International Journal of Engineering Technology and Applied Science

(ISSN: 2395 3853), Vol. 3 Issue 12 December 2017

A Comparative Analysis of Different Approaches of Hybrid Immune Intrusion Detection System Inspired by HIS

[1]Pooja Tiwari, [2]R. N. Sharma
[1]M-Tech Scholar, [2]Assistant Professor
[12]Department of Computer Science Engineering, MPCT, Gwalior
(tpooja121@gmail.com, ramcse1983@gmail.com)

Abstract- Increased connectivity and also the use of the web have exposed the security and safety issue in front of the organizations, therefore need to use of intrusion detection system to protect data system and communication network from malicious attacks or unauthorized access. Associate intrusion detection system (IDS) may be a security system that monitors laptop systems and network traffic, analyze that traffic to spot attainable security breaches and lift alerts. Associate IDS triggers thousands of alerts per day that is tough for human users to investigate them and take acceptable actions. It's vital to cut back the warning alerts, showing intelligence integrate and correlate them so as to present a high level read of the detected security issue to the administrator.

Keywords: NIDS, Detection Approachs, Hybrid or Advanced Immune System, AIDS.

1. INTRODUCTION

Now a day's development of any country or origination is depending upon its information technology system and all the information whether it's confidential, personal or public is shared through internet or network. So any country or organization needs to develop their information sharing network throughout the world with rapid speed. There is a rapid development in making such types of networks which available worldwide and have confidential information. But some time the intruder can attack over network where network based or client based firewall not capable enough to provide complete security against these types of threads [1].

Computer security is a very important issue to any or all users of pc systems. The rise of the web, pc attacks are increasing and may simply cause numerous dollar harm to a corporation. Detection of those attacks is a very important issue of pc security. Intrusion Detection Systems (IDS) technology is a good approach in addressing the issues of network security. The main objective of Intrusion Detection System is to observe unauthorized use, misuse and abuse of pc systems and laptop by each systems insiders and external intruders. There are many strategies following implement intrusion detection like statistical analysis knowledgeable systems, and state transition approaches etc., and these many approaches is based on the system were planned in recent years[2].

In order to provide complete security against these word wide thread IDS system play a key role. IDS system identifies the unauthorized activity that compromise the integrity, confidentially and availability of confidential information [2].

Conventional IDS is based on continuous monitoring of well know attack by their extensive knowledge of signature to detect intrusion. This method based on pattern recognitions of various audit streams and detect intrusion by comparing their pattern provide by human expert. The pattern has been manually revised for a new type of intrusion whenever discover. The basic limitation of this pattern based Method is cannot detect emerging cyber thread.

Artificial Immune System is an emerging technology in order to fine the intruders or making the IDS. Recently AIS is a new bio-inspired model, which is applied for solving various security problems in the field of information security, genetic algorithms, neural networks, evolutionary algorithms and swarm intelligence [4]. As one of the solutions to intrusion detection problems, AIS have shown their advantages. To improve the correlation factor and minimizing the false alarm generation we used the concept of AIS and Dempster-Belief theory (DBT) to identify the intrusion in the system.

2. OVERVIEW OF SECURITY IN NETWORK

Information and resources should be protected over the network. As security is one of the main issues in WSN. Also misbehavior of the nodes should be handled. Below are the main security goals or services [3]:

2.1 Security goals:

Security model that is designed to act as a guide for information security policies. For data to be completely secure, all of these security goal must come to effect.

• Confidentiality: Confidentiality means that the information is available or accessible to the authorized users only. It is the most important security goal. To achieve confidentiality Encryption with security key is used.

• Availability: Data should be available to the authorized user whenever needed despite of any internal or external attacks i.e. DoS attack.

• Integrity: Data should not be altered or manipulated by adversary as it travels from sender to the recipient.

• Authentication: Data originates from confirming that identity data and identified sender with which the node is communicating in the network.

• Non-repudiation: Non-repudiation means a previously send message cannot be denied by a node in a WSN.

• Authorization: Network services or resources can only be accessed by authorized nodes.

• Freshness: Data should be recent it is very important goal for WSNs it ensures that only new messages are received but not the replayed messages of the adversary.

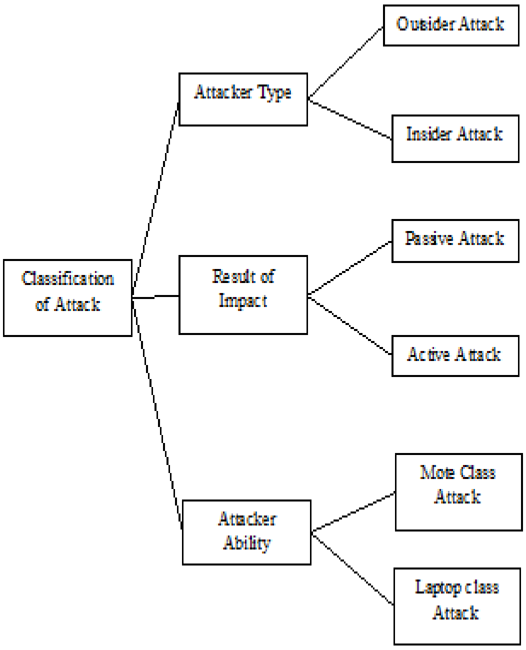

Figure 1: Classification of Attacks in Networks

Figure1 shows the classification of attacks in network: Attacker type, Result of impact, Attackers ability.

2.2 Possible security attacks in WSN [3-4]:

1) Passive Information**:** Gathering Information is gathered by adversary if the information is not in encrypted format with the help of powerful resource.

2) Subversion of node: Captured node reveals all information including cryptographic keys of the whole sensor network.

3) False Node: False malicious data is injected with the help of malicious node by an adversary.

4) Node Malfunction: Inaccurate data is generated by malfunction node which would affect the integrity of sensor network it would be more dangerous if node is cluster head.

5) Node Outage: If a cluster leader node is not working or dead then alternate route should be provided for the proper and secure function of the network.

6) Message Corruption: Message integrity is compromised when a message is modified by an attacker.

7) Traffic Analysis: Traffic is analyzed on the bases of communication pattern. Encrypted messages are analyzed.

8) Routing loops: In this type of attack the data exchanged between nodes is the main target when the attacker replays or alters the routing data and false error messages are generated. Latency is increased because data move between the loops.

9) Selective forwarding: In this attack, attacker node simply drops some of the messages i.e. it does not forward all the messages received by it. Its Effectiveness depends upon two factors: Malicious node location more traffic it will attract if it is closer to the base station and second is percentage of messages dropped by it.

10) Sinkhole attacks: In this attack adversary node attracts most of the network traffic. Sinkhole is created by placing the compromised node closer to the base station, where it attracts most of the traffic.

11) Sybil attacks: during this attack, malicious node creates multiple identities by stealing the identities of legitimate nodes or by fabricating it. Topology maintenance and routing algorithms are stricken by Sybil attacks.

12) Wormholes: during this style of attack a tunnel is made with low latency by the antagonist close to the bottom station making a sink.

13) Hello flood attacks: during this style of attack a hi message is broadcasted simulation the message is returning from base station with stronger transmission power. Nodes receiving hi message send their messages through antagonist node. Plenty of energy is wasted by the nodes.

15) DOS attacks: In Denial of service is physical layer attack includes battery exhaustion, radio jam, and meddling network protocol occur at physical level.

3. INTRUSION DETECTION SYSTEM

Intrusion interference needs a well-selected combination of “baiting and trapping” geared toward each investigations of attacker’s. A musing the intruder’s attention from protected resource is another task of IDS. Information generated by intrusion detection systems is rigirous examined (this is the main task of every IDS) for detection of attainable attacks or intrusion.

The role of the device is to filter data and discard in applicable information can be obtained from the event set related to suspicious activities. The device is integrated with the element chargeable for information assortment from a happening generator. The gathering manner is decided by the event generator policy that defines the filtering mode of event notification data. The event generator produces a policy –consistent set of event that will be a log (or audit) of system events, or network packets.

In sure cases, no information storage is utilized once event information streams are transferred on to the instrument .Once associate intrusion has been detected, IDS problems alerts notifying directors of this reality. consecutive step is undertaken either by the directors or the IDS itself, by taking advantage of extra counter measures (specific block functions to terminate sessions, backup systems, routing connections to a system trap, legal infrastructure etc.) [1, 2].

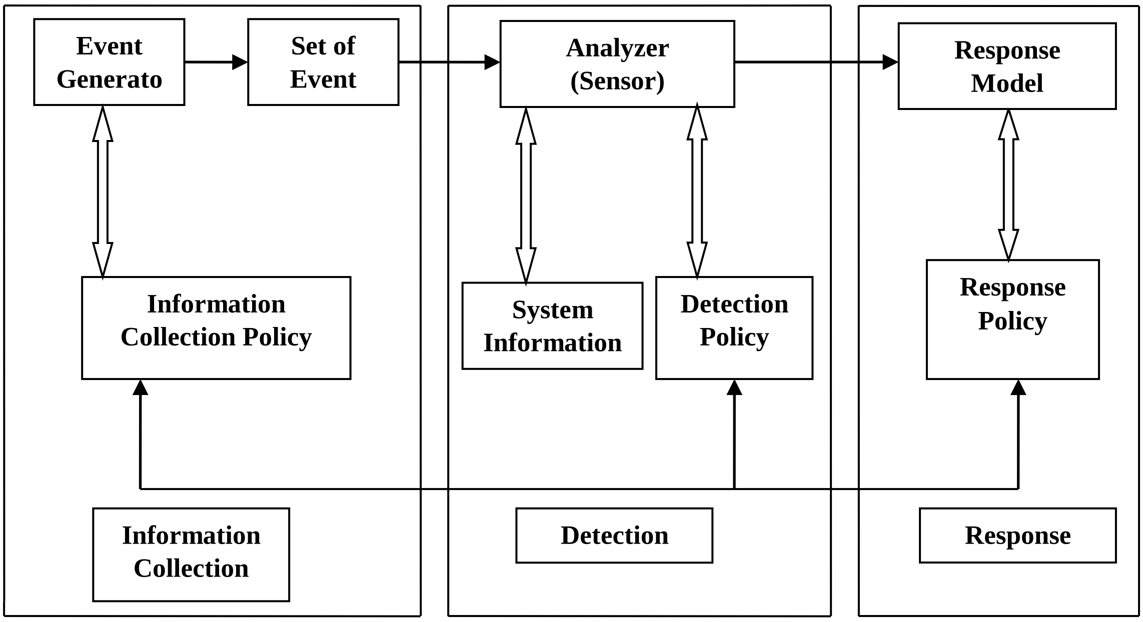

Figure 2 :Components of IDS

Figure 2 shows the element of IDS. Associate intrusion detection systems perpetually has its core element- a device works as associate analysis engine chargeable for detection intrusions. This device contains decision- creating mechanisms concerning intrusion. Device receives information from three major data sources: own IDS, content, system log and audit trails. The system log might embody configuration of filing system, user authorization etc. This data is made on the premise of an additional decision-making method [1, 2].

An IDS is part of the safety policy. Among numerous IDS tasks, trespasser identification is one in all the basic ones. It will be helpful within the rhetorical analysis of incidents and putting in applicable patches to change the detection of future attack tries targeted on specific persons or resources. Intrusion detection might typically turn out false alarms, as an example as a results of out of whack network interface or causation attack description or signatures via email [2].

Intrusion detection is that the method of observance the events occurring in an exceedingly ADPS or network [2]. The aim of IDS is to research the traffic that goes through it and to notice attainable intrusions to the system. Associate IDS is a crucial a part of the policies associated with security problems. IDS will freeform numerous task however identification of intruders is one in all the foremost basic perform. It helps in gathering the proof in laptop crime. It additionally helps within the analysis of digital rhetorical so as to know the activity of aggressor.

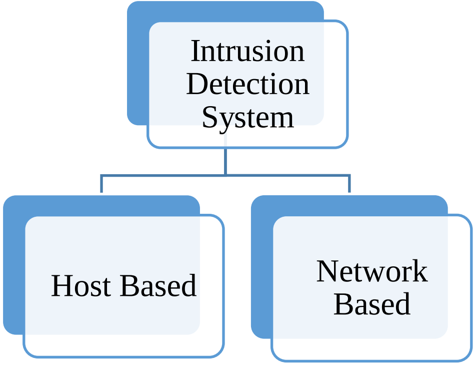

Figure 3: Classifications of IDS

Figure3 shows there are essentially two forms of intrusion detection system.

•**Host-based intrusion detection system:** HIDSs measure info found on a single or multiple host systems, together with contents of operative systems, system and application files.

•**Network based mostly Intrusion Detection:** NIDSs measure infoemation captured from network communications, analyzing the stream of packets that travel across the network.

There are many completely different types of techniques used in Intrusion detection system.

These embody statistical anomaly techniques, fuzzy logic techniques, rule-based anomaly techniques, rule-based penetration identification, state transition techniques, neural network based mostly, data processing techniques etc.

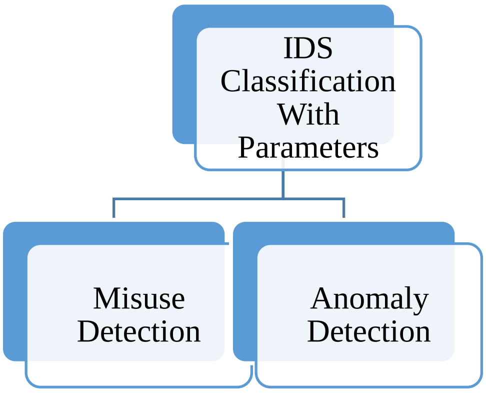

Figure 4 IDS classification with parameters

Figure4 shows the classified IDSs supported numerous parameters, Rule-based Detections and statistical Anomaly Detection [5].

Misuse detection: Misuse detections determine intrusions by matching its broad relevancy to completely different fields. Misuse detectors use pattern matching for the analysis. These detectors rummage around for events that match a predefined pattern outlined within the IDS info. Patterns like best-known attacks are known as signatures and keep in signature info. If match happens, it means that intrusion has been detected. Misuse detection is typically known as "signature based mostly detection." therefore whenever event happens, it's picked up and its pattern is matched with the hold on patterns. If match is found then it implies that Intrusion is there. Misuse detection can fail simply once facing unknown intrusions. a method to deal with this drawback is too often update the cognitive content, either manually that is time intense and arduous, or mechanically with the assisting of supervised learning algorithms. Unfortunately, datasets for this purpose are typically valuable to organize, as they need labeling of every instance within the dataset as traditional or a sort of intrusion. in our own way to resolve this drawback is to follow the anomaly detection model [1, 2].

Anomaly detection: Anomaly detection has the aptitude of detecting new forms of intrusions, and solely needs traditional knowledge once building profiles. However, its major problem lies in discovering boundaries between traditional and abnormal behavior, attributable to the deficiency of abnormal samples within the training part.The anomaly-based detection is very hard to handle: it is really difficult to associate an alarm with the specific event that triggered the alarm. The system is very complex. It is not sure that the alarm is going to be triggered if the intrusive activity is too close to the "Normal" activity or the "Abnormal activity".

For above mention approaches which have used in intrusion detection system their comparison is also mandatory for the study or analysis. In this comparative analysis we have discussed three techniques like signature or pattern based, anomaly based and last but not the least hybrid approach which is our propose methodology. The comparative analysis of these techniques with different characteristics shown in the table 1. In which we have describe these technique at different parameter.

Parameter	Anomaly approach	Signature approach	Hybrid approach
Space Utilization	Min	Min	Average
Power Consumption	Min	Min	Average
Detected Rate	Average	Average	Good
False Alarm	Medium	Medium	Lower
Degree Of Potency	It Has Capacity To Detection Of New Attacks	It Has Detect Only Those Attach Which Have Some Kind of Signature or Pattern	It Has Detect Both Kind Of Attack Existing And New Attack
Weak Point	It Misses Well Known Attack	It Can Not Detect New Attack	It Has Needed More Resources and Computation

Table 1: describe the comparative analysis of these three techniques depend upon different characteristics.

4. LITERATURE SURVEY

In this paper we present on overview of existing intrusion detection techniques for detection DOS attacks. Intrusion detection system in a very popular and computationally expensive task. We describe today's approaches for intrusion detection system that have been developed we will compare the most important ones.

Muhammad Asif Manzoor et al. proposed, [7] Network intrusion detection is crucial part of network management for security, quality of service and different functions. These systems enable early detection of network intrusion and malicious activities; supported this detection, applicable actions may be applied to manage these attacks. Many network intrusion detection systems are projected and evaluated and plenty of them are presently in use to produce higher security. Currently, pc networks are generating high volume of information traffic that can't be analyzed by most network intrusion detection systems. This example needs new techniques that may handle immense volume of real time knowledge traffic and it should maintain the high output. We have projected to network intrusion system supported support vector machine during this work. We tend to conjointly propose to use Apache Storm framework; that could be a period of time distributed stream process framework. This network intrusion system is tested for KDD 99 network intrusion dataset.

J. M. Gore Vidal et al projected, [8] this paper presents an alert correlation system for mitigating the false positives downside on network-based intrusion detection, once abnormal detection techniques are applied. The system permits the quantitative assessment of the probability that an alert issued as a result of an anomaly becomes a real threat. To try and do this the variations between the characteristics of the model representing the habitual and legit network usage are taken under consideration, yet because the most representative options of the traffic that generated the alert.

ManjariJha, dominion Acharya et al. [9] projected that**,** the system is made to defend an organism against each well-known and new attacks, and functions as an adaptation distributed defense system. Artificial Immune Systems abstract the structure of immune systems to include memory, fault detection and adaptation learning. We have a tendency to propose a system based mostly real time intrusion detection system using unsupervised cluster. The model consists of two layers: a probabilistic model based mostly T-cell algorithmic program that identifies potential attacks, and a choice tree based mostly B-cell model that uses the output from T-cells alongside feature info to verify true attacks. The algorithmic program is tested on the KDD 99 knowledge, wherever it achieves an occasional warning rate whereas maintaining a high detection rate. This can be true even just in case of novel attacks, that could be an important improvement over different algorithms.

PriyankaSuyal et al. [10] proposed that information and communication technology inflate day by day, attributable to speedy improvement in technologies has redoubled the necessity of effective IDS (Intrusion Detection System). Here, Intelligent Intrusion Detection methodology that's Rough Set based mostly approach conferred for performance analysis of classifier abnormal behavior. Rough pure mathematics is employed to cut back the input file house, from advanced databases and notice bottom call rules or redact, through this we will manage complexness of system and manage Brobdingnagian network traffic. Rough set based or based mostly or primarily based mostly effective classification models particularly Rule based classifier algorithmic program with discretization, Decomposition tree algorithmic program and Decomposition tree with discretization are applied to search out reduced call rules and classify downside. Comparison of classification results even have perform with varied analysis criteria and acknowledge best suited classifier for intrusion detection system dataset.

Latifur Khan et al. [11] proposed that, whenever an intrusion happens, the protection and price of an ADP system is compromised. Network-based attacks create it troublesome for legitimate users to access varied network services by advisedly occupying or sabotaging network resources and services. This could be done by causation giant amounts of network traffic, exploiting well-known faults in networking services, and by overloading network hosts. Intrusion Detection makes an attempt to notice pc attacks by examining varied knowledge records determined in processes on the network and its split into 2 teams, anomaly detection systems and misuse detection systems. Anomaly detection is a trial to go looking for malicious behavior that deviates from established traditional patterns. Misuse detection is employed to spot intrusions that match well-known attack situations. Our interest here is in anomaly detection and our projected methodology could be an ascendible resolution for detective work network based mostly anomalies. We have a tendency to use Support Vector Machines (SVM) for classification. The SVM is one of the most successful classification algorithms in the data mining area, but it's long training time limits its use.

Safwan Mawlood Hussein et al. [12]proposed that the speedily growth of technology, used web become a crucial part in human life it employed in several sectors of society, communication over international network, sending or receiving sensitive information is risk because totally different techniques are employed by attackers to intercept and exposed information. As a result, robust security technique is needed to guaranteeing the user information. Several strategies planned to boost security problems. Intrusion detection system (IDS) is employed to watch unwanted action on network systems and individual computers. But because of opposite impact of using IDS, using individual strategies of IDS solely misuse or anomaly attacks will be detected. During this paper they planned a model that integrates each approaches signature and anomaly based mostly of IDS to scale back obtained alerts and detects new attacks. false alarm rate, accuracy, and sight attacks are the parameters wont to assess effectiveness of hybrid IDS additionally data Discovery data processing (KDD) CUP 99 dataset and Waikato setting for data Analysis (WEKA) program has been used for testing the planned hybrid IDS.

Chao Deng et al. [13] proposed that the popularization and development of network information, network intruders are increasing, and therefore the attack mode has been updated. Intrusion detection technology could be a reasonably active defense technology, which may extract the key info from the network system, and quickly decide and shield the interior or external network intrusion. Intrusion detection could be a reasonably active security technology, that provides period protection for internal attacks, external attacks and misuse, and it plays a crucial role in making certain network security. However, with the diversification of intrusion technology, the normal intrusion detection system cannot meet the necessities of the present network security. Therefore, the implementation of intrusion detection desires diversifying. During this context, they apply neural network technology to the network intrusion detection system to unravel the matter. During this paper, on the premise of intrusion detection technique, they tend to analyze the event history and therefore the gift scenario of intrusion detection technology, and summarize the intrusion detection system summary and design. The neural network intrusion detection is split into information acquisition, information analysis, pretreatment, and intrusion behavior detection and testing.

Ahmad W. Al-Dabbagh et al. [14] proposed that a topology for a wireless networked system is studied underneath many cyber-attack situations, and a distributed intrusion detection system (IDS) is intended to spot the existence of attacks. Additional specifically, the paper presents a modelling framework for the closed-loop system with the IDS, and a procedure to style and calculate the IDS. The procedure delivers a stable closed-loop system with the IDS being sensitive to cyber-attacks. Also, a simulation example is employed let's say the appliance of the projected procedure furthermore as its effectiveness.

BisyronWahyudi et al. [15] proposed that the IDS capability in detecting associate attacks is extremely dependent on the accuracy of attack detection that typically is depicted by the smallest amount range of false alarms. During this work they tend to alter the massive network dataset by choosing solely the foremost necessary and powerful options within the dataset to extend the IDS performance and accuracy. The creation of smaller dataset is aimed to decrease time for coaching the SVM machine learning in detecting attacks. This work designed and engineered a model of IDS equipped with machine learning models to boost accuracy in detecting DoS and R2L attacks. Machine-learning algorithms is supplementary to acknowledge specific characteristics of the attack at the national web network. New ways and techniques developed by combining feature choice and parameter optimization algorithmic rule are then enforced within the net observance system. Through experiment and analysis, we discover out that for DOS attacks the planned approach improved accuracy for the detection and raised in speed on training and testing section. Even supposing restricted and acceptable choice of parameters slightly decrease the accuracy within the detection of R2L attacks but our approach considerably will increase the speed of the training and testing method.

5. MERITS OF INTRUDERS DETECTION SYSTEM

There are many advantages of IDS in the network System. Some of them discussed below:

- Can analyze what an application is doing
- Can verify the success of an attack
- Can detect attacks that do not involve the network
- No additional hardware is required
- Does not affect hosts performances
- Can detect network attacks that are not visible from single hosts

6. DEMERITS OF THE EXISTING INTRUSION DETECTION SYSTEM

Most of the existing intrusion detection systems suffer from the following problems [4]:

- First, the information used by the intrusion detection system is obtained from audit trails or from packets on a network. . Data needs to traverse an extended path from its origin to the IDS and within the method will probably be destroyed or changed by an assailant. Furthermore, the intrusion detection system needs to infer the behaviour of the system from the information collected, which may end in misinterpretations or lost events. This is often referred because the fidelity downside.
- Second, the intrusion detection system endlessly uses further resources in system its observation even once there aren't any intrusions occurring, as a result of the

parts of the intrusion detection system need to be running all the time. This is often resource usage downside.

- Third, as a result of the parts of the intrusion detection system are enforced as separate programs, they're vulnerable to tampering. Associate trespasser will probably disable or modify the programs running on a system, rendering the intrusion detection system useless or unreliable. This is often dependability downside.

7. CONCLUSION

As rapid increase in unauthorized activities and abuse of computer system by both system internal and external intruder trends to increase the degree of network security. In order to increase network security various technique has been proposed but having a deficiency over IDS system in some of the situation i.e. if correlation alarm is not precise, reduction and prevention of false positive and false negative is high , at last having insufficient measurement of pattern recognition.

REFERENCES

1) FarhoudHosseinpour, Kamalulnizam Abu Bakar, Amir HatamiHardoroudi, NazaninsadatKazazi, “Survey on Artificial Immune System as a Bio-inspired Technique for Anomaly Based Intrusion Detection Systems” International Conference on Intelligent Networking and Collaborative Systems, IEEE , pp 323-324,Nov-2010.
2) D. Barbara, N. Wu, and S. Jajodia, “Detecting novel network intrusions using bayes estimators,” Proceedings of the First SIAM International Conference on Data Mining (SDM 2001), Chicago, USA, Apr. 2001.
3) Chen, Xiangqian, Kia Makki, Kang Yen, and NikiPissinou. "Sensor network security: a survey." Communications Surveys &Tutorials,IEEE11.2 (2009): 52-73.
4) Can, Okan, and OzgurKoraySahingoz. "A survey of intrusion detection systems in wireless sensor networks." Modeling, Simulation, and Applied Optimization (ICMSAO), 2015 6th International Conference on. IEEE, 2015.
5) Maleh, Yassine, and AbdellahEzzati. "A review of security attacks and Intrusion Detection Schemes in Wireless Sensor Networks." (2014).
6) Liao, Hung-Jen, Chun-Hung Richard Lin, Ying-Chih Lin, and Kuang- Yuan Tung. "Intrusion detection system: A comprehensive review."Journal of Network and Computer Applications 36.1 (2013): 16-24.
7) Muhammad Asif Manzoor, Yasser Morgan, “Real-time Support Vector Machine Based Network Intrusion Detection System Using Apache Storm”, IEEE 2016.
8) J. M. Vidal, A. L. S. Orozco, L. J. G. Villalba, “Quantitative Criteria for Alert Correlation of Anomaly-based NIDS”, IEEE LATIN AMERICA TRANSACTIONS, VOL. 13, NO. 10, OCTOBER 2015.
9) ManjariJha, Raj Acharya, “An Immune inspired Unsupervised Intrusion Detection System for Detection of Novel Attacks”, IEEE 2016.
10) PriyankaSuyal, Janmejay Pant, AkhileshDwivedi, Manoj Chandra Lohani, “Performance Evaluation of Rough Set Based Classification Models to Intrusion Detection System”, IEEE 2016.
11) Latifur Khan · MamounAwad · BhavaniThuraisingham, “A new intrusion detection system using support vector machines and hierarchical clustering”,The VLDB Journal 2010.
12) SafwanMawlood Hussein, “Performance Evaluation of Intrusion Detection System Using Anomaly and Signature based algorithms to Reduction False Alarm Rate and Detect Unknown Attacks”, IEEE 2016.
13) Chao Deng, HaiyeQiao, “Network Security Intrusion Detection System based on Incremental Improved Convolutional Neural Network Model”, IEEE 2016.
14) [Ahmad W. Al-Dabbagh, Yuzhe Li, and Tongwen Chen, “An Intrusion Detection System for Cyber Attacks inWireless Networked Control Systems”, IEEE 2016.
15) BisyronWahyudiMasduki, KalamullahRamli, “Improving Intrusion Detection System Detection Accuracy and Reducing Learning Time by Combining Selected Features Selection and Parameters Optimization”, IEEE 2016.