JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-11, Nov 2018 E-ISSN: 2347-2693

A Hybrid Intrusion Detection System Using Hypper-Pipe Classifier and Ant Colony Optimization

K Shukla[1*], R K Gupta[2], V. Namdeo[3]

[1,2,3]Dept. of Computer Science, SRK University, Bhopal, India

[*]*Corresponding Author: csresearch2018@gmail.com, Tel.:9131537884*

Available online at: www.ijcseonline.org

Accepted: 18/Nov/2018, Published: 30/Nov/2018

Abstract— The goal of building Intrusion Detection System is conceptualized with need of making secure and protected publically and privately accessible data so that it can be easily avoided from its unauthorized uses. Since increase of network density and heavy use of development of internet has generated a major challenge of making these network data and traffic protected from intruded attacks. Security of network traffic is becoming a major issue of computer network system. Attacks on the network are increasing day-by day. The most publicized attack on network traffic is considered as Intrusion. Data mining techniques are used to monitor and analyze large amount of network data & classify these network data into anomalous and normal data. Since data comes from various sources, network traffic is large. Data mining techniques such as classification and clustering are applied to build Intrusion Detection system. An effective Intrusion detection system requires high detection rate, low false alarm rate as well as high accuracy. This research paper includes effective Data mining techniques applied on IDS for the effective detection of pattern for both malicious and normal activities in network by strong classification mechanism, it will simplify the task of securing information system through this proposed Intrusion Detection system which is developed by the optimized use of newly Ant Colony optimization followed by Hyper pipes classifier classification. Intrusion detection system has been used for ascertaining intrusion and to preserve the security goals of information from attacks.

Keywords— Accuracy, Attack, Ant Colony, Classifier, Clustering, Data mining, Detection, Information, Intrusion, Signature, optimization,etc.

I. Introduction

In the early days of computers system, hackers rarely used automated tools to break into systems. They were intelligent with high level of expertise and followed their own methodology to perform such actions [1]. The recent scenario is quite different now. A wide number of intrusion tools and applications are available now that can be used to exploit scripts that capitalize on widely known anomalies. It includes the representation of the relationship between the relative sophistication of attackers and attackers from 1980 to present days.

Before the development of latest IDS, intrusion detection consisted of a manual search for malicious attack. Due to the availability of adequate processing speed it now became possible not only to look for attack patterns after the event had occurred, but also to monitor in ‘‘real-time’’ and trigger alerts if intrusions were detected.

Due to the financial losses from computer downtime, loss of image, or even confidential data being affected, in recent years the demand for not only being alerted in the event of an attack, but also to prevent the attack altogether has become an absolute necessity. Especially with the introduction of Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, the market demands have grown stronger for Intrusion Prevention Systems (IPS) rather than mere intrusion detection [2-5].

II. Related Work

[1] In this Article, An intrusion-detection model unsupervised anomaly based introduced, and tried to determine the best configuration of the IDS in terms classification accuracy.

[2] In this Article another anomaly based IDS introduced; the basic task in intrusion detection system is based on providing hybrid mode of working of IDS.

[3] In this Article author tried to classical support vector machine based detection system.

[4] In this Article a comparative analysis of various algorithms of performance classification had been provided.

[5] In this Article an Intrusion Detection System based on fuzzy classification technique presented.

[6] In this Article comparative performance classification analysis given for internal IDS presented by author.

[7] In this Article author provided an Intrusion Detection System which is based on J48 classifier.
[8] In this Article, author proposed an Intrusion Detection System for MANET based on multiple agents.
[9] In Article, An Host based Intrusion Detection System conceptualized with aggregation techniques.
[10] In this Article Computer security and intrusion detection, the basic goal of IDS is detecting suspicious traffic in different ways, in spite of that it comes with various approaches. Here Agentauro system has been introduced.

III. Methodology

The intrusion detection system is described by the use of Hyper pipes classifier method along with Ant Colony Optimization which is implemented in various domains like manufacturing, marketing, fraud detection, process control etc. In the last few years, for solving the several issues of intrusion detection system, the various emerging techniques have also been implemented. In this chapter the Hyper pipes classifier approach in implemented in the domain of detection of the intrusion detection system [11-13, 19 & 23]. Recent computer systems and the networks are not fully protected against the intrusions that are found in the public networks. In order to secure the networks from those unwanted intrusions, there is no proper solution is available yet that may provide the complete security to the network, as for protecting the networks from intrusion an expert system is required that may detect the intrusions as soon they are found and immediately take a necessary action in order to stop it from affecting the system. So for preventing from those malicious activities and approach knows as intrusion detection system is described here [14-18]. Various existing approaches for the intrusion detection are artificial intelligence system, data mining, soft computing etc. In many situations the approach of soft computing has been implemented along with the neural network, fuzzy system and genetic algorithm in which pattern-mining and the classification are the major concern [5 & 30].

Proposed Architecture

Proposed work is for intrusion detection. The architecture in figure 1 shows the skeleton of the work. This is made up of two things:

1. Hyper Pipes Classifier
2. Ant Colony Optimization

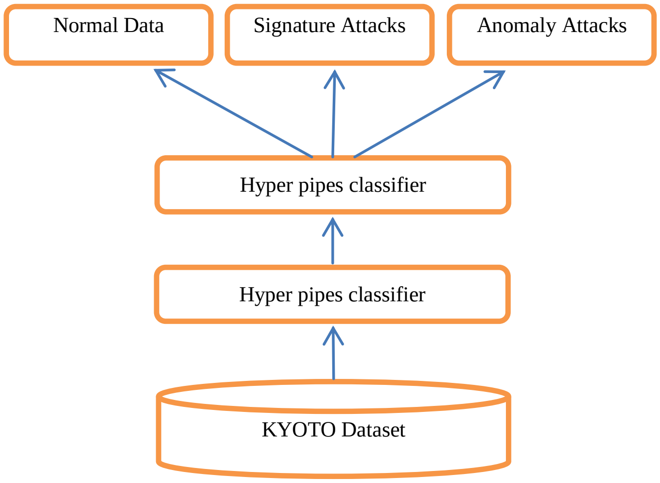

Figure 1: Architecture of proposed work

Proposed Algorithm

This section is dedicated to the description of algorithm of the proposed work which has been given in Figure 2.

```
1.    Load NID Dataset
1. Scan and capture NID n*m-1.
2. Scan and capture labels and associate with records
3. Optimize NID with Ant Colony Optimization
        a.    Initialize pheromone parameters
        b.    Generate initial populations (ants)
        c.    For each individual ant calculate fitness
        d.    For each ant determine its best position
        e.    If best global ant determined
        f.    Update the pheromone trail
        g.    Else
        h.    Go to 'b'
        i.    Output is optimized values
4. Hyper pipes classifier train by NID train
5. Hyper Pipes classifier NID test
6. Output is classified NID
7. Observe classifier ability
```

Figure 2: Proposed Algorithm

Proposed Flow Chart

Here it is being mentioned how the proposed Intrusion Detection System will perform the task of identifying and capturing the intrusions in optimized classification as given in flow chart Figure 3:

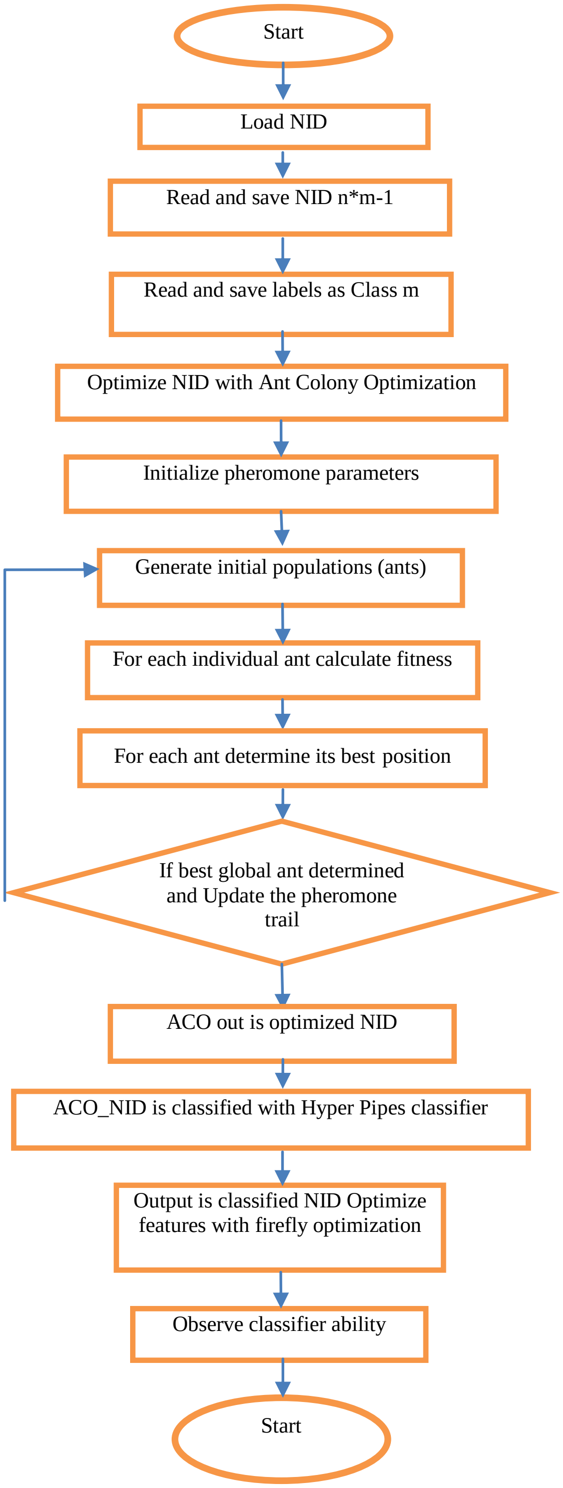
Start
Load NID
Read and save NID n*m-1
Read and save labels as Class m
Optimize NID with Ant Colony Optimization
Initialize pheromone parameters
Generate initial populations (ants)
For each individual ant calculate fitness
For each ant determine its best position
If best global ant determined and Update the pheromone trail
ACO out is optimized NID
ACO_NID is classified with Hyper Pipes classifier
Output is classified NID Optimize features with firefly optimization
Observe classifier ability
Start

Figure 3: Flow Chart of Proposed Work

IV. Results and Discussion

PPV (Positive Predictive Value):
It is ratio between true positive and total number of positive call [10-16 & 20-28]. This analysis is responsible for performance analysis of Intrusion detection System which has been given below for proposed system.

Table 1: PPV of Existing and Proposed Work

	Existing	Proposed
PPV (Positive Predictive Value)	0.89254	0.971474

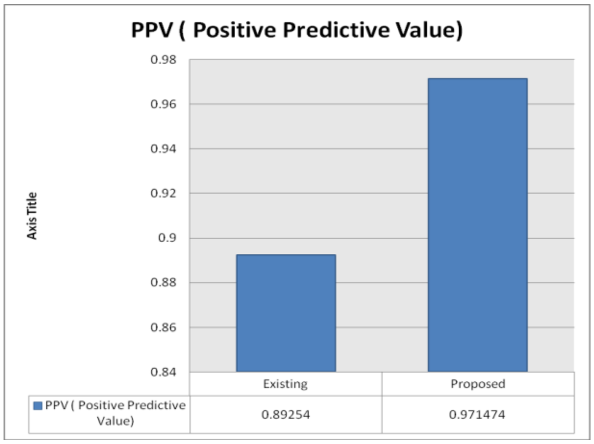

Figure 4: PPV of Existing and Proposed work

Sensitivity:
It is static value which shows the quantifies the avoiding of false negatives [20-22], as specificity does for false positives. It is shown in Table V and Figure 5.6.

Table 2: Sensitivity of Existing and Proposed Work

	Existing	Proposed
Sensitivity	0.56149	0.999672

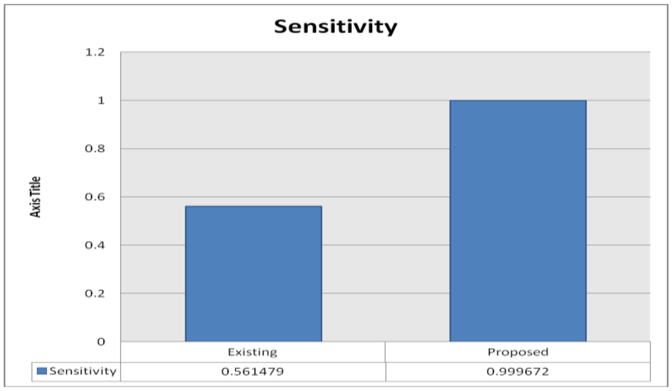

Figure 5: Sensitivity of Existing and Proposed Work

V. Conclusion and Future Scope

This research work is based on the ACO algorithm for optimizing the intrusions identification with the help of noble classification algorithm of Hyperpipe classifier. Ant Colony

Optimization (ACO) is a meta-heuristic approach for solving hard combinatorial optimization problems. The good quality of rules helps in better decision making. On the basis of this new proposed combination of classification and optimization, a new algorithm is proposed based on the Ant Colony Optimization algorithm to improve the result of Intrusion detection. An Ant Colony Optimization optimized the result generated by other general approaches. From this research work which comparatively performs better than existing work in various aspects like sensitivity and positive predictive value it can be concluded that this approach performs better.

As it can be seen that the proposed technique was found very useful from the existing techniques, but still there is a scope for improvement in the proposed approach to extend this approach to handle variety of situations and information. Here time factor and type of attacks identification can be increased. It can further improved in terms of implementation as real time system with neural network concepts.

REFERENCES

[1] Weiwei Chen, Fangang Kong, Feng Mei, Guigin Yuan, Bo Li, "a novel unsupervised Anamoly detection Approach for Intrusion Detection System", *2017 IEEE 3rd International Conference on big data security on cloud*, May 16–18, 2017.

[2] S. Aljawarneh, M. Aldwairi, M.B. Yassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model", Journal of Computational Science, 2017.

[3] J. Yang, T. Deng, R. Sui, "An adaptive weighted one-class svm for robust outlier detection", *Proceedings of the 2015 Chinese Intelligent Systems Conference*, pp. 475-484, 2016

[4] Anbar Mohammed, Abdulah Rosni, H. Hasbullah Izan, Yung-Wey Chong, E. Elejla Omar, "Comparative Performance Analysis of classification algorithm for Internal Intrusion Detection", *2016 14th Annual Conference on Privacy Security and Trust (PCT)*, Dec 12–14, 2016.

[5] Mariem Belhor, Farah Jemili, "Intrusion Detection based on genetic fuzzy classification system", *2016 IEEE 13th International Conference on Computer Systems and Application (AICCSA)*, Nov 29 2016-Dec 2, 2016.

[6] Anbar Mohammed, Abdulah Rosni, H. Hasbullah Izan, Yung-Wey Chong, E. Elejla Omar, "Comparative Performance Analysis of classification algorithm for Internal Intrusion Detection", *2016 14th Annual Conference on Privacy Security and Trust (PCT)*, Dec 12–14, 2016.

[7] Gong Shang-fu ; Zhao Chun-lan,Intrusion detection system based on classification, IEEE International Conference on Intelligent Control, Automatic Detection and High-End Equipment,2012.

[8] J.H. Lee, J.H. Lee, S.G. Sohn, J.H. Ryu, T.M. Chung, "Effective value of decision tree with KDD 99 intrusion detection datasets for intrusion detection system", Advanced Communication Technology 2008 ICACT 2008 10th International Conference on, vol. 2, pp. 1170-1175, 2008.

[9] ShailendraSahu and B M Mehtre ,"Network Intrusion Detection System Using J48 Decision Tree," IEEE , 2015.

[10] Sara Chadli,Mohamed Emharraf and Mohammed Saber "The design of an IDS architecture for MANET based on multi-agent" International Colloquium on Information Science and Technology (CiSt),IEEE,2014.

[11] Difan Zhang, Linqiang Ge, Rommie Hardy, Authersi Yu, Hanlin Zhang and Robert Reschly, "On Effective Data Aggregation Techniques In Host-based Intrusion Detection in MANET," The 10th Annual IEEE CCNC- Green Communications and Computations Track 2013 IEEE.

[12] Jitendra S Rathore, Praneet Saurabh, Bhupendra Verma "AgentOuro: A Novelty Based Intrusion Detection and Prevention System" Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on 3-5 Nov. 2012.

[13] Vasima Khan, Anomaly Based Intrusion Detection And Prevention System, IJERT, 2013.

[14] Mukesh Sharma,Akhil Kaushik, Amit Sangwan Performance Analysis of Real Time Intrusion Detection and Prevention System using Snort.,IJERT, 2012 .

[15] Vaishali T.Deshmukh, Shubhangi Vaikole, Layered Crf A Model To Build More Accurate Intrusion Detection System, IJERT, 2012.

[16] Bhavana G.Rathwa,Prof.Purnima Singh Genetic Algorithm Methodology for Intrusion Detection System, IJERT, 2012.

[17] Bin Zeng , Lu Yao and ZhiChen Chen"A network intrusion detection system with the snooping agents",International Conference on Computer Application and System Modeling, 2010.

[18] Vera Marinova-Boncheva, "A Short Survey of Intrusion Detection Systems", Problems of Engineering Cybernetics and Robotics, 2007.

[19] A. Moore, D. Zuev and M. Crogan, "Descriminators for use in flow based Classification," Queen Marry University of London, August 2005.

[20] Khaled Labib, Computer security and intrusion detection, Crossroads, Volume 11, Issue 1, August 2004.

[21] Yong Zhong, Xiao-lin Qin, Database Intrusion Detection Based on User Query Frequent Itemsets Mining with Item Constraints [J], Proceedings of the 3rd international conference on information security, 2004.

[22] Dheeraj Gupta ; P.S. Joshi ; A.K. Bhattacharjee ; R.S. Mundada, IDS alerts classification using knowledge-based evaluation, Fourth International Conference on Communication Systems and Networks (COMSNETS 2012).

[23] David Ahmad Effendy ; Kusrini Kusrini, Classification of intrusion detection system (IDS) based on computer network; Sudarmawan Sudarmawan, 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE) 2017.

[24] Murthy, S.K. , Automatic Construction of Decision Trees from Data: A Multi-Disciplinary Survey. Data Mining and Knowledge Discovery, 24, 1998.

[25] I Nyoman, Trisna Wirawan, I. E., "Penerapan Naive Bayes Pada Intrusion Detection System Dengan Diskritisasi Variabel", *Jurnal Ilmiah Teknologi Informasi*, vol. 2, 2015.

[26] Aurobindo Sundaram, An Introduction to Intrusion Detection, Crossroads, Volume 2, Issue 4, Pages: 3 –7, 1996.

[27] Northcutt, S. "Network Intrusion Detection: An Analyst's Handbook." New Riders, Indianapolis 1999.

[28] Akthar, F. and Hahne, C. Rapid Miner 5 Operator Reference, 2012.

[29] KDD99, KDDCup 1999 data, 1999, http://kdd.ics.uci.edu/ Databases/kddcup99/10 percent.gz, 1999.

[30] S. Zaman S., F. Karray. Fuzzy ESVDF approach for Intrusion Detection System. The IEEE 23 International Conference on Advanced Information Networking and Applications (AINA-09), Page(s): 539-545, 26-29 May 2009.

Authors Profile

Mr.K.Shukla is pursuing Master of Technology in Computer Science & Engineering Department of Sarvepalli Radhakrishnan University, Bhopal (MP). He focuses on the field of computer security to strengthen computer security learning and importance.

Mr.R.K.Gupta is a well known Professor of Computer Science & Engineering Department of Sarvepalli Rdhakrishnan University, Bhopal (MP). He is pursuing Ph.D. in Computer Science from Barkatullah University Bhopal. His research interest and specialization falls upon intrusion Detection System and various Computer Security Strategies.

Dr.V.Namdeo Head of Computer Science & Engineering Department of Sarvepalli Radhakrishnan of Sarvepalli Rdhakrishnan University, Bhopal (MP). She is equiped with huge knowledge and experience of various fields of Computer Science fields.