Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Modeling and Analysis of Network Direct Reporting Security of Infectious Diseases based on Wireless Communication Technology

Yanling Zhang (jzdxzyl@163.com)
Jiaozuo University
Ting Zhang
Jiaozuo University

Research Article

Keywords: wireless communication technology, infectious diseases, epidemic network, direct epidemic reporting, security model

Posted Date: May 4th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-457692/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Modeling and analysis of network direct reporting security of infectious diseases based on wireless communication technology

Yanling Zhang *, Ting Zhang
College of Information Engineering, Jiaozuo University, Jiaozuo, 454000,China
jzdxzyl@163.com

Abstract: In order to solve the problem of low security in the process of direct reporting of traditional infectious diseases, the corresponding network direct report security model is established by wireless communication technology. According to the network structure of infectious diseases, the transmission path of the information of direct report of epidemic situation is determined, and the data of direct report of epidemic situation is obtained by wireless communication technology. On this basis, the security risk level of wireless communication network is divided. This paper analyzes the negative factors that affect network security from hacker attack, high risk vulnerability of software and user information tampering. Combined with the analysis results of multiple security mechanisms of the direct report network of infectious diseases, the quantitative evaluation of network security is realized, that is, the modeling and analysis of the network direct report security of infectious diseases is realized. Compared with traditional security model, it is found that the network direct report security model can reduce the loss and error of infectious disease data, which has a high application value.

Keywords: wireless communication technology; infectious diseases; epidemic network; direct epidemic reporting; security model;

0 Introduction

The network direct report of infectious disease epidemic situation is to build an information platform by comprehensively using computer technology, network technology and communication technology. It realizes the real-time report, dynamic monitoring and real-time statistics of infectious disease cases from the grass-roots level to the country, and improves the timeliness and accuracy of infectious disease report. The network direct reporting system is an information system composed of medical and health institutions and Internet based VPN system, which can collect, audit, store, process, maintain and use the disease monitoring case information in real time. It can dynamically monitor the occurrence and development of the epidemic situation, and implement case management and analysis of the monitoring results. Starting from the overall situation to assist prevention and control decision-making, the use of monitoring information to develop prevention and control measures to help disease prevention and control institutions achieve disease control objectives [1]. China's notifiable infectious disease reporting and feedback system was established in the 1950s. The network direct reporting of infectious diseases has realized the network direct reporting of medical institutions based on case reports of infectious diseases. Many problems have been solved, such as timely report and correction of epidemic situation, routine monitoring and emergency early warning, automatic early warning and prediction of monitoring results, spatial distribution and analysis of monitoring data, and epidemic situation report management of floating population. It plays an extremely important role in further strengthening the prevention and treatment of major diseases, strengthening early warning and prediction, decision-making of disease control and allocation of health resources.

With the continuous expansion of the content and scope of the direct report of infectious diseases network, the security of the direct report information of infectious diseases network is

seriously threatened. Therefore, the model of the network direct report security of infectious diseases is established to analyze and evaluate the network security. The traditional network security model is based on static open-loop control network protection, which does not adequately describe and respond to dynamic network security threats and system vulnerability [2]. However, the traditional static network security model improves the threshold of hacker attack success, which can block most of the attacks, but it can penetrate the barrier of static network security technology, which will cause great harm to the system. The defense capability of static network security component is fixed and cannot change with the change of environment, while the attack capability of attack is constantly improved. In the initial stage of installation, the defense capability of security components is greater than that of hackers, but as time goes on, the attack capability of hackers will eventually exceed that of security components. In a word, the traditional static network security model is not enough to solve the existing security threats, and can not build an effective network security protection system. In the face of the increasingly popular distributed and collaborative attacks, the defense capability of any single security component is limited. Only when the security components interact effectively and form a dynamic overall security model, can they carry out effective detection and protection.

In order to solve the problems of the traditional network direct reporting security model of infectious diseases, the wireless communication network is applied to realize the optimization design of the network direct reporting security modeling method. Wireless communication technology is a means of information exchange by using the characteristics of electromagnetic wave signals can be spread in free space. The current popular wireless communication technologies include Bluetooth, CDMA2000, GSM, Infrared (IR), ISM, RFID, UMTS / 3GPPW / HSDPA, UWB, WiMAX Wi-Fi and ZigBee. The applicable frequency band, modulation mode, maximum operating distance, data rate and application field of various wireless communication technologies. The relationship between the operating distance and the data rate of these wireless communication technologies, the higher the data rate, the shorter the operating distance. It can extend the range and keep the data rate. Through the application of wireless communication technology, it provides technical support for the direct reporting of infectious disease information, and improves the transmission rate and security of epidemic information to a certain extent.

1 Design of network direct reporting security model of infectious disease epidemic situation

From the perspective of the whole and development, security needs, security system should be a dynamic cycle of the system, can constantly self-improvement and optimization to adapt to new changes and development needs [3]. Combined with the characteristics of direct reporting of infectious diseases, the security modeling of direct reporting of infectious diseases is realized under the principles of integrity, concentration, hierarchy and long-term.

1.1 Analysis of network architecture of epidemic situation of infectious diseases

The wireless direct report network of infectious diseases usually randomly scatters the number of sensor nodes from hundreds to thousands to the target area. Nodes can form a wireless network through rapid self-organization. All sensor nodes not only need to complete the collection and processing of information, but also undertake the routing of information. The collected data will reach the convergence node through multi hop routing [4]. The convergence node is a special node. Since it can communicate with other nodes in WSNs, it can communicate with external network system by means of Internet or wireless network. Because of the limitation of its own volume, price and energy supply, the nodes have short communication distance, so they can only

exchange data with neighbors in their communication range. The node must communicate with nodes outside the communication range by multi hop routing [5]. In order to make the data collected by the nodes of the network can be sent to the sink node smoothly, the distribution density of nodes is usually required to be large. The typical architecture of wireless sensor network is shown in Figure 1.

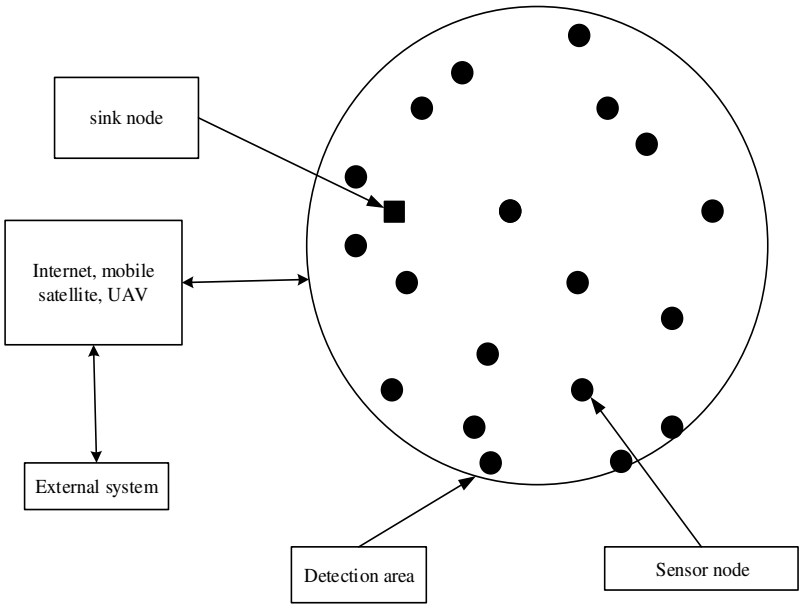


Figure 1 Network architecture of wireless direct reporting of infectious diseases

The sensor node is composed of data acquisition unit, data processing unit, data transmission unit and energy supply unit. The data acquisition unit group is responsible for the data conversion and information collection in the monitoring area, which can be data information such as light intensity, humidity, temperature and atmospheric pressure. The main tasks of data processing unit include processing operation, location, synchronization, routing protocol, task management and data fusion of control node. The main function of data transmission unit is to exchange control messages with other nodes, wireless communication and data collection. The energy supply unit is composed of various micro batteries, which can reduce the volume of sensor nodes.

1.2 Using wireless communication technology to collect and process the direct report data of epidemic situation

In the network architecture of infectious diseases, the direct report data of infectious diseases are obtained by principal component analysis. Information acquisition is basically realized by logging, traffic information or original IDS alarm collection. Through the detection and replication of real-time transmission data, the information of infectious diseases epidemic situation can be obtained [6]. The processing process of direct epidemic reporting data is the classification and fusion process of initial data. The eigenvector matrix of class i data is defined as M_i, and the relation matrix between the eigenvector of class i system state and the data eigenvector of undirected graph model at a certain network level is constructed by calculating the similarity relation r_{ij} between the sub vectors in matrix M. r_{ij} is calculated as follows:

$$r_{ij}=\frac{\sum_{k=1}^{m}\min\left(M_{ik},M_{jk}\right)}{\sum_{k=1}^{m}\max\left(M_{ik},M_{jk}\right)} \quad (1)$$

The matrix r in formula 1 satisfies reflexivity and symmetry. In order to classify the target eigenvectors by fuzzy analysis method, the square method is used to transform the matrix R into the transitive closure matrix $\hat{R}$. $\hat{R}$ is the fuzzy equivalent matrix of data analysis. Taking $\max\left\{\beta_i\right\}$ as the reference point, the calculation method of uncertainty support is as follows:

$$o=1-\max\left\{\hat{r}_{12},\hat{r}_{12},\mathrm{L}\ ,\hat{r}_{12}\right\}=1-\max\left\{\beta_i\right\} \quad (2)$$

In the formula, $\hat{r}_{ij}$ is the row vector in the matrix, and β_i represents the threshold of the target to be identified as the target [7]. Therefore, the basic probability allocation for target θ is as follows:

$$m_k\left(i\right)=\frac{\beta_{ki}}{\sum_{i=1}^{n}\beta_{ki}+o_k\left(i\right)} \quad (3)$$

After getting the basic probability distribution value according to the fuzzy equivalence matrix, it is necessary to use Dempster evidence combination theory to calculate the combination and comprehensive confidence of the evidences, so as to classify them according to the calculation results of formula 3. Finally, the data belonging to the same type are used to obtain the processing results of direct reporting data of infectious diseases.

1.3 Classification of wireless communication network security risk level

In order to analyze the security risk of a wireless communication network, we should first analyze the number of alarms, the number of backdoors implanted in the wireless communication network, the number of attacks, and the number of existing network security vulnerabilities. These indicators can be analyzed by using the least squares vector machine algorithm of computer technology, and the data of these security risk indicators can be collected as indicators [8]. The security risk level of wireless direct reporting communication network of infectious disease epidemic situation is divided into five kinds, and the five kinds of security analysis levels are very low G, low F, middle lower E, middle D, middle upper C, high B, and very high A. The evaluation comes from the relevant calculation and analysis, and experts judge according to the corresponding indicators of each grade. In view of the security risk of wireless direct reporting network under the epidemic situation of infectious diseases, the training sample set is selected according to a certain proportion of samples. The training sample set is used to analyze the security risk of wireless communication network, and the samples are used to test.

1.4 Factors affecting network security of infectious diseases

According to the attacker's network location and network state, it can be divided into two kinds of attack models: external attack and internal attack. External attack often refers to

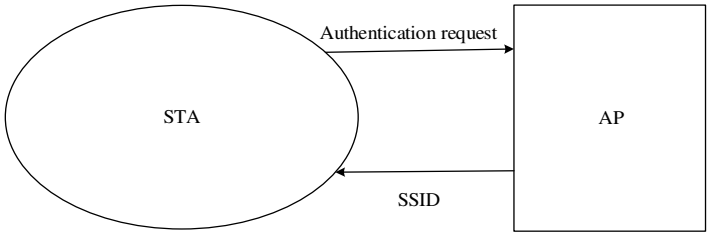
eavesdropping attacks through the link layer between data nodes and obtaining sensitive privacy data. The internal attack often refers to the attack on a node in the WLAN to obtain the secret information stored on the node and the related network configuration parameter information. After the node is captured successfully, the attacker takes this as a springboard to further obtain more privacy sensitive data of the whole network [9]. At present, hacker attacks, high-risk vulnerabilities in network and software, user information tampering, leakage and illegal transmission are the three main factors affecting the network security of infectious disease epidemic. The basic working principle of hackers is to collect the information in the network system, detect each host on the target network according to the information, seek the internal security vulnerabilities of the system, and establish a simulation environment for network attacks. The general attack methods of hackers are: planting Trojans, worms and fabricating false programs into the computer, at the same time, spying on the network data packets, obtaining different user accounts and passwords and other relevant user information, and tampering with them, resulting in problems such as the user's information error, and bringing malignant consequences to computer users. High risk vulnerabilities in computer network and software, including the lack of computer network security design, problems in the design of computer system and application software system, lead to illegal users logging in to other users' computer systems without formal permission for malicious control [10]. The existence of these high-risk vulnerabilities can cause the user's data and information can not be successfully communicated and obtained. High-risk vulnerabilities can make the user's computer subject to network attacks or tracking, bad impact, leading to network information insecurity. User information tampering refers to the interception of user information and illegal changes to the data, resulting in the final information error. User information disclosure refers to the remote control or monitoring of user information. Illegal transmission of user information refers to the illegal transmission of user information without operation. The above factors are the negative factors of the direct reporting network of infectious diseases, and network encryption technology, identity authentication technology, firewall and routing program play a positive role in protecting network security.

1.5 Analyze the security mechanism of each layer of infectious disease epidemic network

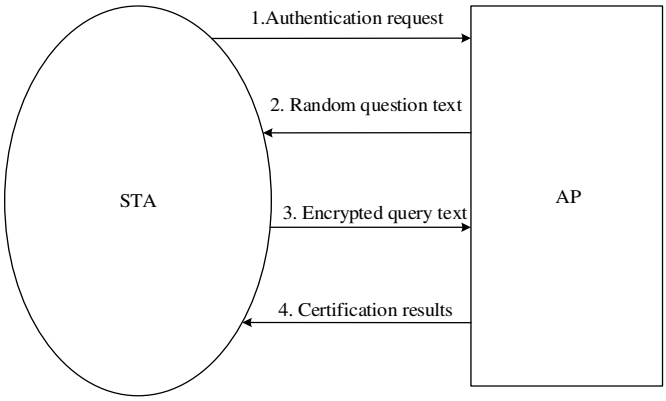
1.5.1 Two way identity authentication mechanism

Bidirectional authentication is a necessary way to connect wireless network, that is to say, any user needs to carry out authentication before accessing wireless network. Under IEEE802.11 standard, there are two kinds of authentication keys: open and shared. The authentication settings must match the communication settings parameters. Open wireless network identity authentication is a relatively simple authentication mechanism: open system is an empty authentication mechanism, which is actually the default authentication method of IEEE802.11 [11]. The authentication process needs to go through two processes: first, the authentication site sends the identity authentication request information to the AP; then, after receiving the request information from the STA, the AP needs to send the confirmation information to the STA according to the authentication situation. If this process is successful, then the authentication process is SSID. Shared key authentication is to authenticate the users of the shared key site. In authentication, authentication is realized by ciphertext transmission. In the shared key authentication, WEP technology is still used for encryption. The specific authentication process is as follows: first, the authentication site sends the authentication request information to the AP; then, after receiving the request information from the STA, the AP sends a 128 byte confirmation information to the STA

according to the authentication situation [12]. The initial vector IV and the shared key K form the key through certain calculation, and then can be extended to pseudo-random bit "key stream". The length of IV in WEP is 24 bits. The use of WEP technology provides great convenience for the security of wireless network. It can establish security protection with the same security performance as wired network and ensure the security of wireless network. AP sends ciphertext formed by WEP encryption and sends it to STA site, which means that the whole authentication process has been completed. If an authentication result containing a failure is sent, the authentication result fails [13]. The two-way authentication process is shown in Figure 2.



（a）Open system authentication process



（b）Shared secret key authentication

Figure 2 Schematic diagram of two way identity authentication

1.5.2 Network data encryption transmission mechanism

When the two-way identity authentication between sensor SN and intelligent mobile device MN is successful, the received data will be encrypted and transmitted to MN. When MN receives the data from all sensors, it will carry out two-way authentication with SS. After the success, all the fusion information encrypted by shared secret is transmitted to SS, and the data security transmission stage is divided into two parts. This paper assumes that each user has three sensor nodes with different functions [14]. The collected information is sent to MN every 6 hours. Every time a new intercycle comes, each part will also carry out the corresponding key update operation.

1.5.3 Intrusion detection mechanism

The watchdog program is used to detect the network internal attack. After node S sends data M to node T, it does not delete the data M immediately, but saves it in the cache, and then listens to node T. After receiving the data M from node S, node T will continue to forward the data M to the next hop node under normal circumstances. At this time, node S is in communication hybrid mode, and can also receive this data, which is recorded as M1. Node S compares data M and data M1. If they are the same, node T successfully forwards the data [15]. If node S does not listen to the data forwarded by node T, or data M is different from data M1, the malicious behavior of node T

will be recorded. Reputation mechanism is set in the detection process, which can evaluate the forwarding behavior of nodes for a long time. Based on the beta reputation structure of probability and statistics, the reputation value is calculated according to the number of packets successfully forwarded and the number of packets lost, as shown in formula 4.

$$T = \frac{s+1}{s+f+2} \quad (4)$$

In the formula, s is the number of packets sent correctly, f is the number of packets lost, and T is the credibility. Malicious nodes will receive data forwarding tasks from different source nodes. Then there are multiple forward hop nodes of the node. Malicious nodes can forward only some of the data sent by the forward hop nodes, and discard the data sent by the remaining forward hop nodes, which results in inconsistent evaluation of the malicious node by different forward hop nodes [16]. In this regard, mobile wireless sensor networks need to communicate with each other, evaluate the situation, implement joint detection, monitor each other among nodes, and collect the monitoring situation of multiple neighbor nodes to better detect malicious nodes.

1.6 Security Modeling of direct network report of infectious diseases

Finally, the security mechanism and attack factors of the direct report network of infectious diseases are comprehensively evaluated to realize the security modeling of direct report [17]. Figure 3 shows the risk quantification assessment framework for network security.

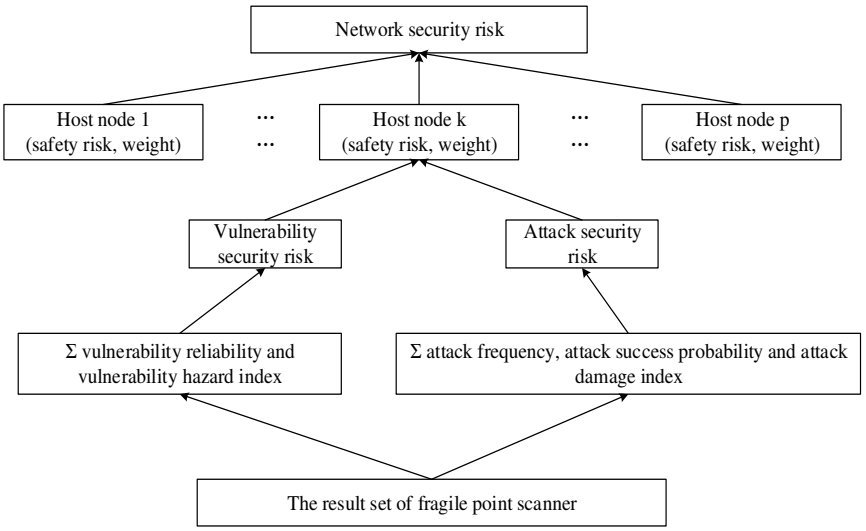


Figure 3 Quantitative assessment framework of network security risk for direct reporting of infectious diseases

The vulnerability security risk R_v, attack success probability p, attack security risk R_a and node security risk R_{h} are defined as network evaluation indexes, and the evaluation result of network security risk R_N is finally obtained [18]. The risk size of a single vulnerability point in the host node is expressed by the product of the vulnerability point reliability and vulnerability point hazard index:

$$R_v = \mu \times \mathrm{e} \quad (5)$$

In the formula, μ and e are the reliability of the existence of a single vulnerable point and the hazard index to its host node [19]. The success probability of atomic attack is defined as the product of vulnerability reliability and the degree of vulnerability being exploited. That is:

$$\begin{cases} p = \sigma \times \exp \\ \exp = 2 \times AccessVector \times AccessComplexity \times Authentication \end{cases} \quad (6)$$

In the formula, σ represents the reliability of the vulnerable point, $AccessVector$, $AccessComplexity$ and $Authentication$ respectively reflect the way the vulnerable point is used, the attack complexity and the number of times the attacker is authenticated by the attack target. The result $\exp$ is the degree of difficulty that the vulnerable point is used. In addition, attack security risk and node security risk can be expressed as:

$$\begin{cases} R_a = c \times 10^y \\ R_h = \sum_{i=1}^{m} R_{v_i} + \sum_{j=1}^{n} R_{o_j} \end{cases} \quad (7)$$

In the formula, c is the frequency of single atomic attack, y is the damage index to the host node after the successful occurrence of a single atomic attack, m is the total number of vulnerable points in a single host node, n is the total number of successful attacks in a single host node, and R_{o_j} and R_{v_i} are the security risks of single attack and vulnerable points respectively [20]. The final network security risk of direct report of infectious diseases can be expressed as follows:

$$R_N = \sum_{k=1}^{\mathrm{num}} \omega_k R_{h_k} \quad (8)$$

In the formula, num is the total number of host nodes in the network, ω_k is the weight of a single host node in the network. Finally, by substituting the calculation result of formula 7 into formula 8, the final quantitative evaluation result of network security for direct reporting of infectious disease epidemic situation can be obtained.

2 Comparative experimental analysis

In order to test the application performance of the network direct reporting security model of infectious diseases based on wireless communication technology in the actual network, a comparative experiment is designed. TinyOS and MATLAB are selected as the two development tools of the experiment. TinyOS is an open source embedded operating system. TinyOS system, libraries and applications are all written in nesC language, which is a new language for writing structured component-based applications. NesC language is mainly used in embedded systems such as sensor networks. NesC has the syntax similar to C language, but it supports the concurrency model of TinyOS. It also has the mechanism of organization and naming. It can link with other software components to form a robust network embedded system. Its main goal is to help application designers build components that can be easily combined into a complete, parallel

system, and can perform extensive checks at compile time. TinyOS defines many important concepts expressed in nesC. First, nesC applications should be built on well-defined components with bidirectional interfaces. Secondly, nesC defines a concurrency model, which is based on task and hardware event handles and detects data contention at compile time. The experimental environment is the corresponding platform of TinyOS. TOSSIM is an environment that runs on PC and supports TinyOS based applications. The simulator can run locally directly and can simulate thousands of nodes at the same time. Each node runs the same TinyOS program. TOSSIM supports runtime output of debugging information, allowing users to analyze and observe the execution of programs from different perspectives. TOSSIM provides a Java based extensible graphical user interface TinyViz for testing, setting up and displaying simulation environment. With TinyViz, it is convenient to track the execution of TinyOS applications, and the wireless messages, virtual location of particles and connectivity between nodes are visualized. In addition, MATLAB tools are mainly used as the analysis platform of structure.

In the experimental scenario, 100 user nodes are randomly distributed in a rectangular area of 1500×1200 m^2. The base station and the data source node are located in the upper left corner and the lower right corner of the region, respectively. Three paths from the source node to the base station are established through the diffusion routing, LEACH routing protocol and TEEN routing protocol algorithm. The light colors of sensor nodes on the same path are red, yellow and green. Node 0 represents the base station, node 33 represents the data source node, and the red, yellow and green lights are on at the same time. Each node that generates sensing data on the path sends the sensing data to the downstream. All sensor nodes have the same initial energy and communication radius. The data packets in the network are sent at the speed of 20Kbps. Launch Sybil attack or HELLO flooding attack on each path. When a node is captured and becomes a malicious node, it will tamper with the sensing data and send it back to the base station. Or when the external malicious node invades, it will produce false information and send it back to the base station. The initial establishment result of the experimental data transmission path is shown in Figure 4.

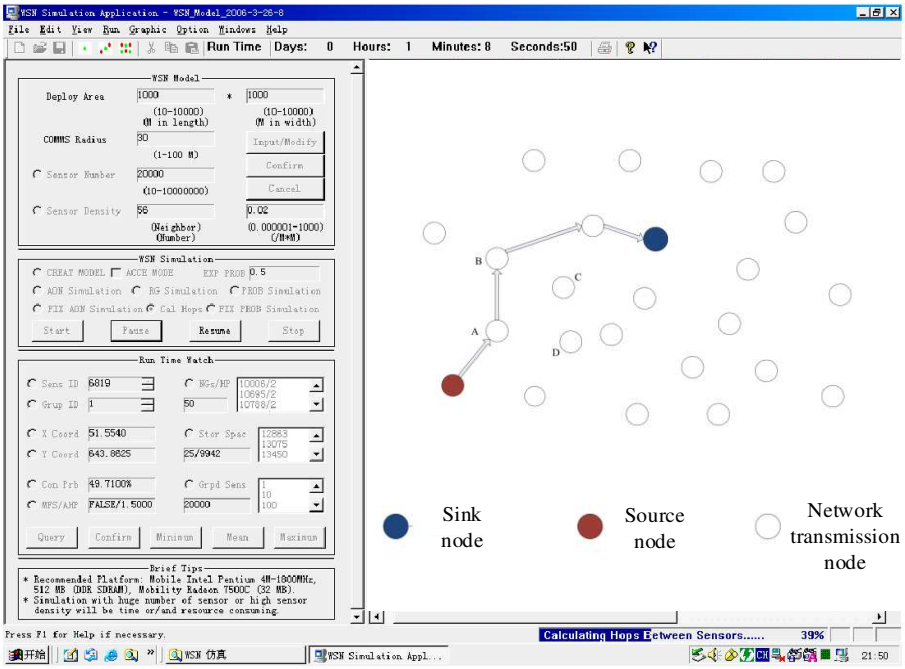


Figure 4 Schematic diagram of data transmission path

Before the experiment, the network direct report data of infectious disease epidemic situation was generated, and the data sample preparation is shown in Table 1.

Table 1 Data sample of direct network report of infectious diseases

Area code	Current confirmed cases / case	Existing severe cases/ case	Existing suspected cases / case	Cumulative confirmed cases / case	Cumulative cured cases / case	Cumulative number of deaths / person
001	1542	390	389	3238	1567	129
002	3595	722	1052	5652	1435	622
003	2421	104	923	4547	1949	177
004	4089	25	1655	6365	1758	518
005	1412	98	231	3273	1608	253
006	2098	124	104	3562	1300	164
007	3144	162	1123	4773	1316	313
008	2678	104	854	4068	1102	288

The data in Table 1 is converted into direct report information, which is used as the transmission content of wireless communication network. In order to reflect the application advantages of design security modeling results, the traditional network security model and cloud computing access control network security model are set up as two comparative models. The comparative experiment is divided into three steps. Firstly, the network attack program is randomly generated in the transmission network, and the direct report information of infectious diseases are input into the communication network. The second step is to implement the security model, detect the network security risk and take corresponding remedial measures. Finally, the data of the network direct report of infectious diseases are collected and compared with the data samples set up. The loss and tampering of the data are observed under different security models. Through the data retrieval and statistics, the experimental results are shown in Table 2.

Table 2 Data table of comparative experiment results

Information number of direct network report of epidemic situation of infectious diseases	Input transmission data / MB	Traditional network security model		Network security model based on cloud computing access control		Network direct report security model designed	
		Actual data received / MB	Error data / MB	Actual data received / MB	Error data / MB	Actual data received / MB	Error data / MB
001	8.35	8.24	0.25	8.32	0.11	8.35	0.06
002	13.52	13.46	0.38	13.50	0.23	13.52	0.14
003	11.44	11.31	0.26	11.35	0.12	11.44	0.08
004	18.67	18.56	0.23	18.61	0.09	18.65	0.04
005	6.38	6.27	0.18	6.35	0.07	6.38	0.04
006	10.14	10.06	0.35	10.11	0.15	10.14	0.11
007	13.23	13.12	0.44	13.16	0.21	13.21	0.13

008	12.04	11.89	0.26	12.00	0.18	12.02	0.12

It can be seen from Table 2 that the data loss of direct network report of infectious disease epidemic under the three models are 0.108MB, 0.046MB and 0.008MB respectively. From the data error amount, the average data tampering amount corresponding to the three security models is 0.29MB, 0.15MB and 0.09MB. In conclusion, the application of the security modeling method based on wireless communication technology can improve the integrity and accuracy of direct reporting data to a certain extent.

3 Conclusion

With society's attention to health and health, the concept of prevention has been deeply rooted in the hearts of the people, and the importance of direct network reporting of infectious diseases will become increasingly prominent. The network reporting system of infectious diseases will be improved day by day, and there will be more integrated, active and creative monitoring methods for public health services. Through the application of wireless communication technology, the stability and security of sensor and epidemic information in the process of direct reporting are improved.

ACKNOWLEDGEMENT

Henan Provincial Philosophy and Social Planning Project Fund, Project No.: 2020BSH012

Conflict of interests:

The authors declare that they have no competing interests in this section.

Reference

[1] Hunter E , Namee B M , Kelleher J D . A Model for the Spread of Infectious Diseases in a Region[J]. International Journal of Environmental Research and Public Health, 2020, 17(9):3119.

[2]S Gündüç. A Study on the Effects of Diffusion of Information on Epidemic Spread[J]. International Journal of Modeling, Simulation and entific Computing, 2019, 10(3):109-122.

[3] Research on Security Situation Assessment Model of Video Transmission Network[J]. International Journal of Modern Education and Computer Science, 2019, 11(4):40-45.

[4] Sun C , Wang X , Zheng Y . An ensemble system to predict the spatiotemporal distribution of energy security weaknesses in transmission networks[J]. Applied Energy, 2020, 258(Jan.15):114062.1-114062.18.

[5] Li S L , Zhang J , Liu Y . Research on the Security Data Transmission based on Linux[J]. IOP Conference Series: Materials Science and Engineering, 2019, 563:052031-.

[6] J Chen, Zhao F , Xing H . Research on Security of Mobile Communication Information Transmission Based on Heterogeneous Network[J]. International Journal of Network Security, 2020, 22(1):145-149.

[7] Ding L , Wang Z , Wang X , et al. Security information transmission algorithms for IoT based on cloud computing[J]. Computer Communications, 2020, 155:32-39.

[8] Choi S Y , Kim J H , Kim J , et al. World Outbreak Trend of Infectious Diseases with Surveillance[J]. Journal of Bacteriology and Virology, 2019, 49(3):141.

[9] PEACOCK: A Map-based Multitype Infectious Disease Outbreak Information System[J]. IEEE Access, 2019, PP(99):1-1.

[10] Wang J , Liu H , Gao R , et al. Research on Computer Aided Computation of Infectious Disease SIR Model Algorithm Based on Parameter Control[J]. Journal of Physics: Conference Series, 2020, 1650(3):032043 (9pp).

[11] Liu S Z , Ji F Y , Li X K . Epidemic situation of malaria in Qingdao City from 2012 to 2017[J]. Chinese Journal of Schistosomiasis Control, 2019, 30(6):664-668.
[12] Zhao G , Song J . Network security model based on active defense and passive defense hybrid strategy[J]. Journal of Intelligent and Fuzzy Systems, 2020, 39(4):1-9.
[13] Zhu B , Y Chen, Y Cai. Three Kinds of Network Security Situation Awareness Model Based on Big Data[J]. International Journal of Network Security, 2019, 21(1):115-121.
[14] Alexander R . Using the Latin Square Design Model in the Prioritzation of Network Security Threats: A Quantitative Study[J]. Journal of Information Security, 2020, 11(2):92-102.
[15] Venkatesh R , Muthalagu R . Network security prediction model using neural networks[J]. Journal of Physics: Conference Series, 2020, 1706(1):012167 (7pp).
[16] Yang H , Zeng R , Xu G , et al. A network security situation assessment method based on adversarial deep learning[J]. Applied Soft Computing, 2021, 102(8):107096.
[17] Kou G , Wang S , Tang G . Research on Key Technologies of Network Security Situational Awareness for Attack Tracking Prediction[J]. Chinese Journal of Electronics, 2019, 28(01):166-175.
[18] Ikhalia E , Serrano A , Bell D , et al. Online social network security awareness: mass interpersonal persuasion using a Facebook app[J]. Information Technology & People, 2019, ahead-of-print(ahead-of-print).
[19] Xu K , Liu J , Lu J . Research and Realization on Smart City Applications Based on eMTC wireless communication technology[J]. Journal of Physics: Conference Series, 2021, 1757(1):012178 (8pp).
[20] Jiang X , Pang Z , Luvisotto M , et al. Using a Large Data Set to Improve Industrial Wireless Communications: Latency, Reliability, and Security[J]. IEEE Industrial Electronics Magazine, 2019, 13(1):6-12.

Figures

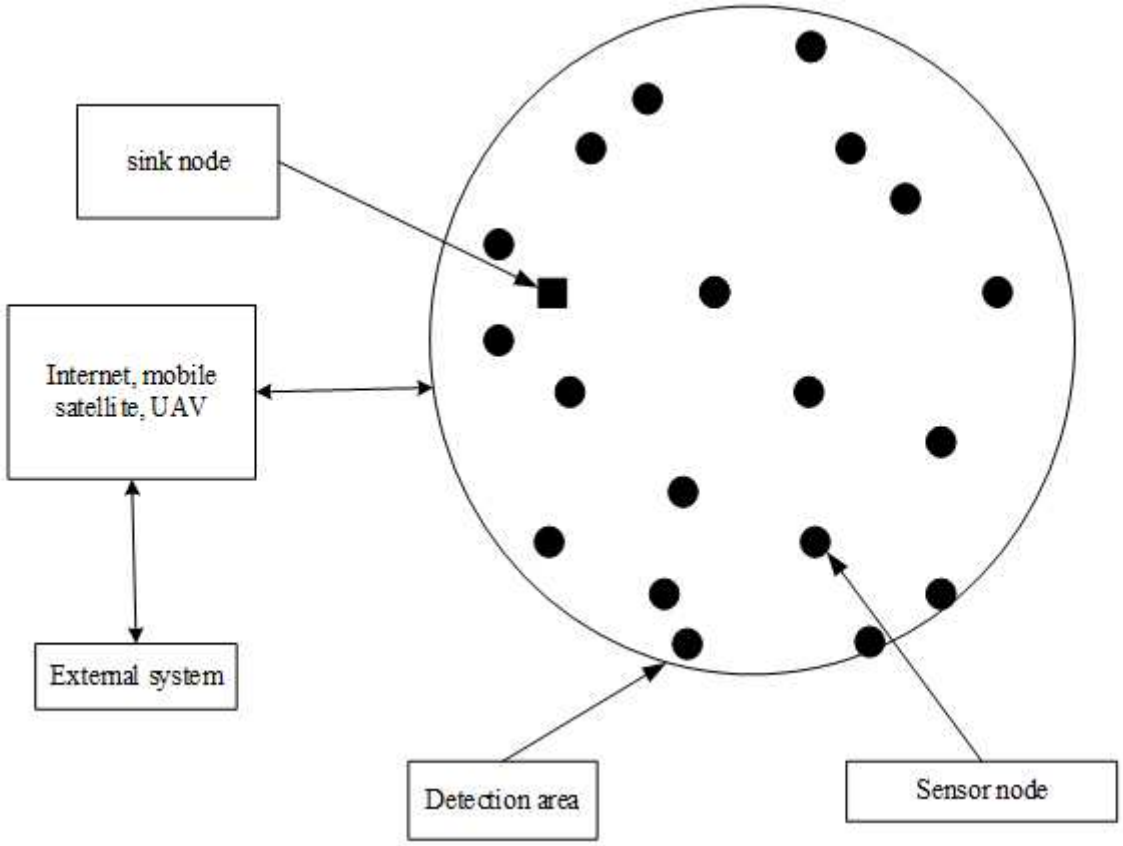


Figure 1

Network architecture of wireless direct reporting of infectious diseases

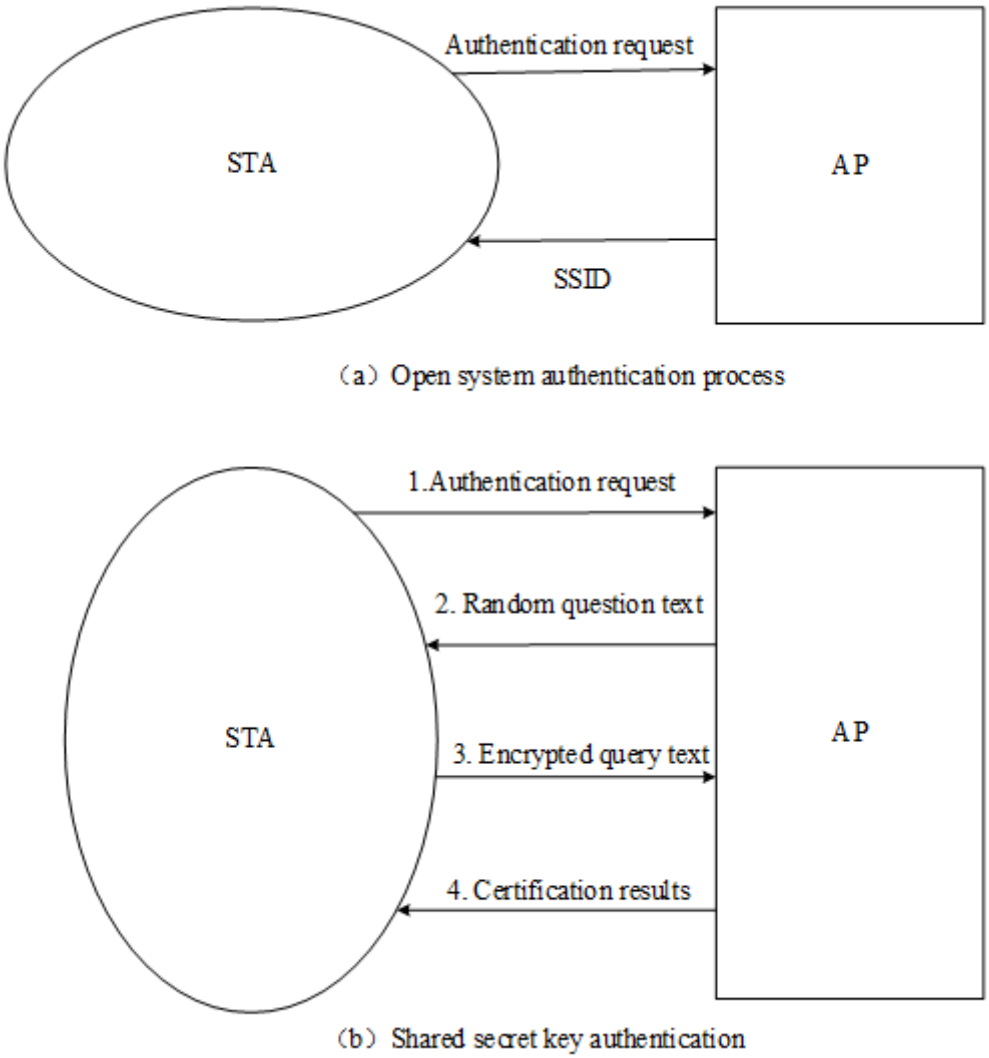


Figure 2

Schematic diagram of two way identity authentication

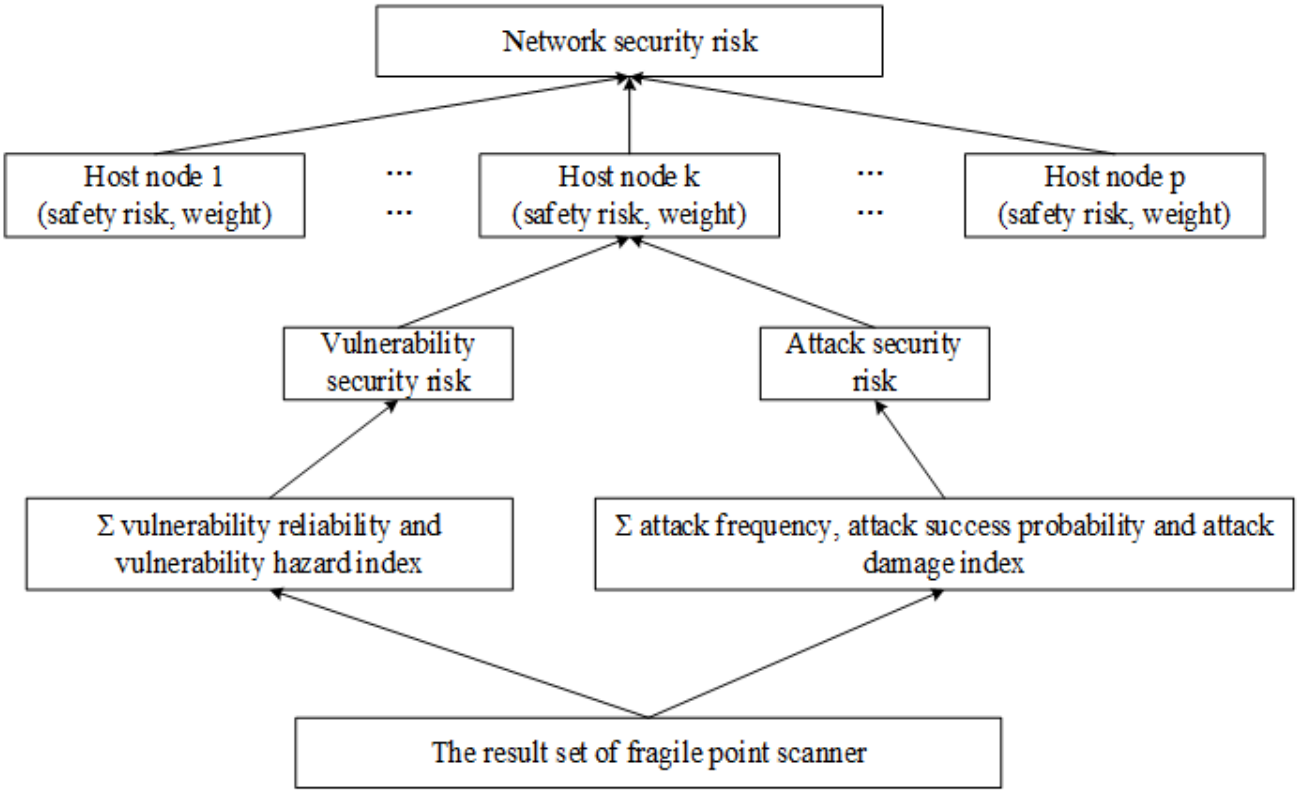


Figure 3

Quantitative assessment framework of network security risk for direct reporting of infectious diseases

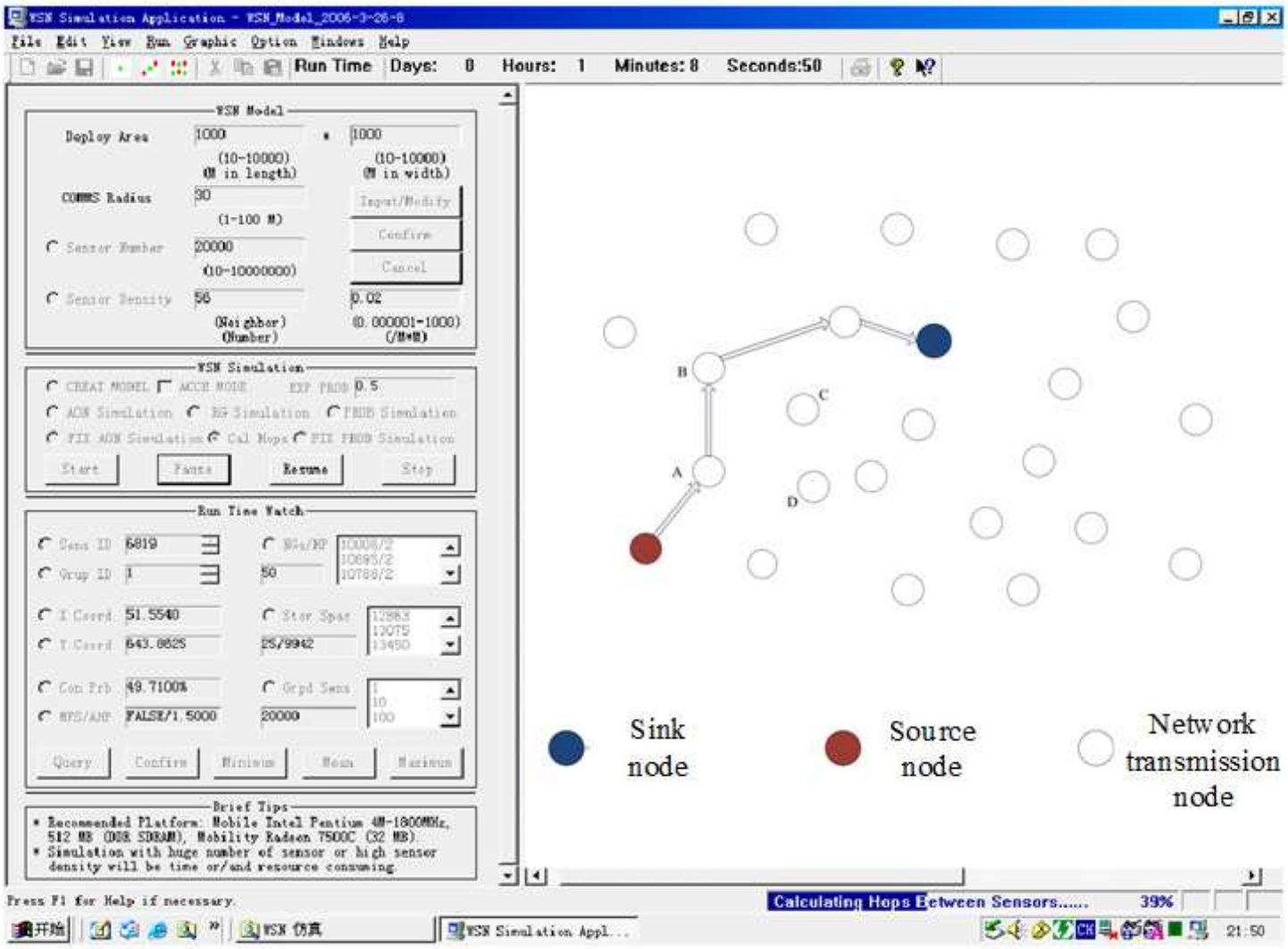


Figure 4

Schematic diagram of data transmission path