# Design of Hybrid Network Anomalies Detection System (H-NADS) Using IP Gray Space Analysis

Yogendra Kumar JAIN, Sandip S. PATIL
Samrat Ashok Tech. Inst., Vidisha (India)
{ykjain_p|san_78004}@yahoo.co.in

*In Network Security, there is a major issue to secure the public or private network from abnormal users. It is because each network is made up of users, services and computers with a specific behavior that is also called as heterogeneous system. To detect abnormal users, anomaly detection system (ADS) is used. In this paper, we present a novel and hybrid Anomaly Detection System with the uses of IP gray space analysis and dominant scanning port identification heuristics used to detect various anomalous users with their potential behaviors. This methodology is the combination of both statistical and rule based anomaly detection which detects five types of anomalies with their three types of potential behaviors and generates respective alarm messages to GUI.*
***Keywords:*** *Network Security, Anomaly Detection, Suspicious Behaviors Detection.*

## 1 Introduction

As network is having a very big and heterogeneous environment, many large and important applications are running at side by side on the network. To handle all these issues, the network security must consider the behavior of the outside users from the internet which may cause the harm to the network and becomes anomalous users. The challenge of detection of anomalous host is accepted by anomaly detection system.

We present three steps Methodology which is used to detect external anomalous host with their scanning behaviors using IP gray space analysis and scanning foreign port used by them. IP gray space is a collection of unassigned IP addresses in a campus network which are not assigned to any active host [1].

### 1.1 Background and Motivations

Intrusion Detection technique is classified in two categories: signature based misuse detection and anomaly detection [2] [3]. In signature based misuse detection technique, approaches are strictly limited to the known abnormal users only. How to detect newly identified abnormal users is one of biggest challenge faced by signature or misuse detection [4]. To overcome this limitation of signature based misuse detection, the concept of anomaly detection was introduced in the work of Denning [5]. According to Denning security, violations could be detected by inspecting abnormal system usage patterns from the audit data.

In reality, most Anomaly Detection Techniques attempts to set up normal activity profiles by computing various metrics and an intrusion is detected when the actual system behavior deviates from the normal profiles [6]. The main advantage of anomaly detection is that, it does not require prior knowledge of intrusion and can thus detect new intrusions. But detecting any attack regardless of whether they are known or unknown with their potential behavior is the major challenge, which is not experienced in early IDS and ADS research. The proposed system overcomes these problems in signature based misuse detection and conventional anomaly detection system. We have designed and implemented a novel network Anomaly Detection System (ADS), which uses both IP gray space analysis and dominant scanning port identification heuristics (DSPI). The proposed ADS system detects three categories of anomaly with their potential behaviors for the campus network. In this paper, we apply the novel notion of IP gray space analysis [1].

### 1.2 Introduction to Network Anomaly Detection

Anomaly is a behavior based system which detects normal and abnormal users in system. An anomaly detection system establishes baseline for all users and depends on it decides anomaly [10]. Network anomaly is an abstraction of existing intrusion detection techniques to the network level allowing us to simultaneously monitor the security of multiple nodes as well as the network infrastructure. Network anomalies typically refer to circumstances when network operations deviate from normal network behavior. The anomalies can arise due to various causes such as malfunctioning network devices, bad configuration in

network services and operating systems, network overload, malicious denial of service attacks, ill advised applications installed by users, high level users' effort to discover network and gather information about it and its devices. These anomalous events will disrupt the normal behavior of some network data [6] [7].

Anomaly detections systems can detect previously unknown attacks [10]. By defining what's normal, they make it possible to identify any variations, no matter whether it is part of the threat model or not

- Faults can be detected indirectly by using pattern matching by considering the behavior of fault this can happened in anomaly detection system
- The goal of Anomalies detection is too able to detect a wide range of abnormal behavior as Ill as malicious intrusions including those for which no previous detection signature exist
- Anomalies detection is statistical in nature and work on the concept of measuring the number of events happening in given time interval for a monitored metric. A simple example of logging in which the incorrect password too many times, causing as account to be locked out and generating a Message to the security log. NAD system can monitored unusual user account activity, excessive file and object access, high CPU utilization inappropriate protocol used, unusual login frequency, high number of concurrent login, high number of sessions, any code manipulations, unusual content . All these features of ADS is used in authentication.

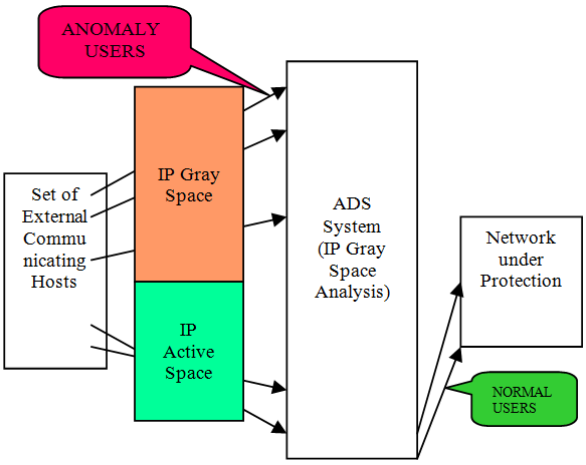


**Fig. 2.** Distributions of Gray IP and Active IP Addresses

Anomaly detection system is statistical based or rule based. Statistical based anomaly detection system gathers network traffic and generates statistics and according to that statistics it detects anomaly. Rule based anomaly detection system is

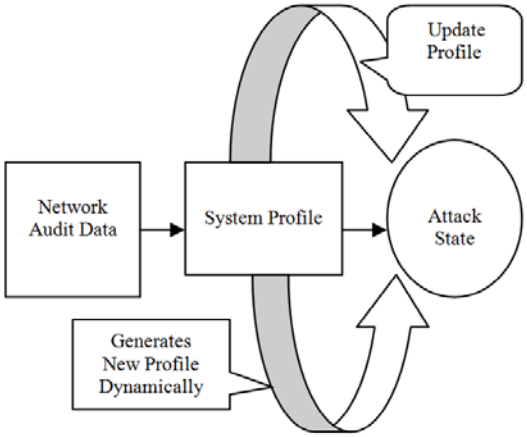


**Fig. 1.** Typical Anomaly Detection Advantages of Anomaly Detection System over Misuse Detection system

having association or heuristic rules with it and according to these rules it detects anomaly. The methodology that we are going to develop is the combination of both statistical and rule based anomaly.

## 2 Introduction to IP gray space and IP active space analysis

Campus or enterprise networks often have many unassigned IP addresses that collectively form IP gray space within the address blocks of such networks [1][8]. The IP space is divided into two address blocks: IP gray space and IP active space. All IP addresses are not likely to be assigned to "active" hosts (i.e., actual machines such as servers, desktops, lap tops, etc.) at any given time period. We refer to these IP addresses within the campus network that are not assigned to any host throughout a given time period, say, an hour or a day, as "inactive" or gray IP addresses. In contrast, the IP addresses within the same address blocks that are assigned to hosts at any point within the time period are referred to as active IP addresses.

The inactive IP addresses collectively forms IP gray space [1] within the address blocks, while active addresses the active space. By definition, IP gray and active space within a campus or any network are time dependent in other words, they are not fixed and vary over time. Unlike the all studied IP "dark space" analysis techniques which are inherently ex situ and can potentially be evaded, IP gray space analysis is in situ and provides us with a direct means to monitor, identify and track anomalous, suspicious and poten-

tially harmful activities launched by the anomalous hosts. In particular, I observe the traffic generated by outside hosts towards both the IP gray space and active space of a network, and correlate them to infer the nature of activities engaged by the outside hosts and isolate potentially harmful ones, which is an anomalous user. After all, it is live hosts (behind active IP addresses) that outside attackers are interested. I will use a simple heuristic algorithm for extracting the IP gray space within a campus/enterprise network, and applied IP gray space analysis for dissecting and classifying various scanning activities of outside and inside hosts.

### 2.1 IP Gray Space Identification

Let I denote the collection of all IP addresses of a network under consideration, and t0 the starting time of a time period of interest, and T the length of the period. We say an (inside) IP address $g \in I$ is a gray (or inactive) address over the time period [t0, t0+T] if and only if no traffic originating from g is observed during [t0-Ť, t0 +T + Ť ] for some fixed Ť. G denotes the collection of all gray IP addresses within the time period, or IP gray space. The Complementary set, A = I-G, is referred to the active space. In other words, for any $a \in A$, there is traffic originating from a at some time during [t0-Ť, t0 +T + Ť] thus a is likely as-

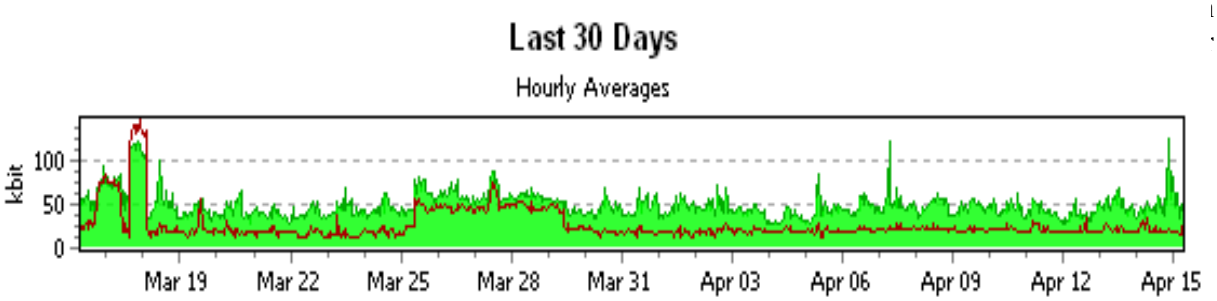


**Fig. 3.** Network Traffic Using IP Active Space and Gray Space

| | 8/19/2008 2:45:00 PM - 8/19/2008 3:00:00 PM | | | | | |
|---|---|---|---|---|---|---|
| | **Source IP** | **Source Port** | **Destination IP** | **Destination Port** | **Protocol** | **Volume** |
| 1 | SSPComputer (192.168.13.59) | 137 (NETBIOS) | [192.168.255.255] | 137 (NETBIOS) | UDP | 8648 bytes |
| 2 | 192.168.1.7 | 137 (NETBIOS) | [192.168.1.255] | 137 (NETBIOS) | UDP | 3036 bytes |
| 3 | [192.168.13.1] | 137 (NETBIOS) | [192.168.255.255] | 137 (NETBIOS) | UDP | 2484 bytes |
| 4 | N/A | 68 | Broadcast (255.255.255.255) | 67 | UDP | 2360 bytes |
| 5 | [192.168.111.17] | 137 (NETBIOS) | [192.168.255.255] | 137 (NETBIOS) | UDP | 1320 bytes |
| 6 | [192.168.1.1] | 67 | Broadcast (255.255.255.255) | 68 | UDP | 1264 bytes |
| 7 | 192.168.255.21 | 138 (NETBIOS) | [192.168.255.255] | 138 (NETBIOS) | UDP | 1159 bytes |

**Fig. 4.** Traffic Scanning for IP Gray Space Analysis at our campus network

### 2.2 IP Gray Space Characteristics

We apply the proposed heuristic to the PRTG Network Traffic Grapher at the router of our ADS client server network in our campus network.

Since no traffic is observed to originate from a gray IP address to any outside host (in the rest of the Internet) for an entire day, it is likely that the address is not assigned to any live host during that day. Ideally one would expect no traffic from any outside host either. This is in general not true at all because external anomalous host doesn't know the IP space.

### 2.3 Anomaly Detection using IP gray space analysis

This work involves the development of three step methodology.

**Step1:** Identification of anomalous external host using IP gray space and relative uncertainty.

In the first step, we set an IP active threshold range that range is called as IP active space. Such a threshold setting is called as association rule generation [11] for supervised learning. If source IP address of communication host is comes from IP Active Space then the respective communicating host is a normal user. In contrast, if communicating host uses gray then that will be anomalous host. To implement this step, we set up thresholds for IP Active Space (192.168.55.1 to 192.168.55.254) if any host crosses that threshold of IP active space then it will be anomalous host.

Here we are calculating relative uncertainty (RU). Relative Uncertainty is standardized entropy which detects observational variety of any anomalous host.

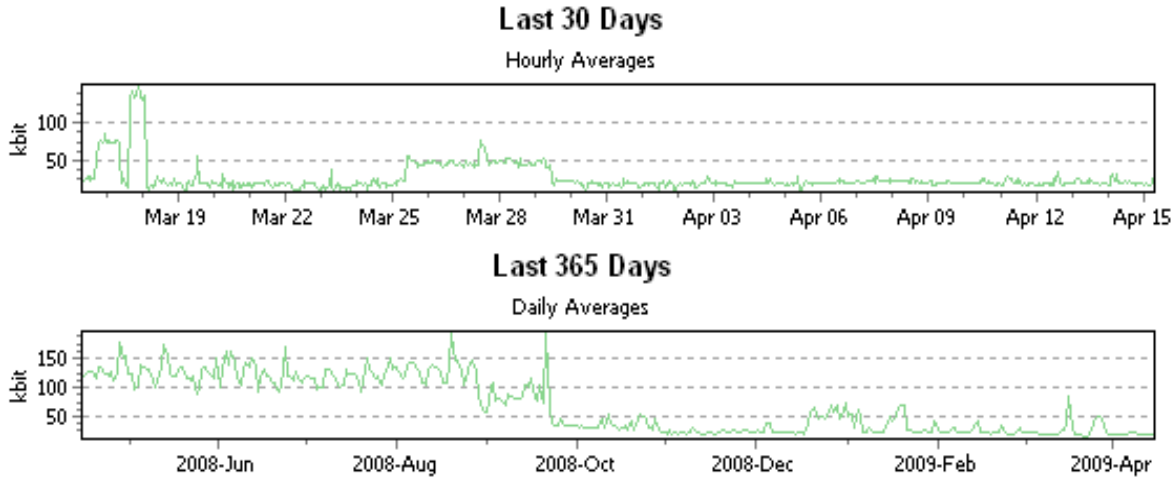


**Fig. 5.** Traffic generated by Gray IP at our campus network

Let Os be the set of outside hosts that we have to characterize for checking anomaly. For any h∈ Os, let GF (h) denote the collection of gray flows generated by h. The destination ports (dstPrt in short) used by gray flows in GF (h) induce an empirical distribution, for each dstPrt i, pi: = mi/m where mi is the number of gray flows in GF (h) with dstPrt i, and m is the total number of gray flows in GF (h), m = | GF (h)|. Entropy is the measurement of the observational variety in the observed values of any variable X [9]. It is denoted by H(X) which is Entropy (empirical) of X. Uncertainty is a empirical probability p (xi) of any variable x on a given time variably, which is denoted as p (xi) = mi/m, xi∈X

The (empirical) *entropy* of *X* is then defined as

$$H(X) = -\sum_{xi \in X} p(xi) \log p(xi) \quad \ldots\ldots\ldots (1)$$

Standardized entropy below referred to as relative uncertainty (RU) which provides an index of variety or uniformity regardless of the support or sample size:

$$RU(X) = \frac{H(X)}{H \max(X)} \quad \ldots\ldots\ldots\ldots\ldots (2)$$

We apply information theoretical metric Relative Uncertainty (RU) or standardized entropy defined below to the destination port distribution of h to identify dominant scanning (destination) ports (if they exist). So from equations (1) and (2) we get RU for destination as well as server port

$$RU\ (dstPrt) := \frac{-\sum_{i \in dst\,Prt} pi \log pi}{\log m} \quad \ldots\ldots\ldots (3)$$

**Step2:** Identification of category of Anomaly using dominant scanning port (DSPI**).**

In this step, we identify five categories of anomalies using their dominant scanning port (DSP). DSP is the foreign port and port service used by scanning flaws SF (h) of anomalous host for communication with internal host. From equation (3) we can define RU (SrcPrt), for source port (srcPrt) distribution of GF (h). Hence RU (srcPrt) and RU (dstPrt) allows us to determine the existence of dominant scanning port in the gray flaws of an outside host[1].

**DSPI Heuristic algorithm**

Statement:-
Parameters GF (h), β=βo;
Initialization: DSP: =Ø;
Compute pro. dist. Pprt and Θ:= RU(prt) from GF(h);
While Θ≤ β and |GF (h)| >= 10 do
Find prti with highest Pprti
DSP: =DSP∪ prti
Remove flaws associated with prti from GF (h)
Remove Pprti from Pprt;
Compute Θ: = RU (prt) from GF (h)
End While

**Working of DSPI Heuristic Algorithm**

This Algorithm presents a heuristic procedure for extracting DSP from either the destination or source port distribution dstprt of host h∈OS (the same procedure applies to both dstPrt and srcPrt). The algorithm starts with an empty DSP

(DSP =: =Ó) set. It iteratively finds the port with the current highest probability, adds the flows associated with it from GF (h). The algorithm terminates when there are not enough flows left (GF (h) < 10) or the ports in the rest of the flows are nearly uniformly distributed (RU (prt) > βo, where we choose βo = 0.7). In this algorithm βo is a gray constant.

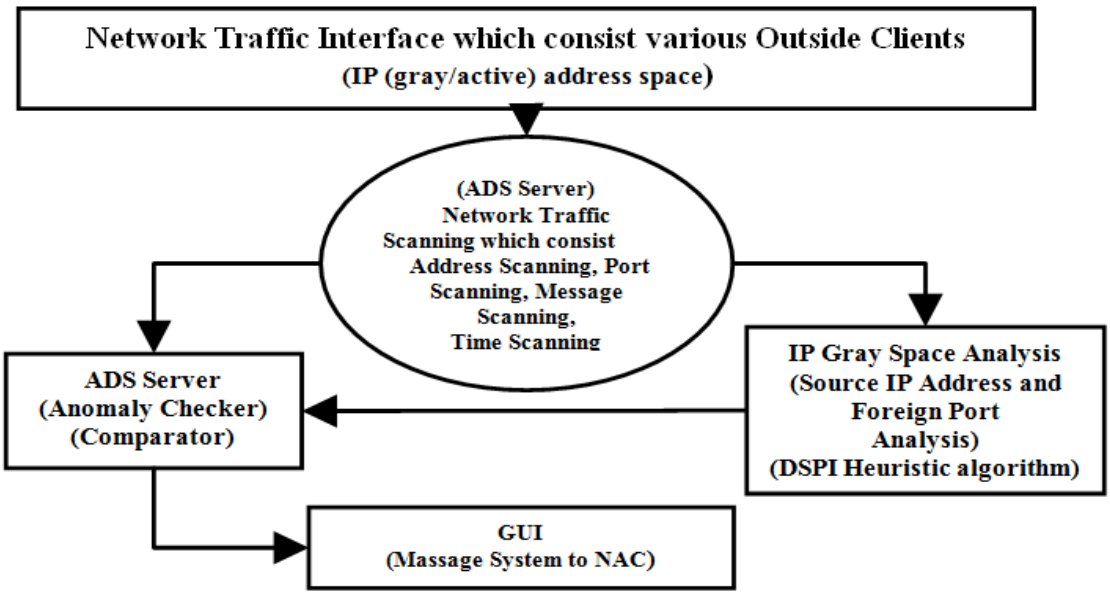


**Fig. 6.** H-NADS Model

**Types of anomalies detected using DSPI algorithm**

**(i) Bad Scanner-I:**

This group includes Bad Scanners that employ ICMP probes in their dominant scanning activities, and upon receiving responses to the ICMP probes from live hosts (From the active space), they follow up with TCP/UDP scanning activities . The Bad Scanners belong to this sub-group, are searching for well-known port service like SSH Remote Login Protocol, SMTP, WWW HTTP and ports 22, 25, 80. These bad scanners receive few successful responses from live inside hosts.

**(ii) Bad Scanner-II**:

A Bad Scanner in this sub-group scans using TCP/UDP probes on a variety of ports, many of which are exploit or service ports furthermore, after responding to the TCP/UDP probes, a few live inside hosts in return initiate an ICMP ping or a TCP connection request on port 113 (the IDENT protocol) to which the scanners respond back. Furthermore, these active inside hosts are being scanned on a variety of ports including service, exploit, and high TCP/UDP ports, to which they all respond successfully via reverse DNS lookup and they are names for DHCP assigned machines. Outside hosts that scan for port 25, a query of their IP addresses in the well known spammers.

**(iii) Bad Scanner-III**:

The bad scanners that also scan using the TCP/UDP probes and receive responses from some live inside hosts furthermore they also have other TCP/UDP connections with these live inside hosts that are initiated by them. Correlating the scanning activities with other activities, we find that most of the other connections initiated by these bad scanners occur after the scanning activities (SF flows) (cursor activities). In the midst of these suspicious activities, he/she also launches a TCP port 80 scanning which also touches the inside host, they are performing queries to an inside DNS server, and then launch scanning for TCP port80. The remaining bad scanners in this sub-group are engaged in some kind of follow-up activities. Some bad scanners of this category make sequential scanning on TCP port 445 for Microsoft DS, UDP port 1023 and TCP port 5554 for SGI ESP HTTP.

**(iv) Focused Hitters**:

The DSP of focused hitters typically belong to a small number of applications, especially, SMTP, Web and peer-to-peer. For example these target the destination port 25, namely, attempting to access email servers, some targets the web service ports, 80 and 443, and some targets the destination ports such as 6881 (Bit Torrent) and 6364 (Gnutella) that are typically associated with peer-to- peer applications, some targets X windows service port 6000, while some focused hitters targets various high ports. We first perform

an in depth analysis of the biggest sub group, Major focused hitters that attempt to access email servers. Focus Hitters probes the port 25 having the service of SMTP.

**(v) Mixed Intruders Anomaly**:

This is the new category of anomaly that we are detecting. Mixed Intruder anomaly detection is one of the biggest challenge in anomaly detection because mixed intruders is do not have fixed behavior they may vary their behavior continuously by changing their scanning flaws and other flaws. Mixed Intruder anomaly is having hybrid behavior of normal and abnormal activities. Some external outside host who are disturbing normal baseline of network also do the normal scanning activities such users are called as mixed intruder anomaly because they are having mixed attitude. To detect such anomaly we first check for bad scanner and focus hitters if any one of them is also doing normal activities which consist to access dynamic ports and their services. once we detect such host who is involve in hybrid activities such hosts are comes in this category of mixed intruders and with that we alert the GUI .

**Step3:** Determination of Potential Behavior of each anomaly using scanning flaws ratio.

In the third step of the proposed methodology, we detect potential behavior of each anomaly using scanning flaws and other flaws. In this step, we calculates scanning flaws ratio $\gamma$ which takes scanning flaws generated by anomalous host h such that $h \in OS$ , where OS is the set of all anomalous hosts. Such scanning flaws are denoted by SF(h). Such anomalous host also generates some other flaws is denoted by OF (h), and again requires DSPI heuristics. The DSPI algorithm has been used to extract dominant destination and source ports for all outside hosts in Os. Using those identified DSP, we then separate incoming flows into two categories scanning flows SF (h) and other flows OF (h). Scanning flows are the flows associated with corresponding source or destination DSP, while the remaining flows are considered as other flows. There are many reasons that a gray outside host produces other flows. In many cases, these other flows can be part of normal activities of the host, e.g. an outside host that inter acts with some inside hosts normally could be infected by worms that generate the scanning flows. In this step, we define the scanning flow ratio $\gamma$ of h as $\gamma = |SF(h)| / (|SF(h)| + |OF(h)|)$ which indicates how dominant the scanning flows are in the outside host's interaction with the network

$$\gamma = \frac{SF(h)}{SF(h)+OF(h)} \quad \ldots\ldots\ldots\ldots (4)$$

IF $\gamma = 1$ then DSP flows having only work to disturb the network not other than this. We calculate $\gamma$ for every anomalous host from equation (4) and decide level of potential behavior of that particular anomalous host. The main purpose behind the detection of behavior is according to behavior network access control will make various provisions for defending the network.

**Table 1.** Criteria to Decide Behaviors

| **Value of $\gamma$** | **Behavior** |
|---|---|
| $\gamma = 1$ | Highly Potential (Harmful) |
| $\gamma >= 0.5$ | Potential |
| $\gamma < 0.5$ | Average |

**2.4 Implementation of proposed Methodology**

We develop an H-NADS Model (Hybrid Network Anomaly Detection Model), which detects anomalies with their potential behaviors. The implementation of methodology has been performed in three steps:

**Working of H-NADS-Model**

H-NADS model first scan the network traffic for Source IP, port, message, after scanning or analyzing model performs anomaly detection according to IP Gray Space Analysis for Gray IP Address and destination scanning ports(DSP)(DSPI Heuristic algorithm). If particular condition matches anomaly detection module generates an alarm or message signal and provides guideline to access control system for access control for a given user or traffic behavior.

**Steps to detect anomalies by using H-NADS Model**

First, transaction data of networks are sampled to highlight potential network service anomalies on a per service class basis. Secondly, temporal based performance thresholds for service classes are built from historical network data for base lining performance Characteristics. Thirdly, anomaly detection proper is executed by comparing the sampled real-time data and the baselines.

| PACKETID | SOURCEIPADDRE | DESTIPADDRE | DESTIPADDRE | DESTIPADDRE | DESTIPADDRE | PORTNUMBER | PACKETTY |
|---|---|---|---|---|---|---|---|
| 5 | 192.168.55.3 | 192 | 168 | 55 | 1 | 1035 | Udp |
| 8 | 192.168.55.3 | 192 | 168 | 53 | 23 | 1044 | Udp |
| 9 | 192.168.55.3 | 192 | 168 | 55 | 33 | 1045 | Udp |
| 11 | 192.168.55.3 | 192 | 168 | 13 | 59 | 1047 | Udp |
| 12 | 192.168.55.3 | 192 | 168 | 55 | 12 | 1048 | Udp |
| 13 | 192.168.55.3 | 192 | 168 | 12 | 15 | 22 | Udp |
| 15 | 192.168.55.3 | 192 | 168 | 53 | 11 | 1051 | Udp |
| 17 | 192.168.55.3 | 192 | 168 | 51 | 10 | 1053 | Udp |
| 19 | 192.168.55.3 | 192 | 168 | 52 | 12 | 1055 | Udp |
| 24 | 192.168.55.3 | 192 | 168 | 52 | 13 | 4588 | Udp |
| 25 | 192.168.55.3 | 192 | 168 | 53 | 45 | 4589 | Udp |
| 26 | 192.168.55.3 | 192 | 168 | 52 | 43 | 4590 | Udp |
| 27 | 192.168.55.3 | 192 | 168 | 55 | 11 | 4592 | Udp |

**Fig. 7.** Knowledgebase used by H-NADS Model

**More specifically the three steps of network anomaly detection are**

• **Sampling or analyzing network traffic :**This model self-consistently and preferentially samples the network (e.g., transaction records generated by network switches) to detect transactions that have high probabilities for being anomalous, according to a sampling strategy that depends on the historical performance of the service class in question. The sampling scheme strikes a balance between sampling frequencies and performance resolution.

**Table 2.** Comparison of Gray Anatomy and H-NADS Methodology

| **Features** | **Gray Anatomy Existing IP Gray Space Methodology** | **Our H-NADS Model/ Methodology ( using IP Gray Space )** |
|---|---|---|
| **Applicable for which Address Block** | 16 bit address block | 24 bit address block |
| **Types of Anomaly Detected** | Two: Bad Scanners Focus Hitters | Five: Bad Scanners (I, II, III), Focus Hitters ,Mixed Intruders |
| **Detection of Harmfulness** | One: Potential | Three: Highly Potential, Potential, Average |
| **Applicable for Protocol** | TCP/IP | TCP/IP and UDP |
| **Type of Communication** | Connection Oriented | Connection Less |
| **Message Type** | Packet | Segment |

• **IP Gray Space generation using Association rules (DSPI Heuristic algorithm):** by generating some sample association rules according to Gray or Active IP and Dominant Scanning Ports (DSP) for static and dynamic user or network device behavior and maintained it as a static or dynamic network traffic knowledge.

• **Anomaly detection:** In this step every ADS client is check by calculating its RU (srcIP) and RU (dstIP). According to RU Here I will classify type of anomalous outside host this is a Bad Scanner, focused hitter or mixed intruder anomalies outside host. Here all the anomalous scanners are classified into five categories three of Bad Scanners anomalous users, focus hitter anomalous user and third is mixed intruder. According to anomalous user separate alert message will supply to the GUI. The outputs of the detector are typically sent to a graphic user interface (GUI) to alert network operators of network anomalies and faults, or are sent directly to network access control modules for automatic feedback and control (e.g., circuit breaker, rerouting module, etc.).

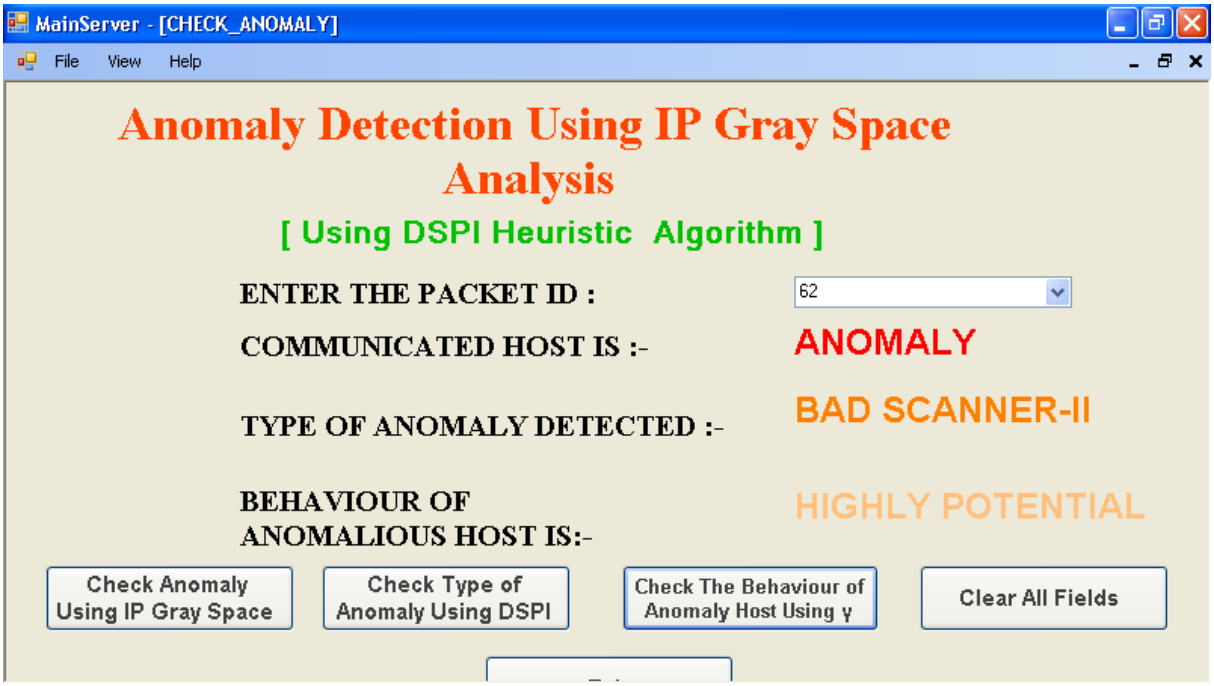


**Fig. 8.** GUI for the Detection of Bad Scanner II Anomaly with its Behavior

**2.5 Knowledgebase Used by H-NADS Model**

Our methodology requires two types of knowledgebase one is static knowledge and other is dynamic knowledge Static knowledge allows identifying those network traffic parameters that are expected to be verified in each network as they have been defined in standard documents. dynamic traffic knowledge, based on the idea that it is possible to identify a small set of traffic parameters, useful for detecting network anomalies, analyzing traffic statistics.

| | PACKETID | SOURCEIPADDRE | PORTNUMBER | Date | Time |
|---|---|---|---|---|---|
| | 43 | 127.0.0.1 | 4631 | 3/17/2009 | 12/30/1899 3:14... |
| | 44 | 127.0.0.1 | 4632 | 3/17/2009 | 12/30/1899 3:14... |
| | 49 | 127.0.0.1 | 4637 | 3/17/2009 | 12/30/1899 3:14... |
| | 63 | 192.168.55.3 | 2127 | 3/17/2009 | 12/30/1899 3:14... |
| | 113 | 127.168.55.3 | 1113 | 3/17/2009 | 12/30/1899 3:14... |

**Fig. 9.** Report Generation after detection of various Anomalies

Some parameters are simple counters or gauges that have been selected according to the lessons learnt during the study of static network knowledge, whereas more complex parameters are derived from the composition of simple parameters using simple operators such as ratio or derivative. What leads the authors to label this knowledge `dynamic' are not the traffic parameters, but the thresholds associated with each parameter, that are not the same for every host

**2.6 Contributions and work extended by our methodology:**

We are removing some loopholes from existing ADS using IP gray space analysis methodology (gray anatomy)

**2.7. Results and Discussion**

After the development of H-NADS Model, we conduct system testing by providing sample set of traffic patterns. In this system testing we measures empirical performance of our H-NADS Model for detection of anomaly and their potential behaviors. Then we represent some sample empirical results in the form of screenshots, table and graph and shown our contribution in the existing work.

With the detection of anomalies our methodology also shows the details of all external host in this detail external host details shows the source IP address of external host which avoids the spoof IP Address problem . Some external host try to make the land attacks such problems are also

avoided. The external host details shows the source and destination ports these ports are required in DSPI heuristic algorithm. The external host details also show the message or any communication made for external host.

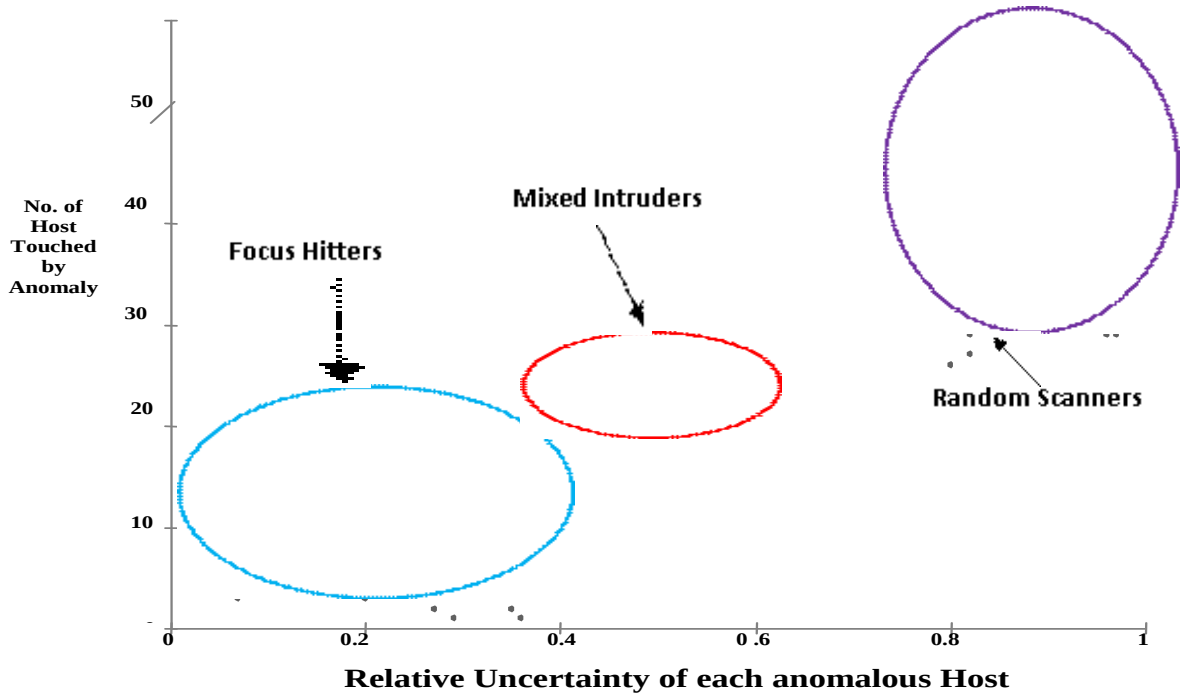


**Fig. 10.** Graphical Analysis of all Anomalies

If the communicating hosts consist of anomalies absolutely it will detect by our methodology. Once methodology detect anomaly the methodology automatically generates reports regarding the anomaly detection as shown above.

**Analysis of All Detected Anomalies:**

In our discussion we are detecting number of anomalies with their potential behaviors. After detection we are clustering them by using any clustering algorithm. Such clustering or grouping is used for identifying the common group behavior of various anomalies. If we identify the group behavior we are able to defend the network using common access denying provision. So for that defending purpose we are graphically analyzing the detected all anomalies.

## 3 Conclusion and Future Work

Anomaly detection is a major issue in network security, so by considering this myth we develop and implement a three step approach for identifying and tracking anomalous host by considering IP Gray Space and their dominant scanning ports identification. Using this methodology we identify five types of anomaly hosts with their three behaviors and obtained some sample results in the form of table and graph.

In future we will extend this work. In extension work we will again try to detect more number of anomalies with their detail behaviors. In present work we are giving only message to GUI when there is anomaly exist but in future we will also makes a lot of provisions to prevent or defend the network by removing such anomalies and this will be the complete work for anomaly detection and prevention. Then that total work will call as design implementation and prevention from network anomalies. In the present work we are using IP Gray Space to detect various anomalies but in future we will also use time series analysis and wavelets patterns to detect and prevent from more number of anomalies.

## References

[1] Y. Jin, K. Xu and Z. L. Zhang, *Identifying and Tracking Suspicious Activities through IP Gray Space Analysis*, UMN, Tech. Rep., 2006

[2] K. Jackson, *Intrusion Detection Systems (IDS): Product Survey*, Los Alamos National Laboratory, 1999.

[3] H. Debar, M. Dacier and A. Wespi, "Towards Taxonomy of Intrusion Detection Sys-

tems", *Computer Networks: The International Journal of Computer and Telecommunications*, vol. 31, no. 9, pp. 805-822, April 1999.
[4] L. Wei, M. Tavallaee and A. A. Ghorbani, "Detecting Network Anomalies Using Different Wavelet Basis Functions", *IEEE Conference on Communication Networks and Services Research*, CNSR 2008, pp. 149-156, Aug. 2008.
[5] D. E. Denning, "An Intrusion Detection Model", *IEEE Transactions on software engineering*, vol. 13, no. 2, pp. 222-232, Feb. 1987.
[6] Y. Yasami, M. Farahmand and V. Zargari, "An ARP-based Anomaly Detection Algorithm Using Hidden Markov Model in Enterprise Networks", *IEEE International Conference on Systems and Networks Communications* (ICSNC 2007), pp. 69-69, Aug. 2007.
[7] G. Maselli, L. Deri and S. Suin, "Design and Implementation of Anomaly Detection System: An empirical approach", *Proceedings of Terena TNC*, 2007.
[8] Y. Jin, G. Simon, K. Xu, Z. L. Zhang and V. Kumar, "Gray's anatomy: dissecting scanning activities using IP gray space analysis Source", Proceedings of the 2nd USENIX workshop on Tackling computer systems problems with machine learning techniques Cambridge, MA, 2007.
[9] K. Xu, Zhi-Li Zhang and S. Bhattacharyya, "Profiling Internet Backbone Traffic: behavior models and applications" *Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communications*, Philadelphia, Pennsylvania, USA SIGCOMM'05, Aug. 2005.
[10] X. Song, M. Wu, C. Jermaine and S. Ranka, "Conditional Anomaly Detection", *IEEE Transactions on Knowledge and Data Engineering*, vol. 19, no. 5, pp. 631-645, May 2007.
[11] G. Bruno, P. Garza, E. Quintarelli and R. Rossato, **"**Ano maly Detection in XML databases by means of Association Rules", *18th IEEE International Conference on Database and Expert Systems Applications*, DEXA'07, pp. 387-391, Sep. 2007.

**Yogendra Kumar JAIN** received the B.E. (Hons.) degree in E& I from S. A. T. I., Vidisha in 1991 and M.E (Hons) in Digital Tech. & Instrumentation from S. G. S. I. T. S., D. A. V. V. Indore (M.P), India in 1999. Pursuing Ph. D. from Rajiv Gandhi Technological University, Bhopal (M.P.), India. Presently working as Head of the Department, Computer Sc. & Eng. at S. A. T. I., Vidisha, since 1991. Research Interest includes Image Processing, Image Compression, Network security, Mobile Communication, Published 20 Research papers in reputed Journals and conferences.

**Sandip S. PATIL** received the B.E. degree in Computer Engineering, in 2001 from SSBT's College of Engineering and Technology, Bambhori, Jalgaon affiliated to North Maharastra University Jalgaon(M.S.), India and pursuing M.Tech. in Computer Science and Engineering from Samrat Ashok Technological Institute Vidisha affiliated to Rajiv Gandhi Technological University, Bhopal (M.P.), India. Research Interests includes developing network security applications for the detection of suspicious abnormal behaviors, studying the performance of various network security tools. Designing and implementing various soft computing tools.