# Wireless Intrusion Detection System using Reputation

**Santosh L Bidve, Bhushan S Deshmukh, Abhilash G Chamwad, V K Pachghare, Rahul B Adhao**

***Abstract*—Development in the field of Information Technology has led to increase in speed of Internet. With the increase in internet users there is a tremendous increase in network traffic. Increase in network traffic has also increased the threat of intrusion over the network. For the ever growing internet speed there is a necessity to modify the intrusion detection system in order to detect the intrusion threats across the network. In order to meet these needs of Intrusion detection system we can use the combination of packet based and flow based systems. Reduction of false alarm is also a matter of concern in intrusion detection.**

***Index Terms*—Intrusion Detection, Reputation, IP Flow, Packet Flow.**

## I. INTRODUCTION

Today's generation can access the internet very easily. Use of internet is increasing day by day. Internet is used in wide aspects of daily life such as online gaming, online shopping, social networking etc. Such an increase in internet has led to tremendous increase in Network traffic. With the increase in usage of internet there is also increase in wireless networking. Wireless Network can be accessed through mobiles, laptops with equivalent speed. With the development in internet large number of intrusion threats are introduced in the network. It is becoming very hard to detect the threats in such a high speed network traffic. Hence security is becoming the main concern. Packet based approach for network intrusion detection system over such a high speed network system is becoming impossible. Hence for efficiency in intrusion detection combination of both packet based and flow based intrusion detection must be used. Intrusion Detection is essential in protecting computer networks from threats. ID systems are categorized depending upon either position or approach used in intrusion detection.

**Revised Manuscript Received on 30 November 2015.**

***** Correspondence Author

**Santosh L Bidve*,** Department of Computer Engineering and Information Technology, College of Engineering Pune, Shivajinagar, Pune, (Maharashtra). India.

**Bhushan S Deshmukh,** Department of Computer Engineering and Information Technology, College of Engineering Pune, Shivajinagar, Pune, (Maharashtra). India.

**Abhilash G Chamwad,** Department of Computer Engineering and Information Technology, College of Engineering Pune, Shivajinagar, Pune, (Maharashtra). India.

**V K Pachghare,** Department of Computer Engineering and Information Technology, College of Engineering Pune, Shivajinagar, Pune, (Maharashtra). India.

**Rahul B Adhao,** Department of Computer Engineering and Information Technology, College of Engineering Pune, Shivajinagar, Pune, (Maharashtra). India.

An intrusion detection system (IDS) is a type of security

## II. INTRUSION DETECTION SYSTEM

An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.
software designed to automatically alert administrators when someone or something is trying to compromise information system through malicious activities or through security policy violations. An IDS works by monitoring system activity through examining vulnerabilities in the system, the integrity of files and conducting an analysis of patterns based on already known attacks. Intrusion Prevention Systems (IPS) extended IDS solutions by adding the ability to block threats in addition to detecting them and has become the dominant deployment option for IDS/IPS technologies. An IDS needs only to detect threats and as such is placed out-of-band on the network infrastructure, meaning that it is not in the true real-time communication path between the sender and receiver of information. Rather, IDS solutions will often take advantage of a TAP or SPAN port to analyse a copy of the inline traffic stream (and thus ensuring that IDS does not impact inline network performance). IDS is a listen-only device. The IDS monitors traffic and reports its results to an administrator, but cannot automatically take action to prevent a detected exploit from taking over the system. Attackers are capable of exploiting vulnerabilities very quickly once they enter the network, rendering the IDS an inadequate deployment for prevention device.

## III. INTRUSION DETECTION SYSTEM CLASSIFICATION

Depending upon position IDS are divided into two types i.e. Host based IDS or Network based IDS. Depending upon the approach used IDS are divided into two types i.e. Signature based IDS and Anomaly based IDS.

**A network-based intrusion detection system** (NIDS) is used to monitor and analyze network traffic to protect a system from network-based threats. A NIDS reads all inbound packets and searches for any suspicious patterns. When threats are discovered, based on its severity, the system can take action such as notifying administrators, or barring the source IP address from accessing the network. Intrusion detection systems (IDSs) are available in different types; the two main types are the host-based intrusion system (HBIS) and network-based intrusion system (NBIS). Additionally, there are IDSs that also detect movements by searching for particular signatures of well-known threats. A NIDS tries to detect malicious activity such as denial-of-service attacks, port scans and attacks by monitoring the network traffic.

**A host-based intrusion detection system** (HIDS) is a system or a program employed to protect critical computer systems containing crucial data against viruses and other Internet malware. Starting from the network layer all the way up to the application layer, HIDS protects from known and unknown malicious attacks. HIDS regularly checks the characteristics of a single host and the various events that occur within the host for suspicious activities. HIDS can be implemented on various types of machines, including servers, workstations, and computers.

In **signature based IDS**, the IDS analyses the information it gathers and compares it to large databases of attack signatures. Essentially, the IDS looks for a specific attack that has already been documented. Like a virus detection system, signature based IDS software is only as good as the database of attack signatures that it uses to compare packets against.

In **anomaly based IDS**, the system administrator defines the baseline, or normal, state of the network traffic load, breakdown, protocol, and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies.

## I. EFFICIENCY PARAMETERS OF IDS

Performance and accuracy are the two vital parameters in IDS. The rate at which the audit events are processed determines the performance of the IDS. IDS with poor performance neglect to recognize real time attacks and make important move quickly. While on the other hand accuracy deals with two characteristics which are sensitivity and selectivity. In the case of accuracy, if the IDS is very sensitive it will lead to low false negative rate while if it is very selective it leads to low false positive.

## II. REPUTATION

The concept of reputation is generally used in the area of network security for tasks like email spam detection, etc. The reputation in systems administration is practically equivalent to the idea of reputation in human culture. Reputation is defined simply as the collective observation, by a society, of a particular nodes past behaviour. By reputation we mean an estimate about a node’s actual quality in terms of its behaviour in the network, which is sometimes also referred as *trust*. Nodes keep track of their peers’ behaviour and exchange this information with others in order to compute a reputation value about other nodes. Nodes with good reputation are then favoured. Such a reputation can be formed locally on a system based on the information that is seen and analyzed on that system, or globally based on information and events analyzed and shared between groups. Between two nodes A and B, to determine the reputation of node B, node A takes into account the communications and iterations between them. If node A suspects about the confidence of node B, node A can ask other nodes for their respective reputation values for node B. The most shared opinion about the confidence of node B can confirm or discard the suspicions of node A.

A variety of trust models exist. The three distinct modelling approaches are:

1) Mechanisms deriving trust via certificates, rules, and policies

2) Centralized trust mechanisms in which witness observations are collected by a central authority; also known as centralized reputation mechanisms.

3) Decentralized systems

In each model, the agent evaluating the trustworthiness of another is called an evaluator, while the evaluated agent is called the target. The evaluator may query witnesses with direct experience with the target. The witnesses respond to the evaluator's queries with ratings. The collective ratings impact the target's reputation, which the evaluator uses along with internal criteria to determine the target's trustworthiness.

In case of centralized reputation mechanisms, following an interaction, a witness conceptually rates the target according to the perceived level of service received. The rating is stored centrally and combined with other ratings to allow the centralized evaluator to determine the resulting reputation.

This reputation can then be used as a criterion by which other agents decide whether to engage the reputation holder, or how to treat any information provided by the reputation holder.

Example of a multi agent system employing reputation is SPORAS [155], 45 which updates reputations with each receipt of a rating according to the following principles [80]:

1. New users start with a minimum reputation value, building up reputation during their activity on the system

2. The reputation value of a user never falls below the reputation of a new user

3. After each transaction, the reputation values of the involved users are updated according to the feedback provided by other parties, which correct their trustworthiness in the latest transaction

4. Users with very high reputation experience much smaller rating changes with each update

5. Ratings must be discounted according to age so that the most recent ratings have more weight in the evaluation of a user's reputation.

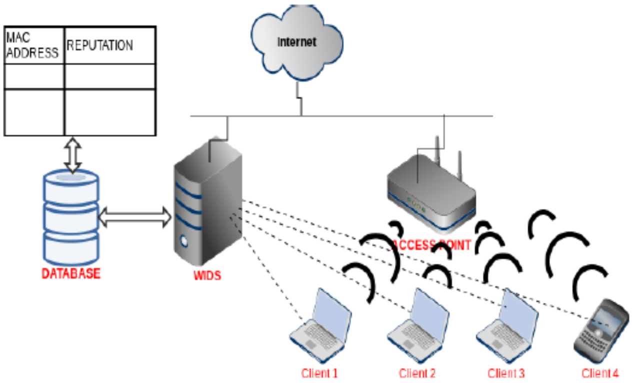
## III. PROPOSED SYSTEM

Due to easy access of the internet the use of Internet has grown tremendously. Due to increased use of Internet the number of packets flowing through the monitoring point is very high. So NIDS running on such monitoring points must be fast so that users get fast access to the request and it must also be accurate at the same time. So the NIDS must be quick in handling the packets. NIDS for such fast networks must mainly focus on efficiency parameters of performance and accuracy. Packet based and Flow based monitoring are the two options that the NIDS can use. Using packet based approach in this case would be very ineffective because we will require a lot of time in monitoring each packet individually and that will affect the performance at a great level. The other option is flow based monitoring of network traffic. The flow based system will monitor the flow, number of packets flowing through the access point, over the network and depending on the flow it will tell whether intrusion has occurred or not.

*Published By:*
*Blue Eyes Intelligence Engineering*
*and Sciences Publication (BEIESP)*

The flow based methodology consists of two steps -flow exporting and flow collection. After the flow is caught by flow exporter it is provided to flow collector. The data given from exporter to collector is called as flow records [12]. These flow are monitored to check for intrusion. Speed is not an issue in case of Flow based system but these systems may lead to any false negative. Thus accuracy is the issue here. As stream is aggregated view of data it cannot give precision as it is given by packet based inspection. So, we propose a system that uses combination of both Flow based ID and Packet based ID for the fast flowing traffic. The system works in two stages, Firstly the flow based ID will try to detect intrusions from suspicious flow, and then the packets in that flow will be feed to second stage to inspect the packets for intrusions. The reputation is used for the IP addresses-one of the distinguishing characteristics of a flow of data packets-which is stored at a central database with the IDS. Reputation is used for a particular MAC address to check the actual quality in terms of its behavior in the network or an opinion that is gathered and maintained based on information in the past, which is also referred to as trust. Reputation helps us to monitor traffic based on relative level of suspicion. Initially all the devices are given a specific value of reputation. These values are stored in reputation database. Later, depending on the behavior of the device in the network these values in the reputation database are modified. An IP address with higher reputation can be given lesser inspection. Further, if the reputation of particular device falls under a particular value then access of that device can be blocked. Thus reputation database helps in improving the efficiency of the IDS.

## IV. ARCHITECTURE OF PROPOSED SYSTEM



## V. CONCLUSION

The proposed system deals with rapidly increasing network speed. The combination of packet and flow based system helps in providing greater accuracy and speed. The use of reputation is making the detection of malicious flow easier at the high traffic networks, as the reputation of the devices in the network will be used. The combination packet and flow based approaches with reputation not only gives a faster and accurate system but reduces false positives as well.

## REFERENCES

1. Bernard Menezes, “Network Security and Cryptography”, Cengage Learning, pp. 235-237.
2. Dr. V K Pachghare , “Cryptography and Information Security”, PHI publication
3. Rahul B Adhao, Avinash R Kshirsagar, Dr. V K Pachghare,”Reputation Based Fast Intrusion Detection”2014
4. F. Sabahi and A. Movaghar, “Intrusion Detection: Survey”, The Third International Conference on System and Network communications, 2008, pp. 23-26.
5. M. Sharma , A Kaushik, A. Sanghwan “ Performance Analysis of Real time Intrusion Detection and Prevention System Using Snort”, International Journal of Engineering Research and Technology, (IJERT), July 2012.
6. C. Kruegel, F. Valeur and G. Vigna, “Intrusion Detection and Correlation: Challenges and Solutions”, Springer- Verlag Telos, 2004.
7. Keldor Gerrigagoitia , Roberto Uribeetxeberria , Urko Zurutuza , and Ignacio Arenaza,”Reputation-based Intrusion Detection System for wireless sensor networks”.
8. Trung Dong Huynh “Trust And Reputation in Open Multi-Agent System”.
9. Chinyang Henry Tseng, Poornima Balasubramanyam, “Specification Based Intrusion Detection Model for OLSR”.
10. L Premaajeshwari, “Enhanced Intrusion Detection Techniques for mobile Ad Hoc networks”.
11. Anna Sperotto and Aiko Pras, “Flow Based Intrusion Detection System”, 12th IFIP/IEEE 2011: Dissertation Digest, 2011, pp. 958-963.
12. G. Sadasivan, N. Brownlee, B. Claise, “Network Working Group” RFC 5470