Hindawi
Science and Technology of Nuclear Installations
Volume 2021, Article ID 6649649, 9 pages
https://doi.org/10.1155/2021/6649649

Research Article

Single-Vehicle Transportation Security System of Radioactive Materials Based on Group Relationship to Prevent Loss and Theft

Tiejun Zeng,[1,2] **Xiaohua Yang**,[1,3,4] **Yaping Wan**,[3,4] **Zhenghai Liu**,[4] **and Panpan Jiang**[1,4]

[1]*School of Nuclear Science and Technology, University of South China, Hengyang 421001, China*
[2]*School of Electrical Engineering, University of South China, Hengyang 421001, China*
[3]*CNNC Key Laboratory on High Trusted Computing, Hengyang 421001, China*
[4]*School of Computer, University of South China, Hengyang 421001, China*

Correspondence should be addressed to Xiaohua Yang; xiaohua1963@usc.edu.cn

Received 20 October 2020; Revised 9 March 2021; Accepted 18 March 2021; Published 31 March 2021

Academic Editor: Han Zhang; han-zhang@mail.tsinghua.edu.cn

For loss and theft in the transport of radioactive materials by a single vehicle, this article summarizes the characteristics of "illegal movement" and establishes a security system that senses its inter-relationship and responds though the group network relationship. The security system reminds the vehicle crew through on-site response and linkage response. A failure detection method for on-site response is proposed, that is, the push model is used first, and when the measurement results are suspected, the pull model is used to further confirm the failure. The failure detection for linkage response adopts the push model. According to the different security requirements of the basic and enhanced transportation, the principle of setting the timeout threshold in the failure detection algorithm is proposed. In the enhanced type, the value is smaller, otherwise the value is larger. A specific timeout threshold quantification scheme is proposed. Experiments show that the method proposed in this article is effective.

1. Introduction

According to statistics from the International Atomic Energy Agency (IAEA) [1], as of December 31, 2019, the database contained and confirmed the theft, loss, or unauthorized incidents of 3,686 nuclear or other radioactive materials reported and confirmed by participating countries. Among them, 189 occurred in 2019. Due to the long transportation distance, complex environment, and relatively weak security measures, the transportation process is more prone to the loss, theft, and destruction of radioactive materials than in fixed places [2]. For example, the CPN 503 device containing 50 mCi Am-241 was stolen from the truck parked in Visalia, California, at the night of July 03, 2020 [3]. A missing Type A package with a radiation warning label was found on the side of a highway near Gleichen, Alberta, Canada on April 19, 2018 [4]. It resulted in the closure of highway 901 until the source of transportation in the package was found. The Troxler 3440 portable package was lost during transportation between Toronto, Canada and Brampton, Ontario on the morning of Wednesday, May 17, 2017 [4]. A previously stolen truck containing the radioactive source Iridium-192 was found in Necadenas, Tabasco, southern Mexico, on April 16, 2015 [5].

Lost and stolen radioactive materials may cause radiation hazards to people or the environment on the one hand [6] and may be used to make nuclear explosive devices, which will cause greater damage on the other hand. Whether lost or stolen, the radioactive material has been illegally moved away enough. How to detect illegal movements, quickly locate and alarm, remind security personnel to respond [7], and become a key issue in the transport of radioactive material.

Radioactive materials in transportation are generally placed in packaging container [8]. Many radioactive materials are often put together during transportation, as shown in Figure 1. Swarm behavior is a common survival phenomenon in nature. It is the innate ability of

Figure 1: Transport of radioactive material (photo: IAEA).

gregarious biological groups to evolve over a long period of time, such as fish in the water, birds in the air, and bee colonies [9]. For the illegal movement of single or part of radioactive materials (or containers) away enough from the original group, the project team proposed the concept of swarm self-security intelligence [10] after the self-security intelligence of radioactive materials [7]. Security device is installed on the radioactive material container. Several radioactive materials (security devices on containers) constitute an interconnected group in network form. The swarm self-security intelligence system senses the existence of each radioactive material node in the system via the network and has the basic ability to deal with the destruction of the association relationship. As shown in Figure 2, the stolen or lost material will be far away from the group of remaining in the compartment, and the communication link with the security device is interrupted. Based on this, it is determined that the corresponding individual has separated from the group, that is, moved illegally.

Since the group relationship is realized through the network, it is very important to improve the antideception attack ability of the network. Due to the vulnerability of vehicle position detection sensor, deception attack against its position information will become possible. An attack detection and estimation scheme for a local vehicle in vehicle platooning based on a modified UFIR estimator is proposed [11]. The experimental results show that the scheme is effective. A modified generalized likelihood ratio (GLR) algorithm is proposed to detect and estimate the sensor deception attacks based on the distributed Kalman filter [12]. The effectiveness of the proposed algorithm is verified by simulations.

From the perspective of the remaining group response, this paper studies the algorithm of identifying individuals who have moved illegally and thus is lost or stolen and then establishes a single-vehicle transportation security system in which the alarm sounds inside the carriageriage, on the cab, and on the portable electronic equipment. If there is only one radioactive substance in the carriageriage, an additional security device can be arranged on the inner wall of the carriageriage, and then, a group network can be formed. Therefore, the method proposed in this paper is not only suitable for the safe transportation of multiple radioactive substances but also suitable for the transportation of a single radioactive substance.

2. Single-Vehicle Transportation Security System of Radioactive Materials Based on Group Relationship to Prevent Loss and Theft

2.1. Security System Design. The single-vehicle transportation security system of radioactive materials in this paper only realizes the identification of illegal movement of radioactive material through group relations (i.e., the network) and alarms. The security device with self-security capability on the radioactive material (container) is called a wireless node, as shown in Figure 3. There are wireless nodes 1, radioactive material (container) 1, radioactive material (container) 2, radioactive material (container) 3, a host computer, and LCD (liquid crystal display) which is arranged in the front of the vehicle. Every person (including the driver) is equipped with a portable terminal. Wireless node 1, radioactive material (container) 1, radioactive material (container) 2, and radioactive material (container) 3 form a network, which perceives each other's existence through failure detection of the communication link (corresponding lost or stolen).

Due to the existence of the wireless node 1, this method is effective even if only a single radioactive material (container) is transported. A small hole is opened in the carriageriage near the front of the vehicle, and the wireless node 1 is connected to the host in the front of the vehicle through a wired cable or optical fiber. The wireless node 1 is installed on a specific occasion (a place that is not easily damaged), and only the antenna for wireless communication is leaked out of the compartment. The host sends the stolen or lost information to the LCD and portable terminal to remind the vehicle personnel to deal with it.

2.2. Illegal Mobile Identification and Response Logic

2.2.1. Illegal Mobile Identification Logic. The lost or stolen radioactive material has been illegally moved away enough from the group. Illegal movement includes two elements: "illegal" and "movement." "Moving" means that the radioactive material has deviated from its original location. From the perspective of theft and loss, it should be far away from the original radioactive material group. When far enough away, the radioactive material will lose communication with the network composed of the remaining nodes (that is, communication failure). Damage to the security device makes it unable to communicate with other remaining nodes. It can also be considered as "communication failure." "Illegal" judgment logic: divide all nodes into "alert state" and "nonalert state." If "moving" is detected in the alert state, it is illegal. If "moving" is detected in the "nonalert state," it is not. The "nonalert state" is mainly used for the normal movement of radioactive materials, such as the process of moving all radioactive materials to the carriageriage.

2.2.2. Response Logic. Lost or stolen radioactive materials are radioactive. They will endanger human health and cause social panic, so we need to find and recover in time. Once illegal movement (lost or stolen) occurs, the remaining network nodes will alarm and respond. The remaining

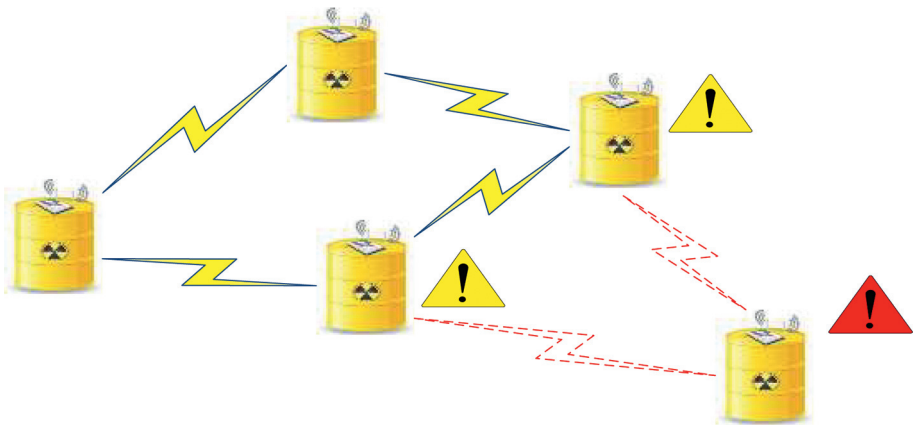

Figure 2: Schematic diagram of group perception and response.

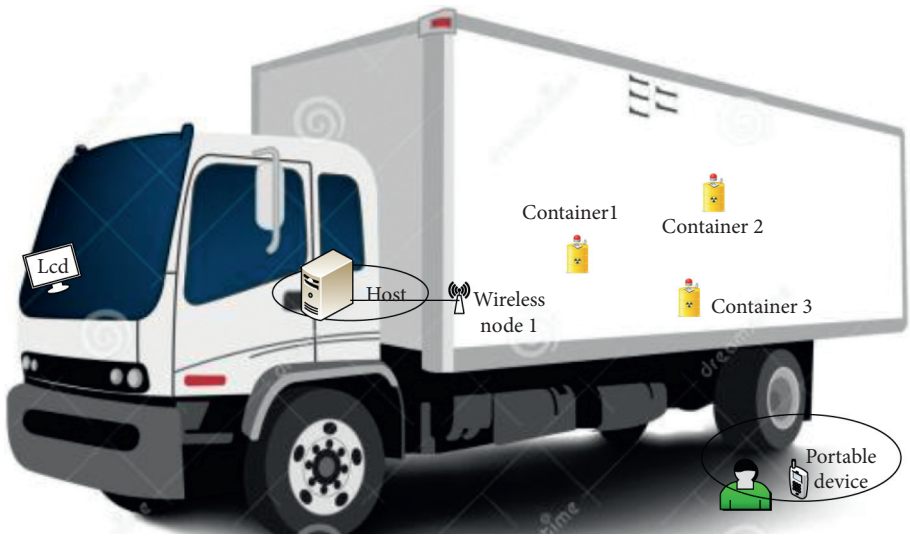

Figure 3: The single-vehicle transportation security system of radioactive materials.

network nodes remind the relevant personnel on duty through on-site response and linkage response to detect theft and loss and retrieve radioactive materials.

2.2.3. On-Site Response. When a certain radioactive material node is illegally moved and loses contact with the remaining nodes, the node that was directly connected to the moved node will give an audible and visual alarm in the compartment. In the nonenclosed compartment, the sound and light alarm can directly remind the personnel accompanying the vehicle.

2.2.4. Linkage Response. The remaining node will report the loss of connection information to the host. Display this information on the LCD, and transmit it to the portable terminal carriageried by vehicle personnel to help find the lost or stolen radioactive material. The alarm signal can also be sent to the monitoring center of the external security system through the external communication system.

2.2.5. Information Security. Since the security function of the radioactive material group is realized through the network, the adversary may attack the network. The adversary may intercept the information on the network and make changes, deliberately adding some data that is beneficial to him, such as changing the information to deceive the group network. The adversary has mastered the communication rules, and may inject illegal information into the network and damage the operation of the central node. For this reason, it is necessary to ensure the information security of the group network and perform identity authentication. First, encrypt the transmitted communication data. Fix a public key on all nodes, and after the network is established, determine a key to prevent the plaintext from being stolen.

Secondly, each node is set with a unified ID to identify, and unauthorized ID node cannot join the network.

3. Failure Detection Model and Algorithm

3.1. Reliability Analysis of Group Network Connection. For the convenience of analysis, taking the star network shown in Figure 4 as an example, an on-site response failure detection model and a linkage response failure detection model are proposed. The network in Figure 4 is divided into 3 layers (the actual network may be greater than 3 layers): the third layer is the end layer, the second layer is the middle layer, and the central node of the first layer is directly connected to the upper computer. When a node (such as node (3) is too far away from the group that it loses communication with the group, it shows that the communication with the node (such as node (2) that directly communicates with it is interrupted. For on-site response, node 2 can detect the loss of connection and issue an audible and visual alarm. For linkage response, it is necessary to let the vehicle crew find that the node 3 loses connection, that is, node 1 finds that node 3 is disconnected.

The process of direct communication between two adjacent wireless nodes is shown in Figure 5. The heartbeat message sent by the process p of the application layer of node 2 is sent from the physical layer after being converted by the software protocol layer. It is then transmitted to the physical layer of node 1 in the form of a radio signal. After receiving the data, the physical layer of node 1 transmits the data to the process FD of the application layer via the software protocol layer.

The causes of communication packet loss between two wireless nodes include electromagnetic interference, heartbeat packet conflict, and hardware failure. The heartbeat packet makes an error due to electromagnetic interference during wireless channel transmission. The physical layer of the receiving node finds that the heartbeat information is incorrect and discarriaged it. The heartbeat information is sent by multiple nodes to a parent node conflicts and is lost. Radiation and other reasons may cause hardware failures of some nodes, causing them to fail to send heartbeat information and detect packet loss. In general, the stronger the electromagnetic interference, the more the child nodes connected to a parent node, and the greater the radiation, the greater the probability of heartbeat message loss.

The causes of communication packet delay between two wireless nodes include packet loss, physical layer buffering, and software protocol conversion.

The total delay tdelay can be expressed as

$$t_{\text{delay}} = t_{\text{chgs}} + t_{\text{link}} + k * t_{\text{chgr}} + t_{\text{lost}}, \quad (1)$$

where t_{chgs} is the time when the sender's heartbeat information is converted from the application layer to the physical layer, t_{link} is the time the data is transmitted in the air, it can basically be ignored, k is the number of child nodes connected to the detection node, t_{chgr} is the time when the receiver's heartbeat information is converted from the physical layer to the application layer, And t_{lost} is the delay caused by packet loss. The more the packets lost, the longer the buffer delay, and the greater the message protocol conversion delay, the greater the total delay.

3.2. Failure Detection for On-Site Response. Since the network node installed on the radioactive material container during transportation is powered by battery, energy saving is one of the constraints of the disconnection detection algorithm. The adaptive failure detector [13] that has been proposed currently requires a sliding window to store heartbeat messages and a large number of calculations about detection parameters and probability distribution model parameters in each detection cycle. These storage costs and computational costs have a serious impact on the energy consumption of nodes, and they become more serious as the number of detection nodes increasing. Therefore, the traditional failure detector is not suitable for this project scenario. It is necessary to study new failure detection models and algorithms.

In the failure detection method based on the PUSH model (in Figure 6), the detected node is an active participant. The detected node p periodically sends an "I am alive" heartbeat message to the failure detector FD. If the failure detector FD does not receive the heartbeat message sent by p before the timeout threshold Δtr, it is suspected that the detected node p has failed. The PUSH model is a unidirectional message transmission, which can achieve higher transmission efficiency. As in Figure 4, the node 3 is the detected node, and node 2 is the failure detector. When there many child nodes connected to node 2 or other reasons cause long delay, the model will fail.

In the failure detection method based on the Pull model (in Figure 7), the detected node is a passive participant. The failure detector FD periodically sends a "are you alive?" heartbeat message to the process p of the detected node. Process p will reply "yes" if it receives the heartbeat message, otherwise not reply. Since the Pull model is bidirectional message transmission in the system, the communication volume will be twice that of the push model. When the number of nodes in the swarm network is large, the increase in the amount of communication will lead to an increase in energy consumption.

In order to improve the accuracy of the disconnection judgment and reduce the misjudgment caused by packet loss, the model proposed in this paper is shown in Figure 8. First, use the Push model to make a preliminary judgment. If a suspected result is obtained, the pull model will further confirm the loss of connection. When multiple child nodes send heartbeat information to a parent node at the same time, the heartbeat information will conflict and cause packet loss. In order to reduce the occurrence probability of this phenomenon, a random time is added to the sending time interval of each child node. The time interval $\triangle$ts for sending heartbeat messages is composed of timing (relatively long) + random time (relatively short), such as a random time within 1s + 50 ms.

As in Figure 4, node 3 sends a heartbeat message "I am alive" at a time interval $\triangle$ts normally. When node 2 cannot

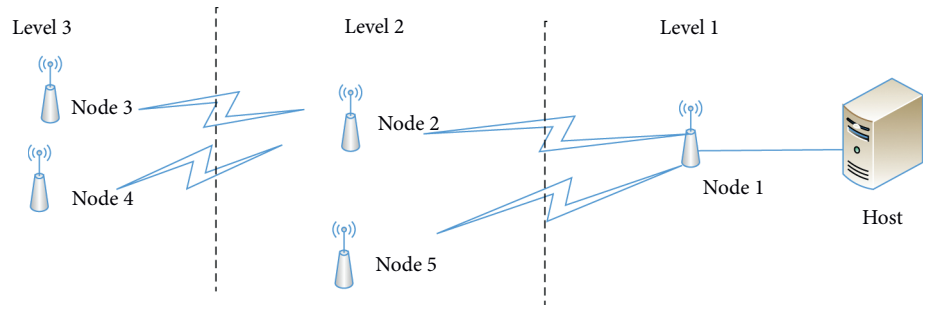

Figure 4: Radioactive material group network with the star structure.

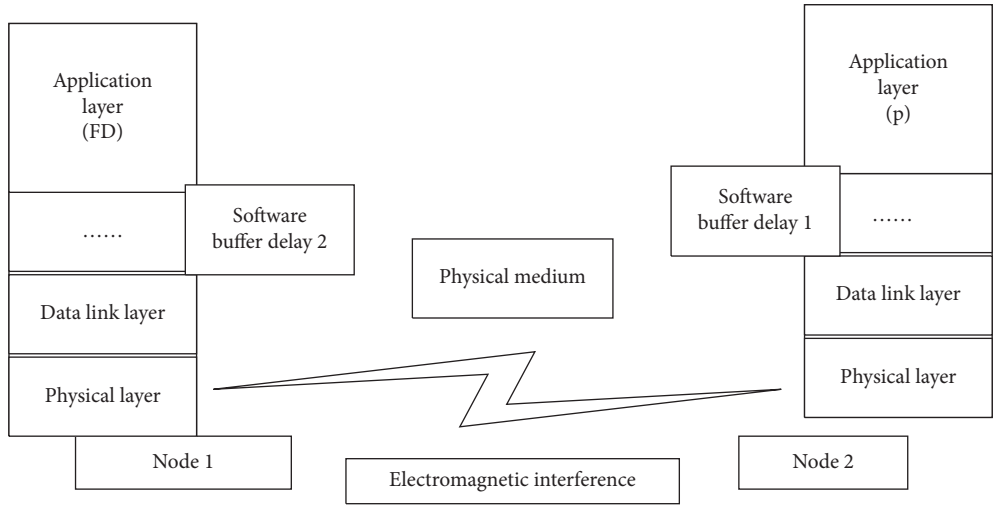

Figure 5: Communication between two wireless nodes.

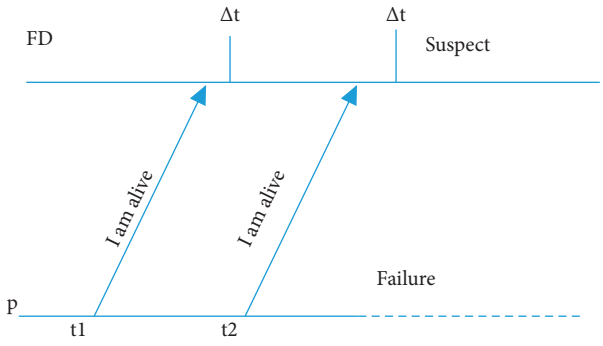

Figure 6: Push model.

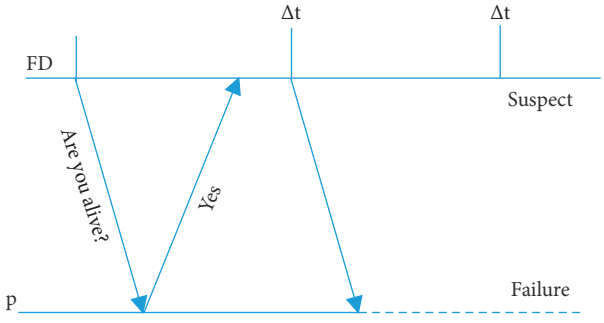

Figure 7: Pull model.

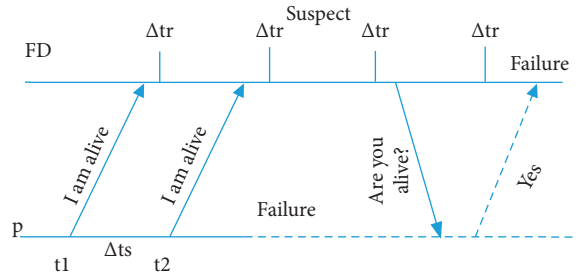

Figure 8: Push-pull failure detection model.

detect the heartbeat message this time, it sends a heartbeat message "are you alive?" to node 3. If the reply message "yes" or the heartbeat message "I am alive" from node 3 is received in the next $\triangle$tr time, the node 2 will return to the normal state, otherwise be judged as invalid.

The adaptive failure detector generally adapts to the changes in the network environment by adjusting the heartbeat message sending interval Δts and the timeout threshold Δtr, so as to improve the detection accuracy under a certain detection speed constraint. Failure detection effectiveness (accuracy and speed) and network load are contradictory. The heavier the network load, the longer the communication delay. The smaller the timeout threshold Δtr

is set, the faster the detection speed and the lower the detection accuracy.

When the activity of the exposed radioactive material is greater than the D value specified by literature [8, 14, 15], it may cause the death of the exposed person or permanent damage to the quality of life of the person. For radionuclides that are not included in the Code of Conduct [15], the traditional transportation safety A value derived from traffic accident scenarios is used to specify the activity threshold. This article considers the "per package" method to specify the transport safety level of radioactive materials. According to the D value and A value, three transmission security levels are determined: prudent management practice, basic transportation security level, and enhanced transportation security level. The latter two require special security measures. The enhanced transport safety level requires the highest level. Once leaked, as analyzed above, the probability of causing the security device to fail is higher. Due to the high importance of the enhanced transportation, the timeout threshold Δtr can be set to be smaller, the detection speed is fast, and the detection accuracy is low. This may result in certain false alarms, but it can reduce missed alarms, thereby reducing the probability of loss or theft. The timeout threshold Δtr in the basic transportation can be set a little larger, the detection speed is slow, and the detection accuracy is high.

The timeout threshold for the ith judgment proposed in on-site response failure detection in this paper is t_{ri}, as shown as

$$t_{ri} = \begin{cases} E(D)_i + SM_i, & E(D)_i > \Delta t_{s\max}, \\ \Delta t_{s\max}, & E(D)_i \le \Delta t_{s\max}, \end{cases} \tag{2}$$

where $E(D)_i$ is the adaptive timeout prediction, and its specific expression is as formula (3), SM_i is the security boundary, and its specific expression is as formula (4), and $\Delta t_{s\max}$ is the maximum in data transmission interval, and this article uses $1\text{s} + 50\text{ ms} = 1050\text{ ms}$。:

$$E(D)_i = \max\left(d_{i-1}, d_i\right), \tag{3}$$

where d_{i-1} is the interval between the i-1th data transmission and reception andd_i is the interval between the ith data transmission and reception.

$$SM_i = \begin{cases} t_{\text{chgs}} + k * t_{\text{chgr}} + \Delta t_{\text{srdmax}}, & \text{basic}, \\ t_{\text{chgs}} + k * t_{\text{chgr}}, & \text{enhanced}, \end{cases} \tag{4}$$

where k, t_{chgs}, and t_{chgr} Their meaning is as formula (1). Δt_{srdmax} is the total communication time for a data transmission, and the reception is equal to Δt_{smax}, Consider 1050 mS. In zigbee network [16], the typical value of t_{chgs} can be 0.58 ms, and the typical value of t_{chgr} can be 0.55 ms.

3.3. Failure Detection for Linkage Response. The linkage response failure detection adopts the push model, and the child node sends heartbeat information to the parent node. After receiving the heartbeat message "I am alive," the parent node forwards it to the central node 1. The node 1 forwards the information to the host via the wired network. The host performs failure detection on each node. The result of the detection is displayed on the LCD as a network topology diagram. When the node is normally connected, it flashes continuously in the topology diagram. It does not flash when the communication link is suspected of failure. It disappears from the topology diagram when the failure is confirmed.

The timeout threshold t_{ri} for the ith judgment proposed in the linkage response failure detection is shown as

$$t_{ri} = \begin{cases} E(D)_i + SM_i, & E(D)_i > \Delta t_{s\max}, \\ \Delta t_{s\max}, & E(D)_i \le \Delta t_{s\max}, \end{cases} \tag{5}$$

$$E(D)_i = \max\left(d_{i-1}, d_i\right), \tag{6}$$

$$SM_i = \begin{cases} n * t_{\text{chgs}} + (n-1) * k * t_{\text{chgr}} + \Delta t_{\text{srdmax}}, & \text{basic}, \\ n * t_{\text{chgs}} + (n-1) * k * t_{\text{chgr}}, & \text{enhanced}, \end{cases} \tag{7}$$

where n indicates the number of layers of network nodes, as shown in Figure 4, $n = 3$. The meaning of other related parameters is the same as formulas (2)–(4).

4. Test Analysis and Discussion

We built a 6-node zigbee network for experimentation in a carriageriage. The internal dimensions of the carriageriage compartment: $3600 \times 1900 \times 1850$ (mm). The height of the compartment from the ground is 920 mm. The zigbee network includes 1 coordinator node and 5 router nodes, as shown in Figure 9. The node hardware is shown in Figure 10. The node includes a zigbee module, antenna, buzzer, and backplane. The zigbee module is responsible for sending and receiving data via the antenna. The buzzer can realize local alarm. The backplane module is used to supply power and connect the zigbee module and the buzzer. The typical output power is set for -12dbm in cc2530.

The main purpose of our experiment is to verify whether the zigbee node can be identified when the communication is interrupted due to the distance from the original group and how far away can it be detected (that is, find the critical distance for communication failure). A person takes a zigbee node and exits from the carriageriage and stays away. This behavior simulates the loss or theft of the radioactive material container with the electronic equipment from the compartment. Since the left and right sides of the carriageriage are symmetrical, the two directions are theoretically the same, so the situation of moving away from the left is not specifically simulated. Among them, the situation where the zigbee node moves away from the rear of the carriage is shown in Figure 11. When the node is far away from the original zigbee network and the communication fails, the wireless zigbee node originally connected to the node will give an alarm via a buzzer. The upper computer connected with the coordinator node will display the network topology after failure detection. Figure 12 is a topology diagram when the node is not lost or stolen. Figure 13 is the

Figure 9: Zigbee nodes arranged in the carriageriage.

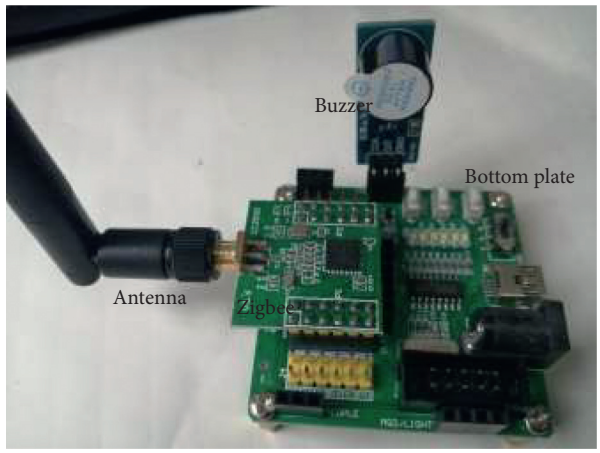

Figure 10: zigbee node.

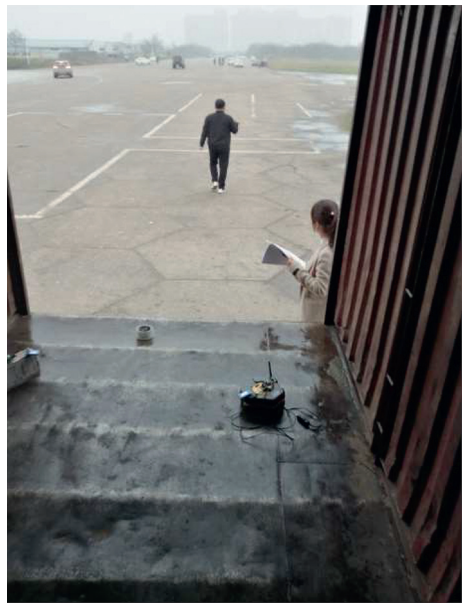

Figure 11: Movement of a single zigbee.

network topology after a single zigbee node is lost. According to the changes in the topology map, not only can it be identified whether the radioactive material (container) is lost or stolen but also which radioactive material (container) can be located. The test results are shown in Table 1.

Since the carriage is a steel-metal enclosed structure, the door faces the rear of the carriage; when a single node reaches the front of the carriage, the network signal is blocked, so communication basically fails. In the test on the right side of the carriage, the person holding the zigbee node starts from the middle of the right side of the carriage and walks straight away to

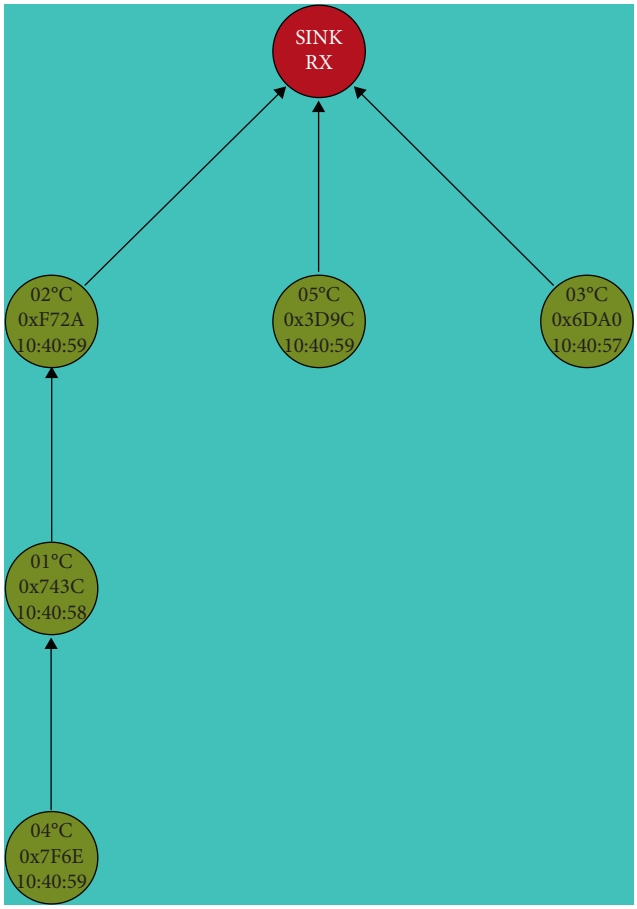

Figure 12: Network topology before a single zigbee node is lost.

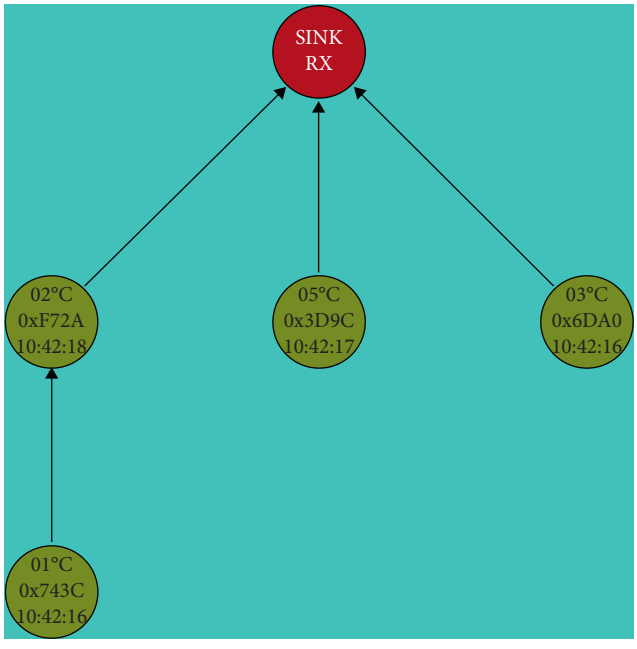

Figure 13: The network topology after a single zigbee node is lost.

the right. Tests have shown that the farthest failure distance in this direction is 7.5 meters. On the rear side of the carriage, because the door is open, the critical distance of failure is farther than the right side, and the farthest distance is 26 meters.

Table 1: Test results.

	Failure alarm distance (unit: meter)									
	1st	2st	3st	4st	5st	6st	7st	8st	9st	10st
Front of the truck	0	0	0	0	0.5	0	0	1	0	0
Right of the truck	14.6	15.6	17	15	15.8	16.5	16.8	15.5	14.8	18
Rear of the truck	22	23.5	24	23	26	26	25	24	24	22.5

5. Conclusions

This article establishes a security system that senses radioactive materials inter-relationship and responds though the group network relationship. When an illegal movement causes loss or theft, the remaining network nodes will alert the vehicle crew through on-site response and linkage response. According to the characteristics of network battery power supply, the reasons for communication packet loss and communication delay between two wireless nodes are analyzed. In order to improve the accuracy and reduce the misjudgment caused by packet loss, this paper proposes an on-site failure detection model: first, use the Push model, and when the measurement results in doubt, the pull model will further confirm the loss of connection. Both the basic transportation safety level and the enhanced transportation safety level require special security measures. The enhanced transportation safety level requires the highest level. In combination with the level of security requirements for the transmission of radioactive materials, it is proposed that the enhanced transportation safety level sets the timeout threshold to be smaller, and the basic type can be set to be larger. A specific quantitative plan is proposed. Experiments show that the scheme proposed in this paper is effective.

Through failure detection to judge the interruption of communication, the loss or theft of radioactive materials can be sensed. However, when the communication is interrupted, the radioactive material may be far away from the transportation means, and the response time will be delayed. The next step is to study the positioning algorithm of the wireless nodes in the carriage. When a certain node is beyond a certain distance from the original network node, it will alarm so that the sensitivity and speed of response can be proposed.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declared that there are no conflicts of interest regarding this publication.

Acknowledgments

This paper was funded by China's 13th Five-Year Nuclear Energy Development Project "Individual Self-Security Intelligence of Radioactive Material."

References

[1] Iaea Incident and Trafficking Database (ITDB): Incidents of Nuclear and Other Radioactive Material Out of Regulatory Control 2020 Fact Sheet.

[2] Y. Pan, F. Cao, and Z. Hong, "The study of building national online monitoring platform for transport of category I and II radioactive," *Material. Progress Report on China Nuclear Science & Technology*, vol. 5, pp. 351–360, 2017, [in Chinese].

[3] T. Zeng, X. Yang, Y. Wan et al., "Vehicle transport security system based on the self-security intelligence of radioactive material," *Science and Technology of Nuclear Installations*, vol. 2020, Article ID 3507167, 7 pages, 2020.

[4] https://nuclearsafety.gc.ca/eng/acts-and-regulations/event-reports-for-major-nuclear-facilities/event-reporting/transport-intransit-events.cfm?pedisable=true.

[5] https://www.bbc.com/news/world-latin-america-32332271.

[6] Code of Conduct on the Safety and Security of Radioactive Sources IAEACODEOC2004.

[7] X. Yang, J. Hu, Y. Wan et al., "Swarm self-security intelligence of radioactive substances," *Nuclear Safety*, vol. 6, pp. 1–5, 2019.

[8] T. A. Przylibski, "Assessment of occupational exposure from radon in the newly formed underground tourist route under Książ castle," *Poland Radiation and Environmental Biophysics*, vol. 2021, Article ID 33742235, 17 pages, 2021.

[9] Z.-bin Fijałkowska-Lichwa, *Dynamic Modeling, Stability Analysis and Simulation on Collective Behavior of Intelligent Swarm Systems[D]*, University of Technology, Lanzhou, China, 2012.

[10] X. Yang, T. Zeng, Y. Wan et al., "Self-security intelligence of individual radioactive substance," *Nuclear Safety*, vol. 18, no. 02, pp. 43–48, 2019, in Chinese.

[11] Z. Ju, H. Zhang, and Y. Tan, "Deception attack detection and estimation for a local vehicle in vehicle platooning based on a modified UFIR estimator," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3693–3705, 2020.

[12] Z. Ju, H. Zhang, and Y. Tan, "Distributed deception attack detection in platoon-based connected vehicle systems," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 4609–4620, 2020.

[13] J. Liu, *Research on Qos-Oriented Failure Detection Service in Distributed Systems*, Harbin Institute of Technology, Harbin, China, 2018, in Chinese.

[14] IAEA, *NSS 26G: Security of Nuclear Material in transport*, Vienna, Austria, 2015.

[15] IAEA, *NSS 9-G (Rev. 1): Security of Radioactive Material in Transport*, IAEA, Vienna, Austria, 2020.

[16] http://www.ti.com/lit/an/swra292/swra292.pdf.