Wireless Network Safety Status Prediction Based on Fuzzy Logic

Xiao Xue[1], Yangbing Zheng[2,4] and Chao Lu[3,*]

[1]*School of Information Engineering, Nanyang Institute of Technology, Nanyang, Henan, 473004, China*
[2]*College of Mechanical and Electronic Engineering, Nanyang Normal University, Nanyang, Henan, 473065, China*
[3]*Nanyang Zehui Technology Co., LTD, Nanyang, 473000, Henan, China*
[4]*Qinghai Wandong Ecological Environment Development Co.LTD, Geermu, Qinghai 816000, China*
E-mail: leo_phi856@163.com
[*]*Corresponding Author*

Received 08 March 2023; Accepted 29 March 2023;
Publication 21 June 2023

Abstract

In WN environment, network safety status means to state of information managing in various WN environments, WN transmission information safety status assessment is one of primary research directions in this territory. Existing network safety status awareness methods are difficult to adapt to real-time changes of network structure, and WN environment is complex and changeable, and they can only analyze the current network safety status, and it is difficult to predict and analyze overall tendency of WN safety status. In order to resist potential attacks, evaluate safety of network and detect attack means in network in a timely manner, this paper introduces fuzzy logic to propose a safety status prediction model for wireless sensor networks, which can help administrators to timely perceive and comprehensively grasp the real-time status of network and predict future advancement direction. In order to assess current network status, a safety status evaluation model for

Journal of Cyber Security and Mobility, Vol. 12_4, 589–604.
doi: 10.13052/jcsm2245-1439.1247

wireless network (WN) depended on fuzzy logic is presented. In cluster head node, neighborhood rough set is used for feature extraction to reduce energy consumption of redundant data on the node. Balance data by synthesizing a few over-sampling techniques, and then use random forest to detect attacks on the network to identify attack types. Combined with the status element acquisition mechanism, three status indicators, namely attack frequency, total number of attacks and threat factor, are extracted. According to the status indicators and status calculation method, the network safety status value is calculated, and current network safety status is evaluated by referring to network safety level divided by National Internet Emergency Response Center. Neighborhood rough set is applied to complete attribute reduction, which can effectively deal with underwater mixed data and obtain feature subsets with same classification capability as initial data. Safety status of WSN is predicted based on random forest. The risk degree of WN status is divided into fuzzy subsets, and the process of dynamic prediction of safety status is designed. Based on test values, highest input signal spectrum of the system is 30 mV, and the lowest input signal spectrum is -15 mV, which is consistent with the selected 120 groups of status data sequence diagram, the fluctuation amplitude of the input signal under $40\sim62$ groups of samples is small, basically unchanged, consistent with the selected 120 groups of status data sequence diagram. Fuzzy logic model represented by star broken line has higher precision than decision tree and the limit learning machine in all five different attack types. mapped network safety status grade can also effectively express the actual network safety status. indicating that the prediction results of the system are accurate.

Keywords: Fuzzy logic, wireless network, safety status, prediction.

1 Introduction

In WN environment, network safety status means to state of information managing in various WN environments. To some extent, this network state is considered as change direction of network status environment. In process of real management, if a user's operating manual action changes, tendency of WN safety status will alter, and direction of WN safety status can indicate tendency of WN safety status with effect. Currently, with the rapid development of computer network, WN communication has been broadly applied to various fields. However, in context of widespread application, information transmitted by customers has also meet with steal, destruction and other

hazards, which immediately causes a serious steal to safety of entire network. Therefore, WN transmission information safety status assessment is one of primary research directions in this territory [1].

In present status of increasingly frequent network attacks, traditional network safety technology only describes current network safety status in a certain way, and can not satisfy requirement of network safety managers to keep abreast of current network safety status. WN safety status real-time assessment technique integrates several uses such as network invade inspection, preventing strategies and inframicrobe inspection system. It can provide reliable decision-making basis for network safety managers and minimize loss of network safety caused by unknown network attacks [2]. The current network safety status awareness method is at the initial stage. For complex attack forms, it is impossible to evaluate the stage and degree of harm of malicious attacks, and it is difficult to correctly predict future safety status of WNs. under these circumstances. How to perceive network safety status in real time and accurately assess future WN safety status has become main matter to be handled in field of WN safety management. It has received widespread attention and has achieved many good results [3].

At present, domestic and foreign scholars have made certain achievements in research of WN safety status. In view of uncertainty and fuzziness of factors affecting the WN safety status, the fuzzy set theory can better quantify the cause of such problems, and quantitatively analyze and obtain the dangerous degree of the WN safety status [4]. Many prediction methods for WN safety status have been developed. Method of network safety status awareness according to Markov game was presented. Based on the Markov game model, by solving the Nash equilibrium point of the network safety status awareness model, effect of game between offensive and defensive sides on WN safety was determined, and the fusion result of the network safety status awareness information was used to evaluate the network safety status. A WN status safety status assessment method based on historical data mining is proposed. This method uses historical data to model current safety status of WN, and inputs modeling results into the real-time operation state estimation model of WN. Get real-time operation status of network at the current stage. The historical data model is used to predict the safety status of the network in the future. The safety status assessment model built by the above methods has strong coupling with the data sources in the actual WN [5]. Some research achievements have been obtained by some scientists, Pranav M. Pawar et al. addressed behavioural modeling of medium access control security attacks in WSNs, which is benefit for establishing efficient

and secure MAC clayer protocols [6]. Elena Doynikova et al. considered development and application of a semantic model for security evaluation [7]. Shishir Kumar Shandilya proposed a network test-bed for examining new security concepts like cyber immunity [8]. Sunil Kumar et al. proposed a trusted third-party auditor (TPA) model which uses lightweight cryptographic system [9]. Existing methods are depended on results of WN safety status assessment. The safety status is acquired by building status model. The disadvantages of these two methods are:

(1) Existing network safety status awareness methods are difficult to adapt to real-time changes of network structure, and WN environment is complex and changeable. To evaluate its safety status, it is necessary to analyze the information systems at all levels of the network. These systems are generally characterized by multiple levels of structure and complex logical structure. When the structure of the network information system changes. Safety status assessment results of model have large deviations, which makes it difficult to quickly and accurately judge network safety status.
(2) The existing methods can only analyze the current network safety status, and it is difficult to predict and analyze overall tendency of WN safety status.

Compared with other risk assessment methods, the fuzzy logic method can solve the uncertainty caused by the lack of or insufficient evidence and the lack of clear boundary attribute. Fuzzy logic can use the language terms expressed by experts to evaluate the safety behavior of the system. Therefore, the fuzzy logic risk assessment proposed in this research can effectively show risk degree of safety status in WNs. Presented method can effectively solve localizations of conventional methods, and has high efficiency and high quality robustness.

2 Quantitative Model of WN Safety Status

In process of real-time quantitative evaluation of WN safety status. Capability opportunity intention model for real-time forecasting of WN safety status is established from three levels of WN attacker, defender and network environment. The uncertain reasoning means is used to enhance analysis ability of WN safety managers on uncertain safety status awareness elements, and WN safety real-time status value is computed by integrating WN node capability, opportunity and intention index set. The analysis flow chart is as follows.

Starting from WN attack and defense environment composed of WN attacker, defender and network environment, WN safety status *SA* is modeled as $SA = (CI, OI, II)$, CI, OI and II represent the capability index set, opportunity index set and intention index set in WN. For the uncertain relationship between the sensing elements in the WN safety statusal awareness model, uncertainty reasoning model is introduced. Enhance analysis capability of uncertain factors in model. Assume that an element in the perception model can be obtained by reasoning n different elements. For instance, a group of network safety attack sequences are triggered according to vulnerability v_1, and n credibility can be obtained during the reasoning process. These credibility can be comprehensively analyzed, and the final credibility can be given by using the following formula [6]:

$$C(h_1, h_2, \ldots, h_n) = |C(h_1) + C(h_2) + \cdots + C(h_n)| \tag{1}$$

According to reliability of WN safety status real-time evaluation model calculated by the above formula, the model capability index, opportunity index and intention index are computed by applying uncertainty reasoning means. The specific steps are as follows.

The capability index of a node in the WN in the observation period is related to corresponding safety status set of node. It is also affected by the safety status element set of its interactive nodes. The capability index of network node *i* in the observation period *t* is calculated by

$$CI_i(t) = q_1(B_i(t), W_i(t), E_i(t)) + \sum_{s_{ij} \in T(t)} C(E_i(t)) \tag{2}$$

Assume that result obtained from the above formula is at a certain observation time $t = 1$. Then it is only necessary to calculate corresponding capability index of the node *i* based on its own safety status elements, $s_{ij} \in T(t)$ represents a certain service that the network node can provide at present, $q_1(\cdot)$ represents the specific capability index calculation method, $B_i(t)$ represents the combination of attack sequences faced by the network node *i* in the observation period *t*, $W_i(t)$ represents the vulnerability set of the network node *i* in the observation period t, and $E_i(t)$ represents the network protection strategy set in the observation period *t*, which is calculated by [7]

$$q_1(B_i(t), W_i(t), E_i(t)) = \sum_{k=1} C(g_i(t) \wedge z_i(t)) \tag{3}$$

where $g_i(t)$ is *k*th group attack sequence in WN, $z_i(t)$ is protection success probability of WN protection mechanism.

It is assumed that the opportunity index caused by the vulnerability of the network node is known. When a new attack occurs, the vulnerability change of the node will cause the change of the opportunity index, resulting in the change of WN safety status, and attack and defense opportunity index of affecting WN safety status assessment model is calculated by [8]

$$OI_i(t) = r_1(W_i(t), E_i(t)) + \sum_{s_{ij} \in T(t)} (C(E_i(t) \vee E_j(t-1)) \tag{4}$$

where $E_j(t-1)$ is network protection policy set during observation period $t-1$.

Intention index of node *i* in observation period *t* is calculated by

$$II_i(t) = b_1(J(t), W(t), T(t)) = \tau_1 J_i(t) + \frac{\tau_2 \sum_{k=1}^{m} W_{ik}(t)}{\sum_{h=1}^{m} W_h(t)} + \frac{\tau_3 \gamma_i}{\gamma_{\max}} \tag{5}$$

where $J_i(t)$ is importance of resources undertaken by node *i* in the observation period t, $\sum_{k=1}^{m} W_{ik}(t)$ is proportion of importance of this part of resources undertaken by this node *i* to the sum of the importance of all network resources. $W_{ik}(t)$ is importance of *k*th resource undertaken by node *i* in the observation period *t*, $W_h(t)$ is importance of *h*th resource in WN attack and defense scenario, γ_i is connectivity of node *i* in whole network, $\gamma_{\max}$ is maximum connectivity of all nodes, τ_1 is importance coefficient of network resource, τ_2 is business importance coefficient, τ_3 is connectivity coefficient of node.

Real-time status value of WN safety is calculated by integrating node capability, opportunity and intention index set is calculated by

$$SS(t) = \sum_{i=1}^{N} (C(CI_i(t), OI_i(t), II_i(t)) \tag{6}$$

where N is number of nodes in WN.

WN safety status is classified to five grades, which concludes excellent, good, medium, poor and dangerous. Use different numerical quantification levels between 0 and 1 to find out the contrast WN safety status level in terms of safety status value, so as to evaluate current WN status. Wireless safety status level is listed in Table 1.

In order to assess safety status of WNs and fully understand impact of safety threats on WNs, status elements are extracted from the perspective of attack. Analyze the correlation between safety data, and according to the

Table 1 Wireless safety status level

Safety Status Value SS	Safety Status Level	WN Status
(0,0.2]	Excellent	Network is normal
(0.2,0.4]	Good	Network is under slight threat
(0.4,0.6]	Medium	Network is under moderate threat
(0.6,0.8]	Poor	Network is under serious threat
(0.8,1]	Dangerous	Network is under super heavy threat

acquisition principle of safety status elements, propose the status assessment factors based on attack indicators, which are attack frequency factor AN_i, attack total amount factor TN and attack threat factor TH_i.

3 WN Safety Status Prediction Model by Using Fuzzy Logic Model

WN safety status evaluation is the key link of WN safety status awareness technology. It extracts status indicators that involve WN safety from information, and evaluates entire status of the current WN by analyzing the quantitative status indicators. In order to fully understand the damage degree of WN caused by attack threat, a WN safety status evaluation model according to fuzzy logic is constructed [9].

(1) Feature extraction by using neighborhood rough sets

Attribute reduction is to dispel attributes with low importance on the premise of preserving classification ability. However, the traditional rough set theory can not deal with continuous data well. To solve this problem, the neighborhood rough set is applied to complete attribute reduction, which can effectively deal with underwater mixed data and obtain feature subsets with same classification capability as initial data. The selection of feature subset directly affects the result of final status assessment, so feature selection technology is very important in network safety status awareness.

Assume that the neighborhood decision system is represented by $NDS = <FV, CA, DA, AV, l, \Delta, \varepsilon>$, where $FV = \{x_i | i = 1, 2, \ldots, m\}$ is non empty finite sample set, $CA = \{c_i | i = 1, 2, \ldots, m\}$ is condition attribution set, DA is decision attribution set, $AV = \bigcup_{b \in CA \bigcup DA} V_b$ and V_b is set of attribution b; $l : FV \times \{CA \bigcup DA\} \rightarrow AV$ is mapping function; $\Delta \rightarrow [0, \infty]$ is distance function, ε is neighborhood radius coefficient, $\varepsilon \in [0, 1]$ [10]. This neighborhood decision system is simplified as $NDS = <FV, CA, DA, \varepsilon>$.

For any sample $x, y \in FV$, condition attribution sub set $SC \in CA$, Δ_{SC} is Euclidean distance function, and then neighborhood relationship of SC and neighborhood class of x on SC are respectively expressed by [11]

$$NB_{\varepsilon}(SC) = \{(x, y) \in FV \times FV | \Delta_{SC}(x, y) \leq \varepsilon\} \tag{7}$$

$$\eta^{\varepsilon}_{SC}(x) = \{y \in FV | \Delta_{SC}(x, y) \leq \varepsilon\} \tag{8}$$

Given $NDS = <FV, CA, DA, \varepsilon>$, for any $SC \in CA$ and $X \in FV$, $x_k \in FV$, upper and lower approximation sets of X about SC are respectively expressed by

$$\overline{SC}(X)_{\varepsilon} = \{x \in FV | \eta^{\varepsilon}_{SC}(x_k) \bigcap \mathrm{X} \neq \Phi\} \tag{9}$$

$$\overline{SC}(X)_{\varepsilon} = \{x_k \in FV | \eta^{\varepsilon}_{SC}(x_k) \subseteq \mathrm{X}\} \tag{10}$$

Given $NDS = <FV, CA, DA, \varepsilon>$, for any $SC \in CA$ and $X \in FV$, neighborhood approximation accuracy and neighborhood roughness of X about SC are respectively expressed by

$$\lambda^{\varepsilon}_{SC}(X) = \frac{\underline{SC}(X)_{\varepsilon}}{\overline{SC}(X)_{\varepsilon}} \tag{11}$$

$$\xi^{\varepsilon}_{SC}(X) = 1 - \lambda^{\varepsilon}_{SC}(X) \tag{12}$$

Given $NDS = <FV, CA, DA, \varepsilon>$, for any $SC \in CA$, $FV/DA = \{DA_1, DA_2, \ldots, DA_n\}$, Positive field and dependence of DA on SC are respectively expressed by [12]

$$PF^{\varepsilon}_{SC}(DA) = \sum_{k=1}^{l} \underline{SC(da_k)_{\varepsilon}} \tag{13}$$

$$\beta^{\varepsilon}_{SC}(DA) = \frac{|PF^{\varepsilon}_{SC}(DA)|}{|FV|} \tag{14}$$

where $da_k \in FV/DA$, $j = 1, 2, \ldots, n$.

In wireless sensor network, cluster head nodes process data, and use neighborhood rough sets to select features at cluster head nodes. To avert problem of excessive load due to excessive data dimension, the redundant characteristics are eliminated in the way of dimensionality reduction in cluster head with strong computing power, and minimum attribution subset with same classification performance as initial information collection is acquired.

The collected information is considered as $NDS = <FV, CA, DA, \varepsilon>$, where FV is domain that represents all attack data samples, $CA = AF \bigcup AK$, AF is attack feature, AK is attack type, DA is each eigenvalue set [13].

The main step of feature selection based on neighborhood rough set is to first calculate neighborhood dependency and signification of data feature properties, obtain the core attributes, then select the suboptimal attributes, obtain the optimal reduction subset, and finally transmit it to aggregation node through cluster head node.

(2) Safety status prediction based on random forest

Two stochastic vectors X and Y are known, components of forest $\{h(X)\}$ are m decision trees $\{h_1(x), h_2(x), \ldots, h_{\mathrm{m}}(x)\}$, then boundary function definition formula is expressed by

$$BF(X,Y) = MEAN_m(FF(h_m(X) = Y)) - \max_{j=Y} MEAN_m(FF(h_m(X) = j)) \tag{15}$$

where $FF(\cdot)$ is feature function, Y and j are correct and wrong classification vectors, $MEAN_m(\cdot)$ is mean value taken, confidence level of the classifier increases with the increase of the function value.

Assume that the classification probability of making a correct decision is $P(h_m(X) = Y)$, the extreme value of the residual classification probability of making a wrong decision is $\max_{j \neq Y, j=1} P(h_m(X) = j)$, and the target variable is not less than two categories, marginal function equation of random forest is derived as follows

$$BR(X,Y) = P(h_m(X) = Y) - \max_{j \neq Y, j=1} P(h_k(X) = j) \tag{16}$$

In process of building a random forest, there is a corresponding original data set and a data set that has not been extracted for any decision tree $h_m(X)$. If $UE_m(X)$ is set to be an un-extracted data set, the proportion of random vector X with voting category Y_j in the set is $ZP_m(X, Y_j)$, the calculation formula is as follows [14]

$$ZP_m(X, Y_j) = \frac{\sum_{m=1}^{M} FF(h_m(X) = Y_j \in UE_m(X))}{\sum_{m=1}^{M} FF(h_m(X), (X,Y) \in UE_m(X))} \tag{17}$$

where, M represents amount of training sample data. Denominator part in above formula represents total number of samples of all the un-extracted data

sets, and numerator part represents total number of correct classification of each decision tree and its corresponding un-extracted data sets.

For probability estimation result of correct classification of random forest, if the proportion $ZP_m(X, Y_j)$ is used, it is necessary to introduce two variables of random forest strength and correlation degree.

Expectation of random forest edge function is its strength variable, and definition formula is as follows [15]

$$SF = E(P(h_m(X) = Y) - \max_{j \neq Y, j=1} P(h_m(X) = j)) \tag{18}$$

where $E(\cdot)$ is mathematical expectation.

Classifier strength estimation formula is deduced as follows:

$$SE' = \frac{1}{n} \sum_{i=1}^{M} ZP(X_i, Y) - \max_{j \neq Y, j=1} ZP(X_i, j)) \tag{19}$$

Random forest correlation variable is calculated by [16]

$$\bar{\upsilon} = \frac{\frac{1}{n} \sum_{i=1}^{N} (ZP(X_i, Y) - \max ZP(X_i, j))^2 - SF^2}{\left(\frac{1}{k} \sum_{v=1}^{M} \sqrt{EP_v + \overline{EP}_v + (EP_v - \overline{EP}_v)^2} \right)^2} \tag{20}$$

where EP_u and $\overline{EP}_u$ are error estimation value of $P(h_v(X_i) = Y)$ and $P(h_v(X_i) = \bar{Y}_j)$.

4 Case Study

To validate availability of proposed WN safety status prediction method depended on fuzzy logic. Operation system is Windows 10, simulation platform is MATLAB 2015a, the simulation experiment environment is illustrated in Figure 1.

120 groups of status data are selected as samples, of which first 110 groups are training samples and last 10 groups are comparison samples. Selected 100 groups of status data sequence diagram is shown in Figure 2. Take the status data as a signal. From Figure 2, it can be seen that the signal is an unstable signal, indicating that the WN is unsafe.

Based on the above signals, the WN safety status prediction system based on network safety diagram, WN safety status prediction system based on multiple unknown data weighted set and WN safety status prediction system

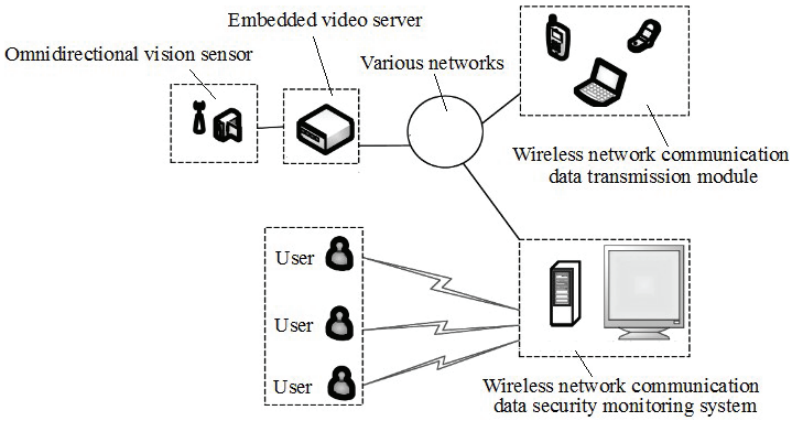


Figure 1 Data safety status prediction experiment system.

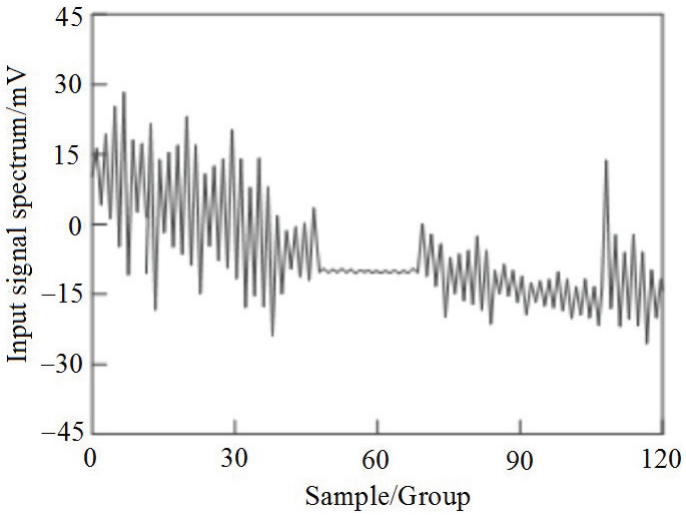


Figure 2 Sequence diagram of 120 group status data.

depended on fuzzy logic are used for signal prediction, and the results are listed in Table 2.

As seen from Table 2, the maximum input signal spectrum of WN safety status prediction system depended on network safety diagram is 36 mV, and minimum input signal spectrum is −26.3 mV; The maximum input signal spectrum of WN safety status prediction system based on weighted set of multiple unknown data is 32 mV, and the minimum input signal spectrum

Table 2 Prediction results of safety status data based on different methods

Method	Maximum Input Signal Spectrum/mV	Minimum Input Signal Spectrum/mV
Network safety diagram	36	−26.3
Multiple unknown data weighted set	32	−22.5
Fuzzy logic	30	−15

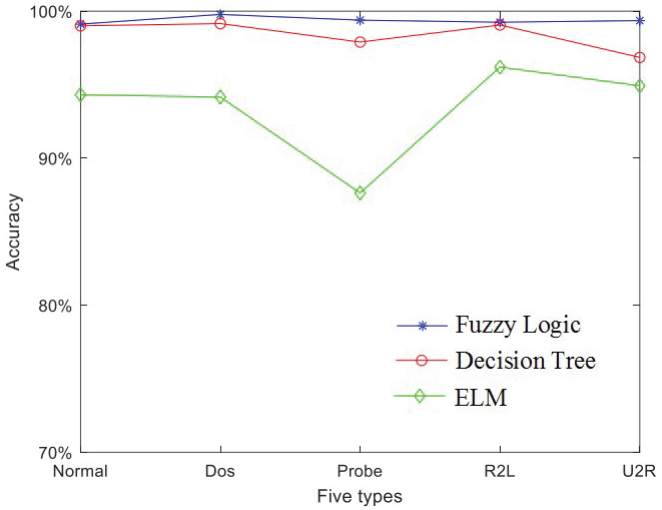


Figure 3 Prediction precision of different attacks of different prediction models.

is −22.5 mV. Therefore, the curve of the comparison method is inconsistent with the actual 120 groups of status data sequence diagram; The maximum input signal spectrum of the WN safety status prediction system based on fuzzy logic is 20 mV, and the minimum input signal spectrum is −15 mV, and the fluctuation amplitude of the input signal under $40 \sim 62$ groups of samples is small, basically unchanged, consistent with the selected 120 groups of status data sequence diagram.

In order to validated availability of presented model, we compared precision of presented fuzzy logic model with the decision tree and extreme learning machine (ELM) in five different attack types, as illustrated in Figure 3. Results show that fuzzy logic model represented by star broken line has higher precision than decision tree and the limit learning machine in all five different attack types.

The status value is calculated according to the number of attacks, total number of attacks and threat elements, and network safety status level and

Table 3 Network safety status evaluation results of test samples

Number	Expected Status Value	Real Status Value	Expected Output Grade	Real Output Level
1	0.186	0.182	Excellent	Excellent
2	0.528	0.529	Medium	Medium
3	0.345	0.342	Good	Good
4	0.429	0.423	Medium	Medium
5	0.645	0.641	Poor	Poor
6	0.492	0.490	Medium	Medium
7	0.748	0.741	Poor	Poor
8	0.592	0.589	Medium	Medium
9	0.436	0.428	Medium	Medium
10	0.834	0.832	Dangerous	Dangerous

current safety status are evaluated by reference. The safety status evaluation results of 10 test samples are illustrated in Table 3.

As seen from Table 3, the actual status value of each sample is basically consistent with the expected status value, and mapped network safety status grade can also effectively express the actual network safety status.

5 Conclusions

To meet functional requirements of analysis system, a WN safety status evaluation system based on fuzzy logic is proposed through applying random forest and rough set. Simulation results show that actual status value and expected status value, the actual status level and the expected status level are highly consistent with their curves within the acceptable error range, indicating that the proposed fuzzy logic model can achieve better results in safety status assessment of WNs, and provide higher accuracy for managers to make decisions.

References

[1] Ziyi Liu, Changsong Yang, Yueling Liu, Yong Ding, A BIPMU-based network safety status assessment method for WN, Computer Standards & Interfaces, 83, 2023, 103661.

[2] Megha. S. Kumar, R. Ramanathan, M. Jayakumar, Key less physical layer safety for WNs: A survey, Engineering Science and Technology, an International Journal, 35, 2022, 101260.

[3] Mona Sayed Abdul-Karim, Kamel Hussien Rahouma, Khalid Nasr, Hardware Implementation of Effective Framework for the Trade-off between Safety and QoS in Wireless Sensor Networks, Microprocessors and Microsystems, 93, 2022, 104590.
[4] Nashab Alikh, Amir Rajabzadeh, Using a lightweight safety mechanism to detect and localize jamming attack in wireless sensor networks, Optik, 271, 2022, 170099.
[5] Yong Dai, Wei Li, Weiwei Miao, Mingxuan Zhang, Jin Fan, Rui Liu, Yang Li, Research on safety strategies in the power wireless private network, Procedia Computer Science, 183, 2021, 395–400.
[6] Pawar PM, Nielsen RH, Prasad NR, Ohmori S, Prasad R. Behavioural Modelling of WSN MAC Layer Security Attacks: A Sequential UML Approach. Journal of Cyber Seccurity and Mobility, 2012, 10(1):65–82.
[7] Doynikova E, Fedorchenko A, Kotenko I. A Semantic Model for Security Evaluation of Information Systems. Journal of Cyber Seccurity and Mobility, 2020, 9(2):301–330.
[8] Shandilya SK. Design and Deployment of Network Testbed for Web Data Security. Journal of Cyber Seccurity and Mobility, 2021, 11(02):127–140.
[9] Kumar S, Kumar D, Lamkuche HS. TPA Auditing to Enhance the Privacy and Security in Cloud Systems. Journal of Cyber Seccurity and Mobility, 2021, 10(3):537–568.
[10] Wei Gao, Fan Xu, Zhi-Hua Zhou, Towards convergence rate analysis of random forests for classification, Artificial Intelligence, 313, 2022, 103788.
[11] Pei Huang, Xiaoqing Zhao, Junwei Pu, Zexian Gu, Yan Feng, Shijie Zhou, Xinyu Shi, Yuanyuan Tang, Pinliang Dong, Linking random forest and auxiliary factors for extracting the major economic forests in the mountainous areas of southwestern Yunnan Province, China, Ecological Indicators, 148, 2023, 110025.
[12] Anand Singh Rajawat, Pradeep Bedi, S B Goyal, Pawan Bhaladhare, Alok Aggarwal, Ravi Shankar Singhal, Fusion Fuzzy Logic and Deep Learning for Depression Detection Using Facial Expressions, Procedia Computer Science, 218, 2023, 2795–2805.
[13] Ilhan Tunc, Mehmet Turan Soylemez, Fuzzy logic and deep Q learning based control for traffic lights, Alexandria Engineering Journal, 67, 2023, 343–359.
[14] Mariana Bárcenas Castañeda, Luis Enrique Calatayud Velázquez, Sandra Silvia Roblero Aguilar, José Solís Romero, Víctor Augusto

Castellanos Escamilla, Expert system through a fuzzy logic approach for the macroscopic visual analysis of corroded metallic ferrous surfaces: Knowledge acquisition process, Expert Systems with Applications, 214, 2023, 119104.

[15] Nitish Varma Ulchi Suresh, Alireza Sadeghi, Mohammad Yazdani-Asrami, Critical current parameterization of high temperature Superconducting Tapes: A novel approach based on fuzzy logic, Superconductivity, 5, 2023, 100036.

[16] De-Gan Zhang, Chen-Hao Ni, Jie Zhang, Ting Zhang, Zhi-Hao Zhang, New method of vehicle cooperative communication based on fuzzy logic and signaling game strategy, Future Generation Computer Systems, 142, 2023, 131–149.

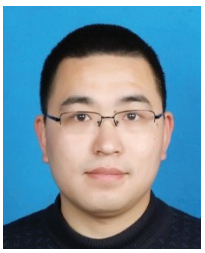
[17] Illia Diahovchenko, Pavlo Korzh, Michal Kolcun, A fuzzy-logic-based method for maintenance prioritization of high-voltage SF6 circuit breakers, considering uneven wear, Results in Engineering, 16, 2022, 100788.

[18] Xiaoyan Zhang, Jianglong Hou, A novel rough set method based on adjustable-perspective dominance relations in intuitionistic fuzzy ordered decision tables, International Journal of Approximate Reasoning, 154, 2023, 218–241.

[19] Dandan Zou, Yaoliang Xu, Lingqiang Li, Zhenming Ma, Novel variable precision fuzzy rough sets and three-way decision model with three strategies, Information Sciences, 629, 2023, 222–248.

[20] Masiur Rahaman Sardar, Mihir Kumar Chakraborty, Rough set models of some abstract algebras close to pre-rough algebra, Information Sciences, 621, 2023, 104–118.

Biographies



Xiao Xue, Associate Professor of School of Electronic and Electrical Engineering in Nanyang Institute of Technology, Nanyang, China. He received

his Bachelor of Engineering Science in Electronic Information Engineering from Nanyang Institute of Technology, Henan, China, in 2003; the Doctor Degree of Engineering in detection technology and automatic equipment from China University of Geosciences, Wuhan, China, in 2015. His current research interests include Detection technology, and intelligent control.

Yangbing Zheng, Associate Professor of control science and engineering, with Nanyang Normal University, Nanyang, China. She received her Bachelor of Engineering Science in Electronic Information Engineering from Nanyang Institute of Technology, Henan, China, in 2006; and the Doctor Degree of Engineering in detection technology and automatic equipment from China University of Mining and Technology, Beijing, China, in 2013, respectively. Her current research interests include active robot control, and nonlinear control.

Chao Lu, Engineer of Nanyang Zehui Technology Co., LTD. He received his Bachelor of Engineering Science in electronic information engineering form Nanyang Institute of Technology, Henan, China, in 2015.