RF Hacking Detection using Spectrum Scanning

Manjunath M
Assistant Professor, Dept. of ECE,
Brindavan College of Engineering,
Dwarakanagar, Baglur Road,
Bangalore - 560063, Karnataka, India,
manjuec043@gmail.com

G Venkatesha
Professor and HOD, Dept. of ECE,
Brindavan College of Engineering,
Dwarakanagar, Baglur Road,
Bangalore - 560063, Karnataka,
hodece@brindavancollege.com

Dinesh S
Associate Professor & HOD, Dept. of
ISE, Brindavan College of
Engineering, Dwarakanagar, Baglur
Road, Bangalore - 560063, Karnataka,
hodise@brindavancollege.com

Abstract: Many wireless communication links quickly hop between narrow frequency channels. Many such connections can occur simultaneously in the same band and hop in a standard pseudorandom frequency pattern dwelling a predetermined time in each channel. To sense modern communication, a real-time spectrum analyser is very useful. One large advantage of real time analysis is that it only records data in active channels because it can determine the activity in each time interval. Another advantage is that communication that is not adhering to FCC standards can also be discerned. A van full of RF amplifiers, digitizers, and Fourier analysis equipment has been used for this job in non-real time. We chose to attack this design by providing many identical signal paths, one for each frequency channel. A number of RF components had to be developed to make this circuit power efficient and fit a small footprint. The initial broad band signal from an antenna sees Low Noise Amplification (LNA) and then is divided into many identical RF signal paths using Silicon Germanium integrated circuits (SiGe RFICs). Each of these RF signals is filtered by one filter in a ladder of frequency adjacent SAW filters. The output of each SAW device is compared with the RF power seen in the previous time interval to see if there is less or more of a signal. Up to this point the system has been low-power analog. Once the RF channel powers are quantified, the system uses a digital signal processor (DSP) to further analyse signal characteristics.

Keywords: Antenna; RF, Spectrum; IDS; Distribution; Intrusion; Prevention.

I. INTRODUCTION

Considering the rise in use of technology by the criminal groups like militants, smugglers, naxalates and other such antisocial groups, it has become more difficult to monitor, track and prevent the antisocial activities of such organizations. If this trend is not controlled on time, it may lead to a nationwide disaster and threat to national safety. So, it is very essential to have a system which can automatically monitor the possible unauthorized means of communication using RF communication.

As the other ways of communication monitoring like telephone tapping, Email scanning, chat room monitoring are already implemented and adopted by National security agencies, there arises a need to scan and monitor other means of communication like RF communication.

The project described here is a step towards easing out the job for RF monitoring authority involved in such RF scanning and monitoring projects. The project presented here, “RF Hacking Detection Using Spectrum Scanning“ is a perfect tool for easing the job of such security agencies. Basically this project is an automatic system, which is designed to monitor the chosen area for an unauthorized RF Spectrum utilization. So typically, the project will be set to scan mode round the clock, and when it intercepts an unauthorized RF activity in that area, it stops scanning and alerts the operator to keep track of the communication it has detected. Further the project also starts recording the communication with the aid of a tape recorder so that one can decode that communication and retrieve meaningful information about the anti-social organizations.

II. METHODOLOGY

The circuit consists of an antenna array for picking up RF signals. Each antenna is connected to a RF receiver. Here the signals picked up by the antenna are amplified and detected. Outputs of the RF receiver are fed to respective Band Pass Filters for filtering out the unwanted signals. Further for the isolation of noise and unwanted signals in the output from the respective radio receiver, an opto-coupler is used with the each RF Receiver. Opto-coupler device provides a cleaner RF free output for the next stage. Filtered output from each band pass filter is multiplexed into a single stream signal using an encoder. Analogue output of the encoder is converted to digital data using an A/D converter. Digitized data is passed on to the I/O interfacing card of the PC via a Signal Data Converter. Buffer is used for isolation of the PC from the rest of the circuit. Strength of the RF signals present in the surroundings is displayed on the monitor of the PC. Using this data, engineers can plan their project.

In addition to displaying the signal strength on the PC screen this system will also drive the rotors of the antennae so as to adjust their position to maximum signal strength. Output of the buffer is applied to the driver stage which is responsible for driving additional device drivers. Additional device drivers will drive the rotors of the antennae.

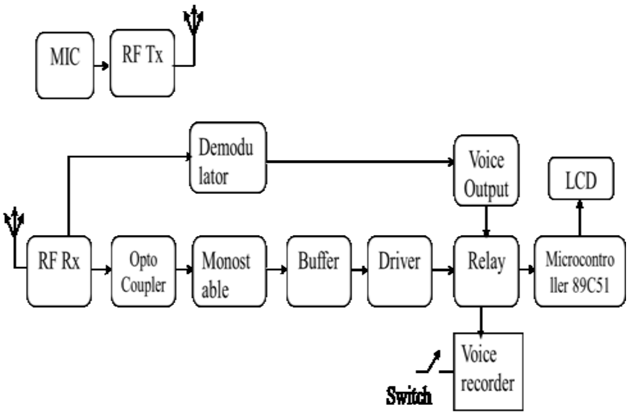

Fig 1. Block diagram

III. INTRUSION DETECTION SYSTEM (IDS)

An Intrusion detection system (IDS) is hardware and/or software designed to sense redundant attempts at accessing, manipulating, and/or disabling of computer through a network, such as the Internet. These attempts may take the variety of attacks like crackers, malware and/or dissatisfied employees. IDS indirectly detect attacks within properly encrypted traffic. An intrusion detection system is used to detect several types of malicious behavior that can give and take the security and trust of a computer system. This affected network attacks against data determined attacks on applications, host based attacks such as unauthorized logins and access to sensitive files, privilege escalation, vulnerable services and viruses. This refers to the collaboration degree of IDS agents on the monitored system. Based on the IDS architecture, we distinguish between autonomous and distributed Intrusion Detection systems.

1) *Autonomous IDS*: In autonomous IDS architecture, each network node operates independently/separately and is responsible for detecting attacks, there is no interaction between the nodes of the network. This architecture is more suitable for the flat networks than multi-layered networks.

2) *Distributed IDS*: It comprises a number of the network nodes which are responsible for collecting local audit data independently and then collaboratively examine it in a broader range in order to carry out a global Intrusion Detection System. This architecture is appropriate for flat networks and also for multilayered networks.

IV. DETECTION METHODS

The majority of intrusion prevention systems utilize one of three detection methods: signature-based, statistical anomaly-based and stateful protocol analysis. [3-7]

1) *Signature-Based Detection*: This method of detection utilizes signatures, which are attack patterns that are preconfigured and predetermined. A signature-based intrusion prevention system monitors the network traffic for matches to these signatures. Once a match is found the intrusion prevention system takes the appropriate action. Signatures can be exploit-based or vulnerability-based. Exploit-based signatures analyze patterns appearing in exploits being protected against, while vulnerability-based signatures analyze vulnerabilities in a program, its execution, and conditions needed to exploit said vulnerability.

2) *Statistical anomaly-based detection*: This method of detection baselines performance of average network traffic conditions. After a baseline is created, the system intermittently samples network traffic, using statistical analysis to compare the sample to the set baseline. If the activity is outside the baseline parameters, the intrusion prevention system takes the appropriate action.

3) *Stateful Protocol Analysis Detection*: This method identifies deviations of protocol states by comparing observed events with “predetermined profiles of generally accepted definitions of benign activity.”[3]

V. REQUIREMENTS OF IDS

Any IDS should discover a considerable share of intrusions into the supervised system, whereas keeping the warning rate at a suitable level at a lower cost. It's expected that a perfect IDS is likely to support many of the subsequent needs :

1) The IDS must not introduce a brand new weakness infrastructure. In the painter. That is, the IDS itself ought to not build a node weaker than it already is.

2) Associate in Nursing IDS ought to run ceaselessly and stay transparent to the system and users.

3) The IDS ought to use very little system resources as potential to observe and stop intrusions. IDS that needs excessive communication among nodes or run advance algorithms square measure not fascinating.

4) It should be fault-tolerant with in the sense that it must be ready to pass though system crashes, hopefully recover to the previous state, and resume the operations before the crash.

5) Excluding sleuthing and responding to intrusions, associate in Nursing IDS ought to conjointly resist subversion. It should monitor itself and observe if it's been compromised by the associate in Nursing offender.

6) Associate in Nursing IDS ought to have a correct response. In other words, Associate in Nursing IDS must not solely observe but conjointly answer detected intrusions, preferably while not human intervention.

7) Accuracy of the IDS is another major consider MANETs. Fewer false positives and false negatives square measure desired

VI. INTRUSION PREVENTION SYSTEM

Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about said activity, attempt to block/stop activity, and report activity. [1] Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity.

The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected. [2][3] More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address. [4] An IPS can also correct Cyclic Redundancy Check (CRC) errors, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options. [2], [5].

- *Classifications*: Intrusion prevention systems can be classified into four different types:[1][6]
- *Network-based intrusion prevention system (NIPS)*: Monitors the entire network for suspicious traffic by analyzing protocol activity.
- *Wireless intrusion prevention systems (WIPS)*: Monitor a wireless network for suspicious traffic by analyzing wireless networking protocols.
- *Network behavior analysis (NBA)*: Examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware and policy violations. Host-based intrusion prevention system (HIPS): An installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.

VII. METHOD OF INTRUSION

For analog stations it is relatively easy to break into the transmission network. All that is needed is to determine the frequency used in the studio-to-transmitter link, then generate a higher-powered signal at the same frequency from a position near the broadcast transmitter site, essentially jamming the original signal. The input stage of a cheap video sender can produce the right kind of signal. A low-power microwave signal generator or a homemade equivalent from easily available components provides the signal (which is pointed at the receiving dish antenna). Most larger stations encrypt their signal, in which case one would just jam the signal, as is the case with digital. Most TV and radio stations are extremely vulnerable, but lack of knowledge has kept this from being a problem.

VIII. FLOW CHART

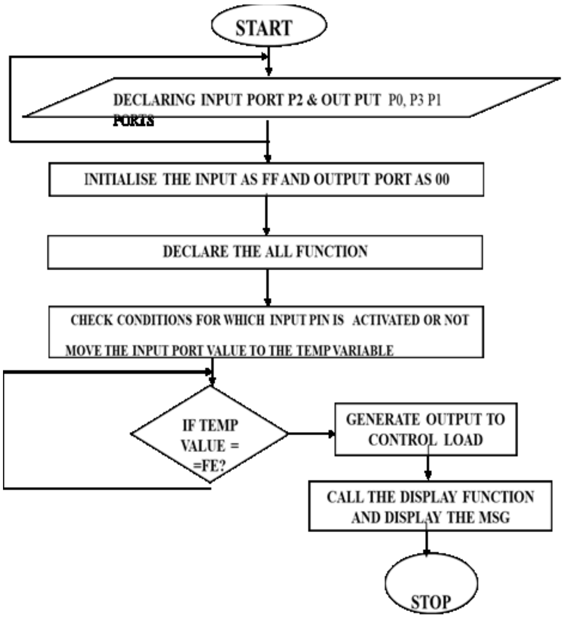
START
DECLARING INPUT PORT P2 & OUT PUT P0, P3 P1 PORTS
INITIALISE THE INPUT AS FF AND OUTPUT PORT AS 00
DECLARE THE ALL FUNCTION
CHECK CONDITIONS FOR WHICH INPUT PIN IS ACTIVATED OR NOT
MOVE THE INPUT PORT VALUE TO THE TEMP VARIABLE
IF TEMP VALUE = =FE?
GENERATE OUTPUT TO CONTROL LOAD
CALL THE DISPLAY FUNCTION AND DISPLAY THE MSG
STOP

Fig 2. Flowchart

IX. APPLICATIONS

This project is an excellent system to detect the illegal/unauthorized RF communication network, like terrorists, smugglers and other antisocial elements. This system can be used to find the strength of the RF signals at any particular area, so that RF strength and spectrum can be analyzed and studied. RF strength meter is used in establishing radio stations, pager stations etc. This project can be used to detect and record the communication which may cause potential threat to the nation.

X. CONCLUSION

If this technology can be put into practical use , we can avoid anti-social activities and nationwide disasters. So it is very useful to have a system which can automatically monitor the possible unauthorized/illegal means of communication using RF communication.

REFERENCES

[1] "NIST – Guide to Intrusion Detection and Prevention Systems (IDPS)" (http:/ / csrc. nist. gov/ publications/ nistpubs/ 800-94/ SP800-94. pdf). 2007-02. . Retrieved 2010-06-25.

[2] Robert C. Newman (19 February 2009). Computer Security: Protecting Digital Resources (http:/ / books. google. com/ books?id=RgSBGXKXuzsC& pg=PA273). Jones & Bartlett Learning. pp. 273–. ISBN 978-0-7637-5994-0. . Retrieved 25 June 2010.

[3] M. Sabah, A. N, M. M, and S. Rupanagudi, "Real Time Rear Vehicle Monitoring & Detection System", pices, vol. 1, no. 12, pp. 187-192, Apr. 2018.

[4] M. Manjunath, "Biorthognal, Symlet & Discrete Meyer Wavelet Based Palm Print Recognition System", pices, vol. 2, no. 7, pp. 319-323, Nov. 2018.

[5] Harold F. Tipton; Micki Krause (2007). Information Security Management Handbook (http:/ / books. google. com/ books?id=B0Lwc6ZEQhcC& pg=PA1000). CRC Press. pp. 1000–. ISBN 978-1-4200-1358-0. . Retrieved 29 June 2010.

[6] John R. Vacca (2010). Managing Information Security (http:/ / books. google. com/ books?id=uwKkb-kpmksC& pg=PA137). Syngress. pp. 137–. ISBN 978-1-59749-533-2. . Retrieved 29 June 2010.

[7] Engin Kirda; Somesh Jha; Davide Balzarotti (2009). Recent Advances in Intrusion Detection: 12th International Symposium, RAID 2009, Saint-Malo, France, September 23–25, 2009, Proceedings (http:/ / books. google. com/ books?id=DVuQbKQM3UwC& pg=PA162). Springer. pp. 162–. ISBN 978-3-642-04341-3. . Retrieved 29 June 2010.

[8] D. S, V. G, and M. M, "An Efficient Approach using Visual Display Matrix Computation for Smart Object Detection", pices, vol. 2, no. 9, pp. 338-341, Jan. 2019.

[9] M. M and H. Kulkarni, "Analysis of Unimodal and Multimodal Biometric System using Iris and Fingerprint", pices, vol. 2, no. 8, pp. 333-337, Dec. 2018.