International Journal of Information Technology and Knowledge Management
July-December 2011, Volume 4, No. 2, pp. 609-612

DETECTION AND PREVENTION OF FLOODING TYPE INTRUSION FOR ANY ENTERPRISE INFORMATION SYSTEM

KP Singh[1], Yogesh Chaba[2], Gaurav Lodha[1] & Yudhvir Singh[2]

Intrusion detection is a security technology that attempts to identify individuals who are trying to break into and misuse a management information system without authorization and those who have legitimate access to the system, but are abusing their privileges. With the rapid growing unauthorized activities in management information system, Intrusion Detection as a component of defence is very necessary because traditional firewall techniques cannot provide complete protection against intrusions. Network – based IDSs are designed to monitor potential attacks in enterprise network information security. Detection of intrusions falls in two categories anomaly and signature detection. In this paper a new IDS is designed for enterprise information system. In designed prevention module two techniques Handle RREQ and Retry RREQ function (HRR) and Disable Broadcasting (DB) are implemented. Performance is evaluated for different parameters and it is found that the proposed system of intrusion detection gives much better performance.

Keywords: IDS, Intrusion, PDR, Security, Information

1. Introduction

Intrusion detection is a tool that attempts to identify intruders who are trying to break into and misuse organization database without authorization and those who have legitimate access to the system, but are abusing their privileges. It dynamically monitors the system and user actions in the network and computer systems in order to detect intrusions. Intrusion Detection Systems[1][2] are software or hardware products that automate this monitoring and analysis process. Because an information system can suffer from various kinds of security vulnerabilities, it is both technically difficult and economically costly to build and maintain a system, which is not susceptible to attacks. Pro-active security techniques are not enough to protect Distributed Information System from attacks, so re-active security technique are required and IDSs are part of re-active defense technique. Intrusion detection[9] is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions, defined as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network. Intrusions are caused by intruders accessing the systems from the Internet, authorized users of the systems who attempt to gain additional privileges for which they are not authorized, and authorized users who misuse the privileges given to them. Intrusion detection is a tool that protect organization systems from the attacks that come with network connectivity.[10][11]. A lot of work has been done in this area. Zaman et al. [3] proposed a novel concept for building lightweight IDS based on two different approaches using a features selection approach by applying fuzzy enhanced support vector decision function (Fuzzy ESVDF) algorithm and second approach by using IDS classification scheme. Roschke et al. [4] proposed an extensible IDS management architecture based on a new design of event gatherer component. By using the known IDS standard IDMEF and a plug-in concept, the Event gatherer ensures flexibility and compatibility. Silva et al. [5] presented a model, an architecture and an implementation of a Remote IDS (Intrusion Detection System) using the technology of Multi-agent Systems, Web Services and MDA (Model-Driven Architecture). This model adapts and extends the NIDIA (Network Intrusion Detection System based on Intelligent Agents) to provide a remote IDS on the Internet. Naveed et al. [6] proposed a very basic way to prevent intrusions without any additional cost. Snort is a free open source IDS, which they have integrated with a Cisco router to prevent intrusions.

[1]Faculty of Management, JNU, Jodhpur, INDIA
[2]Department of Computer Sc. & Engg, GJUST, Hisar, INDIA
E-mail: [2]yogeshchaba@yahoo.com

2. Proposed Intrusion Detection System

The proposed IDS is mobile agent based distributive monitored cooperative and responsive intrusion detection system. The agent is a Host Based agent which detects misuse in node/traffic behavior. It works in real-time scenario i.e. it responses intrusion actively or immediately as intrusion is detected. It has a cooperative module, which takes information from neighbor nodes/agents about intrusion and also provides information about intrusion to neighbor nodes[7][8]. The mobile agents are distributed over some or all nodes in the network. It consists of two parts. First part is Monitoring phase and second is Response phase. The monitoring phase of the IDS agent design contains Data Collection Engine, Intrusion Detection Engine, Intrusion

Analysis Engine and the response phase contains Prevention Module, Cooperation Module and Communication Module.

Implementation of Proposed IDS

The implementation of proposed intrusion detection system is done using Qualnet/Glomosim. Intrusion detection system is implemented and compiled using PARSEC complier ('C/C++' type) languages, which uses the base code of routing protocol / data transmission strategy. The modules of routing protocols are identified for traffic analysis in data collection engine and then the intrusion detection engine, intrusion analysis engine and prevention module are implemented. It also contains various modules for routing, cooperation and communication. The simulation environment used is based on Qualnet/Glomosim, a n/w simulator that provides support for simulating multi-hop wireless networks.The i/p parameters for an experimental setup are shown in Table 1.

Table 1
General Experimental Setup Parameters

Parameter	Value	Description
Number of Nodes	50-100	Network Nodes
Terrain range	(1000,1000)	X, Y Dimension of Area in meters
Bandwidth	2Mbps	Node's Bandwidth
Simulation Time	1-10 Minutes	Simulation Duration
Node-placement	Uniform/Random	Node placement policy

Implementation of Intrusion Types

In prevention module two techniques by Handle RREQ and Retry RREQ function (HRR) and Disable Broadcasting (DB) are implemented. Solution to prevent flooding intrusion type is by calling Handle RREQ and Retry RREQ functions. Flooding intrusion occurs because of initiating various RREQs on a particular node. Because of various RREQs that node is unable to handle more RREQ becomes malicious node. When this node comes in the path, other nodes do not forward packets and busy in handling RREQ. In order to prevent network from this attack, it can call these functions i.e. Handle RREQ and Retry RREQ. Handle RREQ function helps in handling various RREQ which comes on a particular node and mitigate flood attack. In the disabling broadcasts technique, a broadcast is a data packet that is destined for multiple hosts. Broadcasts can occur at the data link layer and the network layer. Network layer broadcasts are sent to all hosts attached to a particular logical network. The broadcasts are recognized by all hosts, a significant goal of router configuration is to control unnecessary proliferation of broadcast packets which cause the flood on the victim node. By disabling broadcasts, host node can no longer be used as amplifiers in flooding intrusion type. However, to defend against this intrusion, all neighboring networks need to disable broadcasts. Code for implementing these types of intrusions is as given below: This code shows that every fifth node send/initiate the route request to all destination nodes.

```
if((((node->nodeAddr)%5)==0)&&(node->nodeAddr<= 100))
{RoutingAodvInitiateRREQ(node, destAddr);}
```

To overcome the effect of these intrusions on the performance of the network the prevention module activates the prevention mechanism according to the intrusion type. The prevention mechanism for few intrusion types is discussed here. Preventing module prevents flooding intrusion type is by disabling broadcast. The broadcast is used in AODV routing Protocols to broadcast RREQ packets on all the nodes in the network. Flood intrusion occurs because of initiating lots of RREQ packets in the network so that network becomes congested and no bandwidth is available to send packets. Hence by disabling the broadcast all the RREQs which are broadcast to all nodes are disabled. These prevention mechanisms are to prevent flooding intrusion types similarly other intrusion types are also prevented with the help of prevention module.

3. RESULTS AND ANALYSIS

This section is focused on the experimental results to evaluate the performance of Intrusion Detection Systems. The performance is analyzed using packet delivery ratio, energy consumed and number of collisions:

Packet Delivery Ratio: Table 2 and Figure 1show the effect of proposed IDS with HRR and DB prevention techniques on PDR with different number of intruders. This figure shows that DB prevention technique mitigate the effect of flooding intrusion type with larger extent. By using DB technique average PDR increases up to 0.624 as compared to PDR 0.45 of HRR prevention technique, while PDR with flooding intrusion type is 0.208.

Table 2
Values Showing Effect of Proposed IDS on PDR Against Flooding Intrusion Type

	Packet Delivery Ratio (PDR)			
Number of Intruders	Without Intrusion	Flooding Intrusion Type	Hrr Based Preventionn Technique	DB Based Prevention Technique
2	0.914	0.302	0.534	0.72
4	0.914	0.3	0.503	0.671
6	0.914	0.212	0.443	0.626
8	0.914	0.19	0.432	0.587
10	0.914	0.143	0.401	0.572
12	0.914	0.11	0.388	0.567

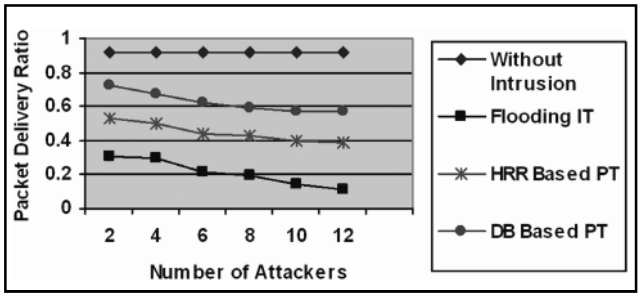

Fig. 1: Effect of Proposed IDS on PDR Against Flooding Intrusion Type.

Number of Collisions: Table 3 and Figure 2 shows the effect of proposed IDS with these prevention techniques on number of collisions with different number of intrusions and it also shows comparison of the prevention techniques. This figure shows that DB prevention technique mitigate the effect of flooding intrusion type with larger extent. By using this technique, average numbers of collisions decreases up to 4322 as compared to the collisions 7344 incase of HRR prevention technique and 8933 for flooding intrusion type.

Table 3
Values Showing Effect of Proposed IDS on Collisions Against Flooding Intrusion Type

		Number of Collisions		
Number of Intruders	Without Intrusion	Flooding Intrusion Type	HRR Prevention Technique	DB Prevention Technique
2	27	8753	7134	4059
4	27	8715	7174	4167
6	27	8912	7315	4258
8	27	9017	7413	4381
10	27	9076	7496	4504
12	27	9123	7532	4565

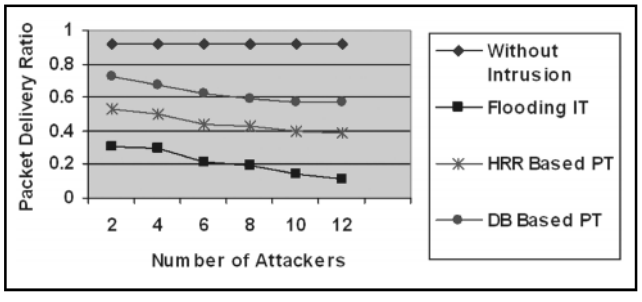

Fig. 2: Effect of Proposed IDS on Number of Collisions Against Flooding Intrusion Type

Energy Consumptions: Table 4 and Figure 3 shows the effect of proposed IDS with these prevention techniques on energy consumption with different number of intruders and it also shows comparison of HRR and DB prevention techniques. This Figure shows that DB prevention technique mitigate the effect of flooding intrusion type with larger extent. The average energy consumption for flooding intrusion type; HRR and DB prevention technique are 225.852, 225.745 and 225.785mWhr respectively.

Table 4
Values Showing Effect of Proposed IDS on Energy Consumption Against Flooding Intrusion Type

	Energy Consumption (MWHR)			
Number of Intrusions	Without Intrusion	Flooding Intrusion Type	HRR Preventionn Technique	DB Prevention Technique
2	225.05	225.718	225.752	225.680
4	225.05	225.701	225.723	225.709
6	225.05	225.910	225.718	225.746
8	225.05	225.925	225.718	225.979
10	225.05	225.922	225.747	225.793
12	225.05	225.935	225.812	225.805

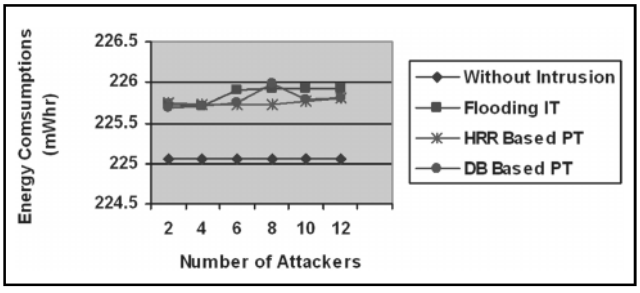

Fig. 3: Effect of Proposed IDS on Energy Consumption Against Flooding Intrusion Type

The proposed IDS architecture provides better network performance at marginal cost of overheads. The proposed system has better PDR, lesser energy consumption and lower number of collisions, scalable, interoperable with other IDS, and is able to detect new attack patterns with higher efficiency.

4. CONCLUSION

In this research work a new distributed intrusion detection system is proposed which is based upon concept of mobile agent running over the nodes. In this research work two parts of IDS are proposed i.e. the detection engine and prevention module. The detection engine is implemented for flooding type intrusions. The prevention module then prevents these intrusion types with prevention technique. The simulation experiments have been conducted to prove the efficiency of proposed IDS system. Proposed IDS is implemented as embedded AODV routing protocol / data transmission strategy and then it is compared with AODV routing protocol / data transmission strategy for PDR, energy consumption and collisions. The proposed IDS

architecture provides better network performance at marginal cost of overheads. The proposed system has better PDR, lesser energy consumption and lower number of collisions, scalable, interoperable with other IDS, and is able to detect new attack patterns with higher efficiency.

REFERENCES

[1] Bace and Rebecca, "An Introduction to Intrusion Detection and Assessment: System and Network Security Management", ICSA White paper, 2, No. 9, 1998.

[2] Chris H, "Detecting Attacks on Network", McGraw Hill, 1997.

[3] Zaman S, Karray F, "Lightweight IDS Based on Features Selection and IDS Classification Scheme", Proc. International Conference Computational Science and Engineering CSE, '09, 3, pp. 365-369, 2009

[4] Roschke S, Feng Cheng, Meinel C, "An Extensible and Virtualization-Compatible IDS Management Architecture", Proc. 5th International Conference on Information Assurance and Security, 2, pp. 130-134, 2009.

[5] Silva M, Lopes D, Abdelouahab Z, "A Remote IDS Based on Multi-Agent Systems, Web Services and MDA", Proc International Conference Software Engineering Advances, pp. 64-67, 2006.

[6] Naveed M, Nihar S, Inayatullah Babar, "Network Intrusion Prevention by Configuring ACLs on the Routers, Based on Snort IDS Alerts", Proc 6th International Conference Emerging Technologies (ICET), pp. 234 – 239, 2010.

[7] Garuba M, Liu C and Fraites D, "Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems", Proc IEEE 5th International Conference on Information Technology, IEEE Computer Society, pp 794-798, 2008.

[8] Hart R, Morgan D and Tran H, "Introduction to Automated Intrusion Detection Approaches", Journal of Information Management and Computer Security, pp 76-82, 1999.

[9] Paul I and Oba M, "An introduction to Intrusion Detection System", John Wiley & Sons, 2001.

[10] Sans, "Intrusion Detection and Vulnerability Testing Tools: 101 Security Solution", E-Alert News letters, 2001.

[11] Tony B, "Introduction to Intrusion Detection Systems:", [Online] www.aboutids.com, 2001.