Impact Of Ant Colony Optimization On The Performance Of Network Based Intrusion Detection Systems: A Review

Ghanshyam Prasad Dubey, Dr. Rakesh Kumar Bhujade

Abstract: As far as current scenario is concerned Internet, computer, electronic gadgets and networking are essential. These are mostly prone to security threads like viruses, Trojan horses and other malware attacks. To check authentication, provide efficient techniques for encryption and decryption, and develop security mechanism intrusion detection system is used. IDS gather information and analyze the unusual activities to find loop holes in security from network traffic in a system. Primary task to identify the elements those are responsible to violate the system security. In this study, impact of Ant Colony Optimization for suitable decision in network based IDS are discussed.

Index Terms: NIDS, ACO, Misuse Detection, Anomaly Detection, True Positive, False Positive.

1. INTRODUCTION

A system that is used to monitor traffic of network for malicious activities and takes action accordingly like, alarm or alert generation and prevent such actions. Systems like these are comes under Intrusion Detection System (IDS). Most of IDS systems are unable to predict new attack patterns, some of them are generate false alarm, some of them unable to detect actual malicious activity [1]. IDS can be defined as either a tools or a solution or a resources applied to identify or assess or sometimes claim unconstitutional or unapproved activities or actions in a network.Protecting networks from numerous computer and social security attacks are vital apprehension of computer security. IDS used to detect programs or activities that tried to compromise the confidentiality, integrity and most importantly availability of a resource in the network. It is a kind of security mechanisms that analyze the working of system and help to detect unpleasant activity in terms of security breach, computational power theft, loss of data etc. With the enhancement of the network and internet various security issues also rises. Network security is a common problem now a day due to attacks and hacking. New attack patterns are discovered day by day [2]. Due to this improvement in existing system is equally important. Intrusion detection system or IDS is a supporting mechanism or system for network security. It can monitor and detect unauthorized network usages or uncharacteristic conditions without distressing host or network performance.

Within this article; the role of ACO i.e. ant colony optimization and its performance in network based intrusion detection system is presented. Remaining of paper is organizing as; in section 2 classification of intrusion detection system, in section 3 ant colony optimization, section 4 as literature review, section 5 present proposed algorithms and section 6 expected outcomes.

- *Ghanshyam Prasad Dubey is currently pursuing PhD degree program in computer science and engineering in Mandsaur University, India, PH-982755366. E-mail:ghanshyam_dubey2@yahoo.com*
- *Dr. Rakesh Kumar Bhujade is currently working as Associate Professor in computer science and engineering in Mandsaur University, India, PH-9229853636. E-mail: rakesh.bhujade@gmail.com*

2. Classification of IDS

As far as traditional detection methods of intrusion detection system are concern, there are two types of approach were used first is misuse (signature) detection and second one is Anomaly detection [3]. In misuse or signature detection scheme, detection is based on characteristic of existing attacks. It means suspicious activity can be detected if it is known or happened earlier [4]. If systems are aware about the malicious activity or suspicious activities, it can recognize the attack and generate alarm. This scheme is failed to detect new attack patterns [5]. In Anomaly detection, System observes the behaviour of network traffic and node. The behaviour of each node is recorded and if deviation of behaviour is observed then it generate alarm and block the activity of this node. If a part of network is miss behave then also alarm is generated and recommended actions can be taken [1] [6].

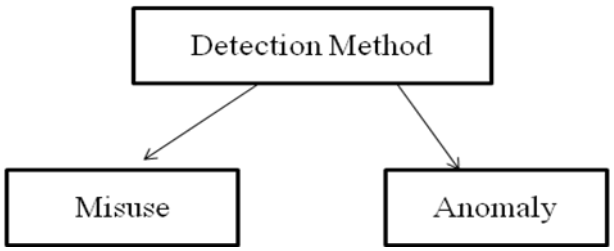

Fig. 1. *Detection methods used in IDS.*

According to location or place (where it can apply) IDSs are divided into two categories namely host-based intrusion detection system abbreviated as HIDS and network-based intrusion detection system shortly known as NIDS [7] [8]. An HIDS installed on particular host and monitor the behaviour of that particular node. An NIDS resides on single system (server or gateway) that lookout network traffic and behaviour of network, monitoring for signs of attacks. As far as recent trends are concerned, intrusion detection combines benefits both HIDS and NIDS to form a efficient and better system called hybrid systems for better results. Such hybrid systems are developed to gain benefits of both. There client versions are used to monitor host behaviour and send report to network manager and manager compare the activity whether it is malicious or not. It takes action after diagnose an attack or deviation in behaviour.

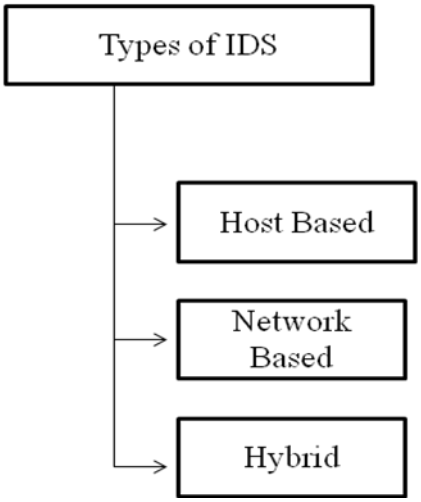

Fig. 2. *Classification of IDS.*

Traditionally, HIDS systems examined log entries for specific information. A new form of H-IDS has examines calls to the operating system kernel; it is programmed with known attack signatures and will alarm after matching the signatures. HIDS are capable of checking files on the system for modification. The HIDS will not miss attack traffic until the attack generates a log message and it can determine if an attack was successful by examining log messages or other indications. The HIIDS can be used to identify unauthorized access attempts by legitimate system users [9].Network intrusion detection systems are based on known pattern or signature and listen on a network interface looking for suspicious traffic. This traffic is investigated according to a set of rules and attack signatures to determine if it is traffic of interest. Some NIDS are anomaly based that look out the suspicious events. In this type of detection false positive rate is usually higher, but the benefit is predictability of new attack style [10]. Such systems can be worked like statistical-based to discover the behaviour, knowledge-based to obtain information, and machine learning-based to learn the new facts or knowledge. In statistical approach system behaviour is represented in some viewpoints to analyze actual and malicious performance. Knowledge based tries to compare event with existing information and decide event is normal or suspicious. Machine learning based NIDS are worked as both statistical and knowledge based, it is not only detect suspicious event but predict possible new attack pattern also [11].

3. Ant Colony Optimization

It is based on intelligence and behaviour of ants, the way or pattern they can search for food and discover minimum distance between food source and ant colony. The same behaviour is used to solve the complex problems through artificial ants. There are many researchers used ACO for various purposes like, it is used for feature selection in network data [1], it helps to construct decision classifier in training module [12], [13], [14] [15] pattern recognition and anomaly detection [16], attack detection [17], decision tree formation [18], and to classify attack data [19]. The technique of ACO is known for slow convergence speed, strong discoverability and fine problem solving ability, strong robustness, simple realizing on computer system with inadequacy of longer searching time and easy stagnation [20]. To enhanced the effectiveness of Ant Colony Optimization (ACO) many researchers put their efforts; few of them are, in year 2006 Leng, Wei & Zhang (2006) [21] try to improved ACO algorithm by updating dynamic pheromone concept and using initial value of pheromone directional diagram was created with weights in scheduling of manufacturing process. This manufacturing process is flexible and considering for the instrument constraint, estimate manufacturing cost and total required processing time. Later on in year 2011 Song and Zhao (2011) [22] developed max-min adaptive ACO that is applied to build inter-cluster based on energy-aware routing involving base station (BS) and cluster heads. This method tries to balances the energy consumption of cluster heads and improves the solution of hot spots problem. This problem occurs in multi-hop or multi-point Wireless Sensor Network routing protocol to maximum. In year 2012 Ugur and Aydin improved ACO in terms of pheromone trails [23], Xu, Qian & Zhang (2012) used chaotic map to enhance the ACO algorithm and many more researchers in similar directions [24].

4 Literature Review

Recently in year 2018 Helmi Md Rais and Tahir Mehmood [1] applied ACO technique to classify feature selection of the network data. It has proved itself a optimum solution. It is capable to search feature space until meeting a best possible solution. In very first iteration traditional ACO is applied to generate pheromone and after that in later iteration every ant designed to find best possible local solution and then among of this set of local solution, global optimal solution is generated. Then optimal feature set was legalizing by another technique called Support Vector Machine. For the classification of normal behaviour and intrusive behaviour in the network support vector machine was used.Generated N ants are free to travel their own path, subset of ants are formed based on their similar path called subset. . In this way optimal features set is discovered based on that intrusion detection is done with high performance. Each ant has a chance to select a single node based on pheromone amount and heuristic value. Heuristic value is responsible for the path discovery in upcoming perception although value of pheromone is conceptualized as essential memory in precedent view of the path. Features correlation values applied to classes that take a part to improve probability function for considering benefits of feature prediction about feature classes. The amount of local pheromone is applied to formulate traversed edges those are less enviable and accordingly enhance chance to investigate the edges those are not visited. Intermediate level pheromone values updated for reinforce. Intermediate pheromone updated on the basis of existing information by each ant's group. Each subset was examined by naive bayes classifier, applied to Recalling that feature subset. This pheromone used to selected feature set that produced high accuracy for Support Vector Machine or SVM. As far as performance of the work is concerned, proposed scheme better is select less classifier and higher accuracy tested on KDD-99 data set [25]. Selected binary feature set used by DACS3-FS algorithm given accuracy of 98.7087% as a result, while full feature set resulted accuracy was 98.5172%.Mehdi Hosseinzadeh Aghdam, and Peyman Kabiri (2016) discovered a approach for ACO based feature selection. The performance of ACO based classifier and the

lengths of subset of selected features are espoused as heuristic information for Ant Colony Optimization technique. The ants are directed to the construct new and better solution. This feature selection (FS) process selects suitable features that are more appropriate than others available schemes. This leads profit of usually enhancing the performance of system via removing extraneous and superfluous features. The process primarily generates multiple ants randomly placed on the graph; it means every ant pick one random feature and starts with it. Instead, several ants were represented on the graph with equal amount of features in the dataset; every ant proceeds to construct path using different feature. If this process generates an optimal subset or the algorithm was iterated certain number of times without generating an optimal solution, then process was terminated and outputs preeminent feature subset encountered. If no suitable results were occurred and then value of pheromone was updated in record and a new set of ants are created and the process repeats for better result. This method minimizes numerous features by around 88% and the rate of error detection minimizes by 24% approx with the help of KDD Cup 99 test data set [12].Anezi, Mafaz Mohsin Khalil et al (2013) applied ACO to data mining classification problem for combinatorial optimization tasks. The Antminer scheme applied to addendum creation of classification rules. On the basis of these classification rules optimal solution is searched by the set of ants. An ant pick empty rule to start and adds term one by one at a time to the rule antecedent. Ant remains adding term to partial rule till at least one term added to the antecedent that would make the rule complete lesser than a threshold predefined by user. After finishing rule construction, first rule that was constructed by the ant is shortened to eliminate inappropriate terms from the rule antecedent. After that, consequent rule is elected to class value that is most recurrent among the training set examples covered by the rule. Lastly, pheromone trails are updated by values and one more ant starts to create a new rule. This procedure is repeated up to numerous time set by user until rules has been reached; otherwise the current ant has constructed exactly the same as rules which works as a rule convergence test [13].Qinglei Zhang and Wenying Feng (2009) presented a framework that targeted to merge the two schemes first one is Clustering based on Self-Organized Ant Colony Network [26] and second is Support Vector Machine [27] for detection of intrusion to attain a superior system performance. Support Vector Machine abbreviated as SVM applied to produce support vector and create a hyper plane to separate both normal and abnormal data at the same time as CSOACN is applied to locate data included to vigorous Support Vector Machine training and thus finally produce models for normal and abnormal data. The support vectors with selected data points will be picked and discernible for the next ant clustering phase after first phase, In Ant clustering phase; the clustering process is classified into numerous clustering periods by means of clustering approximately assured objects with respect to time. In constructing classifier; intrusion detection may be formed by the result generated in SVM training phase. These classifiers further modified gradually by repeating the three steps: first Support Vector Machine training phase, second ant clustering phase and finally constructing the classifier. Two final classifiers are produced after the entire training process is completed. In order to categorize a new data item, there are three methods used: 1) for single SVM classifier; 2) for CSOACN classifier; and 3) for constructing a amalgamation detection classifier based on both classifiers discovered by CSVAC [15].Ravi Kiran Verma, Kumari & Kumar (2016) proposed fuzzy-entropy and ACO for real time IDS feature selection capable to detect most common types of intrusion attacks like DoS, DDoS, probing and account hijacking. IN network traffic 21 attributes were identified, trained and tested. As per result; this scheme is much useful for better results [14]. Gilberto Fernandes Jr et al (2016) presented two different approaches for profile-based anomaly detection (traffic characterization and detection with notification). Both are compared concerning the traffic classification, anomaly detection accurateness of results and respective complexities. In first step they characterized traffic using PCADS statistical technique and the ACODS meta-heuristic. The Principal Component Analysis abbreviated as PCA for Digital Signature (PCADS) [16] is based on PCA to produce a DSNSF for traffic characterization of a network. It is a statistical method applied to diminish the dimensionality of a multivariate hitch by examining the each and every variable among all available input dimensions. To compute the overall efficiency of suggested detection system used the Receiver Operating Characteristics (ROC) graph and the accurateness measure. As far as result is concerned PCADS performed better than ACODS, with compact false-positive rates, reaching a trade-off value of 92% True Positive Rate and 21% False Positive Rate, as ACODS reaches 92% True Positive Rate (TPR) with 24% False Positive Rate (FPR) [16].Ajinkya Wankhade and K. Chandrasekaran (2017) proposed to apply combination of Support Vector Machine (SVM) a very popular machine learning algorithm and Ant Colony Optimization for the detection attack distributed in nature and synchronized with a centralized architecture model. This scheme worked on host and network logs with the help of communication manager. Communication manager equipped with expert system and user interface. Firstly SVM builds and trains the classifiers via small set of data points then these classifiers are adapted by gradually adding new data points for same SVM training. The resulting classifier after such training iteration applied to categorize the original complete dataset. If the classification rate crosses a certain threshold value this will be the stopping condition for this training process. The ACO based intrusion detection classifies these objects into different classes. These classes include normal and different types of intrusions [28].Frans Hendrik Botes, Leenen & De La Harpe (2017) proposed Ant Colony inspired decision trees for Detection of intrusion. In this scheme they combine concept of machine learning and ant tree miner (ATM) for decision tree formation and effective intrusion detection. The benefit of machine learning in intrusion detection is an ability to detect existing attacks as well as predicts future attack patterns. Decision tree are tree like graph that consist of internal nodes that represents test of attribute, branch that denote the test outcome, and leaf node that outline the label. As per the results; their ATM was able to classify attacks with accuracy of 65% with FAR rate of 0% [18].

5. PROPOSED ALGORITHM

The proposed algorithm is shown below:
Step 1: Initialize the KDD-99 data set
Step 2: Reduce the data set (Feature Extraction) using the concepts of Information Gain and Correlation
Step 3: Initialize the Network and IDS
Step 4: Initialize Ants

Step 5: Ants will extract the features of the Running Nodes and provide these features to the Neural Network.
Step 6: Based on the values of the features provided by Ants, Neural Network will decide whether the Node is NORMAL or MALICIOUS.
Step 7: IF Node is NORMAL then IDS will continue its operation (Monitoring)
ELSE IDS will apply the MALICIOUS Node handling mechanism to isolate the Malicious Node from the Network so that it can't damage the network services or other nodes further.
Step 8: Generate the Final Results after completion of the process.
Step 9: Update result to data base for future reference.
Step 10: END.

6. Expected Results

A strong and efficient Intrusion Detection System is designed with the capability of high TRUE Detection Rate (True Positive) and low FALSE Alarming Rate (False Negative). By proposed approach, author wants to improve the performance of the IDS to a certain extent. With the help of this proposed algorithm, author expecting Minimize processing time, Reduce of training time and ACO based specifiers used to effectively detect intrusion. Efficient training and machine learning capability of the network is another expectation.

7. Conclusion

ACO is used to extract the features of the currently live nodes of the network and these features are then provided to the training of the system. Feature extraction also a recent enhancement in the field of IDS. Based on the values of these features, the system will classify the node as Normal or Malicious. If node is Normal, then the system will return back to the task of monitoring the network. If node is malicious, the system will need to take the appropriate decision. As we had incorporated the ACO algorithm in our approach and ACO is an optimization approach, so by using the proposed IDS, we can improve the specificity and sensitivity of the IDS. We can improve the TRUE Detection Rate and reduce the FALSE Alarming Rate of the IDS. TRUE Detection Rate refers to the percentage of Intrusions successfully detected by the IDS and FALSE Alarming Rate refers to the percentage of Intrusions specified by the IDS, when there was no Intrusion occurred in the system. In this paper we are presenting the relation of ant colony optimization with IDS along with various role played by ACO. In near future we will study ACO as effective intrusion detection technique. Some machine learning techniques are also introduced for effective training of the system.

References

[1] Rais, Helmi Md, and Tahir Mehmood. "Dynamic Ant Colony System with Three Level Update Feature Selection for Intrusion Detection." International Journal of Network Security, Vol.20, No.1, PP.184-192, Jan. 2018.
[2] Global Information Security Survey 2017-18 –online accessed on May 2018. https://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2017-18
[3] Baig, Zubair A., Sadiq M. Sait, and AbdulRahman Shaheen. "GMDH-based networks for intelligent intrusion detection", ELSEVIER Engineering Applications of Artificial Intelligence, vol. 26, issue 7, pp. 1731–1740, 2013.
[4] Wu, Han-Ching, and Shou-Hsuan Stephen Huang "Neural networks-based detection of stepping-stone intrusion" Expert Systems with Applications vol. 37, issue 2, pp 1431-1437, 2010.
[5] Lin, Shih-Wei, Kuo-Ching Ying, Chou-Yuan Lee, and Zne-Jung Lee, "An intelligent algorithm with feature selection and decision rules applied to anomaly intrusion detection", Applied Soft Computing, vol.12, issue 10, pp. 3285-3290, 2012.
[6] Bhuyan, M.H., Bhattacharya, D.K., & Kalita, J.K.. "Network anomaly detection: methods, systems and tools", IEEE Communication Surveys and Tutorials, vol. 16, pp. 303-336, 2014.
[7] Sonawane, Sandip, Pardeshi, Shailendra and Prasad, Ganesh "A survey on intrusion detection techniques", World Journal of Science and Technology, vol. 2, issue 3, pp.127-133, 2012.
[8] Javadzadeh, Ghazaleh, and Reza Azmi. "IDuFG: Introducing an Intrusion Detection using Hybrid Fuzzy Genetic Approach." International Journal of Network Security, Vol.17, No.6, PP.754-770, Nov. 2015.
[9] Morin, Benjamin, Ludovic Mé, Hervé Debar, and Mireille Ducassé. "A logic-based model to support alert correlation in intrusion detection." Information Fusion, vol. 10, no. 4, pp. 285-299, 2009.
[10] Garcia-Teodoro, Pedro, J. Diaz-Verdejo, Gabriel Maciá-Fernández, and Enrique Vázquez. "Anomaly-based network intrusion detection: Techniques, systems and challenges." computers & security, 28, no. 1-2 (2009): 18-28.
[11] Kumar, Vipin, Jaideep Srivastava, and Aleksandar Lazarevic, eds. "Managing cyber threats: issues, approaches, and challenges". Vol. 5. Springer Science & Business Media, 2006.
[12] Zhang, Qinglei, and Wenying Feng. "Network intrusion detection by support vectors and ant colony." In Proceedings of the IEEE 2009 International Workshop on Information Security and Application, pp. 639-642., 2009.
[13] Mehdi Hosseinzadeh Aghdam, and Peyman Kabiri "Feature Selection for Intrusion Detection System Using Ant Colony Optimization", International Journal of Network Security, Vol.18, No.3, PP.420-432, May 2016.
[14] Al-Anezi, Mafaz Mohsin Khalil, Omar Nazar Bader, Zainab Mohammad Abdullah, and Ayad Imad Atallah. "Intrusion Detection and Classification Using Ant Colony Optimization Algorithm." Iraqi Journal of Statistical Sciences, Vol. 13, No. 25, pp. 194-209, 2013
[15] Varma, P. Ravi Kiran, V. Valli Kumari, and S. Srinivas Kumar. "Feature Selection Using Relative Fuzzy Entropy and Ant Colony Optimization Applied to Real-time Intrusion Detection System." Procedia Computer Science, vol. 85, pp. 503-510, 2016.
[16] Fernandes Jr, Gilberto, Luiz F. Carvalho, Joel JPC Rodrigues, and Mario Lemes Proença Jr. "Network anomaly detection using IP flows with principal component analysis and ant colony optimization." Journal of Network and Computer Applications, vol. 64, pp.: 1-11, 2016.
[17] Wankhade, Ajinkya, and K. Chandrasekaran. "Distributed-Intrusion Detection System Using Combination of Ant Colony Optimization (ACO) and Support Vector Machine (SVM)." In proceedings of 2016 IEEE International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE), pp. 646-651, 2016.
[18] Botes, Frans Hendrik, Louise Leenen, and Retha De La Harpe. "Ant colony induced decision trees for intrusion detection." In ECCWS 2017 16th European Conference on Cyber Warfare and Security, pp. 53. Academic Conferences and publishing limited, 2017.

[19] Gupta, Chetan, Amit Sinhal, and Rachana Kamble. "An Enhanced Associative Ant Colony Optimization Technique-based Intrusion Detection System." In Artificial Intelligence and Evolutionary Algorithms in Engineering Systems, pp. 541-553. Springer, New Delhi, 2015.
[20] Duan, Ping, and A. I. Yong. "Research on an improved ant colony optimization algorithm and its application." International Journal of Hybrid Information Technology, Vol.9, No.4, pp. 223-234, 2016.
[21] S. Leng, X. B. Wei and W. Y. Zhang, “Improved ACO scheduling algorithm based on flexible process”, Transactions of Nanjing University of Aeronautics and Astronautics, vol. 23, no. 2, (2006), pp. 154-160.
[22] S. Mao and C. L. Zhao, “Unequal clustering algorithm for WSN based on fuzzy logic and improved ACO”, Journal of China Universities of Posts and Telecommunications, vol. 18, no. 6, (2011), pp. 89-97.
[23] A. Ugur and D. Aydin, “Improving performance of ACO algorithms using crossover mechanism based on best tours graph”, International Journal of Innovative Computing, Information and Control, vol. 8, no. 4, (2012), pp. 2789-2802.
[24] H. L. Xu, X. Qian and L. Zhang, “Study of ACO algorithm optimization based on improved tent chaotic mapping”, Journal of Information and Computational Science, vol. 9, no. 6, (2012), pp. 1653-1660.
[25] KDD dataset. (1999). http://kdd.ics.uci.edu/databases/kddcup99.
[26] Y. Feng, J. Zhong, C. Ye, Z. Xiong and Z. Wu, “Intrusion detection classifier based on self-organizing ant colony networks clustering”, Information Assurance and Security, vol.4, PP. 247-256, 2006.
[27] J. C. Burges and Christopher, “A tutorial on supportvector machines for pattern recognition”, DataMining and Knowledge Discovery, vol. 2, PP. 121-167, 1998.
[28] W. Feng, Q.i Zhangc, G. Hud and J. Huange, “Mining network data for intrusion detection through combining SVMs with ant colony networks”, Future Generation Computer Systems, vol. 37, pp.: 127140, 2014.