*Computer Systems Science & Engineering*
DOI: 10.32604/csse.2023.026776
***Article***

Tech Science Press

# Genetic-based Fuzzy IDS for Feature Set Reduction and Worm Hole Attack Detection

**M. Reji[1,*], Christeena Joseph[2], K. Thaiyalnayaki[2] and R. Lathamanju[2]**

[1]Department of Electronics and Communication Engineering, Rohini College of Engineering and Technology, Palkulam, Kanyakumari, India
[2]Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, India
*Corresponding Author: M. Reji. Email: rejieceped@gmail.com

Received: 04 January 2022; Accepted: 23 March 2022

**Abstract:** The wireless ad-hoc networks are decentralized networks with a dynamic topology that allows for end-to-end communications via multi-hop routing operations with several nodes collaborating themselves, when the destination and source nodes are not in range of coverage. Because of its wireless type, it has lot of security concerns than an infrastructure networks. Wormhole attacks are one of the most serious security vulnerabilities in the network layers. It is simple to launch, even if there is no prior network experience. Signatures are the sole thing that preventive measures rely on. Intrusion detection systems (IDS) and other reactive measures detect all types of threats. The majority of IDS employ features from various network layers. One issue is calculating a huge layered features set from an ad-hoc network. This research implements genetic algorithm (GA)-based feature reduction intrusion detection approaches to minimize the quantity of wireless feature sets required to identify worm hole attacks. For attack detection, the reduced feature set was put to a fuzzy logic system (FLS). The performance of proposed model was compared with principal component analysis (PCA) and statistical parametric mapping (SPM). Network performance analysis like delay, packet dropping ratio, normalized overhead, packet delivery ratio, average energy consumption, throughput, and control overhead are evaluated and the IDS performance parameters like detection ratio, accuracy, and false alarm rate are evaluated for validation of the proposed model. The proposed model achieves 95.5% in detection ratio with 96.8% accuracy and produces very less false alarm rate (FAR) of 14% when compared with existing techniques.

**Keywords:** Intrusion detection system; worm hole attack; genetic algorithm; fuzzy logic; wireless ad-hoc network

## 1 Introduction

Wireless networks have gained wide recognition in recent years as it requires very minimal infrastructure. The application of these networks can be seen in the field area of military, agriculture and emergency fields. On the other hand, wireless networks as a transmission medium provides an innate advantage to any adversary who expects to spy in or disrupt the network [1]. Wireless *ad hoc* network is a self-sorting and decentralized system. This network, in general, are prone to a variety of difficulties due to wireless communication, resource constraints, and changeable topology. Security is a serious issue in wireless *ad hoc* networks. Signatures are the sole thing that preventive measures rely on. Reactive methods such as IDS, detect all types of threats [2].

Intrusion detection is becoming a vital approach for screening system movements and identifying attacks in network like anomalous networks, unwanted network access, and hostile attack on computer system. A major segment of present arrangements adheres to systems, but they do not react to unexpected conditions [3]. There are two types of IDS: misuse and anomaly-based IDS. The most common type of intrusion detection is misuse intrusion detection, which uses established criteria to recognize harmful behaviour. These criteria serve as the foundation for identifying attacks that may include diverse fields of system packets, such as source and destination addresses, source and destination ports, or some watchwords in a packet's payload. The problem of this detection method is that all known assaults are programmed or specified in a database. Any new type of attack has to be updated in the database so that the system classifies the new behavior as an attack. As a result, this model needs consistent overhauling, however the advantage is they have less false positive rates. Anomaly based IDS recognize deviation from ordinary audit data and alarm to potential obscure or new attacks without having any earlier information of them. They display high false alarm rates; however, they have the capacity of identifying obscure attack and play out their tasks of searching for deviations much quicker [4,5].

Wormhole attack is one of the common attacks in wireless *ad hoc* networks. It is simple to launch that it requires no previous network knowledge. There is no need of compromising any normal node in the network. It creates false route between the sources to destination that is very short compared with the normal route. It makes confusion on the route discovery process and shows the ad-hoc network with wormhole attack scenario. In this network Node 'S' and 'D' are the source and destination. The attacker 1 and attacker 2 are cooperative wormhole attackers with high end tunnelling connection of wired or wireless. If attacker 1 receives route request packet it forwards to another end attacker 2 which is connected in long distance and it immediately broadcast locally in the destination area. Thus, destination node sends route reply to the node which is sent route request first. Attackers take this advantage to take the route through their tunnel connection. Once Source node receives route reply packet it forwards the data through the attacker node. After that attacker can able to capture the packets, analyze it and may forward or not.

Wireless Sensor Networking is a promising technology with applications ranging from heath care to tactical military. Although WSNs feature enticing characteristics (e.g., minimal installation cost, unattended network operation), the security of such networks is a major concern due to the lack of security (i.e., there are no switches or gateways for monitoring the flow of information). As a result, in order to run WSNs securely, any type of intrusion must be recognized prior to attackers may cause damage to the networks (i.e., sensor nodes) or data destination (i.e., base station or data sink). Security threats on WSN is classified into two types: passive and active. Passive attackers are often hidden and whether taps the communications channel for collecting data or disrupt network's functional aspects. Passive attacks are classified into four types: eavesdropping, node malfunctioning, node tampering/destruction, and traffic analysis. Active attacks are viewed as jamming, Denial-of-Service (DoS), hole attacks (wormhole, blackhole, sinkhole, etc.), floods, and Sybil. All of these threats are detected by intrusion detection systems (IDS). In this research, a genetic algorithm (GA)-based feature reduction intrusion detection system (IDS) is presented to reduce the number of wireless features sets necessary to detect worm hole attacks. The reduced feature set was fed into a fuzzy logic system for attack detection (FLS).

## 2 Literature Review

### 2.1 Genetic Algorithm Based Feature Reduction

A An approach for feature extraction based on GA was proposed in [6]. This method used weighted features for feature reduction. The comparison of this method with linear discriminant analysis provided better accuracy. A new topology based on subset selection method and was compared with dynamic subset selection was introduced in [7]. The fitness value was calculated based on the subset. The selection-based subset was faster than dynamic.

Genetic Programming method was used in [8] for identifying new attacks on systems which reduced low false negative and positive rates and improved high rate of distinguishing obscure attacks. GA technique for taking in the IDS was proposed in [9]. It used KDD cup 99 feature set for intrusion detection. The characters of the attacks such as smurf and warezmaster were summarized through the KDD 99. The average detection rate was 59%. A steady state genetic-based machine leaning algorithm to identify attacks was proposed in [10].

A method based on neural networks and GA was proposed in [11] to reduce the feature set and the model used KDD 99 cup set. This method was able to achieve higher detection rates by keeping up low false positive rate.

GA combined with k-nearest neighbor was implemented in [12] for reduction of features and detect DOS attack. For 19 features the known attacks shows that the accuracy was high and detection rate was also high. For 28 features the unknown attack has an overall accuracy of 78%. The three kinds of genetic fuzzy systems based on Michigan, Pittsburgh and iterative rule learning (IRL) techniques with dimensional reduction principle for detecting the attacks was proposed in [13]. In [14], three techniques based on hop count, neighbour list counts were combined to detect worm hole attack in Ad-hoc network.

IDS framework for wireless mesh networks that used the genetic algorithm-based feature selection and multiple SVM classifiers was proposed in [15]. This approach selected the informative features of ever attack type rather than the features shared by all attacks. GA-based feature selection was better for providing security to wireless networks since it has higher accuracy, lower computational complexity, and lower communication overhead.

A machine learning IDS in conjunction with the GA for features selection was proposed in [16]. For attack classification, decision trees, SVM, random forests, extreme gradient boosting, extra-trees, and naive Bayes were utilized. The fundamental disadvantage of this methodology is that it cannot detect new attacks. Because the model was trained with limited set of attacks. According to a significant number of research works, intrusion detection systems have a big number of feature sets that have been implemented. It can be extrapolated that the vast majority of IDS only used wired offline data (KDDCUP). The majority of intrusion detection systems were created for certain routing protocols. This research work focuses on reduction of feature set and development of genetic and fuzzy based intrusion detection.

### 2.2 Fuzzy Logic System Based Feature Reduction

Various strategies for extricating Fuzzy principles specifically from numerical information yield information for design characterization was proposed in [17]. Fuzzy standards with variable Fuzzy regions were characterized by actuation hyper boxes which demonstrated the presence area of information for a class and hindrance hyper boxes which restrained the presence of information for that class. The fuzzy values were extracted from the numeric data to find the data reduction.

The tuning Fuzzy control runs by GA to make the Fuzzy control frameworks or behavior of network in control process was proposed in [18]. The tuning method was used to find the fitness value. The defuzzification method was used to find the best fit among all the defined values. The results show improvement in Fuzzy GA. A machine learning of Fuzzy controllers, called a Pittsburgh Fuzzy Classifier System was proposed in [19]. Pittsburgh model of learning classifier frameworks utilized variable length run sets and developed Fuzzy set participation capacities to detect the anomaly.

Different strategies used in [20] for developing a smaller Fuzzy arrangement framework comprising of few semantic order rules. Authors used multi objective based genetic programming in order to reduce the feature set and for fuzzy rule for detection. They found that the detection rate was very less compared to GA. A genetic-based machine learning algorithm for outlining an IDS was proposed in [21] that comprises of Fuzzy if-then principles with clear semantic understanding. Their aim was to create few Fuzzy if-then standards from numerical information for a high-dimensional example grouping issue. Their work they looked at the two methodologies of Fuzzy GBML with linguistics fuzzy for high-dimensional data reduction.

A robust cooperative establishment of trust model was proposed in [22] to enhance the unwavering quality of packet delivery in MANETs, especially within the sight of vindictive nodes. In the proposed conspire, every node decides the reliability of alternate nodes as for solid packet sending by consolidating direct trust data acquired autonomously of different nodes and second-hand trust data got by means of suggestions from different nodes. Direct trust data for neighbor nodes is gotten by means of direct perceptions at the MAC layer while direct data for non-neighbor nodes is acquired through criticism from affirmations sent because of information packets. The proposed conspire uses data sharing among nodes to quicken the meeting of put stock in foundation systems, yet is powerful against the proliferation of false confide in data by malignant nodes. A topology for a cyber-attack and IDS was proposed in [23] to identify the presence of attack. The computational methodology was used to calculate the IDS performance parameters and to find source of cyber-attack.

### *2.3 Fuzzy and Genetic Based IDS*

An anomaly-based intrusion detection system (IDS) combining fuzzy and neural network approaches was proposed in [24]. Because of the usage of a fuzzy rule framework, the system is both lightweight and versatile. The NN utilized in this work filtered the nodes, which improves the accuracy of the system. In addition, using a fuzzy inference rule minimizes the quantity of nodes that must be examined in NN. The only considerations that must be taken into account are node mobility and density. However, other than the input parameters, this consideration has no effect on the NN structure.

In [25], for feature selection, a novel adaptive intrusion detection framework based on Fuzzy Rough sets and Allen's interval algebra was developed and tested on networks tracing data sets for selecting a huge level of attack data for better attack predictions in WSNs. Furthermore, a rough set and fuzzy based nearest neighbour approach (FRNN) was developed for the network traced data sets classification in order to improve accuracy. To boost performance even further, this model adds genetic-based feature refining to significantly improve performance.

To detect intrusions in a computer networks, a fuzzy rule–based classification system was deployed in [26]. To increase classification rate, an approach based on GA for rule weights specification was presented. A feature selection method could be used on an intrusion detection dataset to determine the most appropriate feature subsets that will deliver better outcomes in the shortest amount of time.

## 3 Proposed Methodology

As part of this research work, we implement a Genetic based feature reduction system which is used for feature reduction. This eliminates the irrelevant features thereby resulting in reduced training time and increased system performance. This research work describes a model called genetic based fuzzy IDS that is anomaly-based IDS for wireless *ad hoc* networks. An anomaly-based IDS for MANET should incorporate both distributed and cooperative properties in its architecture. It means that every node participating in the network should equip with anomaly IDS that aims to find out any abnormal behavior of wireless nodes.

Fig. 1 shows the conceptual model for this system. This work has four modules namely data collection, data preprocessing, Genetic based feature selection module and fuzzy detection module.

- Data collection module: This module monitors traffic data and captures feature set values from network layer. These values are stored in a table called neighbor table.
- Data preprocessing: This module processes real time data present over the network layer and transfers the same to the next module.
- Genetic based feature reduction module: GA based feature selection determines and eliminates the relevant features if any to minimize misclassification and improve the accuracy and processing time.
- Fuzzy based intrusion detection module: The reduced feature set namely hop count changes, *Rx* power and drop ratio helps to build a faster training and testing process, and it is capable of detecting the anomalies.

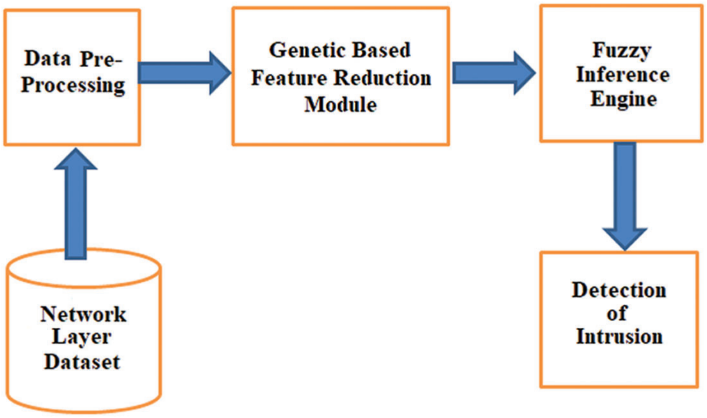

**Figure 1:** Conceptual model of gbf system

### *3.1 Genetic Based Feature Reduction Module*

In-line Fig. 2 illustrate the framework of genetic based selection of features technique. This framework used network data feature like PCH, PCR, Average delay etc., to identify & select the most relevant feature set from the network layer. This is followed by deciding a search strategy. A data set with 3 to 4 features is selected to detect the wormhole attack.

This framework focuses on designing an indirect approach to monitor the performance change of detection approach with change in features. The experiment was performed by selecting network layer features in real time environment. Results indicate that the detection accuracy has increased significantly.

#### *3.1.1 Normalization*

By using normalization, the values in the data sets are converted into the range of 0 to 1. The normalized value of feature data $x$ can be obtained by

$$N(x) = (x(F_k))/(max(F_k) - (F_k)) \tag{1}$$

where $(F_k)$ and $(F_k)$ denote the minimum and maximum values of the $k^{th}$ feature over the training data set (1 <= $k$ <= 12).

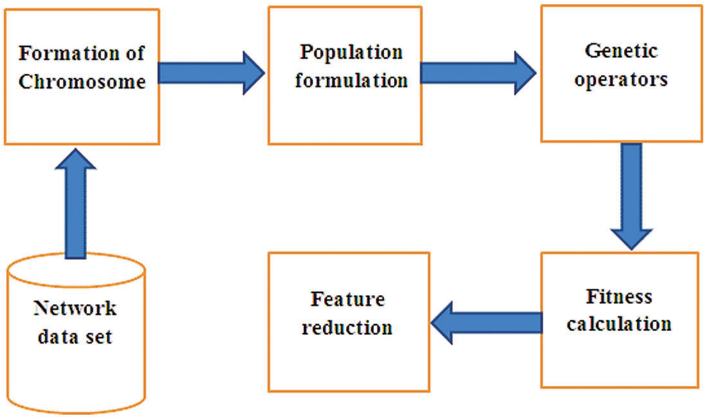

**Figure 2:** Framework of genetic based feature reduction approach

### *3.1.2 Fitness Value*

For this feature reduction main objective is to find the high correlation feature sets. This type of feature sets can able to detect all the anomalies and also accurately. The overall fitness calculation can be computed by taking the average CC of all chromosomes in the population. For example, *x* and *y* indicates the individual feature sets and the CC is computed by using the following equation [27].

$$cc = \left(n\sum xy - \left[\sum x * \sum y\right]\right) \div sqrt\left(\left[n\sum x^2 * \left(\sum x\right)^2\right] * \left[n\sum y^2 * \left(\sum y\right)^2\right]\right) \tag{2}$$

### *3.1.3 Steps for Feature Reduction Using GA*

1. Initialize the population.
2. Take total number of Features–$f_1, f_2, f_3, \ldots., f_n$ ($f_n$– $n^{\text{th}}$ feature).
3. Construct Chromosome - $CS$ - $CS_1$, $CS_2$, …, $CS_n$ ($CS_n$– $n^{\text{th}}$ Chromosome). Based on the level of feature reduction, size of the chromosome is defined as 2, 3 or 4. Example $CS_1 - \{f_1, f_2, f_3\}$, $CS_2 - \{f_3, f_4, f_3\}$, …, $CS_n - \{f_n{-}2, f_n{-}1, f_n\}$
4. Initialize the population P by randomly selecting feature and construct the subset form search space. Initially Chromosomes are filled with randomly picked feature.
5. To evaluate the Fitness function for each subset, CC is computed among the pair of individual features and computes the average CC for each Chromosome $CS_1 - \{f_6, f_3, f_7\}$.
6. Find the Pairwise CC $P(CC)$of features $(f_6, f_3)$, $(f_3, f_7)$, $(f_6, f_7)$.
7. CC of Subset $CS_1$ is defined as $CS_1(CC)$ = Average Pairwise CC.
8. Finally Fitness is calculated as average value of Chromosome CC $F(x) = \sum CS_i(CC)$
9. Crossover – based on predetermined probability of crossover, crossover the chosen feature.
10. Update the new population with Chromosome of new features - $P \leftarrow P_{new}$.
11. Evaluate – evaluate the fitness $f(x_i)$ of all individuals in $P$. Return the most fitted individual from $P$ Maximum Fitness value identified through multiple iteration.
12. Among the best fitness value in the population sets of features in the highest CC chromosome $CS_i$ $(CC)$ are selected for the anomaly detection. For example, $CS_2(CC) - \{f_4, f_8, f_9\}$.

### *3.2 Fuzzy Intrusion Detection System*

The FL system provides a new approach to classification and control problems. This method focuses on what is expected of the system rather than model how it works. FL is a method of reasoning which can be compared to the reasoning of humans. The decision-making process of humans is imitated by FL, involving each intermediate possibility among digital values and NO and YES. Replicating the human's decision of NO and YES, the standard logic blocks that the computer understand takes accurate inputs and provides definite outputs of FALSE and TRUE. Fig. 3 shows the block diagram of FL.

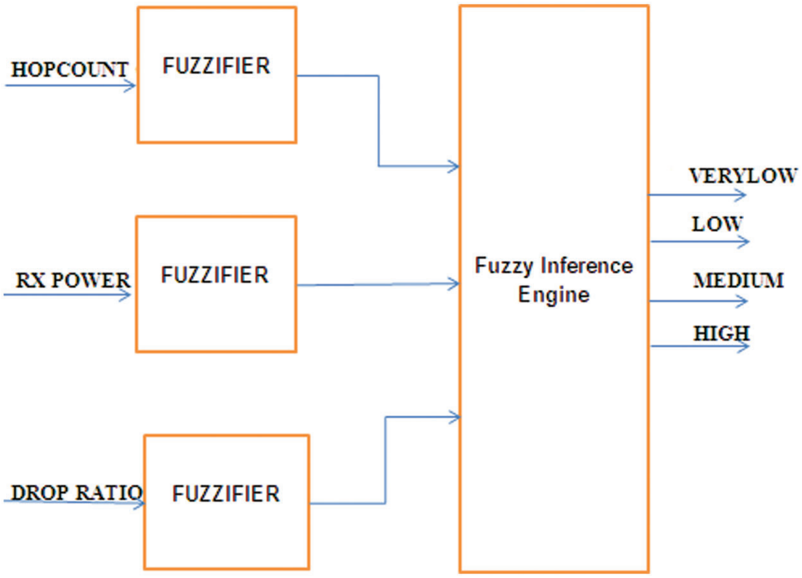

**Figure 3:** Block diagram of fuzzy logic

Lotfi Zadec, the inventor of FL, observed that while the process of human decisions making involves quite the ranges of possibilities among NO and YES, unlike the computers. In order to detect the anomaly and to reduce the features, fuzzy detection system is used. FL approach requires expertise in the knowledge of formulation of the rule base, combination of the sets and de-fuzzing [28–32]. The reduced feature set namely hop count changes, Rx power and drop ratio assists to create the faster testing and testing process, to have lower resource consumptions and to maintain higher detection rate. The key part in any fuzzy based IDS is fixing up the threshold value. It is a very difficult task and requires more reliable technique, so that fuzzy rules are used to fixing up the threshold value in this method. The data from the network are retrieved, finally fuzzy rules are created A node which exceeds this threshold value is malicious node and this malicious node is excluded from the network topology [33–35]. Tab. 1 represents the fuzzy rules for the proposed model.

**Table 1:** Fuzzy rules

| INPUT 1 | INPUT 2 | INPUT 3 | OUTPUT |
|---|---|---|---|
| LOW | LOW | LOW | VERY_LOW |
| LOW | LOW | MED | LOW |
| LOW | LOW | HI | LOW |
| LOW | MED | LOW | MED |

(Continued)

**Table 1 (continued)**

| INPUT 1 | INPUT 2 | INPUT 3 | OUTPUT |
|---|---|---|---|
| LOW | MED | MED | LOW |
| LOW | MED | HI | MED |
| LOW | HI | LOW | HI |
| LOW | HI | MED | HI |
| LOW | HI | HI | MED |
| MED | LOW | LOW | LOW |
| MED | LOW | MED | VERY_LOW |
| MED | LOW | HI | MED |
| MED | MED | LOW | LOW |
| MED | MED | MED | MED |
| MED | MED | HI | HI |
| MED | HI | LOW | MED |
| MED | HI | MED | MED |
| MED | HI | HI | HI |
| HI | LOW | LOW | LOW |
| HI | LOW | MED | MED |
| HI | LOW | HI | MED |
| HI | MED | LOW | HI |
| HI | MED | MED | VERY_HI |
| HI | MED | HI | VERY_HI |
| HI | HI | LOW | MED |
| HI | HI | MED | VERY_HI |
| HI | HI | HI | VERY_HI |

The key part in any fuzzy based IDS is fixing up the threshold value. It is a very difficult task and requires more reliable technique, so that fuzzy rules are used to fixing up the threshold value in this method. The data from the network are retrieved, finally fuzzy rules are created A node which exceeds this threshold value is malicious node and this malicious node is excluded from the network topology.

## 4 Experimental Analysis

Network simulator 2 (NS2) is used for the simulation model. The NS−2 parameters are listed in Tab. 2. In the 1000 × 1000 m field all the nodes are deployed in random position. CBR (constant bit rate) applications traffic was utilized. The range of the nodes was determined as 250 m. Source and destination are selected as random. In this scenario numbers of nodes are fixed as 100 and the remaining parameters are same as in Tab. 2. Attackers are placed randomly and varied from 0 to 10. For each attacker 10 times simulation carried with different scenarios. The average value is plotted.

**Table 2:** Parameters of simulation

| | |
|---|---|
| Simulation area | (1000 × 1000) m |
| Total nodes | 80 to 160 |
| Total time of simulation | 200 s |
| Size of packet | 512 byts |
| Initial energy | 100 J |
| MAC type | 802.11 |
| Attacker | 2 to 10 |
| Antenna model | Omnidirectional |
| Total traffic | 1–5 |
| Application | CBR |

### *4.1 Network Performance Analysis*

The network performance parameters of GBF IDS for wireless *ad hoc* networks were analyzed utilizing the parameters like delay, packet dropping ratio, normalized overhead, packet delivery ratio, average energy consumption, throughput, and control overhead.

From Fig. 4 it is found that by varying the number of attacker delay is minimized in GBF based IDS. It is observed that GBF achieves 57.9% less, statistical parametric mapping (SPM) achieves 44% less and principal component analysis (PCA) achieves 25% less when compared to without IDS detection (Wo-IDS). When comparing the IDS schemes delay is 25% low in SPM, 43.7% low in GBF compared to PCA. GBF achieves 24.9% less delay compared with SPM.

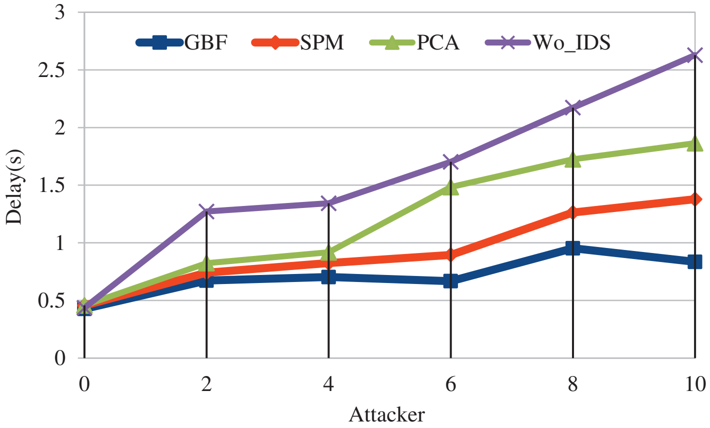

**Figure 4:** Attacker *vs*. delay

Through modifying the number of attackers dropping ratio was minimized in GBF based IDS as shown in Fig. 5. It is observed that GBF achieves 80.8% less, SPM achieves 72.55% less and PCA achieves 69.3% less when compared to Wo-IDS. When comparing the IDS schemes dropping ratio is 10.3% low in SPM, 37.6% low in GBF compared to PCA. GBF achieves 30.48% less dropping ratio compared with SPM.

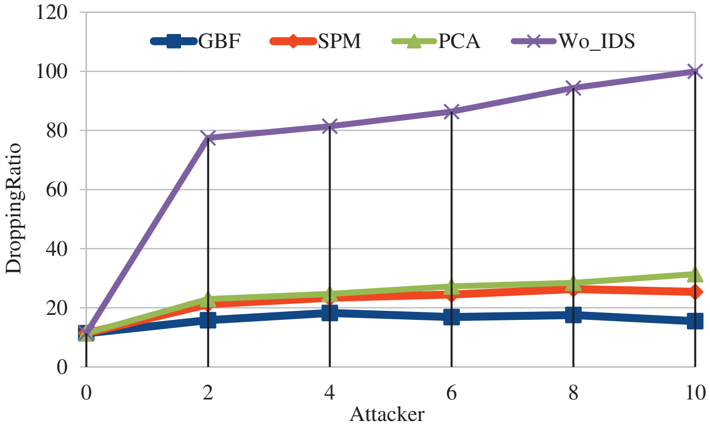

**Figure 5:** Attacker *vs*. dropping ratio

Through modifying the number of attacker packet delivery ratio was improved in GBF IDS as shown in Fig. 6. It is observed that GBF achieves 85.4% more, SPM achieves 84% more and PCA achieves 83% more when compared to Wo-IDS. When comparing the IDS schemes packet delivery ratio is 3% more in SPM, 13.8% more in GBF compared to PCA. GBF achieves 9% more packet delivery ratio compared with SPM.

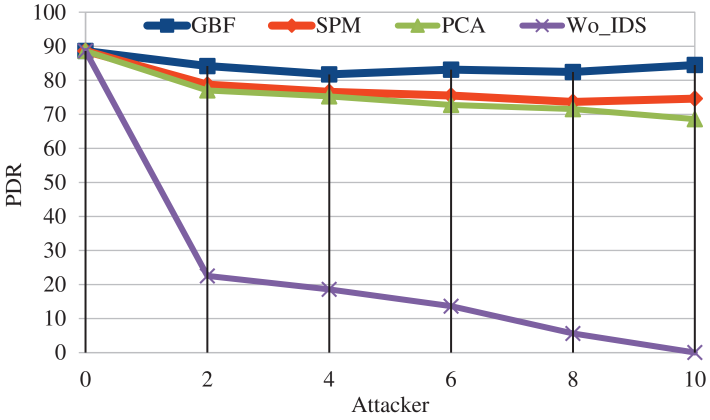

**Figure 6:** Attacker *vs*. packet delivery ratio

From Fig. 7 it is found that by varying the number of attacker average energy consumption is minimized in GBF based IDS. It is observed that GBF achieves 49% less, SPM achieves 45.05% less and PCA achieves 35.6% less when compared to Wo-IDS. When comparing the IDS schemes average energy consumption is 14.8% low in SPM, 21.7% low in GBF compared to PCA.GBF achieves 8% less average energy consumption compared with SPM.

It is found that by varying the number of attacker throughput is improved in GBF based IDS as shown in Fig. 8. It is observed that GBF achieves 85.47% more, SPM achieves 84% more and PCA achieves 83.4% more when compared to Wo-IDS. When comparing the IDS schemes throughput is 3% more in SPM, 13.8% more in GBF compared to PCA. GBF achieves 9% more throughput compared with SPM.

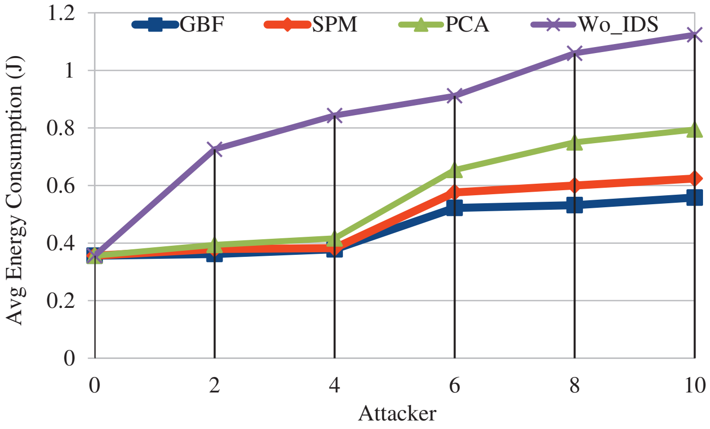

**Figure 7:** Attacker *vs*. energy consumption

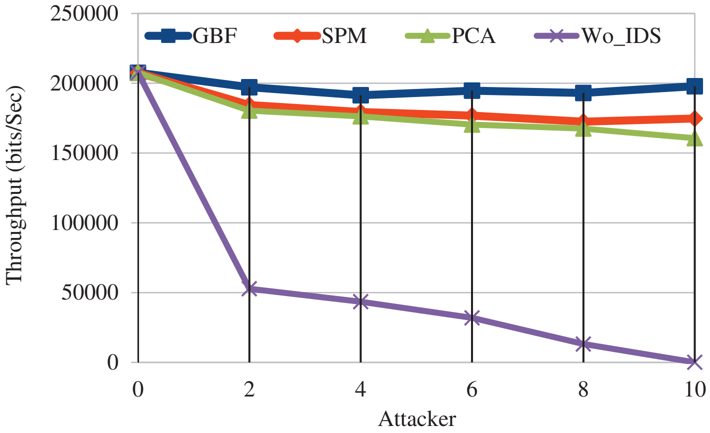

**Figure 8:** Attacker *vs*. throughput

### *4.2 IDS Performance Analysis*

Tables The IDS performance parameters of GBF-IDS for wireless *ad hoc* networks were analyzed utilizing parameters like detection ratio, FAR, and accuracy.

It was discovered that by changing the number of attacker detection ratio was 78.7% higher in SPM, 82.04% higher in GBF compared to PCA. GBF achieves 18.3% high in detection ratio compared with SPM shown in Fig. 9.

Fig. 10 represents by changing the count of nodes accuracy was 4% higher in SPM, 1% higher in GBF compared to PCA. GBF achieves 5% high in accuracy compared with SPM.

Fig. 11 represents by changing the count of nodes, false alarm rate was 22.1% lower in SPM, 68.7% less in GBF compared to PCA. GBF achieves 59.8% high in accuracy compared with SPM.

Detection ratio, accuracy, and FAR were measured as the IDS parameters. The proposed model achieved 95.5% detection ratio, which is 15% to 19% higher than the compared models. The proposed model achieved 96.8% accuracy, which is 5.8% to 8.8% improved than the compared models. The proposed model achieved 14% FAR, which is the lowest FAR compared to the other models. From the simulation results it is found that detection ratio and accuracy is high in genetic based fuzzy Intrusion detection system.

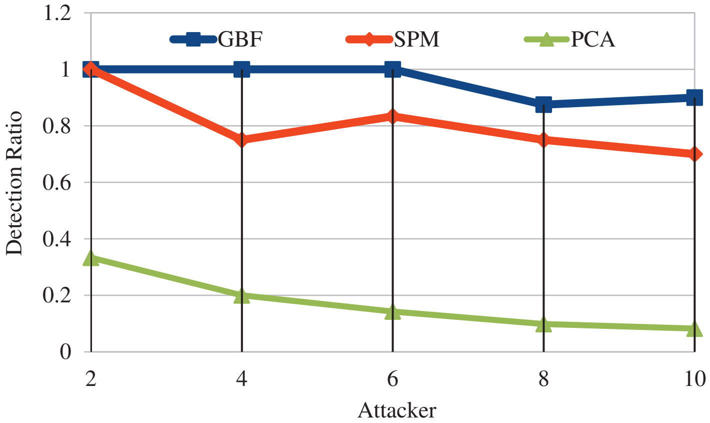

**Figure 9:** Attacker *vs*. detection ratio

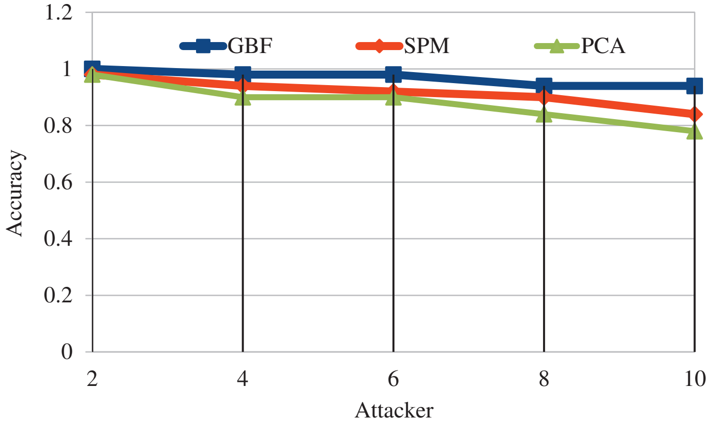

**Figure 10:** Attacker *vs*. accuracy

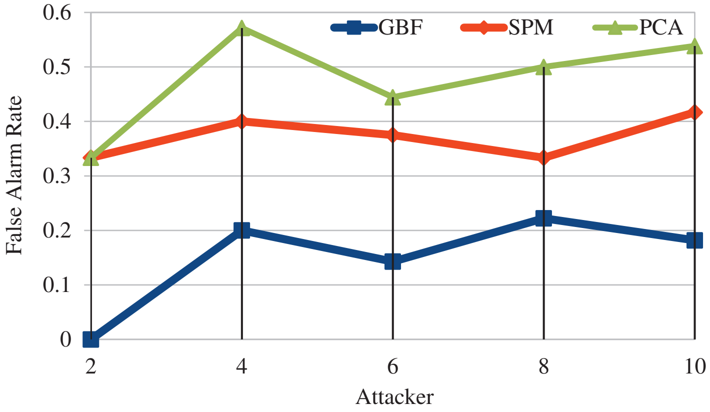

**Figure 11:** Attacker *vs*. false alarm rate

## 5 Conclusion

The primary focus of this research work is directed towards developing a GA based feature selection algorithm with an attempt to reducing the feature set and confining the same to limited number of relevant features. This model deploys genetic approach to identify & select the most relevant features present in the network layer. The feature sets are reduced into three and is given as an input to fuzzy IDS for detecting wormhole attacks. Based on the Fuzzy system output the attacks are detected. It is observed that the accuracy is 96.8% and, detection rate is 95.5% is achieved through GBF based intrusion detection system. From the results of simulation, it was found that by changing the number of attackers IDS performance Metrics Detection ratio & Accuracy is increased for genetic based fuzzy IDS when compared to other techniques. The GBF based IDS scheme achieves 95.5% in detection ratio with 96.8% accuracy and produces very less alarm rate of 14% when compared with existing approaches. In future, the proposed model can be implemented with the Internet of Things (IoT) network for detecting the attacks in the IoT using this IDS model.

**Funding Statement:** The authors received no specific funding for this study.

**Conflicts of Interest:** The authors declare that they have no conflicts of interest to report regarding the present study.

## References

[1] V. Sangeetha and A. Prakash, “An efficient intrusion detection system for cognitive radio networks with improved fuzzy logic-based spectrum utilization,” in *Materials Today: Proc.*, Elsevier, Netherlands, 2021.

[2] K. Khan, A. Mehmood, S. Khan, M. A. Khan, Z. Iqbal *et al.,* “A survey on intrusion detection and prevention in wireless ad-hoc networks,” *Journal of Systems Architecture*, vol. 105, no. 1, pp. 101701, 2020.

[3] T. J. Nagalakshmi, M. Balasaraswathi, V. Sivasankaran, D. Ravikumar, S. J. Gladwin *et al.,* “Evaluation of feature selection techniques in intrusion detection systems using machine learning models in wireless ad hoc networks,” in *Sensor Data Analysis and Management: The Role of Deep Learning*, First. ed., vol. 1. USA: Wiley-IEEE Press, pp. 33–72, 2021.

[4] I. S. Thaseen, J. S. Banu, K. Lavanya, M. R. Ghalib and K. Abhishek, “An integrated intrusion detection system using correlation-based attribute selection and artificial neural network,” *Transaction on Emerging Telecommunication Technologies*, vol. 32, no. 2, pp. e4014, 2021.

[5] K. P. M. Kumar, M. Saravanan, M. Thenmozhi and K. Vijayakumar, “Intrusion detection system based on GA-fuzzy classifier for detecting malicious attacks,” *Concurrency and Computations: Practices and Experiences*, vol. 33, no. 3, pp. e5242, 2021.

[6] M. L. Raymer, W. F. Punch, E. D. Goodman, L. A. Kuhn and A. K. Jain, “Dimensionality reduction using genetic algorithms,” *IEEE Transaction on Evolutionary Computations*, vol. 4, no. 2, pp. 164–171, 2000.

[7] C. W. Lasarczyk, P. P.Dittrich and W. Banzhaf, “Dynamic subset selection based on a fitness case topology,” *Evolutionary Computation*, vol. 12, no. 2, pp. 223–242, 2004.

[8] W. Lu and I. Traore, “Detecting new forms of network intrusion using genetic programming,” *Computational Intelligences*, vol. 20, no. 3, pp. 475–494, 2004.

[9] S. Selvakani and R. S. Rajesh, “Genetic algorithm for framing rules for intrusion detection,” *International Journal of Computer Science and Network Security*, vol. 7, no. 11, pp. 285–290, 2007.

[10] W. Al-Sharafat and R. Naoum, “Steady state genetic-based machine learning for network intrusion detection (SSGBML-NID),” in *Int. Conf. on Education and New Learning Technologies*, Barcelona, Spain, pp. 199–206, 2009.

[11] S. S. Kandeeban and R. S. Rajesh, “Integrated intrusion detection system using soft computing,” *International Journal of Network Security*, vol. 10, no. 2, pp. 87–92, 2010.

[12] M. Y. Su, “Real-time anomaly detection systems for denial-of-service attacks by weighted k-nearest-neighbor classifiers,” *Expert Systems with Applications*, vol. 38, no. 4, pp. 3492–3498, 2011.

[13] M. S. Abadeh, H. Mohamadi and J. Habibi, “Design and analysis of genetic fuzzy systems for intrusion detection in computer networks,” *Expert Systems with Applications*, vol. 38, no. 6, pp. 7067–7075, 2011.

[14] A. Vani and D. S. Rao, “A simple algorithm for detection and removal of wormhole attacks for secure routing in ad hoc wireless networks,” *International Journal on Computer Science and Engineering*, vol. 3, no. 6, pp. 2377–2384, 2011.

[15] R. Vijayanand, D. Devaraj and B. Kannapiran, “Intrusion detection system for wireless mesh network using multiple support vector machine classifiers with genetic-algorithm-based feature selection,” *Computers & Security*, vol. 77, no. 1, pp. 304–314, 2018.

[16] S. M. Kasongo, “Genetic algorithm-based feature selection technique for optimal intrusion detection,” *Preprints*, vol. 1, no. 1, pp. 1–22, 2021.

[17] S. Abe and M. S. Lan, “A method for fuzzy rules extraction directly from numerical data and its application to pattern classification,” *IEEE Transaction on Fuzzy System*, vol. 3, no. 1, pp. 18–28, 1995.

[18] F. Herrera, M. Lozano and J. L. Verdegay, “Tuning fuzzy logic controllers by genetic algorithms,” *International Journal of Approximate Reasoning*, vol. 12, no. 3–4, pp. 299–315, 1995.

[19] B. Carse, T. C. Fogarty and A. Munro, “Evolving fuzzy rule-based controllers using genetic algorithms,” *Fuzzy sets and system*, vol. 80, no. 3, pp. 273–293, 1996.

[20] H. Ishibuchi, M. Nii and T. Murata, “Linguistic rule extraction from neural networks and genetic-algorithm-based rule selection,” in *Proc. of Int. Conf. on Neural Network*, Houston, TX, USA, vol. 4, pp. 2390–2395, 1995.

[21] H. Ishibuchi, T. Nakashima and T. Kuroda, “A hybrid fuzzy genetics-based machine learning algorithm: Hybridization of Michigan approach and Pittsburgh approach,” in *IEEE SMC’99 Conf. Proc., 1999 IEEE Int. Conf. on System, Man, and Cybernetics*, Tokyo, Japan, vol. 1, pp. 296–301, 1999.

[22] Z. Charikleia, L. M. Brian, H. Marek, K. Roshan and T. E. Hermes, “A robust cooperative trust establishment scheme for mobile ad-hoc networks,” *Ad Hoc Network*, vol. 7, no. 6, pp. 1156–1168, 2009.

[23] A. W. Al-Dabbagh, Y. Li and T. Chen, “An intrusion detection system for cyberattacks in wireless networked control systems,” *IEEE Transaction on Circuits and System II: Express Brief*, vol. 65, no. 8, pp. 1049–1053, 2017.

[24] S. Sinha and A. Paul, “Neuro-fuzzy based intrusion detection system for wireless sensor network,” *Wireless Personal Communication*, vol. 114, no. 1, pp. 835–851, 2020.

[25] K. Selvakumar, M. Karuppiah, L. S. Ramesh, S. H. Islam, M. M. Hassan *et al.,* “Intelligent temporal classification and fuzzy rough set-based feature selection algorithm for intrusion detection system in WSNs,” *Information Science*, vol. 497, no. 1, pp. 77–90, 2019.

[26] Z. A. Varzaneh and M. K. Rafsanjani, “Intrusion detection system using a new fuzzy rule-based classification system based on genetic algorithm,” *Intelligent Decision Technologies*, vol. 15, no. 2, pp. 231–237, 2021.

[27] R. Elhefnawy, H. Abounaser and A. Badr, “A hybrid nested genetic-fuzzy algorithm framework for intrusion detection and attacks,” *IEEE Access*, vol. 8, pp. 98218–98233, 2020.

[28] L. A. Zadeh, “Fuzzy logic,” *Computer*, vol. 21, no. 4, pp. 83–93, 1988.

[29] T. Anitha, S. Manimurugan, S. Sridhar, S. Mathupriya, G. C. P. Latha, “A review on communication protocols of industrial internet of things,” in *Proc. of 2022 2nd Int. Conf. on Computing and Information Technology*, Tabuk, Saudi Arabia, pp. 418–423, 2022.

[30] S. Manimurugan, T. Anitha, G. Divya, G. C. P. Latha, S. Mathupriya, “A survey on blockchain technology for network security applications,” in *Proc. of 2022 2nd Int. Conf. on Computing and Information Technology*, Tabuk, Saudi Arabia, pp. 440–445, 2022.

[31] S. P. Sasirekha, A. Priya, T. Anitha, P. Sherubha, “Data processing and management in IoT and wireless sensor network,” *Journal of Physics: Conference Series*, vol. 1712, no. 1, pp. 012002, 2020.

[32] M. Alqdah, “Intrusion detection attacks classification using machine learning techniques,” *Journal of Computational Science and Intelligent Technologies*, vol. 2, no. 2, pp. 1–6, 2021.

[33] C. Narmatha, “A new neural network-based intrusion detection system for detecting malicious nodes in WSNs,” *Journal of Computational Science and Intelligent Technologies*, vol. 1, no. 3, pp. 1–8, 2020.

[34] M. S. Sheela, M. Rekha, R. Samuel, G. Divya, T. Rajendran, B. Umarani, “Multiple-input and multiple-output (MIMO) channel measurement in heterogeneous networks,” in *Proc. of 2022 2nd Int. Conf. on Computing and Information Technology*, Tabuk, Saudi Arabia, pp. 424–427, 2022.

[35] R. Khilar, K. Mariyappan, M. S. Christo, J. Amutharaj, T. Anitha, T. Rajendran, A. Batu, “Artificial intelligence-based security protocols to resist attacks in internet of things,” *Wireless Communications and Mobile Computing*, vol. 2022, no. 1440538, pp. 1–10, 2022.