Hindawi
Complexity
Volume 2022, Article ID 2782811, 8 pages
https://doi.org/10.1155/2022/2782811

Research Article

Mathematical Modeling of Multiattack Behavior Discrimination in the WSN Based on Incidence Matrix

Yu Shuai-Jing and Wang Peng-Fei

Yiwu Industrial & Commercial College, Yiwu, Zhejiang 322000, China

Correspondence should be addressed to Yu Shuai-Jing; 20150810106@m.scnu.edu.cn

Received 24 July 2022; Revised 25 August 2022; Accepted 8 September 2022; Published 22 September 2022

Academic Editor: Zeljko Stevic

The current WSN is vulnerable to a variety of malicious attacks, resulting in the decline of its comprehensive performance. Multihop routing involves a number of safety and privacy issues. Problems such as snooping, sinkhole, manipulation, cloning, wormhole, spoofing, and so on affect the integrity, availability, and confidentiality of the WSNs. Therefore, this paper mainly studies the mathematical modeling of WSN multiattack behavior discrimination based on the incidence matrix. The WSN node model is used to collect relevant data and mark and map the disguised data, so as to determine the characteristics of multiattack behavior and establish the WSN multiattack behavior discrimination model based on the incidence matrix. The experimental results show that the designed multiattack behavior discrimination model can distinguish the attack type according to the characteristics, has high recognition ability, can spend a short time to effectively distinguish the attack behavior, has a low false positive rate, and can effectively improve the antiattack ability of the WSN.

1. Introduction

The wireless sensor network (WSN) has a large number of data nodes in the network, which can be used in different application fields, such as temperature and humidity detection, air pollution monitoring, water quality monitoring, body temperature monitoring, and chemical composition attack in military field [1]. The WSN layer utilises multihop communication systems to route the packets to destination, the black hole attacks, selective forwarding, the symbolic attack, the Hello flood attack, the wormhole attack, and the replicative attack of identity. Compared with the wired network, it has stronger flexibility, can collect and analyze all nodes in the network, and has higher coverage. It can cover all types of data nodes and can use and analyze network nodes flexibly. However, due to the large number of nodes in the WSN, the network structure is more complex, the signal is difficult to maintain stability in the process of wireless transmission, and the information transmission is incomplete. At the same time, WSNs are more vulnerable to malicious attacks. In the process of security research on WSNs, it is found that they are vulnerable to attacks, among which the black hole attack, DoS attack, and selective forwarding attack are the most important attack methods [2–4]. In order to improve the ability of network security and ensure the security of network environment, scholars at home and abroad have carried out relevant research on multiattack behavior. Privalov et al. built a random network contour model by simulating the superposition of the attack and legal effect on the signal by using the extreme value filtering method, detected the WSN attack behavior, and obtained the measurement index characterizing the network attack, which can effectively distinguish the attack behavior [5]. Internal attacks are initiated by nodes that have been compromised or taken. In order to assault behavior, the data are removed, replayed, manipulated, and forged, and fake routing information is provided. Since these malicious nodes are transmitted by the network and by holding the key, the internal attacks are harder, and traditional encryption and other safety mechanisms have no effect. Chi et al. used the detection and defense algorithm based on distance vector jump to analyze the WSN attack behavior and used the DV-hop algorithm to calculate the average value of the minimum hop node distance under the WSN node, so as to improve the security of WSN nodes [6]. The WSNs are independent and spatially distributed. As there is no central government, the WSN is prone to safety threats because of the random deployment of the nodes on the network. WSN attacks are well-known and are malicious. The algorithm for the localization of DV-Hop is a spanning algorithm based on the protocol on the distance vector routing [7, 8]. However, the above methods have the problems of weak recognition ability, high missing rate of attack behavior, and long discrimination time. Therefore, this paper proposes a mathematical modeling of multiattack behavior discrimination in the WSN based on incidence matrix. The incidence matrix is a rational matrix for the relationship in math, which is usually called an occurrence relationship, between two classes of objects. The incidence matrix offers a great capability for comprehensive evaluation. To express the quantitative and direct evaluation relationship, a different matrix can be used in place of the specific value of the evaluation index. It has the traits of a clear distinction between data nodes. In order to make the discriminating process of attack behavior simple, obvious, and tangible, it can mathematically quantify the characteristics of complicated multiattack behavior in the form of a matrix and analyze the data results acquired by discrimination.

The primary focus of this paper is on the mathematical modeling of WSN multiattack behavior discrimination based on incidence matrix. The WSN node model is used to collect relevant data, mark and map the disguised data, so as to determine the features of multiattack behavior, and construct the WSN multiattack behavior discrimination model based on incidence matrix. The experimental results show that the designed multiattack behavior discrimination model can distinguish the attack type according to the characteristics, has high recognition ability, can spend a short time to effectively distinguish the attack behavior, has a low false positive rate, and effectively improves the antiattack ability of the WSN.

2. Feature Modeling of Multiattack Behavior in WSNs

2.1. The WSN Node Model. The WSN is composed of three parts. The composition of sensor nodes is the basis of the WSN node model, which has the functions of data node receiving and operation; the sink node and the management node are components of auxiliary network node construction, and their main function is to connect external networks and receive external information data nodes [9]. Four key components such as the sensor unit, processing unit, transceiver unit, and power unit are used as a sensor node. The sensor architecture of the WSN multiattack behavior discrimination model based on the incidence matrix is composed of four modules, as shown in Figure 1. Each row in the matrix corresponds to a node of the graph. Each row has nonzero entries such as +1 and −1 depending upon the orientation of branch at the nodes. The entries in all other columns of that row are zero.

According to Figure 1, the wireless communication module adopts DH600 data collector to transmit and receive various sensor node information of the WSN and to efficiently collect and exchange node information. The sensor module uses AlphaProx technology to realize the conversion from nonelectric quantity to electric quantity, collect and convert the information in the monitoring area, and improve the discrimination ability of multiattack behavior. The new AlphaProx inductive distance measuring sensors offer more than accurate measurement technology with the Baumer IO-Link interface. The processor module is mainly responsible for storing and processing the data information of sensor network nodes. Another significant advantage of AlphaProx high sensitivity sensors is the quick and easy installation and operation of sensors through the innovative teach-in method. WSN's monitor conditions, such as temperature, sound, and pressure, are either physical or environmental. Modern networks are two-way, both data collection and sensor activity control. Military applications like battleground monitoring were the reason for development of those networks. The W25Q64JVSSIQ memory is selected to expand the storage range and strengthen the embedded operation ability. The energy supply module usually selects Tenda PoE30G-AT Gigabit high-power PoE power supply to provide the required energy for the operation of sensor nodes [10]. Military applications such as combat field monitoring were behind the development of sensor networks. Such systems are used for manufacturing and processing applications such as the monitoring and control of manufacturing applications and device health monitoring. The sink node is the main node connecting the current sensor network with the external network. It can collect and analyze the information of any location at any time and can fully analyze and process the external network data nodes. At the same time, the energy supply is provided by the sink node to provide greater storage space for the WSN and ensure the stable operation of the data node. By detecting the data node, the effective data are transmitted to the management node, and the monitoring task of identifying multiple attacks is issued [11]. With the support of several control and monitoring applications, wireless sensor networks (WSNs) have gained popularity among the research community. These simple and low-priced networks enable remote, real-time, and minimal human intervention monitoring processes.

The management node is a node in the communication transmission network. It can effectively monitor, calculate, and analyze all sensor network data nodes, judge whether the data nodes have multiple attacks, and report and process them in time. The management node can be used in various environments such as shell. It is easy to configure and has strong portability. It supports about 300 nodes and can effectively meet the needs of the cluster.

2.2. Preprocessing of Multiple Attacks in the WSN. WSNs have a large number of nodes and are vulnerable to many kinds of attacks. Therefore, the discrimination of the WSN has great complexity, and it needs to spend more time to

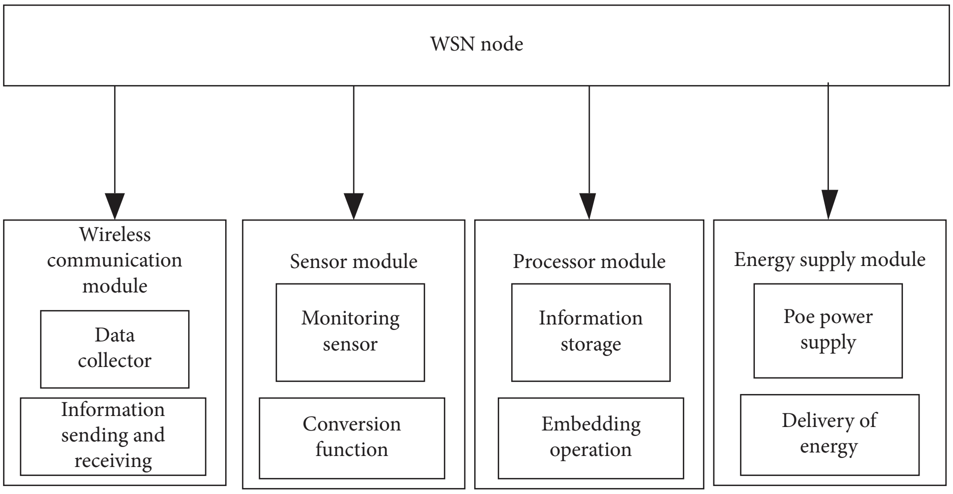

Figure 1: Composition of the sensor network.

distinguish them effectively. Therefore, preprocessing the multiattack behavior of the WSN in advance can effectively shorten the discrimination time and provide convenience for subsequent processing. High demand for bandwidth, high power consumption, service quality (QoS), data processing and compression technologies, and cross-layer design are the challenges of the WSN. Physical environment. Mobile nodes are capable of sensing, calculating, and communicating as still nodes.

2.2.1. Marking Processing of Camouflage Data Samples in Multiattack Behavior. The premise of judging the multiattack behavior of the WSN is to classify the types of the multiattack behavior, and the behavior can be effectively classified according to the characteristics of multiattack behavior [12]. Therefore, in the process of preprocessing, the attack behavior characteristics of WSN nodes are mainly considered, and the detection model of the attack behavior injection is constructed. Imperva Camouflage Data Masking permits institutions, without revealing sensitive data, to secure the way to use data for business operations. The specific process is as follows.

It is assumed that before and after the WSN is attacked, the node dataset distribution is as follows:

$$X = \{x_1, x_2, x_3, \ldots, x_n\}. \tag{1}$$

Mark the attack behavior on the node dataset and transform the original node data composed of N data into a matrix [13], with the expression

$$\mathbf{x} = \begin{bmatrix} x_{11} & x_{12} & x_{13} & \cdots & x_{1m} \\ x_{21} & x_{22} & x_{23} & \cdots & x_{2m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & x_{n3} & \cdots & x_{nm} \end{bmatrix}. \tag{2}$$

The matrix is used as the input of data in the WSN. The matrix is used to mark the attack behavior. Assuming that the camouflage data sample of the WSN subjected to multiple attacks is x', the whole sample set is preliminarily trained, and the marked node data results of the attack behavior are as follows:

$$x' = \begin{cases} -x_{nm}, & a \neq 1, \\ x_{nm}, & a = 1, \end{cases} \tag{3}$$

where a represents the attack system of camouflage data injection. If $a = 1$, it means that the node data are not attacked; if $a \neq 1$, it indicates that the node data have been attacked. At this time, the node data are marked as negative. The Imperva Camouflage Data Masking solution provides protection against theft and ensures compliance with regulations and international policies that govern the privacy and transportation of data. A static data masking software that protects data forever and decrease the exposure to compliance requirements is the Imperva Camouflage Data Masking solution. Thus, the camouflage data marking of WSN data is completed, which paves the way for the follow-up.

2.2.2. Mapping Processing of Camouflage Data. The camouflage data of multiple attacks in the WSN have the function of discrimination. The camouflage sample data in the preset time are collected and effectively distinguished according to the time threshold. When the behavior of camouflage sample data is consistent with the normal nodes of the network, it can effectively distinguish the category of the attack behavior, detect, and output data results at the same time. When it is consistent with the normal behavior, it is necessary to collect and judge the data nodes again in the camouflage sample database in the WSN. The specific process is shown in Figure 2.

The detection of the camouflage attack in the WSN is a data mapping process [14]. In the discrimination process, it is necessary to effectively distinguish the unknown behavior of data nodes, summarize them into known categories after detection and analysis, and set the mapping process as $f\colon A \longrightarrow B$, where A is the node to be detected and B is the

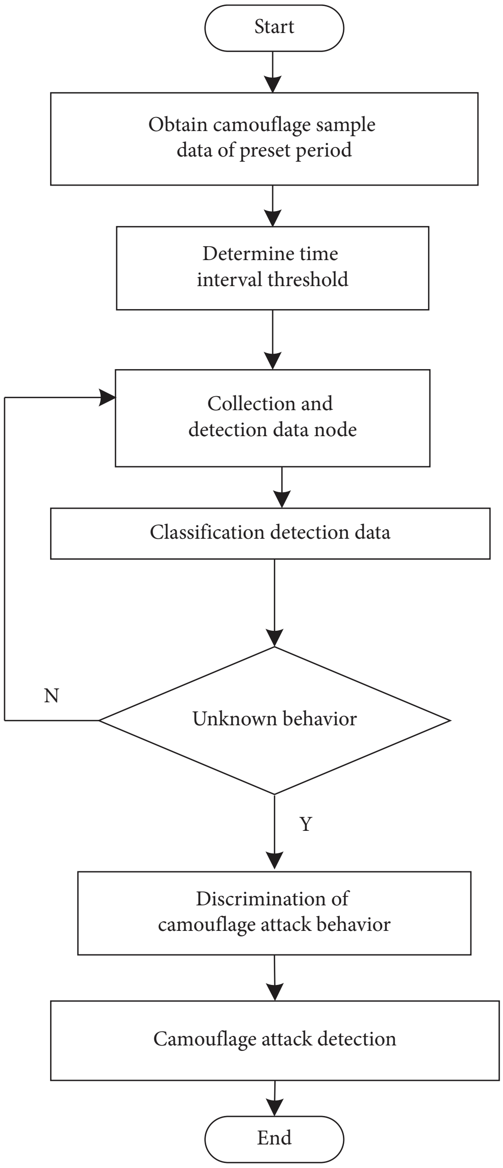
Start
Obtain camouflage sample data of preset period
Determine time interval threshold
Collection and detection data node
Classification detection data
Unknown behavior
N
Y
Discrimination of camouflage attack behavior
Camouflage attack detection
End

Figure 2: Camouflage data mapping processing flow.

known node category database. According to different data node information, it is summarized and sorted, so as to judge the new behavior category. Network mapping understands the physical connections between different network devices. The attack surface represents the sum of the system's vulnerabilities. They come in two different types: the software vulnerability digital attack surface and the hardware vulnerability physical attack surface.

2.3. Determine the Multiattack Behavior Characteristics of the WSN. Suppose that in the WSN, after the attack, the packet loss rate threshold of the whole WSN in the communication process is I, and A, B are used to represent the abnormal node dataset under the attack behavior [15]. In the WSN, a node for transmitting data information is set every t second. In order to reduce the false detection rate of multiattack behavior feature detection in WSNs, the wormhole attack mode is used to judge the attack status of nodes [16]. Set the number of surrounding nodes of node i to H, so that each node can detect and judge by itself by using the following formula:

$$\frac{K_1 Q_1 + K_2 Q_2}{H \cdot T} > I, \tag{4}$$

where K_1 and K_2 are the data test nodes in the wireless network, Q_1 and Q_2 are the information transmission nodes, and T is the transmission time of the data node. If node i meets the conditions of formula (4), the node is judged as an abnormal node. Formula (4) is the self-judgment feature of the multiattack behavior, which can effectively distinguish nodes, improve the preprocessing ability of the multiattack behavior of the WSN, and strengthen the antiattack ability of the WSN. A complex network-theory on the antiattack model is presented in this paper. The mechanism of this model is based on P2P's networks on dynamic compensation and reverse percolation.

3. Discriminant Modeling of the Multiattack Behavior in the WSN Based on the Incidence Matrix

3.1. The Incidence Matrix of Data Node States in the WSN. The incidence matrix method [17] has strong comprehensive evaluation ability when applied to WSN nodes. A separate matrix can be used to replace the specific value of the evaluation index to express the quantitative and direct evaluation relationship. It has the characteristics of concise discrimination of data nodes. It can mathematically quantify the characteristics of the complex multiattack behavior in the form of a matrix and analyze the data results obtained by discrimination, so as to make the discrimination process of attack behavior simple, clear, and concrete. This paper mainly uses the matrix form to express the relationship between multiple attack behaviors and different node states. The construction of the incidence matrix is shown in Table 1. The attack categories and object attributes of the attacked object in the WSN are represented by the matrix $[F, C]$. The object attributes include the number of communication link channels, link bandwidth, and device memory. The incidence matrix A of an undirected graph has a row for each vertex and a column for each graph's edge.

3.2. Matrix Modeling of Multiattack Behavior in the WSN. Taking the attributes and attack modes of multiple attack behaviors as matrix elements [18], the attributes of attack behaviors include the number of attack packets, the port number attacked, and the attack link and IP address. The specific methods include administrator identity intrusion, modifying configuration information, and consuming links. Similar to the matrix modeling of the data node state, the incidence matrix of the multiattack behavior can be constructed. However, due to the need to distinguish the multiattack behavior, the incidence matrix of the multiattack behavior is matrix-modeled. Thus, the correlation matrix between the attack method, attack path, and the process under multiple attack behaviors is obtained as follows:

Table 1: The incidence matrix of data node status.

	C_1	C_2	C_3	…	C_n
$F(1)$	(f_1, c_1)	(f_1, c_2)	(f_1, c_3)	…	(f_1, c_n)
$F(2)$	(f_2, c_1)	(f_2, c_2)	(f_2, c_3)	…	(f_2, c_n)
$F(3)$	(f_3, c_1)	(f_3, c_2)	(f_3, c_3)	…	(f_3, c_n)
…	…	…	…	…	…
$F(n)$	(f_n, c_1)	(f_n, c_2)	(f_n, c_3)	…	(f_n, c_n)

$$\mathbf{Z} = \begin{bmatrix} zx_{11} & zx_{12} & zx_{13} & \cdots & zx_{1m} \\ zx_{21} & zx_{22} & zx_{23} & \cdots & zx_{2m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ zx_{n1} & zx_{n2} & zx_{n3} & \cdots & zx_{nm} \end{bmatrix}. \qquad (5)$$

Formula (5) can be used to describe the attack path and the attack mode of attackers using each node and link between the WSN. In this formula, zx_{nm} represents an attack on the x_{nm} node data object.

3.3. Matrix Modeling and Analysis of the Overall Attack Process under Multiattack Behavior. After constructing the incidence matrix of data node state and the matrix model of the multiattack behavior in 3.1 and 3.2, respectively, the overall attack process is matrix-modeled [19], which is used to describe the attack path and attack process and provide further proof for judging the kind of the attack behavior. At the same time, the model can describe the state change of WSN data nodes after being attacked. The modeling framework of the WSN under multibehavior attacks is shown in Figure 2.

The state changes of information communication nodes after network attack are described, and a corresponding correlation model for the analysis and modeling of the power grid information physical system facing network attack [20] is provided. The attack behavior is calculated and analyzed according to the network attack model framework in Figure 3, where $p^{t_1k_1}$ represents the occurrence and duration of the A network attack, which can be represented by $p^{t_1k_1}$ pure delay link; t_1 indicates the moment when a network attack occurs; and k_1 indicates the duration of the attack. Considering that the attacker's attack on the target system is completed step-by-step, multiple interactions between the information communication network matrix model and the attack matrix model are designed in the modeling, and the logical correlation of the interaction is mainly reflected in the algorithm of the specific model application. So far, multiattack behavior discrimination modeling and multiattack behavior discrimination mathematical modeling of the WSN based on the association matrix are completed. The term learning discrimination refers to links between various stimuli and corresponding results or behavioral patterns. It allows animals to choose various reactions to other stimuli.

4. Experimental Verification

In order to verify the accuracy and efficiency of the proposed multiattack discrimination method, a large number of experiments are carried out under different conditions. The experimental environment is a MATLAB simulation platform, and 200 beacon nodes and 500 ordinary nodes are randomly deployed to effectively distinguish their attack behavior. Among the 200 beacon nodes, each attack corresponds to 20 beacon nodes. Repeat the above steps 1000 times to collect the training dataset and test dataset, in which the training dataset contains the attacked data of 12000 beacon nodes and the normal data of 3000 beacon nodes. In the experimental process, the attack characteristics of three attack behaviors, the relationship between the number of malicious nodes and the recognition rate, and the discrimination results are used as experimental indicators to verify the feasibility of the discrimination model. Once an abnormal behavior detection technology has been developed, intruder detection systems are used for analysing and alarming abnormal behaviors that have a significant variation to the statistical probability modeling of expected behaviors.

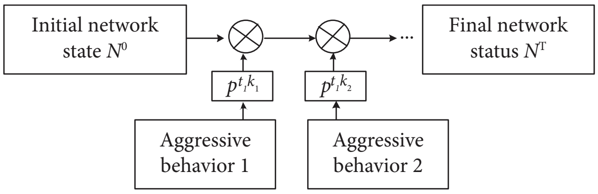

Figure 3: The network attack model framework.

4.1. Comparison of Attack Characteristics. Three attacks are understood from the level of the network layer attack as follows: the black hole attack nodes only receive data nodes and do not send data nodes, which will cause the loss of data nodes; DOS attacking nodes will cause other nodes in the network to only receive the data nodes sent by themselves and constantly send receiving requests, which is easy to cause network congestion; selective forwarding attack nodes only send node data within a specific time, but it is destructive in the selection of node information, which will disrupt the integrity of network data. The specific attack characteristics are shown in Table 2. A denial-of-service attack (DoS attack) in the computer is an attack by a cyber, in which the perpetrator attempts, by interrupting services of a host connected to the Internet, to make a machine or network resource unavailable.

4.2. Relationship between Number of Malicious Nodes and Recognition Rate. This paper analyzes the effective discrimination behavior of the configuration to the attack after several nodes in the beacon node are attacked maliciously. The experiment assumes that when the number of beacon nodes attacked by malicious attacks is 10, 15, 20, 25, 30, and 35, respectively, the model has an effective recognition rate of the black hole attack, DoS attack, and selective forwarding attack. The results are shown in Figure 4. A denial-of-service attack (DoS) is an attack that aims to shut down a machine or a network to prevent its intended users from accessing it. The congestion control is a particularly important area

Table 2: Information table of three attack characteristics.

Type of attack	Attack characteristics
The black hole attack	Only receives data, do not forward data to the base station, and do not send any collected data
The DOS attack	Keeps sending packets, resulting in network congestion
The selective forwarding attack	Sends data packets or forward fusion data to the base station in a specific time period

Table 3: Recognition rate analysis.

	Black hole attack (%)	DOS attack (%)	Selective forwarding attack (%)	Average recognition rate (%)
This method	96.7	95.8	93.7	95.4
The reference [5] method	94.8	93.7	91.2	93.2
The reference [6] method	95.3	94.1	92.6	94.1

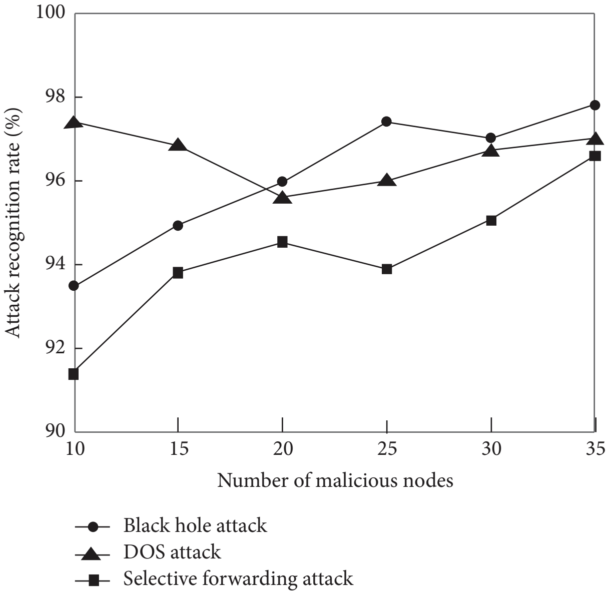

Figure 4: Relationship between number of malicious nodes and recognition rate.

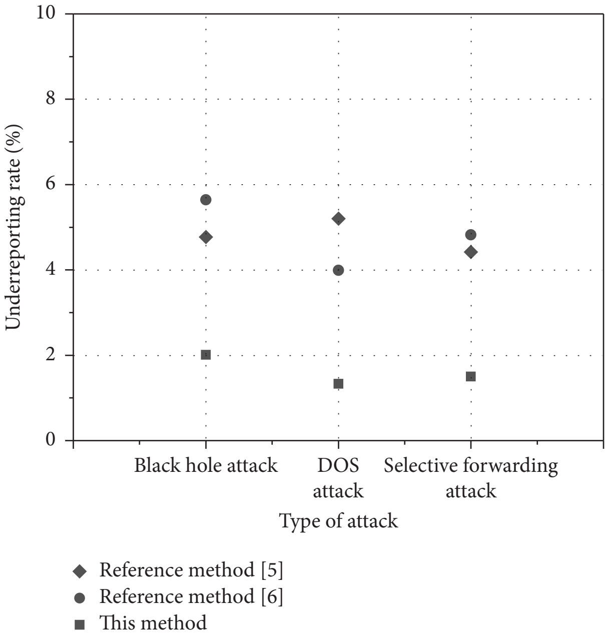

Figure 5: Discrimination results of the false alarm rate.

within WSNs, in which traffic becomes greater than the total or individual capacities of the underlying channels.

According to Figure 4, when the number of beacon nodes attacked by malicious attacks increases, the recognition rate of the algorithm for attack types sometimes increases and sometimes decreases. Therefore, there is no obvious correlation between the attack recognition rate and the number of beacon nodes attacked because this paper fully considers the characteristics of the three attack behaviors in the feature selection stage. Although the number of malicious nodes increases and changes the network topology and other information, the recognition model can still judge the attack type according to the characteristics, and the average recognition rate of the three attack behaviors in this experiment reaches 95.4%.

4.3. Comparison of Discrimination Results under Multiple Aggressive Behaviors. In order to further analyze the reliability of the model discrimination in this paper, the identification rate of the attack behavior can be distinguished by this method, the reference [5] method, and the reference [6] method. The higher the average identification rate is, the better the stability of the model discrimination. Compare the attack recognition rates of the three methods, and the test results are shown in Table 3.

According to the model recognition rate analysis in Table 3, it can be concluded that the method in this paper has certain advantages in judging the attack behavior, with an average recognition rate of 95.4%, which is higher than 93.2% of the reference [5] method and 94.1% of the reference [6] method. Therefore, in order to verify the actual situation of the model under the multiattack behavior of the WSN, this paper compares and analyzes the method in this paper with the reference [5] method and the reference [5] method and obtains the specific results of the missing report rate and discrimination time of the attack behavior. The test results are shown in Figure 5 and Figure 6.

According to Figure 5, the average miss rate of the three attack behaviors in this method is 1.86%. Because this paper uses the incidence matrix algorithm to build a model to effectively analyze the characteristics of the attacked behavior of sensor network nodes, it can effectively distinguish

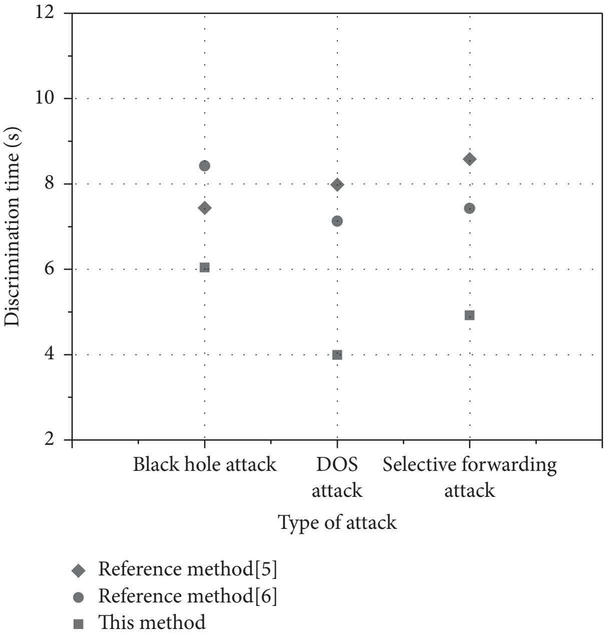

Figure 6: Discrimination of the attack time.

multiple attack behaviors in the WSN and greatly reduce the miss rate of attack behaviors. The missing reporting rates of the reference [5] method and the reference [6] method were 4.54% and 5.12%. The incidence matrix is a Boolean matrix of two dimension in which the vertices and columns represent each side of the incidence matrix. The entries show if the vertex in a line occurs at the edge of a column. One way to display a graph is by the incidence matrix.

According to Figure 6, the discrimination time of this method for the multiattack behavior is short, and the average time is only 5 s, while that of the reference [5] method is 8 s and that of the reference [6] method is 7 s. This shows that the model designed in this paper has strong discrimination ability to attack behavior and can effectively improve the antiattack ability of the WSN.

5. Conclusion

In this paper, a mathematical model of multiattack behavior discrimination in the WSN based on the incidence matrix is designed. Compared with the traditional WSN attack behavior analysis method, the incidence matrix method has a better antiattack ability in the process of data node acquisition and identification. Finally, through experimental verification, in the case of the black hole attack, DoS attack, and selective forwarding attack, the effective recognition rate of data nodes is 95.4%, the false alarm rate of multiattack behavior is 1.86%, and the discrimination attack behavior is 5 s. It is proved that the multiattack behavior discrimination model of the WSN constructed by this method has a good application effect.

Data Availability

No data were used to support the findings of this study.

Consent

Not applicable.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

References

[1] J. Kim, D. Lee, J. Hwang, S. Hong, D. Shin, and D Shin, “Wireless sensor network (WSN) configuration method to increase node energy efficiency through clustering and location information,” *Symmetry*, vol. 13, no. 3, pp. 390–401, 2021.

[2] G. Amudha, “Dilated transaction access and retrieval: improving the information retrieval of blockchain-assimilated Internet of things transactions,” *Wireless Personal Communications*, vol. 2021, pp. 1–21, 2021.

[3] B. M. Sahoo, H. M. Pandey, and T. Amgoth, “GAPSO-H: a hybrid approach towards optimizing the cluster based routing in wireless sensor network,” *Swarm and Evolutionary Computation*, vol. 60, Article ID 100772, 2021.

[4] N. T. Tam, V. T. Dat, P. N. Lan, H. T. Thanh Binh, L. T. Vinh, and A. Swami, “Multifactorial evolutionary optimization to maximize lifetime of wireless sensor network,” *Information Sciences*, vol. 576, pp. 355–373, 2021.

[5] V. M. Kuthadi, R. Selvaraj, S. Baskar, P. M. Shakeel, and A. Ranjan, “Optimized energy management model on data distributing framework of wireless sensor network in IoT system,” *Wireless Personal Communications*, vol. 2021, pp. 1–27, 2021.

[6] X. Chi, Y. Wang, J. Gao et al., “Study of photoluminescence characteristics of CdSe quantum dots hybridized with Cu nanowires,” *Luminescence*, vol. 31, no. 7, pp. 1298–1301, 2016.

[7] S. J. Achar, C. Baishya, and M. K. A. Kaabar, “Dynamics of the worm transmission in wireless sensor network in the framework of fractional derivatives,” *Mathematical Methods in the Applied Sciences*, vol. 45, no. 8, pp. 4278–4294, 2022.

[8] H. Zhao, Z. Liu, X. Yao, and Q. Yang, “A machine learning-based sentiment analysis of online product reviews with a novel term weighting and feature selection approach,” *Information Processing & Management*, vol. 58, no. 5, Article ID 102656, 2021.

[9] N. T. Nguyen, B. H. Liu, V. T. Pham, and T. Y. Liou, “An efficient minimum-latency collision-free scheduling algorithm for data aggregation in wireless sensor networks,” *IEEE Systems Journal*, vol. 12, no. 3, pp. 2214–2225, 2018.

[10] Z. Xi, X. Kan, L. Cao et al., “Research on underwater wireless sensor network and MAC protocol and location algorithm,” *IEEE Access*, vol. 7, pp. 56606–56616, 2019.

[11] C. Thomson, I. Wadhaj, Z. Tan, and A. Al-Dubai, “A mobility aware duty cycling and preambling solution for wireless sensor network with mobile sink node,” *Wireless Networks*, vol. 27, no. 5, pp. 3423–3439, 2021.

[12] S. A. B. Danique, B. B. Erik, F. S. B. E. Barbara, B. Jan, and V. Robbert-Jan, “Associations of multiple trauma types and MAOA with severe aggressive behavior and MAOA effects on training outcome,” *European Neuropsychopharmacology*, vol. 30, no. 6, pp. 66–74, 2020.

[13] K. Sekar, K. Suganyadevi, and P. Srinivasan, “Energy efficient data gathering using s-temporal compressive sensing for WSNs,” *Wireless Personal Communications*, vol. 117, no. 2, pp. 1279–1295, 2021.

[14] J. Leopold, B. Mcmillin, R. Stiffler, and N. Lutes, "Comparison of design-centric and data-centric methods for distributed attack detection in cyber-physical systems," *Critical Infrastructure Protection XIV*, Springer, New York, NY, USA, 2020.

[15] P. Wanda and H. J. Jie, "DeepFriend: finding abnormal nodes in online social networks using dynamic deep learning," *Social Network Analysis and Mining*, vol. 11, no. 1, pp. 1–12, 2021.

[16] S. Kumar and V. K. Chaurasiya, "A multisensor data fusion strategy for path selection in Internet-of-Things oriented WSN (WSN)," *Concurrency and Computation: Practice and Experience*, vol. 30, no. 18, pp. e4477.1–e4477.14, 2018.

[17] W. Lim, G. Khemka, D. Pitt, and B Browne, "A method for calculating the implied no-recovery three-state transition matrix using observable population mortality incidence and disability prevalence rates among the elderly," *Journal of Population Research*, vol. 36, no. 3, pp. 245–282, 2019.

[18] M. Hassani, "105.24 Conditional 2 × 2 matrices with three prime elements and given determinant," *The Mathematical Gazette*, vol. 105, no. 563, pp. 305-306, 2021.

[19] W. Xiong, E. Legrand, O. Åberg, and R. Lagerstrom, "Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix," *Software and Systems Modeling*, vol. 21, no. 1, pp. 157–177, 2021.

[20] M. Kumar Ashok, M. Sethumadhavan, and K. V. Lakshmy, "Holistic analytics of digital artifacts: unique metadata association model," *International Journal of Digital Crime and Forensics*, vol. 13, no. 5, pp. 78–100, 2021.