Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.031876
Article

Tech Science Press

A Rule-Based Approach for Grey Hole Attack Prediction in Wireless Sensor Networks

C. Gowdham* **and S. Nithyanandam**

Department of Computer Science and Engineering, PRIST Deemed to be University, Thanjavur, 613403, Tamilnadu, India
*Corresponding Author: C. Gowdham. Email: gowdhamchinnaraju@gmail.com

Received: 28 April 2022; Accepted: 16 June 2022

Abstract: The Wireless Sensor Networks (WSN) are vulnerable to assaults due to the fact that the devices connected to them have a reliable connection to the internet. A malicious node acts as the controller and uses a grey hole attack to get the data from all of the other nodes in the network. Additionally, the nodes are discarding and modifying the data packets according to the requirements of the system. The assault modifies the fundamental concept of the WSNs, which is that different devices should communicate with one another. In the proposed system, there is a fuzzy idea offered for the purpose of preventing the grey hole attack from making effective communication among the WSN devices. The currently available model is unable to recognise the myriad of different kinds of attacks. The fuzzy engine identified suspicious actions by utilising the rules that were generated to make a prediction about the malicious node that would halt the process. Experiments conducted using simulation are used to determine delay, accuracy, energy consumption, throughput, and the ratio of packets successfully delivered. It stands in contrast to the model that was suggested, as well as the methodologies that are currently being used, and analogue behavioural modelling. In comparison to the existing method, the proposed model achieves an accuracy rate of 45 percent, a packet delivery ratio of 79 percent, and a reduction in energy usage of around 35.6 percent. These results from the simulation demonstrate that the fuzzy grey detection technique that was presented has the potential to increase the network's capability of detecting grey hole assaults.

Keywords: Attack prediction; grey hole; wireless sensor networks; rule-based model; grey attack

1 Introduction

The development of wireless sensor networks has ushered in an exciting new age in the study of personal computer systems (WSN). This WSN connects individuals with one another as well as the gadgets in order to establish a reliable connection to the internet [1]. It is concerned with the improvement of specific devices that rely on options without the interference of people and provide the data with another intelligent device for the purpose of attaining a given goal. These devices enable people to connect with one another, which presents a challenge in terms of safety [2]. The identity management, trust management, and access

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

control are all handled by the WSN. The issue of trust poses the greatest challenge to the operation of heterogeneous device systems, such as those used in wireless sensor networks [3,4]. The current structure serves as an institutionalisation to mention the problem on the WSN portal. The component Network region unit is detected to pick the vital fact to consider due to the uses as the important cities like proper lighting, traffic blockage, needed stopping, emergencies and the security like the difficult and the explosive gases, the levels of radiation, the military applications, and the appropriate setting like the contamination of the air, backwoods fire identification. The fact has the significant impact of causing the apps to continue running in the secure region unit, and it also enables the component area to be identified [5]. The component networks that are related to wireless detection are focused on being the partner degree, not dependent fact, in order to obtain the data that are in the errands of escalation. These errands include discerning the climate like living space, collecting information, the activity of knowledge package, insightful of tremor, and other things that are related to the machine. The essential exercise for the conventions of safety in wireless sensor network (WSN), which is the same as wormhole, sinkhole, special assault, etc., is to plan typically to particular assaults [6,7]. The devices that make up WSN are dispersed throughout large areas of geography. The fact that the systems can only be accessed remotely and in an open environment renders them defenceless against any and all forms of attack [8]. As a result, it has been suggested that the standard component should not be used to identify the differences between grey hole attacks and the technique, but rather that the technique should have the component of a motivator for energising the destination collaboration [9]. When reaching both goals, the method must select the pertinent recognition edge in an adaptive manner in order to increase the identification rates while simultaneously reducing the number of false positives [10]. This choice is determined by the data that have been accessed to perform the measurements. The two truth values are the foundation of the classic logic of the fuzzy. They are both I incorrect, and (ii) correct. It is not sufficient with complete and trustworthy data, and as a result, this cannot provide the judgement that is needed. The fuzzy set theory provides an appropriate method to interpret and represent hazy concepts by making use of partial memberships. The fuzzy set allows the members of any set to have the various membership degrees. This is because the fuzzy set is a set. The work is structured below: Section 2 provides a comprehensive analysis of various prevailing approaches and discusses the pros and cons. In Section 3, the methodology is elaborated, and the rule model is provided for grey hole attack prediction. The numerical outcomes are given in Section 4, followed by a conclusion in Section 5.

2 Related Works

In the real world, many types of irregularities exist in the deployment situation of wireless sensor networks [11] that affect the functions. It is concerned that the hub needs to provide the availability in the gap of inclusion, wormhole, dark opening, and the gaps that have happened in the topology. It eliminates the wireless sensor network from obtaining the goal [12]. Typically, the adversaries are the system of the bargain to create the oddities. These duplicate adversaries the uses of authentic hubs to catch the IDs of the hub and the cryptographic material to give the origin sticking that are related via the shaping sticking gaps. Further, the consecutive threat on the transport layer and network is the black hole. These research summaries that the blackhole, grey hole, and wormhole attack rely on a similar type. Yet, this is achieving various damage techniques. A group of malicious nodes simultaneously launches grey hole attack. These nodes incorrectly guide the source node by employing the shortest path attack. The short presentations of different gaps are followed in the wireless sensor networks. Remarkably, the zone comprises the system in which the sufficient hubs are inaccessible for providing the needed coverage measure for the actual application. If the adversary concentrates on the territory, this occurs to furnish having the capability to jam the radio frequency [13,14]. The locale comprises the wireless sensor network [15] in which the non-appearance of the hub and the previous hub is the way, and others are unable for any kind of job to direct the message. When the sensor network is meant to break down and the energy consumption increases, the routing holes are generated. A black hole is created when the data is missing [16,17] . It is one kind of DoS attack. The collection and the information transmission are uncertain at both ends. The vindictive hubs in the wormholes are setting up a passage in the middle. The sending starts or packets are obtained using the individual channel created for the communication of radio [18]. Black Holes assaults the Mobile Adhoc Network (MANET) dominantly. The fuzzy logic uses the procedures for recognizing the black hole, which is not independent of the endorsement specialist, assessing the vitality, test of bundle exactness, and the hub of belief for growing the Adhoc presentation concerning the demand distance vector (AODV) [19]. The forecast qualities are used to allocate the fuzzy construction, which is the scientific rationale for working on the problems to the unknown information goal [20]. The black hole attack's successor is the grey hole that is not dropping the corresponding packets and generates the illusion between the identity of the attacker and the trusted node [21]. The IDs technique is utilized by having the vote attribute for finding the attacker's node, and the difference between the attacker node and the trusted node is created. The many suggested researchers' methodologies [22]. The grey hole DoS attacks' minimization depends on the contradiction to assume that no collaboration of explicit node having one node by employing the internal knowledge alone to gain using the information of standard routing [23]. The five various threat models, like the different abilities of the attacker, are used to evaluate the technique to permit good knowledge on prevention [24]. Online detection is not attained in the existing study, though prediction performance is better during minimization. Henceforth, the technique is presented to detect the grey hole attacks on the phasor measurement unit to adopt the inherent timing information in the PMU data to detect packet drop attacks. All network attacks support the network infrastructure to obtain better precision and a reasonable accuracy rate [25–28].

3 Methodology

In a network, there are different kinds of attacks are there and these complete types of DoS attacks have characteristics that turn into two types. They are (i) partial Denial of Service (DoS) attacks and (ii) complete DoS attacks. The DoS attack will be the correspondence of mid-way among the target and source node via malicious node in the partial DoS attack. On the other hand, the relevant correspondence is not there between the target and source node over the malicious node in the complete DoS attack.

3.1 Problem Formulation

The number of network parameters is used as the below characteristics by assessing the work. The existing model has the issues that are higher consumption of energy, lower throughput, E2E delay, and the bit error rate (BER). The throughput is depicted as the number of packets delivered appropriately to the destination. The derivation of throughput is provided below.

$$Throughput = \frac{packetsent}{Totaldatapackets} \tag{1}$$

The throughput of the suggested model is computed for all the networks concerning the above equation. The E2E delay is another essential parameter to consider in this proposed system. The most considerable E2E delay of the prior approach enhances the operation time. The data packet is used to occupy the standard time in obtaining the aim and incorporates the complete postponements, which brings using the throughput buffering with the potential of route discovery at the border queue. It is mentioned scientifically as below.

$$AvgEED = \frac{S}{N} \tag{2}$$

The total time required for transmitting the packet to destination is S, and the total number of packets is N that is obtained from the different endpoints. When the network sends the data to the receiver, another major issue is the Bit error rate which is the received data has a more significant error. The different interventions are used during the communication using the BER that helps to compute the number of bits to alter. During the interval of time, big mistakes are separated through the moving bits. It is characterized as the percentage and this is the ratio of units of low executions.

$$BER = \frac{1}{2}\left(1 - \frac{\sqrt{SNR}}{\sqrt{(2 + SNR)}}\right) \tag{3}$$

$$BER = \frac{1}{(2 * SNR)} \tag{4}$$

The ratio of the signal power to the noise power is depicted as the Signal noise ratio (SNR) that is measured in decibels. The $SNR = P_{signal}P_{ratio} = noise's$ signal variance magnitude represents the noisy signal SNR. Like the ABM (Analog Behavioral Modeling), the existing model has greater power consumption. Hence, the proposed model utilizes a few approaches to overcome the energy issue and lower energy utilization. The entire routing protocol in the different scenarios devours the consumption of energy to characterize as vitality. The energy spent summation is obtained in every task mode through the time of re-enactment. It is numerically described below.

$$Energyconsumption = \sum_{i=0}^{n-1}(energy\_cosumed\_by\_node(i)) \tag{5}$$

3.2 Grey Hole Attack

There are two ways to use the grey hole attack, recorded below. The source is simulated by the grey hole attack and verified technique using the sending incompletely. Therefore, the attackers utilize the particular strategy to drop data packet to carry the authentic node and try to attract the attention. The interest is taken by the grey hole malicious node in the procedure of disclosure course, and the source course store is updated or directed to the table in short. A pernicious hub is catching complete relevant packets dropping on the arbitrarily precisely. At the same time, the vindictive hub is considered by the source inconsistent way, as the next bouncing hub, and the packets have similarly forwarded the packets.

1. The reachable User Datagram Protocol (UDP) bundles are dropped.
2. The UDP bundles are dropped, having the determination process arbitrarily.
3. The attack of the grey hole is altered by taking the real to the sinkhole. The hub considers the identification of the state if this is the malicious hub or the ordinary hub since this can go to the predicted hub switch across to the pernicious hub. It considers the variation among attacks where the packets are dropped by the nodes. Then the packets are sent by the nodes to the destination from the source. Thus, this is tracked intuitively. Hence, packets are selected to drop, and a malicious node behaves in the routing path for the chosen packet drop to happen, and grey hole attack is carried out.

4 Proposed System

Machines, humans, and each non-living thing in WSN are allowed to communicate with each other with the assistance of the Internet. Nowadays, WSN devices flood the marketplace. The devices are connected in WSN to send the information directly via the Internet Connection. The active Internet connection is established with the connected devices prone to security attacks. The fuzzy logic in the proposed model addresses the grey hole attack, which occurs in the wireless sensor network nodes deployed in WSN systems. Relate the network through the router to collect the data using the wireless sensor network by deploying the WSN system. The node will identify the attack which takes place in the platform of WSN having the deployment of sensors. Each node is connected to the network in a structured way in WSN to perform the different operations. The user and the client are connected to the base station to establish the WSN connection that behaves as the central controller. The complicated architecture is presented in WSN to make this prone to the grey hole attack. In WSN, the sensor node assists in sensing the attacks on the Wireless Sensor Networks. The routing protocols are utilized and it helps to make the practical decision to forward the packets between the nodes. There are two types of routing protocols deployed in WSN and WSN that are named as reactive and proactive. The reactive routing protocol is used to modify the network's structure. An aggressive routing protocol is utilized to process the network data. The grey hole attack occurs when the communication is begun between the wireless sensor nodes. Generally, the packets are generated by the attack in the communication nodes, affecting the users who need detailed data regarding packet loss.

Different sensor node provides the collected information to the detector of fuzzy logic for recognizing the grey hole attacks with fuzzy logic. Generally, the grey hole attacks are moved between overflowing, different recipient links, and alternate decreasing. Henceforth, the performances of the existing algorithm and the manual detection are not compelling. Subsequently, fuzzy logic is considered the novel approach in the WSN that has the most significant aim of accomplishment. The below steps are involved in the proposed system.

Step 1: In the first step, the grey hole data is collected and acquired from different nodes to notice the attack. The normal condition or the grey hole attacker attacks the sensor node. The network monitor continuously monitors the network in the proposed method.

Step 2: Secondly, the network monitor provides the data extracted into the fuzzy engine for analyzing the nodes' status in the network. Six features are chosen to detect network's status: source IP address, sequence number, forwarded type of packet, time of expiration, and destination IP address.

(1) Sequence number: sequence number of packets is stored.
(2) Source: source node IP address is stored.
(3) Destination: destination node IP address is stored.
(4) Packet Type: packet type like AODV is stored.
(5) Forwarded: The value “0” is stored when packet is not forwarded. If packet is forwarded, value “l” is stored.
(6) Expire Time: Node needs to forward the packet.

The malicious node in the grey hole attack deception by themselves as the CN for tricking another node. The node does not send the critical information, prevented by the grey hole attack, and selectively drops a few packets. The packets are received by working from each node in the network, and the attack is performed. Consider Node R as the sent node, and node B and node M are concerned as the intermediate nodes. For instance, the malevolent node B stops the interaction from node B to find the necessary data, which gets deleted automatically. Node R is unaware of this interaction if the node; M needs to transmit the data packet related to temperature to node R on the AC. The fuzzy logic system helps to detect this attack with the assistance of the proposed method, and the original packets are redirected to the following valid node for attaining the correct reception of data. The grey hole attack avoids communication from happening is nullified. The attack is predicted to provide fuzzy logic to process. The best decision is selected by the fuzzy logic that leads to the efficient processing of the system.

a. Fuzzy phases

Fuzzy can be used when the application encounters uncertainty or when the issues have dynamic behaviour. A fuzzy rule base is a suitable system for dealing with these issues. The author provided the membership function for all variables, and these membership functions can visually portray the fuzzy set and provides the membership object degree to the fuzzy set. The author needs to identify input and output variables in the preliminary step. Fig. 1 represents the general fuzzy logic system. The rule-based evaluation and defuzzification process is described.

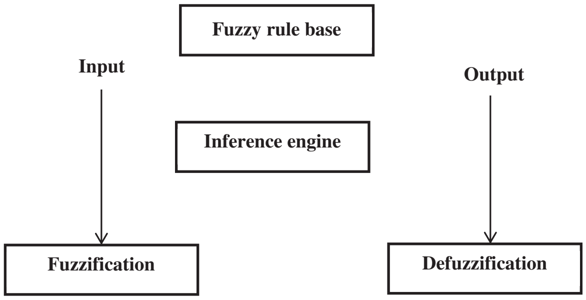

Figure 1: Generic fuzzy logic

i) Fuzzification and membership function

It is the process of fuzzifying the provided inputs and outputs. The degree is determined based on these inputs and outputs that belong to the appropriate fuzzy sets.

ii) Ruleset evolution

In a fuzzy rule set, the generation of rules plays a substantial role during the prediction process. The rule offers a sense of linguistic variables and membership function. Therefore, the process occupies those fuzzified inputs in the antecedent rules. Here, diverse rules are used to predict grey hole attack. The antecedent parts of rules are composed of a single part that offers opinion outcomes of antecedent development. It may govern risk level, and prediction relies on generated rules. The provided rules are applied over the simulation environment MATLAB 2020a based on the rule editor. After the fuzzification process, crisp is examined by provisioning the rule instance.

iii) Defuzzification

In this proposed prediction system, the systems have one output variable partitioned into two fuzzy sets. The model uses the centroid method that describes the functional membership area with a variable output range during the fuzzification process. It is expressed as in Eq. (6):

$$CoA = \frac{\int_{x_{min}}^{x_{max}} f(x).\, dx}{\int_{x_{min}}^{x_{max}} f(x)dx} \tag{6}$$

Here, CoA specifies the centre of the area; x represents linguistic variables, and x_{min} and x_{max} determine the array variables.

5 Numerical Results

This section provides the numerical outcomes of the anticipated model, which is executed in the MATLAB 2020a simulation environment.

a. Average throughput

The numerical results are calculated via the size of the complete packets that are achieved at the endpoint to partition via the entire data packets. Tab. 1 depicts the correlation among the suggested technique and the prevailing technique.

$$Throughput = \frac{packetsent}{Totaldatapackets} \tag{7}$$

Table 1: Throughput comparison

No. of rounds	Throughput		
	ABDUR	Fuzzy	Proposed
1	4.8	5.5	6.5
2	4.7	5.2	7.8
3	8.3	8.6	8.2
4	5.8	6.4	9.2
5	7.5	8.2	9.5

Lastly, the simulation is taken place to compare the throughputs for the suggested fuzzy-based protocol and AB-dynamic source routing (ABDSR) protocol during grey hole nodes. The proposed model and the ABDSR have the 90% of the throughput presented in Fig. 2, although there is no presence of grey hole nodes with the expectation of less throughput and an increase in the number of grey hole nodes. The normalized throughput is about 61%, while the number of malicious nodes is 20%. On the other hand, normalized throughput is about 45%, and the ABDSR has a throughput of about 33%, having the 30% as the grey hole nodes for the suggested fuzzy-based attack detection protocol. Meanwhile, the ABDSR has the 28%, in which 17% is the enhancement compared with ABDSR.

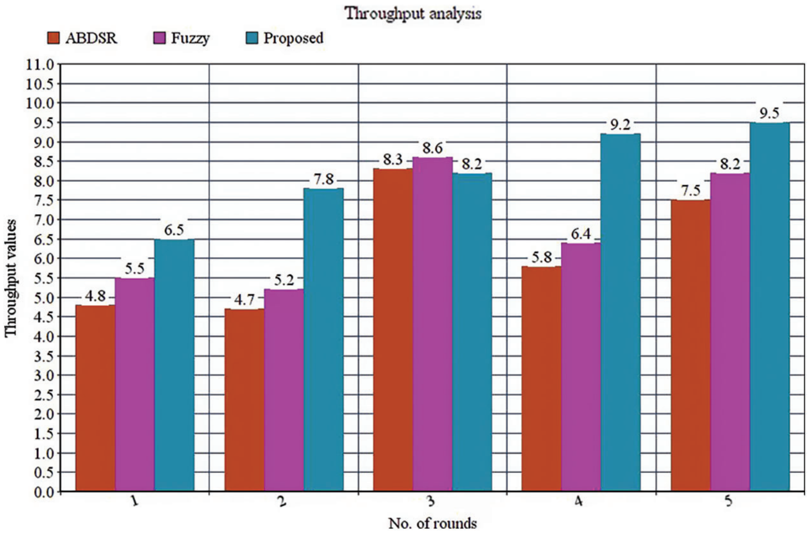

Figure 2: Throughput analysis

b. Packet delivery rate (PDR)

It is calculated by establishing several packets using the divided endpoint using the count of the number of packets to direct by the 100% × source. The comparison of delivery of packets with the different techniques having the suggested model is presented.

$$PDR = \frac{\sum_{i=1}^{n} PR_i}{\sum_{i=1}^{n} PS_i} * 100\% \tag{8}$$

c. Routing overhead

When the grey hole nodes are secure unexpectedly at different areas at total pause times as 5 sec, 10 sec, 15 sec, and 20 sec, the routing overhead is improved to 77.84%. Compared with AODV under attack, the suggested model has the overhead of routing lowered to 40%, 60% and 17.1% having the stability of route and the ABDSR with demand distance vector. The WSN related detection attains less overhead in routing with suggested fuzzy logic deployment lowered successfully to 34.56%, as in Fig. 3.

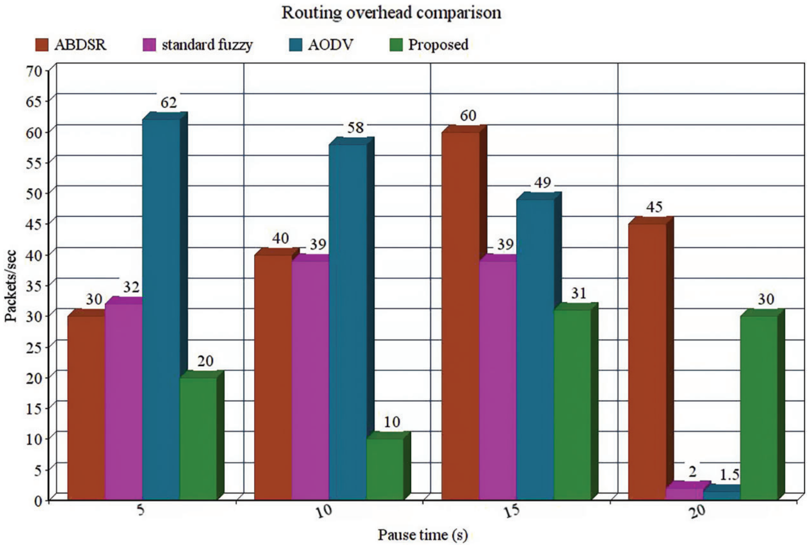

Figure 3: Routing overhead comparison

d. Jitter

When the grey hole nodes are fixed at different regions at all the pause times as 5 sec, 10 sec, 15 sec, and 20 sec accordingly, the attack coverage is enhanced to 0.56%. The total coverage of the technique obtains 25.56% in the occurrence of grey hole nodes, which is represented in Fig. 4 and Tab. 2. The coverage rate is increased successfully to 15.45% with the suggested fuzzy logic-based grey hole prediction.

e. BER

Tab. 3 presents the investigation of the present technique and the suggested technique. The number of bits/unit time is characterized. The bit error partition during time break via the absolute amount of moving bits is measured. It is the proportion of the minor performance unit and is often characterized as the rate. The relationship between the number of rounds and the BER is shown in Fig. 5. The rate of BER is lowered continuously when the number of rounds is increased. The suggested model reduces the BER rate compared with the previous technique like fuzzy, AODV, and ABDSR at 6. Yet, when at the round of 10, the RSDV does not lower the rate of BER to very low. Hence, the suggested model reduces the rate of BER to 50%, 27%, and 36% when compared with fuzzy, AODV, and ABDSR accordingly.

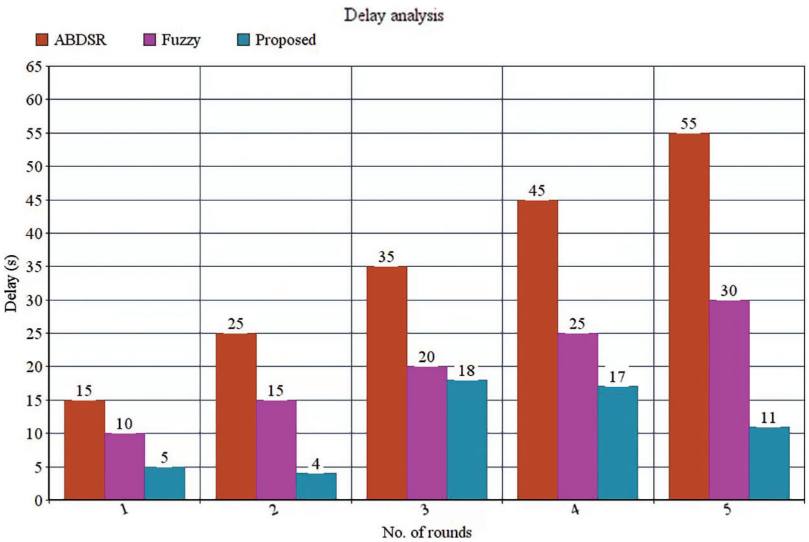

Figure 4: Delay comparison

Table 2: Delay comparison

No. of rounds	Delay		
	ABDUR	Fuzzy	Proposed
1	15	10	5
2	25	15	4
3	35	20	18
4	45	25	17
5	55	30	11

Table 3: BER comparison

No. of rounds	BER			
	ABDUR	ADV	Fuzzy	Proposed
1	10^{-8}	$10^{-0.8}$	$10^{-0.8}$	10^{-1}
2	10^{-1}	$10^{-1.5}$	10^{-1}	10^{-2}
3	10^{-1}	$10^{-3.2}$	$10^{-2.5}$	10^{-5}
4	10^{-2}	$10^{-4.5}$	10^{-3}	Very low
5	$10^{-3.5}$	Very low	$10^{-4.5}$	Very low

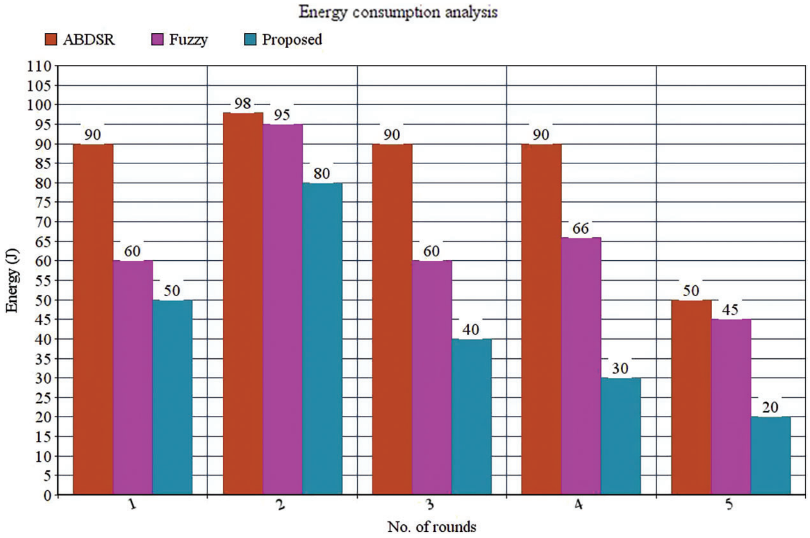

Figure 5: Energy consumption comparison

f. Energy consumption

It is presented as energy consumption via the entire progression of routing in different situations. It is obtained through the summation of spent energy in every node processing through the simulation time. It is given as follows.

$$Energyconsumption = \sum\nolimits_{i=0}^{n-1} (Energy\_consumed\_by\_node(i)) \tag{9}$$

Fig. 5 and Tab. 4 show the suggested model's energy efficiencies compared with previous techniques. The consumption of energy decreases gradually when the number of rounds is increased. Yet, the proposed process lowers energy consumption by about 35% to 40% compared with the previous approach.

Table 4: Energy consumption analysis

No. of rounds	Energy consumption		
	ABDUR	Fuzzy	Proposed
1	90	60	50
2	98	95	80
3	90	60	40
4	90	66	30
5	50	45	20

g. Detection accuracy

The accuracy detection percentage of malicious nodes identified using the normal nodes. It is calculated to find how the suggested model is specified from the previous model. Tab. 5 evaluates the accuracy of the existing model and the proposed model. The accuracy is increased 3.5 times compared to the standard fuzzy with the suggested model presented in Fig. 6. On the other hand, the accuracy is raised about two times compared with ABDSR. Lastly, the accuracy range is increased by one time compared with AODV. In addition, compared with the existing approaches, a better enhancement of accuracy is achieved in the suggested model.

Table 5: Detection accuracy comparison

No. of grey hole attacks	Detection accuracy			
	ABDUR	Standard fuzzy	ADV	Proposed
1	1.75	2	1.40	2
2	2	1.8	1.50	3
3	3	2.5	1.50	3.8
4	3.5	2	1.5	4
5	3.50	2.2	2	4.6

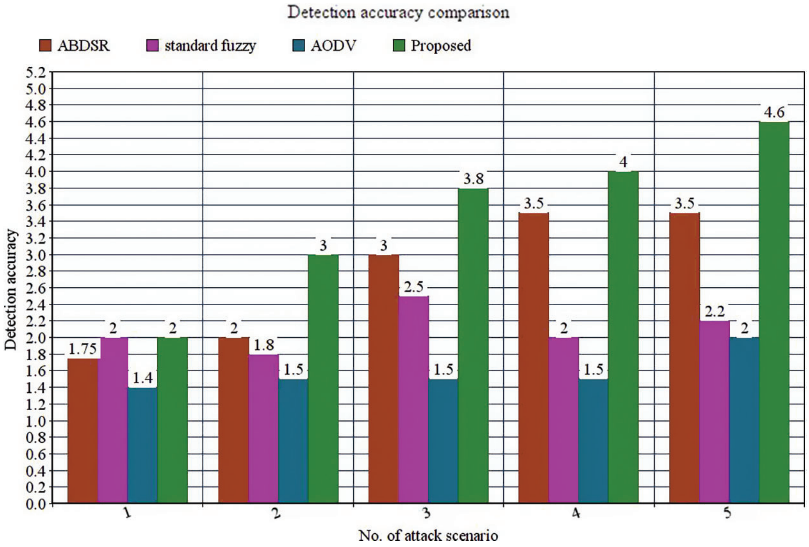

Figure 6: Detection accuracy comparison

6 Conclusion

In this research, fuzzy logic detects grey hole attacks in the suggested technique. The critical part of the proposed model is to find the network having the grey hole attack as the victim link to enhance the network's performance. The suggested fuzzy logic-based detection technique diminishes the energy consumption, complexity and jitter. The precision and accuracy are improved. The accuracy, consumption of energy, delay, the ratio of packet delivery and the throughput are achieved in the experiments of simulation, which is compared with the simulation in the suggested approach, other existing models, and ABM. The accuracy is improved to 45% compared with the current jitter approach. The energy consumption is about 35.6%, and the packet delivery ratio is about 78% in the suggested model. The simulation outputs present the proposed technique for fuzzy grey detection as the efficient technique to improve the network's capability and detect the grey hole attacks.

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] F. Zhang, H. A. D. E. Kodituwakku, J. W. Hines and J. Coble, "Multi-layer data-driven cyber-attack detection system for industrial control systems based on network, system and process data," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4362–4369, 2019.

[2] S. Kumar and K. Dutta, "Intrusion detection in mobile ad hoc networks: Techniques, systems, and future challenges," *Security and Communication Networks*, vol. 9, no. 14, pp. 2484–2556, 2016.

[3] W. Li, P. Yi, Y. Wu, L. Pan and J. Li, "A new intrusion detection system based on the KNN classification algorithm in a wireless sensor network," *Journal of Electrical and Computer Engineering*, vol. 2014, no. 240217, pp. 1–9, 2014.

[4] S. Dhaliwal, A. A. Nahid and R. Abbas, "Effective intrusion detection system using XGBoost," *Information*, vol. 9, no. 7, pp. 149–162, 2018.

[5] A. Nema, "Innovative approach for improving intrusion detection using genetic algorithm with layered approach," in *Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications*, IGI Global: Hershey, PA, USA, pp. 273–298, 2020.

[6] A. H. Hamamoto, L. F. Carvalho, L. D. H. Sampaio, T. Abrao and M. L. Jr. Proenca, "Network anomaly detection system using genetic algorithm and fuzzy logic," *Expert Systems with Applications*, vol. 92, pp. 390–402, 2018.

[7] 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, pp. 304–314, 2018.

[8] Y. Zhang, P. Li and X. Wang, "Intrusion detection for iot based on improved genetic algorithm and deep belief network," *IEEE Access*, vol. 7, pp. 31711–31722, 2019.

[9] Y. Maleh, A. Ezzati, Y. Qasmaoui and M. A. Mbida, "A global hybrid intrusion detection system for wireless sensor networks," *Procedia Computer Science*, vol. 52, pp. 1047–1052, 2015.

[10] M. A. Abdullah, B. M. Alsolami, H. M. Alyahya and M. H. Alotibi, "Intrusion detection of dos attacks in wsns using classification techniques," *Journal of Fundamental and Applied Sciences*, vol. 10, pp. 298–303, 2018.

[11] X. Tan, S. Su, Z. Huang, X. Guo, Z. Zuo *et al.,* "Wireless sensor networks intrusion detection based on SMOTE and the random forest algorithm," *Sensors*, vol. 19, pp. 203–222, 2019.

[12] C. Zhang, Y. Zhang, X. Shi, G. Almpanidis, G. Fan *et al.,* "On incremental learning for gradient boosting decision trees," *Neural Processing Letters*, vol. 50, pp. 957–987, 2019.

[13] C. Liu, Y. Li and N. Liu, "A boosted decision tree approach using Bayesian hyper-parameter optimization for credit scoring," *Expert Systems with Applications*, vol. 78, pp. 225–241, 2017.

[14] O. A. Osanaiye, A. S. Alfa and G. P. Hancke, "Denial of service defence for resource availability in wireless sensor networks," *IEEE Access*, vol. 6, pp. 6975–7004, 2018.

[15] M. C. Belavagi and B. Muniyal, "Performance evaluation of supervised machine learning algorithms for intrusion detection," *Procedia Computer Science*, vol. 89, pp. 117–123, 2016.

[16] N. Lu, Y. Sun, H. Liu and S. Li, "Intrusion detection system based on evolving rules for wireless sensor networks," *Journal of Sensors*, vol. 2018, pp. 1–8, 2018.

[17] Z. Sun, Y. Xu, G. Liang and Z. Zhou, "An intrusion detection model for wireless sensor networks with an improved v-detector algorithm," *IEEE Sensors Journal*, vol. 18, no. 5, pp. 1971–1984, 2017.

[18] Y. Ye, T. Li, D. Adjeroh and S. S. Iyengar, "A survey on malware detection using data mining techniques," *ACM Computing Surveys (CSUR)*, vol. 50, no. 3, pp. 1–40, 2017.

[19] Z. Khorshidpour, S. Hashemi and A. Hamzeh, "Evaluation of random forest classifier in the security domain," *Applied Intelligence*, vol. 47, no. 2, pp. 558–569, 2017.

[20] J. Sun, Z. Shang and H. Li, "Imbalance-oriented SVM methods for financial distress prediction: A comparative study among the new SB-SVM-ensemble method and traditional methods," *Journal of the Operational Research Society*, vol. 65, no. 12, pp. 1905–1919, 2014.

[21] M. A. Hasan, M. Nasser, S. Ahmad and M. K. Molla, "Feature selection for intrusion detection using random forest," *Journal of Information Security*, vol. 7, no. 3, pp. 129–140, 2016.

[22] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for internet of things," *Future Generation Computer Systems*, vol. 82, pp. 761–768, 2018.

[23] N. Farnaaz and M. A. Jabbar, "Random forest modelling for network intrusion detection system," *Proedia Computer Science*, vol. 89, pp. 213–217, 2016.

[24] Y. Liu, C. Xiang and H. Wang, "Optimization of feature selection based on mutual information in intrusion detection," *Journal of Northwest University (Natural Science Edition)*, vol. 47, pp. 666–673, 2017.

[25] J. H. Yan, "Optimization boosting classification based on metrics of imbalanced data," *Computer Engineering Application*, vol. 54, pp. 1–6, 2018.

[26] G. Chinnaraju and S. Nithyanandam, "Grey hole attack detection and prevention methods in wireless sensor networks," *Computer Systems Science and Engineering*, vol. 42, no. 1, pp. 373–386, 2022.

[27] R. Zhang, W. Z. Zhang, W. Sun, H. L. Wu, A. G. Song *et al.,* "A Real-time cutting model based on finite element and order reduction," *Computer Systems Science and Engineering*, vol. 43, no. 1, pp. 1–15, 2022.

[28] R. Zhang, H. L. Wu, W. Sun, A. G. Song and S. K. Jha, "A fast and accurate vascular tissue simulation model based on point primitive method," *Intelligent Automation & Soft Computing*, vol. 27, no. 3, pp. 873–889, 2021.