Journal of Theoretical and Applied Information Technology
15th October 2022. Vol.100. No 19

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

INTRUSION DETECTION IN WIRELESS SENSOR NETWORKS USING FUZZY RELATED FEATURE SELECTION TECHNIQUE WITH OPTIMIZED CLASSIFICATION

GIRIBABU SADINENI[1], DR. M. ARCHANA[2], DR. RAMA CHAITHANYA TANGUTURI[3]

[1] Research Scholar, Department of Computer Science & Engineering, Annamalai University, Tamil Nadu, India.

[2] Assistant Professor, Department of Information Technology, Annamalai University, Tamil Nadu, India.

[3] Professor, Department of Computer Science & Engineering, PACE Institute of Technology And Sciences, Andhra Pradesh, India.

[1]sadinenigiri1521@gmail.com, [2]archana.aucse@gmail.com, [3]trchaitanya@gmail.com

ABSTRACT

The internet related data processing system has several kinds of threats that direct to huge damages in major loss of data in Wireless Sensor Networks. Additionally, the group of data transmission with WSNs is huge in size that will target by the group of attackers regularly. The highest amount of security will be provided for secured data transmission with WSNs. The intrusion detection should be provided for necessary element in network communication, there are several techniques have been developed for effective intrusion detection constantly. This paper proposes Fuzzy related feature selection technique with Optimized classification in spite of selecting a large amount of attack data for detection of attacks in WSNs. Fuzzy related feature selection technique is used for identifying the intrusion and monitoring the network to protect from the malicious activity and unauthorized access. The efficiency of the proposed technique is enhanced according to the utilization of data which also enhances the detection rate and minimizes the error rate.

Keywords: *Intrusion Detection*, *Fuzzy Set*, *Wireless Sensor Networks*, *Feature Selection*.

1. INTRODUCTION

Several security structures have the internet related applications as the Intrusion detection which has both inside and outside attacks. The intrusion detection system has been provided the high security that reduced the internet related attacks [1]. The signature related framework has the highest level of dependency for discovering the intrusion detection using the improved operations and grouping methodologies [2]. The enhancement of security in network transmission with the Internet is a difficult task while processing the pre-processing stage into the discovery of interruption stage [3]. The Intrusion detection can be classified as the network related attacks and server related attacks as the arrangement of the Intrusion detection has been established through the traffic management. The user data has been targeted by the intruder; the soft computing related techniques have been implemented for detecting the malicious intrusion threat [4]. The improved optimization techniques are required for monitoring network data in spite of capturing the anomalies and intrusion efficiently. The soft computing related technique is more effective for intrusion detection as it can analyze the intrusion from the traffic data and handling the attack types in various types [5]. The pre-processing methodology is used for reducing data in spite of enhancing the effectiveness of the network system. The data of attacking the normal information is the difficult process for discovering the attackers successfully from the large amount of dataset and the enough amounts of attributes has been utilized for intrusion detection can minimize the intrusion detection performance.

The intrusion detection methods could identify the known intruders because of the strong learning capabilities. The main aim of implementing the fuzzy set has to exploit the capability of identification among uncertainty, minimizing the false alarm rate efficiently [6]. The Intrusion detection is connected with the techniques of misuse and anomaly detection as every behavior needs to be analyzed briefly. The improved attack types have been identified by

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

updating the profiles in huge organization is the challenging task [7]. The multi featured logic has the specification of the fuzzy sets as the linguistic parameters could be identified with the components of the membership degree functions and utilized the fuzzy rules from the input data to the output data through mapping concept. The fuzzy related intrusion detection methodologies have been used the fuzzy clustering functionality through the classifiers and feature extraction concepts. These techniques have the capacity of identifying the intrusions through the behaviors and uncertain information. An amount of fuzzy techniques have been used for solving the misuse detection issues, the proposed technique is constructed to solve this kind of issues [8].

The primary problem of identifying the intrusion detection is to detect the behavior of the intruders and the malicious attacks. Additionally, the fuzzy logic is utilized for making decisions through uncertainty and the feature selection process can help for increasing the performance by extracting the significant features for efficient performance. The proposed technique employs a fuzzy set related classification process for the group of data is transmitted with the internet for security purpose. The total amount of features is involved for achieving the balance within the real-time scenario and the optimized detection rate. The proposed model is used the dataset with high detection rate by the optimization technique for reducing the computational complexity. The monitoring framework is constructed called as the intrusion detection system which identifies the suspicious activities and produces the alerts while it is identified by the system. According to the alerts, the security operations could be responded and analyze the problem for taking specific actions to enable the security.

2. RELATED WORKS

Several works have been implemented for Intrusion detection process as the classification technique related on SVM and decision trees [9] for enhancing the accuracy and detection rate. The enhanced performance parameters are utilized for evaluating the intrusion detection for enhancing the quality of service in WSN transmission and it is constructed the functionality which handles the effective fault tolerance and energy efficiency with security [10]. A Meta-TMP [11] methodology has been implemented for providing the improved network performance which demonstrates the measurement of the malicious behaviour and it has the reduced network lifetime. The decision trees [12] have been used with the machine learning techniques for several applications like signal discovery and robot management. The intrusion dataset has been gathered from the network database through the internet connectivity. The integration of several techniques utilizing the fuzzy logic mainly for the fuzzy integral [13] concept is used to segregating the large dataset into smaller groups for performing the data mining for sub sets individually. A rule related technique [14] has been used to perform the decision making in networks in support of intrusion detection which is monitoring the abnormal behavior of internal attackers through the classification after the decision making process.

The improved classification technique [15] has been derived a collection of classification process through the dataset and maintained the rules for generated rules which is suited for real-time environment. The main positive of this kind of technique is the utilization of simple rules for producing efficient classification process. Moreover, several intrusion detection techniques have been faced the problem of fault tolerance, low detection rates and minimized accuracy. The feature selection process has been implemented to provide operative classification for intrusion detection. The optimization of the attribute reduction assists the transformation functionality to survive the scrap in the discovering procedure.

The fuzzy enabled feature selection technique has been implemented for discovering the suitable feature subsets which has been evaluated through the dataset for enhancing the performances [16]. The Fuzzy C-means technique has been enabled to discover the intrusion detection through the local optima concept that the probability of computing the local optimal values have been improved through the evaluation process and also indicated the metrics [17]. The hybrid classification technique has been constructed according to ABC and AFS algorithms for implementing the correlation and clustering related feature selection process for removing the unwanted features. The necessary rules have been constructed from the specific datasets. The computational complexity and time cost have been minimized; the detection rate is higher while compared with the other techniques [18].

The GA-Fuzzy technique [19] has been implemented as the hybrid intrusion detection process for discovering the attacks by minimizing the missed alarm rate that the feature selection procedure which eliminates the repeated features and reduces the dataset features for increasing speed of intrusion detection. The fuzzy classifier is used for producing the patterns from the input features that the clusters are used for detecting the packet types from the specified dataset and this technique has enhanced the detection accuracy in efficient way. The fuzzy based rough set theory has been used to perform the intrusion detection and enhanced the detection rate through minimizing the processed information with feature selection technique; it also implements the decision tree technique with feature selection technique [20].

The security and energy efficiency are the key factors of intrusion detection system as the classification process needs to enhance the detection rate. The malicious behaviour has been identified to enhance the network lifetime which also increases the network performance. The fuzzy logic is used for dividing the huge dataset into smaller pieces for performing the decision making and identifying the abnormal behaviors of the attackers. The main drawback of the intrusion detection system is it needs some components for identifying the attacks and produces the false alarms. The intrusion detection system periodically alerts the network to false positives than the threats and produces the log information to the known attacks.

3. PROPOSED FRAMEWORK

The proposed system has been constructed with the two algorithms as the fuzzy set related attribute discovery algorithm produces the final set from the group of input functions of predecessors, resultants through the fuzzy related input and output parameters. The fuzzy based classification algorithm produces the fuzzy group from the set of attributes and the classifier can identify the intrusion detection from the dataset. The proposed framework is constructed with the data pre-processing, feature selection, classification, rule generation, knowledge and testing process and it is illustrated in Figure 1.

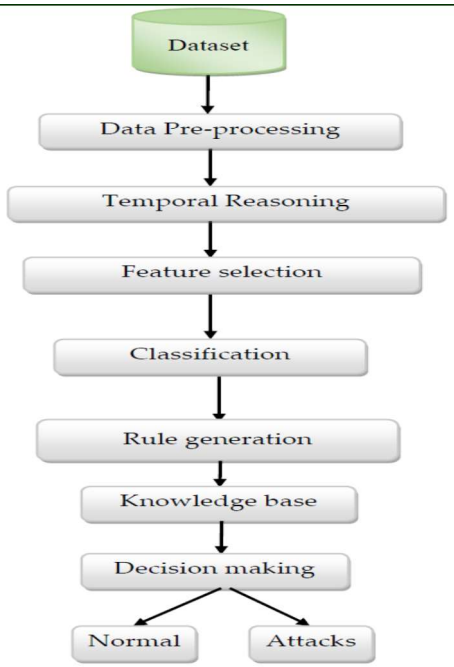

Figure 1: The proposed framework

The pre-processing process has been performed the redundancy check and removes the error values and also it changes the numerical data from the original data for providing the normalization. The network information related dataset are delivered to the redundancy checking process that verifies the redundant information and generates the integrity checking process. According to the procedure, it eliminates the error data and finally it executes normalization of the entire process to produce the unified formation. The normalized data will be stored in the database for testing and training functions that input values, reduced values have the reduction process. The entire pre-processing process is demonstrated in Figure 2.

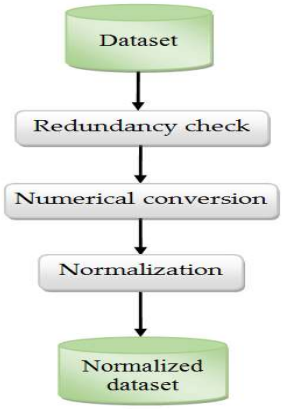

Figure 2: Data Pre-processing

Journal of Theoretical and Applied Information Technology
15th October 2022. Vol.100. No 19

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The fuzzy interference system has the fuzzy rules from the input parameters as the membership function values are used for constructing the proposed architecture. The relationship within the input and output parameters have the knowledge about the information of input and output parameters. Fuzzy logic is used to complete the reasoning through the incomplete data and also the robust functionality as the truth values will range within 0 and 1. The fuzzy set generates the relevant information with uncertainty values and the feature set assists real knowledge base values and user specified information. The classification of the dataset has been used for the continuous data and may be inherently exploited. Let Fs is the finite group, $\alpha, \beta \in Fs$, X is the finite element. Let $Y \subseteq X$ is the group of Y features. The fuzzy based approximations have been identified with the fuzzy equivalence class in Eq. (1).

$$\omega R_Y Z(\alpha) = in\ f_\beta\ \gamma(\omega R_Y(\alpha, \beta), \omega\ Z(\beta)) \quad (1)$$

Another way of defining the equivalence class is defined in Eq. (2).

$$\omega R_Y Z(\alpha) = su\ Y_\beta\ \psi(\omega R_Y(\alpha, \beta), \omega\ Z(\beta)) \quad (2)$$

Where ψ is the implication function, R_Y be the similarity related which is defined in Eq. (3).

$$Y: \omega R_Y(\alpha, \beta) = \psi_a \in Y\{\omega R_a(\alpha, \beta)\} \quad (3)$$

The feature subset ωR_a is the object similarity of α and β. The $\omega R_Y(\alpha, \beta)$ crisp region in a fuzzy set using Eq. (4)

$$\omega R_Y(\alpha, \beta) = Y\{\omega R_a(\alpha, \beta)\} \quad (4)$$

The fuzzy dependence degree of $\psi'_Y(D)$ to the subset Y is defined in Eq. (5).

$$\psi'_Y(D) = \frac{\sum_\alpha \omega_{Y(D)}(\alpha)}{|Fs|} \quad (5)$$

The fuzzy set related attribute discovery algorithm is demonstrated in Algorithm 1.

Algorithm 1 – Fuzzy set related attribute discovery

Begin Procedure

Input: P is the group of predecessors; R is the group of resultants

Output: S, the Final set

$S = \emptyset$

$\psi'_{best} = 0$

$\psi'_{pre} \neq 0$

while $\psi'_{best} \neq \psi'_{pre}$ do

for every $\alpha \in (P - S)$ do

if $\psi'_{S \cup \{\alpha\}} \neq \emptyset$ then

$S = S \cup \{\alpha\}$

$\psi'_{best} = \psi_T(D)$

$Check_{con}(S, \psi', \alpha, T)$

end if

end for

$S = T$

end while

Return S

End Procedure

The fuzziness communicates to the boundary values of the specific parameters which is dependent on the membership functions as the uncertainty measurement of the entropy value. The fuzziness properties contains the degree to reach the highest value as every membership degrees equivalent to the smaller value which demonstrates the fuzzy set. The proposed technique is constructed to maintain the relationship within the input and an output variable with the particular weight value is checked. It should maintain the low error rate, so the produced accuracy is high compared with other related methodologies and the proposed technique utilizes the fuzzy based classification algorithm and the representation is illustrated in Algorithm 2.

Algorithm 2 – Fuzzy based classification

Begin Procedure

Input: The group of classes P, Q, the group of adjacent elements A

Output: Final group of attributes Q

$A = \{\}$

$T = 1$

$total = 1$

For every $\alpha(y) \in (1 \leq y \leq n)$do

$x = ||\alpha - \alpha_y||$

if $i < T$ then

$$A = \{\alpha_y\} \cup A_{total} + +$$

else if $\alpha_y$is closer to then

$$A = A - \{\alpha_y\}$$

$$A = A \cup \{\alpha_y\}$$

end if

end for

Find the adjacent elements

For every $q_y \in Q$ do

$$Fu_x(\alpha) = \frac{\sum_{y=1}^{k} Fu_{xy}[||\alpha - \alpha_y||]^{\frac{-2}{\beta-1}}}{\sum_{y=1}^{k}[||\alpha - \alpha_y||]^{\frac{-2}{\beta-1}}}$$

end for

Output S

End Procedure

Let $\alpha = \{\alpha_1, \alpha_2, \dots, \dots, \dots, \alpha_n\}$ is the training dataset elements, α is the testing data performing the segregation of $\emptyset$ on α that generates the fuzzy sets Fs_1 and Fs_2. The fuzzy set Fs_1 is computed in Eq. (6).

$$Fs_1 = (fs_{11}, fs_{12}, \dots, \dots, fs_{1n}) \quad (6)$$

The range for the fuzzy set $Fs_1$is denoted in Eq. (7).

$$0 \leq \sum_{j=1}^{n} fs_{1j} \leq n \quad (7)$$

The fuzzy set $Fs_2$is computed in Eq. (8).

$$Fs_2 = (1 - fs_{11}, 1 - fs_{12}, \dots, \dots, 1 - fs_{1n}) \quad (8)$$

The upper approximation is computed in Eq. (9).

$$\omega_u(Fs_1) = \max(1 - Fs_{ij}, Fu_{jp}) \quad (9)$$

The lower approximation is computed in Eq. (10).

$$\omega_l(Fs_1) = \min(Fs_{ij}, Fu_{jp}) \quad (10)$$

The proposed technique finds the smallest amount of features and enhances the detection rate while compared with the related techniques. The dataset has been normalized for producing the improved result based on the feature selection. The data has been classified with related techniques on improved features will provide the good accuracy and low error rate.

4. PERFORMANCE ANALYSIS

UNSW-NB15 dataset [21] is the group of host based intrusion detection which has the system call time series as the real data into the detection framework. Several simulated attacks have been included into the network, the training data and the network traffic includes several network communications. The redundant information and duplicated data have been removed from the dataset. The dataset has several attack categories as the normal communication details, Backdoor category for maintaining access to systems through security parameters, Analysis of intrusion technique in several metrics, Fuzzers have the technique for discovering security threats in huge amount of data, Shellcode is the technique which controls the destination machine, Reconnaissance is the attack technique for collecting network data, Exploit is the small code which controls the destination machine, DoS is the technique which damages the resources, Worms is the malicious virus in the network, Generic is the method which utilizes the hash function of the block cipher.

The proposed technique is compared with the related techniques of FCM [16], GA-Fuzzy [19], GA-GOGMM [20] in the performance parameters of True Positive ratio, False Positive Ratio, Precision, Recall, Accuracy, F1-score, Detection rate (%), Error rate (%), RoC and Time taken for intrusion detection. The proposed technique utilizes the dataset for traditional intrusion detection process which specifically minimized attack information and huge element of conventional traffic by implementing the training data, the intrusion detection with the dataset has high attack information traffic and the accuracy rate is eventually enhanced. The detection rate is the ratio of the total amount of attacks with the exactly classified attacks and it is computed in Eq. (11).

$$D_R = \frac{Actually\ classified\ attacks}{Total\ amount\ of\ attacks} \quad (11)$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

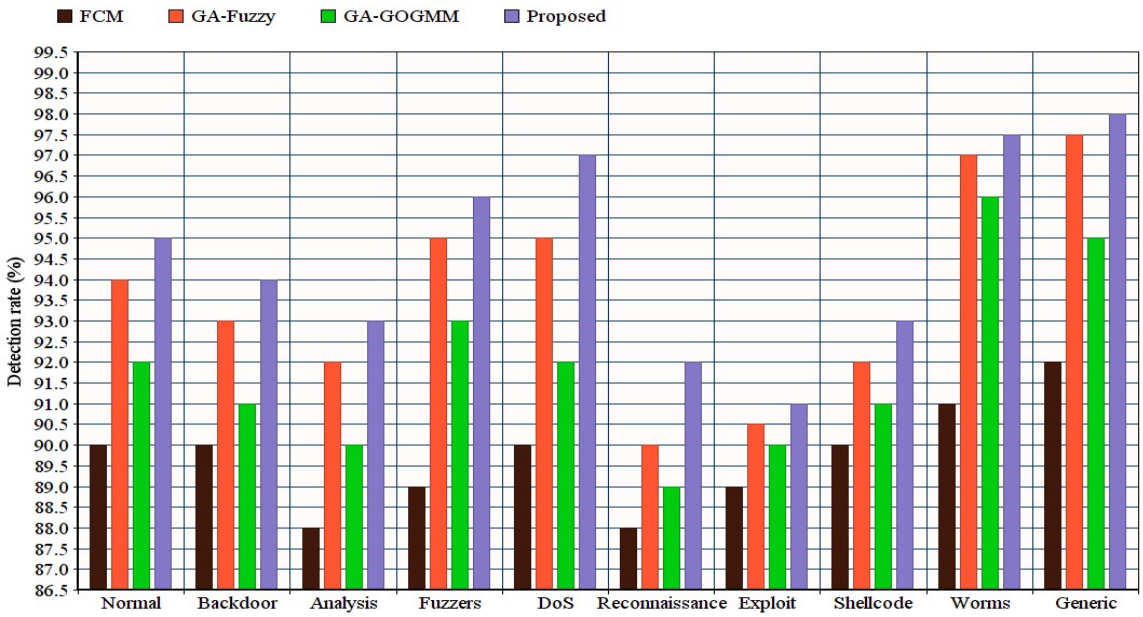

Figure 3: Detection rate (%)

The error rate is the ratio of the wrongly classified attacks with the total amount of attacks and it is computed in Eq. (12).

$$E_R = \frac{Wrongly\ classified\ attacks}{Total\ amount\ of\ attacks} \quad (12)$$

Fig. 3 demonstrates the detection rate and Fig. 4 illustrates the error rate for the proposed technique compared with the related techniques and the results proved that the proposed technique is performed well.

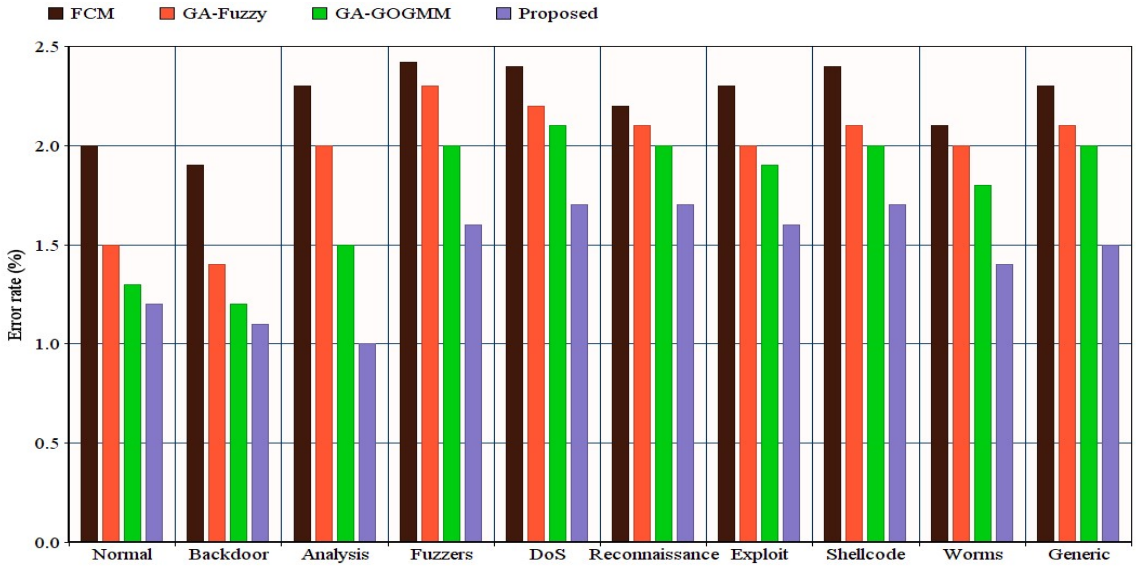

Figure 4: Error rate

The proposed technique with several data elements has been tested and the accuracy is measured as the dataset is used for training the intrusion detection and the ratio of non-attack,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

attack data elements have been identified. The proposed technique has enhanced the accuracy of more than 99%, the features are needed for the detection has been minimized.

The performance parameters are used for evaluation the classification capability of the proposed technique which is compared with the relevant techniques. The accuracy is the estimation of the correctly classified attacks from the total elements in the dataset and it is computed in Eq. (13).

$$Accuracy = \frac{Tr_P + Tr_N}{Tr_P + Tr_N + Fa_P + Fa_N} \quad (13)$$

Where Tr_P is the amount of correctly classified elements into the normal class, Tr_N is the total amount of classification into the attack class, Fa_P is the amount of wrong classification into the normal class and Fa_N is the total amount of wrong classification of the normal class. The precision is computed as the correctly classified attacks into the total amount of detection attack components and it is computed in Eq. (14).

$$Precision = \frac{Tr_P}{Tr_P + Fa_P} \quad (14)$$

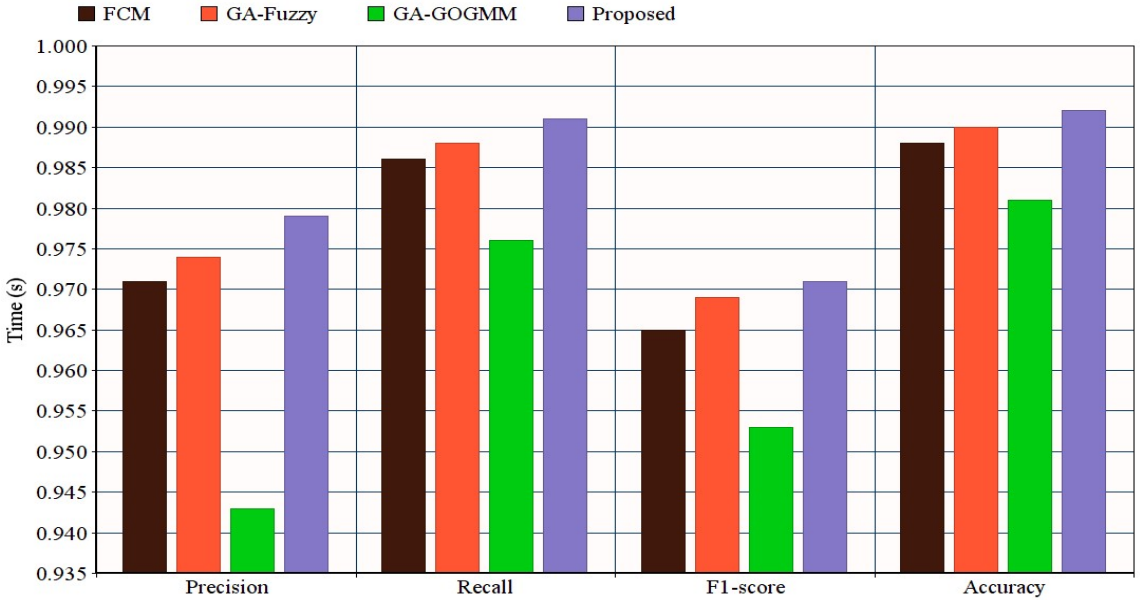

Figure 5: Performance metrics

F1 score is measured as the harmonic mean of Recall and Precision parameters for measuring the detection ratio. Figure 5 illustrates the performance metrics of precision, recall, accuracy and F1-score for the proposed technique compared with the related techniques. The True Positive Ratio is computed as the rate of correct classification of attacks from the total amount of attacks and it is computed in Eq. (15).

$$TPR = \frac{Tr_P}{Tr_P + Fa_N} \quad (15)$$

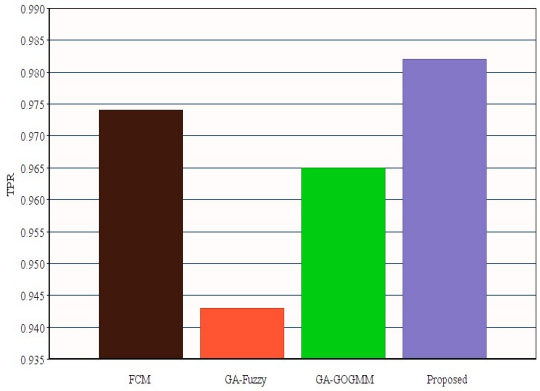

Figure 6: True Positive Ratio

The False positive ratio is computed from the normal classification elements falsely detected as

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

attacks from the total amount of attacks and it is computed in Eq. (16).

$$FPR = \frac{Fa_P}{Tr_N + Fa_P} \quad (16)$$

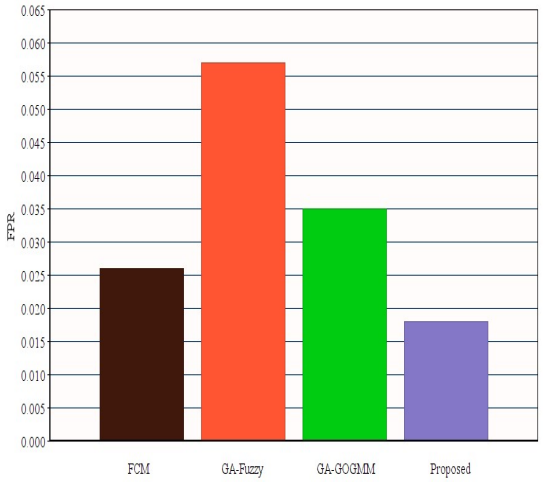

Figure 7: False Positive Ratio

True positive ratio is illustrated in Figure 6 for the proposed technique with the related techniques and false positive ratio is demonstrated in Figure 7. The proposed technique has the enhanced true positive ratio and minimized false positive ratio compared to t he relevant techniques.

The RoC curve is plotted according to the trade-off within the True positive ratio to false positive ratio through several threshold values. The region within the RoC curve is utilized through the performance metric for the detection technique. RoC curve is the indicator for generating FPR and TPR, the total amount of positive and negative values are involved to solve the imbalance issues. The value of RoC has been varied for every instances of the dataset that will ensure the detection rate of the intrusion detection system which is demonstrated in Figure 8. The time taken for performing the intrusion detection is illustrated in Figure 9 that the proposed technique has minimized amount of time taken compared with the relevant methodologies.

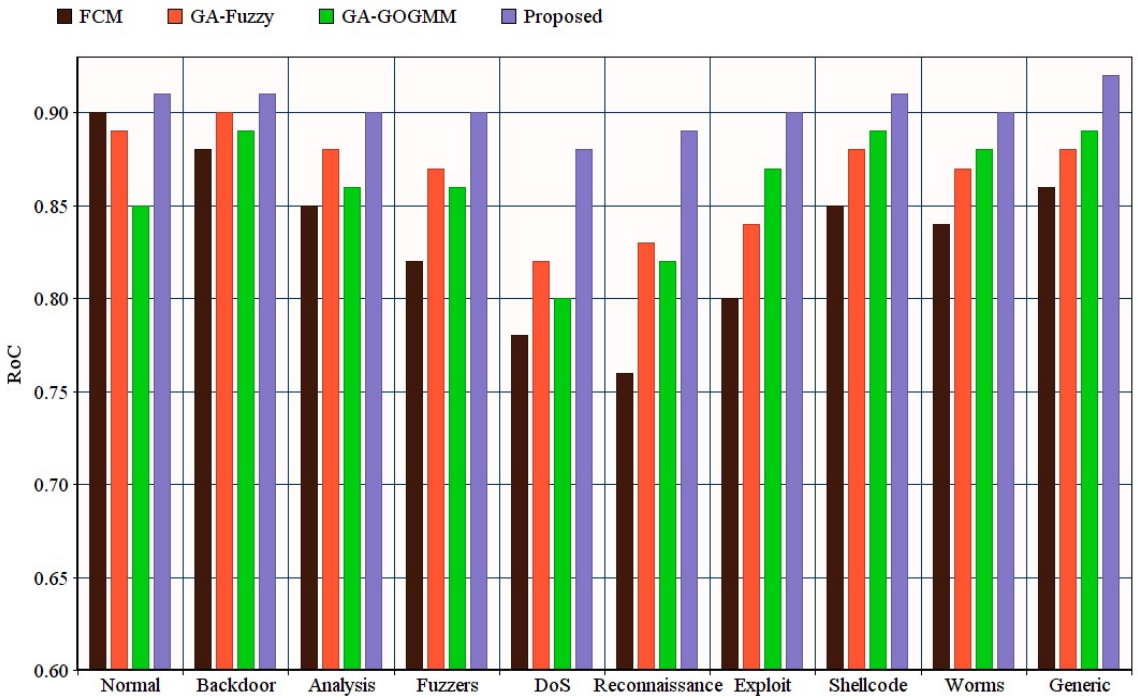

Figure 8: RoC

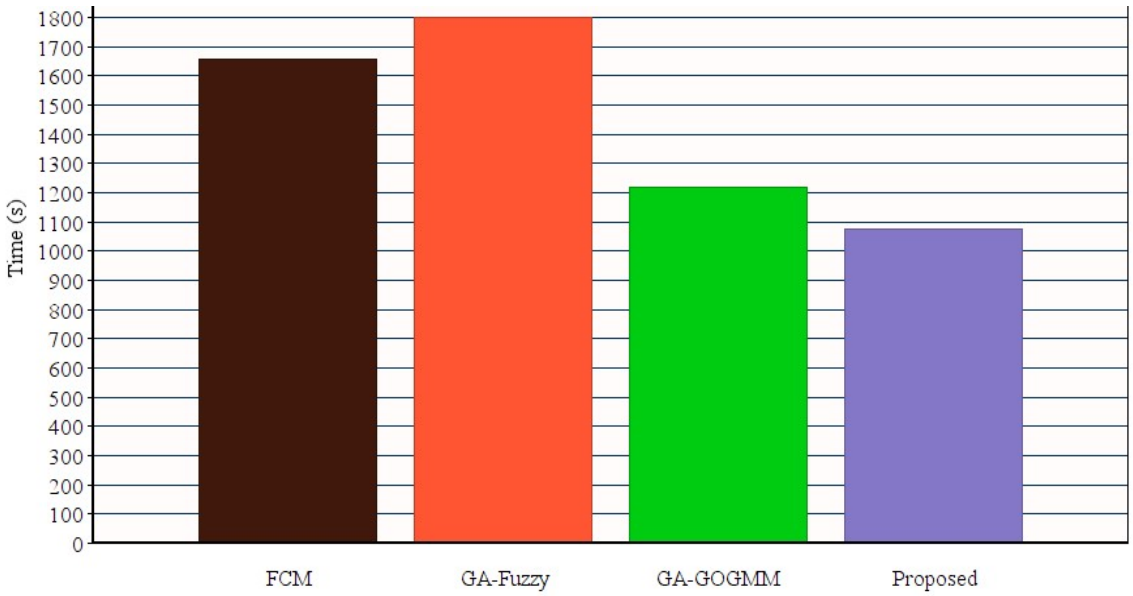

Figure 9: Time taken for intrusion detection

The time complexity of the proposed technique for the training and the testing sample is computed as the $O(\theta_1 * \theta_2 + \theta_2 * \theta_3)$ into the pre-processing stage. The fuzzy based classifier is used for replacing the actual classifier, the time complexity is completely similar and the final time complexity is computed as

$$O\left(m * l * (\theta_{11} * \theta_{21} + \sum_{j=1}^{N} \theta_{2j} * \theta_{2j+1} + \theta_{2N} * \theta_3\right).$$

5. CONCLUSION

In this paper, Fuzzy related feature selection technique with Optimized classification is proposed according to the multi-class classification that improves the detection accuracy and minimized false positives. The traffic pattern information is taken from the Internet in a sequence of big data and that information has been pre-processed to eliminate the redundant data with efficient temporal for completing the feature selection process. Hence, the fuzzy based technique identifies the good features for performing the classification through the dataset. The proposed technique is produced the alert system which identified the intrusion and protected from the unauthorized access and malicious activities. The proposed technique has been evaluated and more than 99% detection rate achieved which is larger than the related techniques.

REFERENCES

[1]. W. Stallings, Cryptography and Network Security: Principles and Practice, Pearson Upper Saddle River, NJ, 2017.

[2]. S. Ganapathy, R. Sethukkarasi , P. Yogesh , P. Vijayakumar , A. Kannan , An intelligent temporal pattern classification system using fuzzy temporal rules and particle swarm optimization, Sadhana 39 (2) (2014) 283–302 .

[3]. B.C. Rhodes , J.A. Mahaffey , J.D. Cannady , Multiple self-organizing maps for intrusion detection, in: Proceedings of the 23rd national information sys- tems security conference, 20 0 0, pp. 16–19 .

[4]. M. Panda , A. Abraham , M.R. Patra , A hybrid intelligent approach for network intrusion detection, Procedia Eng. 30 (2012) 1–9 .

[5]. M.-Y. Su , G.-J. Yu , C.-Y. Lin , A real-time network intrusion detection system for large-scale attacks based on an incremental mining approach, Comput. Secur. 28 (5) (2009) 301–309.

[6]. Q. Hu , S. An , X. Yu , D. Yu , Robust fuzzy rough classifiers, Fuzzy Sets Syst. 183 (1) (2011) 26–43.

[7]. K.R. Prabha, N. Jeyanthi, Intelligent intrusion detection system using temporal analysis and type-2 fuzzy neural

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

classification, Int. J. Internet Technol. Secur. Trans. 8 (2018) 167–184.
[8]. T. Maphatsoe, M. Masinde, Asymptotic analysis of a fuzzy based intrusion detection system for zigbee, in: 2018 International Conference on Intelligent and Innovative Computing Applications, ICONIC, 2018, pp. 1–8.
[9]. S.A. Mulay , P. Devale , G. Garje , Intrusion detection system using support vector machine and decision tree, Int. J. Comput. Appl. 3 (3) (2010) 40–43.
[10]. M. Tavallaee , N. Stakhanova , A .A . Ghorbani , Toward credible evaluation of anomaly-based intrusion-detection methods, IEEE Trans. Syst. Man. Cybern. Part C (Appl. Rev.) 40 (5) (2010) 516–524 .
[11]. A. Gabrielli , L.V. Mancini , S. Setia , S. Jajodia , Securing topology maintenance protocols for sensor networks, IEEE Trans. Dependable Secure Comput. 8 (3) (2011) 450–465.
[12]. Z.-H. Zhou , Y. Jiang , et al. , Medical diagnosis with c4. 5 rule preceded by artificial neural network ensemble, IEEE Trans. Inf. Technol.Biomed. 7 (1) (2003) 37–42.
[13]. J.-f. Tian , Y. Fu , Y. Xu , J.-l. Wang , Intrusion detection combining multiple decision trees by fuzzy logic, in: Parallel and Distributed Computing, Appli- cations and Technologies, 2005. PDCAT 2005. Sixth International Conference on, IEEE, 2005, pp. 256–258.
[14]. L.P. Rajeswari , K. Arputharaj , An active rule approach for network intrusion detection with enhanced c4. 5 algorithm, Int. J. Commun. Netw. Syst. Sci. 1 (04) (2008) 314.
[15]. Z. Xu , D. Gu , B. Yang , Attribute reduction algorithm based on genetic algorithm, in: Intelligent Computation Technology and Automation, 2009. ICI-CTA'09. Second International Conference on, vol. 1, IEEE, 2009, pp. 169–172.
[16]. M. Chen, N. Wang, H. Zhou, Y. Chen, FCM technique for efficient intrusion detection system for wireless networks in cloud environment, Comput. Electr. Eng. 71 (2018) 978–987.
[17]. C. Jin, Z. Ye, C. Wang, L. Yan, R. Wang, A network intrusion detection method based on hybrid rice optimization algorithm improved fuzzy Cmeans, in: 2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing SystemsI, DAACS-SWS, 2018, pp. 47–52.
[18]. V. Hajisalem, S. Babaie, A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection, Comput. Netw. (2018).
[19]. K. Pradeep Mohan Kumar, M. Saravanan, M. Thenmozhi, K. Vijayakumar, Intrusion detection system based on GA-fuzzy classifier for detecting malicious attacks, Concurr. Comput.: Pract. Exper. (2019) e5242.
[20]. J. Liu, W. Zhang, Z. Tang, Y. Xie, T. Ma, J. Zhang, G. Zhang, J.P. Niyoyita, Adaptive intrusion detection via GA-GOGMM-based pattern learning with fuzzy rough set-based attribute selection, Expert Syst. Appl. 139 (2020) 112845.
[21]. https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/UNSW-NB15-Datasets/