IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

INTRUSION DETECTION USING DANGER OR NORMAL MODE

KOMMANA LAKSHMI NARAYANA [#1], B.SURYANARAYANA MURTHY [#2]

[#1] MSC Student, Master of Computer Science,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

[#2] Associate Professor, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

ABSTRACT

Now a days there is a huge demand and interest in using path identifiers (PIDs) for data communication .These PIDs act as a inter-domain routing objects to avoid distributed denial-of service (DDoS) attacks. As we all know that path identifer are designed earlier , those are static in nature and hence it is very easy for the attackers to create any attack on a fixed path. To address this issue, in this present application we try to design and implement a novel path identifiers for data communication like dynamic D-PID, a framework that is not at all implemented in any DTNs till today. In DPID, the PID of an inter-domain path connecting two domains is kept secret and changes dynamically, so there is no chance for any attacker to identify which path the data is travelling and he cant able to convert nodes into faulty state. We simulated our application using socket programming language along with java network package to verify the effectiveness and cost. The results from both simulations and experiments show that dynamic nature of identifying faulty nodes and providing alternate path for data transfer can effectively prevent DDoS attacks.

1. INTRODUCTION

DENIAL-OF-SERVICE (DoS) attack, which aims to make a service unavailable to legitimate clients, has become a severe threat to the Internet security . Traditional DoS attacks mainly abuse the network bandwidth around the Internet subsystems and degrade the quality of service by generating congestions at the network. Consequently, several network-based defense methods have tried to detect these attacks by controlling traffic volume or differentiating traffic patterns at the intermediate routers .However, with the boost in network bandwidth and application service types, recently, the target of DoS attacks has shifted from network to server resources and application procedures themselves, forming a new application DoS attack .

As stated in, by exploiting flaws in application design and implementation, application DoS attacks exhibit three advantages over traditional DoS attacks which help evade normal detections: malicious traffic is always indistinguishable from normal traffic, adopting automated script to avoid the need for a large amount of "zombie" machines or bandwidth to launch the attack, much harder to be traced due to multiple redirections at proxies. According to these characteristics, the malicious traffic can be classified into legitimate-like requests of two cases: 1) at a high inter arrival rate and 2) consuming more service resources.

The identification of attackers can be much faster if we can find them out by testing the clients in group instead of one by one. Thus, the key problem is how to group clients and assign them to different server machines in a sophisticated way, so that if any server is found under attack, we can immediately identify and filter the attackers out of its client set. Apparently, this problem resembles the group testing (GT) theory which aims to discover defective items in a large population with the minimum number of tests where each test is applied to a subset of items, called pools, instead of testing them one by one. Therefore, we apply GT theory to this network security issue and propose specific algorithms and protocols to achieve high detection performance in terms of short detection latency and low false positive/negative rate. Since the detections are me rely based on the status of service resources usage of the victim servers, no individually signature-based authentications or data classifications are required; thus, it may overcome the limitations of the current solutions.

PROBLEM STATEMENT

The DoS attack detection system presented in this paper employs the principles of MCA and anomaly-based detection. They equip our detection system with capabilities of accurate characterization for traffic behaviors and detection of known and unknown attacks respectively. A triangle area technique is developed to enhance and to speed up the process of MCA. A statistical normalization technique is used to eliminate the bias from the raw data. Our proposed DoS detection system is evaluated using KDD Cup 99 dataset and outperforms the state-of the- art systems shown in this system.

PURPOSE

The problem of this system is to present a DoS attack detection system that uses Multivariate Correlation Analysis (MCA) for accurate network traffic characterization by extracting the geometrical correlations between network traffic features. Then it is MCA-based DoS attack detection system employs the principle of anomaly-based detection in attack recognition. This makes our solution capable of detecting known and unknown DoS attacks effectively by learning the patterns of legitimate network traffic only.

OBJECTIVE

In the proposed system, the system proposes a fully distributed and easily implementable approach to allow each DTN node to rapidly identify whether its sensors are producing faulty data. The dynamical behaviour of the proposed algorithm is approximated by some continuous-time state equations, where each and every node is identified based on its state.If any node is not in normal state than how it is constructed before it is immediately identified as attacked node or faulty node and immediately that node need to be ignored in the best path.In this way our proposed mechanism try to identify best paths for data transfer dynamically by identifying each and every node individually.In DPID, the PID of an inter-domain path connecting two domains is kept secret and changes dynamically,so there is no chance for any attacker to identify which path the data is travelling and he cant able to convert nodes into faulty state. We simulated our application using socket programming language along with java network package to verify the effectiveness and cost. The results from both simulations and experiments show that dynamic nature of identifying faulty nodes and providing alternate path for data transfer can effectively prevent DDoS attacks

2. LITERATURE SURVEY

INRODUCTION

Literature survey is the most important step in software development process. Before developing the tool, it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, ten next steps are to determine which operating system and language used for developing the tool. Once the programmers start building the tool, the programmers need lot of external support. This support obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into for developing the proposed system.

RELATED WORK

1) Efficient packet marking for large-scale IP traceback

AUTHORS: M. T. Goodrich

We present a new approach to IP traceback based on the probabilistic packet marking paradigm. Our approach, which we call randomize-and-link, uses large checksum cords to "link" message fragments in a way that is highly scalable, for the checksums serve both as associative addresses and data integrity verifiers. The main advantage of these checksum cords is that they spread the addresses of possible router messages across a spectrum that is too large for the attacker to easily create messages that collide with legitimate messages. Our methods therefore scale to attack trees containing hundreds of routers and do not require that a victim know the topology of the attack tree a priori. In addition, by utilizing authenticated dictionaries in a novel way, our methods do not require routers sign any setup messages individually.

2) Dynamic probabilistic packet marking for efficient IP traceback

AUTHORS: J. Liu, Z.-J. Lee, and Y.-C. Chung

Recently, denial-of-service (DoS) attack has become a pressing problem due to the lack of an efficient method to locate the real attackers and ease of launching an attack with readily available source codes on the Internet. Traceback is a subtle scheme to tackle DoS attacks. Probabilistic packet marking (PPM) is a new way for practical IP traceback. Although PPM enables a victim to pinpoint the attacker's origin to within 2–5 equally possible sites, it has been shown that PPM suffers from uncertainty under spoofed marking attack. Furthermore, the uncertainty factor can be amplified significantly under distributed DoS attack, which may diminish the effectiveness of PPM. In this work, we present a new approach, called dynamic probabilistic packet marking (DPPM), to further improve the effectiveness of PPM. Instead of using a fixed marking probability, we propose to deduce the traveling distance of a packet and then choose a proper marking probability. DPPM may completely remove uncertainty and enable victims to precisely pinpoint the attacking origin even under spoofed marking DoS attacks. DPPM supports incremental deployment. Formal analysis indicates that DPPM outperforms PPM in most aspects.

3) Detection and Localization of Network Black Holes

AUTHORS : J.Yates,A.Greenberg,A.C.Snoren

Internet backbone networks are under constant flux, struggling to keep up with increasing demand. The pace of technology change often outstrips the deployment of associated fault monitoring capabilities that are built into today's IP protocols and routers. Moreover, some of these new technologies cross networking layers, raising the potential for unanticipated interactions and service disruptions that the built-in monitoring systems cannot detect. In such instances, failures may cause data packets to be silently dropped inside the network without triggering any alarms or responses (e.g., the failure is not routed around). So-called "silent failures" or "black holes" represent a critical threat to today's rapidly evolving networks. In this paper, we present a simple and effective method to detect and diagnose such silent failures. Our method uses active measurement between edge routers to raise alarms whenever end-to-end connectivity is disrupted, regardless of the cause. These alarms feed localization agents that employ spatial correlation techniques to isolate the root-cause of failure. Using data from two real systems deployed on sections of a tier-I ISP network, we successfully detect and localize three known black holes. Further, we present simulation results demonstrating that our system accurately and precisely (both greater than 80% according to our metrics) localizes a variety of failures classes.

4) Single-link failure detection in all-optical networks using monitoring cycles and paths

AUTHORS: S.Ahuja,M.Krunz

In this paper, we consider the problem of fault localization in all-optical networks. We introduce the concept of monitoring cycles (MCs) and monitoring paths (MPs) for unique identification of single-link failures. MCs and MPs are required to pass through one or more monitoring locations. They are constructed such that any single-link failure results in the failure of a unique combination of MCs and MPs that pass through the monitoring location(s). For a network with only one monitoring location, we prove that three-edge connectivity is a necessary and sufficient condition for constructing MCs that uniquely identify any single-link failure in the network. For this case, we formulate the problem of constructing MCs as an integer linear program (ILP). We also develop heuristic approaches for constructing MCs in the presence of one or more monitoring locations. For an arbitrary network (not necessarily three-edge connected), we describe a fault localization technique that uses both MPs and MCs and that employs multiple monitoring locations. We also provide a linear-time algorithm to compute the minimum number of required monitoring locations. Through extensive simulations, we demonstrate the effectiveness of the proposed monitoring technique.

3. EXISTING SYSTEM

In the existing system the main reason for occurring a DoS attacks is a node can send any amount of data packets to any destination, regardless whether or not the destination wants the packets. To address this issue, in the existing system, several approaches have been proposed. In the “off by default” approach, two hosts are not permitted to communicate by defaul.Hence there should be a pre-defined path for sending the data from valid source to the destination node which leaves the attacker to convert the nodes into dos state.

LIMITATION OF EXISTING SYSTEM

The following are the main limitations of the existing system. They are as follows:

1. More Time Delay in Routing and less throughput
2. Data security is very less because the attacker try to delay the request and response.
3. All the existing approaches failed in identifying the DOS attack type accurately.
4. There is no group testing approach in order to check the traffic delay.

4. PROPOSED SYSTEM

Till now there is no method which can identify the denial of service attack accurately based on the transfer rate. Here in our proposed application we try to apply a Novel group testing (GT)-based approach in order to check whether the data is transferred under normal mode or danger mode. This can be identified as if the data is reached within the time limit for the end users then it will be called as normal mode.If the same data request is received more than the expected time, then it is identified as Danger mode.

ADVANTAGES OF THE PROPOSED SYSTEM

The following are the advantages of the proposed system, they are as follows:

1. Very Less Time Delay in Routing and high throughput

2. Data security is high because the data is send under encrypted manner.

3. The current system is accurate in identifying the DOS attack type accurately.

There is a group testing approach in order to check the traffic delay in our proposed system

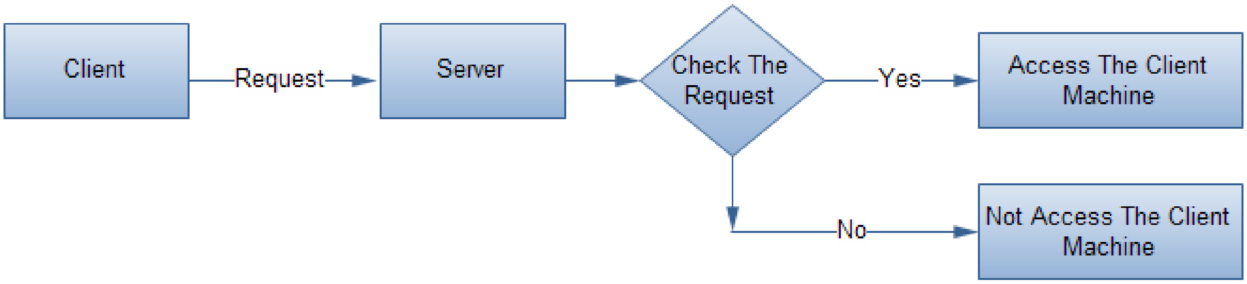
5. SOFTWARE PROJECT MODULES

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. The application is divided mainly into following 4 modules. They are as follows:

1. Login Process
2. Group attacker modules.
3. Group testing modules.
4. Victim/Detection modules.

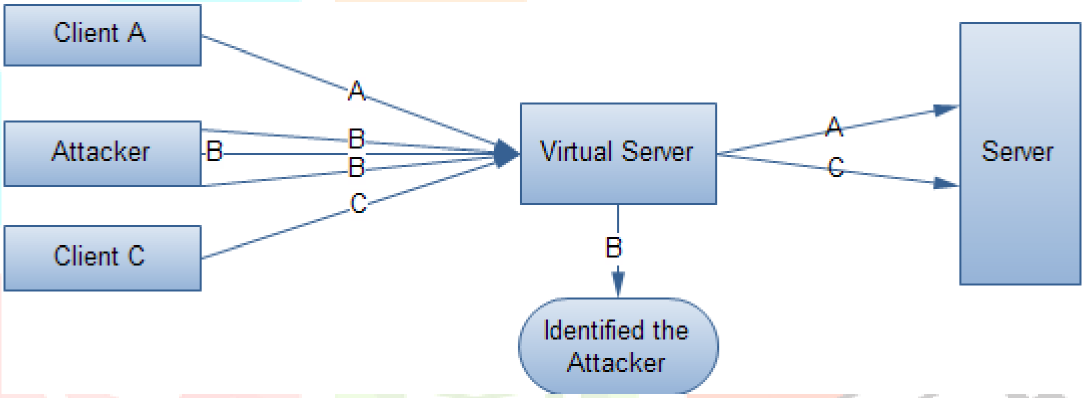
5.1 Login Process

In this module the client has the facility to login into the system with a valid user id and password. If the user enters a valid details he can enter into the system if not he will get a invalid authentication. Here the login will be available for only client and for proxy, router and main server there will be no login available. Here each and every task was monitored by the main server. If the application explicitly states which component of the username/password pair was incorrect then an attacker can automate the process of trying common usernames from a dictionary file in an attempt to enumerate the users of the application. Whilst applications may handle authentication failure messages correctly, many still allow attackers to enumerate users through the *forgotten password* feature.



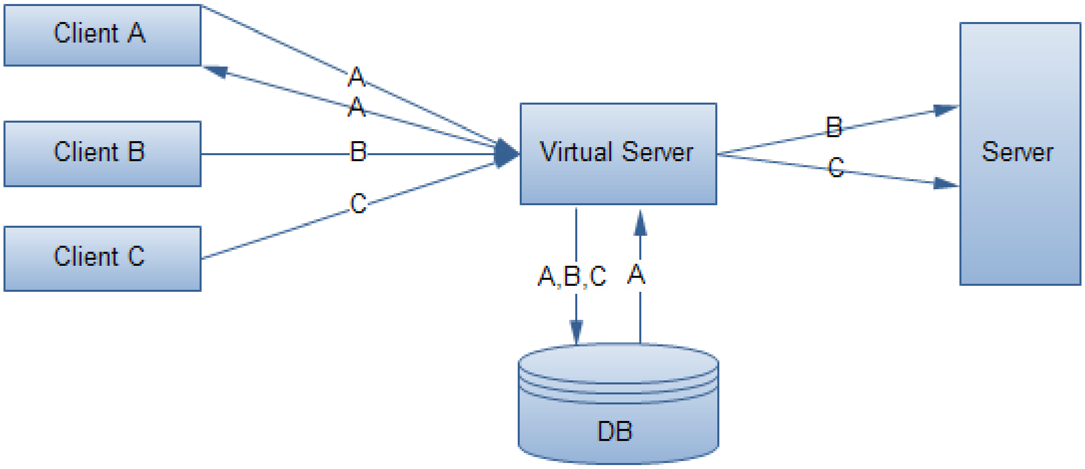
5.2 Group attacker modules.

This is the module in which the group attacker who tries to create the Denial of service attack is monitored and identified in the network. In this module the group attacker is the main person who has the ability to identify the attacker within the network in any of the intermediate level.If the attack was occurred within the client level or proxy level or router level or main level this can be easily identified by the group attacker module.Hence this module is mainly used for monitoring the attack that was caused in the network during data communication. Here virtual server plays a vital role in identifying the attacker that occur within the network.



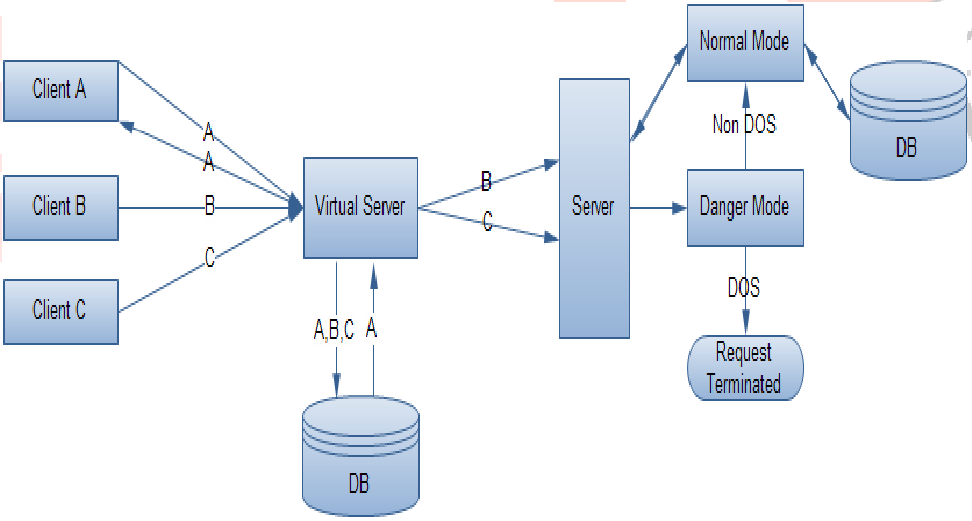
5.3 Group Testing modules

This group testing module is the main module in which the attacker is identified with the help of this approach. This GT approach is mainly used to study the time and delay that take place during the data transfer. The GT based approach is mainly used for identifying the delay based on each and every individual bandwidth .For a low bandwidth system there may be huge delay which cause DOS and for a high bandwidth there may be less delay which will try to send the data intime as per the expected arrival time.This GT based approach mainly calculates the type of attack that occur within the network.



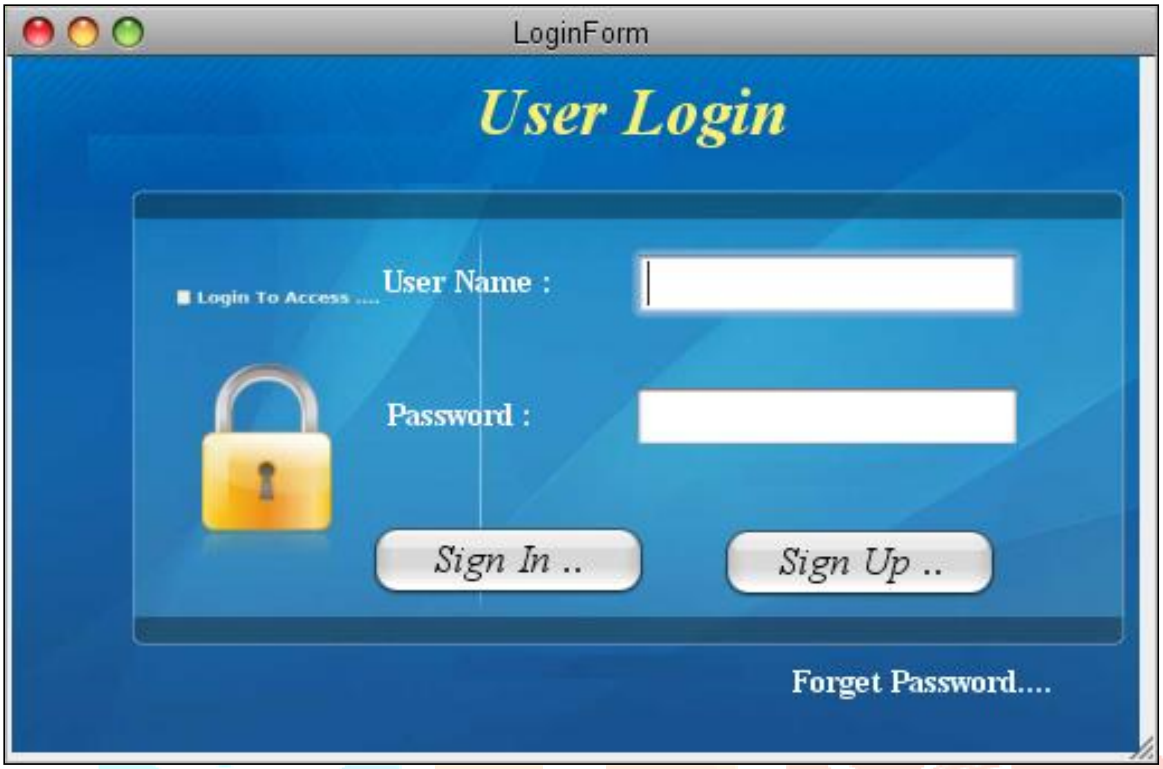
5.5 Victim/Detection modules.

The victim model in our general framework consists of multiple back-end servers, which can be Web/application servers, database servers, and distributed file systems. This victim module is nothing but detection of modes based on user request. Here in the module if the user try to send the request with some delay it is identified as attacker module or danger mode and if the same request is received in within the time ,it is identified as normal mode.

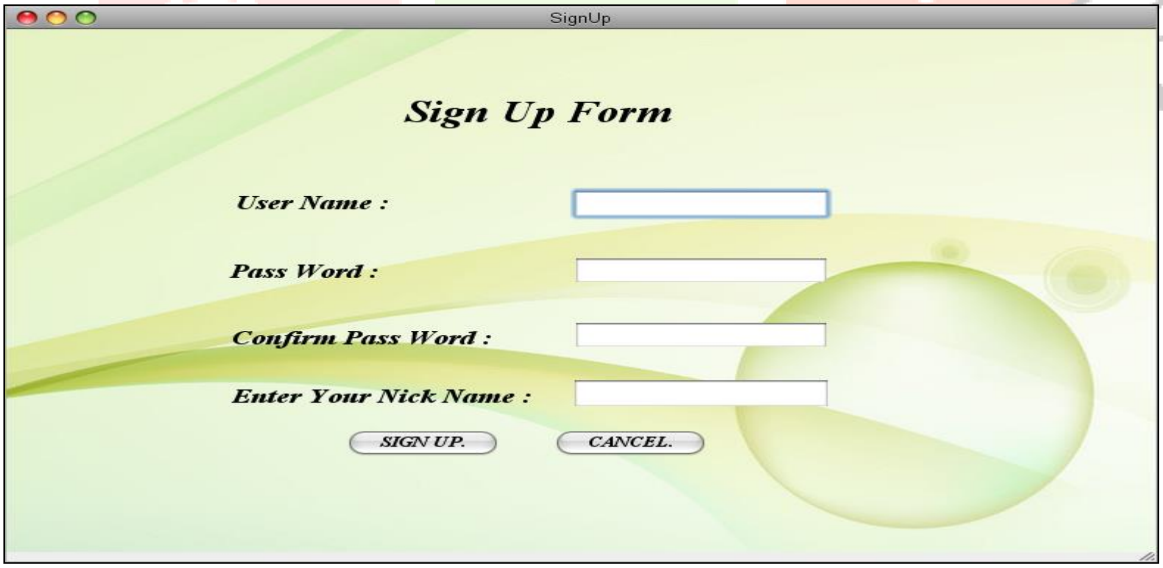


6. RESULTS (OUTPUT SCREENS)

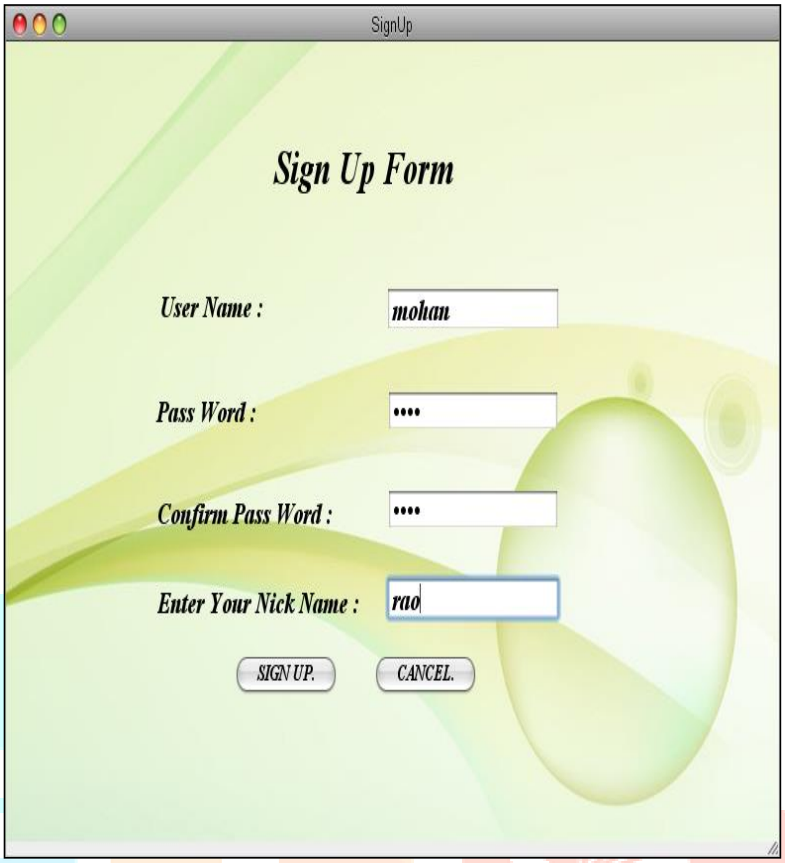
Client login Window



Client Signup Window



Client Registers with a Username "Mohan"



SignUp

Sign Up Form

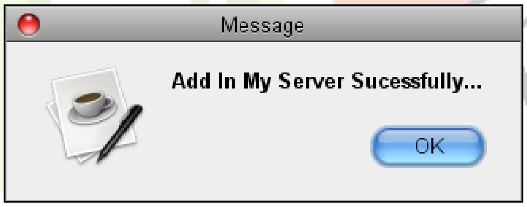
User Name : mohan

Pass Word : ••••

Confirm Pass Word : ••••

Enter Your Nick Name : rao

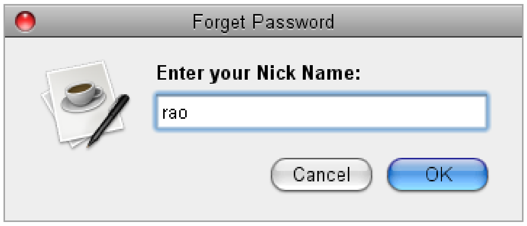
Registration Successful



Message

Add In My Server Sucessfully...

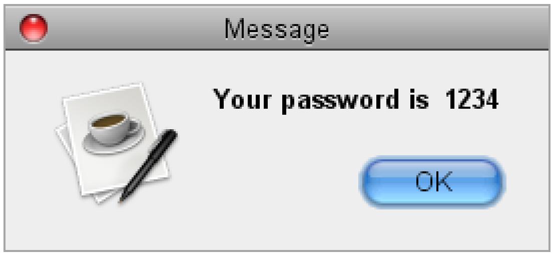
Client Forget the password…He tries for Forget Password Option



Forget Password

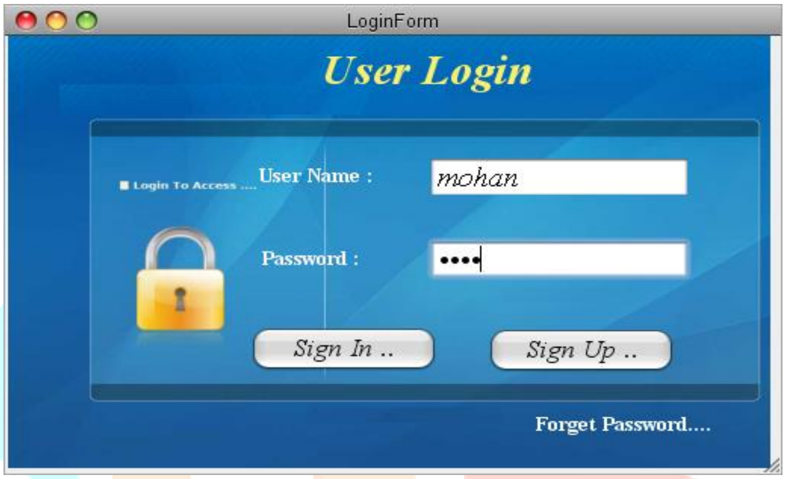
Enter your Nick Name: rao

If the response is true, then he will get the password as below



Your password is 1234

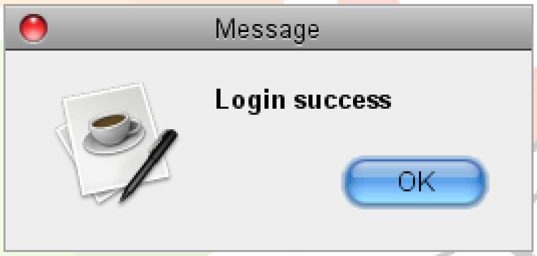
Client Login with his valid Username and Password



User Name : mohan

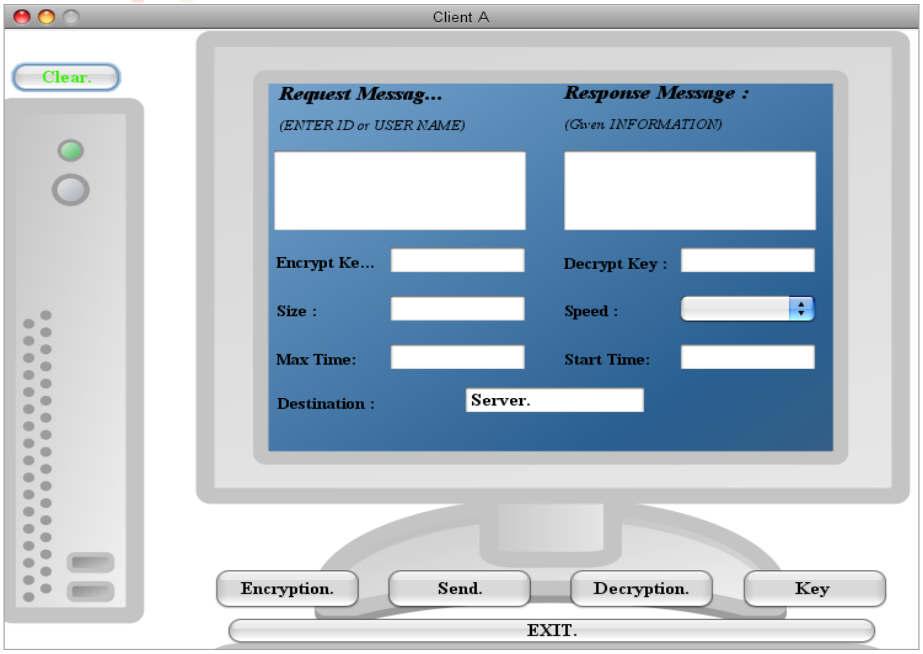
Password : ••••

Login Success



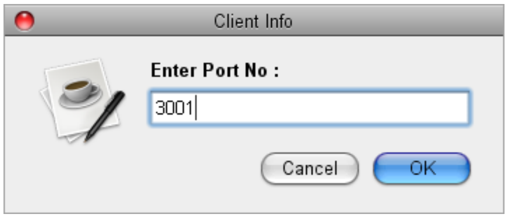
Login success

Client Main Page



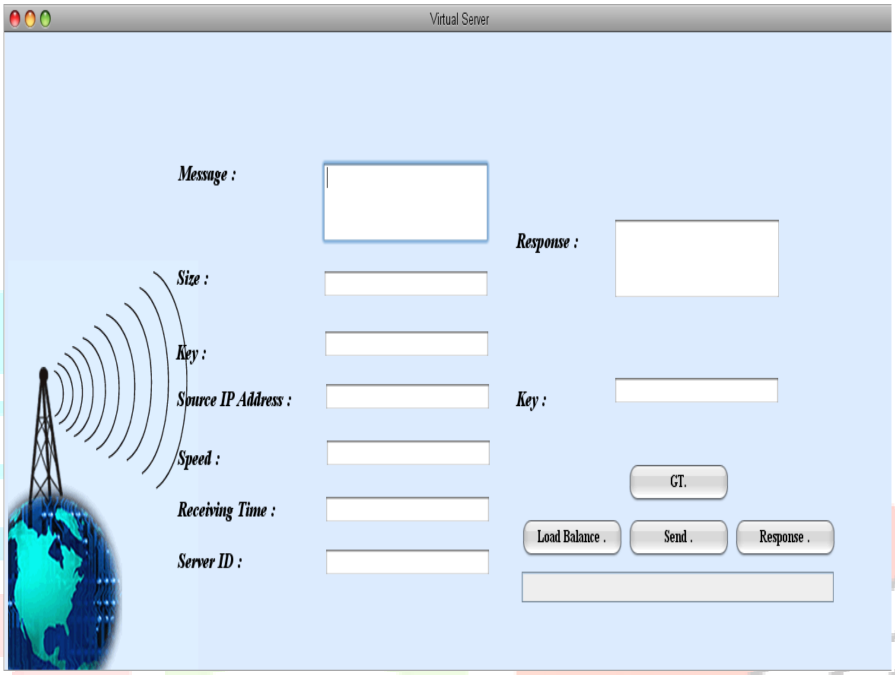
Destination : Server.

Client is asked to enter Port Number

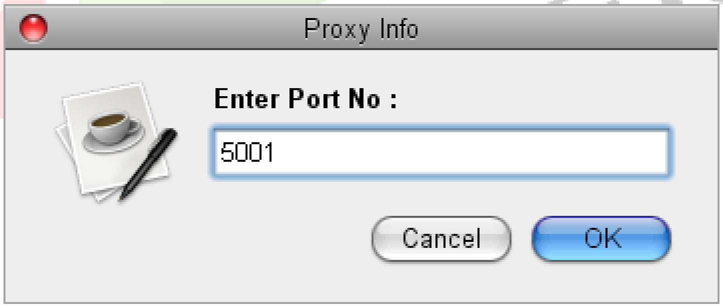


Enter Port No : 3001

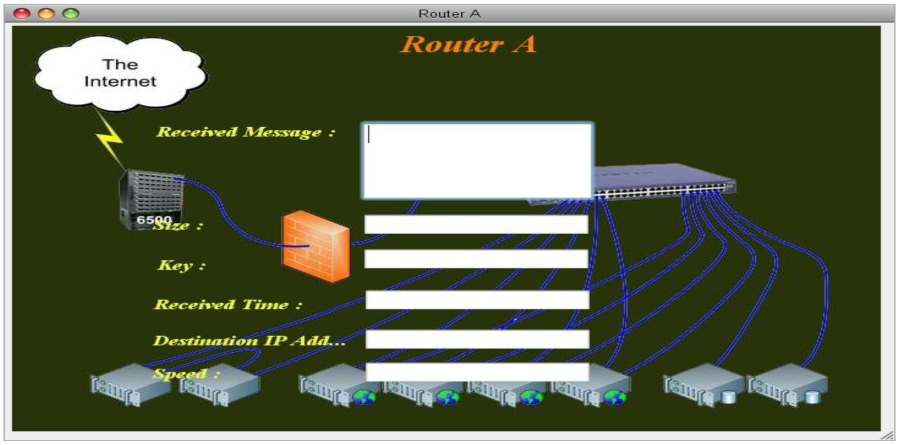
Proxy Server Window is Started



Router Window is started, and then it is asked to enter the port number



Enter Port No : 5001



Router A

Received Message :

Size :

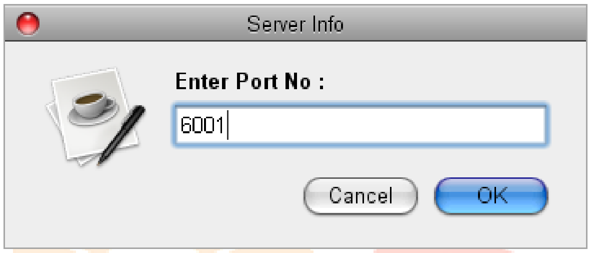
Key :

Received Time :

Destination IP Add...

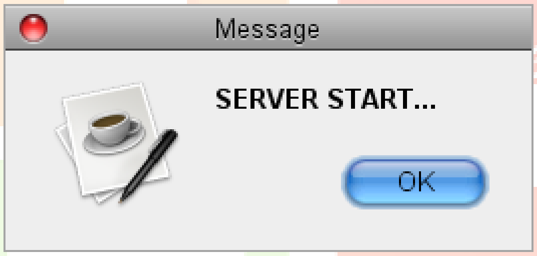
Speed :

Server is Started then it is asked to enter the Valid Distinct PORT Number



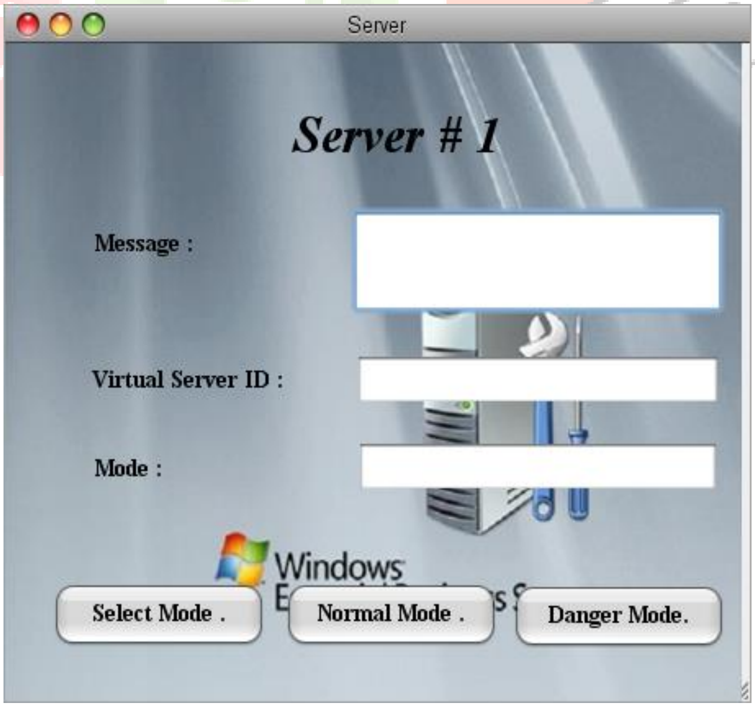
Server Info

Enter Port No : 6001



Message

SERVER START...



Server

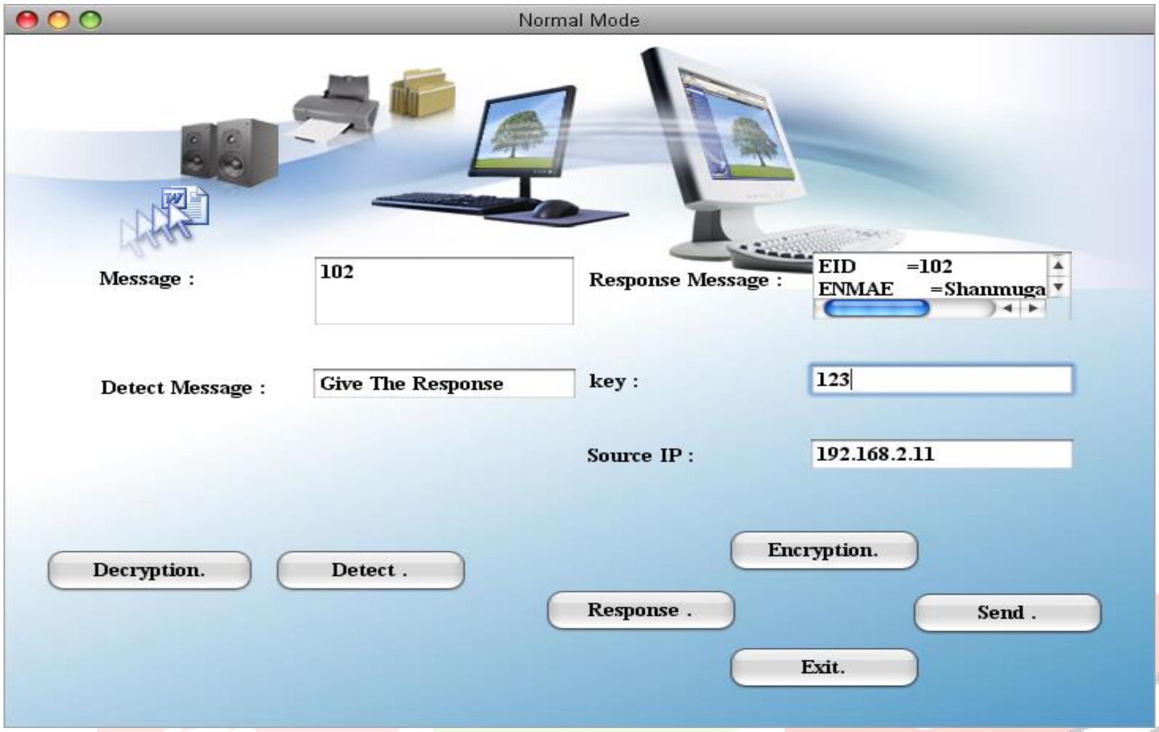
Server # 1

Message :

Virtual Server ID :

Mode :

Normal Mode Window Is Started



Message : 102

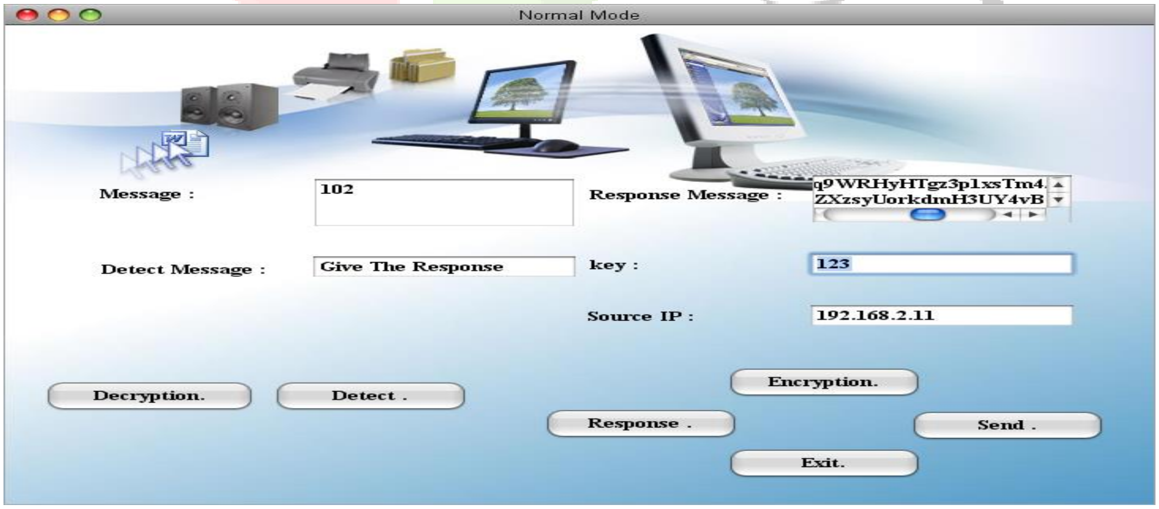
Response Message : EID =102
ENMAE =Shanmuga

Detect Message : Give The Response

key : 123

Source IP : 192.168.2.11

Encrypt the RESPONSE and send back to the client



Message : 102

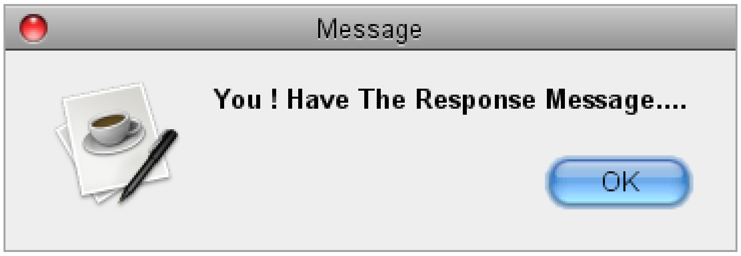
Response Message : q9WRHyHTgz3p1xsTm4.
ZXzsyUorkdmH3UY4vB

Detect Message : Give The Response

key : 123

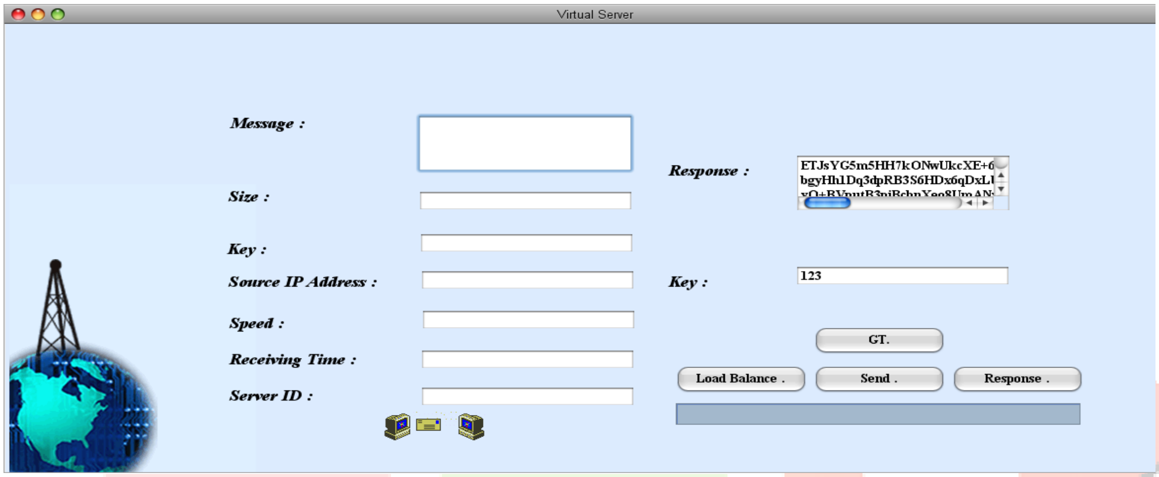
Source IP : 192.168.2.11

Response comes to Virtual or Proxy server



Message

You ! Have The Response Message....



Virtual Server

Message :

Size :

Key :

Source IP Address :

Speed :

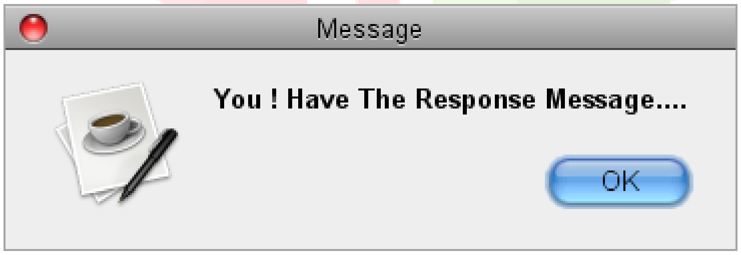
Receiving Time :

Server ID :

Response : ETJsYG5m5HH7kONwUkcXE+6
bgyHh1Dq3dpRB3S6HDx6qDxL
vQ+BVputB3njBchnXeo8UmAN

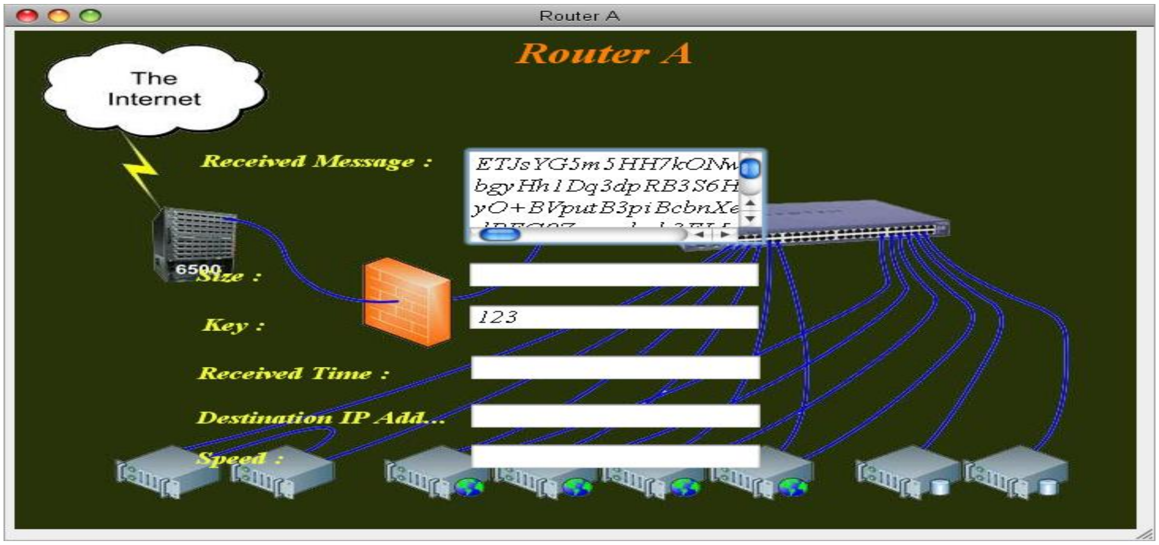
Key : 123

Virtual Node Clicks on Response Button in order to send the response to the client through router window



Message

You ! Have The Response Message....



Received Message : ETJsYG5m5HH7kONw bgyHh1Dq3dpRB3S6H yO+BVputB3piBcbnXe

Size :

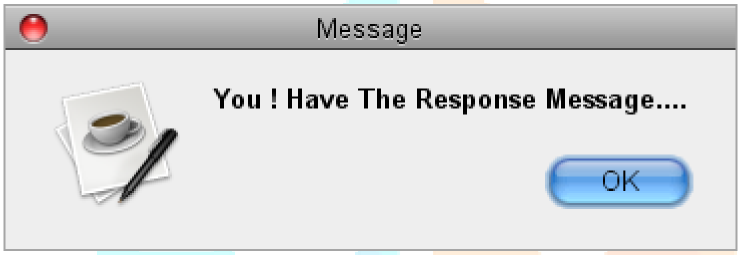
Key : 123

Received Time :

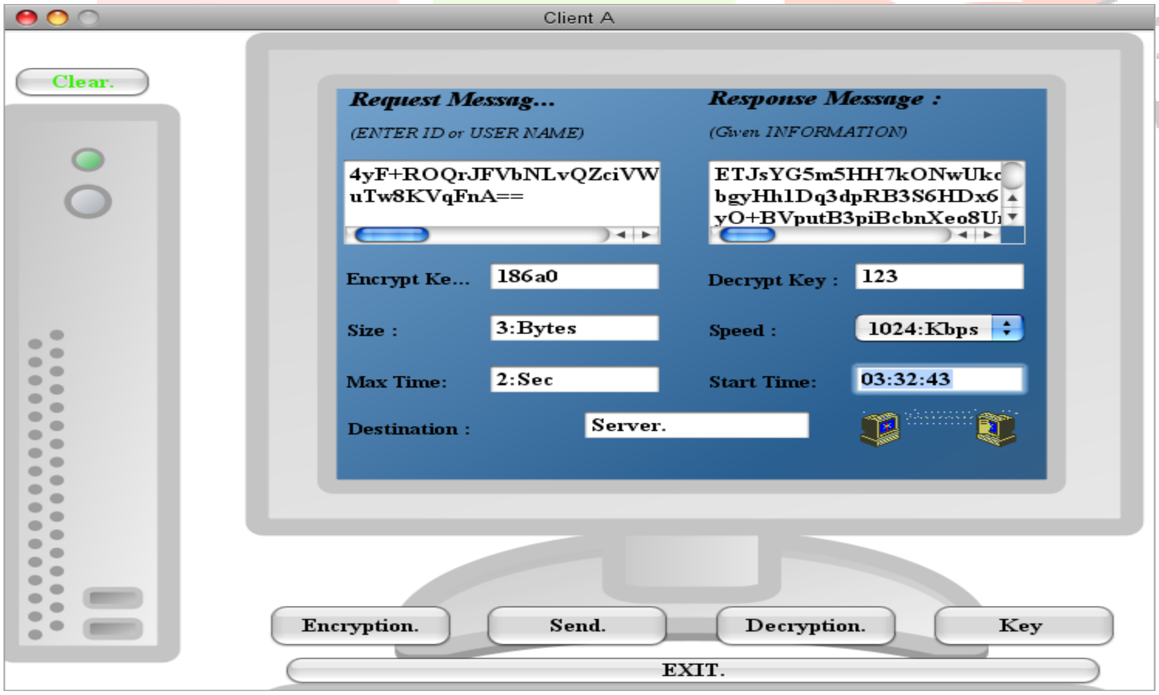
Destination IP Add...

Speed :

Client finally receives the encrypted response in a normal mode



You ! Have The Response Message....



Request Messag... (ENTER ID or USER NAME): 4yF+ROQrJFVbNLvQZciVW uTw8KVqFnA==

Response Message : (Given INFORMATION): ETJsYG5m5HH7kONwUkc bgyHh1Dq3dpRB3S6HDx6 yO+BVputB3piBcbnXeo8U

Encrypt Ke... 186a0

Decrypt Key : 123

Size : 3:Bytes

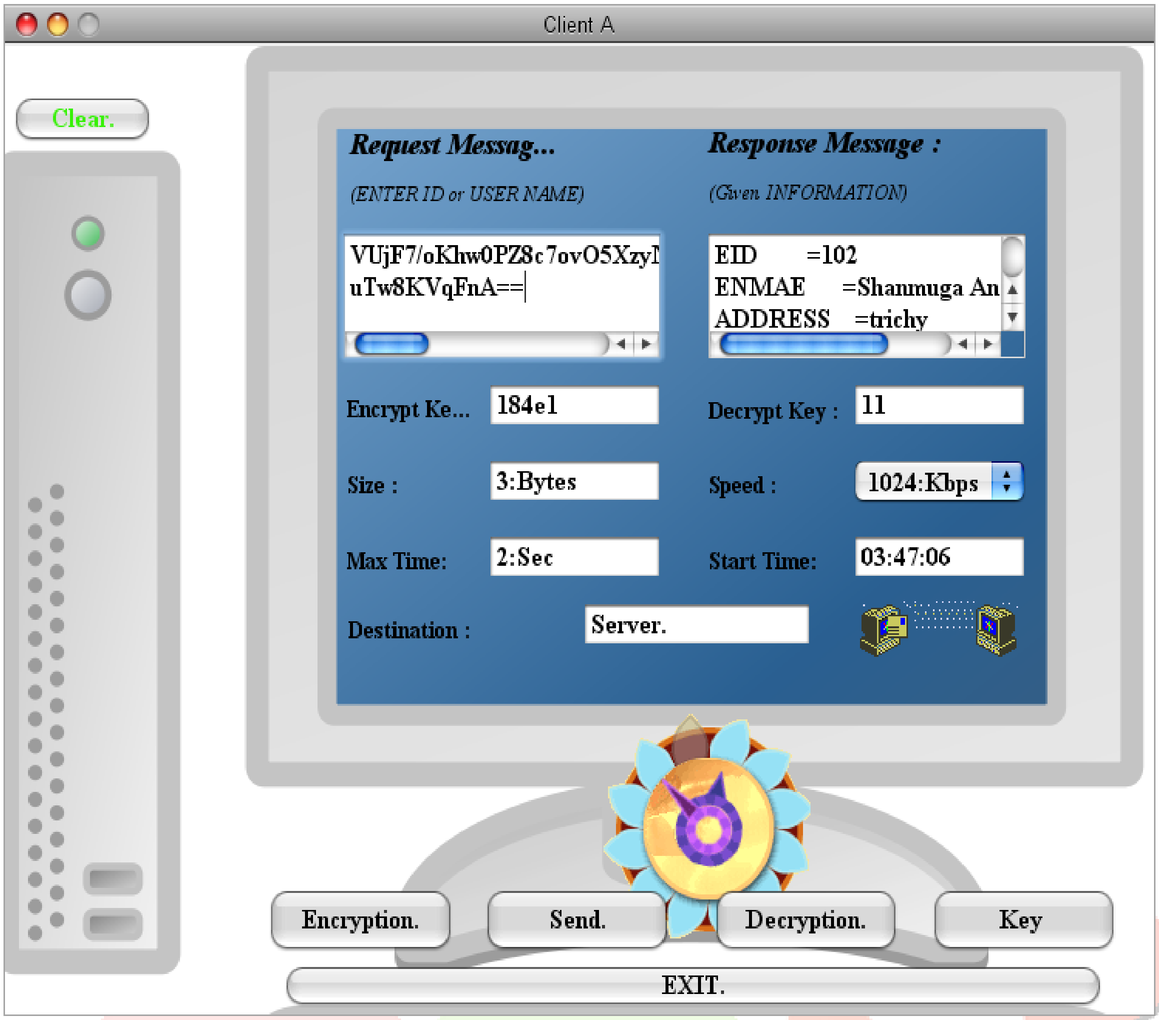
Speed : 1024:Kbps

Max Time: 2:Sec

Start Time: 03:32:43

Destination : Server.

Client Decrypts the Response by click on Decrypt button in order to view the response



VUjF7/oKhw0PZ8c7ovO5XzyI
uTw8KVqFnA==

EID =102
ENMAE =Shanmuga An
ADDRESS =trichy

Encrypt Ke... 184e1

Decrypt Key : 11

Size : 3:Bytes

Speed : 1024:Kbps

Max Time: 2:Sec

Start Time: 03:47:06

Destination : Server.

7. CONCLUSION

This system has presented a MCA-based DoS attack detection system which is powered by the triangle-area based MCA technique and the anomaly-based detection technique. The former technique extracts the geometrical correlations hidden in individual pairs of two distinct features within each network traffic record, and offers more accurate characterization for network traffic behaviors. The latter technique facilitates our system to be able to distinguish both known and unknown DoS attacks from legitimate network traffic. Evaluation has been conducted using KDD Cup 99 dataset to verify the effectiveness and performance of the proposed DoS attack detection system.

8. REFERENCES

[1] V. Paxson, “Bro: A System for Detecting Network Intruders in Realtime,” *Computer Networks*, vol. 31, pp. 2435-2463, 1999.

[2] P. Garca-Teodoro, J. Daz-Verdejo, G. Maci-Fernndez, and E. Vzquez, “Anomaly-based Network Intrusion Detection: Techniques, Systems and Challenges,” *Computers & Security*, vol. 28, pp. 18-28, 2009.

[3] D. E. Denning, “An Intrusion-detection Model,” *IEEE Transactions on Software Engineering*, pp. 222-232, 1987.

[4] K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, “DDoS attack detection method using cluster analysis,” Expert Systems with Applications, vol. 34, no. 3, pp. 1659-1665, 2008.

[5] A. Tajbakhsh, M. Rahmati, and A. Mirzaei, “Intrusion detection using fuzzy association rules,” Applied Soft Computing, vol. 9, no. 2, pp. 462-469, 2009.

[6] J. Yu, H. Lee, M.-S. Kim, and D. Park, “Traffic flooding attack detection with SNMP MIB using SVM,” Computer Communications, vol. 31, no. 17, pp. 4212-4219, 2008.

[7] W. Hu, W. Hu, and S. Maybank, “AdaBoost-Based Algorithm for Network Intrusion Detection,” Trans. Sys. Man Cyber. Part B, vol. 38, no. 2, pp. 577-583, 2008.

[8] C. Yu, H. Kai, and K. Wei-Shinn, “Collaborative Detection of DDoS Attacks over Multiple Network Domains,” Parallel and Distributed Systems, IEEE Transactions on, vol. 18, pp. 1649-1662, 2007.

[9] G. Thatte, U. Mitra, and J. Heidemann, “Parametric Methods for Anomaly Detection in Aggregate Traffic,” Networking, IEEE/ACM Transactions on, vol. 19, no. 2, pp. 512-525, 2011.

[10] S. T. Sarasamma, Q. A. Zhu, and J. Huff, “Hierarchical Kohonenen Net for Anomaly Detection in Network Security,” *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 35, pp. 302-312, 2005.

[11] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, “Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient,” Parallel and Distributed Systems, IEEE Transactions on, vol. 23, pp. 1073-1080, 2012.

[12] S. Jin, D. S. Yeung, and X. Wang, "Network Intrusion Detection in Covariance Feature Space," *Pattern Recognition*, vol. 40, pp. 2185- 2197, 2007.

[13] C. F. Tsai and C. Y. Lin, "A Triangle Area Based Nearest Neighbors Approach to Intrusion Detection," *Pattern Recognition*, vol. 43, pp. 222-229, 2010.

[14] A. Jamdagni, Z. Tan, X. He, P. Nanda, and R. P. Liu, "RePIDS: A multi tier Real-time Payload-based Intrusion Detection System," Computer Networks, vol. 57, pp. 811-824, 2013.

[15] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "Denialof- Service Attack Detection Based on Multivariate Correlation Analysis," Neural Information Processing, 2011, pp. 756-765.

[16] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "Triangle- Area-Based Multivariate Correlation Analysis for Effective Denialof- Service Attack Detection," The 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, United Kingdom, 2012, pp. 33-40.

[17] S. J. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P. K. Chan, "Costbased modeling for fraud and intrusion detection: results from the JAM project," The DARPA Information Survivability Conference and Exposition 2000 (DISCEX '00), Vol.2, pp. 130-144, 2000.

[18] G. V. Moustakides, "Quickest detection of abrupt changes for a class of random processes," Information Theory, IEEE Transactions on, vol. 44, pp. 1965-1968, 1998