Intrusion Detection In Synergistic Radar Technology And Monitoring Tools

M. Puthanial, Dr. P. C.Kishore Raja

Department of Electronics and Communication Engineering, Saveetha School of engineering, Saveetha University, Chennai.

Abstract— **The main purpose of this paper is to avoid unauthorized system or network to access any local area networks or information from wireless devices. In this system the total zone length is subdivided into equal parts with specific intrusion crossing point resolution. Most providers use private communications like mobile e-commerce transactions. However intrusion happens as it exploits the flaws to decrypt the communication transactions. Decryption techniques are developed and distributed to increase the intrusion. This paper mainly concentrates on intrusion detection in radar technology and also highlights some of the tools that is being used in companies for Network Monitoring to avoid the intrusion.**

***Index Terms*— Intrusion, RF, Radar, Routers, Network**

I. INTRODUCTION

Synergistic radar [1] was introduced in 1992, carnahan conference in Atlanta, George. It was commercialized as ENCLOSURE in mid-1995. ENCLOSURE was introduced as passive perimeter intrusion detection system using FM radio signals.

This paper explains the system in which the synergistic radar technology is used for active intrusion detection. Higher number of zones is required in today's systems. This is because smaller the zones higher the resolution of crossing points. Better accuracy is achieved due to increased resolution. The increase in system cost must be reduced. Line sensors have to be installed parallel to physical barriers. This gives better aid to mount the transmitting antenna. A group of miniature antennas are mounted on the physical barrier as a string.

Our system uses the TRD technology that is accustomed in cable fault location. Guidar, introduced in 1970s was the first that applied the TRD in intrusion sensor for leaky coaxial cable [3]. Also correlated concept in fence sensor was also introduced [4].

In synergistic radar principle is that range gating principles and TRD is used for sub-dividing the cable (through which RF pulse is launched) into series of subzones. A normal radar experiences higher attenuation and dispersion. The returned pulses too undergo distortion practically limiting the overall length of the cable.

II. SYNERGISTIC RADAR WITH INTRUSION DETECTION

The active synergistic radar system deals with the above ground RF field. In addition to this the leaky coaxial cable forms the detection envelope. The effect of multipath must be eliminated. For this purpose the multiple frequencies are used in the quasi-spread spectrum.

In our system we use an antenna for transmitting and the receiver is a sensor cable. But the transmitter and receiver can be interchanged.

A number of miniaturized flat antennas which includes an RF switch and address decoder are mounted on a fence separated by a distance of about 50feet. Only one antenna can radiate at a time while the radiation is absorbed by the leaky coaxial cable.

Each antenna is activated based on time multiplexing such that each antenna forms a sub-zone. The sampling rate (1.7milliseconds/sample) is maintained such that we obtain a good resolution.

Puthanial. M, Associate, Professor, Electronics and Communication Engineering Department, Saveetha School of Engineering, Saveetha University, Chennai

Dr. P.C Kishore Raja, Professor and Head, Electronics and Communication Engineering Department, Saveetha School of Engineering, Saveetha University, Chennai

Puthanial. M is pursuing her PhD in Wireless communication related work in the area of smart antennas under the guidance of Dr. P. C. Kishore Raja, Professor and Head, Department of Electronics and communication who completed his Doctorate from Anna university

III. TRACK WHILE SCAN

The sampling rate varies with respect to the number of antennas (sub-zones) used. Due to this variable sampling rate the concept of track while scan can be used. This concept was used for missile detection in electronic warfare [5].

In this technique the sampling rate is variable because the rate varies with the number of intrusions being detected and the efficiency comparatively gets less. This is due to the use of increased number of sub-zones.

At the same time the sub-zones help in minimization of the overall noise. The useful characteristic of the sub-zone is that any sub-zone can be disabled temporarily or permanently at any point of time.

IV. PRESENT WORK

The miniaturized flat antennas that are mounted on the fence are not electrically stable. To make them stable the antenna is placed by means of a thick PVC layer and then is connected with the coaxial cables center conductor using series of 220 ohm resistors. The mini-whip antenna can also be used for this purpose.

A system comprising of 5 subzones of miniaturized flat antennas are mounted on a variety of linked fences to prove the concept. The 32bit processor circuit helps in the time multiplexing.

V. NETWORKS USED IN MAJOR SERVICE PROVIDERS

AGN-(ATM Global Network)	Uses devices running on ATM
IGN-(IP Global Network)	Uses IP devices
ETRALI	Network used for stock exchange purposes. Highly critical network
Voice	Voice Purposes
HSN	High Speed Network
DTN	Data Transport Network
MTN	Mega Transport Network

Fig 1 (simplified MTN network)

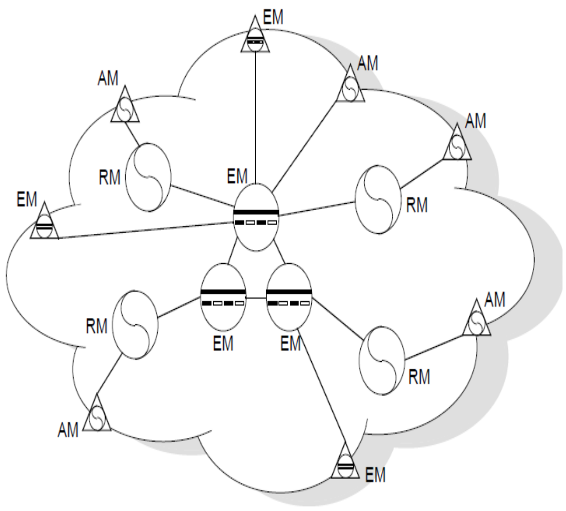
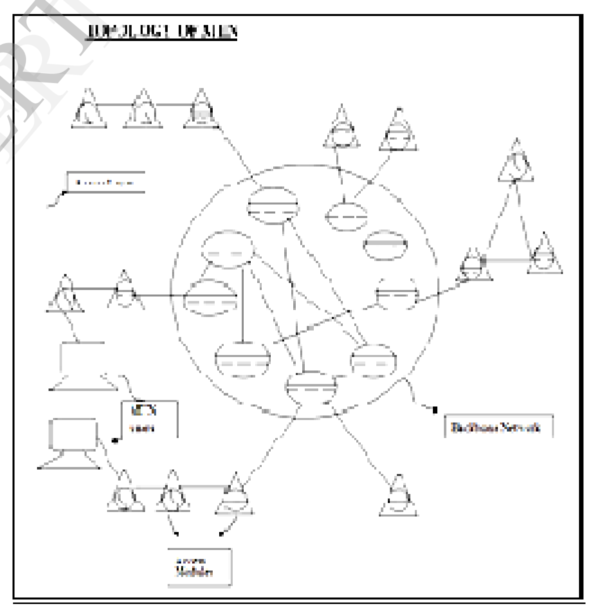


Fig 2 (MTN Topology)



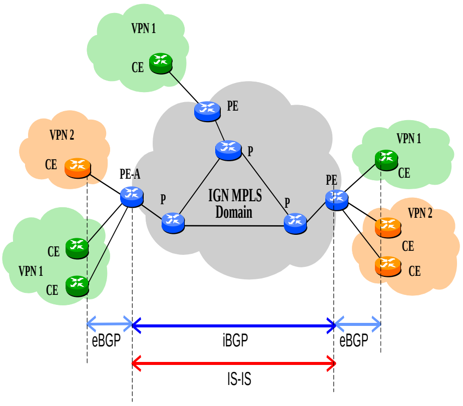
VI. INTRUSION DETECTION MONITORING

MDM- Multiservice Data Management.
XNMS- X.25 Network Management System
CSRM - Call Server Resource Module

IGN

Connectivity between these core devices (Routers/Switches) is either in-house cabling or connectivity taken from different carriers, also having peering links with other providers to carry each other customer traffics on best effort basis. Connectivity for these links are also in-house.

Fig 3 (IGN Network)



VII. Switches Incident Types

1. Link Outage
2. Hardware fault
3. Node Isolation
4. Major outage/Crisis

VIII. MAJOR HARDWARE DEVICES USED

a. DPN- Data Packet Network (Access and Resource)
b. Passport (Access and Resource)
c. XIS – X.25 Interface System
d. Router
e. ACN- Access Concentrator Nodes

DPN is a device that provides good switching performance of traffic for users of X.25, X.28, frame relay, SDLC (Synchronous Data Link Control), SNA (Systems Network Architecture), token ring. Passport equipment was designed in early 90’s to take advantage of new telecommunication chips and more reliable transmission lines. For example: fiber optic cables. Passport offers more improved switching performance compared with DPN.

The switching time is **125 microseconds** and capacity is improved by a **1.6 gigabit/second** bus. Passport supports dual frame and cell switching. A router is a device that forwards data packets between computer networks, creating an overlay internetwork.

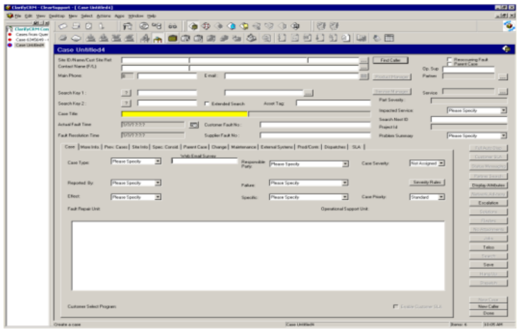
A router is connected to two or more data lines from different networks. When a data packet comes in one of the lines, the router reads the address information in the packet to determine its ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network.ACN (ACCESS CONCENTRATOR NODE). It acts as a gateway between the provider (X.25) and IGN (IP Global Network) and converts X.25 frames to IP packets and vice-versa.

A switch is a telecommunication device which receives a message from any device connected to it and then transmits the message only to the device for which the message was meant. This makes the switch a more intelligent device than a hub (which receives a message and then transmits it to all the other devices on its network).

IX. TOOLS USED

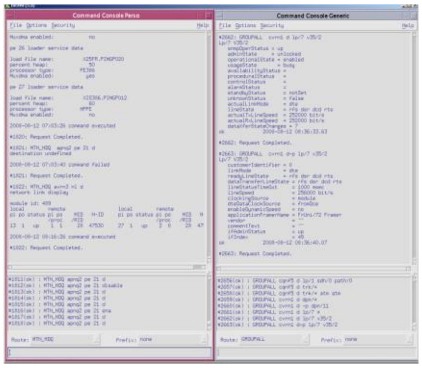
Clarify- It is a ticketing tool used to document the problems and create cases for the same and to work on the case. Working on the case includes testing the problems in the network, raising spare parts, creating dispatches for the Field Engineer to attend, creating sub cases and finally closing the sub cases and as well as the entire case. Each case has a case ID associated with it.

Fig 4 Clarify



Exceed- It is used for knowing the health of the networking devices and troubleshooting as well; i.e. DPN, Passport, XIS, and connection status between them. We can check the connection to the devices by issuing commands. MTN Access is for DPN and GROUPALL for Passports.

Fig. 5 Exceed



```
Mucdma enabled:            no

pe 26 loader service data

load file name:          X25FR.PIMGP020
percent heap:              50
processor type:          PE386
Mucdma enabled:            yes

pe 27 loader service data

load file name:          X2E386.PIMGP012
percent heap:              60
processor type:          HPPE
Mucdma enabled:            no

2008-08-12 07:03:26 command executed

#1820: Request Completed.

#1821: MTN_HDQ  aprq2 pe 21 d
destination undefined

2008-08-12 07:03:40 command failed

#1821: Request Completed.

#1822: MTN_HDQ avrm3 nl d
network link display

module id: 489
local         remote                  local         remote
pi po status pi po    MID   H-ID     pi po status pi po    MID   H
             /proc   /RID                         /proc   /RID
13  1   up    1  1     28  47530     27  1   up    2  0     28  47

2008-08-12 09:16:26 command executed

#1822: Request Completed.
```

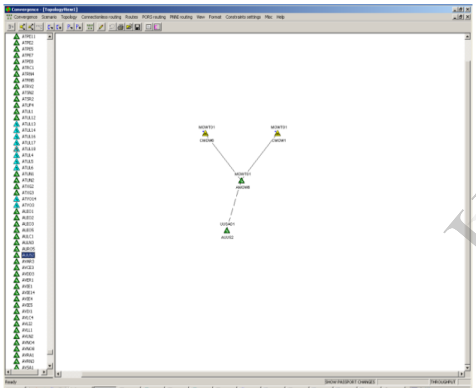
```
#1811(ok) : MTN_HDQ aprq2 pe 21 d
#1812(ok) : MTN_HDQ aprq2 pe 21 disable
#1813(ok) : MTN_HDQ aprq2 pe 21 d
#1814(ok) : MTN_HDQ aprq2 pe 21 d
#1815(ok) : MTN_HDQ aprq2 pe 21 d
#1816(ok) : MTN_HDQ aprq2 pe 21 ena
#1817(ok) : MTN_HDQ aprq2 pe 21 d
#1818(ok) : MTN_HDQ aprq2 pe 21 d
```

```
#2662: GROUPALL  cvrm1 d lp/7 v35/2
Lp/7 V35/2
   snmpOperStatus = up
   adminState      = unlocked
   operationalState = enabled
   usageState       = busy
   availabilityStatus =
   proceduralStatus   =
   controlStatus      =
   alarmStatus        =
   standbyStatus      = notSet
   unknownStatus      = false
   actualLineMode     = dte
   lineState          = rfs dsr dcd rts
   actualTxLineSpeed  = 252000 bit/s
   actualRxLineSpeed  = 252000 bit/s
   dataXferStateChanges = 7
ok              2008-08-12 06:36:33.63

#2662: Request Completed.

#2663: GROUPALL  cvrm1 d-p lp/7 v35/2
Lp/7 V35/2
   customerIdentifier = 0
   linkMode             = dte
   readyLineState     = rfs dsr dcd rts
   dataTransferLineState = rfs dsr dcd rts
   lineStatusTimeOut      = 1000 msec
   lineSpeed              = 256000 bit/s
   clockingSource         = module
   dteDataClockSource     = fromDce
   enableDynamicSpeed     = no
   applicationFramerName = FrUni/72 Framer
   vendor                 = ""
   commentText            = ""
   ifAdminStatus          = up
   ifIndex                = 49
ok              2008-08-12 06:36:40.07

#2663: Request Completed.
```

```
#2656(ok) : GROUPALL cgnf5 d lp/1 sdh/0 path/0
#2657(ok) : GROUPALL cgnf5 d trk/*
#2658(ok) : GROUPALL cgnf5 d trk/* atm atm
#2659(ok) : GROUPALL cvrm1 d dpn/*
#2660(ok) : GROUPALL cvrm1 d -p dpn/11
#2661(ok) : GROUPALL cvrm1 d lp/7 *
#2662(ok) : GROUPALL cvrm1 d lp/7 v35/2
#2663(ok) : GROUPALL cvrm1 d-p lp/7 v35/2
```

Convergence- Convergence is a tool where we can see the topology of the MTN, AGN and IGN network. This is very useful tool for impact analysis. It displays all the devices along with their topology, as well as the link information. Also displays the SITE ID.

Fig 6 Convergence


Convergence - [TopologyView1]
Convergence Scenario Topology Connectionless routing Routes PORS routing PNNI routing View Format Constraints settings Misc Help
MOWT01
CMOW0
MOWT01
CMOW1
MOWT01
AMOW8
UUSA01
AUUS2

X. CONCLUSION

In this way pre-checks are performed on different nodes of the network, health of the devices is checked and the report is prepared. The Problem areas are monitored by the engineers and the problems are rectified. This ensures that the network remains problem- free and no interruption occurs during the events and hence forth avoiding the intrusion or least find the intrusion at an earlier stage.

XI. REFERENCES

[1] Interconnecting Cisco Network Devices Part 1(Second Edition)- Steve Mcquerry

[2] Cisco CCNA in 60 Days- Paul Williams Browning and Farai Tafa. (1 Oct 2012)

[3] Network Fundamentals: CCNA Exploration Companion Guide by Mark Dye, Rick McDonald and Antoon Rufi .(30 Dec 2011).

[4] Intrepid Digital Microwave, A New Approach to Bistatic Radar aNew Outdoor Perimeter Sensor Technology, October 2000,

[5] 34th Annual 2000 Camahan Conference **of** Security Technology.

[6] 28th Annual 1994 Camahan Conference **of** Security Technology.

[7] T. Kaiser, "When will smart antennas be ready for market? Part I", IEEE

[8] Signal Processing Mag., vol. 22, no. 2, pp. 87-92, Mar. 2005.

[9] Lal Chand Godara, Smart antennas, CRC Press Jan. 2004

[10] P.H.Lehne and M. Pettersen, "An overview of smart antenna technologyfor mobile communications systems", IEEE Communication Survey, vol.2, pp. 2-13 1999.

[11] Hsu, Y.P., Tsai, C. C., Autotuning for Fuzzy-PI control using geneticalgorithm, IECON96, pp602-607. 85

[12] N. Celik, M.F. Iskandar, "Genetic-Algorithm-Based Anenna ArrayDesign for a 60-GHz Hybrid Smart Antenna System", IEEE Antenna and Wireless Propagation Letters, vol. 7, pp.1536-1225, 2008.

[13] Z.Zhang, M.F.iskandar, Z.Yun, and A. Honst-Madsen, "Hybrid smartantenna system using directional elernents-Performance analysis in flat rayleigh fading." IEEE Trans. Antenna Propag., vol. 51, no. 10,pp.2926-2935, Oct. 2003.

[14] N.Celik, WKim, M.F.Demirkol, M.F.iskandar, and R. Emrick,"Implementation and experimental verification of hybrid smart-antenm beamforming algorithm." IEEE Antenna Wireless Propag. Lett., vol.5, pp.280-283, 2006.

[15] Y. Yashchyshyn, M. Piasecki, "Improved Model of Smart Antenna Controlled by Genetic Algorithm", CAD Systems in Microelectronics, 2001. CADSM 2001. Proceedings of the 6th International Conference. The Experience of Designing and Application of , pp.147-150, 2001.