A Real Time Host and Network Mobile Agent based Intrusion Detection System (HNMAIDS)

Abhijit Dwivedi
Department of C.S.E
Radharaman Engineering College
Bhopal, (M.P.)

Y.K. Rana
Department of C.S.E
Radharaman Engineering College
Bhopal, (M.P.)

B.P. Patel
Department of C.S.E
Radharaman Engineering College
Bhopal, (M.P.)

ABSTRACT

Computer security is to detect or prevent the process of collecting information or unauthorized access to computers. Detection is a recognition process which helps us to determine if someone tried to enter our system that have been successful, however, and what can be done. Prevention measures help us to pursue unauthorized users called as intruders from accessing any part of the computer system. Computer is being used for everything from banking and investment, businesses to communicate with others via email or messenger programs. Although It may not consider communications top secret, It probably do not want strangers reading email, using computer to attack or intrusion other systems, sending forged messages or email from computer, or examining personal information stored on our computer (such as financial statements). Intruders (also referred to as attackers, crackers) may not care about our identity. Often, they want to take control of the computer, so you can use it to launch attacks on the computer systems. So, they (attackers) hide the control of our computers from their true lease and launch attacks or intrusions, often against very high-profile computer systems like government or financial systems. This research is the study on computer security using proposed A Real Time Host and Network Mobile Agent based Intrusion Detection System (HNMAIDS) which will enhance efficiency as compare earlier agent based intrusion detection system. An Agent based intrusion detection system is intended to detect suspicious behavior on the network/host through agent, where agent will send an alerts signal to the network administrators and so an administrator can prevent intrusions as well as attacks. Presented results are showing the performance of the proposed HNMAIDS.

Keywords

Intrusion Detection System (IDS), Agent Based, Network security(NS) Layers, Attacks, Network Intrusion Detection System (NIDS), Host Intrusion Detection System (HIDS).

1. INTRODUCTION

Over the last fifteen years the world has experienced a wide variety of computer threats and general computer security problems. The problem of managing and protecting information has existed long before information and communication technology came into being [13,14]. However, as technology advances and information management systems become more and more complicated; the problem of enforcing information security also becomes more critical [20]. The widespread use of communication networks for all purposes of computing is posing new serious security threats and increases the potential damage that security violations may cause. As organizations use of and reliance upon information increases, so too does their reliance on computer network and distributed computing environments, which become more vulnerable to security breaches [21]. This reliance requires advanced, intelligent, secure and safe information security systems to protect the organization's assets and information, in autonomic and intelligent ways. As communication advances and information management systems become more and more powerful and distributed, organizations are becoming increasingly vulnerable to potential security threats such as intrusions at all levels of Information Communication Technology (ICT) [22-23]. There is an urgency to provide secure and safe information security system through the use of firewalls, Intrusion Detection Systems (IDSs), Intrusion Prevention Systems (IPSs), encryption, authentication, and other hardware and software solutions [24]. Many intrusion detection and prevention systems have been designed, but still there are significant drawbacks. Some of these drawbacks are low detection efficiency, inaccurate prevention schemes and high false alarm rates. Since IDSs and IPSs have become necessary security tools for detecting and preventing attacks on ICT resources, it is essential to upgrade the previous designs, techniques and methods to overcome flaws [25-26]. Anomaly detection is an essential component of the detection mechanism against unknown attacks but this requires advanced techniques to be better and more effective. Proposed research entitled *"A Real Time Host and Network Mobile Agent Based Intrusion Detection System (HNMAIDS)"* is an intrusion detection system (IDS), conceptualized with mobile agent and works for host system as well as network system. Performance of the Proposed HNMAIDS is evaluated on selected performance parameters like intrusion finding capability on layers wise. The proposed HNMAIDS has three agents for NIDS and working of each agent is separate from each other. These entire agents will work independently but they all are dependent with each other whenever one agent will not pass signal in terms of object then second agent will not work and whenever second agent will not pass signal to third one agent then it will also not work [20-21]. The proposed HNMAIDS offers so many advantages over alternative IDS like higher security, high availability and scalability, and it having good capability to find out normal and abnormal behaviors of captured packet. The HNMAIDS includes integration of individual agent to produced good results. It supports to an administrator of the network as well as host the privileges for finding the intrusions which is reliable, secure and fast. The HNMAIDS implemented in short time and at a low cost. It also provides a best user interface.

2. PROPOSED METHODOLOGY

2.1 Proposed Work

The aim of the presented work is to use a mobile agent based approach for intrusion detection system in NIDS and HIDS, together with low-level high-speed traffic acquisition and reprocessing layer based on dedicated adaptive hardware and high-level operator interface [1, 2, 3]. To face the problem of effectiveness and accuracy in NIDS [4], the proposed research concept of the agents based intrusion detection is very effective and accurate which is based on extension of earlier agent based concept. In proposed approach, it is decide not to design and develop of a novel intrusion detection method, by rather to integrate or use existing agent based intrusion concept with an extended secured and effective models of a pre-specialized agent. This combination allows us to correlate the results of the used concept and to combine them to improve their accuracy and effectiveness [5, 6, 7]. Analysis of the layer supports operator's decisions about detected intrusion by providing additional information from related data sources. Proposed work presents a secure agent based IDS which is core part of the intrusion detection system designed to cope with a wide scale of network threats and anomalies. Proposed system worked on two limitations of earliest intrusion detection systems one is accuracy and another is efficiency [1]. Proposed HNMAIDS is the real time system which is deployed on high-speed network link implies the need to process on packet capturing in NIDS mode, in order to prevent the spread of novel threats. Fig 1 is showing the general diagram of proposed HNMAIDS. In this a system has two types of attacks one is network based if it is connected with internet or another is host based where it can be connected with network or not. In both cases proposed system read information and passes this collected information to proposed IDS where HNMAIDS pass all these received information to agent system. Here agents will work in proper way and find intrusion. To find intrusion there is used a data base which is known as rule based database. Rule base data base has predefine rules related with intrusions in a packet or log file in this work we have used KDD'99 data set [9] as an analysis of attacks and normal packet.

2.2 Proposed HNMAIDS

Architecture of Proposed Intrusion Detection System i.e. HNMAIDS is shown in Fig 2. In this five agents like network/host, rule, signal, intrusion detection and intrusion prevention agent works together but they do not acquire the data from the network/host directly, but receive/capture the preprocessed data in proper way, with the level of detail that is appropriate for host/network-based intrusion detection. Agent communications can be divided into two categories, communication among agents at same host in host mode and communication among agents on network systems in network mode. Communication methods for these situations have been studied in recent years. Communication among agents residing on the same computer need not be transmitted through the network layer [10]. They can communicate using other methods like pipes, message queues, and shared memory.

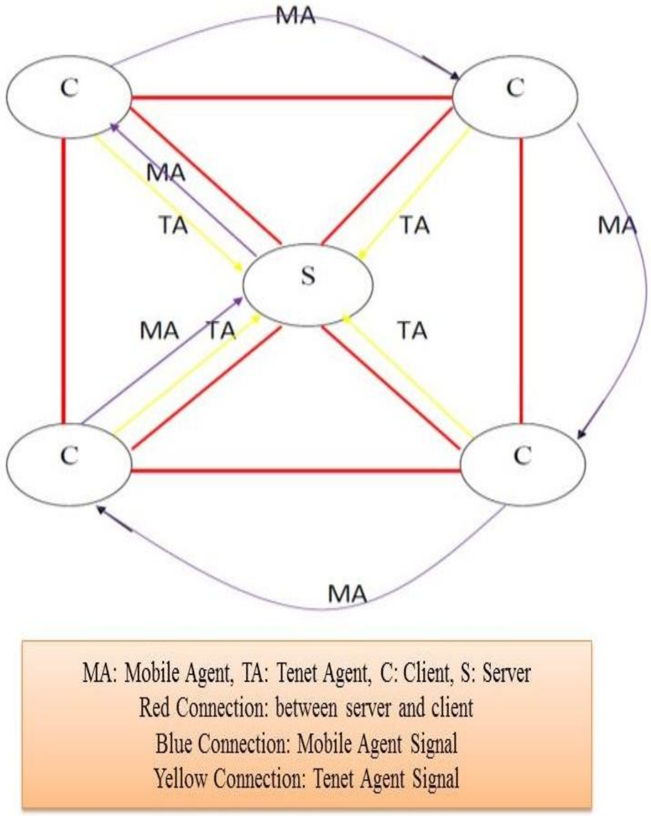

MA
C
C
MA
TA
TA
MA
S
MA
TA
TA
C
C
MA
MA: Mobile Agent, TA: Tenet Agent, C: Client, S: Server
Red Connection: between server and client
Blue Connection: Mobile Agent Signal
Yellow Connection: Tenet Agent Signal

Fig 1: Block diagram of proposed HNMAIDS

It has analyzed all the methods in the context of intrusion detection and identified their advantages and disadvantages. According to its findings, the most effective communication method among these agents is using a signal through a common object. It allows large volume of data to be shared and is efficient for one to many communications. Each detection agent in the object is based on earliest intrusion detection concept. Initially packet/log file will capture through network/host agent in respective mode then they allow whole information (captured packet in NIDS or log record in HIDS) to the rule agent where rule agent extract all the necessary information from received information (packets or log file) and match intrusion criteria if the intrusion found in the captured packets or log file then it passes this information to signal agent. When the signal agent reaches a conclusion regarding the intrusion of captured packets and its flow, then it sends information to intrusion detection agent which tell us detail information of intrusions and it generate a warning to user through message that automatically retrieves context information (intrusion records with full details) to allow rapid analysis by user. After detection of intrusion in the system another agent can be activated which can be called as intrusion prevention agent but this would be the future work. Proposed HNMAIDS architecture contains of two modes and each mode have same components. First is Network mode and second is Host mode. Detailed description of each component is as follow-

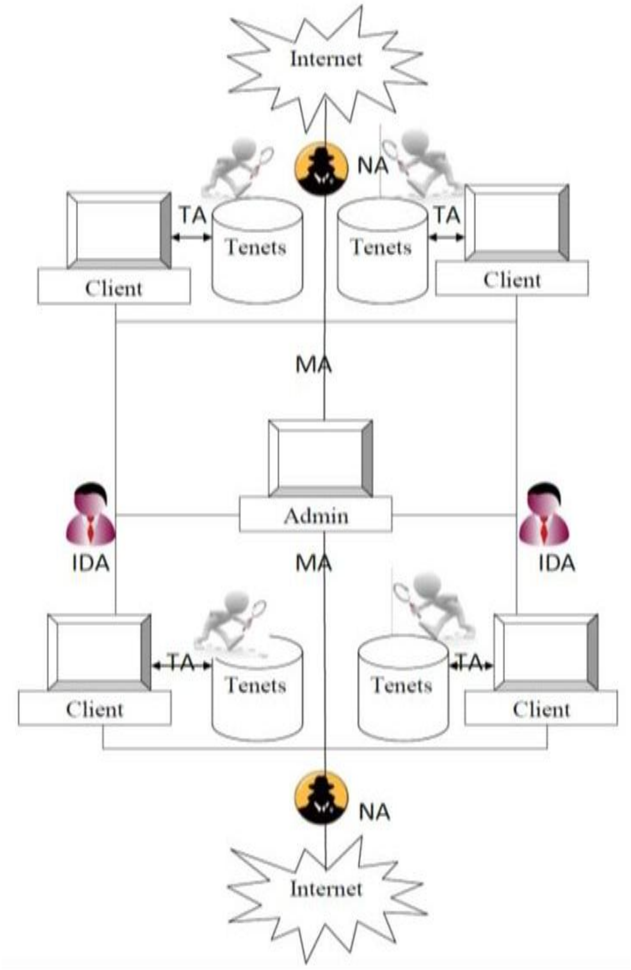


Fig 2: Proposed HNMAIDS architecture

3. AGENT PLATEFORM

Agents are the main component for HNMAIDS. These agents work with together to perform normal and abnormal behavior in captured packets. There are five types of Agents are working in this system, they are as follows:

a) Mobile Agent (MA): First agent is the mobile agent which will roam in the network and activates all the IDS at network system.

b) Network Agent (NA): Network agent will capture network packets from the network for individual network system. In NIDS primary assignment of NA is to sniffing theflows of traffic of the network. During sniffing network agents sniff different types of traffic like UDP, IP, TCP, ICMP, DNS.

c) Tenet Agent (TA): Tenet Agent matches tenets from data base of tenets and find out that capture packets are normal or abnormal.

d) Intrusion detection Agent (IDA): Intrusion detection agent passes all the information about abnormal and normal packets to administrator.

e) Alert (Attentive) Agent (AA**):** Attentive Agent send attentive signal to network system so network system aware from coming network intrusion.

4. PROPOSED WORK-FLOW

Steps of Proposed Concept are as follows (in Fig 3):

1. S→ IDS //Start Server(S) IDS
2. C→ IDS // Start Client(C) IDS
3. Acti → MA // Activate Mobile Agent (MA) at Server End
4. Move→ MA→Ns$_i$ // Move Mobile Agent in Network System(NS)
5. MA→ Acti→ NSIDS

   Move →MA→NS$_{i+1}$ // Mobile Agent activate Network System IDS and move another Network System
6. NSIDS→Acti→NA // IDS of Network System Activate Network Agent(NA)
7. NA→CapPack

   CapPack→TA // Network Agent Capture Packets and Transfer to Tenets Agents (TA)
8. Acti→TA // Activate Tenet Agent at Network System
9. TA→Ana(CapPack, Tenets) // Tenet Agent Analyze to Capture Packets with Tenets. And Send Report to Server
10. Acti→AA // Server System Activate to Alert (Attentive) Agent(AA)
11. Alert→NS // AA Send Alert to Network System
12. Repeat Step 3 to 11 Every 2hrs Duration.

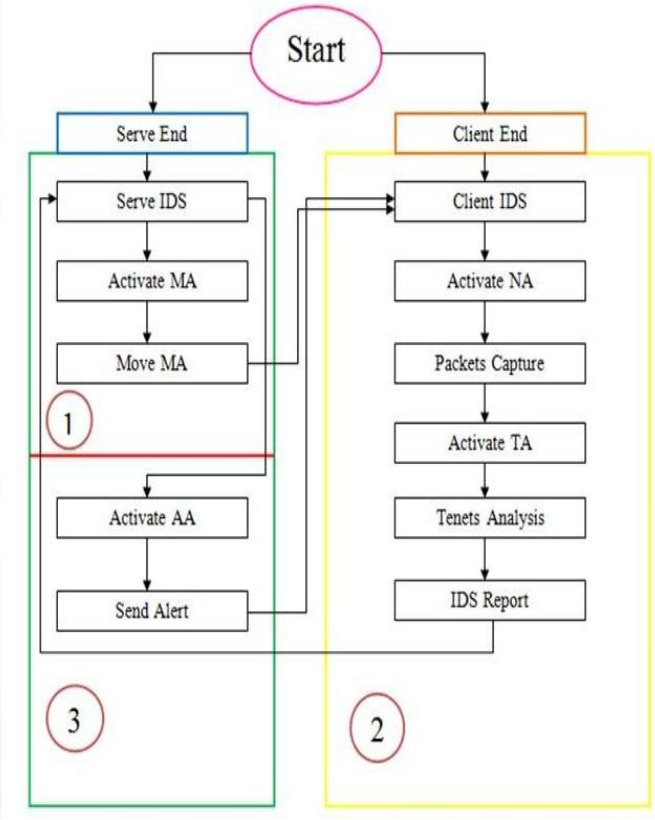


Fig 3: Flow diagram of HNMAIDS

5. PROPOSED TECHNIQUE

HNMAIDS is working in two Modes. One is NIDS and second is HIDS.

5.1 5.1 NIDS

5.1.1 Tenets Phase

In this phase proposed HNMAIDS have created the rules for normal behavior of packets as well as system and maintained in rule base data base. Here HNMAIDS have maintained tenets data base for different types of attacks like U2R, Probe, DOS, R2L and normal packets behavior [11, 12]. That's why Proposed HNMAIDS has created and maintained different behavior to find out some well-known intrusions. Record attributes (see Table 1) from capture packets and stored into tenets data-base. Table 1 shows the result of applying the attribute importance function to dataset of the captured packet. The tool ranks the attributes based on their significance, with the attribute of rank 1 being the most important attribute and all attributes having an importance less than or equal to zero have the same rank and considered as noise [12]. It is clear from this study of the network packet that 13 attributes out of the 41 attributes of the captured packet dataset have an importance value above zero, and the rest have an importance of zero. We will use these attributes in the agent based IDS process. We expect this to be more accurate having only 8 features while keeping the flag through the destination host difference server rate (dst_host_diff_srv_rate).

Table 1. Attribute selection

S. No.	Attributes
1	Flag
2	dst_host_srv_rerror_rate
3	dst_host_rerror_rate
4	dst_host_srv_serror_rate
5	dst_host_serror_rate
6	dst_host_srv_diff_host_rate
7	dst_host_same_src_port_rate
8	dst_host_diff_srv_rate

5.1.2 Detection Phase

In this phase Tenet Agent and Intrusion Detection Agent will work in following way.

Attacks If
{

Dos Attacks:
IF (Cap_Pack.Flag-> "SF"==0)

IF (Dst_Host_Ser_error_Rate<0 to 1>)

IF (Dst_Host_Ser_Rerror_Rate<0 to 1>)

IF (Dst_Host_Ser_Serror_Rate<0 to 1>)

IF (Dst_Host_Server_Rate<0 to 1>)

IF (Dst_Host_Ser_Diff_Host_Rate<0 to .44>)

IF (Dst_Host_Same_Src_Port_Rate<0 to 1>)

IF (Dst_Host_Diff_Ser_Rate<0 to 1>)

R2L Attacks:
IF (Cap_Pack.Flag-> "SF")

IF (Dst_Host_Ser_error_Rate< 0 >)

IF (Dst_Host_Ser_Rerror_Rate< 0 >)

IF (Dst_Host_Ser_Serror_Rate< 0 >)

IF (Dst_Host_Server_Rate< 0 >)

IF (Dst_Host_Ser_Diff_Host_Rate< 0 to 1>)

IF (Dst_Host_Same_Src_Port_Rate< .5 to 1>)

IF (Dst_Host_Diff_Ser_Rate< 0 >)

Probe Attacks:
IF (Cap_Pack.Flag-> "RSTO" || "REJ" || "SF")

IF (Dst_Host_Ser_error_Rate< 0 to 1 >)

IF (Dst_Host_Ser_Rerror_Rate< 0 to 1 >)

IF (Dst_Host_Ser_Serror_Rate< 0 >)

IF (Dst_Host_Server_Rate< 0 >)

IF (Dst_Host_Ser_Diff_Host_Rate< 0 to 1>)

IF (Dst_Host_Same_Src_Port_Rate< .01 to 1>)

IF (Dst_Host_Diff_Ser_Rate< 0 || 1 >)

U2R Attacks:
IF (Cap_Pack.Flag-> "SF")

IF (Dst_Host_Ser_error_Rate< 0 >)

IF (Dst_Host_Ser_Rerror_Rate< 0 >)

IF (Dst_Host_Ser_Serror_Rate< 0 >)

IF (Dst_Host_Server_Rate< 0 >)

IF (Dst_Host_Ser_Diff_Host_Rate< 0 to .5>)

IF (Dst_Host_Same_Src_Port_Rate< .5 to 1>)

IF (Dst_Host_Diff_Ser_Rate< 0 >)

OR

IF (Cap_Pack.Flag-> "SF" || "S3" || "RSTR" || "RSTO")

IF (Dst_Host_Ser_error_Rate< 0 to .96 >)

IF (Dst_Host_Ser_Rerror_Rate< 0 to .96 >)

IF (Dst_Host_Ser_Serror_Rate< 0 to 1 >)

IF (Dst_Host_Server_Rate< 0 >)

IF (Dst_Host_Ser_Diff_Host_Rate< 0 || 1>)

IF (Dst_Host_Same_Src_Port_Rate< .02 to 1>)

IF (Dst_Host_Diff_Ser_Rate< 0 >)

OR

IF (Cap_Pack.Flag-> "SO" || "S1" || "SF" || "SH")

IF (Dst_Host_Ser_error_Rate< 0 || .03 >)

IF (Dst_Host_Ser_Rerror_Rate< 0 >)

IF (Dst_Host_Ser_Serror_Rate< 0 to 1 >)

IF (Dst_Host_Server_Rate< 0 to 1 >)

```
IF (Dst_Host_Ser_Diff_Host_Rate< 0 >)
IF (Dst_Host_Same_Src_Port_Rate< 0 >)
IF (Dst_Host_Diff_Ser_Rate< 0 to 1 >)
}
Other Wise
{
Normal Packets:
}
```

5.2 Host IDS

5.2.1 Tenets Phase

Here HIDS have created the tenets for abnormal behavior and maintained in tenets for data base. For this proposed HNMAIDS has maintained two attribute (log- in & log-out time and authentication) in host mode [15-19]. It is already known that most of the attacker used illegal accessing of the host with in off working time. So that proposed system has created and maintained these two attributes to find out some well-known intrusions in record.

5.2.2 Detection Phase

This work focused on two attributes. In this Phase tenets Agent and intrusion detection Agents will work in following way.

```
        If Cap_ Value > TH
        Then
        Intrusion Detection Agent Activate
        Else
        Intrusion Detection Agent Deactivate
Tenet Agent Calculated tenet
        Authentication_Recorded_Value→
        User_Auth = Wrong( Password) > M
        Where M is 3 time
        Working_Time_Recorded_Value→
        Time = Log_In→10 AM
        &
        Log_Out→5 PM
```

Recorded_Value for authentication and time can be read from log file of the network system.

In tenets agent will sniff Log Record and identified Login filed details if it is more than three time that means any illegal user want access network system which is intrusion and Intrusion Detection Agent (IDA) activate and it circulates that information to admin to take necessary action to prevent such type of attacks. Similarly at the time of working period of user tenets agents checked login and log out time of network system if system is on before 10 am and after 5 PM then that mean illegal activities are happing over system then intrusion detection agent activate and send signal to admin for take necessary action to prevent such type of attacks.

6. RESULTS ANALYSIS

In this workvarious attacks like DOS, R2L, U2R Prob and normal packet during capturing packet in real time Network in NIDS mode are obtained [9]. Where HIDS focuses on two attributes like log in log out time and login details. The intended results are performed in the window-7 OS (32 bits) platform. For results, proposed HNMAIDS used laptop system with configuration, Pentium Dual Core E2300 3.67 GHz, 1 GB RAM, in which routine data is accumulating and viewing. Proposed HNMAIDS run number of times on different-different time and analyzed results which are shown in Table 2 and Graph 1 for NIDS.

Note: During real time network, direct internet line where no firewall and other security concerned was installed in the machine as well as network is used. If other security concerns are installed like firewall, VPN and others then number of captured attacked will low.

6.1 Experimental results

Presented experiment showing day-wise results. Total 6 day results are presented here:

Day 1 (01/11/2014): Start time of NIDS is 10:00 AM and stop time is 12:00 Noon. During this time number of DOS type Attacks packets found are 1007, U2R type Attacks are 889, R2L type attacks are 335, probe type attacks are 669 and normal packetsare 1342.

Day 2 (02/11/2014): Start time of NIDS is 1:00 PM and stop time is 03:00 PM. During this time number of DOS type Attacks packets found are 1500, U2R type Attacks are 982, R2L type attacks are 543, probe type attacks are 769 and normal packets are 1133.

Day 3 (03/11/2014): Start time of NIDS is 8:00 AM and stop time is 10:00 AM. During this time number of DOS type Attacks packets found are 437, U2R type Attacks are 192, R2L type attacks are 132, probe type attacks are 231 and normal packets are 1732.

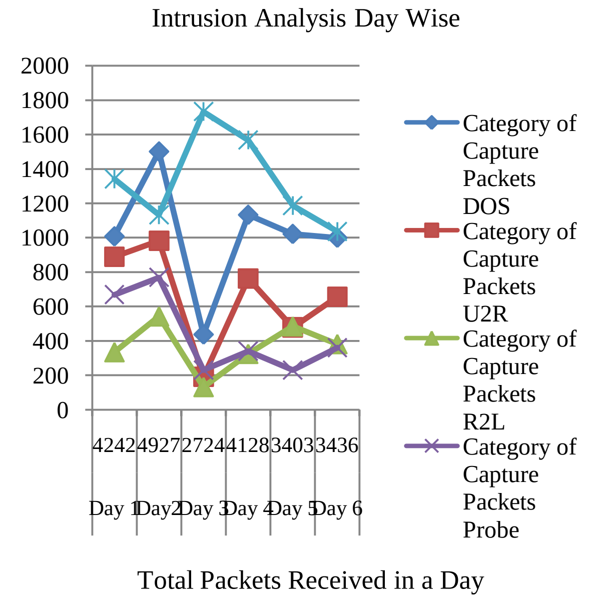
Day 4 (04/11/2014): Start time of NIDS is 5:00 PM and stop time is 07:00 PM. During this time number of DOS type Attacks packets found are 1132, U2R type Attacks are 763, R2L type attacks are 325, probe type attacks are 341 and normal packets are 1567.

Day 5 (05/11/2014): Start time of NIDS is 8:00 PM and stop time is 10:00 PM. During this time number of DOS type Attacks packets found are 1021, U2R type Attacks are 479, R2L type attacks are 485, probe type attacks are 231 and normal packets are 1189.

Day 6 (06/11/2014): Start time of NIDS is 2:00 PM and stop time is 04:00 PM. During this time number of DOS type Attacks packets found are 991, U2R type Attacks are 651, R2L type attacks are 382, probe type attacks are 361 and normal packets are 1037.

Table 2. Attack analysis through NIDS

Days	**Total Packets Received**	**Category of Capture Packets**				
		DOS	**U2R**	**R2L**	**Probe**	**Normal**
Day 1	4242	1007	889	335	669	1342
Day2	4927	1500	982	543	769	1133
Day 3	2724	437	192	132	231	1732
Day 4	4128	1132	763	325	341	1567
Day 5	3403	1021	479	485	231	1187
Day 6	3436	999	657	382	361	1037



Graph 1. Attack analysis over captured packets in NIDS

Secondly presented experiments (see Table 3 and Graph 2) are showing days wise with security concerned. Total 6 day results are presented hear.

Day 1 (01/11/2014): start time of NIDS is 10:00 AM in and stop time is 12:00 Noon. During this time DOS type Attacks packets are 23. U2R type Attacks are 16. R2L type attacks are 7, probe type attacks are 10 and normal packet 33.

Day 2 (02/11/2014): Start time of NIDS is 1:00 PM in and stop time is 03:00 PM. During this time DOS type Attacks packets are 42. U2R type Attacks are 20. R2L type attacks are 12, probe type attacks are 13 and normal packet 51.

Day 3 (03/11/2014): Start time of NIDS is 8:00 AM in and stop time is 10:00 AM. During this time DOS type Attacks packets are 19. U2R type Attacks are 11. R2L type attacks are 9, probe type attacks are 6 and normal packet 33.

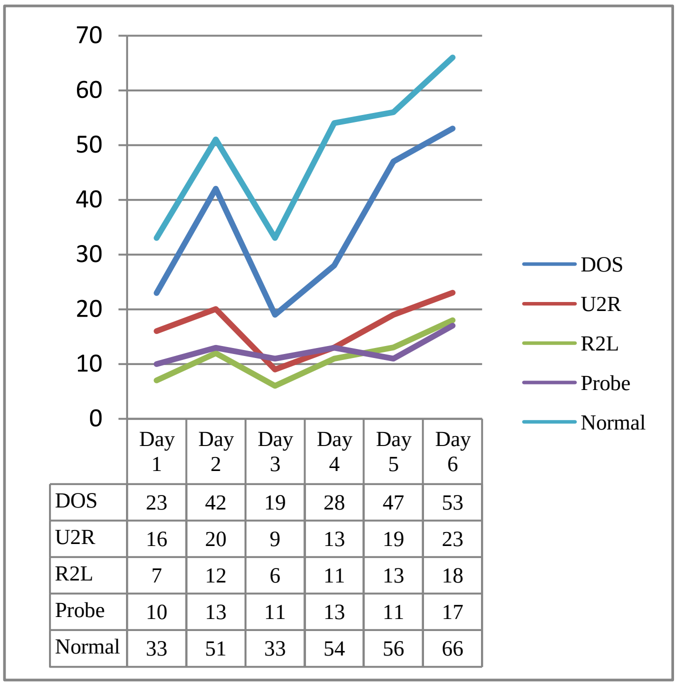
Day 4 (04/11/2014): Start time of NIDS is 5:00 PM in and stop time is 07:00 PM. During this time DOS type Attacks packets are 28. U2R type Attacks are 13. R2L type attacks are 11, probe type attacks are 13 and normal packet 54.

Day 5 (05/11/2014): Start time of NIDS is 8:00 PM in and stop time is 10:00 PM. During this time DOS type Attacks packets are 47. U2R type Attacks are 19. R2L type attacks are 13, probe type attacks are 11 and normal packet 56.

Day 6 (06/11/2014): Start time of NIDS is 2:00 PM in and stop time is 04:00 PM. During this time DOS type Attacks packets are 53. U2R type Attacks are 23. R2L type attacks are 18, probe type attacks are 17 and normal packet 66.

Table 3. Attack analysis through NIDS with security concerned (firewall)

DAYS	TOTAL PACKETS RECEIVED	CATEGORY OF CAPTURE PACKETS				
		DOS	U2R	R2L	PROBE	NORMAL
Day 1	89	23	16	07	10	33
Day2	138	42	20	12	13	51
Day 3	78	19	09	06	11	33
Day 4	119	28	13	11	13	54
Day 5	146	47	19	13	11	56
Day 6	177	53	23	18	17	66



	Day 1	Day 2	Day 3	Day 4	Day 5	Day 6
DOS	23	42	19	28	47	53
U2R	16	20	9	13	19	23
R2L	7	12	6	11	13	18
Probe	10	13	11	13	11	17
Normal	33	51	33	54	56	66

Graph 2. Attack analysis over captured packets in NIDS with security concerned (firewall)

At last proposed HNMAIDS is showing the results analysis of HIDS mode (as in Table 4). During HIDS analysis login and logout time is measured and noted down if any user login after valid time period then it will recorded and send an alert signal by agent to administrator for such type of intrusion.

Table 4. Attack analysis through HIDS

S. No.	User Name	User password	Date	Time	Status
1	Ram	Ram	11/11/2014	8:10:33	Wrong Time
2	Abhi	Abhi	11/11/2014	9:55:58	Wrong Time
3	abhi	abhi	12/11/2014	5:02:34	Wrong Time
4	asd123	asd123	13/11/2014	7:04:12	Wrong Time
5	Jai	Jai	14/11/2014	8:09:34	Wrong Time

6.2 Analysis

During results analysis proposed system has set two modes during real time NIDS one is without security concerned and second is with security concerned. One thing which is observed during these analysis that if security concerned is apply on network then total number of packet receiving is very low as compare without applied security concerned. From the results its observed that proposed AIDS are producing more accurate results as compare existing [2] in both mode for real time NIDS because existing IDS are using threshold values for detecting network intrusion and all these threshold value are assumption based. So there is a probability that produced result can differ from original results. But propose IDS using knowledge of KDD's 99 data set [8, 9, 12] in which we have study of all type of normal and abnormal behaviors of packets along with 41 attribute defined in KDD'99 data set, after that we have select 8 attribute (see Table 1) from 41 attribute which play important role during identification of intrusion in captured packets [12]. It is clear from produced results that 8 attributes out of the 41 attributes of the captured packets from network have a significance value higher than zero, and the rest have a significance of zero and hence not selected for the results. Another important thing of proposed AIDS is that it has the facility of Host IDS apart from network IDS in this if intrusion are coming from host system then it will also produce the report of such type of intrusions this type of facilities is not present in the existing IDS [2]. One more this in proposed AIDS is that it is finding more intrusion in capture packets as compare existing IDS [2] , presented results is six day analysis where proposed AIDS has sniff the network at various time and time interval and then producing the intrusions report.

7. CONCLUSION

As computer and information system attacks become more and more sophisticated, the need to provide effective intrusion detection methods increases. The current intrusion detection systems have some limitations and drawbacks. The deficiency of centralized intrusion detection systems leads to the idea of deploying agents based on autonomic principles. Agents are autonomous object that can act independent from one another and perform different tasks in a collaborative manner. Self-configuring is responsible for ensuring overall system management is coordinated and synchronized by these agents. In addition since agents behave independently, also reconfiguration of sensors is usually difficult but through collaboration and coordination management it can be simplified and made effective. In this research Proposed HNMAIDS that is more effective than current intrusion detection systems. The HNMAIDS provide an intelligent fault tolerant self-managed intrusion detection system with continuous runtime and minimum human intervention due to the use of multi-agents supervised by autonomic manager. With the self-management properties the system can dynamically adapt to changing environments, monitor and tune resources automatically, discover, diagnose and react to disruptions automatically.

Future enhancement is to extend this implementation with the use of mobile agents which have the capabilities to autonomously incarnate, migrate and consolidate inside the network from host to host to detect intrusions and execute prevention as a total solution against all known and some unknown generic threats. Another possible future work is to monitor not only the host resources but also the entire network by distributing these agents in a roving manner to make network based intrusion prevention system to deliver maximum security by anticipating threats as and when they happen.

8. REFERENCES

[1] Jitendra S Rathore, Praneet Saurabh, Bhupendra Verma "AgentOuro: A Novelty Based Intrusion Detection and Prevention System" Computational Intelligence and Communication Networks (CICN), Fourth International Conference on 2012.

[2] Zhang Ran "A Model of Collaborative Intrusion Detection System Based on Multi-agents" IEEE International Conference on (CSSS), 2012.

[3] Djemaa, B. ; Okba, K. "Intrusion detection system: Hybrid approach based mobile agent " IEEE International Conference on Education and e-Learning Innovations (ICEELI), 2012.

[4] Chetan R & Ashoka D.V "Data Mining Based Network Intrusion Detection System: A Database Centric Approach" International Conference on Computer Communication and Informatics (ICCCI), 2012.

[5] Rajashree Shedge and Lata Ragha " Hybrid Approach for Database Intrusion Detection with Reactive Policies" IEEE, 2012.

[6] Gidiya Priyanka V., Ushir Kishori N, Mirza Shoeb A, Ikhankar Sagar D and Khivsara Bhavana A "A Proposed System for Network Intrusion Detection System Using Data Mining" IJCA, 2012.

[7] AnuradhaSainiand Neelam Malik "Agent-based Network Intrusion Detection System Using K-Means clustering algorithm" International Conference on Computing and Control Engineering (ICCCE), 2012.

[8] Kartit, Saidi, Bezzazi, El Marraki, Radi " A New Approach To Intrusion Detection System" Journal of Theoretical and Applied Information Technology, 2012.

[9] Chandolikar, N.S and Nandavadekar, V.D. "Efficient algorithm for intrusion attack classification by analyzing KDD Cup 99" Wireless and Optical Communications Networks (WOCN), 2012.

[10] P.Rama Subramanian and J. Wilfred Robinson2 "Alert Over the Attacks of Data Packet and Detect the Intruders" in International Conference on Computing, Electronics and Electrical Technologies [ICCEET] 2012.

[11] Jeevaa Katiravan, C. Chellappan and J. Gincy Rejula "Detecting the Source of TCP SYN Flood Attack using IP Trace Back" European Journal of Scientific Research, 2012.

[12] Taisir Eldos, Mohammad Khubeb Siddiqui And Aws Kanan "On The Kdd'99 Dataset: Statistical Analysis For Feature Selection" Journal Of Data Mining And Knowledge Discovery, 2012.

[13] V. Jyothsna, V. V. Rama Prasad and K. Munivara Prasad "A Review of Anomaly based Intrusion Detection Systems" International Journal of Computer Applications, 2011.

[14] Asmaa Shaker Ashoor and Prof. Sharad Gore "Importance of Intrusion Detection System (IDS)" International Journal of Scientific & Engineering Research, 2011.

[15] Firkhan Ali Bin Hamid Ali and Yee Yong Len

"Development of Host Based Intrusion Detection System for Log Files" IEEE symposium on business, engineering and industrial application (ISBEIA) Langkawi, Malaysia 2011.

[16] Chung-Ming Ou and C.R. Ou "Immunity-inspired Host-based Intrusion Detection Systems" 2011.

[17] Ferdous A. Barbhuiya, Santosh Biswas, Neminath Hubballi and Sukumar Nandi "A Host Based DES Approach for Detecting ARP Spoofing" IEEE, 2011.

[18] Bin Zeng, Lu Yao, ZhiChen Chen "A Network Intrusion Detection System with the Snooping Agents" IEEE International Conference on Computer Application and System Modeling (ICCASM) 2010.

[19] LIN Ying, ZHANG Yan and OU Yang-Jia "The Design and Implementation of Host-based Intrusion Detection System" Third IEEE International Symposium on Intelligent Information Technology and Security Informatics 2010.

[20] Chundong Wang, Quancai Deng, Qing Chang,Hua Zhang and Huaibin Wang " A New Intrusion Detection System Based on Protocol Acknowledgement" IEEE 2010.

[21] Jianping Zeng and Donghui Guo "Agent-based Intrusion Detection for Network-based Application" International Journal of Network Security, 2009.

[22] Renuka Prasad., Dr.Annamma Abraham, Chandan Prabhanjan, AjayBilotia "Information Extraction for Offline Traffic Anomaly Detection in NIDS" International Journal of Computer Science and Network Security, 2008.

[23] Martin Rehak, Michal Pechoucek, Pavel Celeda, Jiri Novotny, Pavel Minarik "CAMNEP: Agent-Based Network Intrusion Detection System" International Conference on Autonomous Agents and Multiagent Systems, 2008.

[24] Jin-Tae Oh , Sang-Kil Park, Jong-Soo Jang and Yong-Hee Jeon "Detection of DDoS and IDS Evasion Attacks in a High-Speed Networks Environment" published in IJCSNS International Journal of Computer Science and Network Security, 2007

[25] Moad Alhamaty, Ali Yazdian and Fathi Al-qadasi "Intrusion Detection System Based On The Integrity of TCP Packet" World Academy of Science, Engineering and Technology, 2007.

[26] T. S. Sobh "Wired and wireless intrusion detection system Classifications, good characteristics and state-of-the-art", Computer Standards & Interfaces, Science Direct, 2006.