Volume 2, Issue 2, February 2012 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Artificial Intelligence Approach towards Intrusion Detection in Soft Systems

Vishal Sharma
Student, B.Tech.
Department of Computer Science & Engineering,
Amritsar College of Engineering & Technology,
Punjab Technical University, Jalandhar, India.

Takshi Gupta
Student, B.Tech.
Department of Computer Science & Engineering,
Amritsar College of Engineering & Technology,
Punjab Technical University, Jalandhar, India.

Abstract-- **Soft Systems is the terminology given to those systems that have a software base at its working side as a primary or secondary support. These systems may include Wireless system such as cellular networks, ad hoc networks or any other software that may be dealing with encrypted information which is meant for particular receiver. These systems are very delicate in terms of working in harsh conditions and one of the major threats to this system is that of Intrusions. Broadly speaking intrusion can b of two types one that intentionally attacks the system and other that might be a bug that is generated because of human error while deploying. We are dealing with black holes and have proposed a model which is equipped with all necessary requirements that can avoid such intrusions in any type of environment. We have divided our strategy in two formats one for Wireless network and other for the client -server applications. For Network based analysis we have used NS-2 simulator and for client–server system we have developed our own software that justifies its use as an intrusion detection system.**

***Keywords*--- Artificial Intelligence, Intrusion, Ad hoc Networks, Client – Server Model, black holes.**

I. INTRODUCTION

The soft systems are dedicated system that always has a threat of being interrupted by some unwanted routines that affect the working of such system either by shut down of the system or gathering the information that is not actually meant for it. But when these threats are in form of leakage of information this is termed as intrusion. The type of intrusion dealt in this paper is Black Holes. Black holes are those nodes in the network that affect the working by interrupting the actual transmission by capturing the data. These black holes are nothing but a routine code that attacks the loop holes in the programming carried while deploying a particular system. We have been working on black holes and have realized that these can be broadly classified into two categories in the field of networking. One is the Wireless system that includes cellular network and ad hoc networks and other is the Client-Server Applications. Both the systems have independent working environment and thus, both of them should be studied differently and separate approaches are to be applied for intrusion detection and their eradication from the system. We shall be dealing with the both systems separately and have approached in solving the black holes with improved efficiency of system. In case of communication system, we have carried out our analysis on AD hoc networks. Ad Hoc Networks are networks capable of communicating in a set of small, low cost, low power sensing devices. A wireless sensor networks is totally based on the limiting factor i.e. energy consumption. A wireless sensor network consists of large number of sensor nodes distributed or scattered in particular network region. Ad Hoc Networks consist of node that is highly mobile, so in particular the range of the nodes is very important. Each device in an Ad Hoc Networks are free to move independently in any direction, and will therefore change its links to other devices frequently. The energy and the bandwidth of such path are of major concern. The lifetime of the network depends upon these parameters. But these parameters are adversely affected by intrusions. These types of systems can be corrected by use of artificial intelligence at the decision making nodes or points where these systems check for any unwanted node making loop interaction to get into the working of the system. We have proposed two models in this paper, one which operates for ad hoc network and other which operates in client server environment.

II. INTRUSION DETECTION IN AD HOC NETWORK

Ad Hoc Network are the low cost based wireless networks that have ability to show mobility in terms of locations and also dynamic path selection on basis of reactive or proactive routing protocols. The choice of protocol depends upon the deploying conditions of node or the path selection for communication. The protocol on which we have applied our technique is the AODV routing protocol. AODV protocol works on basis of RREQs and RREPs that work and maintain table during transmission on basis of acknowledgement sent to it by receiving node in form of Hello Messages. But what if, the message in forms of packets that is being transmitted from sender towards the destination is caught by some unwanted node; this will lead to adverse effects on the system in form of dead network, delays, fault transmission, wastage of transmission energy. Thus, this will ultimately affect the life time of the network structure which is determined as Θ (1/n log n) $^{1/2}$. The intrusion can be explained with the help of following figure.

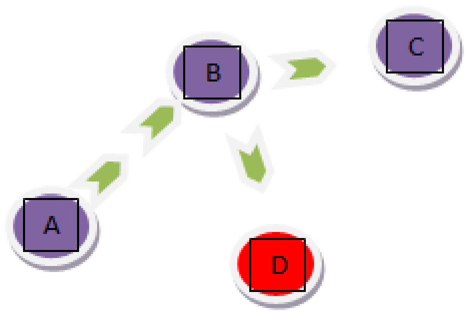


Fig. 1 Intrusion Attacked Network

The fig. 1 shows that the node A-C is communicating via node B. But a node D which is not authorized to get the data from node B attacks it and starts another set of communicating network thus causing delays and fault receiving of packets at node C. This can be corrected by implementation of artificial intelligence technique.

A. Artificial intelligence in intrusion detection and correction

The artificial intelligence is based on some knowledge that has been already derived to operate. In case of ad hoc networks, this can be gathered from the path selection during route discovery performed during the analysis of the network before transmission. We have developed an algorithm that can be incorporated at every node of the network structure. The system check for table and provides each node selected for relaying a sequence number which is the direction sorter for each packet heading towards another destination. The sequence number is already present in AODV protocol. We fetched this component in NS-2 simulator and incorporated it with our algorithm as a basic component and then we coded for selection of relaying node on basis of sequence number provided to every node during the route discovery. Also, this sequence number is generated on time of routing and selection of next relaying node, thus these can't be affected by intruders. But, then one important factor came that what if a intruder node generates the hello message containing a sequence number similar to relaying node. This caused us the serious issue. For this, we opted for a technique which we termed as TELL YOUR SOURCE. This technique asks for source that generated a sequence number for the node to operate in a particular network. This solved the problem of fake sequence numbers. On application of this algorithm in path selection and communication, decreased the delays and increased the fault tolerance to good extent. The pseudo code for the algorithm is shown below:

```
While (route_discovery)
{
Select node
Fetch sequence Number
}
On_transmission (node, relaying node)
{
Check Sequence number.
If (sequence number==found && Source==found)
{
 Node=authorized
Start transmission
On_transmission (node, relaying node)
Exit(0)
}
Else
```

© 2012, IJARCSSE All Rights Reserved

```
{
Route_discovery()
If( Route_discovery !=true)
{
Stop transmission
}
}
Exit(0)
}
```

The various calculations that were performed during the judgement of performance of the network structure are as follows:

Transmission delays = *time of path halt * number of nodes*

***Intrusion rate= β * delays* *transmission delays**

Where ***delays=1/ (link speed) ((Np-N*** $_t$***))N+(N-1)D*** $_I$**.**

Where N is the number of nodes and the N_t is the number of retransmissions, Np is the packet size and D_I is the average delay that is measured taking into account the ideal conditions for transmissions and its value is computed to be 6 ms.

B. Client-server intrusion detection and correction

The Client Server model is the type of system that has a centralized node that act as a server and the other nodes linked to it are the clients. These clients communicate via server; no direct communication between the two clients is available at any time. Thus, all the information has to be passed through the server and must be tested at the server as any part of information passed on by one of the client may be a threat towards the whole network of clients that are communicating via this server. Thus, we developed a system that works at server side. This is advanced application software that can be attached to the server that tests and checks for intruders and removes this information if it is harmful for the network structure. This system works on knowledge base that is the based upon the data fed to it by the server database and list of clients or the authorized list of clients provide by database of various Network service Providers. The working of the software is explained in following steps:

1. Ask for identification from Client.
2. If identification provided, check for server side database for client information.
3. Now check for network service provider for the client information provided.
4. If the information is found, establish connection for transmission.
5. Now the software developed by us will act as gateway towards the information passage between the client and server.
6. Software (IDS- Intrusion Detection System) checks for any coded material in the packet. If it founds so, it is transferred to separate machine where it is debugged for output. If found any harmful effect, client is warned and suspended.

However, these steps described are complex and have complex coding, yet the performance of the system is not harmed in terms of delays as it takes few milliseconds to check the information passed. But the after effect of this little delay is the correct and intruder free environment for transmission.

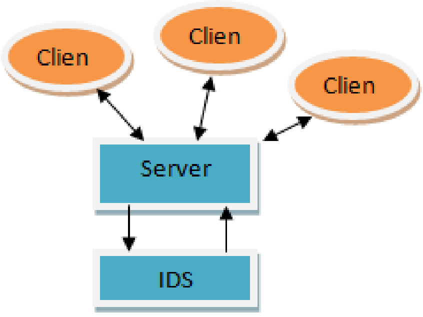


Fig. 2 Client-Server Model

III. SIMULATION ANALYSIS AND RESULTS

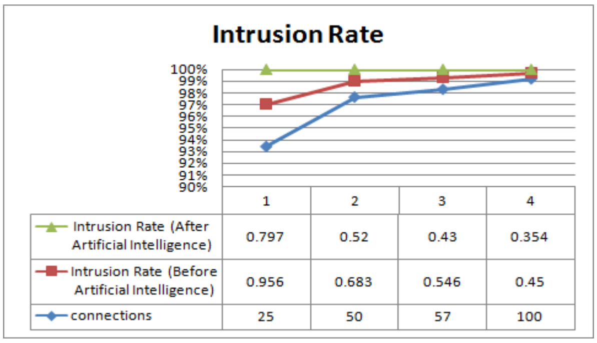
A. Performance Metrics:

For the simulation to be performed using NS-2 simulator, we have considered the following scenarios.

TABLE 1
PARAMETERS VALUES

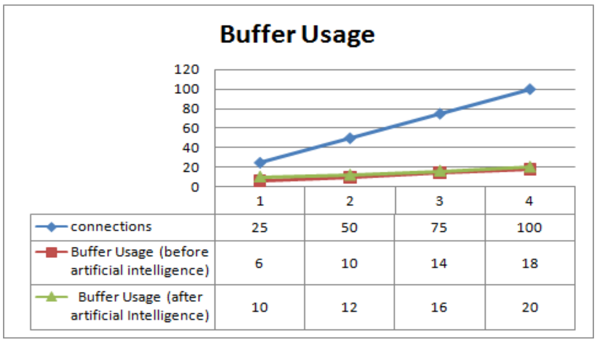
Parameter	**Value**
Dimensions	1500X1500 sq. m.
Number of Nodes	25, 50, 70, 100
Simulation Time	200 s
Source Type	CBR
Number of Connections	10
Packet Size	512 bytes
Mac Layer	IEEE 802.11 b
Buffer Size	200 packets
Propagation Radio Model	Two Ray Ground
Physique layer	Band width as 2 Mb/s
Maximal Speed	30 m/s
Pause Time	10 s
Interval Time To send	2 packets /s

© 2012, IJARCSSE All Rights Reserved



Graph 1

Graph 1 shows the intrusion rate variation before application of artificial intelligence technique and after application of intrusion detection technique. The graph shows the improvement by 21 percent approx.



Graph 2

Graph 2 shows the variation in buffer usage before artificial intelligence and after artificial intelligence technique. The graph shows improvement by 10 percent approx.

IV. CONCLUSION

The artificial intelligence is an important technique that can resolve complex situation problems such as intrusion detection. The intrusion can be resolved by various other means such as bug tracers but these techniques also increases the cost factor. The technique developed by is easy to incorporate and use and is also economical in terms of practical deployment. The results stated by us shows that the system shows an overall improvement by 15 percent approx. whereas the number of intruders is decreased to great extent. In future, the work can be carried out by interfacing the technique with the software defined radio where it will further decrease the number of intrusion attacks and also the delays by increasing the fault tolerance of the system.

REFERENCES

[1] Hsien-tang Wu; Wen-ta Hsiao; Chih-tsang Lin; Tao-ming Cheng; Dept. of Constr. Eng., Chaoyang Univ. of Technol., Taichung, Taiwan, “Application of genetic algorithim to the development of artificial intelligence module system”, Intelligent Control and Information Processing (ICICIP), 2011, 978-1-4577-0813-8

[2] Dr. R.K. Singh, Vishal Sharma:”Dead State Recovery Based Power Optimization Routing Protocol for MANETs”, HPAGC-2011, CCIS 169, pp.424-429,2011. © Springer-Verlag Berlin Heidelberg-2011.

[3] Sunil Taneja and Ashwani Kush:” A Survey of Routing Protocols in Mobile Ad Hoc abstract”. International Journal of Innovation, Management and Technology, Vol. 1, No. 3, August 2010.

[4] Qiang Liu; LixinDiao ; GuangcanTu; Art Acad., China Three Gorges Univ., Yichang, China, “The Application of Artificial Intelligence in Mobile Learning”, System Science, Engineering Design and Manufacturing Informatization (ICSEM), 2010 978-1-4244-8664-9

[5] M.Saravana karthikeyan, M.Murali, Dr.S.Sujatha:“Identifying performance metrics to maximize Manet’s throughput”; 2010 International Conference on Advances in Computer Engineering.

[6] Singh, V.K.; Gupta, A.K.; Dept. of Comput. Sci., Banaras Hindu Univ., Varanasi, India “From artificial to collective intelligence: prespectives and Implications”, Applied Computational Intelligence and informatics, 2009. Saci 09. 978-1-4244-4477

[7] Brunette, E.S.; Flemmer, R.C.; Flemmer, C.L.; Sch of Eng. & Adv. Technol., Massey Univ., Palmerston.” A review of artificial Intelligence” ,SAutonomous Robots and Agents ,2009. ICARA 2009 978-1-4244-2712-3

[8] Manika Vinay Rali, Min Song, Sachin Shetty:”Virtual wired transmission scheme using directional antennas to improve energy efficiency in Wireless Mobile Ad Hoc Network”; 978-1-4244-2677-5, IEEE 2008.

[9] Saeed, N.H.; Abbod, M.F.; Al-Raweshidy, H.S.; Brunel Univ.,Uxbridge, “ Intelligent MANET Routing System ” , Advances Information Networking and Applications-Workshops, 2008.,978-0-7695-3096-3.

[10] http://www. csi.uoregon.edu.

[11] Sehoon Kim, Jinkyu Lee and Ikjun Yeom,” Modeling and Performance Analysis of Address Allocation Schemes for Wireless sensor networks”, IEEE transactions on vehicular technology, vol. 57, NO. 1, JANUARY 2008.

[12] Rekha Patil, Dr. A. Damodaram:”cost basedd power aware cross layer routing protocol for Manet”; 2008 IJCSNS.

[13] Changchun Bae and Wayne E. Stark:”A Tradeoff between Energy and Bandwidth Efficiency in Wireless Networks”; 2007 IEEE.

[14] V. Rodoplu and T. H. Meng: “Bits-per-Joule capacity of energy-limited wireless networks,” IEEE Transaction Wireless Communications, vol.6(3), pp.857-865, March 2007.

[15] B. Rankov and A. Wittneben: “Spectral efficient protocols for half-duplex fading relay channels,” IEEE Journal on Selected Areas in Communications, vol. 25, pp.379-389: Feb. 2007.

[16] Network simulator-2 www.isi.edu/nanam/ns/.