ISSN:0975-9646

Honeypot Based Intrusion Detection System with Snooping agents and Hash Tags

Vishal Joshi[1] and Parveen Kakkar[2]

[1]*Research Scholar, Dept. of CSE, DAV Institute of Engineering & Technology, Jalandhar, Punjab, India*
[2]*Assitant Professor, Dept. of CSE, DAV Institute of Engineering & Technology, Jalandhar, Punjab, India*

Abstract: The security of network is required for improvement of the industries which are dependent on the internet to enhance the business and providing services on the network. So security of network is primary concern of the industries for securing the critical information. A number of attacks have been noticed in recent years on these kinds of industries. Intrusion detection system (IDS) is used for monitoring the processes on a system or a network for examining the threats and alert the administrator. One such IDS is Honeypot. Honeypots are the computer resources purposely established for monitoring and logging the activities of entities that probe, attack or compromise them. Through the log of research, it becomes easy to analyse the attacker's path, the use of the tools, tactics and purpose. Though a lot of research work has been done in this domain still it needs attention and further exploration. In this paper, the performance of the existing Intrusion Detection System has been improved by using Honeypots with Snooping Agents and Hash Tags. The performance of proposed system has been evaluated with benchmark parameters like PDR, Throughput, Delay and Jitter in different scenario of wireless networks where the proposed system shows better results.

Keywords:*Intrusion detection system (IDS), Intrusion prevention system (IPS), Honeypot, Network Security,*

1. INTRODUCTION

With the possibility of connecting numerous computer systems and networks, appeared the need to defense all this information and machines from attackers (hackers) that would like to get a few confidential facts to apply for their very own gain or simply spoil or modify valuable information. In parallel to speedy technological trends, a massive form of attack activities towards to information structures have additionally been increasing. As a consequence of higher informatics crime rates in the technology, information security has become greater essential. There is enormous need of an efficient system that successfully prevents, detects and blocks intrusion with very much less fake high-quality price.Though there are several safety features to defend the computer assets of an organization or a home user, but even after following all the professional tips, the system security is not still ensured. It's far very tough to get an invulnerable system and one may have to spend a lot of money designing and developing it. Some of the most occurring kinds of network assaults are eavesdropping, data amendment, identity spoofing, password-based attacks and denial of service attacks. To triumph over a lot of these kinds of assaults a business enterprise typically has to install an intrusion detection system to defend the confidential statistics exchanged over its network. Intrusion detection system (IDS) is used for monitoring the tactics on a device or a network for analyzing the threats and alert the administrator. With the help of IDs, all network traffic can be observed. It is easy to detect malicious traffic on a honeynet as well as decode and log some interesting packets at a centralized point. The honeypot technology as a strong complement to IDS can greatly reduce the burden of intrusion detection systems, while the greatest degree of access to information the attacker in order to facilitate further tracking the attack source [1].Intrusion detection and prevention systems (IDPS) are generally centered on figuring out feasible incidents, maintaining log facts regarding them, and reporting the log in attempts. Similarly to this, corporations use IDPSes for different capabilities, which includes identifying problems with protection rules, documenting contemporary threats and deterring people from violating protection guidelines. IDPSes have become a crucial addition to the safety infrastructure of nearly each employer [2].

The remaining paper is structured as follows. Related Work is analyzed in Section II. Section III explains the proposed work. In Section IV Experiments and Results are detailed down and finally, Section V summarizes the whole work with future directions.

2. RELATED WORK

The author of [3] discussed the importance and use of Honeypot technologies to detect, identify, and gather information on various network threats. Honeypots are continuously evolving with broad potential. They have remarkable advantages which can be applied in different environments. They reduce false positives, while providing an extremely flexible tool that is easy to customize for different environments and threats. Since long time, common internal and external threats have been addressed using Honeypots. However, by combining the capabilities of Honeytokens and Honeynets, Honeypots contribute to the early indicationand confirmation of advanced insider threats.

The authors of [5] proposed a shadow Honeypot based intrusion detection system. Shadow Honeypot is used to collect the intrusion from the network. To improve the detection performance of intrusion detection system, shadow Honeypot is combined with it. The shadow is an instrumented instance of the application that can detect

specific types of failure and is instrumented to detect potential attacks. In this paper, to overcome the deficiencies of IDS, both anomaly and misuse detection are combined with honeypot. The shadow Honeypot collects packet fromIDS to further check whether the packet is malicious or not. If data is found infected then it is rerouted towards shadow version else routed to its destination application for processing. All kinds of state changes effected by malicious packetare rolled back to its safe state. This proposed system may improve the overall security of thesystem by reducing the rate of false positives and detect better intrusion.

The authors of [7] defined that sole purpose of Honeypot is to divert the intruders away from essential sources and to take a look at an attacker's techniques. One of the maximum used tool for creating honeypots is honeyd. In case of dense attack traffic, there can be large number of logs generated by honeyd further leading to a lot of disk space consumption. The other drawbacks include the massive time and resource consumption during the analysis and processing of huge log. The paper deals with all these drawbacks by proposing two important modules where the first module is to collect the packets in the network which are further analyzed in the second module to generate summarized captured packet information and graphs for the security administrators. This application also monitors packet information regarding web traffic. The experimental results show that the space required by log file reduces significantly and reports generated dynamically as per user needs.

The authors of [9] proposed NIDS-SA (Network Intrusion Detection System Snooper Agent)which includes the integration of the rule-based detection algorithm and the statistical anomaly detection approach. The proposed approach includes three basic components, Intrusion Detection Node (IDN), Intrusion DetectionCoordinator (IDC), and Snooper Agent (RA) to support the active monitoring capability.These three components work in a synchronized manner to perform intrusion detection, intrusioninferring and attacking Snooper in a better way. The first component IDN captures the packets, de-multiplexthem,detect local intrusion and infer intrusion. The second component is installed in an administrationworkstation for communicating and managing IDNs. Various snoop functions are included in RA for informationgathering. NIDS-SA also includes the pattern matching and statistical inference. In addition to this, cryptography-based mechanisms are also applied in the proposed NIDS-SA to achieve the secure communication ability between IDC and IDNs.

Author of [11] offers an idea of coordinating Honeypot and IDS, which can create and set off snort rule in view of the information sending by Honeypot server. Honeypot gathers the information and then send it to IDS further IDS will assess and produce the rules automatically. These rules are made active to filter the packets sent by the user on the network. The automatically generated rulesare compared with default rule in snort system for the same pattern. The comparison showed the better performance of the proposed technique by measuring the effectiveness of IDS server from the attacking.

The author in [12] gives an approach to prevent assaults in MANETs with the aid of deploying intrusion detection nodes. The paper addresses two varieties of assaults wormhole attacks and black hole attack. The modules used to mitigate wormhole and black hole attacks are called AntiWorm and AntiBlackhole. The experimental results show that the IDS nodes can successfully identify and block the malicious nodes. The paper involves an idea to propose an IDS capable of detecting both wormhole and black hole attacks by altering the algorithms. The proposed modulesAntiWorm and AntiBlackhole can share the same tables to fight against corresponding attacks. That means regular nodes and IDS nodes can keep the necessary information for detecting both attacks.

3. THE PROPOSED WORK

A. *Objectives*

The paper aims to improve the performance of the existing Intrusion Detection System by using Honeypots with Snooping Agents and Hash Tags. Following are the various objectives aimed to achieve in this paper:

1. To conduct traffic analysis using different traffic classes in wireless network.
2. To conduct investigation of the proposed Honeypot Based IDS with performance parameters like PDR, Throughput, Delay and Jitter.

B. *Intrusion Detection*

IDS is a set of techniques and resources to help identify, examine, and record intrusions. To achieve information security the basic options include encryption, authorization, firewall, and intrusion detection and prevention systems [4]. Also, as supplementary configurations honeypot structures are proposed. As per the intrusion detection method, IDSs are divided into two groups as "anomaly detection" and "misuse detection" [18].

Misuse detection method is based on a predefined set of attack patterns called "attack signatures" to look for attack traces. The predefined attack signatures are listed in a database as a detection rule. One of the principal benefits of using misuse detection is the detection of known attacks with a low false positive rate. There are three main components to the Intrusion detection system which are Network intrusion detection, Host Based Intrusion Detection, Signature based intrusion detection.

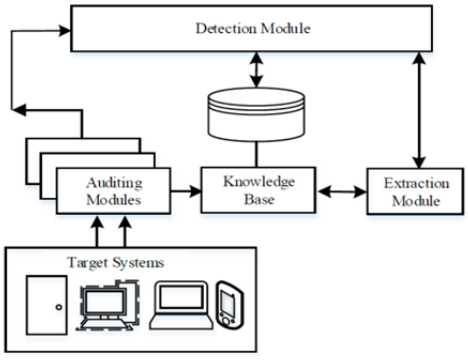

Figure 1: Misuse Detection [18]

Anomaly detection tries to determine whether the deviation from the established normal patterns can be regarded as intrusions. Anomaly detection approach consists of two phases: firstly a training phase which is based on the identification of normal traffic and behavior by constructing profiles of users, servers and network connections; and a testing phase where the learned profile is applied to new data [14] [18].

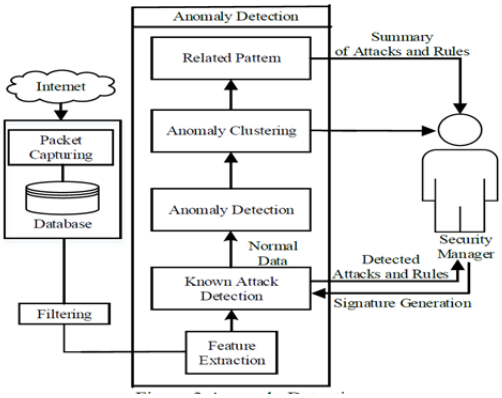

Figure 2: Anomaly Detection

The main advantage of this approach is the capacity to detect new attacks without a priori knowledge of these attacks. These, unknown attacks can be detected.

C. Honeypot System

Honeypot is an exciting technology with great potential for the field of network security. It can be understood as a resource used to divert attackers and hackers away from critical resources i.e. it is an observed trap. It can also be used to study an attacker's methods and tools. [6] The value of a Honeypot lies in unauthorized and illicit use. Neither any authorized activity runs on these resources nor do they have any production value i.e. no legitimate activity is carried out. It provides a large amount of valuable information for analysis and can detect variety of attacks, working even within encrypted environment. [7] It acts as a cherished observation and early warning tool but on the contrary it should be used with caution as it has risks associated with it.

The main functions of a honeypot are:

1. To divert the attention of the attacker from the real network, in a way that the main information resources are not compromised
2. To capture new viruses or worms for future study
3. To build attacker profiles in order to identify their preferred attack methods, similar to criminal profiles used by law enforcement agencies in order to identify a criminal's *modus operandi*
4. To identify new vulnerabilities and risks of various operating systems, environments and programs which are not thoroughly identified at the moment [8].

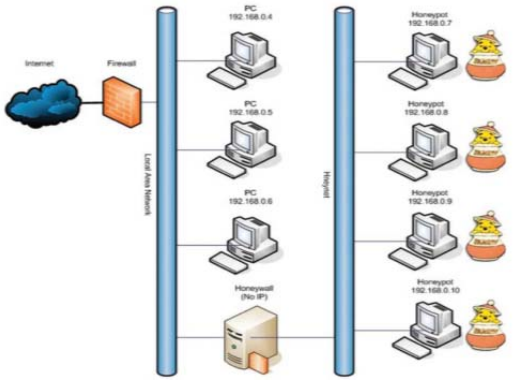

Figure 3: A classical Honeypot deployment [6]

To study about hackers in social network and how they communicate with each other. It is necessary to offer a real operating system to the attacker so that the attacker can gain root privileges on the system and information about the attack can be identify. The amount of activity perform by the attacker with the honeypot is called interaction level. Honeypots are divided into two broad categories, namely low-interaction Honeypots and high-interaction Honeypots.

1) Low interaction Honeypots: In low interaction Honeypots there is no operating system that an attacker can operate on. Instead operating system emulators are installed which interacts with the attacker. It offers limited interaction level to the attackers. It will be used to scan the port and generates attack signatures [17].

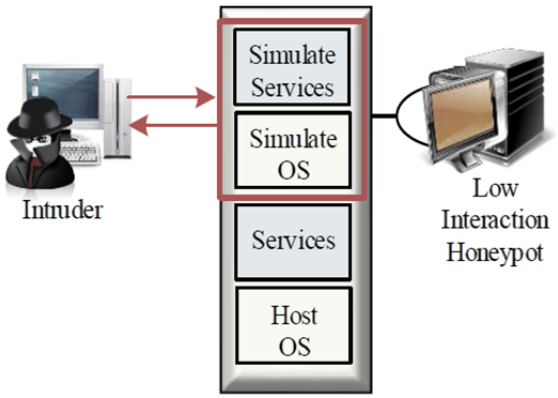

Figure 4: Low Interaction Honeypots

2) High interaction Honeypots: High interaction Honeypots have actual operating system and has tools which motivates the attacker to attack so that their attack strategies can be recorded and later analysed. As high interaction Honeypot offers 24/7 internet connectivity, it attracts the attackers and to reduce the load of these high interaction Honeypots, only traffic filtered by low interaction. Honeypots is passed to them. So high interaction Honeypots basically process the packets sent only by malicious users [17].

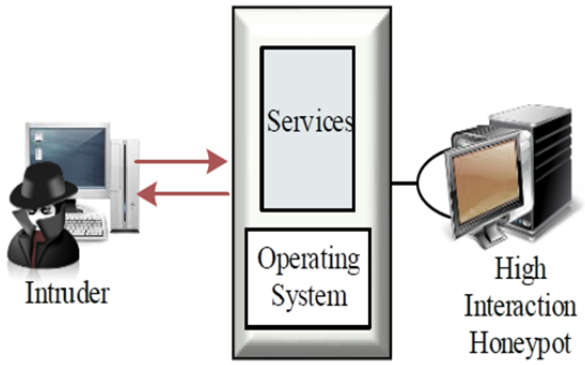

Figure5: High Interaction Honeypots

The collection of Honeypots is called Honeynet [6]. A Honeynet contains one or moreHoneypots, which are computer systems on the network set up to attract and "trap" theattackers. A honeynet usually has real applications and services so looks like a normalnetwork and a worthwhile target. Actually honeynet doesn't serve any authorized users,any attempt to contact the network is likely an illicit attempt to breach its security and anyoutbound activity is likely evidence that a system has been compromised [17], [18].

D. Snooping

Snooper is an optional function in the proposed system. It is installed physically on thesame host with Intrusion Detection Node. It is composed of two components: SnooperLaunching Agent and Snooper functions.
Snooper Launching Agent is responsible for thenetwork information gathering and launching the information gathering process with theSnooper techniques specified in various Snooper functions [9]. Most of cases of snoopingagents are used for the monitoring and filtering purposes for the networks where high endsecurity and priority traffic is required. In our research similar line of snooping agents willbe implemented for the checking of network traffic. Snooping agents in simple process arethe agents built on instruction set to the devices are used [15]. Snooping agents could besoftware based or hardware based. Software based instruction sets are easy to alter so weare using the same for our experimentation.

E. Problem Formulation

The paper includes work on network intrusion detection system and to guard the network with the advent of snooping agents and honeypot on the network in order that any intrusion took place in network may be detected and as a result may be prevented. The concept behind the use of snooping retailers and honeypot is to provide network control in term of tracking. Usually in wireless networks, attacks are main cause of malfunctioning and are difficult to monitor [16]. Different intrusion detection systems have been proposed based on application. In many eventualities in which attackers are able to overcome intrusion scanning, need to be detected. For higher solution honeypots can act as accurate solution. Traditionally honeypots are connected with end clients to detect the uneven behavior of traffic. Activities such as port scanning can be effectively detected by the weak interaction honeypot but much application such as packet scanning, pattern scanning cannot be detected by weak honeypots so snooping agents for better pattern matching will be used [10].This paper proposes a strong mechanism hybridizing honeypot along with snooping agents to gain maximum security within the wireless community. Honey pot can be placed simply after the Firewall and intrusion machine may have strongly coupled synchronize with snooping agents. Tracking might be achieved at packet level and pattern level of the traffic. Simulation will filter and monitor traffic to highlight the intrusion in the network. In our work, we have processed it with snooping agents with hash tags which will cut the overhead and complexity along with enhanced security of network.

F. Proposed Approach

Honeypot implementation and avoidance of malfunctioning in wireless networks is achieved in following steps.

1st Phase: This phase will contain the basic functionality and collection of information of simulator, basic Honeypot functions, intrusion detection systems etc. Layout for comparison will be done in this phase.

2nd Phase: In this phase a network will be created with intrusion detection environment in NS2 simulator and will fetch the difference in the performance of the wireless network.

3rd Phase: The proposed scheme will be implemented for honey pots to avoid the malfunctioning and achieve good monitoring measures. Further a strong honeypot mechanism will also be implemented along with intrusion detection system to achieve maximum security in the wireless network. Honeypot will be placed just after the Firewall and intrusion system will have strongly coupled synchronize with honeypot along with snooping agents. Snooping agents will be part of most of the network activities for filtering and tagging purposes. Snooping agents will be created with help of interrupt type with information of traffic pattern available for communication. Snooping agent will be applied in form of instruction code which will be synchronized with honeypot. Placing of agents will be done in a way to make the filtering process strong with complete monitoring of malicious and uneven traffic. Monitoring will be done at packet level and pattern level of the traffic. Simulation will filter and monitor traffic to highlight the intrusion in the network.

4th Phase: Final step will be testing of the proposed system with benchmark parameters like PDR, Throughput, Delay and Jitter in different classes of wireless networks viz Constant Bit Rate and Variable Bit Rate.

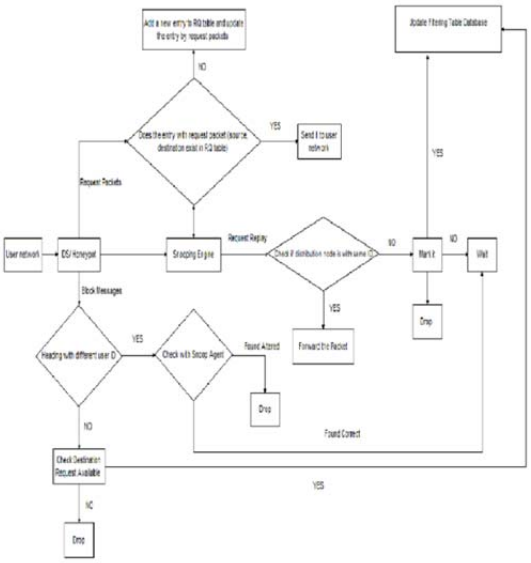

Figure 6: Flowchart

4. EXPERIMENTS AND RESULTS

This section presents the simulation results of the proposed methodology implemented with the help of NS2.

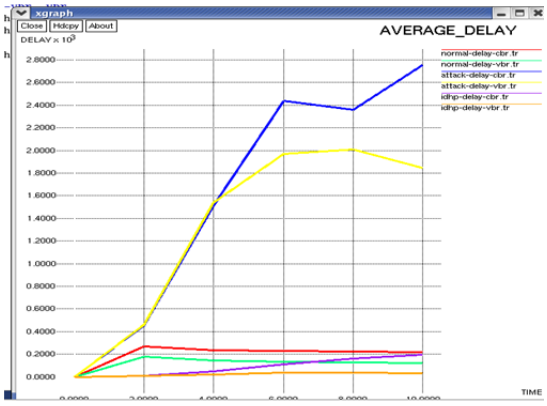

Figure.7 Comparison of Average Delay of the proposed technique with the existing

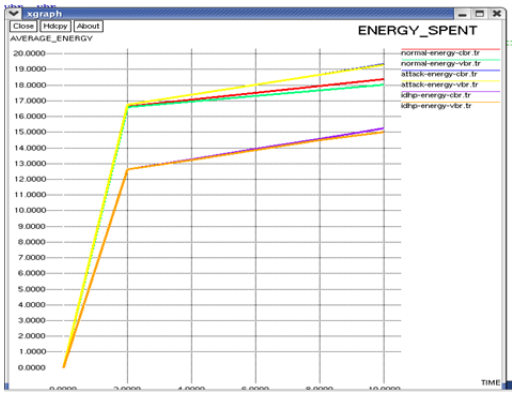

Figure.8 Comparison of Energy spent of the proposed technique with the existing

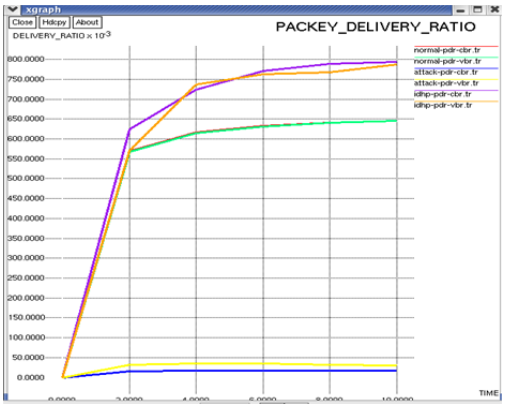

Figure.9 Comparison of PDR of the proposed technique with the existing

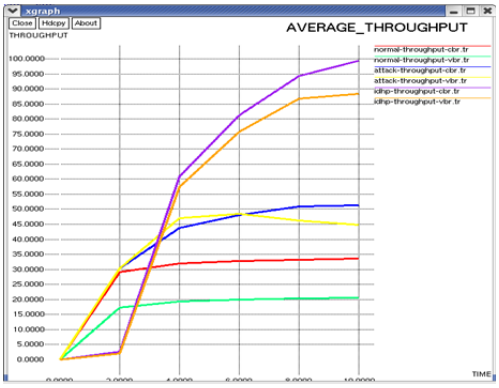

Figure.10 Comparison of Average Throughput of the proposed technique with the existing

5. CONCLUSION AND FUTURE SCOPE

Our proposed Honeypot based Intrusion Detection System has significantly improved detection rate of Intrusion Detection System and drastically reduce false positives hence enhances the overall efficiency of the Intrusion Detection System . Honeypot based Intrusion Detection System has significantly Increased Average Throughput and Packet Delivery Ratio. Proposed System has remarkably reduced Energy Spent and Packet Drop Rate . All above parameter shows better efficiency of the Honeypot Based Intrusion Detection System. However Jitter is not reduced which is undesired.

In future more algorithms can be applied to reduce Jitter. Further our proposed system can be coupled with other Intrusion Detection Systems to enhance their capabilities and overall efficiency of the our proposed system.

REFERENCES

[1] Xiaohui Bao et al., "Network Intrusion Detection Based on Support Vector Machine", International Conference on Management and Service Science MASS '09, 2009, pp.1-4

[2] Sanjay Kumar Sharma et al., "An Improved Network Intrusion Detection Technique based on k-Means Clustering via NaIve Bayes Classification", IEEE-International Conference on Advances in Engineering, Science and Management (ICAESM -2012), 2012, pp.417-422

[3] L. Spitzner, "Honeypots: catching the insider threat", Proceedings of 19th Annual Computer Security Applications Conference, 2003, pp.170-179

[4] Yunlu Gong et al., "Intrusion Detection System Combining Misuse Detection and Anomaly Detection Using Genetic Network

Programming", ICROS-SICE International Joint Conference, 2009, pp. 3463-3467

[5] Navita Sharma and Gurpreet Singh, "Intrusion Detection System Using Shadow Honeypot", International Journal of Emerging Technology and Advanced Engineering, Volume 2, No 8, 498-500, 2012.

[6] Ali Mirzaei and Shahriar Mohammadi, "Use of Honeypots along with IDS in Cluster-Based MANETs" American Journal of Scientific Research, No. 80, pp.155-163, 2012.

[7] Balaji Darapareddy and Vijayadeep Gummadi, "An Advanced Honeypot System for Efficient Capture and Analysis of Network Attack Traffic", International Journal of Engineering Trends and Technology- vol. 3, no. 5, pp.616-621, 2012.

[8] Kartik Chawda and Ankit D. Patel, "Dynamic & Hybrid Honeypot Model for Scalable Network Monitoring", International Conference on nformation Communication and Embedded Systems (ICICES), 2014 , pp.1-524

[9] Bin Zeng, Lu Yao and ZhiChen Chen, "A Network Intrusion Detection System with the Snooping Agents" , International Conference on Computer Application and System Modeling (ICCASM 2010), 2010, pp.232-236

[10] Mukta Rao and Dr Nipur, "Network Security in Organizations Using Intrusion Detection System Based on Honeypots", Global Journal of Computer Science and Technology Network, Web & Security, vol.12, no.16, pp.78-81, 2012.

[11] Albert Sagala "Automatic SNORT IDS Rule Generation Based on Honeypot Log", 7th International Conference on Information Technology and Electrical Engineering (ICITEE), 2015, pp. 576-580

[12] Ming-Yang Su "A Study of Deploying Intrusion Detection Systems in Mobile Ad Hoc Networks", Proceedings of The World Congress on Engineering 2012 ,2012, pp1318- 1322

[13] Sergio Pastrana et at., "Evaluation of classification algorithms for intrusion detection in MANETs", Knowledge-Based Systems, Vol. 36, pp. 217-225, 2012.

[14] A. Patwardhan et al., "Threshold-based intrusion detection in ad hoc networks and secure AODV", Ad Hoc Networks , vol.6, pp. 578–599, 2008.

[15] Sven Ehlert et al., "Survey of network security systems to counter SIP-based denial of-service attacks", computers & security, vol. 2 9, pp. 2 2 5 – 2 4 3, 2010.

[16] Farzaneh Izak Shiri, "A Parallel Technique for Improving the Performance of Signature-Based Network Intrusion Detection System" , IEEE 3rd International Conference on Communication Software and Networks (ICCSN), 2011, pp.692-696

[17] Pushpa Rani1, Yashpal Singh2, S Niranjan, "A Review on Honeypot as an Intrusion Detection System for Wireless Network", International Journal of Engineering Research and Development e-ISSN: 2278-067X, p-ISSN: 2278-800X, Volume 7, Issue 4 (May 2013), PP. 71-74

[18] Muhammet Baykara, Resul Daş, "A Survey on Potential Applications of Honeypot Technology in Intrusion Detection Systems", International Journal of Computer Networks and Applications (IJCNA) Volume 2, Issue 5, September – October (2015)