Journal of Intelligent Systems • *Open Access* • Volume 32, Issue 1 • 1 January 2023 • Article number 20230065

Smart robots' virus defense using data mining technology

Ye, Jiao[a] ; Patel, Hemant N.[b] ;
Meena, Sankaranamasivayam[c] ; Maaliw, Renato R.[d] ;
Ajibade, Samuel-Soma M.[e] ; Keshta, Ismail[f]
Save all to author list

[a] College of General Education, Jilin Animation Institute, Jilin, Changchun, 130013, China
[b] Department of Computer Engineering, Sankalchand Patel College of Engineering, Gujarat, Visnagar, 384315, India
[c] Department of Electronics and Instrumentation Engineering, St. Joseph's College of Engineering, Omr, Chennai, 600119, India
[d] College of Engineering, Southern Luzon State University, Quezon, Lucban, 4328, Philippines
View additional affiliations

Document type
Article • *Gold Open Access*
Source type
Journal
ISSN
2191026X
DOI
10.1515/jisys-2023-0065
View more

Full text options Export

Abstract

In order to realize online detection and control of network viruses in robots, the authors propose a data mining-based anti-virus solution for smart robots. First, using internet of things (IoT) intrusion prevention system design method based on network intrusion signal detection and feedforward modulation filtering design, the overall design description and function analysis are carried out, and then the intrusion signal detection algorithm is designed, and finally, the hardware design and software development for a breach protection solution for the IoT are completed, and the integrated design of the system is realized. The findings demonstrated that based on the mean value of 10,000 tests, the IoT's average packet loss rate is 0. Conclusion: This system has high accuracy, good performance, and strong compatibility and friendliness. © 2023 the author(s), published by De Gruyter.

Author keywords

internet of things; intrusion detection; smart robots

Indexed keywords

SciVal Topics

Metrics

References (19) View in search results format >

Related documents

Scientific Research Management Helping the Development of Regional Cultural Industry from the Perspective of Artificial Intelligence
Wang, J. , Hu, X.
(2022) Mobile Information Systems

Application of Cement-Based Composite Nanomaterials in Prefabricated Thin-Wall Light Steel Structure Composite Wall
Chen, X. , He, H. , Huo, L.
(2022) International Journal of Analytical Chemistry

Application of fractional-order nonlinear equations in coordinated control of multi-agent systems
Jia, X. , Cui, Y. , Patro, R.
(2023) Nonlinear Engineering

View all related documents based on references

Find more related documents in Scopus based on:

Authors > Keywords >

Open Access Published by De Gruyter September 22, 2023

Smart robots' virus defense using data mining technology

Jiao Ye, Hemant N. Patel, Sankaranamasivayam Meena, Renato R. Maaliw, Samuel-Soma M. Ajibade and Ismail Keshta

From the journal Journal of Intelligent Systems
https://doi.org/10.1515/jisys-2023-0065

Abstract

In order to realize online detection and control of network viruses in robots, the authors propose a data mining-based anti-virus solution for smart robots. First, using internet of things (IoT) intrusion prevention system design method based on network intrusion signal detection and feedforward modulation filtering design, the overall design description and function analysis are carried out, and then the intrusion signal detection algorithm is designed, and finally, the hardware design and software development for a breach protection solution for the IoT are completed, and the integrated design of the system is realized. The findings demonstrated that based on the mean value of 10,000 tests, the IoT's average packet loss rate is 0. Conclusion: This system has high accuracy, good performance, and strong compatibility and friendliness.

Keywords: internet of things; intrusion detection; smart robots

1 Introduction

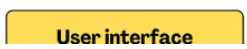
In the course of social growth, computer technology has also been innovated, computer network virus technology has developed synchronously, and has even advanced to a higher level, causing great losses to computer network users due to the computer network infrastructures' vulnerability to danger. Therefore, people began to pay attention to computer network virus defense technology [1]. Systems can effectively solve various current network virus problems and maintain security on computer network systems [2]. Computer network viruses spread rapidly, severely affecting network security and causing great damage [3]. At present, the mainstream anti-virus technology is signature technology, the biggest defect of this technology is that the code is fixed. In the face of changing viruses, the version needs to be updated continuously to ensure Internet security, and users are often in a passive defense state. Therefore, the future development trend of network virus detection is an intelligent active defense system.

A tight connection exists among computer networks and network viruses, the main ways of spreading network viruses include network e-mails, network system loopholes, and bad web pages, etc., which can deliberately damage computer network systems. The spread of computer network viruses is very rich, and the use of network system loopholes spreads network viruses. This kind of virus spread is relatively common. Computer network virus programs can use system loopholes to control each other's computers, at the same time, viruses can also search and scan folders, implement virus replication, which can invade the network system [4].

In the early stages of technological advancements in computer networks, computer network viruses mainly interfered with the programming work of network technicians. With the speedy expansion of computer technology, the development technology and the functional role of computer network viruses have changed. Today the design and development of a number of computer network viruses have been commercialized and have the characteristics to destroy computer network systems. For example, illegally obtaining online bank account numbers and passwords for profit. Nowadays, computer networks are widely used in people's daily life, people store various information on the network; therefore, computer security concerns must be taken seriously to avoid being harmed by computer network viruses [5]. Using data mining technology can, we can change the status quo of computer networks and improve the security of computers, provide conditions for the defense of network viruses, and greatly improve the defense level of computer network virus.

2 Literature review

Data mining mainly refers to analyzing and mining valuable information from massive information [6]. Figure 1 depicts the data extraction system's organizational framework.



Research Article

Jiao Ye, Hemant N. Patel, Sankaranamasivayam Meena, Renato R. Maaliw III*, Samuel-Soma M. Ajibade, and Ismail Keshta

Smart robots' virus defense using data mining technology

https://doi.org/10.1515/jisys-2023-0065
received May 22, 2023; accepted July 28, 2023

Abstract: In order to realize online detection and control of network viruses in robots, the authors propose a data mining-based anti-virus solution for smart robots. First, using internet of things (IoT) intrusion prevention system design method based on network intrusion signal detection and feedforward modulation filtering design, the overall design description and function analysis are carried out, and then the intrusion signal detection algorithm is designed, and finally, the hardware design and software development for a breach protection solution for the IoT are completed, and the integrated design of the system is realized. The findings demonstrated that based on the mean value of 10,000 tests, the IoT's average packet loss rate is 0. Conclusion: This system has high accuracy, good performance, and strong compatibility and friendliness.

Keywords: internet of things, intrusion detection, smart robots

1 Introduction

In the course of social growth, computer technology has also been innovated, computer network virus technology has developed synchronously, and has even advanced to a higher level, causing great losses to computer network users due to the computer network infrastructures' vulnerability to danger. Therefore, people began to pay attention to computer network virus defense technology [1]. Systems can effectively solve various current network virus problems and maintain security on computer network systems [2]. Computer network viruses spread rapidly, severely affecting network security and causing great damage [3]. At present, the mainstream anti-virus technology is signature technology, the biggest defect of this technology is that the code is fixed. In the face of changing viruses, the version needs to be updated continuously to ensure Internet security, and users are often in a passive defense state. Therefore, the future development trend of network virus detection is an intelligent active defense system.

A tight connection exists among computer networks and network viruses, the main ways of spreading network viruses include network e-mails, network system loopholes, and bad web pages, etc., which can deliberately

* **Corresponding author: Renato R. Maaliw III,** College of Engineering, Southern Luzon State University, Lucban, Quezon, 4328, Philippines, e-mail: rmaaliw@slsu.edu.ph
Jiao Ye: College of General Education, Jilin Animation Institute, Changchun, Jilin, 130013, China, e-mail: JiaoYe296@163.com
Hemant N. Patel: Department of Computer Engineering, Sankalchand Patel College of Engineering, Visnagar, Gujarat 384315, India, e-mail: hp15284@gmail.com
Sankaranamasivayam Meena: Department of Electronics and Instrumentation Engineering, St. Joseph's College of Engineering, OMR, Chennai 600119, India, e-mail: meena27681@gmail.com
Samuel-Soma M. Ajibade: Department of Computer Engineering, Istanbul Ticaret University, Istanbul 34445, Turkey, e-mail: asamuel@ticaret.edu.tr
Ismail Keshta: Computer Science and Information Systems Department, College of Applied Sciences, AlMaarefa University, Riyadh, 71666, Saudi Arabia, e-mail: imohamed@mcst.edu.sa

damage computer network systems. The spread of computer network viruses is very rich, and the use of network system loopholes spreads network viruses. This kind of virus spread is relatively common. Computer network virus programs can use system loopholes to control each other's computers, at the same time, viruses can also search and scan folders, implement virus replication, which can invade the network system [4].

In the early stages of technological advancements in computer networks, computer network viruses mainly interfered with the programming work of network technicians. With the speedy expansion of computer technology, the development technology and the functional role of computer network viruses have changed. Today the design and development of a number of computer network viruses have been commercialized and have the characteristics to destroy computer network systems. For example, illegally obtaining online bank account numbers and passwords for profit. Nowadays, computer networks are widely used in people's daily life, people store various information on the network; therefore, computer security concerns must be taken seriously to avoid being harmed by computer network viruses [5]. Using data mining technology can, we can change the status quo of computer networks and improve the security of computers, provide conditions for the defense of network viruses, and greatly improve the defense level of computer network virus.

2 Literature review

Data mining mainly refers to analyzing and mining valuable information from massive information [6]. Figure 1 depicts the data extraction system's organizational framework.

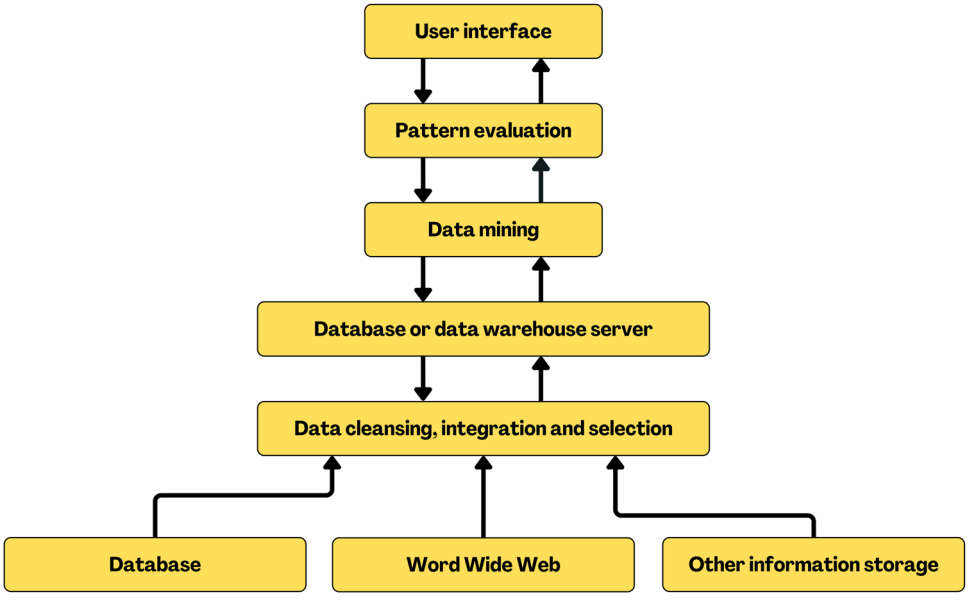


Figure 1: Data mining system structure.

As can be seen from the Figure, the valuable data are analyzed and mined from the original data, take it as the target set, and then start from data selection, data preprocessing, data transformation, etc., are carried out. Comprehensive processing of data are done to reduce data dimensions and simplify data, so as to completely remove the useless data [6].

As the process by which viruses attack systems are becoming more and more advanced and sophisticated, people put forward higher requirements for system security defense performance. Under normal

circumstances, once a computer network is invaded by a virus, lot of data present in the interconnected system are quickly tampered and destroyed by the virus; therefore, the relevant personnel should strictly follow the computer network virus defense process shown in Figure 2 to complete the system design. Because the data mining process is more complicated, during the application of data mining technology, relevant personnel must follow the defense process shown in Figure 2 to further improve the effect of virus defense and control [7].

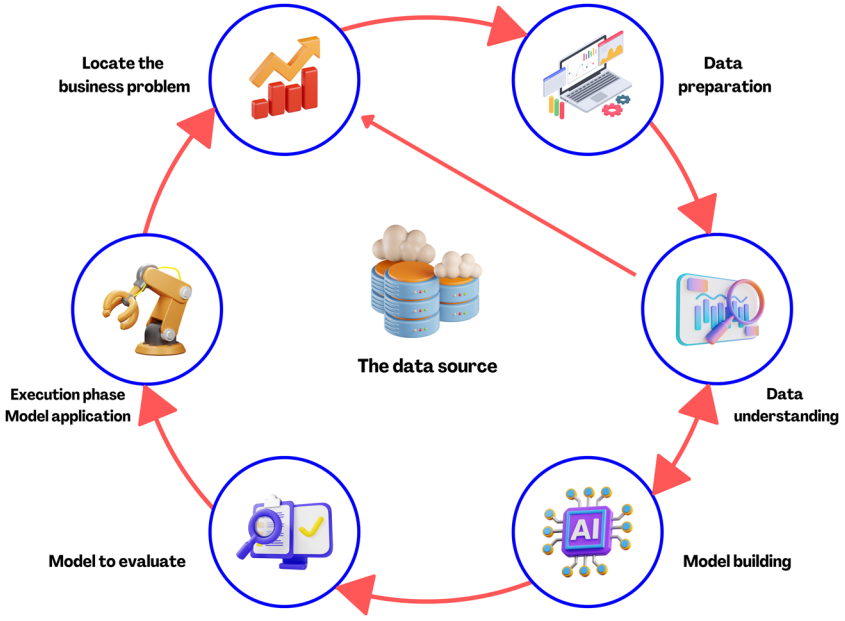


Figure 2: Robot network virus defense process.

The application environment that employs detectors and wireless connectivity has expanded more and more today with the development of wireless sensor network communication technology and Internet of Things (IoT) technology device terminals to transmit data and exchange information, forming a large-scale IoT communication system on the internet. Due to the widely distributed and self-organizing nature of IoT nodes, the IoT network environment is vulnerable to cyberattacks and intrusive viruses, in particular the penetration performance is more pronounced and the intrusion uses communication link vulnerability for identification [8]. The layers and middle layers of the IoT implement virus intrusions that pose a cybersecurity risk. IoT interference uncovering and prevention problems are studied, improving IoT security, and it has significant practical applications in network architecture and networking security of IoT. The related intrusion prevention system design methods are receiving great attention [9].

The IoT intrusion prevention and identification is based on the extraction of informational features and detection of intrusion signals at the time of intrusion. To develop and design intrusion prevention systems, high-speed digital signal processing chips were incorporated and specific research results were obtained. Among them, a method to design an IoT intrusion detection system was proposed on optimal avalanche gain control technology combined with a hardware development environment, to identify intrusion detection in the IoT environment. The intrusion detection accuracy is high, but as a result, the system design is prone to distortion and the intrusion detection accuracy is not high under the influence of strong interference [10]. Another researcher proposed a network intrusion HHT detection algorithm that introduced offset layer control, developed and designed an intrusion prevention system for the IoT using its high-performance chip, and obtained offset characteristics of network intrusion through sampling. Offset control is implemented and combined with the switch to perform the intrusion detection, the optimal design of the network intrusion

prevention system is realized, and a good detection performance is achieved, but the computational cost of the intrusion prevention system is high and the real-time performance is poor. To solve these problems, the authors propose a method to develop an internet-wide signal detection-based protection solution for the IoT and design fixed point kernel forwarding modulation and filtering bits. First, the overall design of the intrusion prevention system is carried out, then the intrusion detection algorithm design is carried out, and finally, the hardware design and software development of the intrusion prevention system is carried out [11]. Anti-intrusion for IoT is implemented. By performance verification, the designed intrusion prevention system shows excellent performance in intrusion detection [12].

3 Methods

3.1 Overall design description and algorithm design of the system

3.1.1 Overall design of IoT-oriented intrusion prevention system

In order to get the best possible architecture for the intrusion prevention system for the Internet of things, the system's total structural model must be built first. The Internet of things routing link layer is the common network followed by the layer structure link that can be summarized. The protocol stack-space layer forms the cognitive layer and the middle layer of the Internet of Things. An intrusion prevention system is vulnerable to compromises from the cognitive layer's association vulnerabilities [13]. Intermediate layer performs virus intrusion detection and is mainly composed. Among them, the virus intrusion detection module is the core unit of the total defense system, and the intrusion prevention system for the IoT uses the embedded system to develop the integrated chip and handle it [14]. Information management and the use of wireless communication technology for data transmission and virus intrusion detection analyses the clock frequency that uses PCI bus technology for data acquisition and a 32-bit or 64-bit data line for power. The IoT consists of four primitive object entities as follows: target, observer node, sensor node, and perceptual field of view. Therefore, during the development and creation of an infrastructure that will avoid intrusions on the IoT, it is necessary to complete the various installations of the intrusion prevention system for the IoT through the central software configuration, such as routing settings, location tracking system settings, location tracking system settings, etc. When a network attack occurs or the power consumption ends, it accepts the interrupt request and when a hardware device or software instruction requests the interrupt, it sends the interrupt/IACK response signal to the register and ST1 state to perform intrusion detection. Figure 3 shows the structural block diagram of the IoT intrusion prevention system designed by the author according to the description of the general design ideas and analysis of the above functional criteria [15].

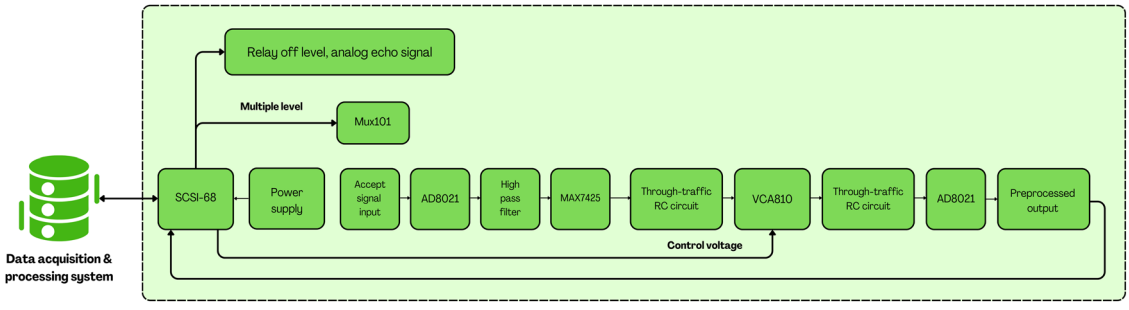


Figure 3: The block diagram of the Sybil intrusion prevention system for the IoT.

3.1.2 Sybil intrusion detection algorithm design

Based on the above construction of the overall design structure model of the Sybil intrusion prevention system for the IoT, the design and system development are carried out. Sybil intrusion prevention system design includes algorithm design, hardware design, and software design. Here the algorithm design of Sybil intrusion prevention system is first carried out. The detection algorithm is based on the signal processing algorithm. Through the construction of Sybil intrusion signal model [16], combined with signal feature extraction and detection algorithm, intrusion detection is carried out in the IoT environment. The signal model expression for Sybil intrusion is given as follows:

$$z(t) = s(t) + js(t) \otimes h(t) = s(t) + j\int_{-\infty}^{+\infty} \frac{s(u)}{t-u}\mathrm{d}u = s(t) + jH[s(t)], \tag{1}$$

where $s(t)$ is the clockwise amplitude of the Sybil intrusion signal $z(t)$, also called the envelope; $h(t)$ is the mapping phase from frequency domain to time domain, $Z(f)$ can be obtained by wavelet transform from $S(f)$, $H(f)$ is the local (or domain) stationary length of the Sybil intrusion signal. Sybil frequency component of an intrusion signal is a set of non-stationary random signals, and the spectrum of the signal is time-varying and nonlinear. Assuming that the short time interval of Sybil intrusion is defined as $v_m, m \in [1, n]$, the power spectrum writing at different moments in the Sybil invasion process is calculated.

$$\tilde{y}(t) = \iint_{\tau\varphi} b(\tau, \varphi)\exp[j2\pi\varphi t]\tilde{f}(t-\tau)\mathrm{d}t\mathrm{d}\varphi, \tag{2}$$

where $b(\tau, \varphi)$ is the non-stationary spread function, $\tilde{f}(t)$ is the frequency component in the vicinity of the window, τ is the short-time Fourier-delay, and φ is the frequency shift characteristic of the Sybil intrusion signal with time. Assuming that Sybil virus data are in the IoT attack, the signal in the vicinity of its window is randomly phase-expanded, and the time-domain expansion function of the output signal is as follows:

$$y(t) = \iint_{a,b} \rho(a, b)\frac{1}{\sqrt{|a|}} f\left(\frac{t-b}{a}\right)\frac{\mathrm{d}a\mathrm{d}b}{a^2}, \tag{3}$$

where $f(t)$ is the non-stationary spectrum of the Sybil intrusion signal, $\rho(a, b)$ is the pseudo-stationary spread function, a is the spectral density, and b is the delay parameter. In order to improve the detection performance, power spectral density weighting is adopted, and the weighting coefficient $b_0 = 0, c_k$ is utilizing an appropriate short-time windows operation, and a short-time windows functionality for adaptive detection, the power spectral density characteristics of the detection output are obtained as follows:

$$y(t) = \frac{1}{c_f}\iint W_f y(a, b)\frac{1}{\sqrt{|a|}} f\left(\frac{t-b}{a}\right)\frac{\mathrm{d}a\mathrm{d}b}{a^2}. \tag{4}$$

The IoT generates network fluctuations and jumps under attack. Using the pseudo-stationary random process analysis and processing method, the detection beam domain is obtained as follows:

$$c_f = \int_{-\infty}^{+\infty} \frac{|F(\omega)|^2}{\omega}\mathrm{d}\omega < \infty, \tag{5}$$

where $F(\omega)$ is the Fourier transform of $f(t)$, and the constant c_f is the beam high-order cumulative characteristic function of function $f(t)$. Through high-order cumulant feature extraction, the complex envelopes of Sybil intrusion features are obtained as follows:

$$s(v) = \int_0^v \sin\left(\frac{\pi}{2}x^2\right)\mathrm{d}x, \tag{6}$$

$$y(t) = u(s(t-\tau))\exp(j\omega_C s(t-\tau)), \tag{7}$$

where v represents the directional characteristic that satisfies the assumption of stationarity, $u(t)$ is the complex envelope, and ω_C is the energy density. For a wideband Sybil intrusion signal, the directional gain is

$$c(v) = \int_0^v \cos\left(\frac{\pi}{2}x^2\right)\mathrm{d}x. \tag{8}$$

Therefore, the decomposition result of the beam directivity characteristic of the Sybil intrusion signal is obtained as follows:

$$|s(f)| = A\sqrt{\frac{1}{2k}}\{[c(v_1) + c(v_2)]^2 + [s(v_1) + s(v_2)]^2\}. \tag{9}$$

The blind source separation method is used to perform intrusion detection under the time-frequency distribution, the scattering characteristic function at time t is

$$P_i(t) = \sum_{n=1}^{N} \frac{A}{r}e^{-jkr}R_{\mathrm{in}}\frac{1}{r}e^{-ikr}, \tag{10}$$

simplified to

$$P_i(t) = \frac{A}{r^2}\sum_{n=1}^{N} e^{-j2kr}a_{\mathrm{in}}e^{j\psi_{\mathrm{in}}}, \tag{11}$$

where A is the reverberation amplitude of Sybil intrusion, r is the initial frequency of the signal, $k = \frac{B}{T}$ is the total energy of the signal, and e is the FM signal bandwidth. According to the above detection algorithm design, the program design of Sybil intrusion detection is carried out, the detection module design of Sybil intrusion prevention system is carried out through the program loading module [17].

3.2 System design and implementation

3.2.1 Hardware modular design of intrusion prevention system

The hardware design and software development of the intrusion prevention system are carried out according to the general layout of the structure and the formulation of the intrusion recognition algorithm. The system is designed in a modular manner, with the main components being the filtering circuit section and the primary controller, the circuit module AD circuit module, and sensor module. It uses a feed modulation filter to perform characteristic matching of intrusion detection and configure a filter circuit.

Using an IoT-oriented intrusion signal as the initial input, a simple filter format is provided.

$$H(z) = \frac{N(z)}{D(z)}, \tag{12}$$

where $N(z)$ is the low-pass channel function of the “Sybil” intrusion prevention system, its zero point is at $z = e$ (j_0), $D(z)$ is the initial state of the equivalent low-pass channel, and from the frequency parameter a and bandwidth parameter r of the filter, the initial frequency and initial phase of the feedforward modulation filter are calculated as follows:

$$\omega_0 = \arccos\left(-\frac{a}{2}\right). \tag{13}$$

In the case that the measurement noises are not correlated with each other, through weighting, the high-frequency response characteristic function of the Sybil intrusion detection feedforward filter is obtained as follows:

$$e^{j\pi} = V(e^{j\omega_0}) = \frac{\sin\theta_2 + \sin\theta_1(1 + \sin\theta_2)e^{j\omega_0} + e^{j2\omega_0}}{1 + \sin\theta_1(1 + \sin\theta_2)e^{j\omega_0} + \sin\theta_2 e^{j2\omega_0}}. \tag{14}$$

Thus, the planned “Sybil” security system for intrusion prevention obtains the transfer function of the feedforward modulation filter.

$$H(z) = \frac{1}{2}[1 + V(z)]V(e^{j\omega}) + e^{j\Phi(\omega)}. \tag{15}$$

When the constraints are met

$$\mathrm{TW} \ll \frac{c}{2|v|}, \left|\frac{2v}{c}\right| \ll 1. \tag{16}$$

The obtained output response feature is the largest, which can meet the performance requirements of Sybil intrusion detection.

The main control circuit module is the control module for Sybil intrusion prevention detection. Using 16-bit fixed point as the control chip, the main control circuit module has 8 32-bit timer/counter functions, adopts ADG3301 for AD/DA conversion, and through AC coupling, using PCI9054's LOCAL bus design method, the data collection of the Sybil intrusion prevention system oriented to the IoT is carried out.

Program load detection module of intrusion detection algorithm recognizes internal clock fluctuations and detect virus intrusion of Internet of Things intrusion prevention system. Digital Signal Processing chip is used to program loader circuit design. The loading program is a function to execute the programming of the intrusion detection algorithm. The reset circuit of the intrusion prevention system for the Internet of Things is taken from the serial TW1 memory. The TW1 is selected to store location information for performing intrusion detection.

3.2.2 Software development

The "Sybil" intrusion prevention system for the IoT's technology is developed in accordance with the hardware architecture, the software development and processing program of the Sybil intrusion prevention system is carried out under the CCS 2.20 development platform. Using "C5409A XDS510 Emulator" for hardware online programming to realize the writing of detection algorithm and reading of data graph. The read and write operations are driven by the program of the system through the DMA controller. In Sybil intrusion prevention detection, the program is divided into user mode and kernel mode, which are generated by assembly and linking out file, intrusion prevention detection through WDM driver, and underlying hardware [18].

3.2.3 Data storage module design

Data storage methods have certain diversity and complexity. By using the system background program, the extraction and reorganization of data packets can be realized, so as to obtain valuable data. Data storage mainly includes two methods, one is the data packet storage method, and the other is the message information storage method. For data files, in specific storage, it is necessary to extract valuable data according to the design of the data link layer, at the same time, it is necessary to complete the safe transmission and storage of data. When the relevant information data of the background data record are effectively stored in the database, it is necessary to visually present these data in front of the user with the help of the foreground interface, so that the user can view and call these data in time. The user data table used in the system is shown in Table 1.

Table 1: User data sheet

Field name	Field description	Type of data	Allow nulls
Username	Log-in name	Varchar (15)	No
Pass wd	Password	Varchar (15)	Yes
Account number	Account	Varchar (15)	No
Role	Optional fields	Varchar (15)	Yes

4 Results and discussion

To evaluate the effectiveness of the "Sybil" preventive security structure for the Internet of Things, system debugging along with simulation tests are run, and the experiment's detection technique is used and is implemented by "Matlab" programming. Sybil intrusion signal center frequency test is f_0 = 1,000 Hz, the discrete sampling rate of Sybil intrusion data information is $f_s = 10 \times f_0$ Hz = 10 kHz, the bandwidth of serial port control is B = 1,000 Hz. In the above design, the WIN32 API function CreateFile () function is used to open the PCI device to execute the detection program loading, the simulation of network intrusion detection is realized, and the original data time domain waveform of Sybil intrusion signal detection oriented to the IoT is obtained as shown in Figure 4.

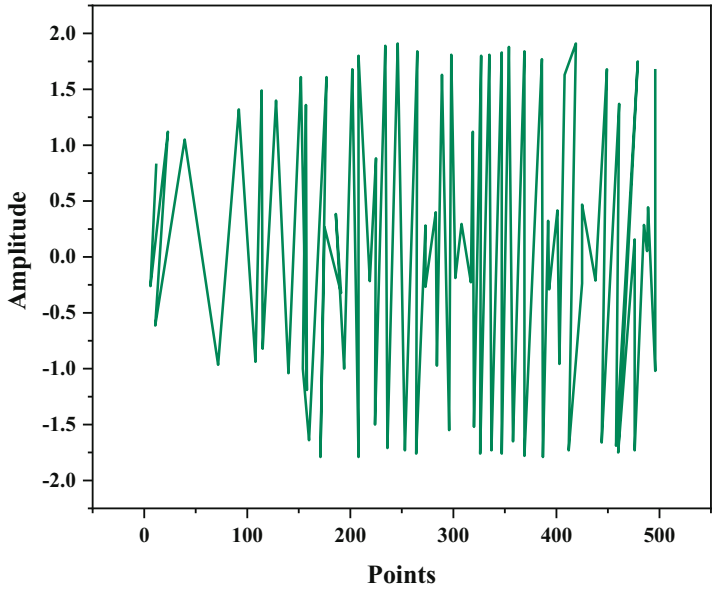


Figure 4: The original data waveform of IoT data acquisition.

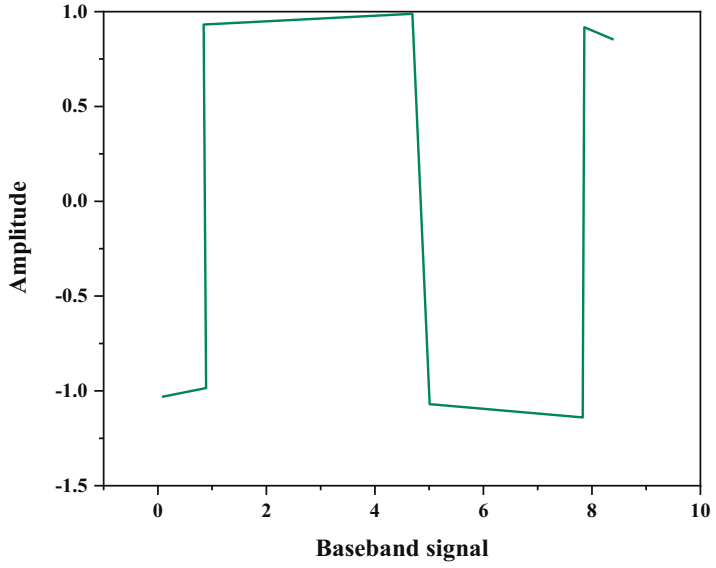


Figure 5: Signal separation results of Sybil intrusion detection.

As shown in Figure 5 below, it is difficult to effectively detect the intrusion signals under the interference of the network environment.

As can be seen in the figure, the author's intrusion prevention system method can achieve accurate separation of intrusion information characteristics, high detection accuracy, and strong anti-interference ability. As shown in Figure 6, the average packet loss rate for information transport in the IoT is 0 per 10,000 attempts on average [19].

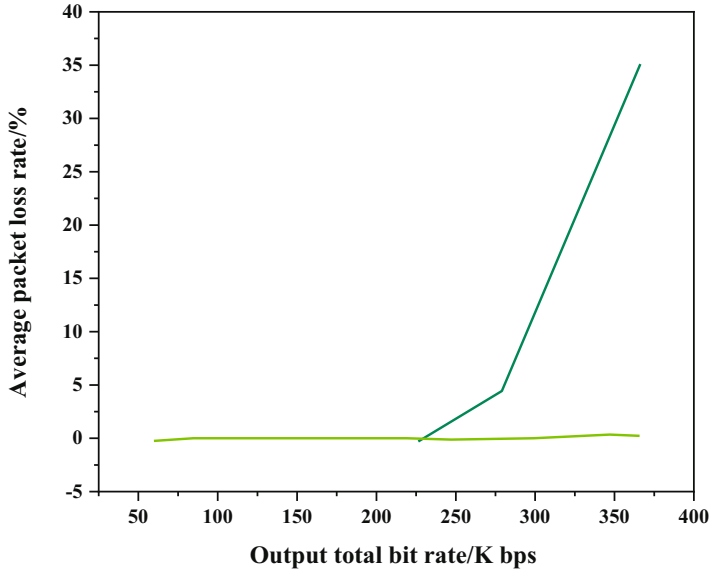


Figure 6: Performance comparison.

As shown in Figure 6, the proposed method is used to design an intrusion prevention system and by integrating the embedded design into the IoT and data transmission, the intrusion information is detected correctly, thus improving network security performance, and reducing data transmission packet loss rate. The tests show that the proposed design system has strong compatibility.

5 Conclusion

The author proposes the prevention of Malware attacks on computer networks via mining information technology. At the same time, the author studies the problem of intrusion prevention detection in the preventive system's design process and the World Wide Web of Things attacks to strengthen the World Wide Web and IoT' safety precautions. We recommend, based on network intrusion detection and 16-bit fixed-point, the Worldwide Web of Things DSP core design. First, the overall design description and functional analysis are performed, the intrusion detection algorithm is designed, the simulator is used to program the hardware online, and IoT software development of intrusion prevention system is carried out on the platform development and system integration design.

Funding information: The authors state no funding involved.

Author contributions: Jiao Ye and Hemant N. Patel provided the conceptualization, software requirement, contributed in methodology and wrote the first draft of the manuscript. Sankaranamasivayam Meena and Renato R. Maaliw III provided the data curation, contributed to the methodology and investigated the results. Samuel-Soma M. Ajibade and Ismail Keshta provided the figures, contributed in the methodology and reviewed the final draft of the manuscript.

Conflict of interest: Authors state no conflict of interest.

Data availability statement: Data shall be made available on request.

References

[1] Wang CL, Wang Y, Zeng ZY, Lin CY, Yu QL. Research on logistics distribution vehicle scheduling based on heuristic genetic algorithm. Complexity. 2021;2021(11):1–8.

[2] Mallik R, Sing D, Bandyopadhyay R. GPS tracking app for police to track ambulances carrying covid-19 patients for ensuring safe distancing. Trans Indian Natl Acad Eng. 2020;5(2):181–5.

[3] Ma J, Luo J. MDS symbol-pair codes from repeated-root cyclic codes. Designs Codes Cryptogr. 2022;90(1):121–37.

[4] Farooq Q, Shaukat Z, Zhou T, Aiman S, Li C. Inferring Virus-Host relationship between HPV and its host homo sapiens using protein interaction network. Sci Rep. 2020;10(1):8719.

[5] Wang L, Wu P. Threshold dynamics of a zika model with environmental and sexual transmissions and spatial heterogeneity. Z Für Angew Mathematik Phys. 2022;73(4):1–22.

[6] Reis F, Martins FB, Torres RR, Florêncio GWL, Cassemiro JM, Monteiro V, et al. Climate change impact on the initial development of tropical forest species: a multi-model assessment. Theor Appl Climatol. 2021;145(1):533–47.

[7] Liu J, Su Y, Lv S, Huang C. Detecting web spam based on novel features from web page source code. Secur Commun Netw. 2020;2020(5):1–14.

[8] Silwattananusarn T, Kulkanjanapiban P. Mining and analyzing patron's book-loan data and university data to understand library use patterns. Int J Inf Sci Manag. 2020;18(2):151–72.

[9] Conard NJ, Brenner M, Bretzke K, Will M. What do spatial data from sibhudu tell us about life in the middle stone age? Archaeologic Anthropologic Sci. 2022;14(8):1–22.

[10] Ramos E, Rosa UA, Ribeiro G, Villanova F, Leal E. High heterogeneity of echoviruses in Brazilian children with acute gastroenteritis. Viruses. 2021;13(4):595.

[11] Boonsong W, Ismail W, Shinohara N, Mahdaliza S, Darul J. Real-time water quality monitoring of aquaculture pond using wireless sensor network and internet of things. J Theor Appl Inf Technol. 2020;98(22):22.

[12] Fotohi R, Abdan M, Ghasemi S. A self-adaptive intrusion detection system for securing UAV-to-UAV communications based on the human immune system in UAV networks. J Grid Comput. 2022;20(3):1–26.

[13] Li B, Ge W, Liu D, Tan C, Sun B. Optimization method of vehicle handling stability based on response surface model with d-optimal test design. J Mech Sci Technol. 2020;34(6):2267–76.

[14] Wang A, Wang W, Zhou H, Zhang J. Network intrusion detection algorithm combined with group convolution network and snapshot ensemble. Symmetry. 2021;13(10):1814.

[15] Sharma A, Kumar R, Talib M, Srivastava S, Iqbal R. Network modelling and computation of quickest path for service-level agreements using bi-objective optimization. Int J Distrib Sens Netw. 2019;15:155014771988111.

[16] Raj MP, Manimegalai P, Ajay P, Amose J. Lipid data acquisition for devices treatment of coronary diseases health stuff on the internet of medical things. J Phys Conf Ser. 2021;1937:012038.

[17] Zhao XL, Liu X, Liu J, Chen J, Fu S, Zhong F. The effect of ionization energy and hydrogen weight fraction on the non-thermal plasma VOCs removal efficiency. J Phys D Appl Phys. 2019;52(14):145201.

[18] Huang R, Yang X. Analysis and research hotspots of ceramic materials in textile application. J Ceram Process Res. 2022;23(3):312–9.

[19] Liu C, Lin M, Rauf H, Shareef S. Parameter simulation of multidimensional urban landscape design based on nonlinear theory. Nonlinear Eng. 2021;10(1):583–91.

JISYS.2023.0065 - Decision Revise with Major Modifications

External Inbox ×

Journal of Intelligent Systems <onbehalfof@manuscriptcentra... Mon, Jun 12, 2023, 8:56 PM
to me

12-Jun-2023

Evidence of Review

Dear Dr. Maaliw III:

Thank you for submitting your manuscript ID JISYS.2023.0065 entitled "Smart Robots Virus Defense using Data Mining Technology" to Journal of Intelligent Systems (JISYS). Your manuscript has been reviewed and requires major modifications before acceptance. The comments of the reviewer(s) are included at the bottom of this letter.

I invite you to respond to the reviewer(s)' comments and revise your manuscript.

To revise your manuscript, log into https://mc.manuscriptcentral.com/jisys and enter your Author Center, where you will find your manuscript title listed under "Manuscripts Awaiting Revision." Under "Actions," click on "Create a Revision." Your manuscript number has been appended to denote a revision.

You may also click the below link to start the revision process (or continue the process if you have already started your revision) for your manuscript. If you use the below link, you will not be required to login to ScholarOne Manuscripts.

PLEASE MAKE SURE TO CONFIRM YOUR CHOICE ON THE WEB PAGE AFTER CLICKING ON THE LINK

https://mc.manuscriptcentral.com/jisys?URL_MASK=2e695d4e7e064b65a0f2feb181962f67

The revised paper needs to be submitted within 6 weeks from now.

When submitting your revised manuscript, you should also respond to the reviewer's comments (s). Please add
1. a point-by-point reply to the reviewers' comments
2. and/or a rebuttal against each point that is being raised

You will be able to respond to the comments made by the reviewer(s) under File Upload - File Designation - Author's Response to Reviewer/Editor Critique. Reply to the reviewer(s)' comments is mandatory; all revised manuscripts without a reply will be sent back to the author.

You will be unable to make your revision on the originally submitted version of the manuscript. Instead, revise your manuscript and save it on your computer. Please also highlight the changes to your manuscript within the document by using underlined or colored text.

Once the revised manuscript is prepared, you can upload it and submit it through your Author Center.

Your original files are available to you when you upload your revised manuscript. You may delete these files or keep them. Please pay attention to the order of your uploaded files; the first one is the reply to the reviewer(s)' comments, followed by the revised manuscript, and, if applicable, Tables and Figures, and Supplementary Material. If you decide to keep the original files, these must be the last ones in the order of your uploaded files.

Once again, thank you for submitting your manuscript to JISYS. I look forward to receiving your revision.

Kind regards
Prof. Hasan Fleyeh
Editor-in-Chief, Journal of Intelligent Systems

Reviewer(s)' Comments to Author:

Reviewer: 1

Comments to the Author
With the development of wireless sensor network communication technology and Internet of Things technology, there are more and more application environments where people use sensors and wireless communication equipment terminals to transmit data and exchange information. What system is formed.

In order to realize the optimal design of the Internet of Things intrusion prevention system, what model is first established, the Internet of Things routing link layer is an ordinary network, and the layer structure is a link. Can be

summarized as follows.

In response to these problems, the author proposes a design method of IoT intrusion prevention system based on network intrusion signal detection, and what wave position is designed.

Under normal circumstances, once a computer network is invaded by a virus, a large amount of data in the network system will be quickly tampered with and destroyed by the virus. Therefore, how should the relevant personnel complete the system design.

Using data mining technology can change the status quo of computer networks, protect the security of computers, and have other advantages.

Computer networks are closely related to network viruses. What are the main ways for network viruses to spread, which may deliberately damage computer network systems.

Reviewer: 2

Comments to the Author
Discuss the characteristics of data storage methods. Using the system background program, the data packets can be extracted and reorganized to obtain valuable data.
As can be seen from the figure, what method of the author can achieve accurate separation of intrusion information features, high detection accuracy and strong anti-interference ability.
At present, the mainstream antivirus technology is signature technology. Explain the biggest flaw of this technology.
What modules does the modular design of the system mainly consist of?
When a network attack occurs or power consumption ends, it accepts interrupt requests, and when a hardware device or software instruction requests an interrupt, where does it send an interrupt/IACK response signal.

FACULTY POSITION RECLASSIFICATION FOR SUCS

(DBM-CHED Joint Circular No. 3, series of 2022)

CERTIFICATION OF PERCENTAGE CONTRIBUTION

(Research Output with Multiple Authors)

Title of Research: Smart Robots' Virus Defense Using Data Mining Technology
Type of Research Output: Journal Article (Scopus-Indexed, De Gruyter Publication)

Instruction: Supply ALL the names of the authors involved in the publication of Research output and indicate the contribution of each author in percentage. Each author shall sign the conforme column if he/she agrees with the distribution. The conforme should be signed by all the authors in order to be considered. Please prepare separate Certification for each output.

	Name of Authors	Current Affiliations	% Contribution	Conforme *(Sign if you agree with the % distribution)*
1	Jiao Ye	Jilin Institute	16.67%	
2	Hemant Patel	Patel College of Engineering	16.67%	
3	S. Meena	St. Joseph's College of Engineering	16.67%	
4	Renato R. Maaliw III	SLSU	16.67%	
5	Samuel Soma Ajibade	Ticaret University	16.67%	
6	Ismail Keshta	AlMaarefa University	16.67%	
	** Should have a total of 100%*		100.00%	

Prepared by:

Renato R. Maaliw III, DIT
(Name and Signature)
Faculty

Certified by:

Nicanor L. Guinto, Ph.D
(Name and Signature)
Director, Office of Research Services