BIOLOGICALLY INSPIRED INTRUSION DETECTION (BIID): A REVIEW

Lalitha Bhavani Jivanadham, Wan Haslina Hassan and Omar Zakaria
Malaysia Japan International Institute of Technology (MJIIT), Universiti Teknologi Malaysia
Kuala Lumpur, Malaysia
E-Mail: *bjlalitha2@gmail.com

ABSTRACT

With recent advances in the network based technology and increased dependability of our everyday life on this technology, assuring continuous and reliable operation is essential. During recent years, more hazardous attacks such as the Distributed Denial of Service (DDoS) attacks are prominent on networks. Functionality of networks is being compromised as these attacks have dramatically increased. This encourages the investment on approaches that is able to sustain with changing conditions without external party intervention. Hence, the interest in bio-inspired network intrusion detection has increased among researchers. Bio-inspired network intrusion detection is able to adapt to varying environmental conditions, providing in-built resiliency to failures and damages, collaborative, survivable, self-organizing and self-healing. Thus this paper provides a review in latest trends of Bio-Inspired Intrusion Detection (BIID) based on three principles established in order to enhance the existing intrusion detection. This study shows that (1) BIID approaches provides both behavior based and knowledge based detection methods, (2) provides both batch mode and real time analysis in intrusion detection system and (3) provides both standalone and distributed intrusion detection. Among the several available bio-inspired intrusion detection approaches, this paper investigates the Genetic Algorithm (GA), Artificial Neural Network (ANN), Artificial Immune System (AIS) and hybrid approaches. Analysis based on the intrusion detection shows that these approaches are being used widely. However, there still remain several obstacles, not allowing these approaches to completely unveil its potential to provide autonomous intrusion detection and continuous network operation. This paper reveals these obstacles and highlights the strengths and weaknesses of the investigated approaches based on the principles established. The analysis shows that bio-inspired approach could play a major role in providing autonomous intrusion detection.

Keywords: security, intrusion detection, bio-inspired, DDoS, survivability, self-healing.

INTRODUCTION

The security of networks and systems can be achieved, either in a preventive approach or curative way. Both data and resources against any unauthorized or abusive access is protected in preventive approach. However, preventing against all security violations is an impractical task. Therefore, the curative approach seems then a better way to assure the security of the networks and systems, since it aims in detecting this attacks when they occur and eventually the caused damages are repaired. Thus the curative approach is achieved through intrusion detection systems (IDS) where the vulnerabilities over the networks and systems are detected. The existing intrusion detection approaches are very complex and costly. Drawbacks of existing IDS inevitably urges the design of a new generation of self-adaptive IDS. This new generation IDSs are expected to acquire flexibility, adaptability and affordability and provide a greater autonomy. Therefore, approaches based on biologically inspired intrusion detection (BIID), which reveals itself as a suitable candidate to make a balance between security requirements, system flexibility and adaptability is arising as a fastest growing research and new application development in telecommunication. This technique seems so promising to embed adaptive features in network entities. These entities become more intelligent, capable of making various decisions with autonomy to detect attacks.

BIID is an amalgamation of Computational Intelligence (CI) and Soft Computing (SC). CI is defined as a field of computation evolved in replacement of traditional Artificial Intelligence (AI) [1]. AI, a field that is intended to develop intelligence in machines [2], is a huge contributor to these autonomous systems and technologies. However the limitations of the traditional AI such as inability to explain the logic and reasoning behind a certain decision and the lack of common sense in reasoning which may cause major problems [3] have encouraged the budding of CI. CI includes Artificial Neural Networks (ANN), Evolutionary Computation (EC) such as Genetic Algorithm (GA), Fuzzy Logic (FL), Swarm Intelligence (SI), Artificial Immune System (AIS), Data Mining (DM) and Natural Language Programming (NLP) [4]. Additionally, in order to extend the capability of intelligent systems and to sustain imprecision tolerance, uncertainty, partial truth and approximation [5], SC is also widely applied in designing intelligent systems. The role model for SC is the human mind. SC includes ANN, EC, FL, SI, Bayesian Networks (BN) and Chaos Theory (CT). This complementing feature of comprehensive observation on nature which is capable of generating cooperative as well as effective configurations in terms of resource management and task allocation, synchronization or de-synchronization without the need for any externally controlling entity [6] supports the implementation of biologically inspired systems and technologies. Among the many BIID, the GA, ANN, AIS and hybrid based intrusion detections are further elaborated in this study, since these approaches are widely applied in the field of intrusion detection. Additionally, the research trend in each area for the past 10 years is also provided.

GA is a search algorithm that imitates genetic evolution process. The basis of GA operation is based on four operators: initialization, selection, crossover and mutation [7]. In GA based intrusion detection, initial population of chromosomes is generated randomly where each chromosome represents a possible solution to the problem, which is a set of parameters. Firstly, the incoming traffic is captured using a packet capture engine, which is then used to extract the payload by removing all the header information present in the packet and the payload is given as input to the GA which in the training phase uses it to build profiles. Then, in the selection phase, parents are selected for crossover by finding the fittest chromosome from the existing population based on pre-defined fitness function and the input data forms the other parent. Since the input data is used to construct profiles, the network behavior is mapped on the profiles efficiently. Crossover is a scheme where parents crossover and produce offspring. Offspring that are identical with parent is discarded and the remaining offspring is tested for fitness. If they are fit enough, then they are added to the population, else they are not. Finally, in the replacement phase, which is also an optional phase, the unfit chromosomes are replaced with fittest chromosomes in order to optimize the population. Thus, there are several replacement techniques such as complete replacement, partial replacement and steady state replacement. Though easy to implement, the complete replacement may lose some fittest chromosomes in the population. However, the partial replacement protect this lose by only replacing certain chromosomes and the rest are retrieved as it is. GA's effectiveness relies on the "Fitness Function", individual representation and the parameters as well.

ANNs on the other hand, is a mathematical model inspired by the process of biological nervous system [8], [9]. It is exposed as a network with large number of simple processors, which is considered as neurons in the biological system [10]. In ANN intrusion detection, firstly the ANN is exposed to normal data and to attacks to automatically adjust coefficients of the ANN during training phase. Then, the performance tests are conducted with real network traffic and attacks. It is involved in information processing, similar to as how the brains perform information processing [11].

AIS however, is a computational technique, inspired by Human Immune System (HIS) [12]. HIS is an extremely complicated yet accurately synchronized process for detecting and eliminating infections. AIS can be applied to security in computing and networking systems [13], since it preserves appropriate state of the system by detecting misbehaviors. The two fundamental components in AIS systems are the antibodies and antigens. Antibodies are part of the system, which are responsible for detection and elimination of antigens. Contrarily, antigens are foreign invaders, which attack a considered system. In the case of network security, any assigned vulnerability detectors [14] such as Nessus, Retina and many more are the antibodies and DDoS and other attacks are antigens. In AIS based IDSs, the antibodies are responsible to detect the antigens by matching them. Unfortunately, the matching of antibodies and antigens in AIS based IDS are never perfect since the number of antigens commonly out numbers the number or the ability of antibodies.

Subsequently, some works have combined the bio-inspired techniques to achieve better intrusion detection. Several works combined Fuzzy with Genetic Algorithm, some have studied the IDS with ANN and AIS and some works detected intrusion with intelligent agents with AIS.

There has been many works featuring the potential of BIID approaches as compared to the traditional IDSs. However, studies highlighting the comparison among these BIID approaches are scarce. Apart from highlighting the differences and potentials of BIID approaches, in principle to the characteristics of the BIID, this study states that the BIID approaches (1) provides both behavior based and knowledge based detection methods (2) provides both batch mode and real time analysis in intrusion detection system (3) provides both standalone and distributed intrusion detection. Finally, through this study, it is expected that the readers are able to distinguish a suitable BIID approach based on their requirement for an IDS implemented to ensure secured networks and systems.

This paper is organized as follow. Section 2, overview of attack classes and description of commonly detected attacks and the fundamentals of intrusion detection such as the categories of intrusion detection are discussed. Following that, related works of approaches in biologically inspired intrusion detection is further explained and the contributions are tabulated in Section 3. Finally the conclusion remarks and future research directions are provided in section 4.

#

Intrusions and Intrusion Detection

#

Network Intrusions

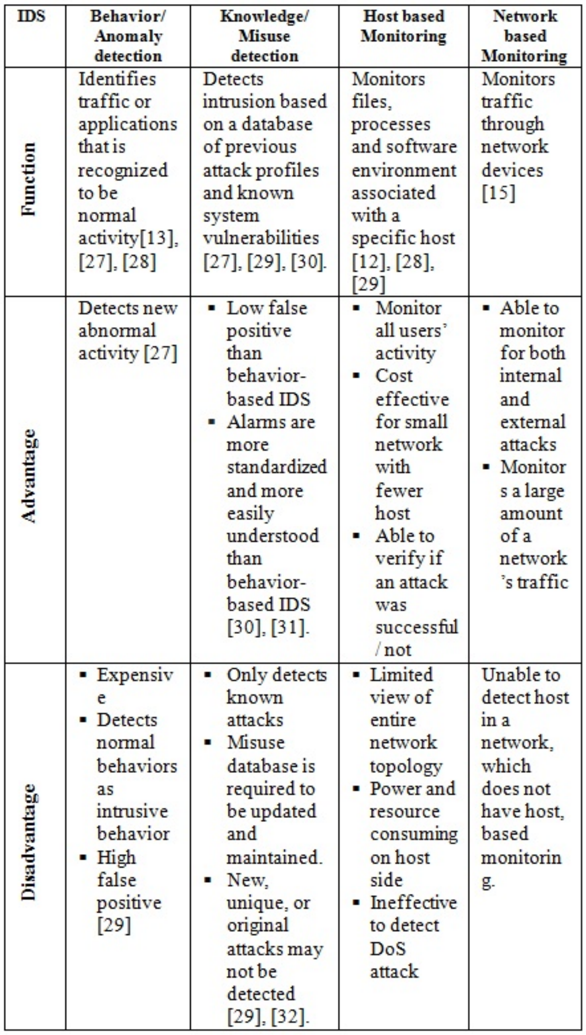
Most intrusions transpire via network to attack their targets. For example, during a certain intrusion, a hacker executes several steps to achieve his goal; first he sets up a connection between a source IP address to a target IP, then sends data to attack the target. These kinds of connections are identified as attack connections and the rest are normal connection [8]. Attack connections and normal connections have their special feature values and flags in the connection head, and package contents that can be used as signatures to distinguish the normal network traffic and intruded traffic. Intrusions belong to the same intrusion category have identical or similar attack principles and intrusion techniques. Therefore they have identical or similar attack connections and are significantly different from normal connections. These attacks can be classified in four categories namely, Remote-to-Local (R2L), User-to-Root (U2R), Probing [15] and Denial of Service (DoS)/ Distributed Denial of Service (DDoS) [17]. Since the DoS/ DDoS attacks are becoming prominent and hazardous among other network attacks, this attack class is the focus of this study. DoS/ DDoS is capable of making a network unavailable for its users. For an instance, remote attackers attempt to exploit the weaknesses of Internet Control Message Protocol (ICMP) by triggering DoS attacks, such as ICMP flood [18]. DoS/ DDoS attacks involve many connections to some hosts in a very short period of time. The DoS/ DDoS is broadly divided into three categories, volume based attacks, protocol attacks and application layer attacks. In volume-based attack, the bandwidth of the attacked site is saturated as in the spoofed packet floods like ICMP and UDP floods. The attacks that consumes actual server resources, or those of intermediate communication equipment, such as firewalls and load balancing are the protocol attacks which includes SYN floods, Ping of Deaths, Smurf attacks and many more. In spite of that, these attacks take place at the Infrastructure Layer (Layer 3) of a network. Based on the Prolexic Quarterly Global DDoS Attack Report [19-23], it is obvious that the contribution of DoS/ DDoS at Infrastructure Layer is evidently high compared to the Application Layer attacks, which constitute more than 75 % of DoS/ DDoS in each year between 2010 till 2014. The reports also emphasizes that the Infrastructure Layer attacks has an up climbing trend over the years. These trends of majority composition and increasing attacks affirm that the Infrastructure Layer is becoming the covet target of attackers as well as a highly vulnerable point. Attackers primarily used infrastructure layer (layer 3 and 4) directed attacks to reach bandwidth or connection limits of hosts or networking equipment. This can affect available network bandwidth and impose extra load on the firewall. Weakening infrastructure layer opens more avenues for higher layers attacks such as application layer, which focuses on reaching resource limits of services and accomplish resource starvation. The SYN flood attack has marked as the highest attack in the last 5 years, in spite having a fluctuating trend. The second highest number of attacks is the UDP flood attacks, which even outnumbered the SYN flood attack in 2012 and 2014. The DNS attack is another attack that has a steady increasing trend. However, the ICMP flood attack alone illustrates a declining trend between 2010 and 2014. Generally, the numbers of attacks have been reducing over these years due to the presence of highly sophisticated network security measures. However, the reduction rates of these attacks are minimal. Thus indicating the need for intrusion detection with the ability of self-control, flexibility, adaptability, autonomy and distributed communication.

#

Intrusion Detection

The earlier section shows the gravity of increasing attacks to compromise network functionality. Thus, the intrusion detection is the practice of discovering a set of actions attempted by intruders to compromise systems security [24]. This discovery is obtained through IDS that is engineered to generate an alert when potentially malicious traffic is observed. It monitors packets from network connections and determines if it is an intrusive activity or not. Once an intrusion is detected, the IDS simply logs in a message into system audit file to be later analyzed by network security experts, or send email alert to a network administrators, and stops such connection to end an intruder’s attack. IDS are divided into two categories based on the data collection mechanism, such as Host based Intrusion Detection (HID) and Network based Intrusion Detection (NID) or based on detection method, such as anomaly or misuse and behavior based or knowledge based [25]. The network based monitoring, provides a more efficient way of protecting against attacks [26]. The IDS categories and monitoring methods, its functions, advantages and disadvantages are summarized in Table-1.

Table-1. Intrusion detection classification.



IDS	Behavior/ Anomaly detection	Knowledge/ Misuse detection	Host based Monitoring	Network based Monitoring
Function	Identifies traffic or applications that is recognized to be normal activity[13], [27], [28]	Detects intrusion based on a database of previous attack profiles and known system vulnerabilities [27], [29], [30].	Monitors files, processes and software environment associated with a specific host [12], [28], [29]	Monitors traffic through network devices [15]
Advantage	Detects new abnormal activity [27]	▪ Low false positive than behavior-based IDS ▪ Alarms are more standardized and more easily understood than behavior-based IDS [30], [31].	▪ Monitor all users' activity ▪ Cost effective for small network with fewer host ▪ Able to verify if an attack was successful / not	▪ Able to monitor for both internal and external attacks ▪ Monitor s a large amount of a network 's traffic
Disadvantage	▪ Expensiv e ▪ Detects normal behaviors as intrusive behavior ▪ High false positive [29]	▪ Only detects known attacks ▪ Misuse database is required to be updated and maintained. ▪ New, unique, or original attacks may not be detected [29], [32].	▪ Limited view of entire network topology ▪ Power and resource consuming on host side ▪ Ineffective to detect DoS attack	Unable to detect host in a network, which does not have host, based monitorin g.

With the understanding of upcoming intrusion attacks and fundamentals of existing intrusion detection, the following section have assembled some related works in BIID whilst focusing on the contribution as IDS.

Biologically Inspired Intrusion Detection (BIID) Related Works

The functionality of a BIID is determined by the intrusion detection methods, which is behavior or knowledge based. The mode of intrusion analysis, whether it is batch mode or real time also matters. Other core consideration is the topology of the target system to be analyzed, which can be standalone computer system or a distributed one. Based on several existing studies, this study has established three principles of BIID functionality, which is supported by their related works. This analysis is expected to assist in distinguishing the competent approaches in facilitating the adoption of BIID for a flexible and self-adaptable intrusion detection system.

#

Behavior and Knowledge based Detection Method

This study asserts that the BIID supports both behavior and knowledge based detection methods. The behavior-based intrusion detection approach allows the detection of unknown intrusions and thus does not require any prior knowledge on intrusions. The approach is to differentiate the user, as the normal behavior entity, and the intruder as an abnormal behavior entity. Thus, all the intrusive activities are inevitably abnormal. Interpretation of the user and system behavior can be achieved through modelisation or prediction [30],[33],[34]. As opposed to the behavior-based detection, the knowledge-based intrusion detects intrusions by manipulating eminent system vulnerabilities. It is based on the fact that any known attack produces a specific trace in audit trail or in the network data. It needs prior information about the attacks it is able to detect. The two methods, widely applied in this detection is the rule based and signature based method [18], [35-37]. Referring to the BIID approaches, the ANN ID approach adopts the prediction, behavior based technique to detect intrusions. Devi Krishna K.S. et.al [38] proposed an approach for ANN based intrusion detection system. The ANN parameters were determined by training and the classification of a single record was done in an insignificant time. Therefore, the proposed model is able to operate as an online classifier for the attack types that it has been trained for. The results show that the implemented and designed system detects the attacks and classify them into six groups. KDD Data set is used for the training and evaluation of the ANN classifier. The implemented system solved classification problem. However, this model was tested on a small number of attack scenarios unlike the practical IDS, which includes several attack types. The complexity of this model is also high, which can be reduced by introducing initial classifications for the normal and attack connections. Dilip Kumar Barman et.al [37], proposes an ANN based IDS with back propagation for predicting intrusion and rough set statistical model. The proposed model consists of three layers: one input, one hidden, and one output layers with one feedback layer from output to the hidden layer. The ANN has been adjusted as per the learning process, based on the selected sample (signature) of attacks. The proposed system was trained by using the KDD99 training dataset and its performance was evaluated by KDD99 test dataset. Adoption of Rough Set in this model is utilized for minimization of the features to be used both for training and testing. Thus reducing the processing time substantially for this model. The proposed model was tested against the KDD 99 test data. The Rough Set based system considers the input signatures of attacks of all the features, and based on the dependency ratios, the system will output the signatures with only the most relevant features. The signatures with the most relevant features are then fed into the Neural Network part of the IDS for training and testing the IDS. The detection rates of this model closely resemble with those available from other IDS systems. In fact, it is at least 20.5 times faster in detection for back attack, which makes this model a potential real time IDS. In contrary, the GA ID adopts the knowledge-based detection. GA is rule-based misuse detection, which is successful in detecting known attacks [39]. GA approach is incompetent of discovering unknown or novel forms of attacks. In order to detect known attacks, all likely variations of attacks have to be defined in GA approach, which is a challenging task. GA elements are simply retrained, which offers the opportunity to develop new rules for intrusion detection, which offers the adaptability of a GA ID [40]. However, the task of defining new intrusion rules becomes the responsibility of the network administrator since it requires a certain level of expertise, security insight and awareness. In addition, determining the relations between these rules is difficult, which implicates the difficulty in verifying the correctness of the rules. Hence rapidly become obsolete and requiring frequent updating [41]. Furthermore, any inaccuracies in the signature increase the false positive rate (FPR) and decrease the detection (DR). Mit. H. Dave et.al [42] proposed an IDS that integrates SNORT IDS with GA. The motivation of this work was to reduce the number of rule set for detection as compared to traditional SNORT. The SNORTGA detect intrusions in two phases. In the first phase, which is the Pre-calculation phase, set of rules is generated using the training data. Subsequently, the detection phase or the second phase is where a population is created for a test data and undergoes some evaluation processes to predict the test data type. The pre-calculated set of chromosome from the first phase is used in this process to find the fitness of each chromosome of the population. The proposed model studies the intrusions using KDDCup 99 dataset. Evaluation results, proves further that the proposed model improves detection time, resource utilization and memory utilization. However, as other GA based IDSs, this model also consumes time in training the data though the detection time is shorter than existing SNORT. Nonetheless, both the behavior and knowledge based detection techniques are leveraged through the adoption of AIS IDs as well as the hybrid IDS. The AIS intrusion detection adopts both anomaly and misuse detection technique. The adaptive system of human immune system is mapped to the anomaly detection and the innate system is compared with the misuse detection [43]. Therefore, AIS ID uses pattern recognition on memory cells or signatures database to detect intrusions and detects future attacks with their trained cells [12]. This is quite the contrary to customary IDS, since it practices either misuse or anomaly detection.

Batch Mode and Real Time Analysis

This study asserts that the BIID supports both batch mode and real time analysis in intrusion detection system. In batch mode intrusion detection, the analysis of audit data occurs sometime after the data has been collected [21]. The disadvantage of this analysis is that it detects the attacks only after the damages are caused. The batch mode intrusion detection can be very useful in environments where periodic summaries of suspicious users are sufficient. In real time intrusion detection, the audit data must be analyzed as soon as they are created [44]. This mode can appear crucial for critical systems in order to identify suspicious user behaviors when they occur and to detect instantaneously any security violation. However, the analysis in real time, can generate hardware and software performance problems. Indeed, a high reliability, a large storage capacity and a high-speed hardware, become key issues. Moreover, to make real-time audit data analysis viable, the delay between the moment when an audit transaction occurs and the moment when it is written on the disk must reduce considerably. Though all BIID approach provide real time analysis, in contrary to the traditional approaches. The GA ID is able to offer real time and optimized analysis to overcome the limitation of other real time analysis approaches. B.Uppalaiah et.al [7], proposed a GA based intrusion detection architecture that contains two phases. The first phase is the learning stage, where rule set is generated for detecting intruders using network audit data. In the second phase the best rule set with highest fitness value generated in phase one, is used for detecting intruders in the Internet. The proposed model studies four categories of attacks i.e. DoS, R2L, U2R and Probe attack using KDDCup 99 dataset. Authors have applied three different features to optimize the rule set generated to detect two types of attacks in each category such as DoS (Smurf, Mailbomb), R2L (Warezmaster, Multihop), U2R (Snmpguess, Buffer-overflow) and Probing attack (IP-sweep, saint). This work produces high detection rate because the three features used to describe data thoroughly with optimized searching by GA in the large data set. Nonetheless, the proposed mechanism requires longer training time due to the complexity of the model. However, the hybrid BIID approaches such as the hybrid of GA and Fuzzy [45] and ANN and DM [46] offers both batch mode and real time processing.

Standalone and Distributed Intrusion Detection

The third principle being established is that the BIID supports both standalone and distributed intrusion detection. On a stand-alone computer system, the audit data collection is performed by a single audit mechanism, which makes the audit record format consistent. In contrary, in a distributed system, the audit data collection is ensured by several audit mechanisms which require a comparison of the audit records of the various components and a coordination of the analysis of different hosts. The heterogeneity of a distributed network multiplies the vulnerabilities of the various systems, contrary to a stand-alone computer system. Collected information is more significant in a distributed environment which implies the use of sophisticated algorithms and large archiving systems. The ability to adopt distributed detection is vital in current network technology advancement especially with the increasing DDoS attacks as reported in [47] . The BIID approaches are more effective in detect these DDoS as compared to the traditional IDS. Fen Zhou et.al [48], proposes an intrusion detection model that combines two hybrid genetic algorithms. The authors applied the GA for global optimal search and supported the local optimization with heuristic algorithms. This attempt produces better feature set of reduction in shorter time. The proposed model studies four categories of attacks i.e. DoS, R2L, U2R and Probe attack using KDDCup 99 dataset. The rule set generated detects SYNFloods (DoS), Password guessing (R2L), Buffer-overflow (U2R) and Port Scanning (Probing attack). Adopting GA enables to achieve expected results based on precisely defined problems, however this solution might or might not be the best possible one. Thus, certain problems are complex and might not be able to get an acceptable solution in an acceptable time. In such cases, adopting heuristic techniques allow to achieve reasonable solution at shorter time. It is common in GA based intrusion detections that the exploration is not so much on obtaining the best solution, but for any solution fitting some constrain. Nevertheless, a good heuristic would help to find a solution in short time, but it may also fail to find any, if the solution is in the states that were reduced. The hybrid of GA and AIS ID, integrates the benefits of both approaches by providing higher DR and lower FPR. This approach allows distributed intrusion detection as well as improves the training of the detectors with the encountered intrusion information retained in the memory and this information also facilitates the detection of unknown intrusions effectively. The hybrid of ANN and IA on the other hand, enhances the features of ANN ID with the ability of distributed intrusion detection by combining the multi-agent method.

FINDINGS

In this section, all the finding of this study is presented to show the research trends in BIID and BIID hybrid solutions. In addition, Table 2 comprising the functionalities of BIID works thus far, is also presented.

RESEARCH TREND

Figure-1 provides the publication statistics for both journals and conference proceedings according to the year of appearance. It is obvious that the increasing number of research work indicates that BIID is a growing research area, particularly since 2008. From this figure, a number of trends become evident in the surveyed works. The first trend is the popularity of ANN. Among 188 papers surveyed, 59 are related to ANN. ANN has been adopted continuously throughout the years. There does not seem much decline except in 2009. The appearance of GA is another trend. GA has been a popular research in IDS since 2010. Out of 188 surveyed papers, 52 were researches on GA IDS. There is also a trend in applying hybrid approached for intrusion detection. Tightly or loosely assembling different methods in a cooperative way definitely improves the performance of IDS. In Fig. 2, the hybrid approaches is classified into GA hybrid and ANN hybrid. Among the GA hybrid approaches categorized in this group are GA+ Fuzzy, GA + Data Mining, GA+AIS, GA+ Statistical. The ANN hybrid consist of ANN + Fuzzy, ANN + Data Mining, ANN + AIS and ANN + Machine Learning. The GA hybrid is shown as the popular hybrids since its adoption throughout 2008–2014 compared to other available hybrid approaches. The ANN hybrid records another trend, whereby it is gaining popularity since 2010. Among 27 papers surveyed on hybrid approaches, 5 are related to GA + ANN hybrid, 5 are related to GA + Data Mining hybrid and 5 are related to ANN + Fuzzy Hybrid.

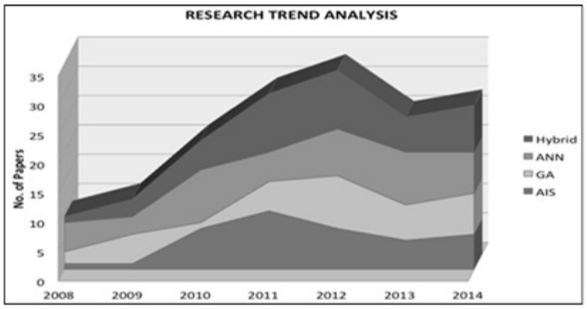


Figure-1. Research trend analysis.

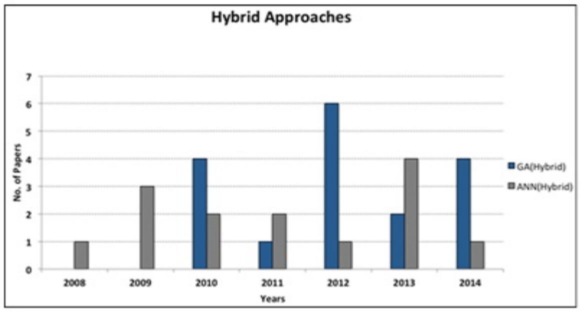


Figure-2. Hybrid approaches analysis.

Table-2. Biologically inspired intrusion detection (BIID).

Approach	DT	K/U	Analysis	Classifier	Technique	Related Works
GA	KW	K	Real Time	Fitness Function	Encoding, Fitness Function, Selection, Crossover, Mutation	[49],[48],[18],[50],[7],[17], [51],[40]
ANN	B	K U	Real Time	External Stimuli	BPNN, SOM, SVM, SA	[52],[8],[53],[54],[31],[41],[16],[13], [37]
AIS	B KW	K U	Batch Real Time	Recognition Function	Clonal Selection, Immune Network theory, Negative Selection, Danger theory	[55],[56],[57],[58],[59],[60],[61],[62],[63],[64]
GA + AIS	B KW	K U	Batch Real Time	Time Slice, Minkowski distance	NicheMGA, Negative Selection	[65], [32]
GA + Fuzzy	B KW	K U	Batch Real Time	Class-Association-Rule Mining	Selection, Crossover Mutation, Trapezoidal fuzzy rule	[66],[45],[67]
ANN+ AIS	B KW	K U	Batch Real Time	PCA	PCA, Deterministic crowding	[68]
ANN+ IA	B KW	K U	Batch Real Time	Feed-Forward	Multi agent	[69]
ANN+ DM	B KW	K U	Real Time	External Stimuli	KMeans, EM Clustering, MLP RBF, C4 Decision Tree, NBTree, CART	[46]
GA +ANN + DM	B KW	K U	Batch Real Time	External Stimuli	K-Means, GA, ANN	[70]

Legend: DT: Detection Technique B: Behavior KW: Knowledge
SA: Simulated Annealing K: Known U: Unknown
GA ID: Genetic Algorithm Intrusion Detection IA: Intelligent Agent
SOM: Self Organizing map RBF: Radial Basis Function
ANN ID: Artificial Neural Network Intrusion Detection AIS ID: Artificial Immune System Intrusion Detection DM: Data Mining
BPNN: Back Propagation Neural Network CART: Classification and Regression Tree PCA: Principal Component Analysis
EM: Expectation Maximization SVM: Support Vector Machine
MLP: Multilayer Perceptron NBTree: Naive Bayes Tree

Table 2 provides a summary of other BIID proposed approaches. These approaches are categorized based on detection technique if it is anomaly based or misuse based detection, whether the discussed approach detects known or unknown intrusions and the types of classifiers required for intrusion classification and feature selection. In addition, types of input data, whether an audit trail or network packets are used for the training and learning [71-73] process of these approaches is also tabulated in Table 2.

PERFORMANCE OF BIID

Figure-3 illustrates the detection rate (DR) and false positive rate (FPR) performance of GA, ANN, AIS and its hybrid based approaches. Based on the performance analysis, hybridization of GA and Fuzzy techniques offers superior performance as compared to pure GA or GA and AIS based intrusion detection approach. This hybrid provides reduced FPR with high DR. providing lowest FPR proves its detection reliability as compared to the other two approaches. Furthermore, any inaccuracies in the signature increase the FPR and decrease the DR. GA elements are simply retrained, which offers the opportunity to develop new rules for intrusion detection [40]. Network administrator, with certain level of expertise, security insight and awareness, defines these rules. In addition, determining the relations between these rules is difficult, which implicates the difficulty in verifying the correctness of the rules. Hence rapidly become obsolete and requiring frequent updating [41] which eventually reflects on the discrepancies of the signatures.

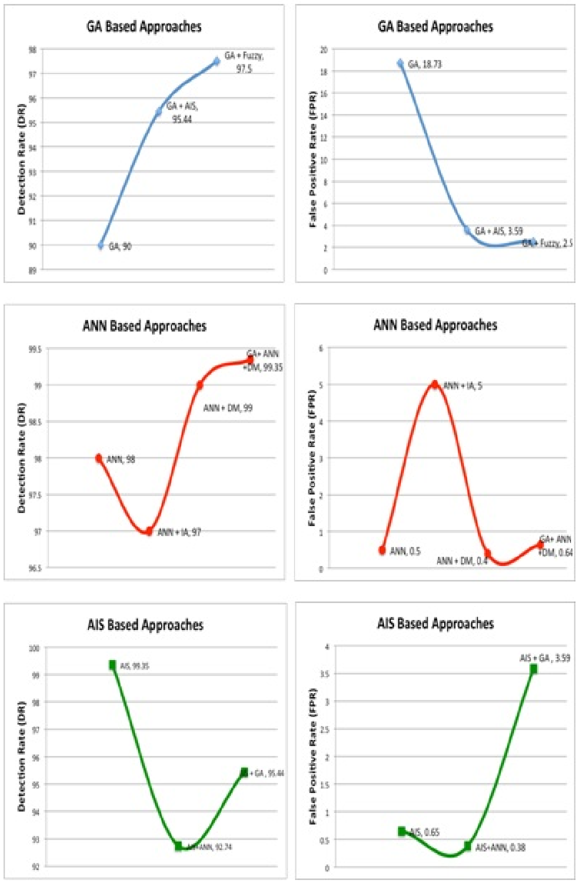


Figure-3. Detection and false positive rate BIID approaches analysis.

As for the ANN approaches, the hybrid of GA, ANN and DM is a more reliable approach as compared to other three approaches. ANN intrusion detection is able to learn from an environment and adjusts its internal structure through training process. The neural network uses non-linear regression to abstract information from the abnormal training cases to predict future attacks [74]. The classifier algorithm used in ANN intrusion detection improves the accuracy of classification by determining the best solution and minimizing the number of incorrectly classified cases during the training process [75]. This is why unlike other ANN approaches, the hybridization of GA, ANN and DM produces high DR and reasonable FPR. Finally, AIS based approaches offers high DR and a moderately low FPR. This is because AIS is capable of retaining memory of the previous intrusions. Thus this immune memory allows AIS to quickly react on repeated intrusions. For these reasons, the DR of AIS ID is better than GA ID but lower than ANN ID, but AIS ID produces the low FPR.

CONCLUSIONS

In conclusion, the biologically inspired intrusion detection approaches adoption offers higher detection and false positive rates compared to the traditional intrusion detection. These approaches offer flexibility in detection technique because majority of approaches such as AIS ID and the hybrid IDs detects intrusion based on both anomaly and misuse method enabling these approaches to acquire the known and unknown attacks. In contrary, the traditional detection approaches do not offer this flexibility since they only offer either one, anomaly or misuse based detection function. In this study, the analysis mode, whether the analysis is a batch mode analysis or real-time analysis is highlighted. With the rise of hazardous and complex intrusions that are able to collapse a network operation efficiently, the need for real-time intrusion detection system are able to detect intrusions more effectively. The BIID approaches reviewed in this study require classifiers to facilitate its operations. These classifiers guide the systems' performance in an arbitrary environment enabling these IDSs to adapt to changing environments. Commonly, the GA ID approach is proposed for optimizing intrusion detection operation, whereas the ANN ID meant for better intrusion classification and AIS ID for distributed intrusion detection. By combining these approaches, ability to achieve higher accuracy, adaptability and other IDS requirements [43] are possible.

Through this review it is obvious that the BIID approached reinstates the three principles of (1) provides both behavior and knowledge based detection methods (2) provides both batch mode and real time analysis in intrusion detection system (3) provides both standalone and distributed intrusion detection. Nevertheless, the performance evaluation study in terms of intrusion detection time is lacking. By exploring into the detection time, the BIID system operations will be boosted. It is clear that the reviewed approaches are only offering the intrusion detection. In order to cater more autonomous networks these biologically inspired approaches may be extended to offer intrusion handling, where the system will be able to detect and rectify the intrusion to provide continuous availability and survivability. This way, intrusion detection is detected and resolved independently without external intervention.

REFERENCES

[1] L. C. Jain, S. C. Tan and C. P. Lim. 2008. “An Introduction to Computational Intelligence,” in Computational Intelligence: Principles and Applications, pp. 1–35.

[2] E. Tyugu. 2011. “Artificial intelligence in cyber defense,” 2011 3rd Int. Conf. Cyber Confl., pp. 1–11, 2011.

[3] G. G. Keswani. 2013. “Artificial Intelligence- Is Our Future Bright or Bleak,” Int. J. Eng. Adv. Technol., Vol. 2, No. 4, pp. 348–350.

[4] M. S. Bittermann. 2010 “Artificial Intelligence (AI) versus Computational Intelligence (CI) for treatment of complexity in design,” no. Ci.

[5] L. Magdalena. 2010. “What is Soft Computing? Revisiting Possible Answers,” Int. J. Comput. Intel. Syst., Vol. 3, No. 2, p. 148.

[6] F. Dressler and O. Akan. 2010 “Bio-inspired networking: from theory to practice,” Commun. Mag. IEEE, no. November, pp. 176–183.

[7] B. Uppalaiah, K. Anand, B. Narsimha, S. Swaraj and T. Bharat. 2012. “Genetic Algorithm Approach to Intrusion Detection System 1 1, 3,” Engineering, Vol. 8491, pp. 156–160.

[8] O. Linda, T. Vollmer, and M. Manic, “Neural Network based Intrusion Detection System for critical infrastructures,” 2009 Int. Jt. Conf. Neural Networks, pp. 1827–1834, 2009.

[9] G. Wang, J. Hao, J. Ma, and L. Huang, “A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering,” Expert Syst. Appl., vol. 37, no. 9, pp. 6225–6232, 2010.

[10] J. Shun and H. A. Malki, “Network Intrusion Detection System Using Neural Networks,” 2008 Fourth Int. Conf. Nat. Comput., vol. 5, pp. 242–246.

[11] R. Beghdad, “Critical study of neural networks in detecting intrusions,” Comput. Secur., vol. 27, no. 5–6, pp. 168–175, 2008.

[12] C. M. Ou, “Host-based intrusion detection systems adapted from agent-based artificial immune systems,” Neurocomputing, vol. 88, pp. 78–86, 2012.

[13] S. T. F. Al-Janabi and H. A. Saeed, “A Neural Network Based Anomaly Intrusion Detection System,” 2011 Dev. E-systems Eng., pp. 221–226.

[14] J. Nilsson, “Vulnerability scanners,” Royal Institute of Technology, Stockholm, 2006.

[15] Prolexic, “Prolexic Quarterly Global DDoS Attack Report,” 2012.

[16] L. M. Ibrahim, “Anomaly Network Intrusion Detection System Based on Distributed Time-Delay Neural Network (Dtdnn),” Sci. Technol., vol. 5, no. 4, pp. 457 – 471, 2010.

[17] M. A. M. M. A. N. B. Mohammad Sazzadul Hoque, “An Implementation Of Intrusion Detection System Using Genetic Algorithm,” Int. J. Netw. Secur. Appl., vol. 4, no. 2, pp. 109–120, 2012.

[18] T. Vollmer, J. Alves-Foss, and M. Manic, “Autonomous rule creation for intrusion detection,” IEEE SSCI 2011 Symp. Ser. Comput. Intell. - CICS 2011 2011 IEEE Symp. Comput. Intell. Cyber Secur., pp. 1–8.

[19] Prolexic, “Prolexic Attack Report,” 2011.

[20] Prolexic, “Prolexic Attack Report,” 2012.

[21] N. Wattanapongsakorn, S. Srakaew, E. Wonghirunsombat, C. Sribavonmongkol, T. Junhom, P. Jongsubsook, and C. Charnsripinyo, “A practical network-based intrusion detection and prevention system,” Proc. 11th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. - 11th IEEE Int. Conf. Ubiquitous Comput. Commun. IUCC-2012, pp. 209–214.

[22] Prolexic, “Prolexic Quarterly Global DDoS Attack Report,” 2013.

[23] Prolexic, “Prolexic Quarterly Global DDoS Attack Report,” 2014.

[24] Y. Yu, “A survey of anomaly intrusion detection techniques,” J. Comput. Sci. Coll., pp. 9–17, 2012.

[25] A. Gupta, B. Singh Bhati, and V. Jain, “Artificial Intrusion Detection Techniques: A Survey,” Int. J. Comput. Netw. Inf. Secur., vol. 6, no. 9, pp. 51–57, 2014.

[26] G. Fedynyshyn, M. Chuah, and G. Tan, “Detection and classification of different botnet C&C channels,” Auton. Trust. Comput., pp. 228–242, 2011.

[27] P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, “Anomaly-based network intrusion detection: Techniques, systems and challenges,” Comput. Secur., vol. 28, pp. 18–28, 2009.

[28] H. Kaur and N. Gill, “Host based Anomaly Detection using Fuzzy Genetic Approach (FGA),” Int. J. Comput. Appl., vol. 74, no. 20, pp. 5–9, 2013.

[29] E. Biermann, E. Cloete, and L. Venter, “A comparison of Intrusion Detection systems,” Comput. Secur., vol. 20, no. 8, pp. 676–683, 2001.

[30] T. Verwoerd and R. Hunt, “Intrusion detection techniques and approaches,” Comput. Commun., vol. 25, no. 15, pp. 1356–1365, 2002.

[31] F. A Barika, K. Hadjar, and N. E. L. Kadhi, “Artificial Neural Network for Mobile IDS Solution,” Secur. Manag., pp. 271–277, 2009.

[32] F. Barani, “A hybrid approach for dynamic intrusion detection in ad hoc networks using genetic algorithm and artificial immune system,” 2014 Iran. Conf. Intell. Syst., pp. 1–6.

[33] A. S. Eesa, Z. Orman, and A. M. A. Brifcani, “A novel feature-selection approach based on the cuttlefish optimization algorithm for intrusion detection systems,” Expert Syst. Appl., vol. 42, no. 5, pp. 2670–2679, 2015.

[34] M. Sliem, N. Salmi, and M. Ioualalen, “Towards Reliability and Performance Prediction of Autonomic Systems with Self-Healing and Protection,” 2014 Int. Conf. Cloud Auton. Comput., pp. 35–43.

[35] M. S. A. Khan, “Rule based Network Intrusion Detection using Genetic Algorithm,” Int. J. Comput. Appl., vol. 18, no. 8, pp. 26–29, 2011.

[36] M. K. Goyal and A. Aggarwal, “Composing signatures for misuse intrusion detection system using genetic algorithm in an offline environment,” Adv. Intell. Syst. Comput., vol. 176 AISC, no. VOL. 1, pp. 151–157, 2012.

[37] D. K. Barman and N. Delhi, “Design of Intrusion Detection System Based on Artificial Neural Network and Application of Rough Set,” Int. J. Comput. Sci. Commun. Networks, vol. 2, no. 4, pp. 548–552, 2012.

[38] K. S. Devikrishna, B. B. Ramakrishna, M. Tech, and C. Science, “An Artificial Neural Network based Intrusion Detection System and Classification of Attacks,” Int. J. Eng. Res. Appl., vol. 3, no. 4, pp. 1959–1964, 2013.

[39] D. Edwards, S. Simmons, and N. Wilde, “Prevention, Detection and Recovery from Cyber-Attacks Using a Multilevel Agent Architecture,” Syst. Syst. Eng. 2007. SoSE ’07. IEEE Int. Conf., pp. 1–6.

[40] O. L. Salah Eddine Benaicha, Lalia Saoudi, Salah Eddine Bouhouita Guermeche, “Intrusion Detection System Using Genetic Algorithm,” in Science and Information Conference, 2014, vol. 1, pp. 564–568.

[41] C.-H. Wu, “Behavior-based spam detection using a hybrid method of rule-based techniques and neural networks,” Expert Syst. Appl., vol. 36, no. 3, pp. 4321–4330, 2009.

[42] M. H. Dave and S. D. Sharma, “Improved Algorithm for Intrusion Detection Using Genetic Algorithm and SNORT,” Int. J. Emerg. Technol. Adv. Eng., vol. 4, no. 8, pp. 273–276, 2014.

[43] J. Kim, P. J. Bentley, U. Aickelin, J. Greensmith, G. Tedesco, and J. Twycross, “Immune system approaches to intrusion detection - A review,” Nat. Comput., vol. 6, no. 4, pp. 413–466, 2007.

[44] M. A. Agangiba, “A Survey of Real-Time Fault-Detection Schemes in Mobile Computing,” no. May 2013, pp. 466–469.

[45] M. M. Hassan, “Network Intrusion Detection System Using Genetic Algorithm and Fuzzy Logic,” Int. J. Innov. Res. Comput. Commun. Eng., vol. 1, pp. 1435–1445, 2013.

[46] O. Oriola, A. Adeyemo, and A. Robert, “Distributed Intrusion Detection System Using P2P Agent Mining Scheme,” African J. Comput. ICT, vol. 5, no. 2, pp. 3–10, 2012.

[47] Prolexic, “Prolexic Quarterly Global DDoS Attack Report,” Prolexic, 2014.

[48] F. Z. F. Zhou and G. Y. G. Yang, “Network Intrusion Detection Using Rough Sets Based Parallel Genetic Algorithm Hybrid Model,” Intell. Inf. Process. Trust. Comput. (IPTC), 2010 Int. Symp., 2010.

[49] S. Selvakani and R. Rajesh, “Genetic Algorithm for framing rules for Intrusion Detection,” Int. Jounal Comput. Sci. Netw. Secur., vol. 7, no. 11, p. 285, 2007.

[50] K. G. Srinivasa, S. Chandra, S. Kajaria, and S. Mukherjee, “IGIDS: Intelligent intrusion detection system using genetic algorithms,” 2011 World Congr. Inf. Commun. Technol., pp. 852–857.

[51] M. Padmadas, N. Krishnan, J. Kanchana, and M. Karthikeyan, “Layered approach for intrusion detection systems based genetic algorithm,” in 2013 IEEE International Conference on Computational Intelligence and Computing Research, 2013, pp. 1–4.

[52] Y. Chen, “NeuroNet: Towards an intelligent internet infrastructure,” 2008 5th IEEE Consum. Commun. Netw. Conf. CCNC 2008, pp. 543–547.

[53] P. Salvador, a. Nogueira, U. Franca, and R. Valadas, “Framework for Zombie Detection Using Neural Networks,” 2009 Fourth Int. Conf. Internet Monit. Prot., pp. 14–20.

[54] Ahmad, A. B. Abdullah, and A. S. Alghamdi, “Application of artificial neural network in detection of DOS attacks,” Proc. 2nd Int. Conf. Secur. Inf. networks, no. Isiea, pp. 229–234, 2009.

[55] O. S. B.Sirisanyalak, “An Artificial Immunity-Based Spam Detection System,” in IEEE Congress on Evolutionary Computation (CEC 2007),pp. 3392–3398.

[56] R. L. Fanelli, “A hybrid model for immune inspired network intrusion detection,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 5132 LNCS, pp. 107–118, 2008.

[57] G. Gianini, M. Anisetti, A. Azzini, V. Bellandi, E. Damiani, and S. Marrara, “An artificial immune system approach to anomaly detection in multimedia ambient intelligence,” 2009 3rd IEEE Int. Conf. Digit. Ecosyst. Technol. DEST ’09, no. Section II, pp. 502–506.

[58] R. C. R. Chao and Y. T. Y. Tan, “A Virus Detection System Based on Artificial Immune System,” 2009 Int. Conf. Comput. Intell. Secur., vol. 1.

[59] Q. Hu and Y. Tang, “A network security evaluate method base on AIS,” Proc. - 2010 Int. Forum Inf. Technol. Appl. IFITA 2010, vol. 2, pp. 42–45.

[60] T. S. Sobh and W. M. Mostafa, “A cooperative immunological approach for detecting network anomaly,” Appl. Soft Comput. J., vol. 11, no. 2011, pp. 1275–1283.

[61] Y. Zhang, L. Wang, and W. Sun, “Artificial immune system based intrusion detection in a distributed hierarchical network architecture of smart grid,” Power Energy …, vol. 43606, pp. 1–8, 2011.

[62] Yang, T. Wang, C. MingLiu, and B. Li, “Improved Agent Model for Network Security Evaluation Based on AIS,” 2011 Fourth Int. Conf. Intell. Comput. Technol. Autom., vol. 1, pp. 151–154.

[63] M. S. A. Ansari and M. Inamullah, “Misbehavior detection in Mobile ad hoc Networks using Artificial Immune System approach,” 2011 Fifth IEEE Int. Conf. Adv. Telecommun. Syst. Networks, vol. 23, no. 0016, pp. 1–6.

[64] G. V. P. Kumar and D. K. Reddy, “An Agent Based Intrusion Detection System for Wireless Network with Artificial Immune System (AIS) and Negative Clone Selection,” 2014 Int. Conf. Electron. Syst. Signal Process. Comput. Technol., pp. 429–433.

[65] A. S. a Aziz, “Artificial Immune System Inspired Intrusion Detection System Using Genetic Algorithm 2 Background,” Informatica, vol. 36, no. 2012, pp. 347–357.

[66] S. Mabu, C. Chen, N. Lu, K. Shimada, and K. Hirasawa, “An Intrusion-Detection Model Based on Fuzzy Class-Association-Rule Mining Using Genetic Network Programming,” IEEE Trans. Syst. Man, Cybern. Part C Appl. Rev., vol. 41, no. January 2011, pp. 130 –139.

[67] P. Jongsuebsuk, N. Wattanapongsakorn, and C. Charnsripinyo, “Real-time intrusion detection with fuzzy genetic algorithm,” 2013 10th Int. Conf. Electr. Eng. Comput. Telecommun. Inf. Technol. ECTI-CON 2013.

[68] Y. Z. Y. Zhou, “Hybrid Model Based on Artificial Immune System and PCA Neural Networks for Intrusion Detection,” 2009 Asia-Pacific Conf. Inf. Process., vol. 1, pp. 21–24, 2009.

[69] A. F. Shosha, P. Gladyshev, S. S. Wu, and C. C. Liu, “Detecting cyber intrusions in SCADA networks using multi-agent collaboration,” 2011 16th Int. Conf. Intell. Syst. Appl. to Power Syst. ISAP 2011, pp. 1–7.

[70] S. A. Kumar, “Adaptive Genetic Algorithm Model for Intrusion Detection,” Indian J. Comput. Sci. Eng., vol. 3, no. 4, pp. 595–599, 2012.

[71] J. Z. Lei and A. a. Ghorbani, “Improved competitive learning neural networks for network intrusion and fraud detection,” Neurocomputing, vol. 75, no. 1, pp. 135–145, 2012.

[72] F. Haddadi, S. Khanchi, M. Shetabi, and V. Derhami, “Intrusion Detection and Attack Classification Using Feed-Forward Neural Network,” Comput. Netw. Technol. (ICCNT), 2010 Second Int. Conf., pp. 1112–1115.

[73] Mohammadi A. Akbari B. Raahemi B. Nassersharif and H. Asgharian. 2013. “A fast anomaly detection system using probabilistic artificial immune algorithm capable of learning new attacks,” Evol. Intell., Vol. 6, No. 2014, pp. 135–156.

[74] R. Ahmed, X. Huang, and D. Sharma. 2012. “A Novel Framework for Abnormal Behaviour Identification and Detection for Wireless Sensor Networks,” pp. 431–434.

[75] Ratnawat and P. A. Jain. 2014. “A Novel Intrusion Detection System Using Neural-Fuzzy Classifier for Network Security,” Int. J. Emerg. Technol. Adv. Eng., Vol. 4, No. 6, pp. 900–905.