DIGITAL ANTS: SMART KILLING AGENTS

Meenal K. Bhalerao[1], Harshada P. Joshi[2], Dr.Bhatambarekar S.S[3], Mrs. Sonal Kulkarni[4]

Department of Computer Science,
Modern College of Arts, Science and Commerce, Ganeshkhind, Pune-16.
Savitribai Phule Pune University, Maharashtra, India
[1]meenal.bhalerao4101991@gmail.com [2]harshu.joshi23@gmail.com
[3]Shubhangi_sb@rediff.com [4]sonalrk7@yahoo.com

ABSTRACT- **In day-to-day life many technologies which are being used to protect our devices from many threats, malwares and worms. One of the protecting technologies is "Digital Ants". The aim of this research paper is to give about a small concept of Digital Ants and how it can be used not only for security but to stop the unwanted processes. In this system under Admin there are many Sergeants and under Sergeant there can be any no. of Sentinels.**

Ants are the agents made up of tiny codes with essential data capturing and executing capabilities, which check for a processes and leave footprints. This concept of digital ants comes under the Swarm Intelligence.

KEYWORDS - Admin, Agents, Digital Ants, Sentinel, Sergeant

I. INTRODUCTION

Digital ant concept is very much similar to real ants; ants are very fast and intelligent in their work. They all stay together in huge colonies and do their work with unity. There is a "Queen" which gives instruction to other worker ants to do work. If enemies come in their colonies, they all come together & kill it.

Similarly, the Digital ants find out the running unwanted processes, it detects the processes, and kill that running process and leaves footprints.

Fig 1.1: - Ant Colony [4]

The small concept of "Digital Ant" which we have implemented, in that there is an admin, sergeant and sentinel. When the admin send the ant to the sergeant it checks for the unwanted processes. Then sergeant sends the ants to sentinels, to kill the unwanted process. While this whole process is running simultaneously. It also creates records for activities which have been done to the unwanted processes.

II. LITERATURE REVIEW

- In many other Research papers the concept of "Digital Ants" is

used to detect the Malware or threats and send its notification to the user, so that user can find the place where the threats were exactly situated.

- Cyber Defense (ABCD) that can run on one or a few physical machines with sufficient resources. We have chosen to run the framework on hundreds of virtual machines whose number is limited only by the available memory and processing power. We collect the distributed logs and visualize the results on a large-scale visualization created to represent up to a million nodes [1].

- Digital ants are an application of Swarm intelligence or SI. Our idea is to deploy 3,000 different ants, each looking for evidence of a threat, Fulp said, "As they move about the network, they leave digital trails modeled after the scent trails ants in nature use to guide other ants. Each time a digital ant identifies some evidence, it is programmed to leave behind a stronger scent. Stronger scent trails attract more ants, producing the swarm that marks a potential computer infection." [2].

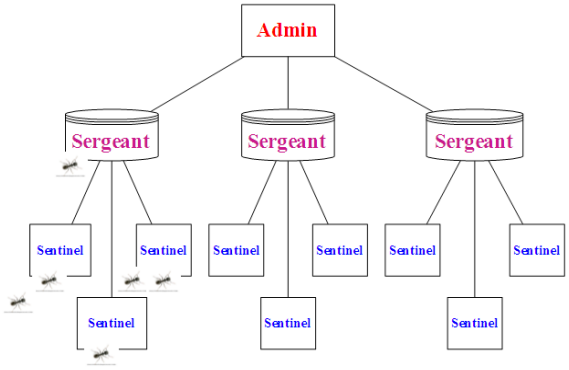
- Scientist has come up with a new way of defending network from worms and other malware that applies a phenomenon from nature to cyber attacks: The defensive behaviors of the tiny ants [3].

III. PROPOSED SYSTEM

Proposed system is a miniature system to represent how digital ant mechanism works in a LAN. Proposed system is capable of detecting unwanted processes on devices and taking action against it by sending ants. It can also take input from the admin to enter the unwanted process to be killed for effective utilization of the processing capacity. Our system has following functionalities.

Fig 3.1:-Work Flow of System

-



Functionalities

- Admin login
- Client list maintenance
- Sergeant and Sentinel declaration
- Constructing agent
- Network discovery
- Send ants
- Executing ant
- Report updating
- Report view

IV. OPERATION

Basic requirement for this system is that all the devices should be connected to each other through Local Area Network (LAN). If the devices are not in a LAN then there is no use of this system. As shown in figure 4.1, Admin logins to the system. Admin selects some devices as Sergeants and adds them with their IP addresses. As shown in figure 4.2, under these Sergeants there can be 'n' no. of Sentinels with their IP addresses. It's not necessary to have Sentinels under every Sergeant.

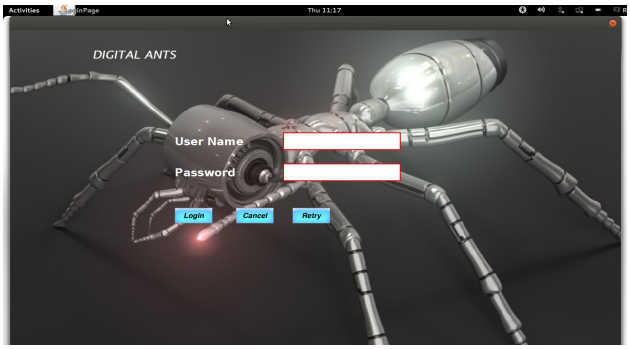


Fig 4.1:- Admin Login

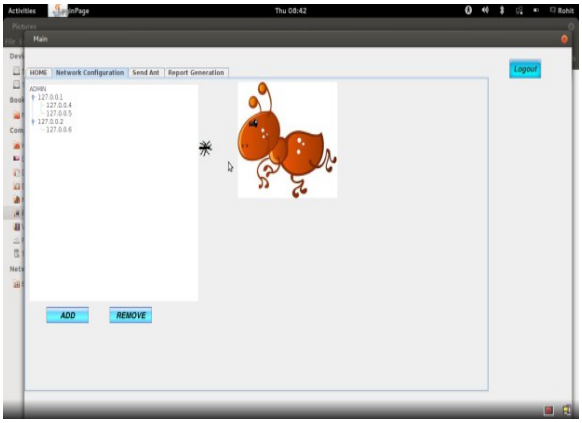


Fig 4.2:- Adding Sergeant and Sentinels

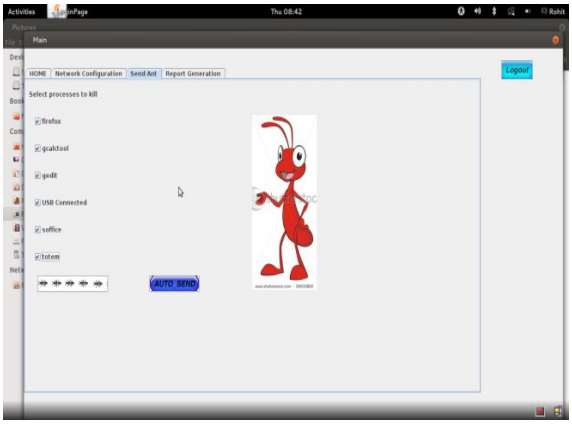


Fig 4.3:- Selection of processes

As shown in figure 4.3, Admin selects unwanted processes which are already listed in the system. If any process of Admin's choice needs to be killed and it is not in the list, Admin can add that process to the list. So further it can be killed. This adds an advantage that depending on the current traffic & priority Admin himself can make decisions run time, which processes to kill.

Admin sends ants to the Sergeants. On the Sergeant side, ant gets executed and searches for the unwanted processes which are selected by Admin. Simultaneously Sergeants forward these ants to their respective Sentinels for the same purpose.

If unwanted processes running on Sentinels, then ants kill those processes as shown in figure 4.4. This report is sent to their respective Sergeants. If this same case happens at Sergeant Side, then it sends the report along with their respective Sentinel's report to Admin.

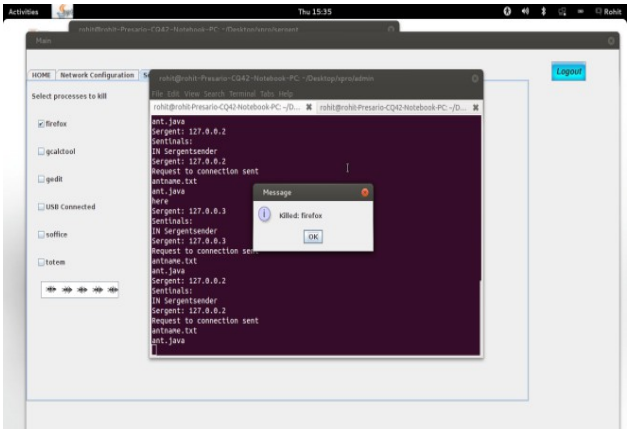


Fig 4.4:- Processes killed by ants

Periodic checking for searching unwanted processes, after the specific time period can be done and automatically ants can be sent to kill the processes.

As shown in fig.4.5, Admin can see report, sent by Sergeants and Sentinels. Report contains information after killing unwanted processes, like IP addresses of Sergeant & Sentinel, Time Stamp, and Status of process killed, etc.

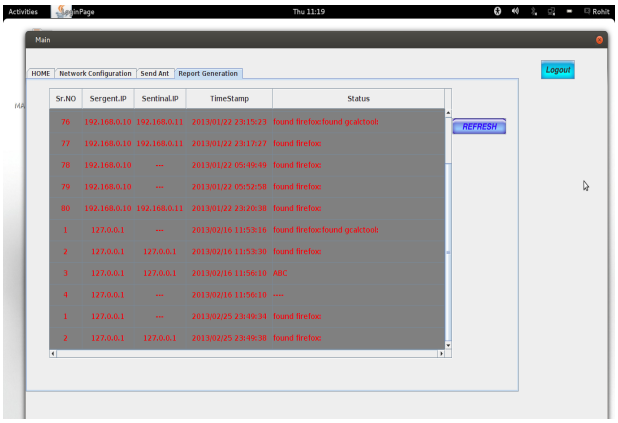


Fig 4.5:- Report generation

The similar concept of digital ants is used in real world. If the Mathematics exam is conducting in a lab, and we don't want calculator to be used by students while exam is going on. Then by selecting gcalctool it blocks or kills process if running.

V. TECHNOLOGIES USED

The Project is developed using the features of OOP's concepts, JAVA , and Swing .

Linux: it is open source, virus free operating system, widely used in IT sectors.

Java : Java is used for programming due to its features of simplicity.

Swing : It is a set of packages built on the top of AWT that provide with a great number of prebuilt classes . From programmers point of view UI Components are probably most interesting.

VI. ADVANTAGES OF THE DIGITAL ANTS

- Any no. of Sergeants and Sentinels can be added.
- Periodic checking for searching unwanted processes, after the specific time period.
- Any no. of processes can be added to the list for killing.
- Several no. processes can be killed at a time according to the selection.

VII. LIMITATION

- All the devices should be connected in a LAN.Without LAN this system cannot be worked.
- If network is disconnected system shows error dialogue box..

VIII. FUTURE ENHANCEMENT

- As this is just a small part of very big concept we have so much scope for improvement.
- Here we are adding IP addresses of the Sergeant and Sentinels. But as the devices in the LAN grow, Sergeant and Sentinels list can be automatically selected depending on some criteria.
- We can also provide such facility that if repeatedly a specific unwanted process is found on same machine we can deny its access.

IX. CONCLUSION

This system is very useful in big organizations like colleges, companies, etc. This system not only provide security but also kills unwanted or the processes which want to restrict by the end users.

X. ACKNOWLEDGMENT

This research paper is done for the completion of MSc computer science under the computer science department of Modern college Ganeshkhind, Pune and under Savitribai Phule Pune University.

XI. REFERENCES

[1]. Ants, To-Go: A Portable Demonstration of Large Infrastructure Cyber Defense- Glenn A. Fink, A. Keith Fligg, and Jereme N. Haack
Pacific Northwest National Laboratory Richland, WA 99352
Email:{Glenn.Fink/Keith/Jereme.Haack}@pnnl.gov

[2]…http://googleweblight.com/?lite_url=http://business.rediff.com/special/2009/sep/28/tech-digital-ants-to-the-rescue.htm&ei=XJcvLsca&lc=en-IN&s=1&m=336&ts=1445704606&sig=APONPFll3wLd8s9wr145qS5idKdfd_qngA

[3]…http://www.darkreading.com/attacks-breaches/nature-versus-hacker--digital-ants-swarm-malware-in-research-project/d/d-id/1132032

[4]...http://searches.vi-view.com/search/images?qsi=31&q=ants%20working&p=4&fcoid=4fcop=bottomnav&fpid=2