ISSN 2347 - 3983
Volume 8. No. 8, August 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter82882020.pdf
https://doi.org/10.30534/ijeter/2020/82882020

Meticulous Elephant Herding Optimization based Protocol for Detecting Intrusions in Cognitive Radio Ad Hoc Networks

J.Ramkumar[1], Dr. R.Vadivel[2]
[1]VLB Janakiammal College of Arts and Science, India, jramkumar1986@gmail.com
[2]Bharathiar University, India, vlr_vadivel@yahoo.co.in

ABSTRACT

Currently, Identification and detection of intrusions in ad-hoc network is a demanding and significant task. Numerous methodologies have been proposed for detecting the intrusions. But, still ad-hoc networks face high-level of internal and external security attacks. Limitations in previous Intrusion Detection System (IDS) provide a way for the development of reliable IDS based routing, which is an independent challenge. In this paper, Meticulous Elephant Herding Optimization based Protocol (MEHOP) is proposed to select the feature of a node using Support Vector Machine (SVM), find the route to destination in an optimized manner and finally send the data to the destination. SVM algorithm is applied to classify the nodes from malicious node. MEHOP is a metaheuristic algorithm designed to make updations from the selected individuals. Once when the intrusions are detected and avoided, the performance of the ad-hoc network will improve. This research use NS2.35 to evaluate the performance. Results indicate that there exist an improvement in the network performance after detecting and avoiding the intrusions.

Key words : ad-hoc, classification, , delay, intrusion

1. INTRODUCTION

Information technology is becoming one of the critical elements for providing support in different research areas. The organizations are providing complicated networked facilities and open ways for their (a) customers, (b) business partners, (c) suppliers. Most of the users are legitimate, but there exist more chances of illegitimate user's access. Greater access expands the complexity of the network and significant emphasis on the networks is becoming more dominant. Besides, the breaches in the security of networks have increased in the past years. IDS of the network are becoming more critical in the contemporary years to decrease the unexplored intrusion. Generally, the intrusion in the network can be detected only by evaluating the trial data of the user to investigate the strange behavior of the user.

Data mining algorithms commonly applied to fetch hidden structures and information from the database. Classification widely used in any data-mining task that elevates the data into classes and groups. In general, it is defined as a supervised type of learning where the classes are discovered while exploring the data. To ensure the security of information systems, an effective intrusion detection system is necessary to be built inside the network, which will be a great challenge. The security of the ad-hoc network faces continuous issues because of the dependence of military, government, and commercial bodies for their routine works. All kinds of ad-hoc networks face numerous attacks. An intrusion defined as the progress of illegal access to the resources of the network. Intrusion Detection System (IDS) acts as a tool for detecting the attacks in prior. Few kinds of intrusions can be tracked using the network logs, but many intrusions are not able to track. IDS generally divided into anomaly-based IDS (AbIDS) and signature-based (SbIDS). In SbIDS, the signatures are stored in the pre-defined database, and networks are analyzed deeply with the signatures. AbIDS monitor the traffic by matching the patterns of normal network usage. If the deviation is present in the typical usage pattern, then it indicates the attempt of intrusion in the network. Besides, AbIDS detects new types of attacks but SbIDS will never discover any new kind of attacks.

Innumerable problems of decision-making will range in the common classes of classification. Nowadays, there is an urgent need to develop novel models of classification, especially for neural nets and machine learning. In classification, the features of the objects presented newly should be examined for the set of pre-defined classes. Methods like Radial Basis Function, Multi-Layer Perceptron, Case-Based Reasoning are some of the categories of supervised learning methods used for solving the problems in classification.

Performance of the network cannot be fulfilled only by routing protocol, because several aspects like, congestion, memory, battery life etc affects it. One of the most important aspects this work found is intrusion. When a node intrudes a network, it will attempt to do malicious activities. There exist more chances for an internal node to act maliciously (i.e., like a intruder node). This research focuses to identify and avoid the malicious node for routing purpose in cognitive radio ad-hoc networks.

2. LITERATURE REVIEW

An approach for detecting the anomaly-based technique was implemented [1] for Industrial Control System. Preprocessing technique applied for scaling the data. To reduce the dimension of research, a separate algorithm proposed. The rule-based nearest neighbor algorithm applied to make the dataset get balanced. New attacks detected using the bloom filtering methodology. A sensing system for detecting the intrusion [2] proposed to detect intrusions in the network. It works by generating noise signals and transmitting the detection signal, where it accurately fetches the intrusions with the assistance of the correlation technique. Results show its possible support for a huge-scale network. Minimum Covariance Determinant (MCD) proposed based on multivariate control chart and kernel density estimation. The main intention focuses on detecting the outliers and reduces false alarm rates. NSL-KDD dataset used to measure the performance and the result came with better detection accuracy in decreased time. Probabilistic based Cross-Layer IDS [4] proposed to detect the attacks based on spoofing in electric vehicles. It makes use of a machine-learning algorithm for classification. It makes use of the distance between nodes and speed of communication for detecting the intrusions in the network. Detection of Dissolved Tracer Intrusion model [5] proposed to evaluate the feature variables towards detecting the network traces. Communication between variables and their effects are studied, and analysis was conducted based on Behnken design. The proportion of salinity was also evaluated which was higher in range and the performance improvement was detected.

Machine cum Deep Learning Methodology [6] proposed to detect the intrusion in the wireless networks. It makes use of the clustering technique to detect intrusions. The performance of the classifier evaluated numerically and proved its efficiency against baseline methods. Effective Intrusion Detection [7] developed to reconfigure the routing of the network. It uses a host-based intrusion technique for reconfiguration. It founds that the mobility of the node has more impact on the severity of intrusion. Packet overhead analysis conducted to enhance the accuracy of intrusion detection. Proxy logs based Detection Method [8] proposed to fetch feature vectors and discriminate it among malicious nodes in heavy network traffic. A corpus value was generated when traffic imbalances were found out. Cross-validation cum timeline analysis was done with logs in the proxy. Anomaly-based IDS [9] designed particularly for Bluetooth Mesh Networks. To classify the network traffic and identify the malicious nodes, the machine-learning algorithm was the used Anomaly-based concept used in simulation in BMWatchSim to detect the intrusions in the real world. Hybrid Technique for Dimensionality Reduction [10] proposed for distinguishing the intrusion in modern networks. It combines principal component analysis, information gain concept with the SVM algorithm. The performance evaluation with datasets called NSL-KDD and Kyoto 2006+.

Enhanced Fuzzy Minimum–Maximum Neural Network [11] proposed for improving the intrusion detection rate in minimum time. Network attacks detection performed with Rule-Based, Neuro-Fuzzy based, and SVM based classifiers through the standard datasets. Topology Verification based IDS [12] proposed as a security model and it safeguards the network using the triggering concept. The triggering event created multiple warning messages, which reduced the overall performance of the network. Even though some of the significant intrusions are detected, it affected the performance. Improved Convolutional Neural Network-based IDS [13] proposed to extract the features in an optimized manner to detect the intrusions. KDD Test + dataset used for evaluating the performance against the baseline methods. It increased the packet delay in the network but the classification accuracy of intrusions was improved. Trust-based Mechanism for Node [14] proposed to detect the malicious node based on the responses received for the request. This work focuses mainly on Passive Message Fingerprint Attacks (PMFA) because it was found to be vulnerable while sending information to another node. Statistics based AutoEncoder with the intelligent system [15] proposed for detecting the intrusion. Data analytics and statistical methods grouped with new machine learning-based theory for optimization. NSL-KDD datasets used for the performance evaluation and results have better improvement than the baseline methods. Several Security Algorithms [18], [19], [20] were also proposed to overcome the attacks in modern networks. Bio-Inspired Optimization Based Routing Protocols [21], [22], [23] are proposed for finding the best route in the network, but didn't focus on security issues.

3. METHOD

3.1 Adaptive Support Vector Machine

Support Vector Machine (SVM) is one among the most commonly used binary classification methods. SVM is applied for practical multi-classification issues, with well-known one-against-one (OAO) and one-against-all (OAA) approaches. The OAA system produces o templates, in which o means the class count. Each model distinguishes a class from other classes. On the opposite, the OAO method builds structures for all class pairs. For training the SVM with the OAO method, this research work makes utilization of LibSVM [16]. By voting, the final class decisions are made, i.e., new instances are graded by utilizing $(n(n-1)/2)$ classifications.

SVM classification is done through distinguishing the instances by hyperplane from various classes. A hyperplane needs to be as far as feasible towards cases of both types of classes. The optimum hyperplane is described as below:

$$1 \leq z_i(x.y_i + c) \quad for\ o \geq j \geq 1\ x \in S^e, c \in S \qquad (1)$$

where y_i indicates the instances, corresponding labels are represented by $z_i \in \{-1,1\}$, intercept term is denoted by c, x represents the hyperplane's normal vector, e shows the count

of individual instance's attribute and input vector dimension, count of instances is denoted by o. In addition, a hyperplane is described using instances closest to it. Such instances referred to as vectors of support.

The earlier SVM model necessarily requires every instance of the similar class to fall on hyperplane's right-side, and outside the margin space between the supporting vectors. Such features are generally not present in real-time issues. Beyond human errors, real data include outliers when entering data and computing the errors of instances dramatically vary from other instances of matching class. The SVM (often referred to as the hard margin) concept is not suitable for such problems. A soft description of the margin introduced to beat this issue and formulate SVM available for classifying the data in real-time data classification. Eq.(1) has been relaxed and the ideal hyperplane is newly defined as:

$$(1 - e_i) \leq z_i(x.y_i + c), \quad e_i \geq 0, \quad n \geq i \geq 1 \qquad (2)$$

where slack variables are indicated by e_i that make margin fall off for the instances. To find the ideal hyperplane, the following quadric programming problem needs to be solved more precisely:

$$\text{ideal hyperplane} = \min\left(D\sum_{i=1}^{m} e_i + \frac{1}{2}\|x\|^2\right) \qquad (3)$$

where D is the soft margin function parameter. With that parameter, the efficiency of SVM depends heavily on the decision. Larger D values correspond to a similar model to that achieved from the concept of a hard margin.

Adopting a soft margin methodology solves the first issue. The second issue gets initiate when sequentially separable data is used for soft margin solutions. Unfortunately, it will not be suitable for multiple real-time problems. The solution for the second issue is to avoid using the dot product and use kernel function. The main advantage of using kernel function is, it maps the instances into wider spaces where they are sequentially separable. Several kernel functions widely used are Sigmoid, Radial Basis Function (RBF), and Polynomial. It is necessary to remember that if the kernel function is essential, and then RBF is usually the first option.

$$K(y_i, y_j) = \exp\left(-r\|y_i - y_j\|^2\right) \qquad (4)$$

where r indicates the classification accuracy parameter which has significant consequences and it determines every training instance's effect. Low r values represent that the impact is high. The scope is very similar for r which have high values. The accuracy of classification depends hugely on the parameters C and r described above. The pair of values $(C; r)$ should be calculated for every research issue. Grid quest is one of the most simple yet very costly methods of tuning parameters. For the tuning of SVM parameters, nature-inspired algorithms have been proposed in recent years, particularly swarm intelligence based algorithms. In this article, we suggest optimization for the SVM algorithm based on elephant herding and it will be used for enhancing the classification accuracy.

3.2 Meticulous Elephant Herding Optimization

Fundamental steps involved in Elephant Herding Optimization are simplified in the following:

- Matriarch leads the elephants that are belong to various clans but living jointly. There exist a threshold value for elephants count in clan. For modeling purpose this research work makes an assumption that clan holds specific cum stable number of elephants.
- The current positions of elephants in the clan are made to update by depending on relationship with matriarch. EHO models this behavior via a updating operator.
- Sophisticated male elephants will leave their clan and live separately. It is assumed that at every generation threshold value of elephants will leave their own clans. Updating Process in EHO is carried out via a separating operator.
- Commonly, matured elephant is termed as matriarch in the clan. Matriarch is treated as the best elephant having highest fitness value to solve the optimization issues
- Meticulous Elephant Herding Optimization ($MEHO$) is one of the latest swarm intelligence-based algorithm. Since it's a modern optimization algorithm, it is being applied for many applications. EHO algorithm is mainly applied for detecting the intrusion in highly complex ad-hoc social networks.

Elephants herding activity was used for developing $MEHO$. In order to construct a swarm intelligence algorithm, natural complicated behaviour of elephants were simplified. The entire population of elephants is split into a variety of clans. In one clan, the elephants reside under a matriarch's leadership. Specific counts of sophisticated elephants abandon their own clan and live far away.

EHO is defined formally as follows. The first move is to break the population of elephants into j clans. Any elephant (i.e., member) of the clan d_i moves towards the best fitness value based on clan matriarch. The following equation indicated in [5] applies to each member movement:

$$y_{new,d_{i,j}} = y_{c_{i,j}} + a \cdot \left(y_{best,d_i} - y_{d_{i,j}}\right) \cdot r \qquad (5)$$

where $y_{new,d_{i,j}}$ indicates the recent location of elephant j in clan d_i, $y_{d_{i,j}}$ indicates previous position of elephant j, y_{best,d_i} represents the best-fit colution of clan d_i, matriarch influence is indicated using $a \subset [0,1]$ parameter, $r \subset [0,1]$ is a arbitrary number utilized to enhance population range in subsequent algorithm stages.

Location of clan matriarch d_i, y_{best,d_i} is computed using Eq.(6)

$$y_{best,d_i} = B.y_{center,d_i} \qquad (6)$$

where $B \subset [0,1]$ represents the algorithm's second parameter which monitor the control of $B.y_{center,d_i}$ and it is described as Eq.(7)

$$y_{center,d_i,e} = \frac{1}{n_{d_i}} \sum_{l=1}^{n_{d_i}} y_{d_i l,e} \quad (7)$$

where $E \leq e \leq 1$ is the e^{th} dimension, and E indicates search space overall dimension, n_{d_i} indicates the count of clan d_i elephants. The research is focused on sophisticated elephants that stay apart from the clan. Stable number of members (i.e., elephants) having worst value with fitness function are progressed (i.e., moved) to new location. Such members' position shall be described as:

$$y_{worst,d_i} = y_{min} + (1 - y_{min} + y_{max}) \cdot rand \quad (8)$$

where y_{max} and y_{min} indicates search spaces upper limit and lower limit, , the parameter $rand \subset [0,1]$ indicates a number arbitrarily selected via uniform distribution.

This research work has updated the SVM parameter optimization through EHO algorithm. In 2-dimensional space, elephant locations are identified using C and r. For SVMtuning the parameter, logarithmic search space has been identified as a appropriate method. The exponent search range for C was set as [-15, 25] and SVM was optimized for 2^y, where y is attained by EHO algorithm's C. The range of search for r was set to [10;1].

3.3 Node Selection for Routing

A model of energy dissipation was considered here for proper selection of routing nodes. When a node failure happens in ad-hoc networks it may be due to an attack or because the node's energy ends because it is drained from resources. When such a scenario occurs, unavoidable search for an alternative or back-up route gets start for transmitting the data to avoid the loss of packet. In this research, Node distances are determined are calculated using the function of distance vector. The average distance (D_{bs}) that exists between source node and destination node is calculated using

$$D_{bs} = \frac{Estimated\ Distance}{\sqrt{2\pi}} \quad (9)$$

$$D_{bs} = \frac{0.765 \times Estimated\ Distance}{2} \quad (10)$$

Distance between active node and failed node is calculated using distance vector calculation. The node is analyzed for its energy level and if it falls in the range of threshold value then it is selected for future routing purpose.

$$Threshold\ Distance = \sqrt{\frac{E_{fs}}{E_{mp}}} \quad (11)$$

where E_{fs} indicates the consumption of energy needed for transmitting the data in shorter distance, and E_{mp} represents the actual energy transmission used for transmission.

If a node is selected for future routing purpose gets failed for various reasons, then it immediately start looking for some other nodes to act as backup node using the function of distance vector. If the energy level is greater than the threshold value, then that node is selected for data transmission.

Nodes having higher level energy than the threshold values are called as persuasive node. These kinds of nodes are averagely used for sending the data and the reason is most nodes make use of persuasive node and chances exist for failure during transmission.

4. SIMULATION SETTING

The current section makes a discussion about evaluating the MEHOP using NS2 simulations. In general, there exists no trusted simulator for evaluating protocols for CRAHN. Furthermore, the details that are available regarding the protocol implementation or simulation for CRAHN are unclear to understand, especially the performance of protocols. This paper attempts to compare BISRP against WPIP [16] and GRP [17]. This research work prefers the C++ language to use in the NS2 simulator. Table 1 shows the simulation setting used for evaluating the proposed protocol.

Table 1: Simulation Settings and parameters

Parameters of Simulation	Values
Simulation Area Size	$2500 \times 2500\ m^2$
Simulator Name	*Network Simulator*
Simulation Version	2.35
Count of nodes	$10\ to\ 100\ varying\ with\ 10$
Mobility Model	*Randomway Point*
Speed of Mobility	$4\ m/s\ to\ 40\ m/s$
Type of Traffic	*Constant Bit Rate*
Type of Channel	*Wireless*
MAC	802.16
Transmission Range	$500\ m$
Initial Energy	$15\ Joules$
Size of Packet	$0.512\ kb$

5. PERFORMANCE METRICS

This research works make use of below mentioned metric for analyzing the performance of proposed protocol MEHOP against WPIP [16] and GRP [17].

- **Throughput:** Measure of the overall quantity of data transmitted (or processed) from source to destination in a threshold time
- **Packet Delivery Ratio:** Measure of packets successfully received in destination against total packets sent by the source

- **Packet Drop:** Percentage of packets that not yet reached the destination due to different reasons like route failure, node failure, expiry of the packet, etc
- **Delay:** Consumed time by the protocol to deliver the packet to the destination
- **Energy Consumption:** Energy consumed to deliver the packet to the destination from the source.

6. RESULTS AND DISCUSSION

6.1 Throughput Analysis

Figure 1 portrays the result of simulation obtained for the throughput metric. Two routing protocols namely WPIP and GRP illustrate average and below average performance while the nodes are increased. WPIP and GRP lack when nodes in the network move fastly or face security attacks. MEHOP based protocol discovers more routes in a short duration even the route gets failed or faces security attacks. MEHOP makes an effective classification on node and optimizes the newly discovered route towards destination. MEHOP based protocol adapts the scalability to give its best performance.

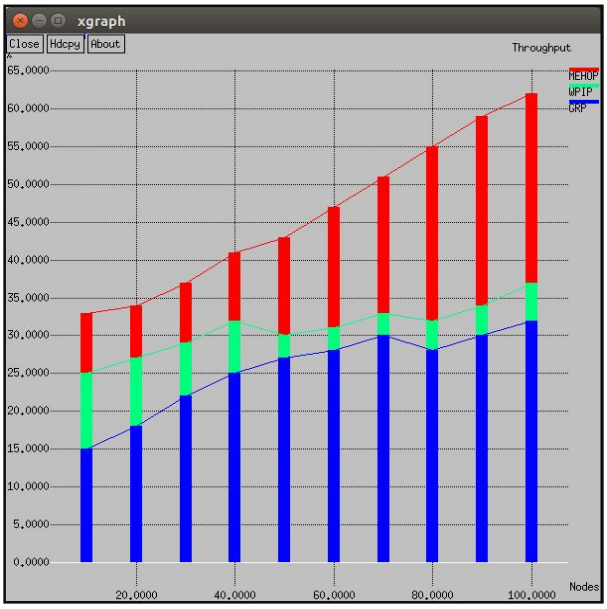

Figure 1: Throughput vs. Nodes

6.2 Packet Delivery Ratio Analysis

Figure 2 portrays the results of simulation obtained for the throughput metric. It is clear that MEHOP has better performance in delivery the packet to destination even it faces the security attacks. With the classification concept MEHOP classifies the node, optimizes the node and discovers the new route in a reduced time period. This makes efficient delivery of packet more than WPIP and GRP. Due to unaware of intrusions and attacks, WPIP and GRP deliver low number of packet.

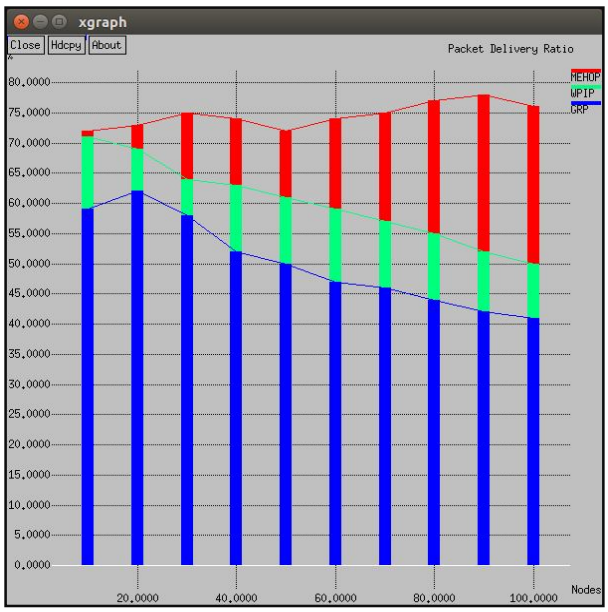

Figure 2: Packet Delivery Ratio vs. Nodes

6.3 Packet Drop Analysis

Figure 3 demonstrates the results of simulation obtained for packet drop metric. Delay faced by the proposed protocol is minimum than WPIP and GRP. MEHOP avoids sending the broadcast message continuously; instead it collects information of nodes for classifying and optimizing, which makes sure the packet reach the destination safely. When the count of node gets increased, WPIP and GRP act erratically. This erratic behavior affects the transmission of packet during congestion and increases packet drop.

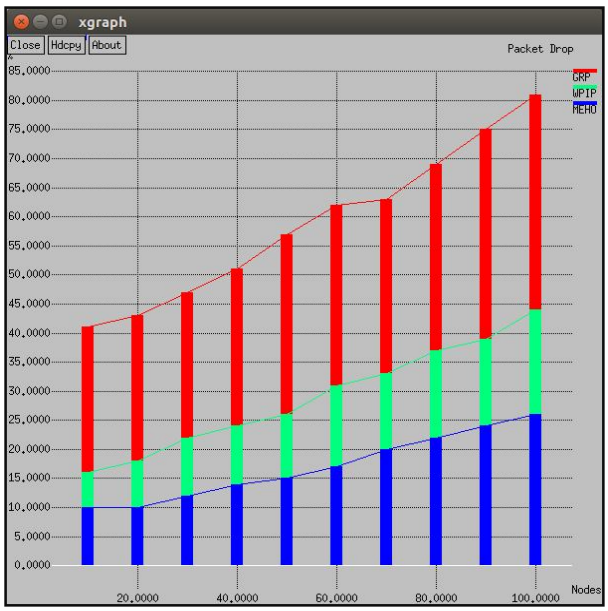

Figure 3: Packet Drop vs. Nodes

6.4 Delay Analysis

Figure 4 evident the results of simulation obtained for the delay metric. It indicates that an increase in node count will

increase the delay. Processing more number of broadcasting messages delay gets enhanced. When analyzing the protocols for the delay, it was found that MEHOP is also facing delay when node count increases gradually. While analyzing WPIP and GRP protocols, it is clear to understand that the presence of delay keeps get increased when node count increases. The main reason for that is WPIP and GRP chooses the node that low energy for forwarding the packet that results in route failure.

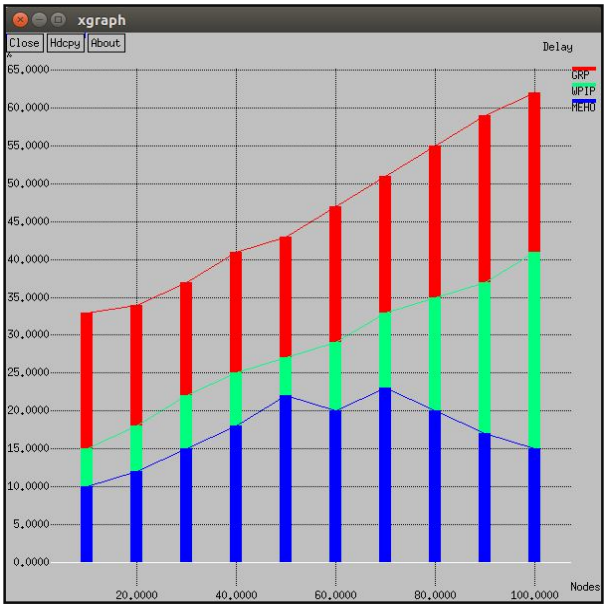

Figure 4: Delay vs. Nodes

6.5 Energy Consumption Analysis

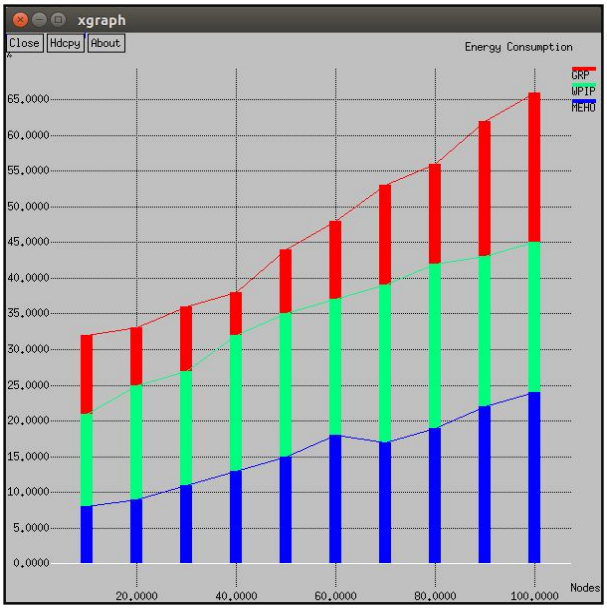

Figure 5: Energy Consumption vs. Nodes

Figure 5 illustrates the results of simulation obtained for energy consumption metric. It is found that MEHOP has consumed less energy than WPIP and GRP. Generally, nodes consume more energy when it does more work unlimitedly crossing the threshold time. In MEHOP, nodes process data transmission only after sending its energy level. MEHOP works in 2 stages, in the first stage it collects information about the node for classification and optimization, and in the second stage it send the data. MEHOP prioritize the nodes in stage 1 for future purpose, and it makes the less spending of energy for transmitting the data.

7. CONCLUSION

In the domain of optimization-based research, the minimum number of metaheuristic algorithms only makes use of preceding information to control the upcoming process. In this research paper, meticulous elephant herding optimization, preceding information regarding the population is obtained to utilize it for the succeeding process of searching. This research work selects 2 or 3 individual elephants from the preceding iterations, and it will be processed either randomly or fixedly. Results of the iterations are incorporated to the EHO for future use. In this manner, intrusions are identified and separated from the network. The simulation results demonstrate that the proposed MEHOP has outperformed significantly than other protocols towards improving network performance. The follow-up work focuses on using fuzzy logic to increase intrusion detection and improve network performance even more.

REFERENCES

[1] I. A. Khan, D. Pi, Z. U. Khan, Y. Hussain and A. Nawaz, **HML-IDS: A Hybrid-Multilevel Anomaly Prediction Approach for Intrusion Detection in SCADA Systems**, *IEEE Access*, vol. 7, pp. 89507-89521, 2019. https://doi.org/10.1109/ACCESS.2019.2925838

[2] H. Xu, R. Xie, H. Han, Z. Zhang, J. Zhang, L. Liu, B. **Wang and L. Li A LCX-Based Intrusion-Detection Sensor Using a Broadband Noise Signal**, *IEEE Access*, vol. 7, pp. 161928-161936, 2019. https://doi.org/10.1109/ACCESS.2019.2951576

[3] M. Ahsan, M. Mashuri, M. Lee, H. Kuswanto and D. Prastyo, **Robust adaptive multivariate Hotelling's T2 control chart based on kernel density estimation for intrusion detection system**, *Expert Systems with Applications*, vol. 145, p. 113105, 2020. https://doi.org/10.1016/j.eswa.2019.113105

[4] D. Kosmanos, A. Pappas, L. Maglaras, S. Moschoyiannis, F. J. Aparicio-Navarro, A. Argyriou and H. Janicke, **A novel Intrusion Detection System against spoofing attacks in connected Electric Vehicles**, *Array*, vol. 5, p. 100013, 2020. https://doi.org/10.1016/j.array.2019.100013

[5] P. Jacob, T. Zhang, S. Laborie and C. Cabassud, **Influence of operating conditions on wetting and wettability in membrane distillation using Detection of Dissolved Tracer Intrusion (DDTI)**,

Desalination, vol. 468, p. 114086, 2019. https://doi.org/10.1016/j.desal.2019.114086

[6] S. Otoum, B. Kantarci and H. T. Mouftah, **On the Feasibility of Deep Learning in Sensor Network Intrusion Detection**, *IEEE Networking Letters*, vol. 1, no. 2, pp. 68-71, June 2019. https://doi.org/10.1109/LNET.2019.2901792

[7] J. Zuniga-Mejia, R. Villalpando-Hernandez, C. Vargas-Rosales and A. Spanias, **A Linear Systems Perspective on Intrusion Detection for Routing in Reconfigurable Wireless Networks**, *IEEE Access*, vol. 7, pp. 60486-60500, 2019. https://doi.org/10.1109/ACCESS.2019.2915936.

[8] M. Mimura, **Adjusting lexical features of actual proxy logs for intrusion detection**, *Journal of Information Security and Applications*, vol. 50, p. 102408, 2020. https://doi.org/10.1016/j.jisa.2019.102408

[9] M. Krzysztoń and M. Marks, **Simulation of watchdog placement for cooperative anomaly detection in Bluetooth Mesh Intrusion Detection System**, *Simulation Modelling Practice and Theory*, vol. 101, p. 102041, 2020. https://doi.org/10.1016/j.simpat.2019.102041

[10] F. Salo, A. Nassif and A. Essex, **Dimensionality reduction with IG-PCA and ensemble classifier for network intrusion detection**, *Computer Networks*, vol. 148, pp. 164-175, 2019. https://doi.org/10.1016/j.comnet.2018.11.010

[11] N. Upasani and H. Om, **A modified neuro-fuzzy classifier and its parallel implementation on modern GPUs for real time intrusion detection**, *Applied Soft Computing*, vol. 82, p. 105595, 2019. https://doi.org/10.1016/j.asoc.2019.105595

[12] T. Yu and X. Wang, **Topology Verification Enabled Intrusion Detection for In-Vehicle CAN-FD Networks**, *IEEE Communications Letters*, vol. 24, no. 1, pp. 227-230, 2020. https://doi.org/10.1109/LCOMM.2019.2953722

[13] H. Yang and F. Wang, **Wireless Network Intrusion Detection Based on Improved Convolutional Neural Network**, *IEEE Access*, vol. 7, pp. 64366-64374, 2019. https://doi.org/10.1109/ACCESS.2019.2917299

[14] W. Li and L. Kwok, **Challenge-based collaborative intrusion detection networks under passive message fingerprint attack: A further analysis**, *Journal of Information Security and Applications*, vol. 47, pp. 1-7, 2019. https://doi.org/10.1016/j.jisa.2019.03.019

[15] C. Ieracitano, A. Adeel, F. Morabito and A. Hussain, **A novel statistical analysis and autoencoder driven intelligent intrusion detection approach**, *Neurocomputing*, vol. 387, pp. 51-62, 2020. https://doi.org/10.1016/j.neucom.2019.11.016

[16] J. Ramkumar, R. Vadivel, **Performance modeling of bio-inspired routing protocols in Cognitive Radio Ad Hoc Network to reduce end-to-end delay**, *International Journal of Intelligent Engineering and Systems*, vol. 12, pp. 221–231, 2019. https://doi.org/10.22266/IJIES2019.0228.22

[17] X. Jin, R. Zhang, J. Sun and Y. Zhang, **TIGHT: A Geographic Routing Protocol for Cognitive Radio Mobile Ad Hoc Networks**, *IEEE Transactions on Wireless Communications*, vol. 13, no. 8, pp. 4670-4681, 2014.https://doi.org/10.1109/TWC.2014.2320950

[18] H. Mohapatra, S. Rath, S. Panda and R. Kumar, **Handling of Man-In-The-Middle Attack in WSN Through Intrusion Detection System**, *International Journal of Emerging Trends in Engineering Research*, vol. 8, no. 5, pp. 1503-1510, 2020. https://doi.org/10.30534/ijeter/2020/0585202

[19] S. Ajiniyazovna, T. Sabirovna, Q. Erkinovna and E. Dilshod Ugli, **Implementation of E-Commerce Security Methods and Tools**, *International Journal of Emerging Trends in Engineering Research*, vol. 8, no. 5, pp. 1545-1551, 2020. https://doi.org/10.30534/ijeter/2020/12852020

[20] I. Jeena Jacob, N. Dayanand Lal, S. Parikshith Nayaka, B. Pillai and N. Kouser, **Ensuring Network Security using Secured Privileged Accounts**, *International Journal of Emerging Trends in Engineering Research*, vol. 8, no. 5, pp. 1959-1963, 2020. https://doi.org/10.30534/ijeter/2020/80852020

[21] J.Ramkumar and R.Vadivel, **Improved frog leap inspired protocol (IFLIP) – for routing in cognitive radio ad hoc networks (CRAHN)**, *World Journal of Engineering*, vol. 15, no. 2, pp. 306-311, 2018. https://doi.org/10.1108/WJE-08-2017-0260

[22] J.Ramkumar and R.Vadivel, **CSIP—Cuckoo Search Inspired Protocol for Routing in Cognitive Radio Ad Hoc Networks**, *Advances in Intelligent Systems and Computing*, Vol. 556, pp. 145-153, 2017. https://doi.org/10.1007/978-981-10-3874-7_14

[23] J.Ramkumar and R.Vadivel, **Intelligent Fish Swarm Inspired Protocol (IFSIP) For Dynamic Ideal Routing in Cognitive Radio Ad-Hoc Networks**, *International Journal of Computing and Digital Systems*, Vol. 10, pp. 2-11. 2020. https://journal.uob.edu.bh:443/handle/123456789/3961