Review Paper on RF Interference in Armed Forces, SES, BPSMV

Savita Kumari

School of Engineering and Sciences, BPSMV Khanpur Kalan -131306

Email:savi4system@gmail.com

Abstract

This paper gives a review, regarding India's national security. India has some neighboring countries, due to which security in border area is a big concern. Security system has become an important component in Indian defense. Attacks like 26/11, are the tragic events in terms of security is concerned. Due to lack of security analysis, the incident took place and shook the nation badly. As there were broken clues but no perfect figures were there to relate the incident. These are the intruders, who intercept the information communicated between different people working in a system. So the information is intercepted by outsiders, the problem areas so far, developments done in this field and the work that has been done to make the security system strong and reliable so far are expressed here.

Keywords-Educational Broadband Service (EBS),Broadband Radio Service (BRS), Radio-frequency interference (RFI), Advanced Microwave Scanning Radiometer(AMSR), Electronic order of battle (EOB).

1. Introduction

There are several ways of intercepting the information while communicating. Any intruder can intentionally intercept through any cable, wire, oral, radio or electronic communication and intercept the information. Information security is the process of protecting information, it protects the availability, privacy and integrity[1].The frequency hopping interceptors are special advanced reconnaissance; wide band receivers capable of simultaneously tracking a large number of frequencies hopping encrypt information, even in high background noise environment[2]. There are recent activity of Indian navy has shown the strength of security system, that has been increased, when they intercepted suspicious Pakistani boat on early morning of 1st Jan 2015. 4 people occupants were killed after a confrontation with the coast guard in Indian waters .The boat was carrying massive explosives. "Finding a small boat in the sea is like looking for a needle in a haystack" [3].

This review paper describes an investigation into, and solutions for, radio frequency interference to radars from communication systems operating in another band, specifically interference from licensed radio communications stations in the (BRS) and the (EBS) into Federal radar receivers above 2700 MHz[8]. Commanders and their subordinates throughout the Department of the Navy use the facilities of naval communications as a primary method of communicating. Naval communications relies on top performance from all of its assigned personnel. Reliable, secure, and timely transmission and receipt of

information, based on wartime requirements, is the ultimate goal [11].

Radiotelephone is one of the most useful military communications methods. Because of its directness, convenience, and ease of operation, radiotelephone is used by ships, aircraft, and shore stations. It has many applications and is used for ship-to-shore, shore-to-ship, ship-to-ship, air-to-ship, ship-to-air, air-to-ground, and ground-to-air communications [11].

2. Security Advancement

2.1 Physical security
2.2 Intelligent video surveillance system
2.3 Alarms and their managements
2.4 Artificial intelligence video surveillance
2.5 Computer security
2.6 Door security
2.7 Information security
2.8 Logical security

To avoid collisions and wasting of time on retransmissions, the system should be able to sense the spectrum for possible interference and exploit the spectrum in an intelligent way [4].

Radio-frequency interference (RFI) in the space borne multichannel radiometer data of Wind Sat and the (AMSR) is currently being detected using a spectral difference technique. Such a technique does not explicitly utilize multichannel correlations of radiometer data, which are key information in separating (RFI) from natural radiations. Furthermore, it is not optimal for radiometer data observed over ocean regions due to the inherent large natural variability of spectral difference over ocean [10].

3. Interference Mechanisms

Radio frequency interference at a shared site is typically caused by one of the following: mechanisms that have their origin in some form of equipment or other non-linearity: Inter modulation, Transmitter, Receiver, Passive, Out-of-band emissions, Transmitter noise, Transmitter spurious emissions, Transmitter harmonics, Receiver spurious emissions, Other effect, Receiver desensitization[9].

4. Taping/Intercepting

There is a simple process of putting extra load on a wired network where voices travel making the loops .the extra load in the form of other phone, tapper listens the conversation. Radio interception: intruders use scanners/radio scanners which can basically operate in multiple frequencies .they program scanner search devices which are working between two frequencies and receive voices in scanners microphone [12].

.

4.1 Problems faced while intercepting:

4.1.1 Intercept points can't be directly measured.
4.1.2 No valid distortion curves as receiver approaching overload.
4.1.3 Values sometimes are frequency dependent.
4.1.4 Distortion slopes are not perfect

5. Background and Development

5.1.1 There are several correction requirements in the signal systems.
5.1.2 Need for multiple receivers which should be coordinated.
5.1.3 Intercept management.
5.1.4 Counter measure to interception.
5.1.5 Finding the direction.
5.1.6 Analysis of traffic.
5.1.7 (EOB)

6. FRRS-SCS-TACDB-BEI-EC/S

6.1 Network builds up
6.2 Data fusion
6.3 Signal separation.

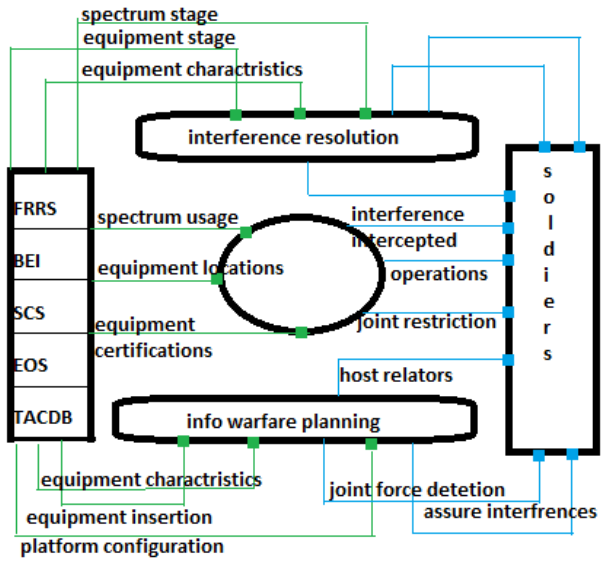

Fig1: Interference

7. Signal Intelligence

Signal intelligence plays the crucial role in air operations and technology, today intelligence data is directly passed to fighters via a secure data link in the cockpit on a "heads up" display [5].(SIGINT) is the primary means of collecting immediate threat warning and updates on targets. SIGINT is made up of two components, electronic intelligence (ELINT) and communications intelligence (COMINT). ELINT is information on enemy threats and capabilities of systems such as radars, surface-to-air missile systems, and non-voice data-links. It also provides accurate location information. It is however susceptible to deception and suffers from only being able to intercept signals on a line of sight. COMINT provides information on enemy intentions and assists in determining the enemy command and control structure. A SIGINT operation to tactical military commanders includes a dynamic update capability during the execution phase of military operations, especially in direct support to combat aircraft [5].

8. Voice Interception

The basic technique is to listen for communications if else is encrypted. The analysis of traffic still given the information.

9. Text Interception

Each every person has different voice due to different vocal chords, vocal cavity and oral cavities is specific to the individual [6]. Spectrographs are basically used to record sound of person with magnetic disks. Then the sound is amplified. After that sound is passed via frequency analyzer .This is actually measurement of air vibrate as sound wave pass them [6]. After converting signals into electrical signals, it's recorded on drum. And finally the voice is analyzed or we can say matched to the person.

10. Analyzing Interference.

10.1 Detection
10.2 Identification and location

We can first find the location of interference. Since it is a lengthy process which is based on the directional testing at different positions, by finding the intersection area we can locate the intruder.

11. Preamplifiers

11.1 Attenuation
11.2 Minimum and maximum traces
11.3 Frequency span
11.4 Resolution bandwidth,
11.5 Echolocation [7].

12. Improvements

12.1Sensitivity (covering instruments resolution bandwidth)

12.2 Eliminating trace noise (narrowing video bandwidth filter) Charactizing minimum and maximum power tests properly.

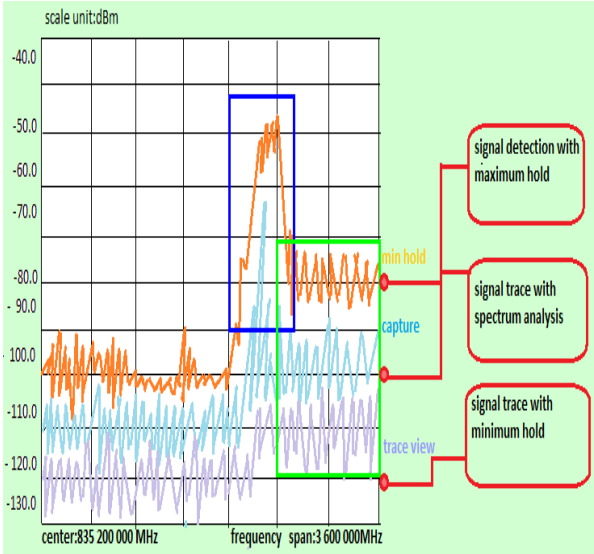

Fig2: spectrum analysis- over the air

13. TDD (time division duplex)

Interference detection in TDD signals is made for domain analysis with gate sweep testing enabling time control uplink interference detection.

14. Intermittent Signals

15.1 Long treatment
15.2 Intermittent interference
15.3Interference analysis

15. Conclusion

RF interference is a great challenge due to the growing number of transmitter internal devices and externals elements that can greater interference so automated should be done. Systematic test approach of detection location and identification needed. Reduction in the maintain time. The whole process is done to secure the privacy of the armed forces, and its needs to be advanced. Spacing between antennas at radio sites depends on the configuration of each individual site. In many cases only the physical dimensions of the antennas dictate the antenna spacing requirements. However, without detailed information on the site, and use of sophisticated analysis software, it is difficult to know when significant spacing is needed, and even more difficult to know how what the minimum spacing requirements are, particularly on antenna sites with many collocated systems.

REFRENCES

Captain Gillies Van Nederveen, “Signal Intelligence Support To The Cockpit” College of Aerospace Doctrine, Research, and Education Airpower Research Institute 401 Chennault Circle Maxwell AFB, AL 36112-6428.

Defense information services agency, “http//en.wikipeddia.org/wiki/files:JSC-Databases-and-Flow.GIF”,Oct2007.

Eduardo Inzunza, “Detecting ,Identifying and locating RF Interference”,RF Test Business Devlopment, retrived from http://www.youtube.com/watch?v=j2013.

Frank H. Sanders Robert L. Sole John E. Carroll Glenn S. Secrest T. Lynn Allmon. Analysis and Resolution of RF Interference to Radars Operating in the Band 2700–2900 MHz from Broadband Communication Transmitters.

Kiran Yadvelli, Bhaskar Krishnamchari, Sharmila Ravula ,Bhaskar Srinivasan, “Ecolocation:A Sequence Based Technique For RF Localization In Wireless Sensor Network, ∗Department of Electrical Engineering - Systems University of Southern California, Los Angeles, CA.

NAVEDTRA 14189, Navy Electricity and Electronics Training Series Module 17—Radio-Frequency Communications Principles.

Pranesh Parmar, Udayabhanu R, "review research paper :Voice Fingerprinting :A Very Important Tool Against Crime",March 2012,vol 34,no.1.

Quasim Nauman and vibhuti Agarwal, "India Intercepts Suspicious Pakistani Boat",Jan 2015.

Robert S. Mawrey, Radio Frequency Interference and Antenna Sites *How much spacing to you really need between antennas at radio sites?* Ph.D. Vice President of Systems and Technology.

Venik, "How Military Radio Communications Are Intercepted?",March 2003.

VishwaGupta, Gajendra Singh, Ravindra Gupta, "International Journal Of Advanced Research In Computer Science and Software Engineering:Advanced Cryptography Algorithm For Improving Data Security",2012,volume 2,issue 1.

Weng,Z.;Orlik,Kim,K.J., "Classification Of Wireless Interference On 2.4 GHz Spectrum",April 2014.

WindSat Radio-Frequency Interference Signature and Its Identification Over Land and Ocean L. Li, *Member, IEEE*, Peter W. Gaiser, *Senior Member, IEEE*, Michael H. Bettenhausen, *Member, IEEE*, and William Johnston.

.