I.J. Modern Education and Computer Science, **2019, 4, 40-45**
Published Online April 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2019.04.05

Research on Security Situation Assessment Model of Video Transmission Network

Gao Jian
Information technology and network security College, People's Public Security University of China, BeiJing, China
Email: gaojianbeijing2006@163.com

Yue Ting
Information technology and network security College, People's Public Security University of China, BeiJing, China
Email: m18728789629@163.com

Zhu RongChen
Information technology and network security College, People's Public Security University of China, BeiJing, China
Email: m18896617866_1@163.com

Received: 24 January 2019; Accepted: 13 February 2019; Published: 08 April 2019

***Abstract*—**In this paper, we propose a situation assessment model for video transmission network, which evaluates the security risk of video transmission network information from four aspects: front-end perception layer, transmission layer, application layer and other risks.We divide the video network security evaluation system into three layers, and use AHP to determine the weight of each index.The weights of these four aspects are calculated by analytic hierarchy process.The method proposed in this paper can provide an evaluation system and a calculation method for the safe operation of video transmission network and important systems, and can provide specialized information security services for the construction project of video transmission network.

***Index Terms*—**Video Transmission Network, Analytic Hierarchy Process, Evaluation Model.

I. Introduction

"China has built the world's largest video surveillance network, with more than 20 million video cameras," CCTV's documentary "Glorious China" reported. But on the other hand, the invasion, hijacking and legal information sales of cameras once constituted an industrial chain, and their impact was not limited to privacy leakage, but is also spreading to criminal cases and even to some areas such as national defense security information, financial trading information, commercial office secrets[1], etc.During the outbreak of blackmail virus in May 2017, more than 120, 000 network cameras around the world were hacked as springboards for virus transmission and attacks[2].On July 26, 2018, the Science, Technology and Information Technology Bureau of the Ministry of Public Security informed the Ningdu County Public Security Bureau that on July 24, a video private network and a dual network card server in public security network of the Traffic Control Brigade of the Ningdu County Public Security Bureau scanned a large number of servers of the national public security network servers[3].After the initial investigation by Ningdu County Public Security Bureau, it was found that the server was illegally invaded.Someone used hacker technology to invade the computers of public security network and install the Monroe coin mining software[4, 5].

Enea Tsanai[6, 7], propose a cross-layer design that aims to improve the performance of video transmission using TCP Friendly Rate Control .Thomas Kunkelmann[8], give an overview of the security requirements of multimedia conferencing systems and of applicable security functions.For real-time video transmission, it is necessary to selectively encrypt the transmitted data.The existing methods are investigated and their advantages and disadvantages are pointed out.Chuanping Hu[9], focus on the area of public security and build an Intelligent Video and Image Analysis Evaluation Platform for Public Security (IVIAEPPS).They introduces some existing works on building this platform, as well as a video and image challenge based on it.Cha Sungyong[10], proposed a novel security evaluation framework for Military IoT Devices.

In recent years, the Party Central Committee and the State Council have attached great importance to the integration of social video resources, and have successively introduced a series of policy measures: In April 2015, the General Office of the CPC Central

Committee and the General Office of the State Council jointly issued the " Opinions on Strengthening the Construction of Social Security Prevention and Control System ", which is required to improve the technical standards, strengthen the system networking, effectively integrate all kinds of video and image resources at different levels, and gradually expand the application fields[11, 12, 13].In May 2015, the National Development and Reform Commission and the nine ministries and commissions issued a document “Several Opinions on Strengthening the Network Application of Public Security Video Surveillance Construction”[14, 15].It was suggested that by 2020, the networking rate of video surveillance in key public areas should reach 100%, and the networking rate of video and image resources in key industries and fields involving public areas should reach 100%[16].

The content of this paper is arranged as follows: The second part introduces the overall framework of video transmission network, the third part introduces the security evaluation model and evaluation system, and finally summarizes the paper.

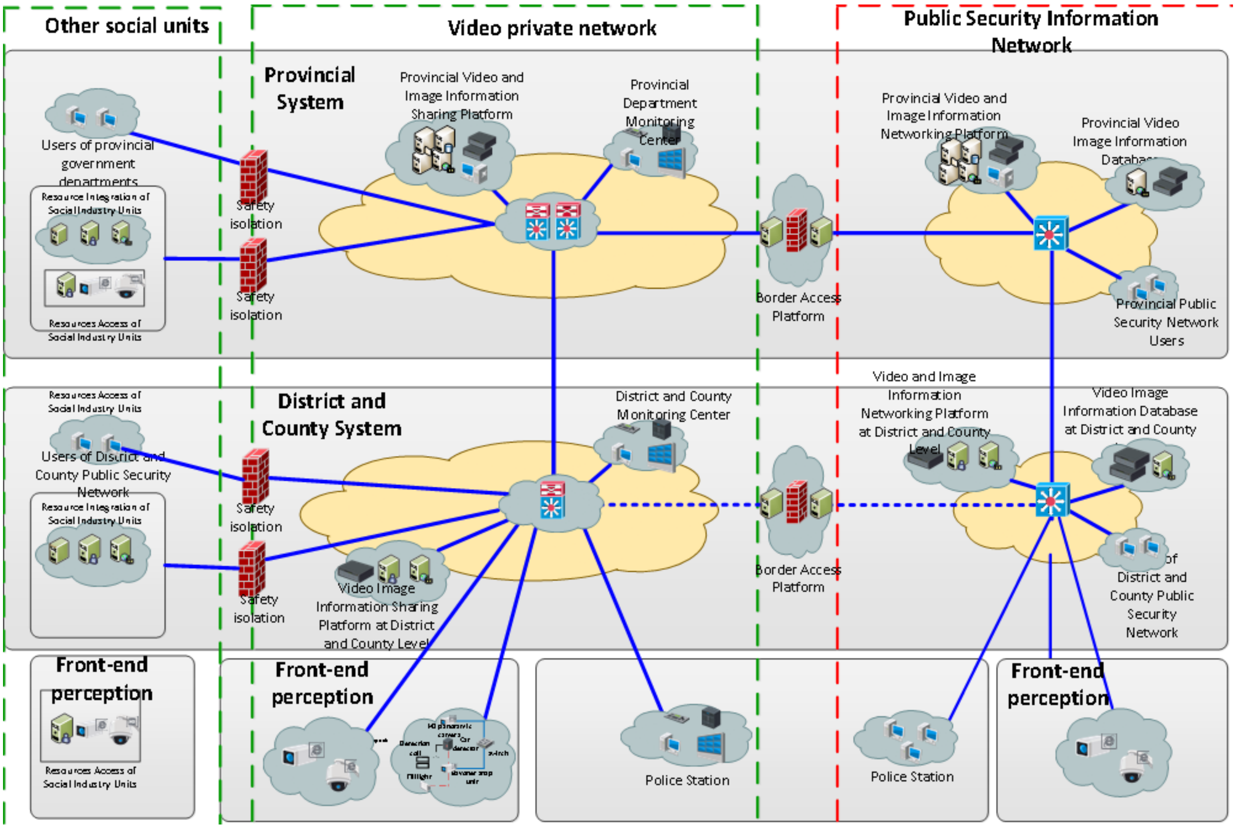
Other social units
Video private network
Public Security Information Network
Provincial System
Provincial Video and Image Information Sharing Platform
Provincial Department Monitoring Center
Users of provincial government departments
Resource Integration of Social Industry Units
Resources Access of Social Industry Units
Safety isolation
Safety isolation
Border Access Platform
Provincial Video and Image Information Networking Platform
Provincial Video Image Information Database
Provincial Public Security Network Users
District and County System
District and County Monitoring Center
Resources Access of Social Industry Units
Users of District and County Public Security Network
Resource Integration of Social Industry Units
Safety isolation
Safety isolation
Video Image Information Sharing Platform at District and County Level
Border Access Platform
Video and Image Information Networking Platform at District and County Level
Video Image Information Database at District and County
of District and County Public Security Network
Front-end perception
Resources Access of Social Industry Units
Front-end perception
HD panoramic camera
Car detector
Detection coil
Switch
Filllight
Police Station
Police Station
Front-end perception

Fig.1. Overall architecture of video transmission network

II. Overall Architecture of Video Transmission Network

The video transmission network uses a special network for video transmission.The video information is collected in the private network and transmitted to the public security information network or other law enforcement departments through the network security border device.

Problems in the video private network are as follows:

1. There is a threat of illegal replacement of cameras.Most of the front-end cameras are outdoors, and they are at risk of being replaced by others. If there is no access control for illegally replaced devices in the network, it is very likely that the lawbreakers can easily enter the video private network through a camera.
2. The camera has weak passwords and vulnerabilities.Cameras have a web interface for remote login management.There are many cameras in each province, so in general many administrators do not change their default passwords.It is not possible to patch some of the camera's vulnerabilities in time.
3. The data transmission is not encrypted.Most of the video data and control data transmitted in the video private network are not encrypted, and there is a risk of being sniffed and tampered by the man-in-the-middle.The national standard "Technical Requirements for Information Security of Public Security Video Surveillance Networking" published in 2017 clearly defines the standards and requirements of video encryption.
4. There are high-risk vulnerabilities in the application systems.If operating system vulnerabilities, platform vulnerabilities, and system security policies are not fixed or configured, they will pose a risk to the entire network.If an attacker enters the video network, he or she can obtain server

permissions through the vulnerabilities to obtain video resources of the entire network.

5. Other risks include natural disasters (such as earthquakes, fires, etc.) and non-compliance with regulations, such as connecting the intranet computer to the external network through dual network cards or wifi.

III. Safety Assessment Model

In this paper, AHP (Analytic Hierarchy Process) is used to analyze the information security risk of video transmission network.Based on the hierarchical model of video transmission network, the evaluation index system is established from four aspects: front-end perception layer, transmission layer, application layer and other risks.The perception layer includes illegal replacement, weak password and camera vulnerabilities; the transmission layer includes physical security of transmission lines and data transmission security; the application layer includes server vulnerabilities, platform vulnerabilities and security policies; and other risks include natural disasters and illegal outreach, as shown in the Figure 2.

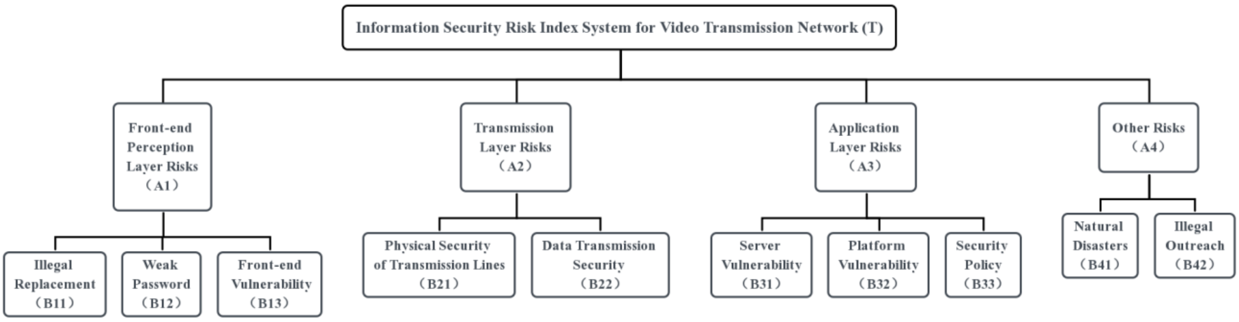
Information Security Risk Index System for Video Transmission Network (T)
Front-end Perception Layer Risks （A1）
Transmission Layer Risks （A2）
Application Layer Risks （A3）
Other Risks （A4）
Illegal Replacement （B11）
Weak Password （B12）
Front-end Vulnerability （B13）
Physical Security of Transmission Lines （B21）
Data Transmission Security （B22）
Server Vulnerability （B31）
Platform Vulnerability （B32）
Security Policy （B33）
Natural Disasters （B41）
Illegal Outreach （B42）

Fig.2. Video transmission network information security risk indicator system (T)

Table 1. Scale Principles of 1-9

Scale	**Definition and Explanation of Comparison of Two Elements**
1	Both have the same importance (or the same strong)
3	One element is slightly more important (or slightly stronger) than the other
5	One element is more important (or stronger) than the other
7	One element is obviously more important (or obviously stronger) than the other
9	One element is absolutely more important (or absolutely stronger) than the other
2, 4, 6, 8	Scale between the above two standards

We use analytic hierarchy process to construct discriminant matrix.In the whole index system, the discriminant matrix is constructed by comparing the importance of N indexes in the same layer with those in the upper layer.In this paper, the expert scoring method is used, and the discriminant matrix is obtained by comparing each index in pairs according to the scale principles of 1-9.

Firstly, we used the AHP to analyze the impact of each principle's various types of risks on the IoT information security system.According to Table 1, the principle layers are compared in pairs, and we can obtain six ratios of $\mathrm{A}i/\mathrm{A1}\cdot$

$\mathrm{A}i/\mathrm{A1}, \mathrm{A}i/\mathrm{A2}, \mathrm{A}i/\mathrm{A3}, \mathrm{A}i/\mathrm{A4}\left(i{=}1{,}2{,}3{,}4\right)$, constitutes a discriminant matrix $\mathbf{P}$ of 4 rows and 4 columns that judges the importance of four factors.

$$\mathbf{P}=\begin{bmatrix} \mathrm{A1/A1} & \mathrm{A1/A2} & \mathrm{A1/A3} & \mathrm{A1/A4} \\ \mathrm{A2/A1} & \mathrm{A2/A2} & \mathrm{A2/A3} & \mathrm{A2/A4} \\ \mathrm{A3/A1} & \mathrm{A3/A2} & \mathrm{A3/A3} & \mathrm{A3/A4} \\ \mathrm{A4/A1} & \mathrm{A4/A2} & \mathrm{A4/A3} & \mathrm{A4/A4} \end{bmatrix} \tag{1}$$

Suppose the vector consisting of sub-factors is:

$$\mathbf{Q}=\left(\mathrm{A1} \quad \mathrm{A2} \quad \mathrm{A3} \quad \mathrm{A4}\right)^{T} \tag{2}$$

$$\mathbf{P}*\mathbf{Q}=\begin{bmatrix} \mathrm{A1/A1} & \mathrm{A1/A2} & \mathrm{A1/A3} & \mathrm{A1/A4} \\ \mathrm{A2/A1} & \mathrm{A2/A2} & \mathrm{A2/A3} & \mathrm{A2/A4} \\ \mathrm{A3/A1} & \mathrm{A3/A2} & \mathrm{A3/A3} & \mathrm{A3/A4} \\ \mathrm{A4/A1} & \mathrm{A4/A2} & \mathrm{A4/A3} & \mathrm{A4/A4} \end{bmatrix}\begin{bmatrix} \mathrm{A1} \\ \mathrm{A2} \\ \mathrm{A3} \\ \mathrm{A4} \end{bmatrix} \tag{3}$$

$$\mathbf{P} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}$$

$$= \begin{bmatrix} \mathrm{A1}/\mathrm{A1} & \mathrm{A1}/\mathrm{A2} & \mathrm{A1}/\mathrm{A3} & \mathrm{A1}/\mathrm{A4} \\ \mathrm{A2}/\mathrm{A1} & \mathrm{A2}/\mathrm{A2} & \mathrm{A2}/\mathrm{A3} & \mathrm{A2}/\mathrm{A4} \\ \mathrm{A3}/\mathrm{A1} & \mathrm{A3}/\mathrm{A2} & \mathrm{A3}/\mathrm{A3} & \mathrm{A3}/\mathrm{A4} \\ \mathrm{A4}/\mathrm{A1} & \mathrm{A4}/\mathrm{A2} & \mathrm{A4}/\mathrm{A3} & \mathrm{A4}/\mathrm{A4} \end{bmatrix} \quad (4)$$

$$= \begin{bmatrix} \mathrm{A1}/\mathrm{A1} & \mathrm{A1}/\mathrm{A2} & \mathrm{A1}/\mathrm{A3} & \mathrm{A1}/\mathrm{A4} \\ \mathrm{A2}/\mathrm{A1} & \mathrm{A2}/\mathrm{A2} & \mathrm{A2}/\mathrm{A3} & \mathrm{A2}/\mathrm{A4} \\ \mathrm{A3}/\mathrm{A1} & \mathrm{A3}/\mathrm{A2} & \mathrm{A3}/\mathrm{A3} & \mathrm{A3}/\mathrm{A4} \\ \mathrm{A4}/\mathrm{A1} & \mathrm{A4}/\mathrm{A2} & \mathrm{A4}/\mathrm{A3} & \mathrm{A4}/\mathrm{A4} \end{bmatrix}$$

The element $a_{ij} \succ 0, (i, j = 1, 2, 3, 4)$ satisfies the following conditions:

(1) $a_{ii} = 1$.

(2) $a_{ij} = \dfrac{1}{a_{ji}}$, the matrix is reciprocal.

According to the information consulted and common sense judgment, each risk item was assigned.The scale is as shown in the Table 2.

Table 2. Value-added Risks

	Front-end Perception Layer Risks	**Transmission Layer Risks**	**Application Layer Risks**	**Other Risks**
Front-end Perception Layer Risks	1	7	3	5
Transmission Layer Risks	1/7	1	1/5	1/3
Application Layer Risks	1/3	5	1	4
Other Risks	1/5	3	1/4	1

According to the eigenvectors and eigenvalues calculated by the reciprocal matrix, we used Matlab to calculate the weights corresponding to the various types of risks, as shown in the Table 3.

The eigenvector corresponding to the maximum eigenvalue of the judgment matrix is normalized (so that the sum of the elements in the vector is equal to 1) and then written down as W. The elements of W are ranking weights of the relative importance of the same level factor to the upper level factor. This process is called hierarchical single ranking. Confirmation of hierarchical single ranking requires consistency testing, which means determining the allowable range of inconsistencies for A. The unique non-zero eigenvalue of the n-order uniform matrix is n; the maximum eigenvalue of the n-order positive and reciprocal matrix A, if and only then, is a uniform matrix.

Because of the continuous dependence of λ, the greater the ratio of λ to n, the more serious the inconsistency of A. The smaller the CI is, the greater the consistency is. When the eigenvector corresponding to the maximum eigenvalue is used as the weight vector of the influence degree of the comparative factor on the upper factor, the greater the degree of inconsistency, the greater the judgment error. Therefore, the inconsistency of A can be measured by the value of λ-n.

Table 3. Weights of Principal Layer Risks

Principal Layer	**Front-end Perception Layer Risks（A1）**	**Transmission Layer Risks（A2）**	**Application Layer Risks（A3）**	**Other Risks（A4）**
Weights	0.5565	0.0542	0.2809	0.1085

Verifying the consistency of P: C.I=0.0574 C.R=0.0645, we can know that the consistency of the matrix is acceptable.

Similarly, we used AHP to determine the weights of other risk indicators of video transmission network information security.

In the front-end perception layer risks, the weights of illegal replacement, weak password, and front-end vulnerability are as shown in the Table 4

Table 4. Weights of Front-end Perception Layer Risks

Front-end Perception Layer Risks	**Illegal Replacement（B11）**	**Weak Password（B12）**	**Front-end Vulnerability（B13）**
Weights	0.6483	0.2297	0.1220

In the transmission layer risks, the weights of physical security of transmission lines and data transmission security are as shown in the Table 5.

Table 5. Weights of Transmission Layer Risks

Transmission Layer Risks	Physical Security of Transmission Lines （B21）	Data Transmission Security （B22）
Weights	0.7500	0.2500

In application layer risks, the weights of server vulnerability, platform vulnerability, and security policy are as shown in the Table 6.

Table 6. Weights of Application Layer Risks

Application Layer Risks	Server Vulnerability （B31）	Platform Vulnerability （B32）	Security Policy （B33）
Weights	0.2583	0.6370	0.1047

Among other risks, the weights of natural disasters and illegal outreach are as shown in the Table 7.

Table 7. Weights of Other Risks

Other Risks	Natural Disasters （B41）	Illegal Outreach （B42）
Weights	0.7500	0.2500

Finally, we determined the weight of each indicator in the information security risk indicator system of the video transmission network, as shown in the following Figure 3.

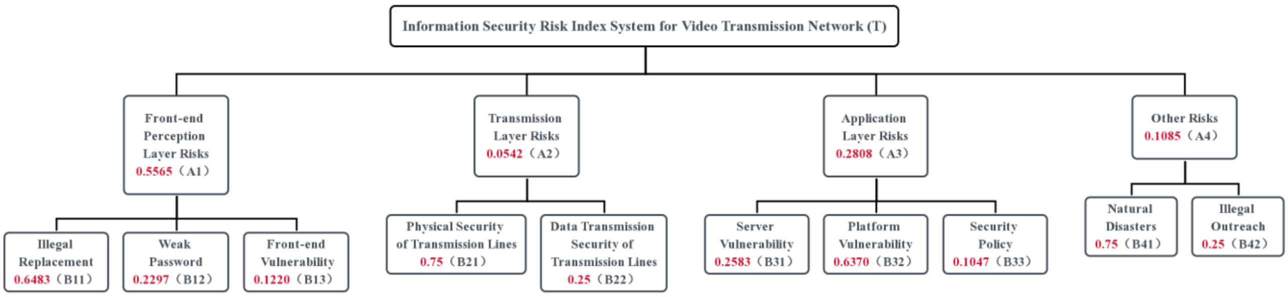
Information Security Risk Index System for Video Transmission Network (T)
Front-end Perception Layer Risks 0.5565（A1）
Transmission Layer Risks 0.0542（A2）
Application Layer Risks 0.2808（A3）
Other Risks 0.1085（A4）
Illegal Replacement 0.6483（B11）
Weak Password 0.2297（B12）
Front-end Vulnerability 0.1220（B13）
Physical Security of Transmission Lines 0.75（B21）
Data Transmission Security of Transmission Lines 0.25（B22）
Server Vulnerability 0.2583（B31）
Platform Vulnerability 0.6370（B32）
Security Policy 0.1047（B33）
Natural Disasters 0.75（B41）
Illegal Outreach 0.25（B42）

Fig.3. Video transmission network information security risk indicator system (T) and their weights

When assessing the information security risks of video networks, the third-level indicators can be scored by the percentage system, that is, the scores of the overall evaluation are calculated through the indicator system framework proposed in this paper.

IV. Conclusions

The method proposed in this paper can provide an evaluation system and calculation method for the safe operation of video transmission network and important systems, provide specialized information security services for the construction project of China’s video transmission network , promote the development of security assessment and risk assessment technologies of China’s video transmission network, and enhance the research and development level of information security technology of China’s video transmission network, and ultimately provide an effective means to achieve video transmission network information security leap-forward development[17].

Well-known network security enterprises and institutions have built a threat information sharing and exchange platform, and related sharing and exchange standards and technologies have accelerated the process of threat information sharing and utilization. However, threat intelligence sharing in dynamic, open and diversified video surveillance network space has the characteristics of massive data, low value information density and ambiguous quality[18] .A large number of deceptive, misleading or confused false information and counter-intelligence make it difficult to find the real correct and valuable information for security analysis and decision-making. In the security defense and early warning emergency system centered on threat intelligence, how to create reliable and fidelity information from shared intelligence and maintain low false alarm rate is very important for network security defense, detection and traceability applications[19].

The model can be further improved on the evaluation criteria and testing methods to improve service capabilities and service processes, which is of great significance for promoting the construction and development of China's video transmission network.

ACKNOWLEDGMENT

This paper is supported by the project (2017 GABJC38) and project(2019 JKF221).

REFERENCES

[1] Houtgast T, Steeneken H J M .Evaluation of speech transmission channels by using artificial signals[J].Acta Acustica United with Acustica, 1971, 25(25):355-367.

[2] Wong T, Findlay J, Mcmurtrie A .An On-Line Method for Transmission Ampacity Evaluation [J].IEEE Transactions on Power Apparatus & Systems, 1982, PAS-101(2):309-315.

[3] Kim H .Evaluation of power system security and development of transmission pricing method[J].Dissertation Abstracts International, Volume: 65-07, Section: B, page: 3606.;Chair: Chanan Singh. 2003.

[4] Xie L , Yang Z , Zhang C , et al.Security evaluation and auxiliary decision-making method for integrated generation and transmission outage schedule[J].Automation of Electric Power Systems, 2012, 36(15):116-119.

[5] Gupta R, Goel L .Security constrained well-being evaluation of a sub-transmission system[C]// International Conference on Electrical & Electronics Engineering. IEEE, 2005.

[6] FarrukhEhtisham, Panaousis E A, Politis C .Performance Evaluation of Secure Video Transmission over WIMAX[J].International Journal of Computer Networks & Communications, 2011, 3(6):28-38.

[7] Tsanai E , Bouras C , Kioumourtzis G , et al.Evaluation of Video Transmission in Emergency Response Ad Hoc Networks[C]// 4th International Conference on Data Communication Networking - DCNET.IEEE, 2013.

[8] Kunkelmann T, Reinema R, Steinmetz R , et al.Evaluation of Different Video Encryption Methods for a Secure Multimedia Conferencing Gateway[J].From Multimedia Services to Network Services, 1997, 1356:75-89.

[9] Hu C, Xue G, Mei L , et al.Building an intelligent video and image analysis evaluation platform for public security[C]// IEEE International Conference on Advanced Video & Signal Based Surveillance.IEEE, 2017.

[10] Sungyong C, Seungsoo B, Sooyoung K, et al.Security Evaluation Framework for Military IoT Devices[J].Security and Communication Networks, 2018, 2018:1-12.

[11] Jiarun S , Ziqiang X U, Fuzheng Y .Parametric-planning model combining the transmission characteristics of network video service[J].Journal of Xidian University, 2016.

[12] Hörsch, Jonas, Hofmann F, Schlachtberger D, et al.PyPSA-Eur: An open optimisation model of the European transmission system[J].Energy Strategy Reviews, 2018, 22:207-215.

[13] Wang P , Zhang G , Ni C, et al.A Two Time-Scales Network Bandwidth Measurement for Video Transmission[C]// 2016 International Conference on Network and Information Systems for Computers (ICNISC).IEEE, 2016.

[14] Nagashino H, Kinouchi Y .Oscillatory modes in a neuronal network model with transmission latency[J].Social Science Electronic Publishing, 2018, 52(02):843-848.

[15] Fu Y, Zhu J, Gao S .CPS Information Security Risk Evaluation System Based on Petri Net[C]// IEEE Second International Conference on Data Science in Cyberspace.IEEE, 2017.

[16] Rizvi S, Ryoo J, Kissell J, et al.A security evaluation framework for cloud security auditing[J].The Journal of Supercomputing, 2017.

[17] Lee J H, Kim S J .Analysis and Security Evaluation of Security Threat on Broadcasting Service[J].Wireless Personal Communications, 2017.

[18] Gulve S P, Khoje S A, Pardeshi P. Implementation of IoT-Based Smart Video Surveillance System[J]. 2017.

[19] Hasan R, Mohammed S K, Khan A , et al. A color frame reproduction technique for IoT-based video surveillance application[C]// IEEE International Symposium on Circuits & Systems. IEEE, 2017.

Authors' Profiles

Dr.Gao Jian is a lecturer in information technology and network security college, People's Public Security University of China .In teaching, he has been focusing on Work Process concepts and Problem Based Learning approaches in Cyber Security Education.In research, his current interests include Botnet, Malware, DDoS.

How to cite this paper: Gao Jian, Yue Ting, Zhu RongChen, "Research on Security Situation Assessment Model of Video Transmission Network", International Journal of Modern Education and Computer Science(IJMECS), Vol.11, No.4, pp. 40-45, 2019.DOI: 10.5815/ijmecs.2019.04.05