A Review On data mining approach for network security

Er. Vibha[1], Er. Ankur gupta[2]
[1]*P.G. Student, Department of Computer Science & Engineering, Doon Valley College of Engineering & Technology, Karnal, Haryana, India*
[2]*Asst. Professor, Department of Computer Science & Engineering, Doon Valley College of Engineering & Technology, Karnal, Haryana, India*

***Abstract*- Over the last decade, we have become too much technology dependent. Now-a-days we rely on networks to receive emails, banking, stock price, news and online shopping. The need for protecting files in computer systems became more evident with the advent of shared systems. The need became even more severe for systems being accessed over a public network, the Internet. Information in transit must be protected from unauthorized release and changes. The connection itself must be securely established and maintained. The term network security defines that, Network is interconnection (or link) for example network of computers and Security is the freedom from danger or anxiety so Network Security is about securing and protecting the network (externally and internally) from Distributed Denial of Service attacks, rapidly spreading viruses, self-replicating worms, destructive malware and other attacks. Network security begins with authorization and authentication. Organizations are spending billions of dollars just to make their network secure and protect their data from outside and inside attack. However securing and protecting today's complex network in not so easy, it is challenging and demanding [1]. There are many traditional security solutions existing but these solutions do not perform well. here we discuss a survey on various proposed security solution for data.**

***Index Terms*- data mining, network security, cyber attack**

I. INTRODUCTION

Over the last decade, we have become too much technology dependent. Now-a-days we rely on networks to receive emails, banking, stock price, news and online shopping. The excessive use of the communication networks leads to terrorism. Due to that it raises the need of secure and safe system. Because of the dependence on the computer technology, we have to appreciably improve computer network security, so that data integrity, confidentiality and availability do not hinder. All computers are vulnerable to compromise and every network is at risk to unauthorized access and leakage of private and sensitive information and that information stored had to be protected since introduction of computers. The need for protecting files in computer systems became more evident with the advent of shared systems. The need became even more severe for systems being accessed over a public network, the Internet. Information in transit must be protected from unauthorized release and changes. The connection itself must be securely established and maintained.

The term network security defines that, Network is interconnection (or link) for example network of computers and Security is the freedom from danger or anxiety so Network Security is about securing and protecting the network (externally and internally) from Distributed Denial of Service attacks, rapidly spreading viruses, self-replicating worms, destructive malware and other attacks. Network security begins with authorization and authentication. Organizations are spending billions of dollars just to make their network secure and protect their data from outside and inside attack. However securing and protecting today's complex network in not so easy, it is challenging and demanding [1]. There are many traditional security solutions existing but these solutions do not perform well.

In digital word, network security is primary goal because network services are extremely growing day by day and are effortlessly targeted by hacker. They affect network or host computer and network by attacking them using destructive attack [2]. From past few years attacks are increased, so deal with this type of problem there are diverse methods like firewalls, control access, VPN (virtual private network)[3,4],

Intrusion Detection, and Intrusion Prevention are used. These methods only goal is to examine network action and detects, prevent, or counter suspicious incident. Security of network defines level of protection and primary objective of security is to achieve these seven security principles:

- **Confidentiality:** This term is used to ensure that information is not disclosed to unauthorized individuals or system. This means some important information is only accessible to those who have been authorized to access it [5].
- **Availability:** Availability defines that all computer resources are accessible to authorized user whenever user required these resources to access data. This guarantees the survivability of network services despite denial of service (DoS) attacks.
- **Integrity:** In which only authorized users are able to construct, alter, and delete the data as per granted terms and conditions. This is directly related with the accuracy of data. Any changes by unauthorized user are impossible. In which preserve internal and external consistency.
- **Authenticity & Identification:** Authenticity ensures that participants in communication are genuine (original) and not impersonators (fabrication). Identification is an assertion of who is someone by username & password.
- **Non-repudiation:** Non-repudiation prevents either receiver or sender from denying receiving or sent message. This means it makes certain that sender and receiver of message cannot deny that they have ever sent or received such a message.
- **Accuracy:** Accuracy means that the Information is accurate. When it is free from fault and has expected values.
- **Access Control:** Access control is the ability to bound and control the access to user system and applications via communications links. For achieving this, each entity trying to gain access must first be identified, so that right user gains access of data [3].

So that cyber security is subsequently turn to main concern. Researchers create a method for securing system from external device, programs and users whose only goal to destroy security services of network.

1.1 Attacks on Network

There are different types of attacks which harm the network which are comes from internal, own enterprise's employees or their business partners or customers and External coming from outsiders and frequently via the internet.

Flood Attack

The earliest form of denial of service attack was the flood attack. The attacker simply sends more traffic than the victim could handle. This requires the attacker to have a faster network connection than the victim. This is the lowest-level of the denial of service attacks, and also the most difficult to completely prevent, for example a UDP flood attack is a denial of service attack (DOS) attack using User Datagram protocol, a session less/connectionless computer networking protocol. An UDP protocol attack can be initiated by sending large number of UDP protocol packets to random ports on a remote host. As a result the random host will:

- Check for application listening on that host.
- Sees that no application listens on that port.
- Reply with an ICMP destination unreachable packet.

Phishing Attacks:

Phishing attacks are also known as spoofing attacks. Phishing is an illegal method utilizes both social engineering and technical ploy to steal users' personal identity and financial account credentials [7].

Techniques:

Various techniques are developed to perform phishing attacks and make them less suspicious.

- **Email Spoofing:** It is used to make fake emails seems like to be from genuine senders, so that receiver more likely to believe in the message and take actions according to instruction from senders.
- **Web Spoofing:** It makes counterfeit websites which looks similar to genuine ones, so that users trust and enter confidential information into it and results of that attack performed.
- **Pharming**: In which redirect traffic to the counterfeit websites.
- **Malware:** These are installed into victims' systems to gather information directly or assist other techniques.

- **PDF documents:** This technique supports scripting and fillable forms, are also used for phishing.

- **Spyware**

Spyware is computer software that is installed surreptitiously on a personal computer to collect information about a user, their computer or browsing habits without the user's informed consent. As spyware, attackers set up software in users system that track keystrokes to get passwords or electronically secret agent on users network, to gain access to secret information or watching to gain way in to unidentifiable information. Spyware is computer software that is entering secretly in user personal computer to gather information about a user, computer or browsing behavior without user's cognizant approval.

1.2 Malicious Attack on network:

This class includes full logging and collecting information along with sending private and confidential information to the server. There are different types of malicious attacks are defined below:

- **Modification**

Modification is the mostly common attack, in which malicious node modifies the content fields of routing packets that transit through it. "A malicious node could modify packets
before rebroadcasting them, so that they include less attractive metrics, false addresses, and fake hop count in order to redirect network traffic. This attack can cause severe routing disruptions such as; conflicted and suboptimal routes, erroneous routing table, network partition and lose of connectivity" [8].

- **Fabrication**

This attack refers to the generation of faked routing messages, in order to disrupt network operation or to deplete other nodes' resources. Such attack is difficult to detect.

- **Impersonation**

Impersonation also called spoofing attack; it usually constitutes the first step in the majority of attacks. The malicious node hides its real identity and takes legitimate node's identity, thus it can receive all the messages destined to this node and gain access to the network. This attack can also be used for creating loops in order to isolate a target node from the rest of the network [9].

- **Black Hole**

Black Hole attack exploits the vulnerabilities of routing protocols and it is carried out in two steps. First, "the malicious node attracts traffic through itself by advertising better routes to the requested destinations". Afterward, "the malicious node drops all the data or
control packets passing through it without any forwarding". The Figure 1.1 below shows the Black Hole Attack [10].

- **Gray hole**

This attack is a refined form of black hole attack, "in which a malicious node drops only selected packets and forwards the others, depends on the source or the destination of Packets. Another kind of gray hole may behave maliciously for a given period by dropping all packets then switch to normal behaviour later. This attack defeats trust-based mechanisms and makes the detection of malicious node more difficult to achieve" [11]

- **Wormhole**

Also called tunneling attack, it is one of the most sophisticated attacks in MANETs. In this attack, "a malicious node captures packets from one location in a network and tunnels them through an out-of-band channel to another malicious node located several hops away, which replays them to its neighbouring nodes. The tunnel between the malicious nodes is actually faster than links between legitimate nodes, so the tunneled packets arrive sooner than packets through other routes. Therefore, the malicious nodes are more likely to be included in the route and take an advantage for future attack.

Detection of wormhole attack is generally difficult, and requires the use of an unalterable and independent physical metric, such as time delay or geographical location". The Figure 1.2 below shows the wormhole attack [12].

1.3 Intrusion Detection system (IDS)

An intrusion detection system is a network security technology originally built for detecting vulnerability in a computer or network. Intrusion detection system can be a software or physical appliance that monitors network traffic in order to detect unwanted activity and malicious traffic and trigger an alarm [15]. IDS are a most convenient tool

for protecting network and system from an intrusion attack. Primary goal of Intrusion Detection Systems (IDS) is to identify (detect) attacks from insecure networks such as internet to our computer system. IDS are work on both Network as well as Host. From Intrusion Detection Systems, we can obtain all the Intrusion related information that occurs during the monitoring of system. We then analyse these information to determine whether our computer system is intrusive against any attack or security breach or not. When Intrusion Detection System detects something disturbing then it gives signal to the network administrator and performs some types of acts already defined to protect the system [16]. The advantage of IDS is, it is easier to deploy and detect many attacks just by checking packet header. The disadvantage of IDS's is, it gives many false positive alarms and false negatives. IDS work on knowledge and behavior bases, on bases of these, two types of techniques are defined named signature-based detection and Anomaly-based detection [17]. When the blocking capabilities of a firewall are combined with the deep packet inspection of IDS, it is called Intrusion Prevention Systems (IPS). IPS are combination of hardware and software or completely a software deployed on hardware that monitors network traffic and can react in real time in blocking or prevent the intrusion attack.

1.4 ARCHITECTURE OF IDS:

789i?h6tgnl:5

IDS are mostly used tool for secure network from intrusion type attack. The IDS working are based on the principle that supervising network traffic or system abnormal behavior is nasty /malicious and triggers an alarm. The basic element of intrusion detection system is - a sensor or analysis engine that is responsible for detecting intrusions because sensor have decision-making system about intrusions. The various components of Intrusion Detection System are shown in Figure 1.4. The main components of Intrusion Detection System are Information Collection, Detection, Sensor (Analyzer), and Response.

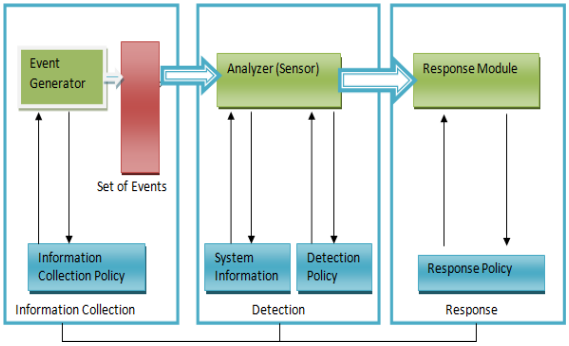

Figure 1.4 Architecture of Intrusion Detection System [18]

- ***Information Collection:***

Collecting data from monitored system is the responsibility of Information collection component. There are some example of input collection resource are network packets, log files and system logs. This Model contains all data which was input from various sources and then provide this input data to the event generator block which converted this input data to set of events. After that set of events are transferred to sensor.

- ***Sensor (Analyzer):***

Sensors (Analyzer) are work like a supervisor which monitors or observes the networks in real times. The input for a sensor is from information collector of a system that could have evidence of an intrusion. Capture network and management network, are two interface of sensor which main purpose to detect and report intrusion. Sensor gives attention to network traffic and detains interface passes into a buffer. This buffer is then examines by detection block [19].

- ***Detection:***

Detection processed the collected data from sensor to recognize abnormal intrusive activity and which generate alarms for security events received. It examines the buffer content and executes network protocol analysis. In this which contains information of known attack signature is system information or knowledge base [18]. A known attack signature is provided by security experts and presents these signatures in databases. When sensor detects any malicious activity or signature, then it compare it with current database and report to response component based on detection policy.

- ***Response:***

This component of the model contains report about malicious activity and authority to take action when any intrusion detected. These responses either automatic or involve human interactions [20]. Response component can either trigger an alarm or send an email notification regarding the incursion detected to the administrator depending on the type of configuration.

1.5 APPLICATIONS OF IDS

IDS are a popular and effective mechanism to secure network or provide protection to the user, organization, industry, and society from intruders and have following application:

- **Banking sector:** Data related to a bank account are stored on systems which are connected to any network and if any intrusion occurs may be damage of account data so IDS are used to protect against any malicious activity on the banking sector.
- **Education field:** All educational departments contain information related to employees are essential which store on particular department's system or on the website, so IDS are placed there for securing from attacks.
- **Business Purpose:** In any organizations data, essential information, and project details etc which was not authorized to anyone are may be hacked or stolen by intruders, for that purpose Business industry using IDS.
- **Medical field:** In term of Healthcare patients records related to diseases, treatments are may be hijacked so for that in medical field IDS used to secure network inside hospital infrastructure.
- **Hotels:** It is the moral and official responsibility of hotel to protect its guest and their assets against threats. IDS provide sophisticated integrated security for safety, liability, mitigation and loss prevention regarding biometric access control, visitor's management, and panic alerts etc.
- **Cloud security:** Cloud Security is the main concern in today life because mostly user stores their data on a cloud so IDS are placed on cloud network to secure that data from attackers.

Automatic Evidence collection: As all know that IDS track records related to the regular activity or behavior of system or networks so may be any abnormal activity is occur then IDS trigger an alarm so it automatically collect evidence related to that behavior. Thus IDS used for automatic evidence collection.

II. LITERATURE SURVEY

The idea of detecting the intrusions or system misuses by looking at some kind malicious patterns in the network or user activity was initially conceived by James Anderson in his report titled "Computer Security Threat Monitoring and Surveillance" [2] to US Air Force in the year 1980. In the year 1984, the first prototype of Intrusion Detection System which monitors the user activities, named "Intrusion Detection Expert System" (IDES) was developed. In the year 1988, "Haystack" became the first IDS to use patterns and statistical analysis for detecting malicious activities, but it lacked the capabilities of real time analysis.

Meanwhile, there were other significant advances occurring at University of California Davis' Lawrence Livermore Laboratories. In the year 1989, they built a IDS called "Network System Monitor" (NSM) for analyzing the network traffic. This project was subsequently developed into IDS named "Distributed Intrusion Detection System" (DIDS). "Stalker" based on DIDS became the first commercially available IDS and influenced the growth and trends of future IDS. In the Mid 90's, SAIC developed "Computer Misuse Detection System" (CMDS), a host based IDS. US Air Force's Cryptographic support centre developed "Automated Security Incident Measurement" (ASIM), which addressed the issues like scalability and portability.

The intrusion detection market began to gain in popularity and truly generate revenues around 1997. In that year, the security market leader, ISS, developed a network intrusion detection system called "Real Secure". A year later, Cisco recognized the importance of network intrusion detection and purchased the Wheel Group, attaining a security solution they could provide to their customers. Similarly, the first visible host-based intrusion detection company, Centrex Corporation, emerged as a result of a merger of the development staff from Haystack Labs and the departure of the CMDS team from SAIC. From there, the commercial IDS world expanded its market-base and a roller coaster ride of start-up companies, mergers, and acquisitions ensued [21]. Martin Roesch, in the year 1998 launched a

light weight open source Network IDS named "SNORT" [22], which has since then gained much popularity. In year 1999 Okena Systems worked out the first Intrusion Prevention System (IPS) [23] under the name "Storm Watch". IPS are the systems which not only detect the intrusions but also are able to react on alarming situation. These systems can co-operate with firewall without any intermediary applications.

2.1 NEEDS OF INTRUSION DETECTION SYSTEM

When in user's system firewall installed, operating system is patch, sound passwords and updated antivirus so why user require IDS? Because other security tools cannot give all security policies and intrusion may be occurred. Sometimes, in case of firewall or antivirus user forget to update a firewall or an antivirus so intrusion can arise. Even the most secure systems with all the protection are still not fully(100 %) secure, like Passwords can be cracked or users may be forget their passwords and software can have bugs that compromise the security of system. From all these perspective users needs IDS for detecting intrusion from network or system effortlessly. According to the 14th version of issued by Symantec Corporation there is a important spike in new malicious code threats occurred during 2008. There is a 165 percent increment over 2007, when new malicious code signatures were added. The data is shown below:

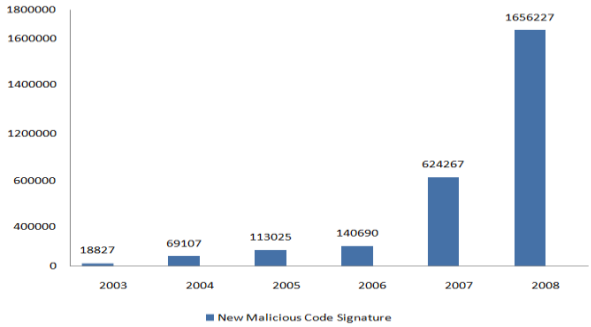

Figure 2.2: Symantec Report on the new malicious code signature [25].

According to the current available internet security threat Report India is appear as third most susceptible country in terms of risk cyber threats, like malware, spam, and ransomware in 2017. India comes one place upper from previous year. In figure shows the ransomware detection rate from 2015-2017. So we need to develop IDS systems and new intrusion detection techniques to detect and discover against all intrusion attack. IDS done diverse things which other system software can't do:

i. It identify anomalous packet content or patterns of traffic that are different from normal Network.
ii. It also identifies signatures of malicious content within packets coming into network.
iii. It provides real time detection before significant harm take place and also completeness to detect known attack.
iv. It reacts as quickly as possible to prevent system form attacks and also increased performance for identifying any malicious activity.
v. It can be transformed and altered according to necessities of particular user and helps to detect attack.
vi. It provides a greater degree of integrity to infrastructure ofthe
vii. organization and also helps in monitoring novel attacks on the Internet.
viii. Able to trace user activity from entry point to exit point, record modification of data and provide report.

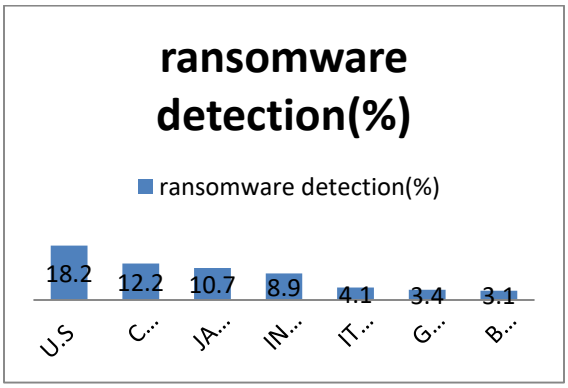

Figure 2.3 Ransomware detection from (2015-2017) [26]

Jiong Zhang and Mohammad Zulkernine et al.(2008), author proposed new approach using Data mining technique called Random forest using misuse, anomaly, and hybrid- network IDSs. Random forest constructs pattern repeatedly for detecting intrusion by matching patterns with network activity. After building patterns anomaly detection uses outlier detecting algorithm for detect intrusion on network. Hybrid network intrusion detection system uses property of both misuses as well as anomaly

detection. This approach of IDS improves the detection work. Using unsupervised anomaly detection technique this gains high detection rate and low false positive rate so we can say that overall performance for detecting anomalies was increased by hybrid approach [24].

Mohammed Hasana Ali and Bahaa Abbas Dawood AL Mohammed et al.(2017),Author developed model for Fast Learning Network (FLN) based on Particle Swam Optimization (PSO) which has been compared against meta-heuristic algorithm for training classifier, ELM and FLN. The PSO-FLN provides output in the testing accuracy of the learning and has increased accuracy for all models with increased the number of hidden neurons. In this model there is problem arise from restricted amount of training data for such class results in less accuracy for certain number of class [15].

Adtiya Nur Cahyo and Risanuri Hidayat et al. (2016),the author proposed an effective scheme based on supervised learning algorithms that are used for comparison of Anomaly-based IDS using ANN and SVM with all dataset features. Using KDD Cup 99 data set for finding accuracy preprocessing applied to filtering and normalized attribute, which are DOS, U2R, R2L, and Probe. Support Vector Machine is not performing better than the Artificial neural network. ANN contains high accuracy and detection rate in all categories where author proved that NN has high accuracy for attack detection than SVM [26].

III. PROBLEM STEMENT

CLASSIFIERS:

There are various supervised learning algorithm are used to classify the problem. Some of them are following:

3.1 Random Forest(RF):

Random forests is also known as Random decision forests which ensemble learning method for classification, regression and other tasks, that function by building a multiple decision trees during training and outputting the class that is the mode of the classes (classification) or mean prediction (regression) of the individual trees.

Random decision forests correct for decision trees' habit of over fitting to their training set. Random forest classifier creates a set of decision trees from randomly selected subset of training set. It then aggregates the votes from different decision trees to decide the final class of the test objects [27].

RF produces additional facilities, especially the variable importance by numerical values. The main features of random forests algorithm are listed as follows:

1. It is unsurpassable in accuracy among the current data mining algorithms.
2. It shows efficient performance on large data sets with many features.
3. It can give the estimate of what features are important.
4. It has no nominal data problem and does not over fit.
5. It can handle unbalanced data sets.

3.2 k-Nearest Neighbor(KNN):

k- Nearest neighbor algorithm (k-NN) is a non-parametric method used for classification and regression. *K-NN* is a type of instance-based learning, or lazy learning, where the function is only approximated locally and all computation is deferred until classification. The *k*-NN algorithm is among the simplest of all machine learning algorithms. In both cases the input consists is the k closest training example in the future space. Output is depending on selecting Classification and Regression [57].

- In *k-NN classification*, the output is a class membership. An object is classified by a majority vote of its neighbors, with the object being assigned to the class most common among its *k* nearest neighbors (*k* is a positive integer, typically small). If $k = 1$, then the object is simply assigned to the class of that single nearest neighbor.
- In *k-NN regression*, the output is the property value for the object. This value is the average of the values of its *k* nearest neighbors [58].

KNN is a kind of classification algorithm that is also called K Nearest Neighbor. It is simple algorithms that work as a distance function.

3.3 Support Vector Machine(SVM):

SVM is known as Support vector machine and is most popular Data mining technique for detecting intrusion but it take too much time for training. This will be worked previously with pattern recognition, hand writing recognition etc [52]. For training in SVM takes more time for large data set for improving

detection rate. There is new method for enhancing training process is Clustering with SVM [59]. In which on basis of decision boundaries classification are performed and split boundaries into two hyper plain or classes or group. For recognizing patterns from training data, each occurrence lies in one of the group. Thus, from binary classifier researcher inspire to use this technique with their model for classification. Here, in figure 4.2 Z1 separate with the maximum margin.

IV. CONCLUSIONS

In this work a new model is proposed which is based on data mining technique supervised learning algorithm Random Forest (RF) with feature selection ACO, which gives better performance and provide security to network and system from dangerous cyber-attack. In which Feature selection using Information gain IG) and Ant Colony Optimization (ACO) are performed, those are further used with classifier k-NN, RF, and SVM. So in future work we can give improvement in these algorithm to provide much better security to network and system from dangerous cyber-attack.

REFERENCES

[1] Matthew Bailey, Connor Collins, Matthew Sinda and Gongzhu Hu, “Intrusion Detection Using Clustering of Netwrok Traffic Flows”, IEEE, 978-1-5090-5504-3,2017.

[2] Annu, Monika Poriye, and Vinod kumar, “Ransomware: Detection and Prevention”, International Journal of Computer Science of Engineering, Issue 6, Vol 5, pp 900-905, May 2018.

[3] Monika and Swati Kapoor, “Mitigating DoS Attack in VPN”, International Journal of Computer Trends and Technology (IJCTT), volume 4, Issue 5, pp 1191-1195, 2013

[4] Monika and Swati Kapoor, “Virtual Private Network-A Review”, National conference on Advanced Computing Technologies, Vol 1, March 2013.

[5] Rashmi Ravindra Chaudhari and Sonal Pramod Patil, “Intrusion Detection System: Classification, Techniques and Datasets to Implement”, International Research Journal of Engineering and Technology, e-ISSN: 2395-0056, p-ISSN: 2395-0072, Vol. 04, Issue. 02, Feb 2017.

[6] Muhammet Baykara and Baran Sekin, “A Novel Approach to Ransomware: Designing a Safe Zone System”, 978-1-5386-3449-3, IEEE, 2018.

[7] Engin Kirda and Christopher Kruegel, “Protecting Users Against Phishing Attack”, Published by Oxford University Press on behalf of The British Computer Society, doi:10.1093, 2005.

[8] C.H. Tseng, S.H. Wang, C. Ko and K. Levitt., “DEMEM: Distributed evidence driven message exchange Intrusion detection model for MANET”, IEEE 2006.

[9] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato and A.Jamalipour, "A survey of routing attacks in mobile ad hoc networks,"IEEE 2007.

[10] H. Deng; Q. Zeng, D.P. Agrawal, "SVM-based Intrusion detection system for wireless ad hoc networks," IEEE 2003.

[11] N. Deb, M. Chakraborty, and N. Chaki, “A state-of-the-art survey on IDS for mobile ad-hoc networks and wireless mesh networks,”IEEE 2011.

[12] Amara korba,**“**Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks”,IEEE 2014.

[13] J.V. Mulert, I. Welch and K. G. W. Seah, “Review: Security threats and solutions in MANETs: A case study using AODV and SAODV,”IEEE 2012.

[14] G. Xiaopeng and C. Wei, “A novel gray hole attack detection scheme for mobile ad-hoc networks,” IEEE 2007.

[15] Mohammed Hasana Ali, Bahaa Abbas Dawood AL Mohammed, Madya Alyani Binti Ismail, Mohamad Fadli Zolkipli, “A new intrusion detection system based on Fast Learning Network and Particle swarm optimization”, Vol. XX, doi:10.1109, Access.2018.2820092, IEEE, 2017.

[16] Su-Yun Wua, Ester Yen “Data mining-based Intrusion detectors”, Published by Elsevier Ltd., IEEE 2008.

[17] V. Jyothsna and V.V. Rama Prasad, “A Review of Anomaly based Intrusion detection System”, International Journal of Computer Application, ISSN:0975-8887), Volume 28,No 7, September 2011.

[18] Rohini Rajpal and Sanmeet Kaur, “A hybrid intrusion detection approach using misuse detection and genetic algorithm”, International conference on signal processing 2015.

[19] Mr Mohit Tiwari, Raj Kumar, Akash Bharti, and Jai Kishan, "INTRUSION DETECTION SYSTEM", International Journal of Technical Research and Applications, Volume 5, Issue 2, pp: 38-44, April 2017.

[20] Lazarevic, Aleksandar, Vipin Kumar, and Jaideep Srivastava, "Intrusion detection: A survey." In Managing Cyber Threats, pp: 19-78, Springer US, 2005.

[21] Asmaa Shaker Ashoor and Sharad Gore, "Intrusion Detection System (IDS): Case Study", International Conference on Advanced Materials Engineering IPCSIT, vol 15, 2011.

[22] Muhammad Imran Shafi, Muhammad Akram, Sikandar Hayat, and Imran Sohail, "Effectiveness of Intrusion Prevention Systems (IPS) in Fast Networks", Journal Of Computing, Vol 2, ISSUE 6, JUNE 2010.

[23] J. Rene Beulah and D. Shalini Punithavathani, "Applying Outlier Detection Techniques in Anomaly-based Network Intrusion Systems – A Theoretical Analysis", International Journal of Computer Applications on International Seminar on Computer Vision, ISSN: 0975 – 8887, 2013.

[24] Jiong Zhang and Mohammad Zulkernine and Anwar Haque, "Random-Forests-Based Network Intrusion Detection Systems", ISSN: 1094-6977, Vol.38, No.5, IEEE, September 2008.

[25] Hatim Mohammad Tahir, AbasMd Said, Nor Hayani Osman, and Nur Haryani Zakaria, "Improving K-Means Clustering Using Discretization Technique In Network Intrusion Detection System", Third International Conference On Computer And Information Sciences (ICCOINS), IEEE, 2016.

[26] Adtiya Nur Cahyo, Risanuri Hidayat, and Dani Adhipta, "Performance Comparison of Intrusion Detection System based Anomaly Detection using Artificial Neural Network and Support vector Machine ", Advances of science and technology for society, 978-0-7354-1413-6, doi-10.10631/1.4958506, 2016.