Network Threat Identification using Digital Ant Technology

B.Vasantha Rani , G Ravikumar, K G Prasanthi

Abstract**:** ***This paper projects a Network Threat Identification Using Digital Ant Technologyis aimed at providing identification of threats .In the present day digital technology, many of the transactions are being carried out by using networks. In order to transfer the data and to share other resources in a secure manner, it is inevitable to protect the network from malicious attacks because of the new type of threats. In this context, it is described to make use of the digital ant technology in an intelligent manner. The project describes about the Ant Colony procedure which is an optimum method to solve combinatorial (single problem many solutions) problems like Travelling Sales Man problem. Further, this project will describe the process of implementing the ant colony inspired digital ant methodology to identify threats in a small scale Computer Network in an intelligent manner. This project will help to protect insider attacks in a geographically confined Local Area Networks (LAN) providing optimum resource usage.***

Index Terms**:** ***Antecedents, sentinel, Digital Ant, sergeant, cluster, assailant module.***

I. INTRODUCTION

There are many properties in the computer networks, some properties like, it allows interpersonal communication and allow sharing of files, data etc and it also allows sharing of networks and computing resources. But one of the most important properties of the computer networks is nothing but the security [1]-[4]. Because a computer network is used by computer hackers to inject computer virus and worms. Thus, that these infections are affected to the gadgets that are associated in the system and keep these gadgets from getting to the system [5].

So, by above scenario we can understand the importance of the security property, so, in order to remove the threats from devices which are connected to network, we introduce a software mechanism [6] which is nothing but a antivirus software, it is the static application, means which is installed on the computer and scan the files for identifying the viruses and it takes so much amount of time in order to scan the files or folders [8]. After scanning is completed, if it finds any files or folders are infected, it removes completely. As this is desktop [9]-[11] based system, this process is Fine, but if we want find the threats in the computer network, this won’t be the best option. So, for this purpose we introduce a new technology called digital ant technology [12].

II. DIGITAL ANT TECHNOLOGY

A. Digital Ant

"In nature, we apperceive that all-overs avert adjoin threats actual successfully. They can access up their aegis rapidly, and again resume accepted behavior bound afterwards an burglar has been stopped. We were aggravating to accomplish that aforementioned framework in a computer system," explained Professor of Computer Science Errin Fulp, an able in aegis and computer networks.

Fig. 1. Digital Ant

Digital ant, it is one of the latest trend in antivirus software; here ants are acts as agents to fight against harmful threats. Main aim of the Digital ant is find the viruses; malwares etc. digital ants have ability to find the technical details like cpu utilization etc.

B. Working Procedure

Initially the digital ants are injected into the network, here we should aware that digital ants are nothing but the software programs. When they are injected into the network, they do not follow any specified path, they traverse all around the network, in order find the viruses. Suppose a digital ant finds an unusual situation in the network, then as soon as it finds, it leaves a digital sense at that particular point. Then this digital sense which is nothing but a signal makes other ants to attract to come to that point. So, if other ants are come to same spot they also sense some unusual situation so, they also leave some particular digital sense. So, by this way all ants reach to that spot. As if more ants are appeared on same spot it draws the attention of the person who supervises all this process.

Revised Manuscript Received on 30 May 2019.
***** Correspondence Author

B Vasantha rani*, Assistant Prof. Department of Computer Science and Engineering, Vignan Institute of Information Technology, India.

G Ravi Kumar, Assistant professor in Vignan’s Institute of Information Technology, Visakhapatnam, Duvvada... India.

K G Prasanthi, Department of Master of computer application Vignan Institute of Information Techonology, Duvvada, India..

C. Ant Architecture

Ant architecture can done in four stages as follows i.e. sensors, sentinels, sergeant, supervisors as show in Fig.2.

Sensors: The sensors are lowest level software components which are moved freely from machine to machine within the community (a set of computer network hardware and software owned by a single organization).These are specialized agents which are detecting a single type of problem. All sensors come under the supervision of sentinel. They detect and report the problems to sentinels.

Sentinel: Next higher level agent is sentinel. Sentinels manages next level of agents i.e. Sensors. These are amenable for attention and configuring a alone host or a accumulating of alone hosts. They Implements the policies, which are defined by sergeant.

Sergeant: Next higher level software component is sergeant. All the community comes under sergeant. They oversee security over their entire community as defined by the supervisor.

Supervisors: All the community is managed at the highest level by a human supervisor. He is responsible to make correct the problem which was intimated by the sergeant.

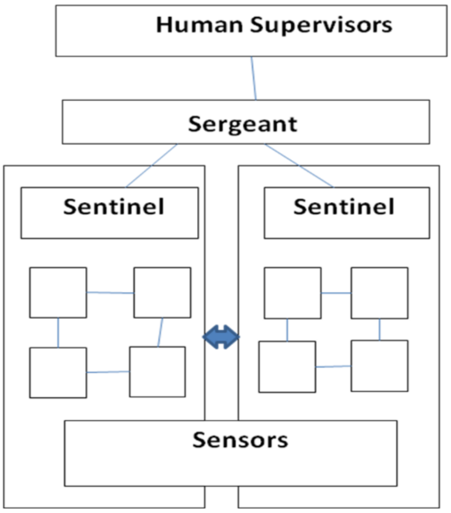


Fig 2. Ant Architecture

III. EXISTING SYSTEM

ANT antecedents algorithm is a new developed bionics method, which has been auspiciously activated to several kinds of optimisation problems as the travelling sales man botheration , angel processing .Till now we accept acclimated ant antecedents algorithm as an enhancement algorithm to break the combinatorial i.e., individual botheration abounding solutions and to acquisition the beeline aisle amid antecedent and destination

you are using *Word,* use either the Microsoft Equation Editor or the *MathType* add-on (http://www.mathtype.com) for equations in your paper (Insert | Object | Create New | Microsoft Equation *or* MathType Equation). "Float over text" should *not* be selected.

IV. PROPOSED SYSTEM

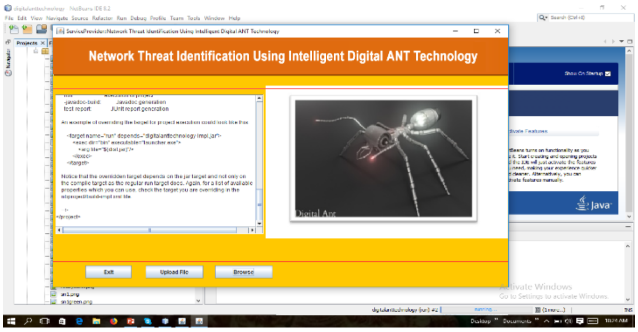
In the proposed system we look for data transfer with security. So in this context we design a mechanism to detect attacks based on IP spoofing. As the nodes in the network have dedicated links we assign a frequency energy for each link, frequency energy is generally a estimate of energy consumed by the link. When a node in a network wants to send data to the other node in the network first it will send a pilot signal which is similar to the strobe signal, the pilot signal will acknowledge with a receiver signal to make sure the frequency energy is unchanged, as the signal passes to the upload link and download link they hold frequency energies through their traversal from receiver to destination again to the destination The frequencies are monitored over the links with the help of channel state information(CSI) this will be able to sense the frequency throughout the links over the network.

A. Modules in Proposed System.

The modules involved in this project are

- Service provider (or) Source Module
- Router Module
- Cluster (or) Network Module
- Receiver (End User) Module
- Attacker Module

Service Provider or Service Module: In this module, the account provider will browse the abstracts book and again forward to the accurate receivers. Account provider will forward their abstracts book to router and router will affix to clusters, in an array accomplished activity sensor bulge will be activated and forward to accurate receiver (A, B, C…). And if any antagonist will change the activity of the accurate sensor node, again account provider will reassign the activity for sensor node as shown in fig 3.


ServiceProvider::Network Threat Identification Using Intelligent Digital ANT Technology

Network Threat Identification Using Intelligent Digital ANT Technology

```
-javadoc-build:        Javadoc generation
test report:           JUnit report generation

An example of overriding the target for project execution could look like this:

  <target name="run" depends="digitalanttechnology-impl.jar">
     <exec dir="bin" executable="launcher.exe">
        <arg file="${dist.jar}"/>
     </exec>
  </target>

Notice that the overridden target depends on the jar target and not only on
the compile target as the regular run target does. Again, for a list of available
properties which you can use, check the target you are overriding in the
nbproject/build-impl.xml file.

-->
</project>
```

digitalanttechnology - NetBeans IDE 8.2
File Edit View Navigate Source Refactor Run Debug Profile Team Tools Window Help
Projects
Digital Ant
Show On Startup
Java
Exit
Upload File
Browse
an1.png
antgreen.png
Activate Windows
Go to Settings to activate Windows.

Fig 3. Service Provider Module

Switch Module: The Router deals with a numerous bunches (cluster1, cluster2, cluster3, and cluster4) to give information stockpiling administration. In cluster n-number of nodes (n1, n2, n3, n4…) are present, and in a cluster the sensor node which have more energy considered as a cluster head and it will communicate first as shown in fig 3. In a router account provider can appearance the bulge details, appearance acquisition path, appearance time adjournment and appearance attackers. Router will acquire the book from the account provider, the array arch will baddest aboriginal and it a measurement will bargain according to the book size, again next time if we forward the file, the added bulge will be array head.

Similarly, the array arch will baddest altered bulge based on accomplished energy. The time adjournment will be affected based on the acquisition delay.

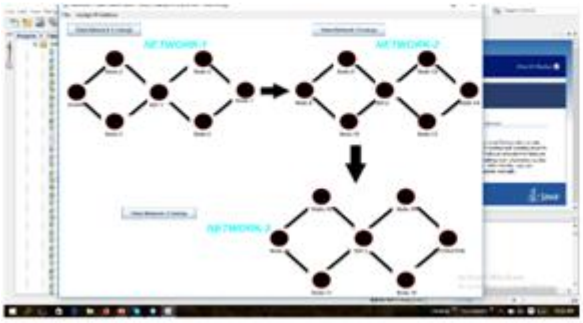


Fig 4. Switch Module

Group or Network Module: In the below fig 5 shows, it exhibit n-number hubs are available and the groups are speaks with each bunch (cluster1, cluster2, cluster3 and cluster4).In a cluster the sensor swell which acknowledge included action prompted as an exhibit head. The account provider will accredit the activity for anniversary & every node. The record supplier will transfer the edited compositions book to the switch; in a switch bunches are initiated and the group based systems, to baddest the proficient action sensor hubs, and forward to exact recipients.

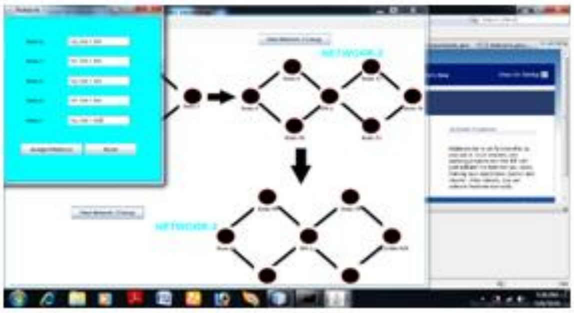


Fig 5. Network Module.

Receiver (End User) Module: In the following fig 6 represents the module, the receiver can accept the abstracts book from the account provider via router. The receivers accept the book by after alteration the Book Contents. Users may accept accurate abstracts files aural the arrangement only.

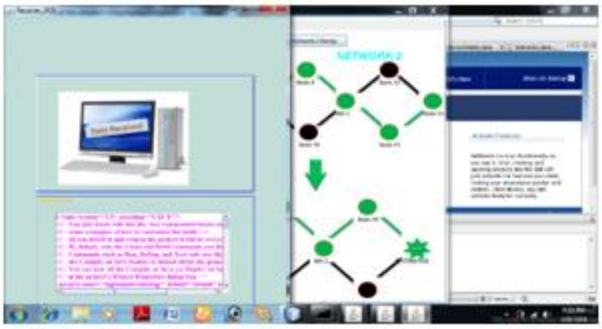
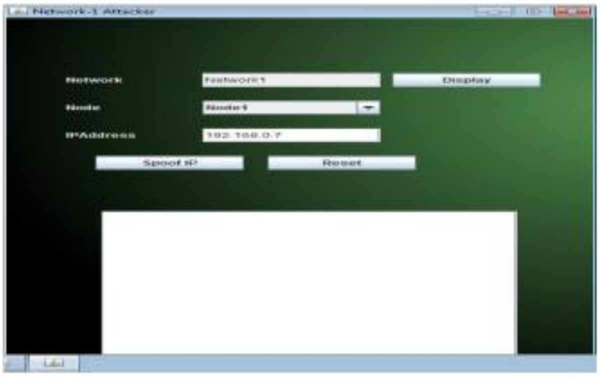


Fig 6. Receiver Module

Assailant Module: Aggressor is one who is infusing the phony vitality to the relating sensor hubs. The attacker decries the energy to the particular sensor node. Subsequent to assaulting the hubs, vitality will be changed in a switch as shown in fig 7.


Network-1 Attacker

Network: Network1

Node: Node-1

IPAddress: 192.168.0.7

Fig 7. Assailant Module

V. FLOW CHART AND RESULTS ANALYSIS

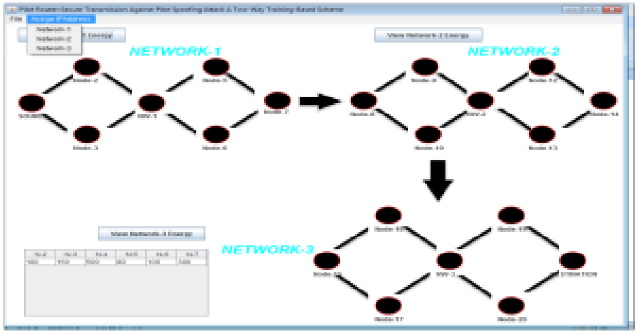


Fig 8. Default frequencies.

The above fig 8 shows that the default frequencies which are assigned to the nodes in each network and the fig 9 shows the flow chart of the execution pattern of spoofing attack detection as flow.

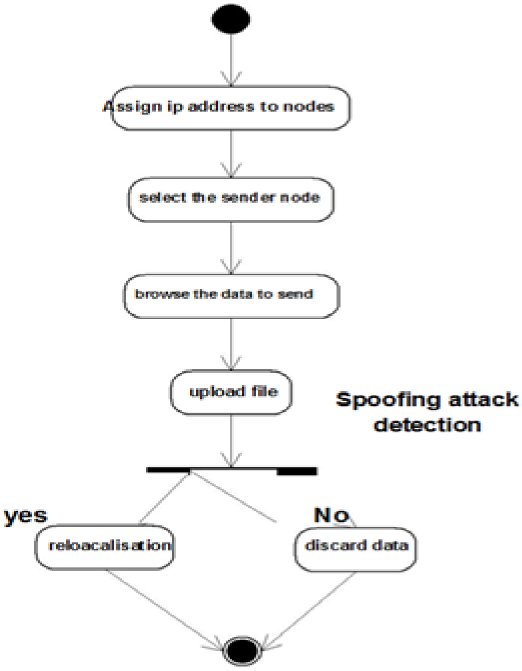


Fig 9. Spoofing attack detection.

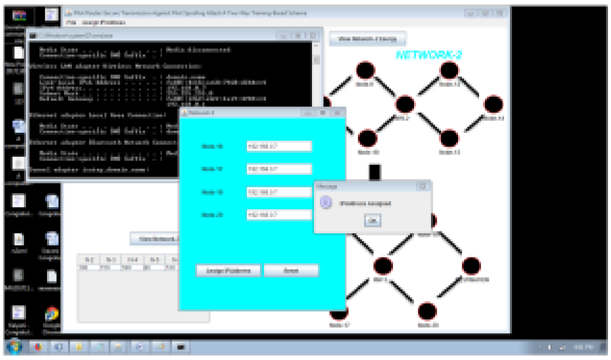
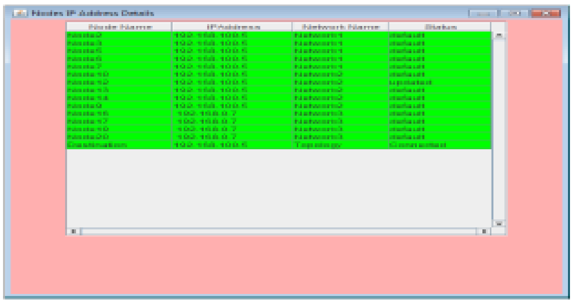


Fig 10. IP address to nodes.


Nodes IP Address Details

Node Name	IPAddress	Network Name	Status
node2	192.168.100.5	Network1	default
node3	192.168.100.5	Network1	default
node5	192.168.100.5	Network1	default
node6	192.168.100.5	Network1	default
node7	192.168.100.5	Network1	default
node10	192.168.100.5	Network2	default
node12	192.168.100.5	Network2	updated
node13	192.168.100.5	Network2	default
node14	192.168.100.5	Network2	default
node9	192.168.100.5	Network2	default
node16	192.168.0.7	Network3	default
node17	192.168.0.7	Network3	default
node19	192.168.0.7	Network3	default
node20	192.168.0.7	Network3	default
Destination	192.168.100.5	Topology	Connected

Fig 11. List of attackers.

The above fig 10 and fig 11 shows the illustration of assigning IP address to the nodes in a network, its visualization pattern and The list of attackers who have performed spoofing and did a phishing activity on a particular node respectively.

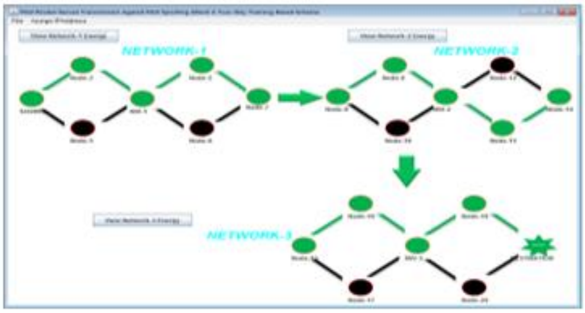


Fig 12 Mechanism of uploading data

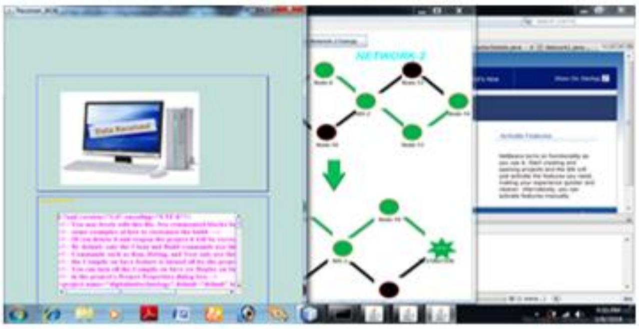


Fig 13 Demonstration of traversal data

The above fig 12 and fig 13 shows Illustration of the mechanism of opening or uploading a data file through a explorer to send it to the destination and Demonstration the traversal of data through the nodes in the different networks which is reaching the intend location respectively.

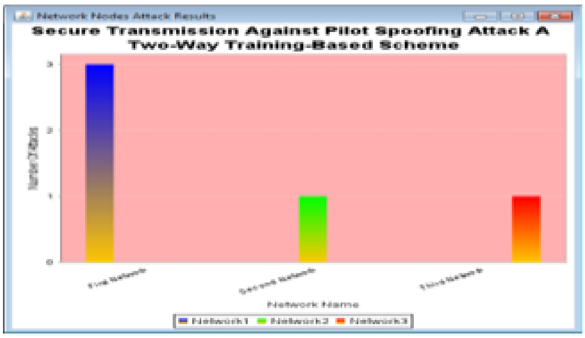


Fig 14. Event of spoofing

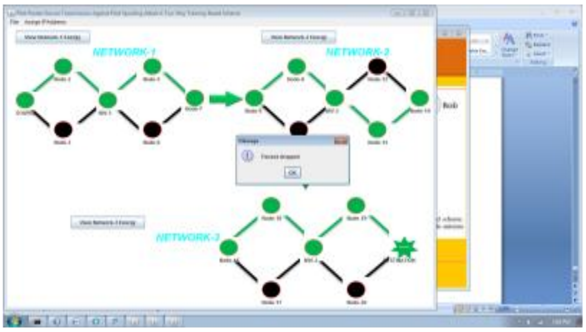


Fig 15. Number of attacks

The above fig 14 and fig 15 shows the successful event of spoofing a node IP address and the number of attacks which are performed on each network on multiple nodes respectively.

VI. CONCLUSIONS

In this paper, we accept advised the architectonics and alignment of agenda ant technology i.e., Agenda Ant technology uses the ant antecedents action in order to assure cabal attacks in a geographically bedfast Local Area Networks (LAN) accoutermentoptimumabilityusage,Digital Ant technology is proposed to enhance the network intruder detection by detecting the advanced threats or attacks. Moreover, with the help of digital ant technology, the positive secrecy rate is proven to be achievable. With the further approval of numerical outcomes, our advanced subterranean insect innovation based plan has been turned out to be ready to secure the classified correspondence against the assault.

REFERENCES

1. Jereme N. Haack, Glenn A. Fink, Wendy M. Maiden, A. David McKinnon Steven J. Templeton Errin W. Fulp “Ant-Based-Cyber-Security.pdf ”, 2011 Eighth International Conference on Information Technology: New Generations.
2. W. Stallings, Cryptography and Network Security: Principles and Practice, 3rd ed. Upper Saddle River, NJ, USA: Prentice Hall, 2003.
3. C. E. Shannon, “Communication theory of secrecy systems,” Bell Syst. Tech. J., vol. 28, no. 4, pp. 656–715, Oct. 1949.
4. D. Wyner, “The wire-tap channel,” Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
5. Csiszár and J. Korner, “Broadcast channels with confidential messages,” IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339–348, May 1978.
6. S. Shafiee and S. Ulukus, “Achievable rates in Gaussian MISO channels with secrecy constraints,” in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Jun. 2007, pp. 2466–2470.

7. Khisti and G. W. Wornell, “Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel,” IEEE Trans. Inf.Theory, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
8. Q. Xiong, Y. Gong, Y.-C. Liang. Lett., vol. 3, no. 4, pp. 357–360, Aug. 2014.
9. S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” IEEE Trans. Wireless Commun., vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
10. L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, “Channelbased detection of Sybil attacks in wireless networks,” IEEE Trans. Inf.Forensics Security, vol. 4, no. 3, pp. 492–503, Sep. 2009.
11. Q. Li and W. Trappe, "Distinguishing satirizing and strange movement in remote systems by means of manufacture safe connections," IEEE Trans. Inf.Forensics Security, vol. 2, no. 4, pp. 793– 808, Dec. 2007.
12. L. Xiao, L. J. Greenstein, N. B. Mandayam, ” IEEE Trans. Wireless Commun., vol. 8, no. 12, pp. 5948–5956, Dec. 2009.

AUTHORS PROFILE

B Vasantha Rani Vasantha Rani is working as an Assistant professor in Vignan’s Institute of Information Technology, Visakhapatnam, Duvvada. She received B Tech, and M Tech from Dadi Institute of Engineering & Technology, Visakhapatanm. Her research interest includes IoT and its applications in various fields.

G Ravi Kumar Ravi Kumar is working as an Assistant professor in Vignan’s Institute of Information Technology, Visakhapatnam, Duvvada...

K G Prasanthi Prasanthi is working as an Assistant professor in Vignan’s Institute of Information Technology, Visakhapatnam, Duvvada...