International Journal of Engineering Technology and Applied Science

(ISSN: 2395 3853), Vol. 3 Issue 1 January 2017

A Survey Review on Hybrid Immune or Artificial Network Intrusion Detection System

[1]Rachna Lodhi
[2]Anoop Singh
[1]M-Tech Scholar, [2]Guide and Head of Department
[12]Department of Electronics and communication Engineering, VITS, Bhopal, India

Abstract- Increased connectivity and also the use of the internet 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 and 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.

I INTRODUCTION

Computer security is an important issue to all users of computer systems. The rapid growth of the internet, computer attacks are increasing and can easily cause millions of dollar damage to an organization. Detection of these attacks is an important issue of computer security. Intrusion Detection Systems (IDS) technology is an effective approach in dealing with the problems of network security.The main goal of Intrusion Detection System is to detect unauthorized use, misuse and abuse of computer systems by both systems insiders and external intruders. There are several methods used to implement intrusion detection such as statistical analysis expert systems, and state transition approaches etc., and these several approaches is based on the immune system were proposed in recent years[2].

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].

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 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.

II OVERVIEW OF SECURITY IN NETWORK

Security Goals

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]:

• 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 manipulatedby adversary as it travels from sender to the recipient.
• Authentication: Data originates from the 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.

Security Attacks

Figure 1 provides classification of attacks in WSN: Attacker type, Result of impact, Attackers ability.

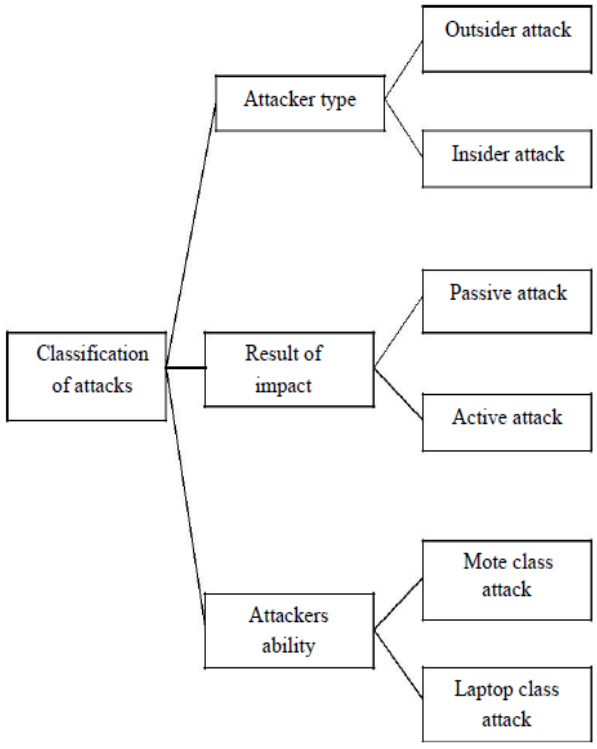

Figure 1 Classification of Attacks in Networks

Possible security attacks in WSN [3-4]:

1) Passive Information: Gathering Information is gathered by adversary if the information is notin encrypted format with the help of powerful resource.
2) Subversion of node: Captured node reveals all information including cryptographickeys of the whole sensor network.
3) False Node: False malicious data is injected with the help of maliciousnode by an adversary.
4) Node Malfunction: Inaccurate data is generated by malfunction node which wouldaffect the integrity of sensor network it would be moredangerous if node is cluster head.
5) Node Outage: If a cluster leader node is not working or dead then alternateroute should be provided for the proper and secure function ofthe network.
6) Message Corruption: Message integrity is compromised when a message ismodified 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 themain target when the attacker replays or alters the routing dataand false error messages are generated. Latency is increasedbecause data move between the loops.
9) Selective forwarding: In this attack, attacker node simply drops some of themessages i.e. it does not forward all the messages received byit. Its Effectiveness depends upon two factors: Malicious nodelocation more traffic it will attract if it is closer to the basestation and second is percentage of messages dropped by it.
10) Sinkhole attacks: In this attack adversary node attracts most of the networktraffic. Sinkhole is created by placing the compromised nodecloser to the base station, where it attracts most of the traffic.
11) Sybil attacks: In this attack, malicious node creates multiple identities bystealing the identities of legitimate nodes or by fabricating it.Topology maintenance and routing algorithms are affected bySybil attacks.
12) Wormholes: In this type of attack a tunnel is created with low latency bythe adversary near the base station creating a sinkhole.
13) Hello flood attacks: In this type of attack a HELLO message is broadcastedpretending the message is coming from base station withstronger transmission power. Nodes receiving HELLOmessage send their messages through adversary node. A lot ofenergy is wasted by the nodes.
15) DOS attacks: In Denial of service is physical layer attack includes batteryexhaustion, radio jamming, and interfering network protocol occurat physical level.

Layering Based Security Approach [3]

1) Application layer: At application layer manages data collection. So the reliability of the data should be ensured at application layer.

2) Transport Layer: Establishment of communication for external networks is the main objective of transport layer.
3) Network Layer: Network layer performs routing of messages from cluster head to base station, cluster head to cluster head, node to node, node to cluster head, cluster head to the base station and vice versa.
4) Data Link layer: Data link layer performs multiplexing of data stream, the error detection and correction, medium access control, and encryption of data.
5) Physical Layer: Physical layer focuses on Signal detection, frequency selection, carrier frequency generation, signal strength, encrypting data, media of transmission between sending and receiving nodes.

III INTRUSION DETECTION SYSTEM

Intrusion prevention requires a well-selected combination of "baiting and trapping" aimed at both investigations of attacker's. Diverting the intruder's attention from protected resource is another task of IDS. Data generated by intrusion detection systems is carefully examined (this is the main task of each IDS) for detection of possible attacks or intrusion.

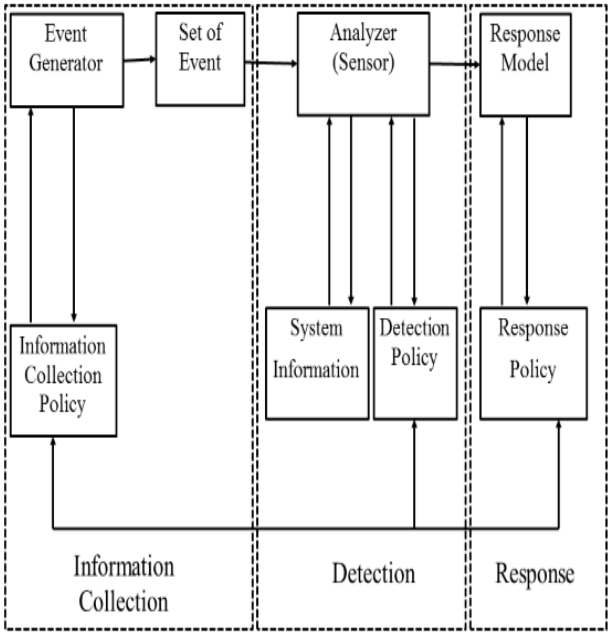

Figure 2 Components of IDS

Figure 2 shows the component of IDS .An intrusion detection systems always has its core element- a sensor works as an analysis engine responsible for detection intrusions. This sensor contains decision-making mechanisms regarding intrusion. Sensor receives raw data from three major information sources: own IDS, knowledge base, system log and audit trails. The system log may include configuration of file system, user authorization etc. This information is created on the basis of a further decision-making process [1, 2].
The role of the sensor is to filter information and discard any irrelevant data obtained from the event set associated with suspicious activities. The sensor is integrated with the component responsible for data collection from an event generator. The collection manner is determined by the event generator policy that defines the filtering mode of event notification information. The event generator produces a policy – consistent set of event that may be a log (or audit) of system events, or network packets. In certain cases, no data storage is employed when event data streams are transferred directly to the analyzer .Once an intrusion has been detected, IDS issues alerts notifying administrators of this fact. The next step is undertaken either by the administrators or the IDS itself, by taking advantage of additional counter measures (specific block functions to terminate sessions, backup systems, routing connections to a system trap, legal infrastructure etc.) [1, 2].
An IDS is an element of the security policy. Among various IDS tasks, intruder identification is one of the fundamental ones. It can be useful in the forensic research of incidents and installing appropriate patches to enable the detection of future attack attempts targeted on specific persons or resources. Intrusion detection may sometimes produce false alarms, for example as a result of malfunctioning network interface or sending attack description or signatures via email [2].
Intrusion detection is the process of monitoring the events occurring in a computer system or network [2]. The purpose of IDS is to analyze the traffic that goes through it and to detect possible intrusions to the system. An IDS is an important part of the policies related to security issues. IDS can freeform various task but identification of intruders is one of the most basic function. It helps in gathering the evidence in computer crime. It also helps in the research of digital forensic in order to understand the activity of attacker.
There are basically two types of intrusion detection system:

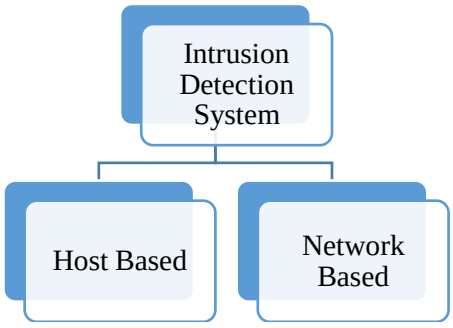

Figure 3 Classifications of IDS

- **Host-based intrusion detection system:** HIDSs evaluate information found on a single or multiple host systems, including contents of operating systems, system and application files.
- **Network based Intrusion Detection**: NIDSs evaluate information captured from network communications, analyzing the stream of packets which travel across the network.

There are several different kinds of techniques used to design Intrusion detection system. These include statistical anomaly techniques, fuzzy logic techniques, rule-based anomaly techniques, rule-based penetration identification, state transition techniques, neural network based, data mining techniques etc. William Stallings [6] classified IDSs based on various parameters, Rule-based Detections and Statistical Anomaly Detection.

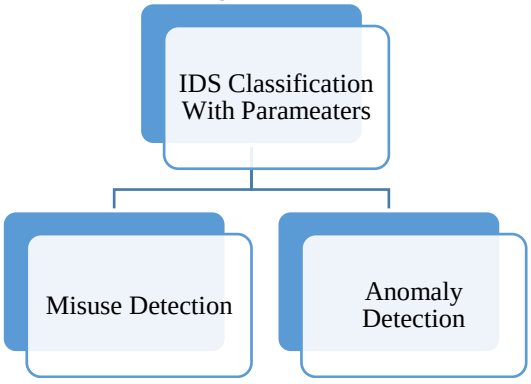

Figure 4 IDS classification

Misuse detection: Misuse detections identify intrusions by matching its broad applicability to different fields. Misuse detectors use pattern matching for the analysis. These detectors look for events which match a predefined pattern defined in the IDS database. Patterns corresponding to known attacks are called signatures and stored in signature Database. If match occurs, it means intrusion has been detected. Misuse detection is sometimes called "signature based detection." So whenever event occurs, it is picked up and its pattern is matched with the stored patterns. If match is found then it means that Intrusion is there. Misuse detection will fail easily when facing unknown intrusions. One way to address this problem is to regularly update the knowledge base, either manually which is time consuming and laborious, or automatically with the help of supervised learning algorithms. Unfortunately, datasets for this purpose are usually expensive to prepare, as they require labeling of each instance in the dataset as normal or a type of intrusion. Another way to solve this problem is to follow the anomaly detection model [1, 2].

Anomaly detection: Anomaly detection has the capability of detecting new types of intrusions, and only requires normal data when building profiles. However, its major difficulty lies in discovering boundaries between normal and abnormal behavior, due to the deficiency of abnormal samples in the training phase. 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".

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

PARAMETER	ANORMALY 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

IV LITERATURE SURVEY

Muhammad Asif Manzoor et al. proposed, [25] Network intrusion detection is critical component of network management for security, quality of service and other purposes. These systems allow early detection of network intrusion and

malicious activities; based on this detection, appropriate actions can be applied to manage these attacks. Several network intrusion detection systems are proposed and evaluated and many of them are currently in use to provide better security. Currently, computer networks are generating high volume of data traffic which cannot be analyzed by most network intrusion detection systems. This situation requires new techniques that can handle huge volume of real time data traffic and it must maintain the high throughput. We have proposed to network intrusion system based on support vector machine in this work. We also propose to use Apache Storm framework; which is a real-time distributed stream processing framework. This network intrusion system is tested for KDD 99 network intrusion dataset.

J. M. Vidal et al proposed, [26] this paper presents an alert correlation system for mitigating the false positives problem on network-based intrusion detection, when anomalous detection techniques are applied. The system allows the quantitative assessment of the likelihood that an alert issued because an anomaly becomes a real threat. To do this the differences between the characteristics of the model representing the habitual and legitimate network usage are taken into account, as well as the most representative features of the traffic that generated the alert.

ManjariJha, Raj Acharya proposed paper, [27] the immune system is built to defend an organism against both known and new attacks, and functions as an adaptive distributed defense system. Artificial Immune Systems abstract the structure of immune systems to incorporate memory, fault detection and adaptive learning. We propose an immune system based real time intrusion detection system using unsupervised clustering. The model consists of two layers: a probabilistic model based T-cell algorithm which identifies possible attacks, and a decision tree based B-cell model which uses the output from T-cells together with feature information to confirm true attacks. The algorithm is tested on the KDD 99 data, where it achieves a low false alarm rate while maintaining a high detection rate. This is true even in case of novel attacks, which is a significant improvement over other algorithms.

Priyanka Suyal et al. proposed paper, [28] Information and communication technology inflate day by day, due to rapid improvement in technologies has increased the need of effective IDS (Intrusion Detection System). Here, Intelligent Intrusion Detection method that is Rough Set based approach presented for performance evaluation of classifier abnormal behavior. Rough Set Theory is used to reduce the input data space, from complex databases and find minimal decision rules or redact, through this we can manage complexity of system and manage huge network traffic. Rough set based effective classification models namely Rule based classifier algorithm with discretization, Decomposition tree algorithm and Decomposition tree with discretization have been applied to find reduced decision rules and classify problem. Comparison of classification results also have perform with various evaluation criteria and recognize best suited classifier for intrusion detection system dataset.

Latifur Khan et al. proposed that, [29] whenever an intrusion occurs, the security and value of a computer system is compromised. Network-based attacks make it difficult for legitimate users to access various network services by purposely occupying or sabotaging network resources and services. This can be done by sending large amounts of network traffic, exploiting well-known faults in networking services, and by overloading network hosts. Intrusion Detection attempts to detect computer attacks by examining various data records observed in processes on the network and it is split into two groups, anomaly detection systems and misuse detection systems. Anomaly detection is an attempt to search for malicious behavior that deviates from established normal patterns. Misuse detection is used to identify intrusions that match known attack scenarios. Our interest here is in anomaly detection and our proposed method is a scalable solution for detecting network based anomalies. We 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.

VMERITS 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

VIDEMERITS OF THE EXISTING INTRUDERS 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 has to traverse a longer path from its origin to the IDS and in the process can potentially be destroyed or modified by an attacker. Furthermore, the intrusion detection system has to infer the behaviour of the system from the data collected, which can result in misinterpretations or missed events. This is referred as the fidelity problem.
- Second, the intrusion detection system continuously uses additional resources in system it is monitoring even when there are no intrusions occurring, because the components of the intrusion detection system have to be running all the time. This is resource usage problem.
- Third, because the components of the intrusion detection system are implemented as separate programs, they are susceptible to tampering. An intruder can potentially disable or modify the programs running on a system, rendering the intrusion detection system useless or unreliable. This is reliability problem.

VIIPROPOSED SYSTEMS FOR NETWORKS

Group-based intrusion detection system in wireless sensor networks: In group based scheme sensor network ispartitioned in groups. Sensor nodes in each group arephysically close to each other. Attacker is detected usingmultiple attribute of the sensor nodes [10].

Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks: Network traffic isanalyzed and a mechanism is defined for detecting attacks[13].

A Global Hybrid Intrusion Detection System for Wireless Sensor Networks: Support vector machine (SVM) algorithmfor anomaly detection and set of signature for maliciousbehavior detection is used in this method [14].

An Energy-Efficient Routing Method with Intrusion Detectionand Prevention for Wireless Sensor Networks: Both intrusiondetection and prevention scheme are implemented with lesscommunication overhead and low energy consumption [15].

An Integrated Intrusion Detection System for Cluster-based Wireless Sensor Networks: It is a cluster based scheme.Intrusion detection systems are implemented at different levelsin cluster. Misuse Intrusion detection technique has applied atsensor nodes, Hybrid IDS at cluster-head and integrated HIDSat sink node [16].Using artificial intelligence in routing schemes for wireless networks: Artificial neural network is used at every sensornode which provides self-learning capability to system [17].

Intrusion Detection System In wireless Sensor network based on Mobile Agent: Mobile agent is used for detecting theintrusion. Three main mobile agents are used: Collector agent,Misuse detection agent and anomaly detection agent whichuses SVM [18].

Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks: In this game theory method is used along with fuzzyQ-learning. Attacker, base station and sink nodes are threeplayers in the game. Base station and sink nodes are decisionmaker players for detection DOS attack [23].

An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks: Algorithm for detectingthe sinkhole attack is proposed. Firstly list of suspected nodesis generated checking data consistency, and then using dataflow information intruder is identified [24].

VIIICONCLUSION

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 Niki Pissinou. "Sensor network security: a survey." Communications Surveys & Tutorials,IEEE 11.2 (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 InternationalConference on. IEEE, 2015.

[5] Maleh, Yassine, and AbdellahEzzati. "A review of security attacks and Intrusion Detection Schemes in Wireless Sensor Networks." arXivpreprint arXiv:1401.1982 (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] Huo, Guangcheng, and XiaodongWang. "DIDS: A dynamic model of intrusion detection system in wireless sensor networks." Informationand Automation, 2008. ICIA 2008. International Conference on. IEEE, 2008.

[8] Garcia-Teodoro, Pedro, J. Diaz-Verdejo, Gabriel Maciá-Fernández, and Enrique Vázquez. "Anomaly-based network intrusion detection: Techniques, systems and challenges." computers & security 28.1 (2009): 18-28.

[9] Rajasegarar, Sutharshan, Christopher Leckie, and MarimuthuPalaniswami. "Anomaly detection in wireless sensor networks." Wireless Communications, IEEE 15.4 (2008): 34-40

[10] Li, Guorui, Jingsha He, and Yingfang Fu. "Group-based intrusion detection system in wireless sensor networks." ComputerCommunications 31.18 (2008): 4324-4332.

[11] Stetsko, Andriy, Lukáš Folkman, andVashekMatyáš. "Neighbor-based intrusion detection for wireless sensor networks." Wireless and MobileCommunications (ICWMC), 2010 6th International Conference on. IEEE, 2010.

[12] de Sousa Lemos, Marcus Vinícius, Líliam Barroso Leal, and RaimirHolandaFilho. "A New Collaborative Approach for Intrusion Detection System on Wireless Sensor Networks." Novel Algorithms andTechniques in Telecommunications and Networking. Springer Netherlands, 2010. 239-244.

[13] Baig, Zubair A. "Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks." ComputerCommunications 34.3 (2011): 468-484.

[14] Maleh, Yassine, et al. "A Global Hybrid Intrusion Detection System for Wireless Sensor Networks." Procedia Computer Science 52 (2015): 1047-1052.

[15] Moon, Soo Young, Ji Won Kim, and Tae Ho Cho. "An energy-efficientrouting method with intrusion detection and prevention for wireless sensor networks." Advanced Communication Technology (ICACT),2014 16th International Conference on. IEEE, 2014.

[16] Wang, Shun-Sheng, et al. "An integrated intrusion detection system for cluster-based wireless sensor networks." Expert Systems withApplications 38.12 (2011): 15234-15243.

[17] Barbancho, Julio, et al. "Using artificial intelligence in routing schemes for wireless networks." Computer Communications 30.14 (2007): 2802-2811.

[18] El Mourabit, Yousef, et al. "Intrusion detection system in Wireless Sensor Network based on mobile agent." Complex Systems (WCCS),2014 Second World Conference on. IEEE, 2014.

[19] Shamshirband, Shahaboddin, et al. "D-FICCA: A density-based fuzzy imperialist competitive clustering algorithm for intrusion detection in wireless sensor networks." Measurement 55 (2014): 212-226.

[20] Shamshirband, Shahaboddin, et al. "Co-FAIS: cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks." Journal of Network and Computer Applications 42 (2014): 102-117.

[21] Kumarage, Heshan, et al. "Distributed anomaly detection for industrial wireless sensor networks based on fuzzy data modelling." Journal ofParallel and Distributed Computing 73.6 (2013): 790-806.

[22] Reddy, Yenumula B., and S. Srivathsan. "Game theory model for selective forward attacks in wireless sensor networks." Control andAutomation, 2009. MED'09. 17th Mediterranean Conference on. IEEE, 2009.

[23] Shamshirband, Shahaboddin, et al. "Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks." Engineering Applications ofArtificial Intelligence 32 (2014): 228-241.

[24] Ngai, Edith CH, Jiangchuan Liu, and Michael R. Lyu. "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks."Computer Communications 30.11 (2007): 2353-2364.

[25] Muhammad Asif Manzoor, Yasser Morgan, "Real-time Support Vector Machine Based Network Intrusion Detection System Using Apache Storm", IEEE 2016.

[26] 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.

[27] ManjariJha, Raj Acharya, "An Immune inspired Unsupervised Intrusion Detection System for Detection of Novel Attacks", IEEE 2016.

[28] Priyanka Suyal, Janmejay Pant, AkhileshDwivedi, Manoj Chandra Lohani, "Performance Evaluation of Rough Set Based Classification Models to Intrusion Detection System", IEEE 2016.

[29] Latifur Khan · MamounAwad · BhavaniThuraisingham, "A new intrusion detection system using support vector machines and hierarchical clustering" ,The VLDB Journal 2010.