A Hybrid Approach for Black-hole Intrusion Detection using Fuzzy Logic and PSO Algorithm

M. Rohani hajiabadi [a], S. Gheisari [b], A. Ahvazi [c]

[a] Department of Computer Engineering, Information Technology and Electrical, Islamic Azad University, Qazvin, Iran.
[b] Department of Computer, Science and Research Branch, Islamic Azad University, Tehran, Iran.
[c] Department of Electrical & Computer Engineering, Tarbiat Modares University, Tehran, Iran.

Abstract
Wireless *Sensor* Networks (WSN) includes a large number of small sensor nodes and low cost, which are randomly located in a region. The wireless sensor network has attracted much attention from universities and industry around the world over the past decades, with features denser levels of node deployment, self-configuration, uncertainty of sensor nodes, computing, and memory constraints. Black-hole attack is one of the most known attacks on this network. In this study, the combination of fuzzy logic and particle swarm optimization (PSO) algorithms is proposed as an effective method for detecting black-hole attack in the AODV protocol. In the current study, a new function has been proposed in order to determine the membership of fuzzy parameters based on the particle swarm optimization algorithm. The proposed method was evaluated in different scenarios and was compared with other state of arts. The simulation result of this method proved the better performance in both detection rate and delivered packet rate.

Keywords:
Wireless sensor networks, AODV, Fuzzy logic, Particle swarm optimization

1. Introduction

Wireless sensor networks are known with features such as dense levels of node deployment, self-configuration, uncertainty of sensor nodes, lower consumption energy, computing and memory constraints compared to traditional networks. These sensor nodes can generally control physical and environmental conditions such as pressure, temperature, humidity and vibration of the sound. Such features ensure a wide range of applications for wireless sensor networks. In many WSN applications, the nodes cannot communicate directly with the base station due to limitations in their transmitters and receivers and the cost and the limited lifetime of the network. For this reason, in cases where the base station is not node in its radio range, the data is transmitted through other nodes that play the role of the routing station [1]. So, in WSNو the intrusion detection system is essential in case of data security assurance.

Intrusion detection system in WSN has been proposed using fuzzy logic [2]. A method for detecting black-hole attacks is developed using the SVM algorithm. The strategy of this method is to classify the network density based on the parameters of the total sent, received, forwarded and abandoned packets [3].

An Intrusion Detection System (IDS) has been proposed through combining the firefly optimization algorithm and k-means clustering algorithm in [4]. In this study, NSL-KDD data set was applied. The proposed combined method is compared with other methods such as k-means, k-means ++, k-means + bat and k-means + Cuckoo. A combination of observer and non-observer methods have been represented for a strong respond to the intrusion detection problem. In this study, the k-means algorithm has been used as an un-observer algorithm and has been combined with the adaptive SVM (Support Vector Machine) backup as a classification algorithm .The NSL-KDD dataset, which is the extensive version of the KDD 99, is also applied in this work [5]. K-means and k-mediods are used with Forward Neural Network in order to solve the problem of big data in intrusion detection [6].

A classifying tree of Naive Bayes is proposed in order to expose the profound infiltrate in the network. In order to scrutinize deeply, some challenges such as the missing data and alters in noise level have been added. Evaluating this task has been done on KDD99 data set and the findings indicates a favorable detection rate [7].

In [8], three objectives were considered: 1- Selecting the effective features and lessening the dimensions. 2- Selecting a sturdy algorithm for categorization and 3- Exposuring eccentric matters using split-based clustering

Manuscript received October 5, 2024
Manuscript revised October 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.10.13

algorithms. To accomplish the first aim, the methods of genetic algorithm and particle swarm optimization (PSO) have been applied. Classification has also been utilized by the nearest neighbor (NN) classification method. As a final point, by comparing diverse clustering methods, the Expectation Maximization (EM) clustering method has shown the best performance.

Intrusion detection system in the cloud computing environment have been proposed in [9]. In this case, the intrusion detection in the hyper-observer layer is performed through employing the Fuzzy-K means combination algorithm with the neural network algorithm (FCM-ANN). The findings have been tested on DARPA KDD CUP data set and the results demonstrated that the proposed method was able to discover infiltration with high detection accuracy and low error rate in contrast with two other comparative methods.

In [10], non-instantaneous approach have been proposed to detect network intrusion. In this work, fuzzy clustering C-means has been applied for labeling data and then the Multi-Layer Perceptron neural network has been used as a classifier.

A mixture of supervised and unsupervised data-mining techniques have been exploited with the purpose of detecting intrusion in the network. Subsequently, after initial preprocesses, an expert considered the approximate labels for data and indicated the number of clusters. As a final point, data has been evaluated using combined k-means and Random forest (KM-RF) clustering method [11].

As mentioned, numerous methods have been presented to supply an intrusion detection system. In this article, a framework was proposed in order to detect black-hole attacks in computer networks. To this end, fuzzy logic model was utilized whose parameters were set using particle swarm optimization (PSO).

The organization of the rest of paper was as follows: In section 2, the proposed framework was presented along with the utilized theory of algorithm. In section 3, results of simulation were in attendance along with the comparison of other states of art, and finally in section 4 the conclusion was arised.

2. The proposed method

Most of previous methods suffered from the implementation complexity and low detection rate in multi-attackers scenarios. In this paper, it was sought to consider the previous disadvantages in designing the proposed algorithm. The proposed algorithm was designed based on the behavior of an annoying node performing a black hole attack. An attacker node sends path response packets for each path request packet. It also does not send packets to the destination and throw them away. As a result, by tracking the behavior of the nodes, the attacker's node could be detected faster and some actions could be considered against that. Our proposed framework was based on following three stages:

1- Record of information: The behavior of nodes was always controlled during the network connection. By sending the packets for requesting path, information such as the source node, destination node, packet senders and etc. were recorded.
2- Fuzzy Algorithm: If the node encountered a path response packet and the packet information was pre-registered, it would be entered into this step; otherwise, it would be treated like an inexistence package.
3- Final decision: In this step, the fuzzy output was compared to the threshold, if it was larger, it was known as the attacker node and the state of that node would be changed to the inactive state. After that, the packages of this node would be inexistence.

2.1. Recording information

Each node requesting a path generated a row in Table 1. By receiving each route request packet (RREQ), this table was updated. The node receiving the path request message, if such a message existed in the rows of the table, would add the sender node to the sender list. Otherwise, the message would be destroyed. In this table, no node could add itself to the list of senders because it was done by its next node (the node that the packet has sent to it).

Table 1. Activity Record of the nodes

Senders list	Origin order number	Destination node	Origin node
3,4	1001	1	2

Table. 1 shows that a message with the order number of the Origin 1001 has been sent from node 2 to node 1, which has also participated in forwarding this message to nodes 3 and 4.

Since the attacking nodes can join together and acknowledge each other in Table 1, a field with verifiers would be obtained in Table 2. Each node that received the Routing Request Package (RREQ) encoded itself in the list of verifiers that received the message from it. In Table 2, a field called the number of suspicions was used to increase the intrusion detection rate. Maximum opportunity given to nodes was considered 3 , to give Answer the path without sending forward. If the field value was maxed out to be suspicious (3), the status of the node would be turned off. Inactive node messages were ignored.

Table 2. Status record of nodes

list of verifiers	number of suspicions	Status of nodes (active, Inactive)	node
3	1	active	2

2.2 Fuzzy Algorithm

The fuzzy criteria of the proposed method were characterized by the following two parameters:

1. The number of forward packets
2. Number of acknowledged nodes

Since the attackers did not send any forward messages (i.e. they do not send the request for the rout that they received), these criteria were used to detect the Being an attacker's nodes. By recording nodes activity in Table 1, the list of nodes were found that forwarded the rout request packets. So the absence of the names in this list indicated the inactivity of that node. If the attackers wanted to be partner with each other and endorsed each other in Table 1, second fuzzy parameter would be needed. This parameter was used by the number of verifiers. This parameter is available in Table 2. To specify these criteria, input and output membership functions were needed using fuzzy logic. In terms of both simplicity and high accuracy, triangular membership functions were used. To illustrate the fuzzy rules, the membership functions of the first input variables were used from symbols H, M, L, respectively, to represent low, moderate, and high amounts (Figure 1). For the second input variable, the L and H symbols were used for low and high amounts (Figure 2). In our proposed method, the membership functions` parameters were chosen using particle swarm optimization (PSO) algorithm. In this method mean square error was considered as the cost function in PSO.

The variation of membership function was considered as below:

$$\boldsymbol{q}^* = 10^{\pm\alpha} \times \boldsymbol{q}$$

Where $\boldsymbol{q}$ is initial parameter and $\boldsymbol{q}^*$ is optimum parameter vector. The correction coefficient α is set to 5.

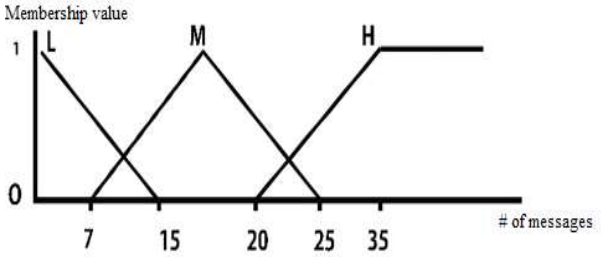

Figure 1. Membership functions for the input variable with respect to transmitted packets.

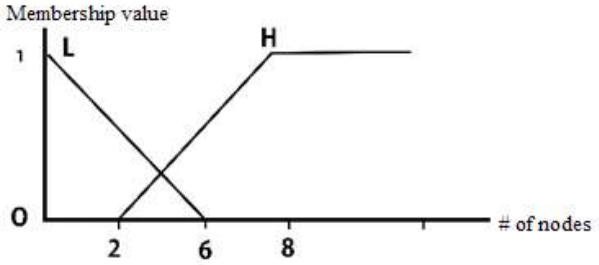

Figure 2. Membership functions for the input variable

Also, to describe the fuzzy rules, the output membership functions of the H, M, and L symbols were used as before. The fuzzy rule base is shown in Table 3. In this rule base, 6 occurrences may occur which are divided in 3 states. The most probable of attacking node existence is represented by the output of H and in the same way, the least probable of attacking node existence is represented by the output of L The defuzzification phase of the algorithm is also performed by the center gravity method.

Table 3. Fuzzy Rules` Base

output	number of verifiers	The number of packets sent
H	L	L
M	H	L

M	L	M
L	H	M
L	L	H
L	H	H

Finally, the output result was compared with the threshold for each scenario. If the output value was greater than the threshold, the target node would be considered as an attacker and would be added to the suspect field in Table 2. If its value reached the maximum, the status field for that node would be inactive in Table 2 and since then, the Packs of that node would be removed. In this research, the threshold was considered to be 8. If the threshold value was considered larger, the time to detect the attacker's node would be greater, which would cause more messages to be lost. Also if the value was considered smaller, the error would be increased.

3. Simulation Results

Ad hoc On-Demand Distance Vector Routing (AODV) protocol was considered in NS2 environment. The simulation environment parameters are shown in Table 4. The base parameter of this simulation was set to 10 node, 1 attacker and 40 meter distance of attacker to origin.

Table 4. Simulation environment parameters

parameters	value
Number of nodes	10,50,100
Number of packet drop nodes	5,1,3
Simulation time	700S
Type of traffic	UDP-CBR
Attacker nodes distance	50,40,30
Pack size	512 bytes
MAC protocol	802.11
Routing protocol	AODV
Simulation environment size	500×500m ^{2}

Firstly, it was shown that network efficiency was in time domain. The simulation run time was considered 700 seconds. The criteria for lost packets, delivered packets and network throughput are shown in the time series graphs in Figures 3 to 5, respectively. It can be seen from Figure 3 that the number of delivered packages was zero without using black-hole detection system. On the other hand, the delivery rate has been increased 88% using our proposed method. The same result is shown about lost packages in Figure 4. In addition, it can be seen that the throughput was getting better as the black-hole attack detection algorithm was detection intrusion in Figure 5. So, the above result clearly showed the benefit of using our approach.

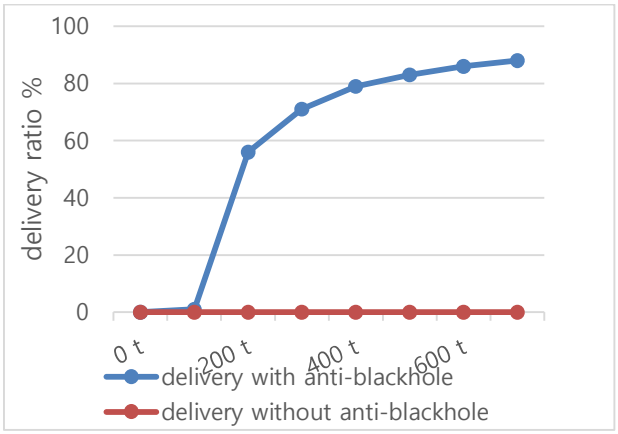

Figure 3. Received packet rate with and without using black-hole detection

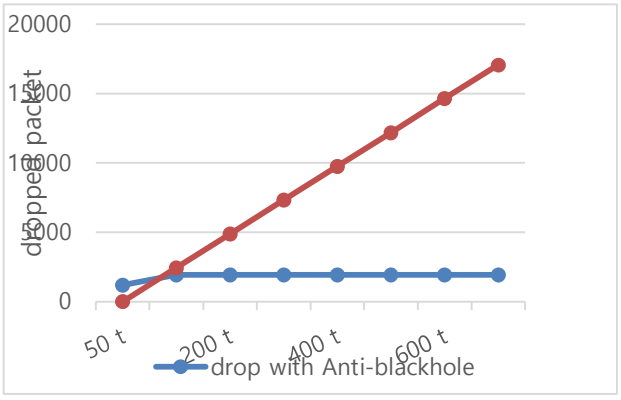

Figure 4. Lost packet rate with and without using black-hole detection

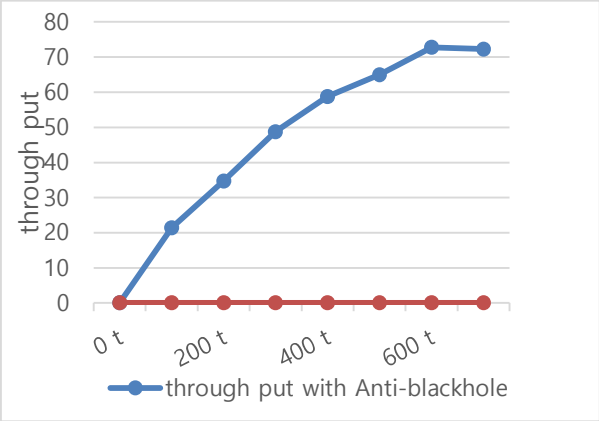

Figure 5. Throughput value with and without using black-hole detection

Our proposed method was compared with the state of art in [12] in order to prove the better performance of our algorithm. The delivered package rate is represented in Table 5 through comparing by OWCA and OWCAS methods. It can be seen from Table 5 that our proposed method showed the best result in all nodes` number scenarios. Furthermore, throughput rate is represented in Table 6 which proved that our method was completely efficient.

Table 4. Throughput packet percentage with comparison

# of nodes	OWCA [12]	OWCAS [12]	Our method
10	45%	70%	75%
50	63%	70%	74%
100	15%	68%	72%

Table 5. Delivered packet percentage with comparison

# of nodes	OWCA [12]	OWCAS [12]	Our method
10	45%	70%	75%
50	44%	43%	65%
100	48%	59%	62%

4. Conclusion

In this paper, a novel combination method based on fuzzy and meta-heuristic algorithm was proposed to provide an intrusion detection system in wireless *sensor* networks. The proposed method involved improving the fuzzy algorithm by selecting parameters with the particle swarm optimization algorithm in such a way that increased the accuracy in detection. The proposed hybrid algorithm was evaluated in different scenarios and the criteria were compared with the state of arts presented in [12]. The comparison results showed that the proposed algorithm has provided better performance in all cases.

References

[1] Taneja, Sunil and Kush, Ashwani,"A Survey of Routing Protocols in Mobile Ad Hoc Networks", International Journal of Innovation-management and Technology, 2010, Vol.11, No. 3

[2] Siddiqui, Shadab, Khan, Parvez.Mahmood and Khan, Muhammad.Usman," Fuzzy Logic Based Intruder Detection System in Mobile Adhoc Network ", BIJIT, December, 2014, ISSN 0973-5658, vol.6 No.2.

[3] Ortiz Antonio.M and Olivares, Teresa," Fuzzy LogicApplied to Decision Making in Wireless SensorNetworks", Fuzzy Logic – Emerging Technologies andApplications, 2012, ISBN 978-953-51-0337-0.

[4] Kaur, Arvinder, Saibal K Pal, and Amrit Pal Singh. "Hybridization of K-Means and Firefly Algorithm for intrusion detection system." International Journal of System Assurance Engineering and Management:1-10.

[5] Chahal, Jasmeen K, and Asst Prof Amanjot Kaur. "A Hybrid Approach based on Classification and Clustering for Intrusion Detection System." 2016.

[6] Chitrakar, Roshan, and Huang Chuanhe. "Anomaly detection using Support Vector Machine classification with k-Medoids clustering." Internet (AH-ICI), 2012 Third Asian Himalayas International Conference on.

[7] Chitrakar, Roshan, and Chuanhe Huang. "Anomaly based intrusion detection using hybrid learning approach of combining k-medoids clustering and naive Bayes classification." Wireless Communications, Networking and Mobile Computing (WiCOM), 2012 8th International Conference on.

[8] Syarif, Iwan, Adam Prugel-Bennett, and Gary Wills. "Data mining approaches for network intrusion detection: From dimensionality reduction to misuse and anomaly detection." Journal of Information Technology Review, 2012, 3, (2), 70-83.

[9] Pandeeswari, N, and Ganesh Kumar. "Anomaly detection system in cloud environment using fuzzy clustering based ANN." Mobile Networks and Applications, 2016, 21, (3), 494-505.

[10] Sunita, Swain, Badajena J Chandrakanta, and Rout Chinmayee. "A Hybrid Approach of Intrusion Detection using ANN and FCM." European Journal of Advances in Engineering and Technology, 2016, 3 (2), 6-14.

[11] Soheily-Khah, Saeid, Pierre-François Marteau, and Nicolas Béchet. "Intrusion detection in network systems through hybrid supervised and unsupervised mining process-a detailed case study on the ISCX benchmark dataset.", 2017.
[12] Lal, Chunnu and Shrivastava, Akash," An energy preserving detection mechanism for blackhole attack in wireless sensor networks "International Journal of Computer Applications, 2015 – Citeseer.