International Journal of Computer Science and Security (IJCSS)

ISSN : 1985-1553

VOLUME 1, ISSUE 3

PUBLICATION FREQUENCY: 6 ISSUES PER YEAR

Editor in Chief Dr. Haralambos Mouratidis

International Journal of Computer Science and Security (IJCSS)

Book: 2007 Volume 1, Issue 3
Publishing Date: 31-10-2007
Proceedings
ISSN (Online): 1985-1553

IJCSS Journal is a part of CSC Publishers
http://www.cscjournals.org

Published in Malaysia

Typesetting: Camera-ready by author, data conversation by CSC Publishing Services – CSC Journals, Malaysia

CSC Publishers

Table of Contents

Volume 1, Issue 3, September/October 2007.

Pages

Integrating – VPN and IDS – An approach to Networks Security

Yudhvir Singh, yudhvirsingh@rediffmail.com
Department of Computer Science and Engineering,
Guru Jambheshwar University of Science & Technology
Hisar –125001
Haryana, INDIA

Dr. Yogesh Chaba, yogeshchaba@yahoo.com
Department of Computer Science and Engineering,
Guru Jambheshwar University of Science & Technology
Hisar –125001
Haryana, INDIA

Prabha Rani, prabharani_ys@yahoo.co.in
Computer Science
Kurukshetra University, Kurukshetra
INDIA

Abstract

The Internet and recent global cyber terrorism have fundamentally changed the way organizations approach security. Recent worm and virus incidents such as Code Red, Nimda, and the Slammer worm have heightened security awareness. Also, numerous other threats have emerged recently that are particularly troublesome. Hence some solution must be provided to encounter the new generation of complex threats. Building up this solution requires the Integration of different security devices**.** Also system administrators, under the burden of rapidly increasing network activity, need the ability to rapidly understand what is happening on their networks. Hence Correlation of security events provide Security Engineers a better understanding of what is happening for enhanced security situational awareness. Visualization leverages human cognitive abilities and promotes quick mental connections between events that otherwise may be obscured in the volume of IDS alert messages. Keeping all these points in mind we have chosen to integrate VPN and IDS to provide an efficient solution for security engineers.

Keywords: Integrating security devices, IPSecVPN and Intrusion Detection Systems.

1. INTRODUCTION

To provide the end-to end security solution, we must keep in mind the security products chosen which can be integrated and provide a balance between the access and protection by performing the following functions:

- Access control, including identity services, authentication, authorization, accounting (AAA), access control
- Servers and certificate authorities
- Network and host-based intrusion detection and protection

- Centralized security (and policy) management
- Secure connectivity through encryption and VPNs.

Hence we have chosen the VPN and IDS to provide an in depth solution, because VPN and IDS guarantee the secure operations of the enterprise network access control to traffic, encryption / authentication to protect traffic from interception Modification/Fabrication and IDS must be placed at the edge of the enterprise network to discover attacks.

1.1 Virtual Private Networks

A virtual private network can establish secured virtual links among different organizations, such as branch offices. Tunneling by appending additional headers facilitates the virtual lease line while cryptographic technologies prevent private information passing through the public Internet from being intercepted, modified, or fabricated. However, when complex cryptographic algorithms are employed for encryption and decryption within VPN tunnels, it becomes the performance bottleneck. Hence, dedicated hardware has been proposed to maximize the throughput and minimize the latency. Modern VPN technologies include PPTP, L2TP, and IPSec PPTP and L2TP work at the data link layer and are suitable for secure remote access between mobile users and enterprises. In contrast, IPSec works at the network layer

1.2 IPSec VPN

IPSec provides secure tunnels among the subnets. The important features that IPSec provides are the encryption and authentication mechanisms for the IP protocol suite. IPSec can also be configured to provide data encryption, device authentication and credential, data integrity, address hiding, and security-association (SA) key aging.

1.4 IP Addressing [2]

Proper IP addressing is critical for a successful VPN as any large IP network. In order to maintain capability, performance, and manageability, it is highly recommended that remote sites use a subnet of the major network to allow for summarization. This way, the cryptographic ACLs will contain a single line for every local network, possibly a single entry if the local networks are themselves summarizable on all devices to classify traffic flows. IP addressing also affects many facets of VPNs including remote management connection of overlapping networks.

1.5 Network Address Translation

NAT can occur before and after IPSec. It is important to realize when NAT will occur since in some cases NAT may interfere with IPSec by blocking tunnel establishment or traffic flow through the tunnel.

1.6 NAT Before IPSec

When two sites are connected via IPSec if any of the network address ranges at each site overlap, the tunnel will not establish. This occurs because it is not possible for the VPN termination devices to determine the site to which to forward the packets. Utilizing NAT before IPSec overcomes this restriction by translating one set of the overlapping networks into a unique network address range that will not interfere with the IPSec tunnel establishment. This is the only scenario where the application of NAT is recommended.

1.7 NAT After IPSec

We may consider applying NAT after IPSec encryption for address hiding. However, this provides no benefit because the actual IP addresses of the devices utilizing the tunnel for transport are hidden via the encryption. Only the public IP addresses of the IPSec peers are visible, and address hiding of these addresses provides no real additional security. NAT application after IPSec encapsulation will occur in cases where IP address conservation is taking place.

1.8 Intrusion Detection Systems (IDS)

Many network intrusions cannot be identified until the traffic has been passively analyzed. For example, denial of service (DoS) attacks such as ICMP-flooding are difficult to recognize until

numerous ICMP packets have arrived within a small time interval; application-specific buffer-overflow attacks to obtain root privilege, such as subverting an FTP server by a long “MKDIR” command, may require buffering and reassembling several packets before seeing the whole FTP command. A network-based IDS can detect such attacks by matching a sub-string, for example, the “phf” in “ GET/cgi-bin/phf?,” to identify those network packets as vehicles of a web server attack. When such kinds of potential hostile activities are detected, IDS will alert system administrators and may block the activity. The above examples describe the basic functions of a network based IDS.

In fact, the IDS model can be host-based IDS (HIDS) or network-based IDS (NIDS). HIDS is installed at a host to periodically monitor specific system logs for patterns of intrusions. In contrast, an NIDS sniffs the traffic to analyze suspicious behaviors. A *signature-based* NIDS (SNIDS) examines the traffic for patterns of known intrusions. SNIDS can quickly and reliably diagnose the attacking techniques and security holes without generating an over-whelming number of false alarms because SNIDS relies on known signatures. However, *anomaly-based* NIDS (ANIDS) detects unusual behaviors based on statistical methods. ANIDS could detect symptoms of attacks without specific knowledge of details. However, if the training data of the normal traffic are inadequate, ANIDS may generate a large number of false alarms.

2. RELATED WORK

In this section we are presenting the wok that has been done up to now in the area of Integrity of various security tools and correlating the events from the integrated tools and at last how the visualization tools can help in providing the results that can be interpreted easily**.** YING-DAR LIN, HUAN-YUN WEI AND SHAO-TANG YU, [1] discusses how the integrated security gateway can be implemented using the open source packages. These open source packages ensure the interoperability between the packages. Glenn A. Fink, Paul Muessig, and Chris North [4] introduces Portall, visualization tool that gives system administrators a view of the communicating processes on the monitored machine correlated with the network activity in which the processes participate.

Ron Gula[5] presents the vulnerability correlation with the IDS alerts and specify two methods of correlating the vulnerability with the IDS alerts. These are Persistent VA/IDS Correlation and near time VA/IDS Correlation. netForensics[6] integrates three distinct yet complimentary forms of event correlation – the first is rules based correlation which separates false positive security alarms from potentially significant security incidents by invoking “time aware” security policy rules for each event received from IDS, OS, APPS, or AVS devices monitored by netForensics. The second is Statistical Correlation and third one is Vulnerability correlation. Robert Ball, Glenn A. Fink, Anand Rathi, Sumit Shah, and Chris North [7] explains a tool named VISUAL (Visual Information Security Utility for Administration Live) that provides insight for networks with up to 2,500 home hosts and 10,000 external hosts, shows the relative activity of hosts, displays them in a constant relative position, and reveals the ports and protocols used.

3. PROBLEM DEFINITION

Studying and going through all the references, we have found that the existing problems in today’s network security are most relevant to the – insertion and evasion techniques. Furthermore the limitation is that NIDS can’t deal with switched and encrypted data.

- To deal with the switched data we have implemented the NIDS in the switch itself. As far as the encrypted data is concerned, we configure the IPSecVPN Server within the proxy server or gateway then the encrypted data coming will be first decrypted at the VPN server and forwarded to the NIDS.

- To handle for the insertion and evasion techniques and for reducing the False alarms we must have some technique for correlating the IP traffic to host where the IP traffic is going to reside finally.

4. CONFIGURATIONS AND IMPLEMENTATION

We are having the following requirements for implementation:

- Cisco Catalyst 3750 24-Port Ethernet Switch [8]
- Cisco Intrusion Detection System 4215 Sensor [9]

4.1 Architectural Description

In this paper, we have integrated the VPN and IDS. The physical and logical architecture of the experimental set up is as shown in the Figure 1 and Figure 2 respectively.

The PIX firewall has been configured as VPN to which the remote client installed on the windows machine will connect over the Internet. Since we know that a traditional VPN sever has two network interface cards (NICs), one reachable through the Internet (eth0) and the other on the more trusted network (eth1). These two are connected to the ports 3 and 7 respectively. The victim server is connected to the port 20. There is distribution switch that is working in the DMZ zone between the firewall and the Internet to which the Internet router is connected. The IP addresses used are as shown in the table 1:

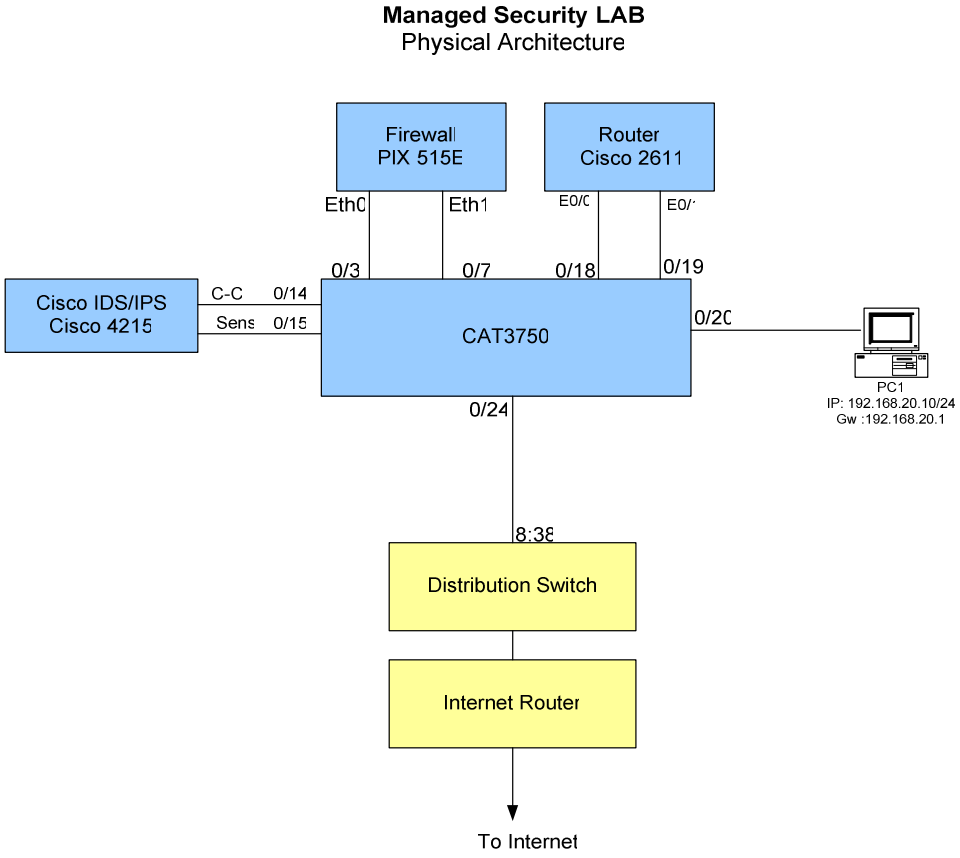


FIGURE 1: Physical Architecture of Managed Security Lab.

Parameter	IP Addresses
Eth0 Server	203.166.97.52/28
Eth1 Server	192.168.20.3/24
Router	203.166.97.50/28
Gateway	192.168.20.1
Clients on LAN	192.168.20.60/24
NAT IP	203.166.97.60

TABLE 1: Logical IP Addresses

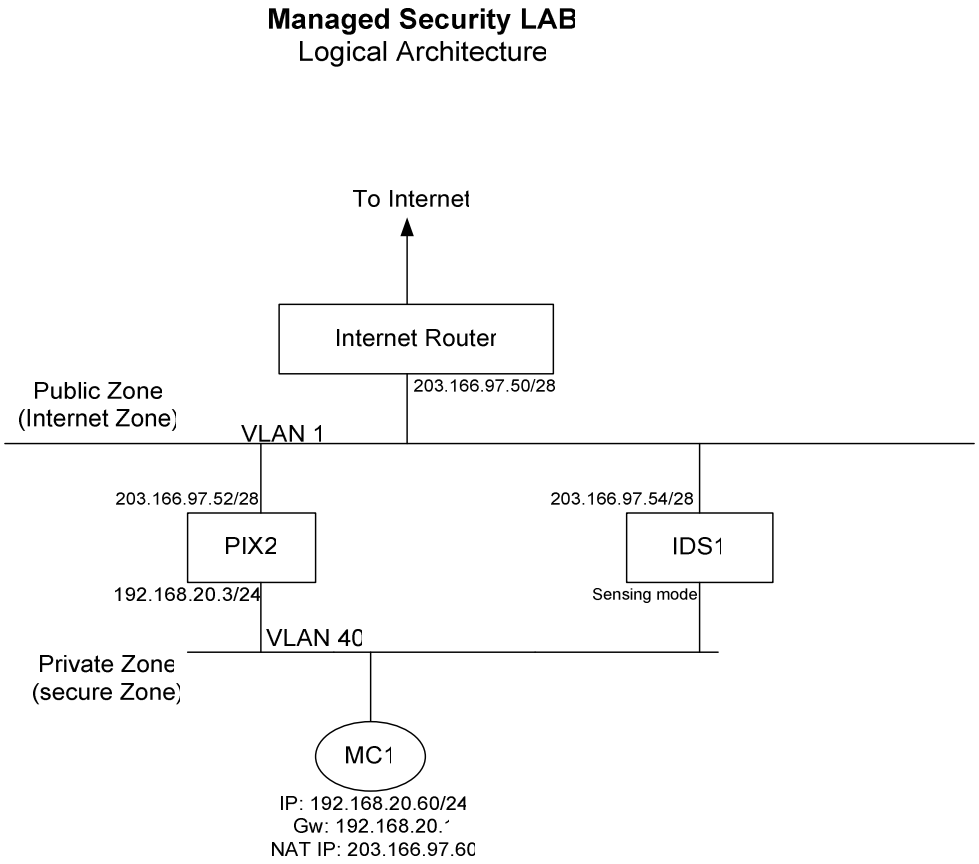


FIGURE 2: Logical Architecture of Security Lab

4.1 Integration network with IDS

The IDS box will sit in the LAN behind the proxy server or gateway in the Private (secure zone) and it will sense all the traffic passing through the proxy server or gateway. The IDS is defined with the relevant rules for the sensed traffic, so it will generate alarm or take action based on the defined rules. In our test setup we have defined the rules for ICMP traffic (Ping), it will detect the ICMP traffic from Internet to an inside server and it take action. In our case IDS box will automatically login into proxy server or gateway and apply the desired rules on the ICMP traffic.

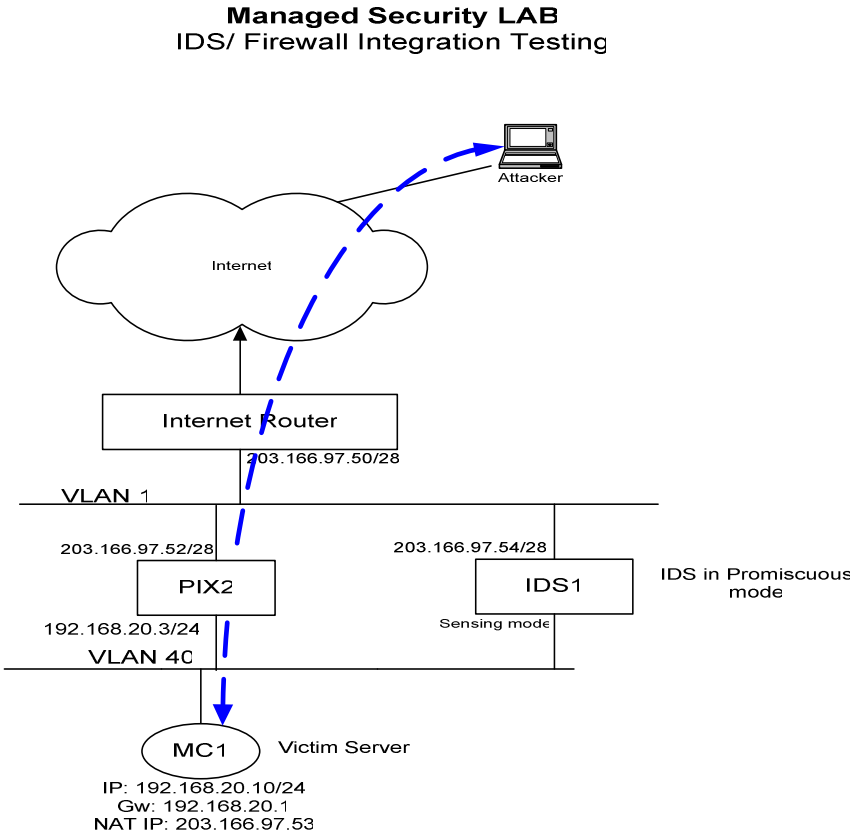


FIGURE 3: Network with IDS Integrated

4.2 Integration of Network and VPN

PIX firewall / proxy server / gateway has been configured as a VPN concentrator (VPN server Box), to which a remote client installed on a Windows machine will connect over Internet. This client will initiate IPSEC tunnel parameters for data encryption while forwarding it to PIX firewall /proxy server / gateway. Once the session is established between client and firewall, the traffic between them will flow encrypted**.**

4.3 Configuration Rules

To implement the above structural diagrams, we defined some configuration rules; based on these configuration rules only few snapshots of the final results have been shown here. The different configuration rules defined are as:

4.3.1 Configuration Rules for Network and IDS Integration

- Defining the interface configuration
- Defining the interface security value for inside highest secure zone
- Defining the rules for ICMP traffic on allowed to pass through
- Defining the interface IP addresses
- Defining the access rule applied for ICMP traffic
- Defining the rules for proxy server/gateway /firewall login/ management configuration
- Defining the rules for IDS box to apply dynamic Access control list on firewall proxy server or gateway

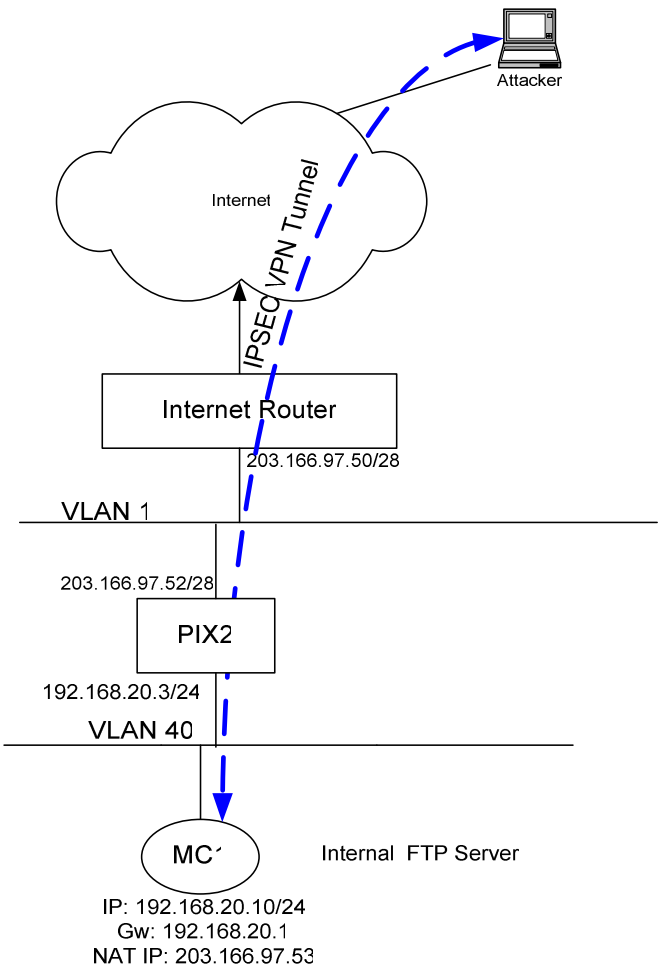


FIGURE 4: Network and VPN Integration

4.3.2 Configuration Rules for Network and VPN Integration

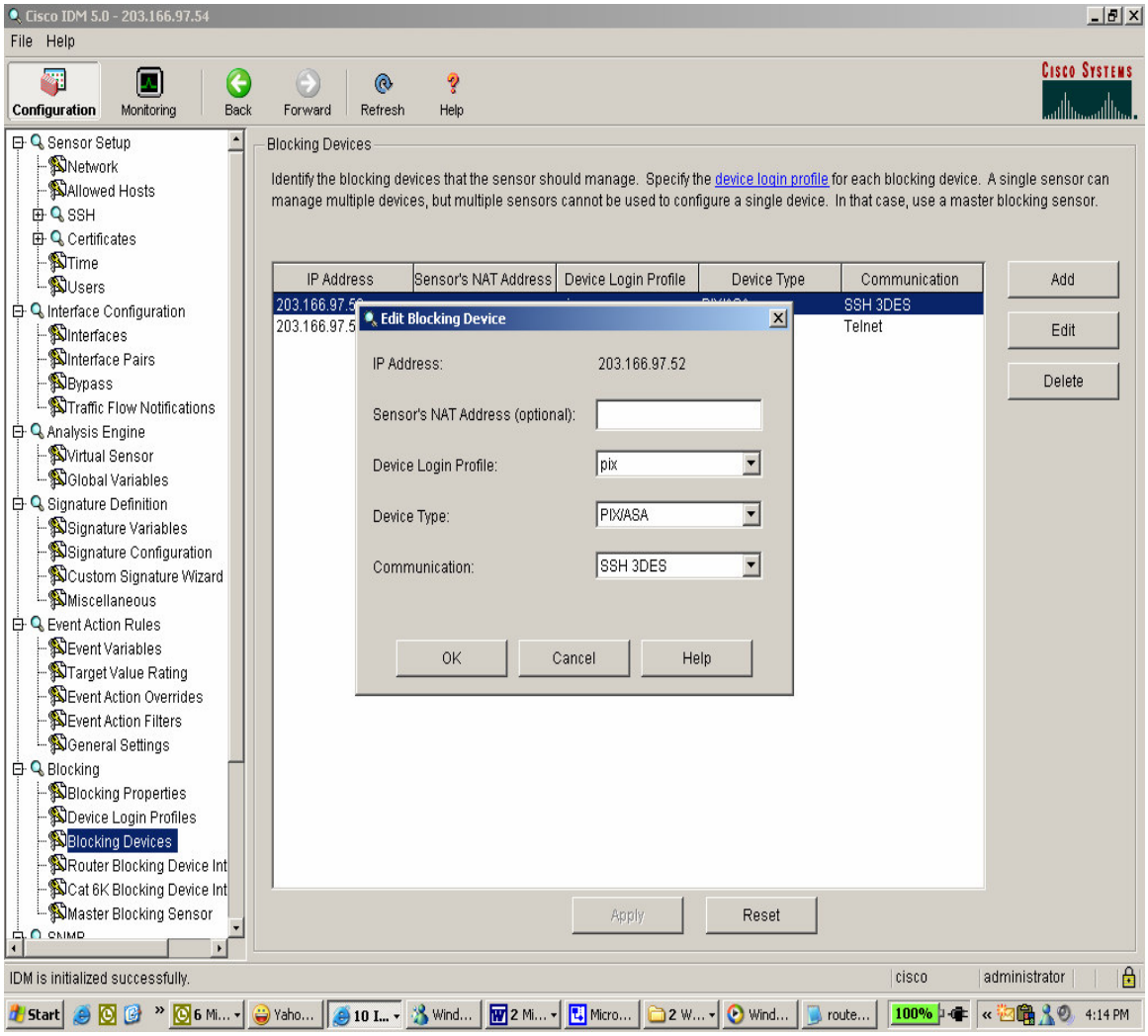
- Defining the rules for physical interface configuration.
- Defining the rules for interface security configuration.
- Defining the access rule for allowing FTP/ICMP services.
- Defining the interface IP address configuration
- Defining the local IP pool for VPN connected customers.
- Defining the rules fro IPSEC VPN configuration and VPN group configuration
- Defining the rules for Firewall Management

4.3.3 PIX logs before the IPSEC session is established

- Defining the IP pool details
- Defining ISAKMP session before tunnel establishment

4.3.4 PIX logs during IPSEC tunnel establishment

- ISAKMP negotiation logs
- IP Pool details after session is established



IGURE 5: Snapshot for blocking device Configuration (PIX 515E)

4.3.5 FTP/ICMP session between client and the FTP server over IPSEC VPN as shown in Figure 8.

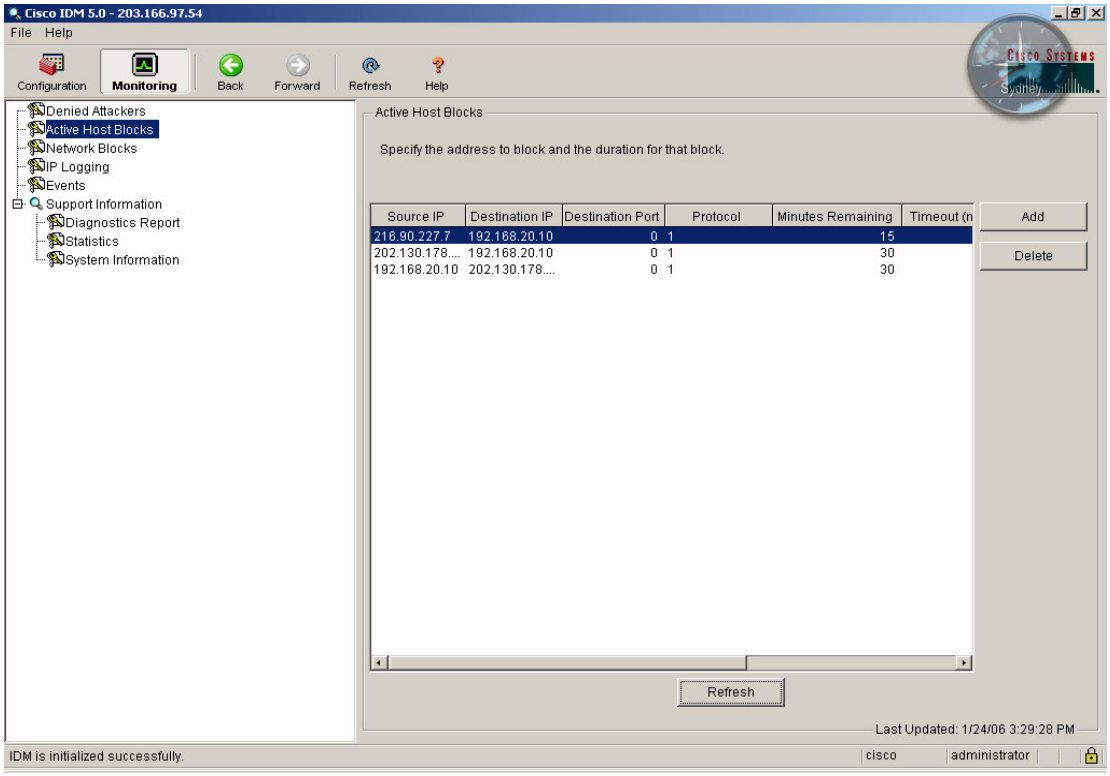


FIGURE 6. Snapshot showing Active Blocking Of Intruders

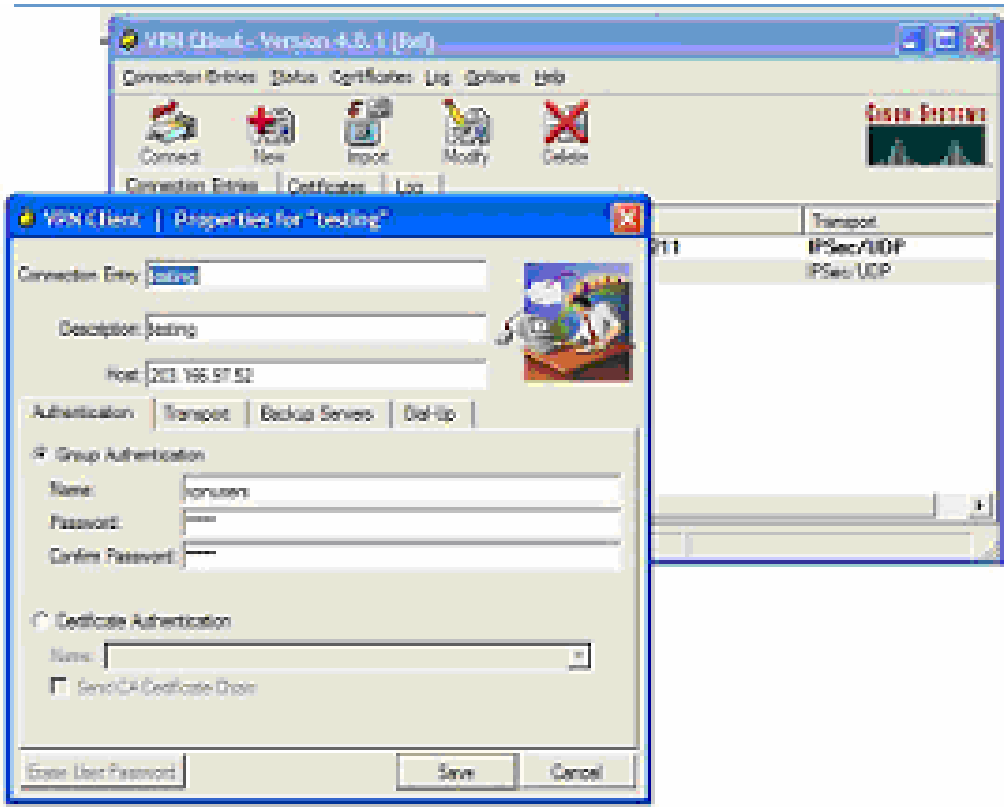


FIGURE 7. VPN Client Configuration

5. RESULTS

5.1 Networks and IDS Integration

In this paper the TCP/UDP and ICMP protocols have been used. After integration of network and IDS the IDS/IPS login to the network as per the configuration rules.

To get the access control list applied by the IDS after logging into the network, we have used the command ***sh log*** as shown below.

fw1-lab1.syd4# sh log

Now the PIX 515E log details appeared highlighting the blocking profile applied by the IDS box. This blocking profile applied by the IDS/IPS in the terms of access rules. The corresponding snapshots showing the details of the active hosts blocked are given in the figure 6.

5.2 Networks and VPN Integration

In this paper, we have used the FTP and ICMP protocols to test the performance of our proposed solution. The different snapshots obtained before the session and after the session are shown as in Figure 8. After the VPN client is configured and connected to the server it is assigned the dynamic IP address. As we specify the configuration rules, the following output will be shown before the IPSec tunnel establishment. To get the IP pool details before the session is established type “show IP local after the # and we will get the following output:

IP pool details

Fw1.lab1.syd4.# show ip local pool

Pool Begin End Mask Free In use vpnpool configured
172.16.20.10 172.16.20.250 Not 241 0

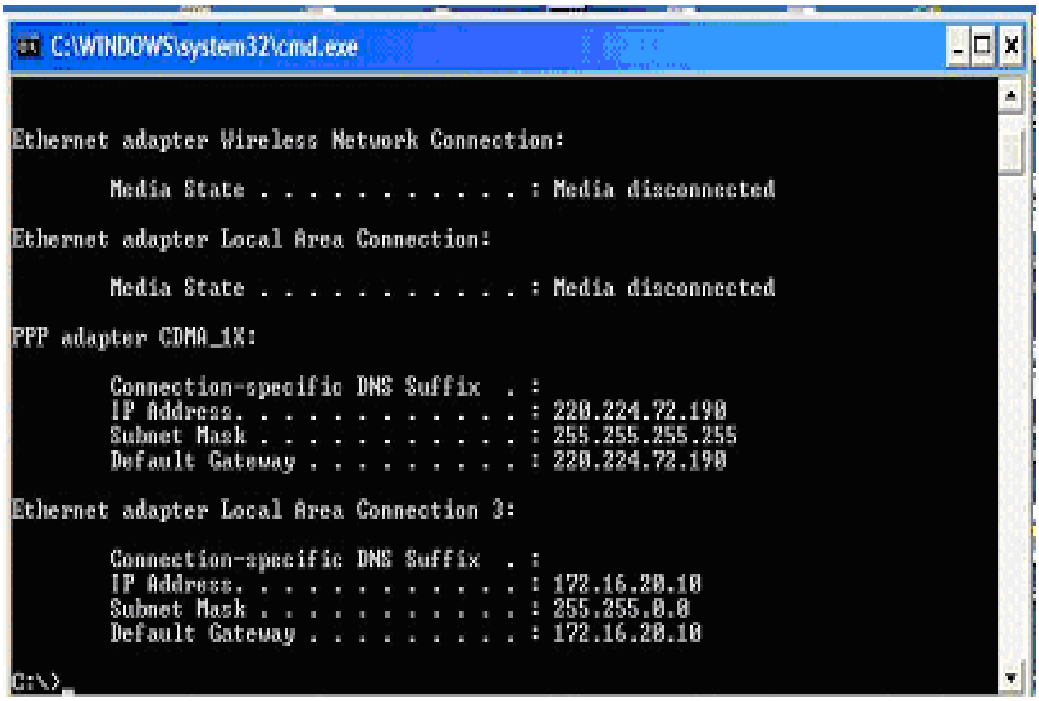


FIGURE 8: PIX Logs before the session is established

And when typed '***sh run'*** after the #, output obtained is as:

```
fw1.lab1.syd4# sh run
Total     : 0
Embryonic : 0
       dst             src       state     pending     created
fw1.lab1.syd4#
```

This above output shows that there are no security associations established in the before the IPSec tunnel establishment. During the IPSec tunnel establishment- The ISAKMP negotiations rules are defined whose corresponding output. Now when the IPSec Tunnel is established between the client and server, the IPSec/ISAKMP associations are created which can be verified by typing the command "***show isakmp sa***" after #
Hence the final output after the creation of tunnel is as:

```
Fw1.lab1.syd4# show isakmp sa
Total     : 1
Embryonic : 0
       dst             src       state     pending     created
  203.166.97.52   220.224.72.190    QM_IDLE        0          1
fw1.lab1.syd4#
```

The above output shows that one session is established between the client and the server.

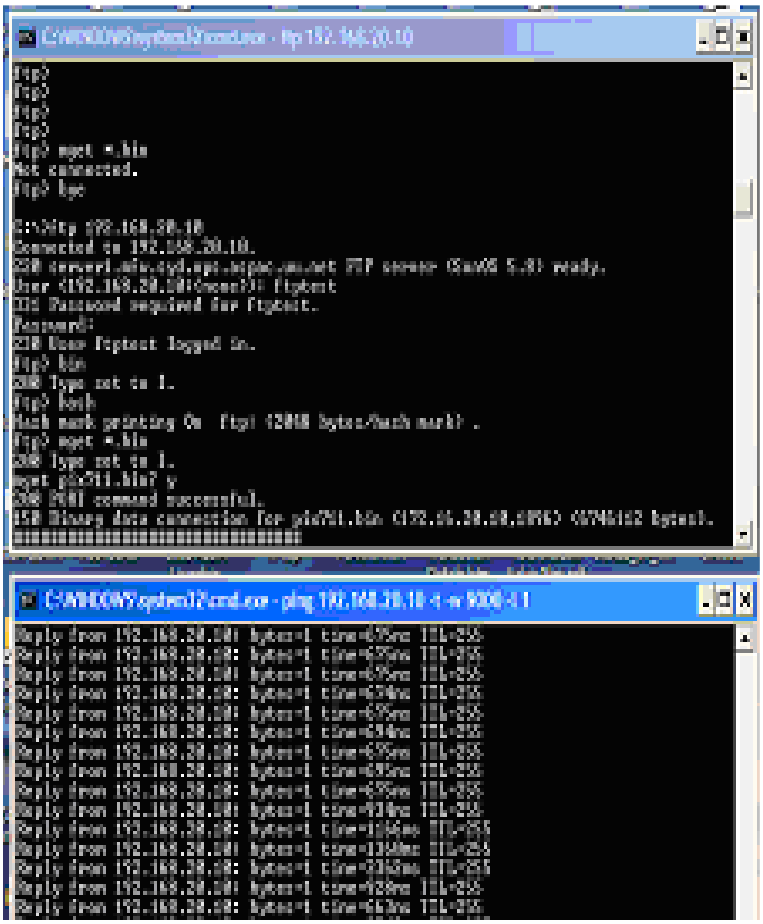


FIGURE 9: Active FTP and ICMP session from the connected client to the FTP Server over IPSEC tunnel

The snapshot in figure 9, demonstrates the creation of Active FTP and ICMP session from the connected client to the ftp server over IPSEC tunnel after the creation of IPSec Tunnel.

The integration of IDS and VPN definitely change the way the security is implemented with in an infrastructure. Also a number of security parameters are affected whenever a change is made. The same is there within this paper is implemented by us.

The different parameters affected by the implementation of this work are**:**

- System Status and Traffic status before and after the creation of a IPSec tunnel
- Time
- Security
- Cost

6. CONCLUSION & FUTURE WORK

Summing up all the things the concluding remarks that account for the implementation are as:

- The integration of various security devices helps in changing the security strategy and making it implement in a better way to defend the attacker.
- The results produced after the integration is satisfactory.
- The correlation of HIDS and NIDS placed at the edge helps in reducing the number of alerts.

Hence the overall point of conclusion is that integration of different devices in the networks security is workable only if deployed in the proper way at proper place.

The areas that can be worked upon to improve the overall security strategy are:

- Inter-IDS correlation
- Data Mining
- Visualization

9. References

[1] Ying-Dar Lin, Huan-Yunwei, and ShaoTangYu, Building an Integrated Security Gateway: Mechanisms performance Evaluations, Implementations and Research Issues, EEE communications Survey, the electronic Magazine of original peer reviewed survey articles. http://www.comsoc.org/pubs/surveys.

[2] Jason Halpern, Safe VPN IPSec Virtual Private Networks in Depth, White Paper, Page 5-8. [April 2001].

[3] Char Sample, Mike Nickle and Ian Poynter, Firewall and IDs shortcomings, first presented at SANS Network Security, Monterey, California. [October 2000].

[4] Glenn A. Fink, Paul Muessig, and Chris North, Visual Correlation of Host Processes and Network Traffic. http://infovis.cs.vt.edu.

[5] Ron Gula, Correlating IDS Alerts with Vulnerability Information, Tenable Network Security http://www.tenablesecurity.com , (December 2002).

[6] netForensics,Comprehensive Correlation: A Three Tiered Approach, http://www.netforensics.com,(2004).

[7] Robert Ball, Glenn A. Fink, Anand Rathi, Sumit Shah, and Chris North, Home-Centric Visualization of Network Traffic for Security Administration, http://infovis.cs.vt.edu/.

[8] Cisco Catalyst 3750 24-Port Ethernet Switch: Product Reviews.

[9] Cisco Intrusion Detection System 4215 Sensor (IDS-4215-K9) Network Monitoring Device: Product Features.

[10] CISCO PIX 515E SecurityAppliance, Datasheet Cisco Systems, (2005).

[11] Thomas H. Ptacek , "*Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection*", whitepaper from windows security, http://www.windowssecurity.com/.

[12] Corbin Del Carlo, "*Intrusion detection evasion: How Attackers get past the burglar alarm*", SANS Great Lakes, Chicago Illinois, May 18-23, 2003.

[13] Joshua Heling, CISSP CTO and Co-founder, Secure Pipe Inc." *Balancing Detection and Prevention in the Deployment of Network Intrusion Technology*", White Paper from Secure Pipe Managed Network Security.

[14] Haluk Aydin, "*NAT Traversal: Peace Agreement between NAT and IPSEC*", SANS Institute, August 12, 2001.

[15] Christopher Smith, "*IPsec's role in Network Security: Past, Present, Future*" SANS Institute, September 2001.

[16] S. Kent and R. Atkinson, "*IP Authentication Header*", IETF Network Working Group RFC 2402, November 1998.

[17] S. Kent and R. Atkinson, "*IP Encapsulating Security Payload*", IETF Network Working Group RFC 2406, November 1998.

[18] Joshua Haines, Dorene Kewley, Ryder ,Laura Tinnel, Stephen Taylor, "*Intrusion Alert Correlation- Validation of Sensor Alert Correlators*", Published by the IEEE Computer Soceity,2003.

Development of Irregular Routing Algorithms for Parallel Computing Environment

Dr Yogesh Chaba yogeshchaba@yahoo.com
Chairman, Dept. of CSE,
GJUS&T, Hisar,India

Ranjana Gulati ranju2604@gmail.com
Dept. of CSE,
GJUS&T, Hisar,India

ABSTRACT

In this paper, a review of various regular and irregular parallel computing networks routing algorithm is done. Since irregular networks are usually less costly and multipath in nature as compared to regular Parallel computing networks, hence analysis of irregular and regular Parallel computing networks is important. It can be deduced from the analysis that irregular Parallel computing networks performs better than regular ones.

In this paper, a new class of irregular fault-tolerant multistage interconnection network named fault tolerant interconnection (FTI) network is also proposed and analyzed. The FTI network can achieve significant tolerance to faults and good performance with relatively low costs and a simple control scheme. The construction procedure of the FTI network, algorithms for allocation of path length, routing along with the routing procedure, fault-tolerance aspect is described too.

Keywords:- Permutation passability, Multistage Interconnection Network

I. INTRODUCTION

In the present era of technology and development, it is very much possible to design and develops multi-processing system with many of multi-processors[10]. Multistage Interconnection network (MIN) play an important role in these systems, which enables processors to communicate with themselves and with memory modules. Multistage Interconnection network consists of more than one stage of switching elements, links that interconnect them[12].

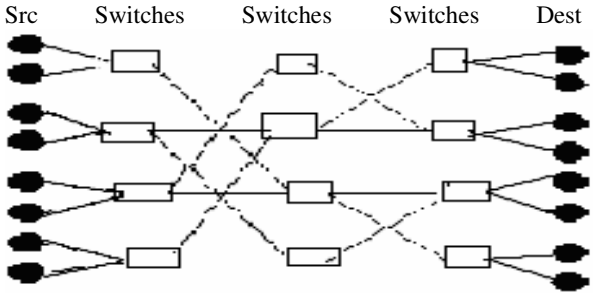


Figure 1: A 3 Stage Interconnection Network

An MIN with 3 stages is illustrated in fig 1. In this paper, a new MIN is designed which is irregular and more cost-effective and simple in a way. Regular network has equal number of switching elements per stage so they impose equal time delay to all requests passing through them. Irregular network has unequal number of switching elements per stage, so for a given source to destination pair, there are different path lengths available in this network[9].

Different networks are available offering varying degrees of reliability, efficiency, and cost and fault tolerance. The flip network, omega network, indirect binary n-cube network, and regular SW banyan network (S = F = 2) are topologically equivalent. CROSSBAR, OMEGA[2][4][13][14] are the examples of regular MIN. MDOT,

RMDOT, FT, FTD, ESC[5] are the examples of irregular MIN. These all kind of networks is studied, analyzed in details. They all have some kind of limitation. The reliability, performance and limits of these MINs is stated by [6][8][13].So attempt to find out a new network which proves to be more fault tolerant and cost effective too. FTI algorithm is developed which is very fault tolerant and cost effective too for parallel computing system.

2. FTI: ROUTING ALGORITHM FOR IRREGULAR PARALLEL COMPUTING SYSTEM

In MIN, more than one path from a source to destination is available. Here, request is routed through an alternative path if the most favorable path is not available due to any reason like faulty switches in path or busy path[7][11]. An important performance parameter in the MIN is permutation passability[1]. Desirable characteristics of a network are that maximum requests should get matured with the shortest favorable path so less time is taken to reach to its destination. So we developed an algorithm, which will fulfill these desired requirements of the network. At a particular moment of time if more than one request occurs at source or demands to reach at the same destination than less fault occurs and all the requests will be matured. This paper is aimed at addressing this kind of problem, which arises when multiple requests are made for the same destination in a network or more than request is made from the same source for different destinations. This paper is an attempt to solve the permutation passability problem in MIN imposed. In order to solve it, we design an algorithm, which will help in maturing maximum number of requests by giving an alternate path if one is busy or faulty. In the next section, we detailed the assumption we made for the algorithm and then the algorithm is explained.

Our algorithm is mainly based on two main parameters i.e. number of requests matured i.e. reaching the destination and average path length is calculated on the basis of how many switches it has to pass through to complete the request. A simulation of permutation passability is applied on the other available networks also to calculate the requests matured and average path length is calculated for them, which clears to us that our algorithm is very fault tolerant and cost effective as compare to others.

.

2.1 Algorithm For FTI Network:

In a FTI network, each source and destination is connected with multiplexers, demultiplexers. A FTI network of size $2^n * 2^n$ consists of 2^n multiplexers and 2^n demultiplexers. Each MUX and DEMUX is of size 2*1 and 1*2 respectively. In FTI network, we are using switches of size 3*3 also so that if primary switch is faulty then the request can be routed to the conjugate switch connected to this due to which less fault are occurred and request still can be matured.

2.1.1 Assumptions

- Multiplexers are simple with no routing capability.
- Switches have routing capability based on destination tags.
- More than one source destination pair cannot have the same values.
- No looping takes place between conjugate pair of switches.
- Path matrix is used for storing the paths of respective pairs.
- FCFS algorithm is used for serving the requests.

2.1.2 Routing algorithm

In the MIN, there are multiple paths available for a given source to destination, minimum path length is checked if available then routed through it else other route is taken.

Let S be the source and D be the destination of the network and

S=SnSn-1_ _ _ _ _ _S2S1S0

D=DnDn-1_ _ _ _ _ D2D1D0

Then to check if the minimum path is available for each S to D, XORing of each source to destination is performed

(S0DO) XOR (S1D1) XOR (SnDn) = 0

if it equals to zero then there is a minimum path available else the request has to pass through alternate path which will be comparative longer. If there is a minimum path exists between each S to D then Set min_path_flag_array to 0 which signifies that there a minimum path exists between S to D and other possible path is also available. In other case, if this flag values not equal to zero then it means that no any path length with minimum route is available but the path with maximum length is available (length can maximum be 10). Now, for routing to take place if switches in the route are not faulty then routing is done through it. But in other case if switches in the routing path are faulty then request is routed to the conjugate switch connected to it.

3 PERFORMANCE EVALUATION OF FTI ALGORITHM

The simulation of permutation passability behavior of a network will generate the number of requests appearing on source side at a particular instant of time and out of these total requests, how many of them are getting matured and the length of the path taken by the requests is calculated. These are the basic parameters for the simulation.

Simulation environment:

- For the simulation, we are assuming that there are 16 nodes on each side i.e. there is 16 sources and 16 destinations for each network.
- The values are inputted using the algorithm of each network.
- This simulation analysis of permutation passability behavior is checked for 50 times. For the simulation, different values are inputted for 50 times for each network and thus the result is calculated.

Results of Simulation:

Figure 2 shows the average path length of various networks. Path length is calculated on the basis of total switches a request has to go through in the path to reach to its destination.

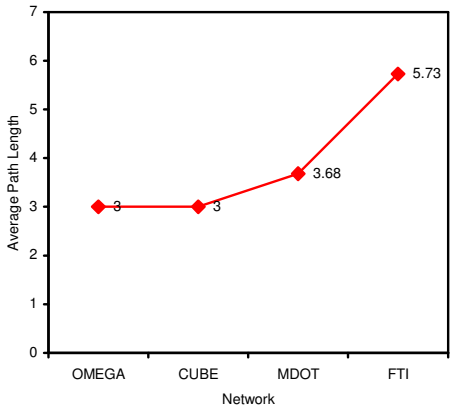


Figure 2: Comparison of Average Path Length of various Networks

The results of simulation show that Average path length of regular networks like OMEGA, CUBE is fixed at 3 because here number of switches in each stage is equal while it varies for the irregular networks. In irregular network like MDOT, FTI network, because here numbers of switches vary for each stage so path length also varies. In our FTI network, path length is more, as a request has to pass through the conjugate switch if the switches in the shortest path are faulty or busy. It results a long path and maturing maximum requests.

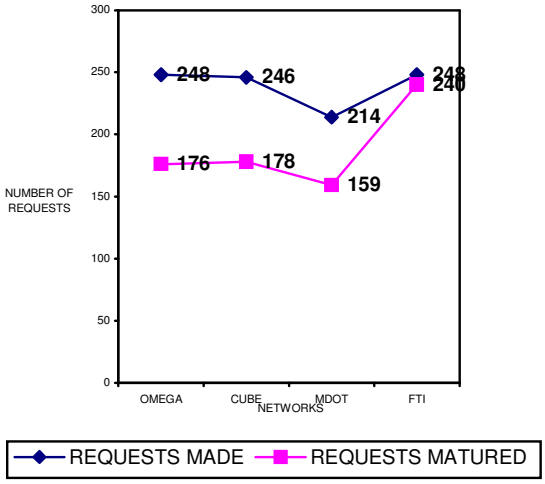


Figure 3: Comparison of Requests made and Requests matured for various Networks

Figure 3 tell about the requests sent and requests matured. The results of simulation shows that in our FTI algorithm total requests matured are almost equal to the requests sent to it. In omega network, total requests made are 240 amongst them 176 requests are matured. And in cube network out of total 246 requests 178 are matured at the time. It is also seen that if destination of more then one requests appears at the same block then only one request gets matured. But in our proposed network, this problem is eliminated. In this way, performance is improved.

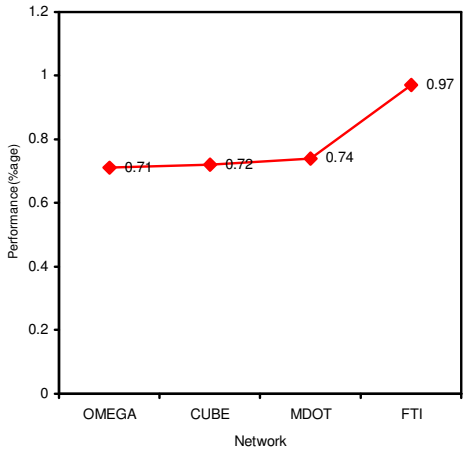


Figure 4: Comparison of performance of various networks

Figure 4 helps in showing the performance improved using our algorithm. Omega network is providing 0.71% performance while cube's performance is 0.72% and irregular network MDOT's performance is somewhat better than these regular ones. MDOT provides 0.74% performance. In our FTI network, performance is improved. FTI provides the 0.97 % performance. It improves the performance from regular ones by approximately 25 % and from other irregular MDOT network by 23 %.

4. CONCLUSION

In this paper, we have analyzed the permutation passability behavior of FTI network, which is an irregular network. An irregular MIN is more cost effective and efficient than a regular MIN also they are as reliable and fault tolerant as other similar regular ones. Also we know that the minimum path length in MDOT Network is 2 whereas regular MINs like Omega have minimum path length 3. It can be depicted that irregular MINs have better performance in terms of average path length. Thus, it makes them a strong candidate of permutation passibility analysis.

FTI network has the highest permutation passability. We have calculated the number of requests successfully maturing and it has been found that if more number of requests are having the same destination or more number of requests are having the destination values that are lying in the same block then it resulted in more the number of clashes but FTI achieves more fault tolerance as sources and destinations are connected to MUX, DEMUX directly so fault is tolerated at both the ends even when the request has to be routed on the alternate path.

5. REFERENCES

1. Yuanyuan Yang, Jianchao Wang and Yi Pan," Permutation Capability of Optical Multistage Interconnection Networks", *Journal of Parallel and Distributed Computing*, Volume 60, Issue 1, January 2000, page(s) 72-91.

2. Jacques Lenfant and Serge Tahé, "Permuting data with the Omega network", *Acta Informatica* ,Volume 21, Number 6,Nov 2004, page(s) 629-641.

3. Mahgoub, Imad, Huang, Chien-Jen," A novel scheme to improve fault-tolerant capabilities of multistage interconnection networks", *Telecommunication Systems*, Volume 10, Numbers 1-2, October 1998, page(s): 45-66.

4. Siegel, H.J. Nation, W.G. Kruskal, C.P. Napolitano, L.M., "Using the multistage cube network topology in parallel supercomputers", *IEEE Computer society*, Dec 1989, Volume77, Issue 12, page(s): 1932-1953.

5. Chuan-Lin Wu, Tse-Yun Feng," On a Class of Multistage Interconnection Networks", *Transactions on Computers*, august2006, Volume: C-29, Issue: 8, page(s): 694- 702.

6. Blake, J.T. Trivedi, K.S, "Multistage interconnection network reliability", *Transactions on Computers*, Nov 1989, Volume: 38, Issue: 11, page(s): 1600-1604.

7. Aydogan, Y. Stunkel, C.B. Aykanat, C. Abali, B**. , "**Adaptive source routing in multistage interconnection networks", *Parallel Processing Symposium, 1996,* Proceedings of IPPS '96*,* Apr 1996, page(s): 258-267.

8. Chuan li wu, manjai lee," Performance Analysis of Multistage Interconnection Network Configurations
9. and Operations", *IEEE Transactions on Computers***,** 1992, Volume 41, Issue 1, page(s): 18 - 27.

10. Aude, J.S.; Young, M.T.; Bronstein, G.," A high-performance switching element for a multistage interconnection network", *Integrated Circuit Design*, 1998.Volume 23, Issue 9, 1998, page(s): 154 – 157.

11. Dong Li; Mei Ming; Bo Fu,"New multistage interconnection network for multicast", The 9th Asia-Pacific Conference on Communications, 2003, *APCC 2003*, Volume 3, Issue 21, Sept. 2003, page(s): 993 – 997.

12. López de Buen, Víctor," Multistage interconnection networks in multiprocessor systems. A simulation study", *Qüestiió*, 1987, volume11, Issue 3, page(s): 73-86.

13. Siegel, H.J.," Interconnection Networks for Parallel and Distributed Processing: An Overview", *Transactions on Computers,* Apr 1981, Volume: C-30, Issue 4, page(s): 245- 246.

14. Nasser S. Fard, Indra Gunawan" Reliability Bounds for Large Multistage Interconnection Networks", *Lecture Notes in Computer Science*, 2002,Volume 2367,page 762.

Decimal genetics Algorithms for Null steering and Sidelobe Cancellation in switch beam smart antenna system

Reza Abdolee reza.ab@ieee.org

Wireless communication centre (WCC)
Faculty of Electrical
Universiti Technologi Malaysia (UTM)
Skudai, Johor, 81310, Johor, Malaysia

Mohd Tarmizi Ali *mizi732002@yahoo.com*

Wireless communication centre (WCC)
Faculty of Electrical
Universiti Technologi Malaysia (UTM)
Skudai, Johor, 81310, Johor, Malaysia

Tharek Abd Rahman *tharek@fke.utm.my*

Wireless communication centre (WCC)
Faculty of Electrical
Universiti Technologi Malaysia (UTM)
Skudai, Johor, 81310, Johor, Malaysia

Abstract

Sidelobes cancellation is challenging task in beamforming and beam steering in smart antenna systems. The high level of sidelobes can significantly degrade the system performance as well as antenna power efficiency. In this paper, we present the new decimal genetic algorithm to reduce the sidelobe and at the same time create the nulls toward interferers and jammers. This technique takes advantage of Chebyshev coefficients window as an initial weight vector to speed up the optimization process. The simulation results have shown that this technique is able to find the most suitable weights vector to reduce the sidelobe power and at the same time create the nulls toward interferers. Verification has been done for Uniform Linear Array (ULA) structure. However, this technique can be used for non regular geometrical antenna array structure with variety of beam pattern requirements

Keywords: *Genetic algorithm; Smart antenna; Null steering; Sidelobe cancellation*

1. INTRODUCTION

The principle objective of switch beam antenna array is to steer the main beam to desired location. The uniform linear array (ULA), which is an array of uniformly spaced antenna, can produce the sufficient narrow beam. However, the first sidelobe of a ULA radiation pattern is only

about 13.2 dB down from the main lobe level. This is undesirable phenomenon for directive applications, such as radar and direction finding. The sidelobes can be reduced to any desired level by tapering the amplitude of the elements excitation. In tapering process the main task is to calculate an appropriate weights vector which can produce the narrow beam with minimum level of sidelobe. One drawback of amplitude tapering is beamwidth expanding. It means to gain lower amount of sidelobe we must accept the wider value of beamwidth.

Various analytical and numerical techniques have been developed to provide the finest trade-off between sidelobe level and beamwidth value. Examples of analytical techniques include the well-known Taylor and Chebyshev method [1]. In recent years, numerical approaches have become more popular as they are applicable not only to regular arrays such as linear arrays and circular arrays but also to arrays with complicated geometry layout and radiation pattern requirement. Examples of numerical techniques include the linear or nonlinear optimization methods [2], [3] and adaptive methods [4], [5]. Another interesting technique to reduce the sidelobe level is non-uniform spacing or space perturbation. In this technique, the sidelobes can be reduced in height to approximately 2/N times the main lobe level, where N is the number of elements [6] while the beamwidth remains essentially the same as for the uniform array. However, space perturbation is far away to apply for real time application since it depending on servo motor functional speed. Recently, the genetic algorithm has found more popularity to optimize the antenna radiation pattern. In conventional genetic algorithms usually the binary coding and decoding is used for crossover mating. In [7] the decimal GA algorithm has been proposed. This technique is applicable for real as well as complex decimal numbers. However, this technique needs the initial weights calculated using other techniques like MMSE, therefore it makes the technique computationally intensive.

This paper presents the new decimal GA technique to taper the amplitude of array excitation which avoids priory MMSE calculation. Instead, the initial weights vector can be adapted from simple look-up table calculated using conventional array weighting such as Chebyshev window function. This technique can use either real or complex weights vector without binary coding and decoding for crossover process. The remaining material of the paper is organized in four sections, section two describe the proposed GA algorithms, the evaluation or fitness function is described at section three, the results are presented in section four and the paper concludes at section five.

2. THE GENETIC ALGORITHM

The proposed decimal GA algorithm is similar to decimal GA proposed in [7]. However, there are some differences which make this technique faster to apply for sidelobe cancellation and null steering. The flow of this technique is briefly explained herein.

2.1 CONSTRUCTION OF CHROMOSOMES

Unlike the binary GA which chromosomes are represented by the string of binary number, in this technique the chromosome are represented by either complex or real decimal numbers. To fit this technique to smart antenna structure, the chromosomes are corresponded to weights of antenna elements. In the other words each chromosome is consist of M number of genes where M is the number of antenna elements. As an example chromosome one $\overline{w}_1$ can be represented by equation 1.

$$\overline{w}_1 = \left[w_{11}\ w_{12} \mathrm{L}\ w_{1M} \right] \qquad (1)$$

Here, $w_{11}\ w_{12} \mathrm{L}\ w_{1M}$ are the antenna elements weights or genes. Each of this weight has boundaries with up and down limit. The random set of chromosome can be easily constructed using following relation represented by equation 2.

$$\overline{w}_n = (u_1 - u_2) \times \overline{r} + u_2 \qquad u_2 < \overline{w}_n \leq u_1 \qquad (2)$$

Where, u1 and u_2 are the maximum and minimum limit value of the weights and $\overline{r}$ is real random vector between zero and one. For instance, when real amplitude weighing is considered for the problem, the value of u_1 and u_2 are one and zero respectively, and $\overline{r}$ is the vector whose elements can be any real number between zero and one.

2.2 INITIAL POPULATION

The initial population number is double of good population number. The top fifty percent of initial population is chosen as a good population after evaluation of each chromosome in initial population by the fitness function.
Some literature use term evaluation function instead of fitness function, however these two terms are equivalent. To speed up the convergence of GA iteration, the initial population can include approximate of the best chromosome which in sidelobe cancellation issue this approximation can be achieved from conventional array weighting [8] such as Kaiser or Taylor weighting.

2.3 REPRODUCTION

When the initial population is created, the top fifty percent of this population having better fitness value are chosen. Now it is the time for parent selection process. To do so, among different available techniques such as tournament, genitor, roulette wheel and ranking [9], roulette wheel can suit the application. This technique randomly chooses the chromosomes with higher fitness value as parents for next generation. It means the higher the value of the fitness function the more chance chromosome has to be selected as a parent. The top 50 percent of the population is chosen as the parent for next generation and the remained 50 percent are discarded at this stage. Next step is reproduction; the reproduction process consists of three basic genetic operations: crossover mating, mutation and Elite principle. Crossover mating is common term in binary coding and decoding GA algorithm however, for decimal GA the operation is slightly different, for the GA here we proposed the crossover as a linear summation and subtraction operation. Since, these operations can carry the good feature of parent to the next generation. Unlike the other technique, four children are created from two parents who can be represented by following equations:

$$\overline{c}_n = \frac{1}{4}\left(3\overline{w}_n + \overline{w}_{n+1}\right) \qquad (3)$$

$$\overline{c}_{n+1} = \frac{1}{2}\left(\overline{w}_n + \overline{w}_{n+1}\right) \qquad (4)$$

$$\overline{c}_{n+2} = \frac{1}{2}\left(2\overline{w}_n - \overline{w}_{n+1}\right) \qquad (5)$$

$$\overline{c}_{n+3} = \frac{1}{2}\left(2\overline{w}_{n+1} - \overline{w}_n\right) \qquad (6)$$

In this process, four children will be results of crossover mating. It means if the parent population is p_p the children population p_c would be equal to $2\mathrm{p}_\mathrm{p}$. Now, the whole population of offspring and parent is $3P_P$. this population is evaluated using fitness function. In the next process, before mutation operation, the elite children who have the best fitness function in the population directly

go to the next generation; this mechanism is called Elite principle. Therefore the mutation process will not affect the best chromosome or individual, and it keeps the trend of GA iteration always rising trend, therefore the value of the fitness in each iteration never get worse from the previous iteration in the algorithm. In proposed GA two chromosomes with the best fitness value after crossover mating are picked of as Elite members. Then the next process which is mutation is done. Different numbers of simulation have shown that the mutation with the probability of 1/M has always better results than the other probability value. Where M is the number of antenna arrays.

The mating process can be simply applied to the whole population, if we create a matrix of population. For instance, If the number of population after crossover process is $3P_p$, the mutation matrix has a dimension of $(3\mathrm{Pp}\text{-}2)\times\mathrm{M}$ genes. Then number of genes with the rate of 1/M will be changed base on equation 7.

$$w_{nk} = (u_1 - u_2)\times r + u_2 \qquad u_2 \; < \; w_{nk} \le u_1 \qquad (7)$$

Where, r is the random number between zero and one. After mutation process, the population is ranked again, and 33 percent with worse fitness value are directly discarded before roulette wheel parent selection. The best chromosome after the crossover mating is evaluated and if the criteria are met the algorithm will be stopped otherwise this procedure is continuously repeated to achieve the desirable results.

3. THE LINEAR ARRAY AND RADIATION PATTERN SYNTHESIS

The array structure considered for this research is linear. However, the technique can be applied to any type of array with unknown geometrical shape. The equispaced array factor with different excitation amplitude can be written as equation (8).

$$AF = \sum_{k=1}^{M} w(k).e^{j(k-1).\frac{2\pi}{\lambda}.d(\sin(\theta)-\sin(\theta_o)).\cos\phi} \qquad (8)$$

Where, d is the distance between array with the value of half a wavelength and θ, ϕ and λ are the azimuth angle, elevation angle and wavelength of carrier signal respectively, θ_o is the pointed angle of main beam in the azimuth. Herein, we assume that the elevation angle ϕ is zero for more simplicity. M Is the number of antenna and W is the weight vector for the antenna array.

3.1 THE EVALUATION OR FITNESS FUNCTION

The evaluation function can be written as the main beam power ratio to sidelobe power ratio. So it can be written as equation 9.

$$E1 = \frac{P_M}{\sum P_S} \qquad (9)$$

Where, P_M and P_S are the main beam power and sidelobe power respectively, however the GA performance is directly depend on the evaluation function equation. If minimum amount of sidelobe for all direction is required then the evaluation function changes to following relation.

$$E2 = \frac{P_M}{\min_{sidelobe}(P_S)} \quad (10)$$

It means that the algorithm, in each iteration will find the maximum amount of sidelobe and try to find the best weight to reduce this sidelobe to lower level. So all of sidelobe by this technique can be found and suppressed into minimum level. In the case when the null steering is required for the system, the evaluation function can have a relation represented in equations 11,12,13,14.

$$E3 = E2 + \alpha_1.E2 + \alpha_2.E2 \text{L } \alpha_n.E2 \quad (11)$$

$$P_{null1} = \alpha_1.E2 \quad (12)$$

$$P_{null2} = \alpha_2.E2 \quad (13)$$

$$\text{M}$$

$$P_{null_n} = \alpha_n.E2 \quad (14)$$

In this relation $\alpha_1, \alpha_2 \ldots \alpha_n$ are the real numbers which show the depth of the null in compare with the minimum sidelobe level in the pattern. Therefore the depth of each sidelobe can be defined by these coefficients.

4. NUMERICAL RESULTS

The simulations parameters are list down in table 1. The results have shown in figure 1, 2, 3 and 4.

Desire beam pattern / Simulation parameters	One main beam and 3nulls	Two main beam and 2nulls
array type	16 elements ULA	16 elements ULA
Main beam angle	θ_0 =30 degree	θ_0 =0 and ---45 degree
Null direction	β=[-30,0,60] degree	B=[-20,60] degree
Chromosome type	Decimal Real & complex numbers	Decimal Real & complex numbers
Cross-over technique	Decimal Sum &subtraction	Decimal Sum& subtraction

Mutation probability	0.10	0.10
Population number	32 and 64	32 and 64
#of independent run	10	10
#of iteration	50	50

Table 1: Simulation parameters

The GA is repeated for ten independent run, each consist of 50 iterations. Note that even the number of independent run is ten; the close optimized values usually can be achieved after 2 independent run equivalents to one hundred iterations. The population number for figure 1 and 2 is 32 while for figure 3 and 4 is 64

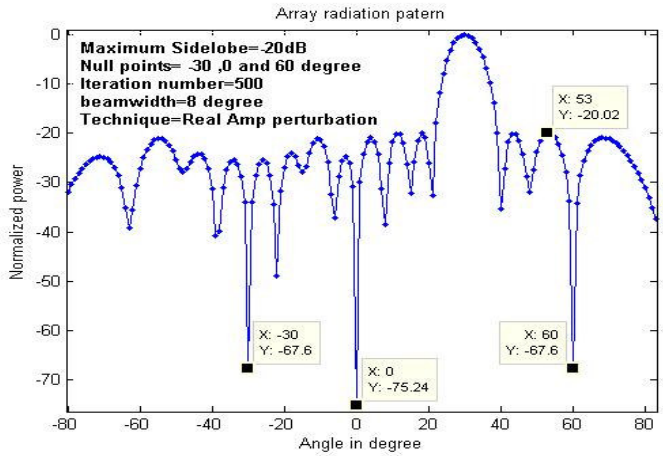


Figure 1: GA with real decimal chromosome type

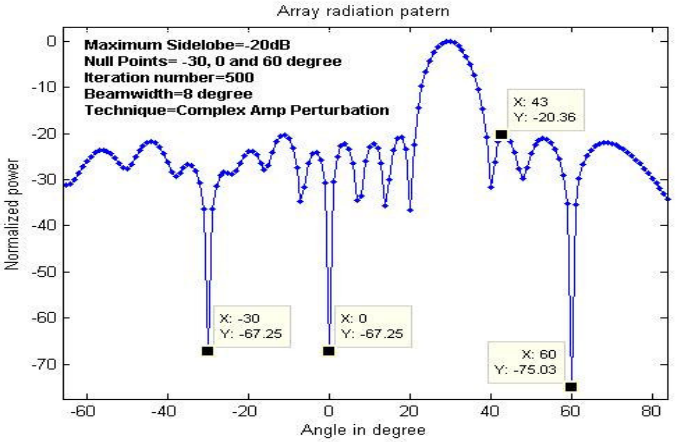


Figure 2: GA with complex decimal chromosome type

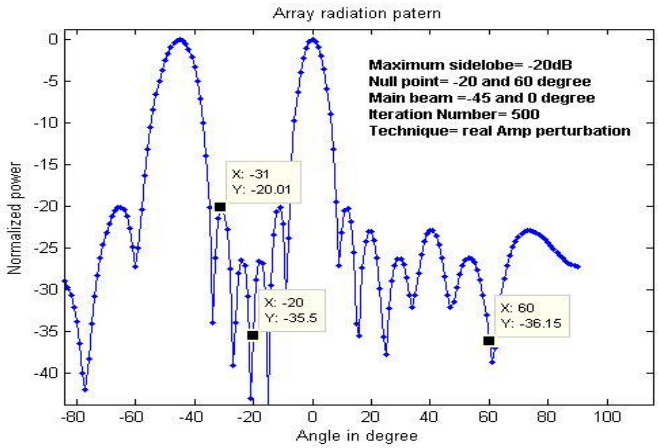


Figure 3: GA with real decimal chromosome type

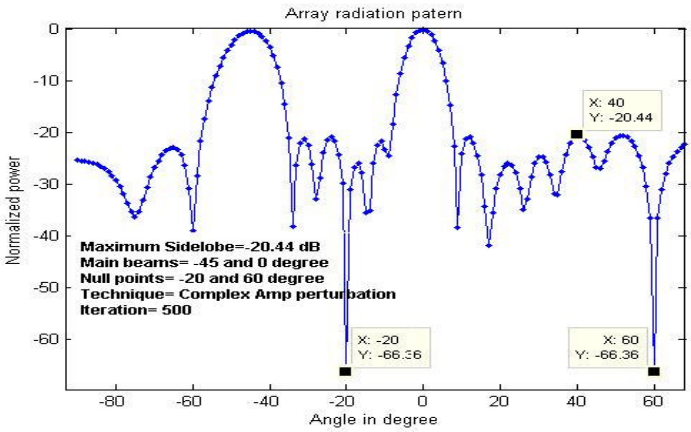


Figure 4: GA with complex decimal chromosome type

The summary of results is organized in table 2.

Beam parameters	Fig 1	Fig 2	Fig 3	Fig 4
Chromosome type	real	complex	real	complex
Main beam	1	1	2	2
Nulls number	3	3	2	2
Maximum sidelobe	-20	-20	-20	-20
Maximum null level(dB)	-67.6	-67.2	-35.5	-66.3

Table 2: summary of the results

Important results is shown in table 2, In the context of antenna and beamforming techniques, when the multiple beam and null steering in different direction is required, the GA with complex weights always outperform than the GA with real chromosomes value. However, the results shown that for sidelobe cancellation and minimization, the GA with real chromosome has a better performance and also has a lower beamwidth penalty. In the other words, the GA with complex chromosome causes to wider the beam more than real chromosome GA algorithms. Therefore, careful choice of chromosome type is needed for different problem of beam pattern optimizations.

4. CONCLUSION

The results have shown the effectiveness of the proposed GA algorithm to find the optimized weights vector. The main advantage of this algorithm over other numerical technique is its flexibility to adopt with different constraint and requirements of the problem. A little modification on the evaluation function is adequate to fit in different assumptions and requirements of different problems. Note that the integration of the GA with conventional numerical technique can speed up the optimization process.

5. REFERENCES

[1] C. L. Dolph, "A current distribution for broadside arrays which optimizes the relationship between beam width and side-lobe level," Proc. IRE, vol. 34, pp. 335-447, June 1946.
[2] Y. C. Jiao, W. Y. Wei, L. W. Huang, and H. S. Wu, “A new lowside-lobe pattern synthesis technique for conformal arrays,” IEEE Trans. Antennas Propagat., vol. 41, pp. 824–831, June 1993.
[3] M. H. Er, S. L. Sim, and S. N. Koh, “Application of constrained optimization techniques to array pattern synthesis,” Signal Processing, vol. 34, pp. 323–334, Nov. 1993.
[4] E. C. Dufort, “Pattern synthesis based on adaptive array theory,” IEEE Trans. Antennas Propagat., vol. 37, pp. 1011–1018, Aug. 1989.
[5] C. A. Olen and R. T. Compton, Jr. “A numerical pattern synthesis algorithm for arrays,” IEEE Trans. Antennas Propagat., vol. 38, pp. 1666–1676, Oct. 1990.
[6] Harrington, R. ”Sidelobe reduction by nonuniform element spacing” Antennas and Propagation, IEEE Transactions, Volume 9, Issue 2, Mar 1961 Page(s):187- 192
[7] K.-K. Yan and Y. Lu, “Sidelobe reduction in array-pattern synthesis using genetic algorithm,” IEEE Trans. Antennas Propagat., vol. 45, pp,1997
[8] C. Balanis, “Antenna Theory—Analysis and Design”, New York: Wiley, 2005.
[9] L. Davis, Ed.”Handbook of Genetic Algorithms”, New York: Van Nostrand Reinhold, 1991.

COMPUTER SCIENCE JOURNALS SDN BHD
M-3-19, PLAZA DAMAS
SRI HARTAMAS
50480, KUALA LUMPUR
MALAYSIA