployment. Nodes transmit hidden information with routine data until died without running the third step.

3.2.3. Performances Analysis: Generally, sensor nodes' transmit power can be divided into more than 30 levels, RIHA only makes use of the highest and lowest transmit power, and filters are used at the receiving end, which is sufficient to distinguish RSSI value. Therefore, the rate of packet loss is the greatest impact factor for receive hidden information correctly. Assume the number of continuously received signal in the same strength section is N_{RSSI} , the repetition number of each hidden information code is T_N , the number of encoding message in the same section I_R is:

$$I_R = \left\lceil \frac{N_{RSSI}}{T_N} \right\rceil \tag{2}$$

The number of continuously send hidden information in the same section is I_S , network packet loss rate is $Loss$, to ensure $I_s = I_R$, then

$$I_S * T_N * Loss < T_N \quad I_S < 1/Loss \tag{3}$$

Thus, to ensure receiving hidden information correctly, the number of continuous hidden information coding in the same section should less than the reciprocal of packet loss rate.

The hidden information transmission delay relates to the hidden information code number and time of iteration. The hidden information transmission delay is $I_S * T_N$. Visibly, increasing the repetitions of hidden information coding improves reliability, but also increases transmission delay. We should regulate the repetition time according to the environment and data's importance degree.

In addition, the amount of hidden information associates with the coding rules, simple coding rule's information hiding ability is limited, coding rules with large information hiding capacity often more complex in computation. It should consider the requirement of information hiding and design rational encoding rules.

4. Experiment Analyses

RIHA's reliability and validity is verified by simulation experiments. This section mainly analyzes two aspects of its performance: hiding information acquisition ratio and energy consumption.

We set the distance between the nodes is 80m, the maximum transmission power is 0dBm, energy consumption is 17.4nW, the minimum transmission power is -24dBm, energy consumption in transmission process is 8.5nW, the transmission frequency is 2400MHz, path attenuation index is 2.5, random Gauss noise from environment is 5 in the simulation. Assuming the hidden information is: 0011 0101 0110 0111 1110 1010 1011 1111.

RSSI without repeat hidden information code transmission is shown Figure 4. The horizontal axis is the number of received packet, and the vertical axis is the RSSI correspond with the packet. From the figure we can see the change of RSSI clearly. The upper limit of RSSI is 170 and the lower limit of RSSI is 160. Thus the RSSI higher than 170 is 1, and less than 160 is 0, we can obtain the hidden information for this group RSSI is: 0011 0101 0110 0111 1110 1010 1011 1111, which is the same as the hidden information is sent.

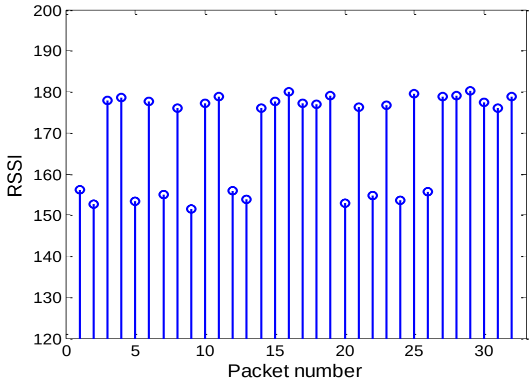


Figure 4. RSSI Without Repeat Hidden Information Code Transmission

In these experiments, the hidden information acquisition rate is 100%. When the packet transmission correctly, the receiver can extract the hidden information completely. The simulation results prove the correctness of RIHA. Packet loss did not occur in the simulation, in actual situation the data may lose due to conflict or other reasons. The efficient filtering algorithm and reasonable data processing technology are used. The receiver can recover the hidden information through redundancy checking and correct errors in transmission to improve the accuracy of hidden information acquisition further.

Next, we analyze the energy consumption of RIHA. Figure 4 compares the energy consumption of nodes with or without hidden information. The horizontal axis is the packet number, and the vertical axis is the energy consumption. The blue dashed line represents the energy consumption without hidden information transmission, in which the sender selects transmission power randomly. The red solid line represents the energy consumption with hidden information transmission.

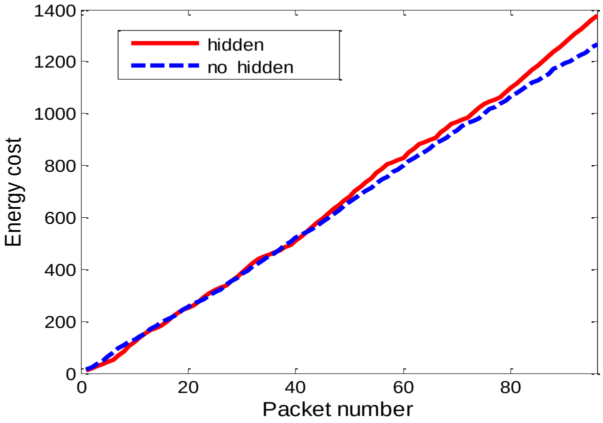


Figure 5. Comparison of Energy Consumption

As can be seen from the Figure 5, energy consumption of hidden information transmission almost the same as no hidden information transmission in the first half, and increases in the last half slightly. It related to the encoding rule and data to be transmitted. In this simulation, the middle part and the last part of hidden information have several 1 multiply, so that the node has to transmit information with maximum power continuously, which leads the increase of energy consumption. Sending more 0 in hidden information will make its energy consumption lower than no hidden information transmission. That is to say the network energy consumption depends on the original data, whether transmission hidden information has little effect on it.

5. Conclusion

With the development of food safety electronic food security sensor management, the food safety electronic food security sensor management for next generation can present integrated feature, modular feature, complicated feature and so on, which also has the characteristics with high degree of resource sharing, high degree of information fusion and highly intensive degree of software, compared with the independent type of food safety electronic food security sensor management. Each module of the integrated food safety electronic food security sensor management can share the interactive resources together and complete the common task together, therefore, the problem of information security has become one of the main challenges that it should face.

References

[1] C. B. Watkins, “Integrated modular avionics: managing the allocation of shared intersystem resources”, 25th digital avionics systems conference/ ieee/aiaa., vol. 8, **(2006)**, pp. 1-12.

[2] J. Graham, “Producing a safety case for ima blueprints. digital avionics systems conference”, dasc, vol. 24, **(2005)**, pp. 11-14.

[3] B. Ames, “Real-time software goes modular”, military & aerospace electronics, vol. 14, **(2003)**, pp. 24-29.

[4] J. Rushby and B. randell, “a distributed secure system,” ieee, computer, vol.16, **(1983)**, pp. 55-67.

[5] A. Proano, l . Lazos,. “Hiding contextual information in wsns”, ieee, international symposium on a world of wireless, mobile and multimedia networks, (wowmom) **(2012)**.

[6] J. Feng and M. Potkonjak, “Real-time watermarking techniques for sensor networks. spie security and watermarking of multimedia contents”, **(2003)**.

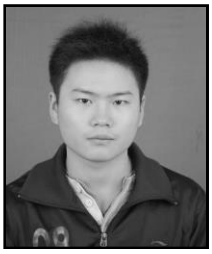
[7] J. R. Smith. and B. Jiang, “Id modulation: embedding sensor data in an rfid time series”, 7th information hiding **(2005)**.

[8] J.E. Kleider, S. Gifford, S. Chuprun and B. Fette, “Radio frequency watermarking for ofdm wireless networks”, icassp, **(2004).**

[9] R. Sion,. M. Atallah and S. Prabhakar, “Rights protection for discrete numeric streams”, ieee, transactions on knowledge and data engineering, **(2006)**.

[10] H. Wang, D. Peng, W. Wang, , H. Sharif, H.-H. Chen, “Energy-aware adaptive watermarking for real-time image delivery in wireless sensor networks”, ieee, international conference on communications (icc), **(2008)**, pp. 19-23.

Author



Zhehui Xiao, male, professor, mater tutor, Research direction: signal analysis and system integration.