ANUSANDHAN- AISECT University Journal
Vol. 06, Issue No. 13, March-2018, P-ISSN 2278-4187, E-ISSN 2457-0656

Implementation of Mobile Agent Intrusion Detection System Based on Significant Parameters

Aumreesh Kumar Saxena[1]* Dr. Sitesh Sinha[2] Dr. Piyush Shukla[3]

[1]Asst. Prof. (AP) in CSE Dept of SIRTS, Bhopal (M.P.) India

[2]Prof. CSE Dept. RNTU, Bhopal (M.P.) India

[3]Prof. CSE Dept. UIT RGPV, Bhopal (M.P.) India

Abstract – Unauthorized accesses of computer application and network are biggest issue in the field of computer security. Due to the popularity of the computer system and computer applications, new kinds of attacks are emerging rapidly. The Intrusion Detection Systems (IDS) detects this type of intrusion activity. This paper is design and development of IDS using mobile agent to enhance the efficiency as compared to previous IDS based on Mobile Agents. Furthermore this paper is also the deep study of significant parameters called features of NSLKDD data set and its values. On the basis of deep analysis of 41 feature of NSLKDD dataset, 13 significant features and its threshold values identified by proposed IDS. Total five rules for the identification of normal and abnormal (DOS, U2R, Probe, R2L) packet is designed which is based on 13 significant features. Our deep analysis of significant parameters and experiments clearly shows that proposed IDS is more effective and accurate which is also reducing response time and false alarms rate.

Keyword—Intrusion Detection System (IDS), Network, Host, Agent, Mobile Agent (MA), Alert Agent, Network Agent, Packet Capture Agent, Tenet Agent

----------♦----------

I. INTRODUCTION

The Internet is a network of computer networks. It has evolved from the interconnection of networks around the globe (Naser Fallahi, et.al. 2016). Internet connection may be used by hackers (or as some would rather call them crackers) to gain unauthorized access to local network (Audrey 2016). Availability of computing facilities can also be targeted by Denial of Service (DoS) attacks numerous techniques have been produced to secure the network infrastructure and correspondence over the Web, among them the utilization of firewalls, encryption, decoding and virtual private networks systems (Zhang Ran 2012). Intrusion detection is a new extension to such techniques. Intrusion detection system began showing up over the most recent couple of years. Utilizing intrusion detection system, we can gather and utilize data from known sorts of attacks and see whether somebody is attempting to access system or specific hosts (Gidiya Priyanka et.al. 2012). IDS are commonly mistaken for a firewall or as a substitute for a firewall. While they both relate to network security, IDS differs from a firewall in that a firewall looks out for intrusions in order to stop them from happening (Gidiya Priyanka et.al. 2012).

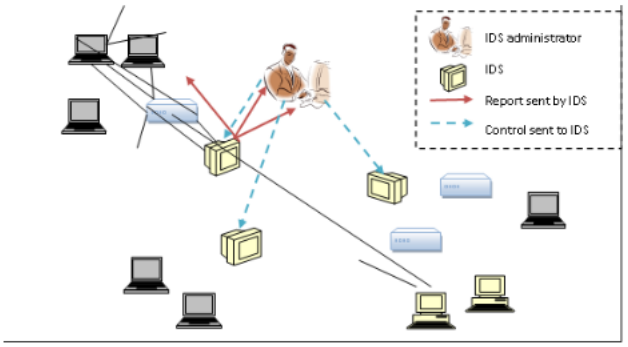


Fig. 1: Working of IDS

The firewall limits the access between networks in order to prevent intrusion and does not signal an attack from inside the network. Figure 1 shows the working of IDS in a network. The Major IDS Classifications (see figure 3) are Active IDS, Passive IDS, Network Intrusion Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS) (Anuradha Sainiand Neelam Malik 2012). On The

Bases of Detection Method IDS are Anomaly Detection Based and Signature Detection Based.

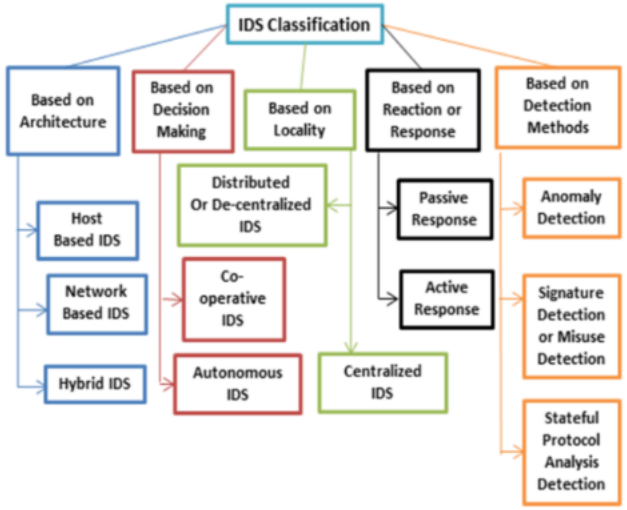


Fig. 2: IDS Classification (Anuradha Sainiand Neelam Malik 2012)

2. RELATED WORK AND PROBLEM FORMULATION

Earlier research introduced a methodology to identify attack intrusion using agent based, time based and many more type detection. The method used to identify anomalies based and misuse on the number of connection made in predefines threshold values (Rajashree Shedge, 2012, Djemaa 2012). In this they have capture approximately one thousands of packet in given value but they have not cleared about packets due to unreliable in nature, so this is very difficult task to identify normal and abnormal behavior of packet with accurate way. In existing misuse detection IDS unknown type of attacks may not be detected or may be improperly classified (Bin Zeng, et.al. 2010). The major issues of misuse based IDS are database must be continually updated and maintained (Bin Zeng, et.al. 2010, LIN Ying, 2010). Anomaly detection is another important problem that has been researched within diverse research areas. The main limitation is that it may not be able to describe attack pattern and may have high false positive rate (DuXianFeng 2010). There are numerous issues in existing anomaly detection IDS like anomaly detection IDS produces usually large number of false-positive alarms, which events are signaling an IDS to produce an alarm when no attack has taken place (Weijian Huang 2010). Another issue is a legitimate system behavior may also be recognized as abnormal patterns (Wang Yu 2011). Since normal behavior can change easily, anomaly-based IDS systems are prone to false positives where attacks may be reported based.

3. PROPOSED WORK

Basically proposed IDS is divided into two phase. In first phase we design and developed mobile agent (Jitendra et.al. 2012) based IDS and in second phase we design rules on the basis of 13 sleeted features out of 41 from NSLKDD data sets (L. Dhanabal 2015).

(a) Phase-I

This is the phase one of proposed IDS wherein one mobile agent and three other agents designed by the proposed IDS and working of each agent is separate from other. These all agents will work autonomously however they all are reliant with each other at whatever point one agents won't pass signal regarding object then second agent won't work and at same as second operator won't pass signal to third one agent then it will also not work. Figure 3 shows the Mobile Agent over Client Server Architecture where mobile agent move over clients in the network and collected all related information with normal and abnormal packets which is captured at particular clients. After that it sends compiled report to sever for further action. Once this report received by server then it send a suitable alarm if abnormality finds. The aim of the presented work is to use a mobile agent based approach for intrusion detection system, together with low-level high-speed traffic acquisition and reprocessing layer based on dedicated adaptive hardware and high-level operator interface.

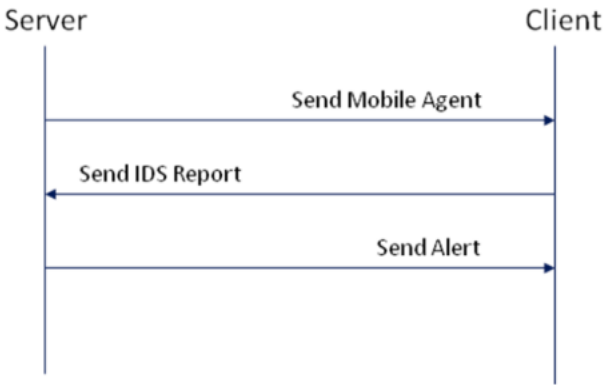


Fig. 3: Mobile Agent over Client Server Architecture

Architecture of proposed IDS is shown in figure 4. In this four agents like Mobile Agent, network agent, rule agent and alert agent works together but they do not procure the information from the network directly, yet get/catch the pre prepared information in legitimate path, with the level of detail that is proper for network-based intrusion detection. Agents are conveying among specialists on network systems in network mode.

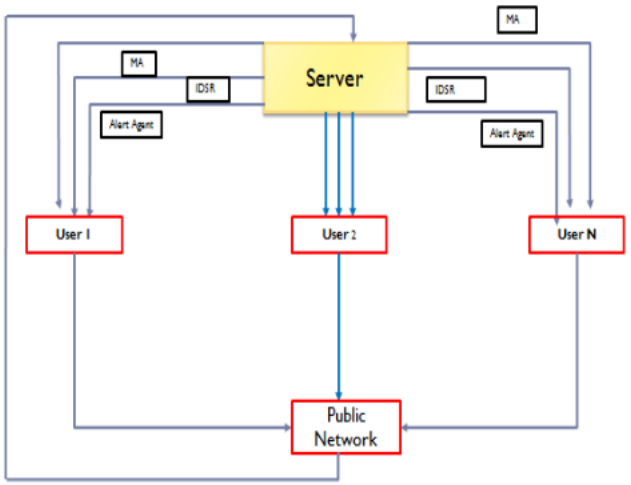


Fig. 4: Architecture of Proposed IDS

Agent Structure: There are four types of agents that are involved in Proposed IDS:

(i) **Mobile Agent (MA):** Mobile Agent is the main agent is which roams in the network system and activates IDS at host.

(ii) **Network Agent (NA):** In this primary assignment of Network agent is to sniffing the flows of traffic of the network. Network agent captures network packets from the network and sniff different types of traffic like TCP, UDP.

(iii) **Rule Agent (RA):** Captured packet is normal or abnormal is identified by rule Agent, they match rules from received packet which is stored in database to find out normal or attacked packets.

(iv) **Alert Agent (AA):** In case of any coming network intrusion, alert agent sends signal to network system to make the system aware of coming intrusion.

To adapt to a wide size of system threats and anomalies, any IDS depends on secure specialist mobile agent IDS which is center some portion of the IDS. To essential components system efficiency and accuracy is contemplated while planning the system and work on to enhance both the elements in proposed IDS. So as to keep the spread of novel threats, the proposed IDS which is deployed on rapid system interface suggests the need to prepare on packet capturing. Figure 5 is showing the working model of proposed IDS based on real time. In this model each agents working is defined that mobile agent (MA) move to clients over network and activated client IDS, once it is activated then it start sniffing and capturing network packets through Network Agent (NA) and stored in database. To find intrusion among the network packets, Rule Agent used database which is known as rule based database. Rule base database has predefined rules related with intrusions in a packet or log file in this work. A consolidate report send by the client to sever and then Alert Agent send alert by the server if any abnormality find in captured packets.

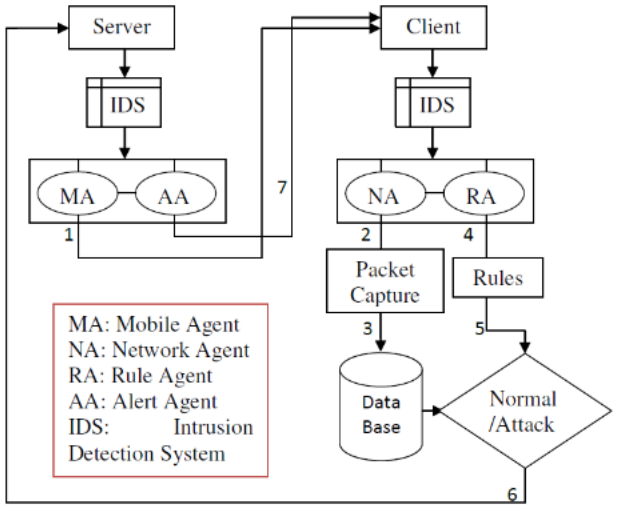


Fig. 5: Working Model of Proposed IDS.

(i) Step wise step processes of working model are as follow:

(ii) Run ➔ IDS at Server.

(iii) Initialize ➔ Mobile Agent ➔ Initialize (MA) at Server.

(iv) Client ➔ Mobile Agent Move to All Client System over network and activate Clients IDS.

(v) Client ➔ IDS ➔ Activate.

(vi) Sniffing ➔ Network Agent sniffing the flow of Network Packet and Capture Packet.

(vii) Data Base ➔ Captured Packets Stored in Data Base.

(viii) Rules Matching ➔ Rule Agent Checked and Verified to Capture Packets with pre-defined rules. And Send Report to the Server

(ix) Alert ➔ Alert Agent Send Alert to Clients.

(b) **Phase-II**

This is the second phase of the proposed IDS wherein, we used NSLKDD dataset which is a enhance version of KDDCUP-99 dataset [17]. NSL-KDD data has 41 features these features include numeric, symbolic, and binary where features 2, 3,

www.aujournals.ipublisher.in

and 4 are nominal, features 7, 12, 14, 15, 21, and 22 are binary, and the rest of the features are numeric type attributes recommended by. During the study of NSL KDD data set it is observed that one of the most important features of NSL KDD is flags feature which has some different values; it is a very important feature to identify intrusion at initial level. The description of the different 'flag' values are listed in Table 1.2.

Table 1.2 NSL KDD Dataset Features Flags Description

Flag	Description
RSTOS0	Originator sent a SYN followed by a RST, never see a SYN ACK from the responder
RSTR	Established, responder aborted
RSTO	Connection established, originator aborted (sent a RST)
OTH	No SYN seen, just midstream traffic (a "partial connection" that was not later closed)
REJ	Connection attempt rejected
SF	Normal establishment and termination Originator sent a SYN followed by a FIN (finish 'flag') ,

Now NSL-KDD dataset contain various types of attacks which categorized in four major categories are as follow:

(i) **DOS Attack**: full name of DOS is Denial of Service by this attack hackers or outsiders makes a processing or memory assets excessively busy or too full.

(ii) **Probe Attack:** where the hacker is scans to the network and find out the active port on a machine with the aim of exploiting is a known vulnerability.

(iii) **Remote-to-Local (R2L) Attack**: attacks, where an attacker tries to gain local access to unauthorized information.

(iv) **User-to-Root (U2R) Attack:** where an attackers picks up root access of network to utilizing his ordinary client account to endeavor vulnerabilities.

After the deep analysis NSLKDD data set (50000 approx.) database packet, proposed IDS identify threshold values of 13 features out of the 41 feature set that have significance esteem over zero. Table 1.3 is showing the threshold value of these 13 features for various types of attacks and normal packet.

Table 1.3 Selected 13 Feature out of 41 for attack and its threshold value

Features	Dos	Normal	Probe	R2l	U2R
Protocol_Type (2)	Tcp, Udp,	Tcp, Udp	Tcp, Udp	Tcp	Tcp
Flag (4)	SF,REJ,RSTO	SF,REJ,RSTR,RSTO, OTH	,SF,SH,REJ ,RSTR, RST0S0,OTH	SF,RSTO	SF
Src_Bytes (5)	0 To 54540	0 To 76355876	0 To 215	0 To 7045	0 To 6274
Land (7)	0 ,1	0	0	0	0
Wrong_Fragment (8)	0,1,3	0	0	0	1 ,2,4
Hot (10)	0 To 2	0 To 77	0 To 1	0 To 28	0 To 5
Logged_In (12)	0,1	0,1	0,1	0,1	0,1
Count (23)	0 To 511	0 To 511	0 To 511	1 To 4	0
Diff_Srv_Rate (30)	0 To 0.75	0 To 1	0 To 1	0	0 To 0.5
Dst_Host_Same_Srv_Rate (34)	0 To 1	0 To 1	0 To 1	0 To 1	0 ,1
Dst_Host_Diff_Srv_Rate (35)	0 To 0.75	0 To 1	0 To 1	0 To 0.20	0 To 0.02
Dst_Host_Same_Src_Port_Rate (36)	0 To 1	0 To 1	0 To 1	0 To 1	0 ,0.5,1
Dst_Host_Srv_Diff_Host_Rate (37)	0 To 0.54	0 To 1	0 To 1	0 To .31	0 To 0.4

Proposed IDS used these selected 13 features that is used for experiment and implementation of mobile agent based IDS. On the basis of 13 features proposed IDS designed total five rules which are used by Rule Agent see figure 6, 7, 8,9,10.

Rule-1 For Dos Attack

IF

(Cap_Packet.Protocol_type="TCP"||"UDP"||"ICMP")

IF (Cap_Packet.Flag = "S0" || "SF" || "REJ" ||"RSTO")

IF (Cap_Packet. Src_bytes < 0 to 54540 >)

IF (Cap_Packet_Land <0 || 1 >)

IF (Cap_Packet_ Wrong_fragment <0 to 3>)

IF (Cap_Packet_Hot <0 to 2>)

IF (Cap_Packet_logged_in <0 || 1>)

IF (Cap_Packet_Count <0 to 511>)

IF (Cap_Packet_ Diffrent_srv_rate <0 to 0.75>)

IF (Cap_Packet_ Dst_host_same_srv_rate <0 to 1>)

IF (Cap_Packet_ Dst_host_diff_srv_rate <0 to 0.75>)

IF (Cap_Packet_ Dst_host_same_src_port_rate <0 To 1>)

IF (Cap_Packet_Dst_host_srv_diff_host_rate <0to 0.54>)

Fig. 6: Rule-1 for DoS Attack

Rule-2 For Probe Attack

IF(Cap_Packet.Protocol_type="TCP"||"UDP "|| "ICMP")
IF(Cap_Packe.Flag = "S0"||"SF"||"SH"||"REJ"||"RSTR" ||"RSTO"|| "RST0S0" ||"OTH ")
IF (Cap_Packet. Src_bytes < 0 to 215 >)
IF (Cap_Packet_Land < 0 >)
IF (Cap_Packet_ Wrong_fragment <0 >)
If (Cap_Packet_Hot <0 ||1>)
IF (Cap_Packet_logged_in <0 || 1>)
IF (Cap_Packet_Count <0 To 511>)
IF (Cap_Packet_ Diff_srv_rate <0 to 1>)
IF (Cap_Packet_ dst_host_same_srv_rate <0 to 1>)
IF (Cap_Packet_ dst_host_diff_srv_rate <0 to 1>)
IF (Cap_Packet_ dst_host_same_src_port_rate <0 to 1>)
IF (Cap_Packet_ dst_host_srv_diff_host_rate <0 to 1>)

Fig. 7: Rule-2 for Probe Attack

Rules-3 For R2L Attack

IF (Cap_Packet. Protocol_type = " TCP")
IF (Cap_Packet.Flag = "S0" ||"RSTO ")
IF (Cap_Packet. Src_bytes < 0 to 7045 >)
IF (Cap_Packet_Land <0 >)
IF (Cap_Packet_ Wrong_fragment <0 >)
If (Cap_Packet_Hot <0 To 28>)
IF (Cap_Packet_logged_in <0 || 1>)
IF (Cap_Packet_Count <0 To 4>)
IF (Cap_Packet_ Diff_srv_rate <0>)
IF (Cap_Packet_ dst_host_same_srv_rate <0 to 1>)
IF (Cap_Packet_ dst_host_diff_srv_rate <0 to .20>)
IF (Cap_Packet_ dst_host_same_src_port_rate <0 to 1>)
IF (Cap_Packet_ dst_host_srv_diff_host_rate <0 to .31>)

Fig. 8: Rule-3 for R2L Attack

Rules-4 For U2R Attack

IF (Cap_Packet. Protocol_type =" TCP")
IF(Cap_Packet.Flag ="SF")
IF (Cap_Packet. Src_bytes < 0 to 6074 >)
IF (Cap_Packet_Land <0 >)
IF (Cap_Packet_ Wrong_fragment <0>)
If (Cap_Packet_Hot <0 To 5>)
IF (Cap_Packet_logged_in <0 || 1>)
IF (Cap_Packet_Count <1 to 5>)
IF (Cap_Packet_ Diff_srv_rate <0 to 0.5>
IF (Cap_Packet_ dst_host_same_srv_rate <0 to 1>)
IF (Cap_Packet_ dst_host_diff_srv_rate <0 to .02>)
IF (Cap_Packet_ dst_host_same_src_port_rate <0 to 1>)
IF (Cap_Packet_ dst_host_srv_diff_host_rate <0 to .4>)

Fig. 9: Rule-4 for U2R Attack

Rules-5 For Normal Packet

IF (Cap_Packet.Protocol_type="TCP'||'UDP' ||' ICMP")
IF (Cap_Packet.Flag ="SF" || "REJ" || "RSTR" ||"RSTO")
IF (Cap_Packet. Src_bytes < 0 to 76355876>)
IF (Cap_Packet_Land <0 >)
IF (Cap_Packet_ Wrong_fragment <0>)
If (Cap_Packet_Hot < 0 to 77>)
IF (Cap_Packet_logged_in <0 || 1>)
IF (Cap_Packet_Count <0 to 511>)
IF (Cap_Packet_ Diff_srv_rate <0 to 1>)
IF (Cap_Packet_ dst_host_same_srv_rate <0 to 1>)
IF (Cap_Packet_ dst_host_diff_srv_rate <0 to 1>)
IF (Cap_Packet_ dst_host_same_src_port_rate <0 to 1>)
IF (Cap_Packet_ dst_host_srv_diff_host_rate <0 to .1>)

Fig. 10: Rule-5 for Normal Packet

www.aujournals.ipublisher.in

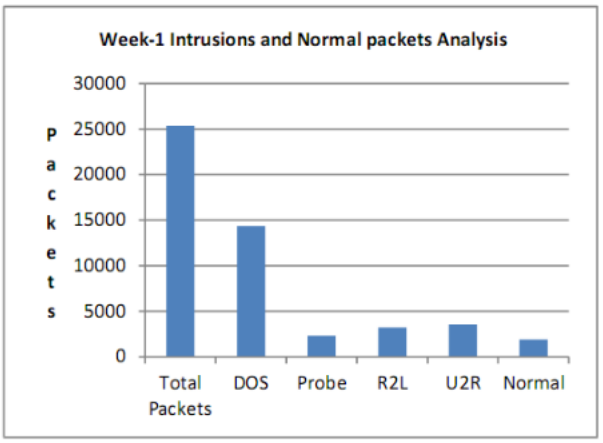
4. RESULTS

To evaluate the performance of the proposed IDS we set machine configuration which is (Intel core i5 second generation with 4GB RAM at Window platform). Proposed IDS is developed at java language with JDK1.8 version, which easiest the development of mobile agent and other agents. During experiment, real time network has developed where two machines were setup, one for client and other for sever and both machine connected through public network like internet. At this scenario proposed IDS prepared data record set of two week. First week data collection was 25368 packets in which 23463 packets were intrusion packets and 1905 packets were normal packets. Time duration of data collection of first week was 9 am to 10 am in which data traffic load are average. Second week data collection was 40766 packets in which 39233 packets were intrusion packets and 1339 packets were normal packets. Time duration of data collection of first week was 2 pm to 3 pm in which data traffic load are high. Detail descriptions of intrusion are as follow: Table 1 shown week 1 analysis where total packet received 25368 in which we have found 14372 DOS attacks, 2315 probe attacks, 3231 R2L attacks , 3345 U2R attacks and 1905 normal packets.

TABLE 1: WEEK-1 INTRUSION AND NORMAL PACKETS ANALYSIS

Total Packets	DOS	Probe	R2L	U2R	Normal
25368	14372	2315	3231	3545	1905

Graph 1 is showing graphical analysis of intrusion of week 1



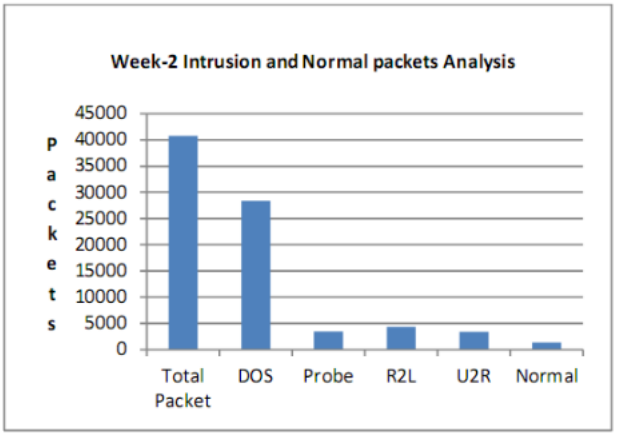
Graph 1: Intrusion Vs Normal Packet in Week 1

Table 2 shown week 2 analysis where total packet received 40766 in which we have found 28354 DOS attacks, 3411 probe attacks, 4321 R2L attacks , 3341 U2R attacks and 1339 normal packets.

TABLE 2: WEEK-2 INTRUSION AND NORMAL PACKETS ANALYSIS

Total Packet	DOS	Probe	R2L	U2R	Normal
40766	28354	3411	4321	3341	1339

Graph 2 is showing graphical analysis of intrusion of week 2.



Graph 2: Intrusion Vs Normal Packet in Week 2

5. CONCLUSION AND FEATURE WORK

In this paper Proposed IDS that is more successful than current IDS and with nonstop runtime and least human intervention because of the utilization of multi-agents technique can also acts as an intelligent fault tolerant self-managed intrusion detection system. With the self-adjustable and manageable nature of the system it can dynamically change environments, monitor resources automatically without human intervention, diagnose, discover and react automatically. In Future with the advancement in the network system the mobile agent's parameter is to be reconfigured to cope of various types of intrusion and also make it more and more effective.

REFERENCES

Naser Fallahi; Ashkan Sami; Morteza Tajbakhsh (2016). "Automated flow-based rule generation for network intrusion detection systems" 2016 24th Iranian Conference on Electrical Engineering (ICEE) Page(s): 1948 - 1953,

Audrey A. Gendreau; Michael Moorman (2016). "Survey of Intrusion Detection Systems towards an End to End Secure Internet of Things" IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud) Year: 2016 Page(s): 84-90,

Zhang Ran (2012) "A Model of Collaborative Intrusion Detection System Based on Multi-agents" IEEE International Conference on Computer Science & Service System (CSSS), Page(s): 789–792

Gidiya Priyanka V., Ushir Kishori N, Mirza Shoeb A, Ikhankar Sagar D and Khivsara Bhavana A. (2012). "A Proposed System for Network Intrusion Detection System Using Data Mining" IJCA Proceedings on International Conference in Computational Intelligence (ICCIA2012) © by IJCA Journal

Anuradha Sainiand Neelam Malik (2012). "Agent-based Network Intrusion Detection System Using K-Means clustering algorithm" IEEE International Conference on Computing and Control Engineering (ICCCE 2012), pp. 12 & 13.

Rajashree Shedge and Lata Ragha (2012). "Hybrid Approach for Database Intrusion Detection with Reactive Policies" IEEE Fourth International Conference on Computational Intelligence and Communication Networks

Djemaa, B. ; Okba, K. (2012). "Intrusion detection system: Hybrid approach based mobile agent "IEEE International Conference on Education and e-Learning Innovations (ICEELI), Publication Year: 2012 , Page(s): 1–6

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

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

Du Xian Feng, Qiang Zan Xia, (2010). "A Model of Intrusion Detection System Based on Aglet with Multi-Agent" International Conference on Computer Application and System Modeling (ICCASM 2010)

Weijian Huang, Yan An, Wei Du (2010). "A Multi-Agent-Based Distributed Intrusion Detection System " 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE) Page(s): VS141-VS144

Wang Yu, Cheng Xiaohui, Wang Sheng, (2011). Anomaly "Network Detection Model Based on Mobile Agent" 3rd International Conference on Measuring Technology and Mechatronics Automation Page(s): pp. 504-508

David L. Hancock, Gary B. Lamont. (2012). "Multi Agent System For Network Attack Classification Using Flow-Based Intrusion Detection" IEEE, Page(s): 1535-1542.

Jitendra S Rathore, Praneet Saurabh, Bhupendra Verma (2012). "Agent Ouro A Novelty Based Intrusion Detection and Prevention System" Computational Intelligence and Communication Networks (CICN), Fourth International Conference on 3-5 Nov. 2012 Page(s): 695 - 699

L.Dhanabal, Dr. S.P. Shantharajah, (2015). "A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms" International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 6, Page(s): 446-452

Chetan R & Ashoka D.V. (2012). "Data Mining Based Network Intrusion Detection System: A Database Centric Approach" IEEE 2012 International Conference on Computer Communication and Informatics (ICCCI - 2012), Coimbatore, INDIA Jan. 10–12, 2012.

S. Revathi, Dr. A. Malathi (2013). "A Detailed Analysis on NSL-KDD Dataset Using Various Machine Learning Techniques for Intrusion Detection " International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 12, December-2013, Page(s): 1848-1553

Sanoop Mallissery, Sucheta Kolekar, Raghavendra Ganiga (2013). "Accuracy Analysis of Machine Learning Algorithms for Intrusion Detection System using NSL-KDD Dataset" July 2013

Shailesh Singh Panwar, Dr. Y. P. Raiwani (2014). "Data Reduction Techniques To Analyze NSL-KDD Dataset" International Journal of Computer Engineering and Technology (IJCET), ISSN 0976-6367 Volume 5, Issue 10, October (2014), Page(s): 21-31

Vajihe Abdi, Marzieh Ahmad (2014). "Implementing A New Semi-Supervised Approach For Internet Traffic Classification Using NSL-KDD Database International" Journal of Computer Science and Information Technology

Research ISSN 2348-120X (online) Vol. 2, Issue 3, pp. 386-393, Month 2014

Corresponding Author

Aumreesh Kumar Saxena*

Asst. Prof. (AP) in CSE Dept of SIRTS, Bhopal (M.P.) India

E-Mail – aumreesh@gmail.com