Enhancing Intrusion Detection System Performance using Firecol Protection Services based Honeypot System

Rajalakshmi Selvaraj
Department of Computer Science, BIUST, Botswana & Faculty of Engineering and the Built Environment, University of Johannesburg, South Africa

Venu Madhav Kuthadi
Department of AIS, University of Johannesburg, South Africa

Tshilidzi Marwala
Faculty of Engineering and the Built Environment, University of Johannesburg, South Africa

ABSTRACT
Nowadays, Internet is one among the famous technique to connect each computer all around the world. The development of nonstop communication creates a number of opportunities and also it develops new possibilities for malicious users. As the size and number of the Internet and Network traffic has become greater and the requirement for the Intrusion Detection grows in step to minimize the Information communication overhead required for the Intrusion Detection and diagnosis. It has made the public servers gradually more vulnerable to incursion of Intrusions and unauthorized accesses. In addition to this, one of the major concerns of a server administrator are maintaining poor performance, low latency for the user and filtering illegal accesses. So the System Administrator utilizes Honeypot systems for handling Intrusions in the network. Honeypot systems are system or decoy server setup together data concerning an intruder or attacker into the Network system. In this research, Firecol Protection Services based Honeypot System (FPS-HPS) is proposed to prevent and handle the various network intrusions in the Internet. This approach perform the operations in the following way: 1) firecol protection services indentify the network intrusion, 2) the load balancer generate two types of tokens to intrusion user as well as authenticated user and forward to mail server 3) mail server send token key to the attacker and original user 4) token verifier verify the received token is valid or not. If the token is valid then they forward the request to the original server otherwise it is considered as an attack and this verifier forward request to honeypot system. 5) Finally, The honeypot system sends irrelevant messages to attacker. The experimentally deployed proposed system results shows that our framework prevents the intrusions effectively rather than other tools or framework.

Keywords
DDoS attacks, Intrusion Detection System, Honeypot System, Firecol Protection Services, Network Security

1. INTRODUCTION
Recent years, Computer system and Internet have raised many security problems due to the usage of network explosive [1]. In CERT statistics it reports that, the number of Intrusions has extremely increased over to years. Any malicious attack or Intrusion on vulnerabilities of the network, information systems or computers may lead dangerous disasters, and violate the security policies of computer, i.e, (CIA) Confidentiality, Integrity and Availability. Until now, information security and the threats on network are important issues [4]. To address the challenges in Information security, reach statutory compliance and to reduce the threats, Information security tools such as Firewalls, Antiviruses, IDS/IPS (Intrusion Detection/Prevention System) and etc are deployed. In [3] Andre Yee states that "Intrusion Detection System have become a part of multilayered security architecture", as they discover a system or network is under attack or Intrusion. The Intrusion Detection System don't fully assurance security, but when used with vulnerability assessments, security policy, user authentication, access control, data encryption, and firewalls IDS can greatly improve network safety. Intrusion Detection System serves three necessary security functions such as: 1) monitor, 2) detect, and 3) respond to illegal activity. IDS uses set of policies to describe certain events, if detected will issue an alert or respond automatically to the event. Such a response might consist of disabling a user account, launching of scripts and logging off a user [2].

Intrusion Detection System has thus appeared a solution to provide better information security as compared to other existing techniques [7]. Intrusion Detection System runs continuously in a system background, monitors network traffic and computer systems and analyzes network traffic for potential hostile intrusion (or) attacks originating from exterior organization and in addition for system attacks or misuse originating within the organization [8]. System Administrators depend on such tools to monitor and protect their systems and network. The System Administrator identifies inappropriate activity or use of a computer system or network by checking events and forwarding alerts when certain events, like scanning the network to resolve computer systems take place.

An IDS (Intrusion Detection System) examines the entire inbound and outbound network activity and recognize doubtful patterns that may specify a network or system attack from somebody attempting to compromise or break into a system. Intrusion Detection Techniques are conventionally categorized into two different methodologies such as Misuse detection and Anomaly detection.

In Misuse detection, the Intrusion Detection Systems examine the data it collects and compares data to huge databases of attack or Intrusion signatures. Fundamentally, the Intrusion Detection System search for a definite attack that has been previously documented. Like a VDS (Virus Detection System), Misuse detection system is only as higher as the database of Intrusion or attack signatures, which is regard as measuring the anomaly in this system. In Anomaly detection, the computer systems base their choice on anomalies, things that do not normally occur. The SA (System Administrator) describes the typical packet size, baseline, or normal,

breakdown, state of the network's traffic load, and protocol. There are three major components to the IDS.

In a Network Intrusion Detection System or Network-based system, the particular data packets fluent through a network are examined. The Network-based system can identify malicious data packets that are intended to be unnoticed by a naïve filtering rules of firewall. In a Host-based system or Host Intrusion Detection Systems (HIDS), reside on a resource which HIDS supervise. Host-based systems look at produced log files, modifications in the respected file system or verify for changes in the process table. The goal of HIDS is to identify intrusions into a host. The SIDS or Signature based Intrusion Detection is based on known attack signatures. These kinds of signatures are stored and compared against incoming network traffic or events. When a pattern matches, at a time an alert is generated. Honeypot systems are introduced to monitor the idle Internet Protocol (IP) spaces to learn about attackers. The benefit of Honeypot system over other existing monitoring solutions is to gather suspicious activity only. A Honeypot system attracts the attacker or Intrusion and thus gives an invitation for attack [5], [6]. To prevent and handle the abovementioned network Intrusions in the Internet a new approach is proposed in this research work using Firecol Protection Services based Honeypot System (FPS-HPS). There are five major components deployed in handling the network Intrusions such as Firecol Protection Services, Load Balancer, Mail Server, Token Verifier and Honeypot System. Firecol Protection Services checks the status of user/attacker, Load balancer generates token based on Firecol Protection Services result. Mail Server forwards the generated token into user/ attacker. Token verifier verifies the received token range then based on the token range this verifier forward token into Honeypot System and Original server. Honeypot System sends irrelevant messages to respected attacker based on the attacker query.

2. RELATED WORK

A Fire Collaborator or Firecol is Software or Hardware device that prevents the system from Intrusion detection. A client is registered with firecol in the stage of ISP. After successful registration a personal unique identifier is allocated to the client. If the unique identifier is used by more users, then firecol will detect the malicious user. Firecol detects malicious traffic by its ISP rules.

Fig1.Firecol Functional Diagram

A Firecol function has three managers namely Selection Manager, Score Manager and Detection manager. Selection Manager will establish the rules and observe the abnormal traffic. Score manager allocate the score for the generated rules. The assigned scores are shared between the nearest clients for the significance of trust. Detection manager detects unauthorized and authorized traffic in the data transmission.

There are three methods proposed in IDS and are

1. Attack Prevention and Pre-emption -In this method, attack is identified at client interface and mitigation is completed away from destination. In pre-emption an authorized attacker transmits malicious data that data will be swapped using nearest network devices.

2. Attack Detection and filtering-An attack in this method is detected by traffic patterns registered in the network devices. The detected attack is filtered by registered in the network devices.

3. Attack source trace back and identification-The attack in this method is identified by its source ip address and the load balancer will add the ip address to its block list.

The Research works stated below are developed with detailed and extended communication algorithms. Experiments were conducted on real-time datasets and traffic is generated at different patterns to compute the performance of the algorithm. In addition to that complexity of the algorithm is also systematically analyzed. Although a well-known dataset is used, it is not a statistical measure similar to research works. The true and false positive rates are calculated for every time window and every router globally. For this reason, it is important to concentrate more on measurable features.

A firewall rule exchanging mechanism and firewall detection of attacks is proposed in [14]. In the research work [15], intrusion is distributed and it is detected near to victim. Many solutions did not use the advantage of collaboration except firecol. In [16] newly identified threads are exchanged using mobile agents. An effective solution is provided by firecol with simple metrics, while previous techniques are expensive due to consumption of resource. Many techniques supporting efficient statistics is not considered. A packet counter approach to detect intrusion in each packet flow is described in [17] and entropy based expressiveness is proposed in [18]. The deviation in an identified profile is determined using conditional probability method stated in [19]. Using traffic aggregation a new approach is proposed in [20] for identifying overloaded links.

A clustered architecture is proposed in [21] to evaluate the firewall observations using DoS based overload issues. The work proposed DoS aware communication technique by end host acknowledgements. In spoofed address are identified by marking the path from source to destination and also to detect the flooding attacks using routers. An alternative approach to observe previous packets and traffic to develop a common approach is proposed, flooding attacks are prevented by sharing information among network nodes. To improve information sharing firecol uses ring semantics.

An IDS is built in using an agents as an element for collecting and examining data. This method also developed a new format for measuring scalability. A common problem in the distributed IDSs is the delay of intrusion detection in the inference module. The access controls system developed in the design does not identify different level of access to different users. Therefore a new Firecol Protection Services based Honeypot System (FPS-HPS) is proposed to overcome these abovementioned issues.

3. PROPOSED WORK

The Intrusion (or) attacks will be prevented by using our proposed (FPSIDS-HPS) approach. The figure 1 shows our proposed system structure where there are five major components deployed to handle and prevent various network intrusions such as Firecol Protection Services, Load Balancer, mail server, token verifier and Honeypot System. 1). Initially the original user connected with the internet and then he/she communicates with Firecol Protection Service, which initially checks the user status and it will forward into load balancer. 2). The Load balancer generates the token key for user and attacker who attacks the network. The load balancer generates

two different token keys with different range. Then the load balancer forwards the generated token keys to the mail server. 3) The mail server forwards the token key to user/attacker separately. Whenever the user/attacker receives the token key he/she sends the token key into the token key verifier. 4).

The Token verifier verifies the received token range; whether a received token is sent from the original user thus the received token is valid. Then the token verifier forward the request to original server also this server send respected data to the corresponding user. Otherwise, the token key is sent by the attacker and the range of received token is different. Hence the request should be forward to honeypot system. 5).Finally, honeypot system sends irrelevant data to the attacker. Here honeypots provides tremendous intrusion detection system (IDS) that can be used to determine if a computer network or server has experienced an unauthorized intrusion.

3.1 Firecol Protection Services

Firecol system detects the flooding IDS attacks of victim host and attacked source(s) at ISP (Internet Service Provider) level. Firecol is a distributed architecture built with large number of Internet Service Providers ISPs connected with overlay networks. These networks are protected with rings for all subscribed customers. FPS (Firecol Protection Service) has five processes namely Packet Processor, Metrics Manager, Selection Manager, Score Manager and Collaboration Manager.

(i). The Packet Processor (PP) initially recognize the traffic, frequencies and the counters of every selected rule.

(ii). The Metrics Manager (MM) computes each rule and the frequencies. A rule demonstrates a particular traffic instance to monitor is basically a network traffic filter; the metrics manager can be based on Internet Protocol (IP) address or ports.

(iii). The Selection Manager (SM) estimates the current network traffic profile deviation from the stored ones, chooses out of profile rules, and then forward them to SM.

(iv). From the Decision table the Score Manager (SCM) allocates a core value to every selected rule depend on the entropies and frequencies received from the upstream IPS.

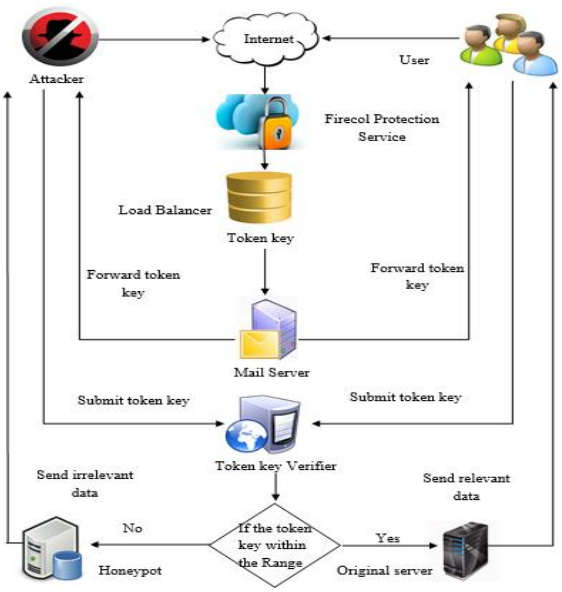

Figure 2. Proposed Network Architecture

(v). The Collaboration Manager (CM) is the final component of Firecol Protection Services as well as charge of confirming potential attacks or intrusions. They claiming that discovering a flooding attack can be confirmed only if the network traffic generated is greater than the customer's capacity.

3.2 Load Balancer

In this research, Load Balancer generates the tokens for both the original user and attacker. Token is an important part of Intrusion Detection. The uses of token are, once the attacker is identified at that time, load balancer identify the IP address, system ID of respected attacker. After that, the attacker cannot able to access the Internet because of the token key. On receiving the result of Firecol Protection Services, the load balancer takes the decision. If the result from the Firecol Protection Services was "true" (Indicating the presence of an attack) then load balancer generates the token for respected attack and is forwarded to the attacker through mail server. Otherwise, the token is forwarded to the original user through mail server.

3.3 Mail Server

Generally, Mail server contains the user details like IP address, system ID and etc. Once the user and intruder or attacker connected into the Internet, details should be forwarded to this mail server. This server manages the network traffic. Mail server sends token for original user and attacker frequently. This server receives a token from load balancer then it forwards the tokens into respected user and the attacker.

3.4 Token Verifier

This is an important component of our proposed system. User/ attacker once receive a token then they send a token into token verifier. This verifier receives a token, it checks the token structure. If the token structure matched with the original user then it forward the request into original server. Else the token structure matched with the attacker then it forwards the request into Honeypot system for sending irrelevant data.

3.5 Honeypot System

Honeypots are decoy Computer system resources developed for the intention of logging and monitoring the entity activities that probe, attack or compromise the network Intrusions [11-13]. Activities on Honeypot systems should be considered suspicious by the above definition, as there is no position for gentle users to interact with Honeypot systems. These systems come in many sizes and shapes; examples contain irrelevant items in a database, low interaction network traffic components such as high interaction hosts with OS (Operating Systems) and services and preconfigured network traffic sinks [9],[10].

3.5.1 Deployment Classification

Honeypot system can be categorized using their deployment and involvement level. Production honeypot systems are simple to utilize, capture limited information only, and are used mainly by corporations or companies; Production Honeypot systems are positioned within the production network with various production servers by an organization to increase their overall security state. Generally, Production Honeypot systems are low interaction Honeypots, which are simple to deploy. They provide a small amount of information about the attackers and attacks than Research Honeypot systems do. The intention of Production Honeypot system is

to support mitigates risk in an organization. The Honeypot system includes value to an organization's security measures.

Research Honeypot systems are run by a non-profit research organization, a volunteer or an Educational institution have to collect data about tactics and motives of the Blackhat group targeting various networks. These Honeypot systems do not include direct value to a particular organization; as an alternative, these Honeypot systems are used to systematic investigation and study of the threats organizations face and to study how to better protect in opposition to those threats. This collected information is also used to protect in opposition to those threats. Research Honeypot systems are difficult to deploy and cause to continue (maintain), capture far-reaching information, and are mainly used by government organizations, research and military.

Spam Versions: Spammers misuse vulnerable resources like open proxies and open mail relays. Some System Administrators (SA) has created Honeypot source codes that impersonate as these misusable resources to find out spammer activity. There are various capabilities such Honeypot systems provide to these System Administrators and the fact of such irrelevant misusable systems make misuse more complex or risky. Honeypot system can be powerful action taken to misuse from those who depend on maximum volume misuse (e.g., Spammers).

These Honeypot systems can disclose the obvious misuse IP address and which gives bulk spam capture (enables the operators to find out spammers' response mechanisms and Uniform Resource Locators.) For Open rely Honeypots, it is potential to find out the e-mail addresses ("Dropboxes") spammers use as destination for their test messages, dropboxes are the device the spammers used to discover open relays. After that, it is easy to mislead the spammer: transmit some unlawful relay electronic-mail received addressed to that dropbox electronic-mail address. That explains the spammer the Honeypot system is a real misusable open relay, and the Honeypot system frequently respond by sending huge amount of relay spam to that Honeypot, which stops it. The obvious source may be different misused system- abusers and spammers may use a misused systems chain to make detection of the original starting point of the misuse traffic difficult.

Electronic-mail trap: An electronic-mail address i.e. only used for acquiring spam can also be determined as spam Honeypot. While comparing the two terms "spamtrap" and "Honeypot", Honeypot might better be reserved for methods and systems used to counter attacks or detect and probes. Spam reaches its destination "legitimately"- precisely as non-spam electronic-mail would arrive. A mixture of these methods is Project Honeypot. The distributed, Open-Source Project utilizes Honeypot pages installed on websites in the region of the world. These Honeypot pages hand-out exclusively tagged spam trap electronic mail address. Electronic-mail address spammers and harvesting can then be pathway as the Honeypot system collect and subsequently send to these spam trap electronic-mail addresses.

Database Honeypot: The intruders frequently attacked the databases with the help of Structured Query Language (SQL) injection. Because some activities are not identified by fundamental network firewalls, organizations frequently use database network firewalls. While the web application still runs as usual a few of the available Structured Query Language (SQL) database firewalls support/provide Honeypot system architectures to let the attacker or intruder execute against a trap database.

4. RESULTS AND DISCUSSION

4.1 Experimental Setup

In order to measure the performance of our proposed approach, a sequence of experiments on extracted dataset were conducted. Based on the following configuration our proposed method should be implemented 1) Windows 7, 2) Intel Pentium(R), 3) CPU G2020 and 4) processer speed 2.90 GHz.

The extracted dataset includes two thousand connection records, set of forty one features based on each connection and a label which clearly defines the status of connection records as either normal type or particular attack type. These features are in the forms like symbolic variables, discrete and continuous features significantly fall into four groups: (i) the 1st group contain the common feature of a connection, which consists of the fundamental features of individual Transmission Control Protocol connections. Some of the features are connection duration, network service (telnet, http, and etc) and the protocol type (UDP, TCP and etc). (ii) The domain knowledge suggest the content features inside a connection are used to evaluate the payload of the original Transmission Control Protocol (TCP) packets like amount of failed login attempts. (iii) The same host features observe recognized connections in the earlier past two seconds that have the similar target host as the current connection, and compute the statistics related to service, the protocol behavior etc. (iv) The similar service features examine the connections in the past two seconds that have the equivalent service as the present connection.

4.2 Results

Table 1 Fragmentation of Attributes from the IP datasets

S. No	Attributes	S.NO	Attributes
1.	Duration	6	Destination bytes
2.	Protocol type	7	Number failed logins
3.	Service	8	Service received error rate
4.	Flag	9	Different service rate
5.	Source bytes	10	Destination host count

The table 1 shows the partial attributes names which are obtained from network datasets to detects the received network dataset is normal or anomaly based on these attribute values.

ID	Duration	Flag	Source byte	Destination byte
1.	81	18	522	0
2.	12	61	0	0
3.	22	61	0	0
4.	65	184	520	0
5.	45	47	0	0
6.	66	28	522	0
7.	78	132	18	0
8.	45	134	0	0
9.	74	58	89	0
10	35	1	50	0

Table 2: Fragmentation of normal big-data set

Table 2 shows the fragmented details about the normal dataset. The datasets are collected from various network communication levels with various internet service providers' policy because, every internet service provider's policy can be differ from one to another.

4.3 Number of Login Vs Detected Malicious User

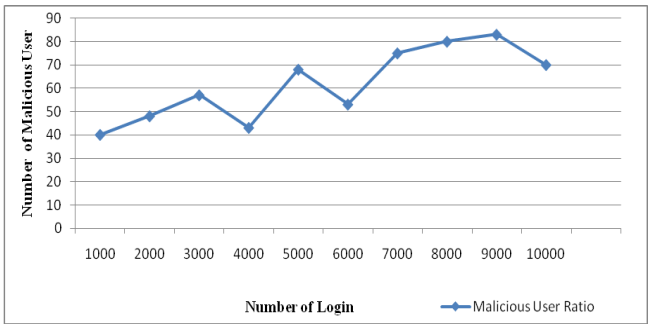

Figure 3: Number of Login Vs Detected Malicious User

Figure 3 shows the comparison between numbers of login to the number of malicious user. The fluctuations in the figure describe the malicious user's ratio increases gradually with respect to number of login.

4.4 Number of Malicious Request Vs Number of Honeypot System Response

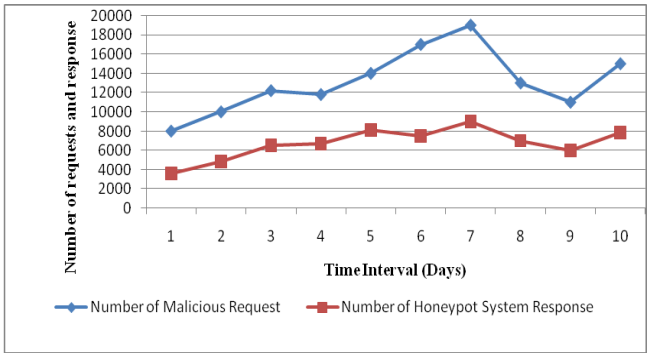

Fig.4 . Number of Malicious Request Vs Number of Honeypot System Response

The figure 4 shows the comparison between malicious user's request and the honeypot system response in the given time interval. It states that the honeypot system averagely responses to all the number of malicious request in the time interval.

4.5 Number of Token Generation Vs Minimized Computation Overhead of Proposed System

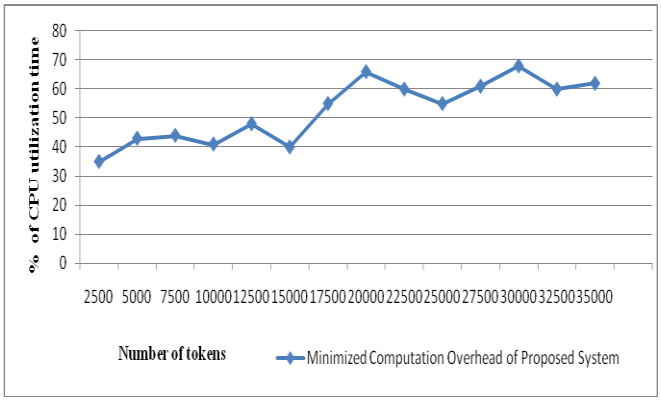

Fig. 5: Number of Token Generation Vs Minimized Computation Overhead of Proposed System

Figure 5 shows the comparison of CPU utilization with number of tokens. The results state that the utilization of CPU gradually increases with respect to number of tokens and also the computation overhead is reduced to 70% by this proposed system.

5. CONCLUSION

In this work, we have proposed a new approach Firecol Protection base Honeypot System (FPS-HPS) to reduce the network intrusion in the computer network. Our proposed approach consists of Firecol Protection Services, Load Balancer and Honeypot system which improves the performance of Intrusion detection system. The Load balancer generates tokens for authenticated user and attacker based on Firecol Protection Services result. It avoided unnecessary communication and computation on Firecol system and Load Balancer. It also reduced time and cost to the malicious internet packets which is discussed in the results and discussion section. The proposed Honeypot system is a irrelevant information handling system. The purpose of this research work was to describe what Honeypot systems are and their value to the system security community. The proposed Honeypot can be used for production purposes by detecting, preventing and responding to attacks. The proposed Honeypot system can also be used for research, collecting information on threats so they can better understand and defend against them.

6. REFERENCES

[1] H.J. Liao et al., Intrusion detection system: A comprehensive review, Journal of Network and Computer Applications 36 (2013) 16–24.

[2] G. Jacob Victor, Dr. M Sreenivasa Rao, Dr. V. CH. Venkaiah, Intrusion Detection Systems - Analysis and Containment of False Positives Alerts, International Journal of Computer Applications (0975 – 8887) Volume 5– No.8, August 2010.

[3] Andre Yee(January 22, 2004), NFR Security "Making false positives go away", http://www.computerworld.com/ securitytopics/security/story/0,10801,89122,00.html?f=x 15", accessed on 21.08.07.

[4] Swapnali, Sundar, Sadamate, Review Paper on Honeypot Mechanism – the Autonomous Hybrid Solution for Enhancing, International Journal of Advanced Research in Computer Science and Software Engineering 4(1), January - 2014, pp. 854-858

[5] Selvaraj, R., Kuthadi, V.M. & Marwala, T. (2015). An Effective ODAIDS-HPs approach for Preventing, Detecting and Responding to DDoS Attacks. British Journal of Applied Science & Technology, Vol.5 (5): 500-509

[6] (2007) The Honeypot Website. [Online]. Available: http://www.honeypots.net/

[7] William Stallings, Cryptography and Network Security: Principles and Practice, 2nd ed., Prentice-Hall, 2000.

[8] John Carroll, Computer Security, 3rd ed., Butterworth-Heinemann, 1997.

[9] Sainath Patil, Nageshri B Karhade, Yogini K Kothekar, Honeyweb: a web-based high interaction client honeypot , International Journal of Engineering Research and Applications (IJERA), March 2012.

[10] Christian Kreibich, Jon Crowcroft, Honeycomb . Creating Intrusion Detection Signatures Using Honeypots

[11] C. Stoll, The Cuckoo's Egg. Addison-Wesley, 1986.

[12] W. R. Cheswick, .An Evening with Berferd, in which a Cracker is lured, endured, and studied,. in Proceedings of the 1992 Winter USENIX Conference, 1992.

[13] Kuthadi, V.M, Rajendra.C & Selvaraj, R (2010). A study of security challenges in wireless sensor networks. JATIT Vol.20 (1):39-44.

[14] S. Ioannidis, A. D. Keromytis, S. M. Bellovin, and J. M. Smith, "Implementing a distributed firewall," in Proc. 7th ACM CCS, 2000, pp. 190–199, ACM Press.

[15] S. H. Khor and A. Nakao, "Overfort: Combating DDoS with peer-topeer DDoS puzzle," in Proc. IEEE IPDPS, Apr. 2008, pp. 1–8.

[16] R. Janakiraman, M. Waldvogel, and Q. Zhang, "Indra: A peer-to-peer approach to network intrusion detection and prevention," in Proc. IEEE WETICE, Jun. 2003, pp. 226–231.

[17] K. Hwang, S. Tanachaiwiwat, and P. Dave, "Proactive intrusion defense against DDoS flooding attacks," in Proc. Int. Conf. Adv. Internet, Process., Syst., Interdiscipl. Res., 2003 [Online]. Available: http://gridsec.usc.edu/hwang/papers/IEEES&P414Final.pdf

[18] L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, "Statistical approaches to DDoS attack detection and response," in Proc. DARPA Inf. Survivability Conf. Expos., 2003, pp. 303–314.

[19] Kuthadi, V.M., Selvaraj, R., & Marwala, T. (2015).An Efficient web services framework for secure Data collection Wireless sensor Network. British Journal of Science. Vol.12 (1):18-31.

[20] R. Mahajan, S. M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker, "Controlling high bandwidth aggregates in the network," Comput. Commun. Rev., vol. 32, no. 3, pp. 62–73, 2002.

[21] M. Vallentin, R. Sommer, J. Lee, C. Leres, V. Paxson, and B. Tierney, "The NIDS cluster: Scalable, stateful network intrusion detection on commodity hardware," in Proc. 10th RAID, Sep. 2007, pp. 107–126.