Detection of black hole attacks in Manet

Prerika Agarwal
Student Ajay Kumar Garg Engineering college

Sangita Rani Satapathy
Department of Computer Science& Engineering
Ajay Kumar Garg Engineering college

Abstract- Internet connectivity is turning out to be discriminating view point day by day. As the technology is advancing, there are more risks of the information to be accessible to users which are malicious while giving it to the regular clients and the likelihood of attack gets increasing in that ratio. An intrusion detection system is needed for network securing. Signature based detection is utilized for identifying attacks which are known since many attacks have particular signatures. An anomaly based IDS tries to identify suspicious activity on the framework. In this paper, a technique is proposed which is combination of both these techniques. These two techniques have disadvantages if they are used alone. So combination of these two techniques is implemented and packet delivery ratio and throughput of the system is increased than the existing systems. This system is also used for detecting black hole attacks.

Keywords— IDS, NIDS, WIPS, HIDS, IP

I. INTRODUCTION

Internet is a global public network. With the growth of the Internet and its potential, there has been subsequent change in various models of organizations across the world. More and more people are getting connected to the Internet every day to take advantage. Internetwork connectivity has therefore become very critical aspect of today's scenario. With the advent of new technologies from the internet, there are some risks while enjoying the technology. Risks are both harmless and harmful users on the Internet. While an organization makes its information system available to harmless Internet users, at the same time the information is available to the malicious users as well. Security of network is a critical field of computer science. With the development of the Internet as a medium for exchanges at wide scale of financial transactions and sensitive information, maintaining the integrity and security of messages which are sent over network of public is extremely critical. [1]

Increasing traffic of Internet obliges the backbone of operators and large end users to implement network links at high speed to match the demands of bandwidth. The bandwidth increase is apparent not on the backbone links only but the hosts of consumer are connected more and more with the capacity of bandwidth that was only available for enterprise clients only few years ago.

Nevertheless besides all the beneficial effects, this new infrastructure with high bandwidth shows novel challenges in the domain of robustness and security, as the manual oversight of such high volumes of traffic is almost not possible and the events having scale extraordinary are reported typically only. [2]

Security is a major problem for all networks in today’s environment of enterprise. Intruders and attackers have made numerous attempts to cut down web services and company networks at high profile. Numerous methods have been developed for securing the communication and infrastructure of network over the Internet, among them the utilization of virtual private networks, encryption and firewalls. Intrusion detection is a generally new expansion to such type of systems. The methods of intrusion detection began showing up in the most recent couple of years. By utilizing methods of intrusion detection, you can collect and utilize information from attacks of known type and figure out if anyone is attempting to attack your network or specific hosts. The collected information along these lines can be utilized to solidify the security of the network, and also for legal purposes. Both open source and commercial products are available now for this work. Numerous tools for assessment of vulnerability are likewise accessible in the market that can be utilized to assess various types of holes of security in the network. A comprehensive system of security comprises of multiple tools, comprising:

- Firewalls that are utilized to block undesirable incoming and in addition outgoing traffic of data. There is scope of products of firewall which are available in the market in commercial as well as Open Source products. The most common Open Source firewall is the Netfilter/Iptables. The most common products of commercial firewall are from Netscreen, Cisco and Checkpoint.
- Intrusion detection systems (IDS) which are utilized to see if somebody has gotten into or is attempting to get into your network. The very well known IDS is Snort, which is available at http://www.snort.org.
- The tools for assessment of vulnerability that are utilized to discover and plug holes of security which are present in your network. The information gathered from tools of assessment of vulnerability is

utilized to decide rules on firewalls so that these holes of security are defended from malicious users of Internet. There are various tools for assessment of vulnerability like Nessus (http://www. Nessus.org) and Nmap (http://www.nmap.org). [3]

II. INTRUSION DETECTION SYSTEM

An Intrusion Detection System is utilized to recognize a wide range of usage of computer and network traffic which is malicious which can't be detected by a traditional firewall. This incorporates attacks of network against vulnerable services, attacks based on host like privilege escalation, attacks which are data driven in applications, malware (worms, trojan horses and viruses) and unauthorized logins. [4]

Intrusion detection systems (IDSs) are generally deployed alongside other preventive mechanisms of security like authentication and access control, as a second line of guard that protects systems of information. There are numerous reasons that make detection of intrusion a vital part of the whole system of defense. Firstly, many conventional systems and applications to work in an alternative environment and may become vulnerable when deployed detection of intrusion supplements these mechanisms of protection to enhance the security of system. In addition, regardless of the possibility that the preventive mechanisms for security can protect systems of information successfully, it is still required to know what type of intrusions have occurred or are occurring, so that we can comprehend security risks and threats and in this way be better prepared for the attacks occurring in future. [5]

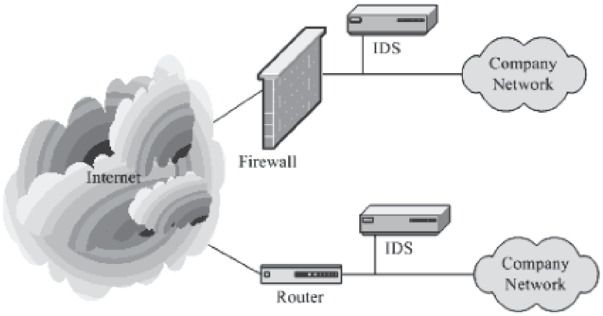

Fig. 1 Intrusion Detection System [5]

An IDS is composed of the following three components [4]:
1. Sensors: which sense the traffic of network or activity of system and create events.
2. Console: to monitor alerts and events and also control the sensors.
3. Detection Engine: that records events logged by the sensors in a database and utilizes an arrangement of rules to create alerts form the events of security which are received.

III. TYPES OF IDS

There are numerous ways to categorize an IDS relying upon the location and type of sensors and the procedure utilized by the engine for generation of alerts. In numerous basic implementations of IDS all the three components are consolidated in a single appliance or device.

1. Network Intrusion Detection System: A Network Intrusion Detection System (NIDS) is one regular type of IDS that examines traffic of network at all the layers of OSI (Open Systems Interconnection) model and settles on about the traffic purpose, examining suspicious action. Major NIDSs are very simple to install on a network and can regularly see traffic at once from many systems. A term turning out to be all the more generally utilized by vendors is "Wireless Intrusion Prevention System" (WIPS) to depict a device of network that analyzes and monitors the radio spectrum which is wireless for intrusions.

2. Host Based Intrusion Detection System: Host based intrusion detection systems (HIDS) examine traffic of network and settings which are system specific like local log audits, local security policy, software calls and many more. There must be installation of HIDS on every machine and needs configuration particular to that software and operating system. [6]

IV. TECHNIQUES FOR DETECTING INTRUSION

There are mainly two techniques which are used for detecting intrusions:

1. Signature Based Detection: Signature based detection is the most common method that antivirus software uses to identify malware. This method is somewhat limited by fact that it can only identify a limited amount of emerging threats, e.g. generic, or extremely broad, signature. Signature based detection works in a similar fashion to a virus scanner. This style of detection relies on rules and tries to associate possible patterns to intrusion attempts. Viruses are known to often attempt a series of steps to penetrate a system.

2. Anomaly Based Intrusion Detection: Anomaly-based intrusion detection is a newer method in the fight against exploits and misuse. By itself, anomaly-based detection is not a cure-all. But when used in conjunction with an effective signature-based detection solution, anomaly based detection is a viable and effective means of protecting your network infrastructure and your company is ability to do business. Anomaly-based intrusion detection triggers an alarm on the IDS when some type of unusual behavior occurs on your network. This would include any event, state, content, or behavior that is considered to be abnormal by a pre-defined standard. [7]

V. RELATED WORK

Lots of work have been done in the area of intrusion detection and also in signature based intrusion detection as well as anomaly based intrusion detection. Some important work in the area of intrusion detection is as follows:

In reference [8], a survey has been done on the techniques of anomaly detection and clustering. As the technology is propelling, there is danger of information which is available to the malicious users while giving it to the normal users and the possibility of attack is also increasing in that ratio. An intrusion detection system is required for securing network. Signature-based detection is used for detecting known attacks as many attacks have distinct signatures. An anomaly-based IDS tries to find suspicious activity on the system. Clustering is suitable for anomaly detection, since no knowledge of the attack classes is needed whilst training. In this paper a survey has been done on anomaly detection techniques and clustering. It also consist idea to our research of integrating Snort with Clustering Algorithm for anomaly detection.

In Paper [9], authors propose a method of anomaly detection with fast incremental clustering. Anomaly detection in information (IP) networks, detection of deviations from what is considered normal, is an important complement to misuse detection based on known attack descriptions. Performing anomaly detection in real-time places hard requirements on the algorithms used. First, to deal with the massive data volumes one needs to have efficient data structures and indexing mechanisms. Secondly, the dynamic nature of today’s information networks makes the characterisation of normal requests and services difficult. What is considered as normal during some time interval may be classified as abnormal in a new context, and vice versa.

Reference [10] presents a Network Intrusion Detection System (NIDS) embedded in a smart-sensor-inspired device under a service-oriented architecture (SOA) approach which is able to operate independently as an anomaly-based NIDS, or integrated transparently in a Distributed Intrusion Detection System (DIDS). The proposal is innovative because it combines the advantages of the smart sensor approach and the subsequent offering of the NIDS functionality as a service with the SOA use to achieve their integration with other DIDS components. The main goal of this paper is to reduce the huge volume of management tasks inherent to this type of network services, as well as facilitating the design of DIDS whose managing complexity could be restricted within well-defined margins. This paper also addresses the construction of a physical sensor prototype.

In reference [11], author addresses the security issues of storing sensitive data in a cloud storage service and the need for users to trust the commercial cloud providers. It proposes a cryptographic scheme for cloud storage, based on an original usage of ID-Based Cryptography. Our solution has several advantages. First, it provides secrecy for encrypted data which are stored in public servers. Second, it offers controlled data access and sharing among users, so that unauthorized users or un-trusted servers cannot access or search over data without client's authorization.

In paper [12], a survey of anomaly detection methods in networks is presented. Despite the advances reached along the last 20 years, anomaly detection in networks is still an immature technology, Nevertheless, the benefits which could be obtained from a better understanding of the problem itself as well as the improvement of these methods. Therefore, in this paper we present a survey on anomaly detection in networks. In order to distinguish between the different approaches used for anomaly detection in networks in a structured way, we have classified those methods into four categories: statistical anomaly detection, classifier based anomaly detection, anomaly detection using machine learning and finite state machine anomaly detection. We describe each method in details and give examples for its applications in networks.

VI. MOTIVATION

One fundamental problem of intrusion detection research is the limited availability of good data to be used for evaluation. Producing intrusion detection data is a labor intensive and complex task involving generation of normal system data as well as attacks, and labeling the data to make evaluation possible. The techniques for detecting intrusion have disadvantages if they are used alone.

The main drawback of signature based IDS is failure to identify novel attacks, and sometimes even minor variations of known patterns. Anomaly detection has an advantage over signature-based detection in that a new attack for which a signature does not exist can be detected if it falls out of the normal traffic patterns.

But there is also drawback of anomaly detection as it suffer high false detection rate. Thus it is needed to combine both algorithms which are signature based and anomaly based in order to improve the detection of new malicious packet and reduce excessive false alarm rate.

There are two main approaches to study or characterize the ensemble behavior of the network: the first is inference of the overall network behavior and the second is to analyze behavior of the individual entities or nodes. The approaches used to address the anomaly detection problem depend on the nature of the data that is available for the analysis. Network data can be obtained at multiple levels of granularity such as network-level or end-user-level.

The main objective is to combine signature-based algorithm and anomaly detection algorithm to improve the detection of new malicious packet and reduce excessive false alarm rate. This objective will be achieved by integrating Anomaly Detection using AODV routing with Signature-based detection using RSA cryptography.

VII. PROPOSED SCHEME

In order to implement the objective, we combine both the techniques i.e. cryptography and anomaly based detection and get better performance of packet delivery ratio.

Anomaly-based intrusion detection is a newer method in the fight against exploits and misuse. By itself, anomaly-based detection is not a cure-all. But when used in conjunction with an effective signature-based detection solution, anomaly based detection is a viable and effective means of protecting your network infrastructure and your company is ability to do business.

An anomaly is defined as something that is not nominal or normal. Simply put, anomaly-based intrusion detection triggers an alarm on the IDS when some type of unusual behavior occurs on your network. This would include any event, state, content, or behaviour that is considered to be abnormal by a pre-defined standard. Anything that deviates from this baseline of normal behaviour will be flagged and logged as anomalous. Normal behaviour can be programmed into the system based on offline learning and research or the system can learn the normal behaviour online while processing the network traffic.

Cryptography Algorithm:-

There are various cryptography algorithms, which can be divided into two broad categorize –

- Symmetric key cryptography
- Public key cryptography

1. *Symmetric Key Cryptography:-* The cipher, an algorithm that is used for converting theplaintext to ciphertext, operates on a key, which is essentially a specially generated

   number (value). To decrypt a secret message (ciphertext) to get back the original message (plaintext), a decrypt algorithm uses a decrypt key.

In symmetric key cryptography, same key is shared, i.e. the same key is used in both encryption and decryption.

2. *Public key Cryptography:*

In public key cryptography, there are two keys: a private key and a public key. The public key is announced to the public, where as the private key is kept by the receiver. The sender uses the public key of the receiver for encryption and the receiver uses his private key for decryption

VIII. RESULTS AND DISCUSSIONS

This section presents the simulated results of combination of cryptography and anomaly based detection. The performance of packet delivery ratio and throughput gets improved than the existing systems.

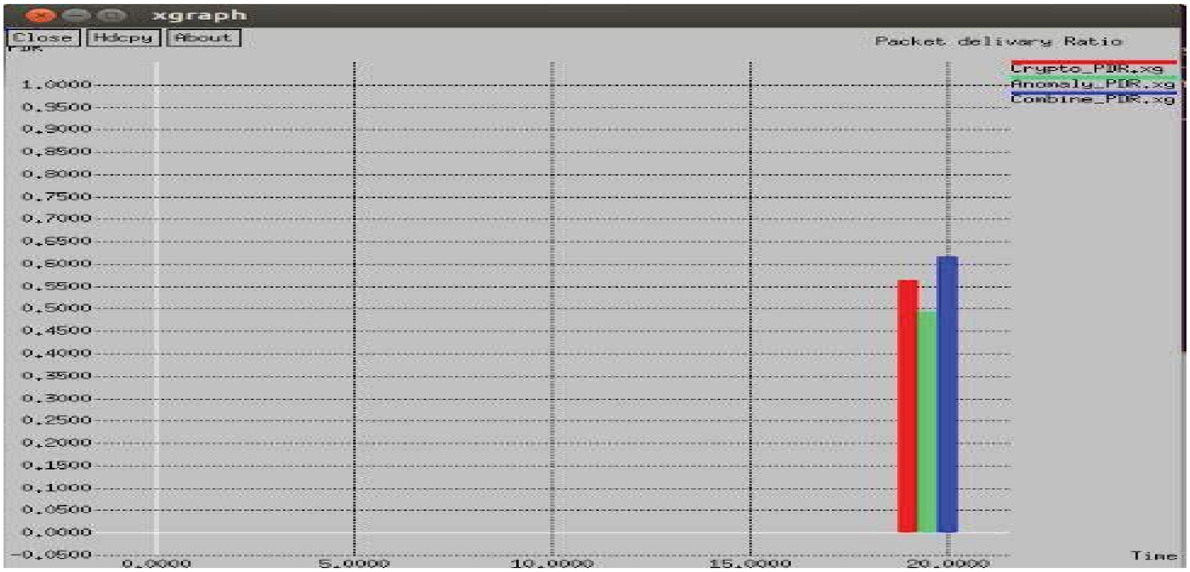

Fig. 3 Packet Delivery Ratio

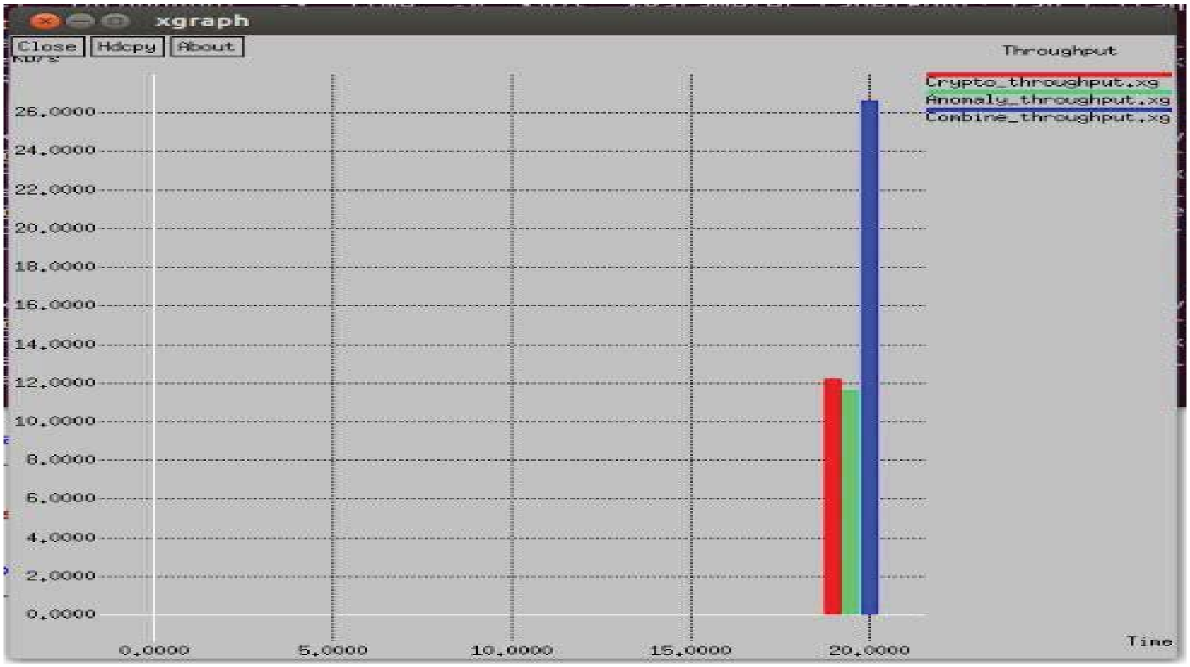

Fig. 4 Throughput of the system

IX. CONCLUSION

The main aim of this research work is to combine cryptography technique and anomaly based intrusion detection technique. The packet delivery ratio and throughput of the system gets increased which is better performance than the already existing techniques. In this method, black hole attack is detected. In future, this scheme can be implemented to detect wormhole attack and also various other attacks that effect performance of the network.

REFERENCES

[1] Alec Yasinsac, Sachin Goregaoker, “An Intrusion Detection System for Security Protocol Traffic” Department of Computer Science, Florida State University.

[2] Martin Rehak, Michal Pechoucek, Karel Bartos, Martin Grill, Pavel Celeda, Vojtech Krmicek, “CAMNEP: An intrusion detection system for high-speed networks”, Progress in Informatics, No. 5, pp 65-74, 2008.

[3] Rafeeq Ur Rehman, “Intrusion Detection Systems with Snort”, Prentice Hall PTR, New Jersey.

[4] Dhawal Khem, Harin Vadodaria, Manish Aggarwal, Mitesh M. Khapra, Nirav Uchat, “Intrusion Detection Systems”, Indian Institute of Technology, Mumbai.

[5] Amrita Anand, Brajesh Patel, “An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 8, August 2012.

[6] Tzeyoung Max Wu, “Intrusion Detection Systems”, Information Assurance Tools Report, Sixth Edition, Spetember 2009.

[7] Nitin.; Mattord, verma (2008). Principles of Information Security. Course Technology. pp. 290– 301. ISBN 978-1-4239-0177-8.

[8] Prerika Aggarwal, Sangita Rani Satapathy, “Integartion of Signature Based and Anomaly Based Detection”, International Journal of Computer Science and Network, Vol. 3, Issue 3, June 2014.

[9] Burbeck K, Nadjm-Tehrani S. “ADWICE – anomaly detection with fast incremental clustering” In: Proceedings of the seventh international conference on security and cryptology (ICICS’04). Springer Verlag; December 2004**.**

[10] Maci - rez, F. Mora-Gimeno, F. Marcos-Jorquera, D. il-Mart nez-Abarca, J.A. “Network Intrusion Detection System Embedded on a Smart Sensor” Dept. of Comput. Sci. & Technol., Univ. of Alicante, Alicante, Spain.

[11] Boudguiga, A. ; Laurent, M. Kaaniche, N. “ID Based Cryptography for Cloud Data Storage” Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on June 28 2013-July 3 2013.

[12] Weiyu Zhang Qingbo Yang ; Yushui Geng “A Survey of Anomaly Detection Methods in Networks”, Computer Network and Multimedia Technology, 2009. CNMT 2009. International Symposium on 18-20 Jan. 2009.

[13] Manasi Gyanchandani, J.L. Rana, R.N. Yadav “Taxonomy of Anomaly Based Intrusion Detection System: A Review” International Journal of Scientific and Research Publications, Vol.2, Issue 12, December 2012.

[14] Hichem Sedjelmaci, Mohamed Feham, “Novel Hybrid Intrusion Detection System for Clustered Wireless Sensor Network”, International Journal of Network Security & Its Applications, Vol. 3, No. 4, July 2011.

[15] Shaimaa Ezzat Salama, Mohamed I. Marie, Laila M. El-Fangary, Yehia K. Helmy, “Web Anomaly Misuse Intrusion Detection Framework for SQL Injection Detection”, International Journal of Advanced Computer Science and Applications, Vol. 3, No. 3, 2012.

[16] Sheetal Thakare, Pankaj Ingle, Dr. B.B. Meshram, “IDS: Intrusion Detection System the Survey of Information Security”, International Journal of Emerging Technology and Advanced Engineering, Vol.2, Issue 8, August 2012.