ISSN : 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 5, July 2012

A New Approach of Internet Firewalls based on Biological Computation

Adel Hassas[1], Farzane Kabudvand[2], Carlo Lucas[3]

Department of Computer, Zanjan Branch,Islamic Azad University,Zanjan,Iran[1,2,3]

adel_hassas@yahoo.com[1], fakabudvand@yahoo.com[2], lucas@ipm.ac.ir[3]

Abstract - ***The purpose of this paper is to find a new technique on issue of network security using Biological algorithm of bees and presenting new methods of establishing security in a network and reduce its amount of traffic by eliminating the presented disruptive packets. A sample of an application to this method is discussed in continue.***

Key words - biologic mechanism,network security , worker bees, firewall

I. INTRODUCTION

By increasing the usage of networks specially the internet demands of having security algorithms is being felt more and more, it may seem that security has been considered as a restraint technology and many tasks are done without security parameter and seem that are more complicated with security mechanisms but what is important is the fact that security of a technology is rehabilitation. only when a standard security system is available different services can be utilized and used.

As we know one of the new methods of solving problems and algorithms is to samplized biotic algorithms taking place in nature and by this means, different algorithms and problems can be solved by biologic mechanisms. Of these kinds of algorithms colonies of ants, natural choice in survival of giraffes and worker bees can be named which each one of these mechanisms can be used in different problems and solve problems in different way, an example for colonies of ants might be to find the shortest way for ants and etc. In this paper the purpose is to find a new method on the issue of security based on the behavior of worker bees in defense against invaders. In continue different application of this method in network systems will be discussed.

II. CLASSIFICATION OF SECURITY

Basically there are 3 different perimeters of security (figure 1).

- Hardware security is referring to physical security; this security class also includes un
- intentional signals such as electromagnetic waves broadcasted by CRT plates.
- Information security includes security of computer and communication. Security of computer discusses prevention and detection of illegal activities done by users to a computer system, security of communication includes some parameters and controlling acts in which remote access to information by users is prevented and accuracy of the communication is guaranteed.
- Administration or managerial security includes security of personals and operations.

In this paper the purpose is to study and present a new security mechanism in the course of information security. In subject of data packet security, different algorithms have been offered which have some advantages and disadvantages and mostly they try to establish balance among parameters such as run time of algorithms, level of security and the influence of algorithm on the network's traffic.
We see in bellow. Security classification:

A. Security

- Hardware Security
  - Physical security
  - Emanation Security
- Information security
  - Computer Security
  - Communication Security

ISSN : 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 5, July 2012

- Administration security
- Personal Security
- Operation Security

III. THE STUDY OF BIOLOGICAL BEHAVIOR OF WORKER BEES

With the studies done by biologists on behavior of worker bees, it was specified that bee show an interesting behavior in distinguishing invader bees or these with a certain illness.

In this defense mechanism the first bee who is noticed with the presence of the invader sends alerts to other worker bees who are the defenders of the hive and asks for help against the invader, because of the expanse of the hive and the low sight of the bees and their lack of control over the area of the hive this mechanism can be useful technique in distinguishing unison invaders.A honeybee colony typically consists of a single egg-laying long-lived queen, anywhere from zero to several thousand drones (depending on the season) and usually 10,000 to 60,000 workers [7]. Queens are specialized in egg laying [8]. A colony may contain one queen or more during its life-cycle, which are named monogynous and/or polygynous colonies, respectively. Only the queen bee is fed "royal jelly," which is a milky-white colored, jelly-like substance. "Nurse bees" secrete this nourishing food from their glands, and feed it to their queen. The diet of royal jelly makes the queen bee bigger than any other bee in the hive. There are usually several hundred drones that live with the queen and worker bees. Mother nature has given the drones just one task, which is to provide the queen with some sperm. After the mating process, the drones die.

IV . PRESENTED TECHNIQUE

As it was mentioned before, the purpose is to present a defense strategy against disruptive nodes in a network which has rised from behavior of bees, the presented strategy is as follow: imagine a network (internet for example)with different routers at different levels and with a hierarchy like a tree(figure 2)

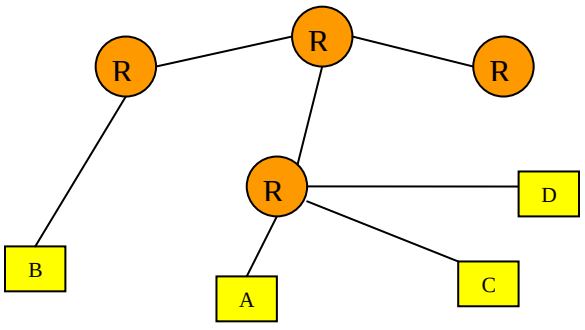

Figure 2 - Simple network with Routers and clients

Now suppose that client B wants to illegally gains access to client A, at the first sight the probability of this clients disrupcy is zero, immediately after receiving the first package by client A, by means of firewalls installed on the system, this client can distinguish that the package can be an intruder in this way that if the client just considers it's requests from different networks and if there is no such request from client B but has received a package from the client, there is a probability of an invader named B, therefore A blocks this package and will not allow it's access to higher levels of network in the system and also sends a message to it's up level router which ha received the package from, this message contains information indicating that the sent IP from B is an invader package, in case of receiving such message to router, router will sort this IP in a chart and will give a value to a field in front of it ,with every encounter of router with this message [5], the value of the IP field will be increased, in case that the value of the field becomes greater than a certain number, the router will block the package and will not allow the deliverance of the package to client A and also sends a message to it's up level router so this router can create a chart and the process can continue in a hierarchical way.

By repeating this process, in case client B continues it's interruption, the blocking level of packages sent by client B will be increased and might reach a level in which sending process be blocked at the very first step and results in reduction of network traffic.

The biological appearance of this method can be observed in behavior of worker bees against invaders in which the first bee tries to defend against the invader and in case of failing a message will be sent to other neighboring bees by it's feelers asking for help against the invader, so other bees will cooperate and help in defending the bee[4].

An other example of this problem can be observed in behavior of tele communication systems with annoyance, in this system by receiving the first complain from a user the complained number would be investigated an since the date of the complain the phone number of the annoyer would be noticed and in case of further annoyance the phone number of the annoyer will be blocked and no other annoyance would be possible by the user[5].

ISSN : 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 5, July 2012

V. SIMULATION OF THE ALGORITHM

In this section for demonstrating the efficiency of the algorithm a program has been designed in "C" language.
In this program which it's structure is like internet,1000 nodes are randomly considered as clients and proportionately some nodes have been considered as routers, by starting the simulation some nodes are settled to be clients some to be servers.
Clients start to request information from the server in random times and with adjustable distribution average, therefore an area like the internet would be created.

Considering that the routers have the responsibility of path finding in this system and follow some pre defined path finding algorithms, after a certain times of repetition of this process, a group of clients start sending un related packages to the network. In this case the suggested algorithm of this paper which has been simulated in the network will execute and as can be seen in (figure 3) after a short while the intruder client will be blocked and the network will stop further sending of these intruder nodes[6].

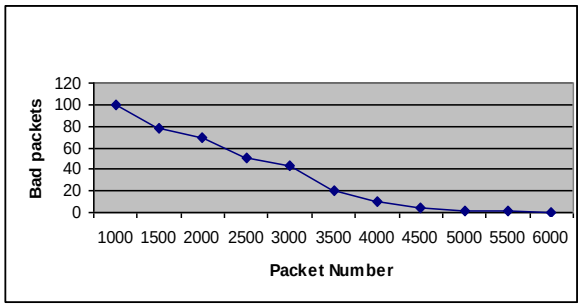

Figure 3 – number of detected bad packets

An other parameter which has been studied in this simulation is the number of clients involved in finding and detecting the information packages from the intruder. In this case, like the previous case, first the system starts producing random packages in which some packages are considered infected or invader packages, after a while some clients start distinguishing the invader and seek help from neighboring clients in identifying the invader.

In (figure 4) number of clients which are involved in the cooperation and succeeded in blocking an invader client is shown.

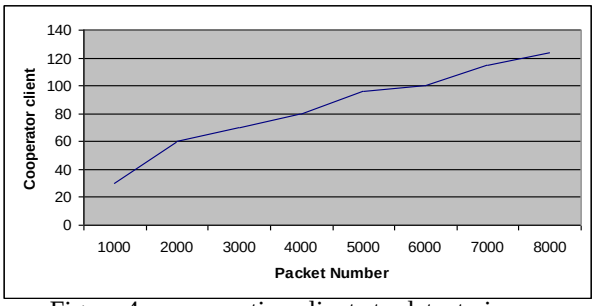

Figure 4 – cooperative clients to detect virus

VI. CONCLUSION AND FUTURE WORKS

Because of the importance of security in a network a strategy was suggested which the followings can be named from the advantages:

- reduction of network traffic by eliminating invader packages
- reduction of firewall tasks installed on each client
- appliance of limitations in activities if invader client

Presenting a technique in wireless network based on biotic algorithms on ODMRP protocol which is considered an important protocol in wireless network, is under study. Considering the mechanism presented in this paper, this can be applied on different levels of network.

REFERENCE

[1] R.E. Page, The evolution of multiple mating behavior by honey bee queens (Apis mellifera L.), J. Genet. 96 (1980) 263–273.

[2] How honeybee queen attendants become ordinary workers *Journal of Insect Physiology, Volume 27, Issue 8, 1981, Pages 515-519*

[3] H.H. Laidlaw, R.E. Page, Mating designs, in: T.E. Rinderer (Ed.), Bee Genetics and Breeding, Academic Press Inc., New York, NY, 1986, pp. 323–341.

[4] A survey of issues in computer network security *Computers & Security, Volume 5, Issue 4, December 1986,Pages 296-308* Linda S. Rutledge, Lance J. Hoffman

[5] R.F.A. Moritz, E.E. Southwick, Bees as Superorganisms, Springer, Berlin, Germany, 1992.

[6] Security in open networks and distributed systems *Computer Networks and ISDN Systems, Volume 22, Issue 5, 21 October1995, Pages 323-346* P. Janson, R. Molva

[7]:L. Adleman. Molecular computation of solutions to combinatorial problems. Science, 266:1021{1024, 1998.

ISSN : 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 5, July 2012

[8]:D. Roo and K. Wagner. On the power of bio-computers. Technical report, Universit at W urzburg, 2001.

[9] A.R. Simpson, H.R. Maier, W.K. Foong, K.Y. Phang, H.Y. Seah, C.L. Tan, Selection of parameters for ant colony optimization applied to the optimal design of water distribution systems, in: Proceeding of International Congress on Modeling and Simulation, Canberra, Australia, 2001, pp. 1931–1936.

[10] H.H. Laidlaw, R.E. Page, Mating designs, in: T.E. Rinderer (Ed.), Bee Genetics and Breeding, Academic.