Risk assessment optimization for decision support using intelligent model based on fuzzy inference renewable rules

Abdulkareem Merhej Radhi
College of Information Engineering, Al-Nahrain University, Iraq

Article Info

Article history:

Received Jan 5, 2020
Revised Mar 3, 2020
Accepted Mar 17, 2020

Keywords:

Cipher key
Encryption
Fuzzy
Risk assessment
WLAN

ABSTRACT

Due to the unreliability of wired communications and the risks of controlling the process of transmitting data besides the complications that affecting data protection and the high costs of systems infrastructure, led to use wireless communications instead of wires media, but these networks are vulnerable towards illegal attacks. The side effects of these attacks are modifying data or penetrate the security system and discover its weaknesses, which leads to great material losses. These risks and difficulties led to the reluctance of wires communications and propose intelligent techniques and robust encryption algorithms for preventing data transmitted over wireless networks to keep it safe from cyber security attacks. So, there is a persistent need for providing intelligent techniques and robust algorithms to preserve conveyed information using wireless network. This paper introduces scenario for proposing intelligent technique to increase data reliability and provides a new way to improve high level of protection besides reduces infrastructure cost. The proposed system relies on two models, where the first model based on producing a knowledge base of risk rules while the aim of the second module is a risk assessment outcomes and encryption process according to attacks type. In this system, reducing risks levels based on renewable rules whereas a novel security system established on non-periodic keys with unsystematic operations using fuzzy system. We concluded that the proposed system has the ability to protect the transmitted data, increases its reliability and reduce the potential risks. MATLAB Toolkit 2014 then Weka open source package was used in encryption and data mining for the proposed system.

Corresponding Author:

Abdulkareem Merhej Radhi,
Department of Information and Communication Engineering,
College of Information Engineering,
Al-Nahrain University, Baghdad, Iraq.
Email: abdulkareemradhi@gmail.com

1. INTRODUCTION

Wireless networks have a most advantages when it is compared with wires networks, especially after the growth of demand to utilize information resources to support decision-making, such as its ability in transmitting a huge data in the real-time applications and its economic characteristics in improving transmission speed for massive data. However, wireless technology also creates a new threats via alters the existing transmitted information. Unlike wired networks, wireless networks transmit data through the air using radio frequency transmission or infrared. Current wireless technology in use enables an attacker to monitor a wireless network and in the worst case may affect the integrity of the data. The above vulnerabilities and threats which are arisen in adapting wireless communication are very important to make sure that the wireless network is secure whether for a home or an enterprise network [1]. Also, this networks transfer a sensitive data which may be vulnerable when it is intercepted by malicious users and illegal threats. This would maximize the risks to the user's data that use these communications. To overcome these risks, this paper presents a framework of utilization a novel and intelligent encryption methodology with a reliable classification methodology to maximize authenticity. Encryption is the key to keep information more secure in a Wi-Fi network. However, commonly utilized known encryption techniques have big weaknesses and are susceptible by attackers via compromising confidentiality and risks [2]. WEP transfer data as 64 bit or 128 bit [3] but the actual transmission keys are 40 bits and 104 bits long where the other 24 bits is an Initialization Vector (IV) to send in the packet along with the data [4].

The organization should implement a continuous attack and vulnerability monitoring and perform periodic technical security assessment to measure the overall security of the WLAN [5]. The use of strong encryption standards protects WLANs from the worst threats [6]. This research paper depicts a new technical method for protecting data from illegal threats. Moreover, this method provides a novel methodology in creating an intelligent and self-adaptive system based on creating a renewable rule and encrypts data when it is at a high level of risks. This technique is easiest if we take into consideration both the simplicity of management of the encryption key distribution and reducing the infrastructure cost for protecting transmitted data and achievement of the maximum degree for encryption parameters (i.e. Safety, reliability, and authenticity). Its designs capable to reduce risks in various situations, such as a noise that affect the accuracy of data sent via investment of fuzzy scheme concepts to reduce all possible likelihood of risk levels. The objectives of various related techniques are to safe data transferred via wireless networks, therefore Sedghi and Kaghazgaran [7], introduces a public key cryptography to secure wireless network security.

2. FUZZY LOGIC AND RISK ASSESSMENT

Fuzzy set theory signifies the ambiguous data in an essential procedure. Due to the lower computational complexity, the applications of fuzzy logic associated to wireless communication [8].

2.1. Fuzzy logic

Fuzzy Logic is part of Artificial Intelligence (AI) that tries to solve the problem depart by using human intelligence [9]. Fuzzy logic is a set of collective functions and relations to assess fuzzy sets. Fuzzy logic risk assessments are determined by sets of logical rules. Results of risk assessment by fuzzy logic are easy for decision-making [10]. The creation of a Fuzzy inferenece system includes the creation rule system that defines how an output is inferred from given fuzzy inputs [11].

2.2. Decision support

For decision support, the unique method, to correctly predict the risk of activities is by congregation as much of related historical data and analyzes the correlation between the features which contribute to the activities occurrences [12]. A Fuzzy Rule Learning in a Fuzzy Decision Support System incorporates the knowledge in the design of a system whose input-output relationships are defined by a set of fuzzy rules [13]. Decision making is a complicated process which depends on different criteria such as availability of capital, safety, time, etc. [14]. The multi objective decision theory assumes that the decision producer is completely rational in choosing the optimal solution [15]. Multi-agent technology which is a subfield of artificial intelligence can be also tackled for intelligent optimization [16].

2.3. Risk assessment

Risk assessment is the process of risk identification, analysis and evaluation. Identifying risk comprises understanding the sources of risk and their sources and probable drawbacks [17]. The membership functions are linked by a linguistic conjunction: “and” (for maximization) and “or” (for minimization). For a maximization problem, the highest degree of membership in the decision set for the optimal solution is depicted by [17]:

$$x^* \equiv \arg[\max\min\{\mu_G(x), \mu_c\,(x)\}] \tag{1}$$

where G is the goal and C represent the constraints. While the optimal solurion for the optimal decision via the lowest degree of membership in the decision set, is as follows [17]:

$$x^* \equiv \arg[\min\max\{\mu_G(x), \mu_c\,(x)\}] \tag{2}$$

3. METHODOLOGY

Minimizing risks and optimizing management of the control for the transmitted packets is the main aim of this research. Due to security and system reliability characteristics, this research covers all risks of expected security disasters in several circumstances. Surveillance the network and identifies the behavior of malicious intruders via unsupervised learning was used. Features are extracted and evaluated after data collection to test the conveyed packets.

3.1. Fuzzy renewable rules

First of all, the main core of this step is a creation of fuzzy rules to produce a knowledge base of risk rules which was satisfied via two specific models as follows: The first module is a construction of a risk knowledge base. This module aims to create a repository of risk levels and a subject oriented experts from the inference part for many risks and focus on cause-and-effect relationships based on their knowledge [18]. The aim of the second module is a risk assessment outcomes model, (i.e. Flow into the risk decision-making process and the outcome of the decision are fed back into the system to refine the fuzzy sets, rules. Fuzzy logic models used with other risk models such as decision trees to model complicated risk issue). In the proposed system, “the packet encryption should be tackled rendering to its type. A key feature of fuzzy sets is that there are no hard rules about how their membership functions are defined [19]. In order to establish inference rules from fuzzy data in WLAN security system, independent and dependent variables selected and then fuzzy sets with numeric values adopted. In this research, robust and unbreakable data are dependent variables while true packets are the independent variable.

3.2. Proposed algorithm

Radhi [20] was previously adopted algorithm to achieve two important features which are data security and satisfying its reliability, while the second is the creation of recordable security automated system. In this paper, a different technique adopted to have higher security for the transmitted data, which are formed as packets. We can specify this algorithm as follows:

a. An initial key (Basic Key) stated and represented by a shift register as 16-bits (Two Bytes).
b. A message key (64 bits) long represented by (4 shift registers).
c. Every single bit of the message key integrates with shift register output for the basic key, according to the following sequence of nonlinear function:

$$Output = B_k \oplus M_k \oplus \wedge I_k \tag{3}$$

d. Specifying a random permutation for the output.
e. Final output will be organized using the mathematical form: $O_f = output_n \oplus \sim(P_k)$, where P_k is packet bit.

The recipient decrypts encrypted packets via a reversing cycle of the proposed algorithm which is shown in Figures 1 and Figure 2 respectively. Figure 1 presents the general block diagram of the proposed system architecture, where the naïve Bayesian classifier was used to classify packets and renewable rule generator with risk level base for risk assessment optimization.

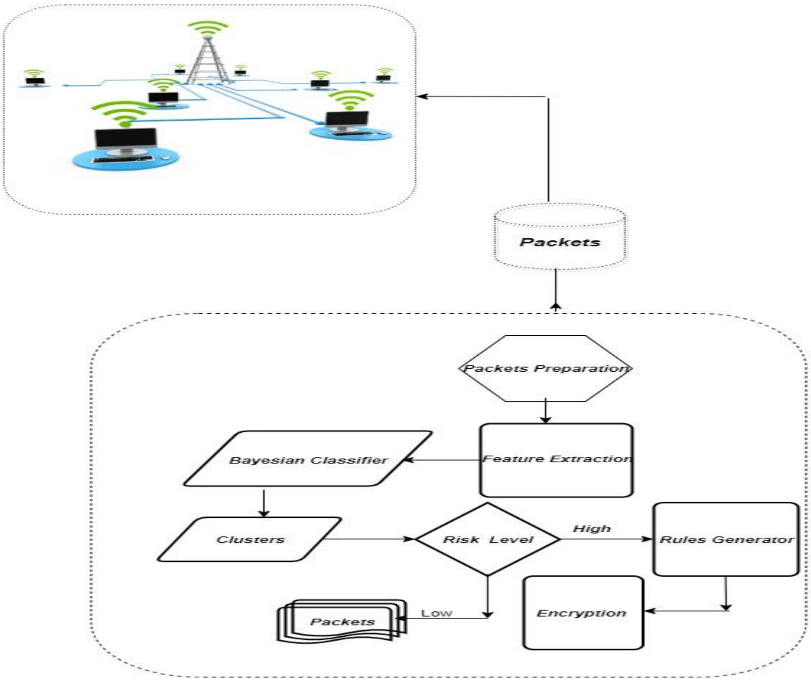


Figure 1. Block diagram of the proposed system

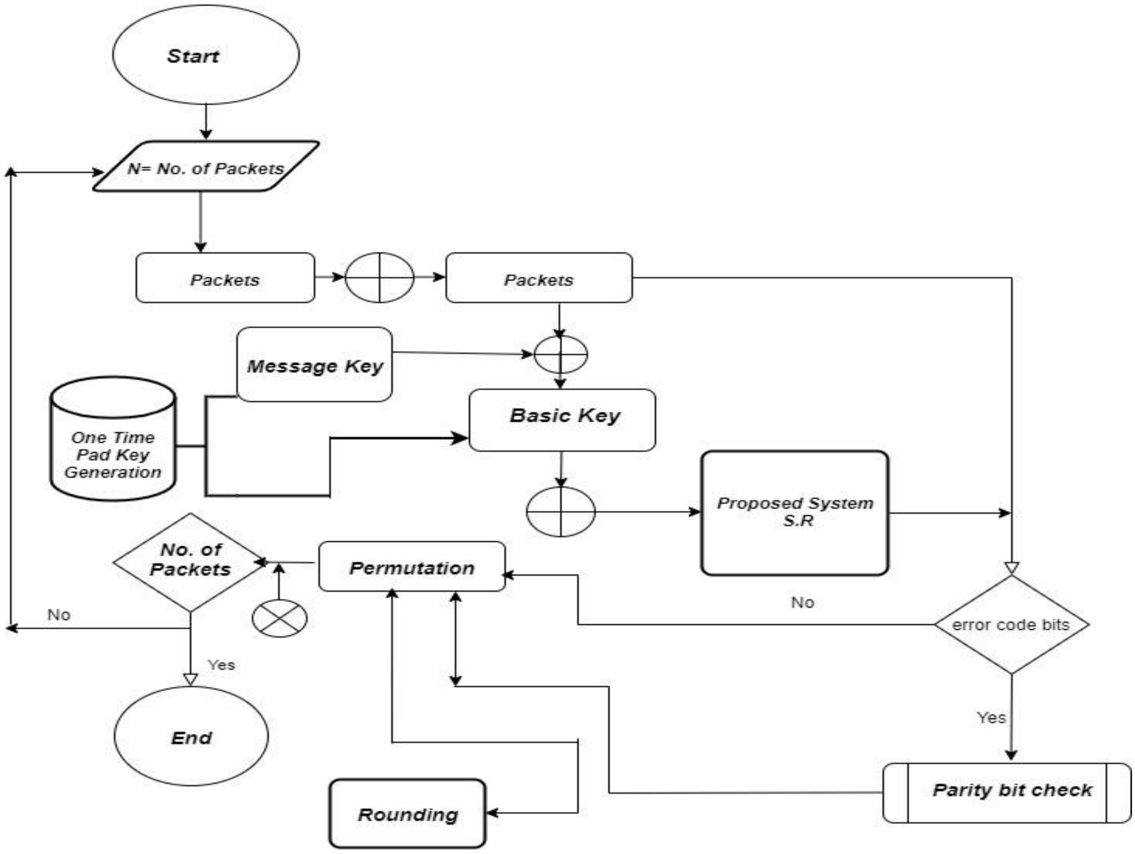


Figure 2. Proposed system with security control

3.3. Rule knowledgebase

This paper adopts a novel methodology for creating a knowledge base of rules. Proposed rules and mathematical hypothesis used to improve and induct facts and rules with logical and discrete theory. The inductive rules are: modus ponens, modus tollens, addition, simplification, hypothetical syllogism, Disjunctive syllogism, and resolution. The reasoning models of inference rules are seeds for the rules of the proposed system. It depends on the condition and consequence of the following form: (if risk, then packets) is accepted, but the antecedent risk holds, then the consequent encryption cannot be activated.

Analyzing the data, there are four variables from QoS parameters. They are delayed, jitter, packet loss, and throughput. A technique for analyzing the data of IP network quality in this paper implemented via calculating the value of each Quality of Service parameters such as delay rata which is the number of delays divided by the number of receiving packets, and the Percentage Packet Loss [21], as shown in (4):

$$percentage\ Packet\ Loss = \frac{(\text{Number of sent packets} - \text{Number of received packets})}{\text{Number of sent packets}} \times 100 \tag{4}$$

$$Throughput = \frac{Number\ of\ Packets \times 8}{Simulation\ time} \tag{5}$$

The proposed system achieves these parameters concerning QoS for the transmitted packets after risk optimization as shown later implicitly in the Tables 2 and 3.

3.4. Naïve bayes classifier

It is a probabilistic classifier based on Bayes' statistics theorem with (Naive) or independence attributes and hypothesis. It is a descriptive technique and “independent feature model”. Naive Bayes classifiers can be trained very efficiently in a supervised learning set. Parameter estimation uses the method of maximum likelihood. Figure 3 presents cascading steps of this method, where the probability of a classification can be determined using (6).

$$P(H|X) = \frac{P(X|H)P(H)}{P(X)} \quad (6)$$

where P (H|X) is the a posteriori probability of H conditioned on X. In contrast, P (H) is the a priori probability of H. Similarly, P (X|H) is the a posteriori probability of X conditioned on H. P(X) is the a priori probability of X.

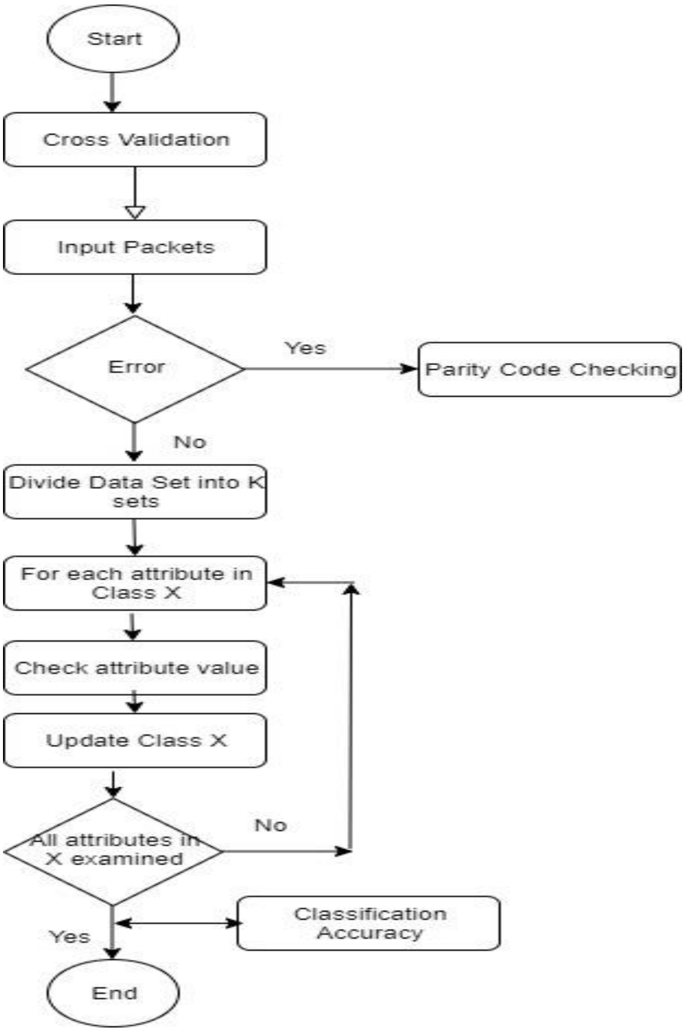


Figure 3. Naive bayesian classifier

It is a method for estimating parameter values θ = (K,(n)^{k} ,h^{k}) which is based on the information from the data y_n (expressed in the probability distribution f(y| θ)) and information from the parameter θ (expressed in the prior distribution π(θ)) [22].

4. OPTIMIZATION OF RISK ASSESSMENT

Risk assessment is the aim of this research, such that the objectives of the proposed technique are maximizing the reliability and confidentiality of data and network via reducing and minimizing risk level. Table 1 depicts risks and rules assessment, where there are three parameters for assigning encryption using the proposed model directed and controlled via threshold. Threshold specified, modified and updated according to data sensitivity and packet size. So, the risk management is the identification, assessment and prioritization of risks (by risk measurements) followed by coordinating and economical application of resources to minimize, monitor and control the probability and/or impact of unfortunate events (by risk treatments) [23].

Table 1. Risks and rules assessment

Packets Size	Risk	Encryption
Low	Low	Negative
High	Low	Positive
Low	Med	Negative
High	Med	Positive
Low	High	Negative
High	High	Positive
Low	Very Low	Negative
High	Very Low	Negative
Low	Very High	Negative
High	Very High	Positive

Table 2 presents a support mean in decision- making for data transmitted via WLAN vs a probable risks. The attackers can try to find vulnerabilities through diffrent methods [24]. There are various types for cipher attack as shown in Table 2, where the risk level depends on the attack type. So, comprehensive studying for the attacking techniques is an essential topic to identify risks using the proposed model. This table depicts a related attacking type according to its methods and a risk level when applying a security technique to safe data in a suitable and confidential mode.

Table 2. Decision making and attack type

Attack type	Packets size	Risk Threshold	Risk Level	Encryption (Decision)
Masquerade	Low	0.213	Low	Negative
Rogue Point	High	0.681	Low	Positive
MITM	Low	0.114	Med	Negative
DOS	High	0.752	Med	Positive

Table 3 in the later section presents packets classification precision using theNaïve Bayesian classifier. Entropy measurement used as a tool to check the performance of the obtained classifier that detects set of packets in a specific cluster. So, if a set of packets (M) belonging to a cluster then:

$$\text{Entropy (S)} = -p_{+} \log_2 (p_{+}) - p_{-} \log_2 (p_{-}) \quad (7)$$

Performance measured in terms of recall and precision. Precision is the total number of positive class that is classified appropriately divided by the total data categorized as positive [25].

Table 3. Clustering accuracy of the proposed system

TP Rate	FP Rate	Precision	Recall	F-Measure	MCC	ROC Area	PRC Area	Risk Level
0.973	0.007	0.955	0.937	0.946	0.937	0.997	0.986	Low
1.000	0.000	1.000	1.0000	1.0000	1.000	1.0000	1.000	Low
0.793	0.024	0.842	0.793	0.817	0.789	0.974	0.889	Med
0.845	0.040	0.785	0.845	0.814	0.781	0.976	0.875	Med
0.770	0.030	0.801	0.770	0.785	0.752	0.974	0.840	High
0.970	0.010	0.946	0.970	0.958	0.950	0.998	0.991	High
1.000	0.001	0.995	1.000	0.998	0.997	1.000	1.000	Very Low
Weighted Avg.	0.904	0.016	0.904	0.904	0.904	0.888	0.989	0.941

5. RESULTS AND DISCUSSION

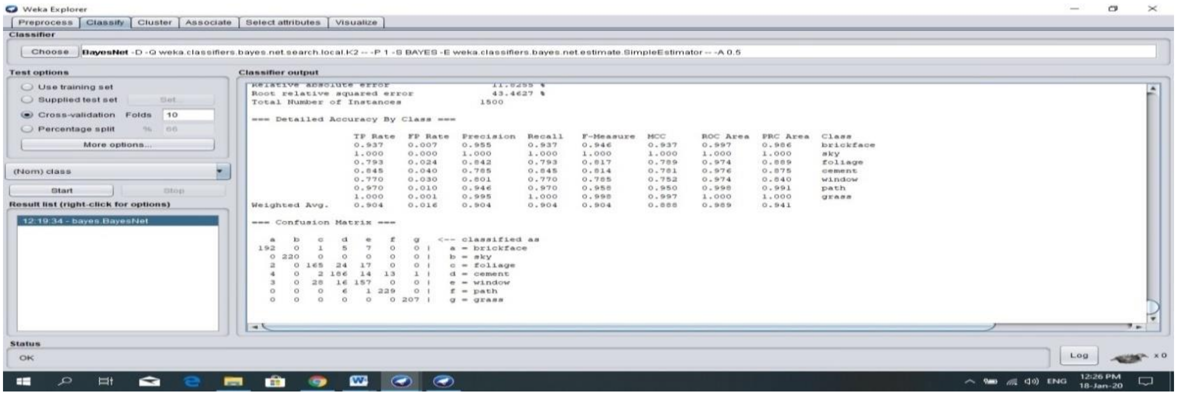
Due to a processing of huge data with several instances in wireless communication as a problem introduced in this paper as a case study to test the proposed system accuracy, Weka open source package have been used to classify and clustering data based on a Naïve Bayesian classifier with the following properties:

a. Number of instances = 1500
b. Multifactor for all attributes based on region-centroied.
c. Test operations: Cross validation.
d. Output prediction format: CSV.
e. Hieratical clustering using training set.

Output results:

a. Minimum = 1
b. Maximum = 254
c. Mean = 125.197
d. Standard Deviation = 73.228

So, we conclude that (1356) correctly classified instances which is (90.4%) precision rate for weighted average for all possible risk levels, and (144) incorrect classified instances (i.e. 9.6%) precision rate. Recall and precision rate of the implemented proposed technique value 95% with very low minimum risk. Figure 4 presents WEKA GUI for the processed training data.



BayesNet -D -Q weka.classifiers.bayes.net.search.local.K2 -- -P 1 -S BAYES -E weka.classifiers.bayes.net.estimate.SimpleEstimator -- -A 0.5

○ Use training set
○ Supplied test set Set...
● Cross-validation Folds 10
○ Percentage split % 66

(Nom) class

12:19:34 - bayes.BayesNet

OK

```
Relative absolute error                 11.8255 %
Root relative squared error             43.4627 %
Total Number of Instances             1500

=== Detailed Accuracy By Class ===

                 TP Rate  FP Rate  Precision  Recall   F-Measure  MCC      ROC Area  PRC Area  Class
                 0.937    0.007    0.955      0.937    0.946      0.937    0.997     0.986     brickface
                 1.000    0.000    1.000      1.000    1.000      1.000    1.000     1.000     sky
                 0.793    0.024    0.842      0.793    0.817      0.789    0.974     0.889     foliage
                 0.845    0.040    0.765      0.845    0.814      0.781    0.976     0.875     cement
                 0.770    0.030    0.801      0.770    0.785      0.752    0.974     0.840     window
                 0.970    0.010    0.946      0.970    0.958      0.950    0.998     0.991     path
                 1.000    0.001    0.995      1.000    0.998      0.997    1.000     1.000     grass
Weighted Avg.    0.904    0.016    0.904      0.904    0.904      0.888    0.989     0.941

=== Confusion Matrix ===

   a   b   c   d   e   f   g   <-- classified as
 192   0   1   5   7   0   0 |   a = brickface
   0 220   0   0   0   0   0 |   b = sky
   2   0 165  24  17   0   0 |   c = foliage
   4   0   2 186  14  13   1 |   d = cement
   3   0  28  16 157   0   0 |   e = window
   0   0   0   6   1 229   0 |   f = path
   0   0   0   0   0   0 207 |   g = grass
```

Figure 4. WEKA GUI for the processed training data

6. CONCLUSIONS

The proposed work in this paper presents a new method to have a reliable and safe conveyed data against the attacker and illegitimate interceptors. Optimization assessment of risks level is the main key to minimizing risks via data encryption. In this paper the risk minimization based on the proposed encryption system. The proposed models based on the training, learning, and classification phases in order to be adaptable and immune against different attacks. WEKA open source package was used based on naïve Bayesian classifiers with specific features. The average accuracy rate was (90.4%). Recall and precision reflects a precision rate value was 95% with very low minimum risk.

REFERENCES

[1] M. Choi, et al., “Wireless Network Security: Vulnerabilities, Threats and Countermeasures,” *International Journal of Multimedia and Ubiquitous Engineering*, vol. 3, no. 3, pp. 77-86, Jul 2008.

[2] P. Bhatia and R. Sumbaly, “Framework for Wireless Network Security Using Quantum Cryptography,” *International Journal of Computer Network and Communications*, vol. 6, 2014.

[3] M. Waliullah and D. Gan, “Wireless LAN Security Threats and Vulnerabilities” *International Journal of Advanced Computer Science and Applications*, vol. 5, no. 1, 2014.

[4] M. Waliullah, et al., “An Experimental Study Analysis of Security Attacks at IEEE 802.11 Wireless Local Area Network,” *International Journal of Future Generation Communication and Networking*, vol. 8, no. 1, pp. 9-18, 2015.

[5] P. S. Kahai and S. K. Kahai, “Deployment Issues and Security Concerns with Wireless Local Area Networks: The Deployment Experience at A University,” *Journal of Applied Business Research*, vol. 20, no. 4, 2004.

[6] T. Liu, et al., “An Evaluation of Feature Selection for Text Clustering,” *Proceedings of the 20th International Conference on Machine Learning*, 2003.

[7] A. R. Sedghi and M. R. Kaghazgaran, “Data Security via Public-Key Cryptography in Wireless Sensor Network,” *International Journal on Cybernetics & Informatics (IJCI)*, vol. 2, no. 3, pp. 1-11, Jun 2013.

[8] M. Subramani and V. B. Kumaravelu, “A fuzzy based vertical handover network selection scheme for device to device communication,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 17, no. 1, pp. 324-330, Jan 2020.

[9] M. S. Sulaiman, et al., “Course recommendation system using fuzzy logic approach,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 17, no. 1, pp. 365-371, Jan 2020.

[10] M. H. A. Abdullah, et al., “Evolving spiking neural networks methods for classification problem: a case study in flood events risk assessment,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 16, no. 1, pp. 222-229, Oct 2019.

[11] C. Ameur, et al., “Intelligent optimization and management system for renewable energy systems using multi-agent,” *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 8, no. 4, pp. 352-359, Dec 2019.

[12] F. Camastra, “Rule Learning in a Fuzzy Decision Support System for the Environmental Risk Assessment of GMOs,” *International Workshop on Fuzzy Logic and Applications WILF 2013*, pp. 226-233, 2013.

[13] A. F. Shapiro and M. C. Koissi, “Risk Assessment Applications of Fuzzy Logic,” Casualty Actuarial Society, Canadian Institute of Actuaries, Society of Actuaries, pp 1-89, 2015.

[14] K. Karimpour, et al., “New Fuzzy Model for Risk Assessment Based on Different Types of Consequences,” *Oil & Gas Science and Technology*, vol. 71, no. 1, p. 17, 2016.

[15] A. Fallahpour, et al., “A fuzzy decision support system for sustainable construction project selection: an integrated fpp-fis model,” *Journal of Civil Engineering and Management*, vol. 26, no. 3, pp. 247-258, 2020.

[16] S. Xin, et al., “Research on Fuzzy Adaptive Intelligent Decision-making in Complex Environment,” *Journal of Physics: Conference Series*, pp. 3-12, 2019.

[17] M. Kozlova, et al., “New investment decision-making tool that combines a fuzzy inference system with real option analysis,” *Fuzzy Economic Review*, vol. 23, no. 1, pp. 63-92, 2018.

[18] J. Lynne, “Hot Tips for Securing Your Wi-Fi Network,” SOPHOS, 2012.

[19] M. Malik, et al., “Rule Based Technique detecting Security attack for Wireless Sensor Network Using Fuzzy Logic,” *International Journal of Advanced Research in Computer Engineering & Technology*, vol. 1, no. 4, pp. 244-251, 2012.

[20] A. M. Radhi, “Risk Surveillance Control of Wireless Security Attack with Fuzzy Rules,” *International Journal of Science and Research (IJSR)*, vol. 6, no. 7, pp. 1006-1012, 2017.

[21] N. Ameen, et al., “Comparative analysis of energy based optimized dynamic source multipath routing protocol in WSNs,” *Indonesian Journal of Electrical Engineering and computer Science*, vol. 16, no. 1, pp. 441-455, Oct 2019.

[22] Suparman and M, Doisy, “Bayesian Segmentation in Signal with Multiplicative Noise using Reversible Jump MCMC,” *TELKOMNIKA Telecommunication Computing Electronics and Control*, vol. 16, no. 2, pp. 673-680, Apr 2018.

[23] O. Hadzic and Smajo B., “Risk assessment for ancillary services,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 3, pp. 1561-1568, Jun 2019.

[24] F. I. Khan, et al., “Security assessment of four open source software systems,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 16, no. 2, pp. 860-881, Nov 2019.

[25] M. Jupri and R. Sarno, “Data mining, fuzzy AHP and TOPSIS for optimizing taxpayer supervision,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 1, pp. 75-87, 2020.

BIOGRAPHY OF AUTHORS

Dr. Abdulkareem Merhej Radhi is Assistant Professor and has a Doctorial in computer science Philosophy. He is a teacher in AL-Nahrain University-Iraq and a Director of Computer Center and Avin-cina for E-Learning in the university. Interested in data security, soft computing, distributed databases, engineering analysis, wireless networks, data mining, social network analysis and Internet of Things. He published many novel researches in artificial intelligence, text classification, image processing, and cyberforensic. He is author of a book in artificial intelligence concepts and its applications in 2017.