Overview of Security Risk in Satellite Communication and their Possible Solutions

Tarun Varma[1] Dr. Akhilesh R. Upadhyay[2]
[1]Research Scholar [2]Director
[1]Department of Electronic and Communication Engineering
[1]Mewar University, Raj [2]SIRTS Bhopal(MP)

Abstract— Performance of satellite communication under security risk and its possible solution are presented in this paper. Risk analysis is a four step process that includes; threat assessment, vulnerability assessment, impact assessment, and risk mitigation.The top five risks associated with satellite communications systems can be identified as Meaconing, Intrusion, Jamming, Interference, (MIJI) and physical security. Meaconing is the interception and rebroadcast of signals to confuse communications between organizations. Intrusion in the penetration of the system using processes such as hacking or cracking. Jamming is a technique of preventing RF signals from reaching their destination. Interference caused by the generation of noise or atmospheric conditions makes it difficult to send intelligible message traffic. Electromagnetic Interference (EMI) hardening must considered a high risk item. RF broadcasts directed at the system can damage equipment and disrupt communications. The possible solution are to prevent these security risks are Anti-jamming Communication without Shared Secrets, for these is one solution another is Uncoordinated Spread-Spectrum Techniques, Detection of Reactive Jamming, Error-correcting codes of reliable transmission of information on a noisy channel detecting unknown intrusion using abstract signatures, Diversity Techniques for Broadband Wireless Communications etc.[1][2][3][4].

Key words: Meaconing, interference, jamming, Intrusion. Spoofing, etc

I. Introduction

Existing Global Navigation Satellite Systems offer no authentication to the open service signals and so stand-alone receivers are vulnerable to meaconing and spoofing attacks. These attacks interfere with the integrity and authenticity of satellite signals: they can delay signals, or re-broadcast signals. Positioning is thus compromised and location-based services are at risk. The risk is the probability that a particular threat will exploit a particular vulnerability. Threats can be broken down into three common threat sources, natural, human and environmental. Natural threats would be floods, earthquakes, electrical storms, or atmospheric in nature. Human threats both unintentional and intentional are enabled or caused by humans. Unintentional or human error threats to examine would be inadvertent data entry, configuration changes, or data programming errors. MIJI threats are more difficult to mitigate is physical security is not kept under control. Strict inventory control and tracking of these assets are extremely important. Minimal requirements it's helpful to consider that SATCOM's main purpose/goal is to provide assured communications to/from anywhere in the world, even in areas without communications infrastructure, in order to support the military mission. For protected communications,(modulation/coding/encryption), Robust system/network control Basically these can be categorized as requirements for avoidance and/or robustness against the threat. Jamming-resistant communication is crucial for safety-critical applications such as emergency alert broadcasts or the dissemination of navigation signals in adversarial settings. In such applications, mission-critical messages are broadcast to a large and unknown number of (potentially untrusted) receivers that rely on the availability, integrity, and authenticity of the messages; here, availability primarily refers to the ability to communicate in the presence of jamming.[1][2][3][4][5]

II. Techniques to prevent MIJI

- Anti-jamming Communication without Shared Secrets by Uncoordinated Frequency Hopping Communication.
- Detection of Reactive Jamming.
- Error-correcting codes of reliable transmission of information on a noisy channel.
- Diversity Techniques for Broadband Wireless Communications.
- Detecting unknown Intrusion using abstract signatures.
- Intrusion detection by Hidden Markov model
- Spoofing detection using Receiver Autonomous Integrity Monitoring (RAIM) method
- Spoofing detection by Consistency Cross Check with Other Navigation Systems
- Spoofing detection by Time of Arrival (TOA) Methods
- Spoofing detection using Navigation Message Analysis
- Spoofing detection Correlation Peak Monitoring
- Spatial Discrimination of Spoofing Signals
- Spoofing detection by Power Based

III. Anti-jamming Communication without Shared Secrets by Uncoordinated Spread-Spectrum Techniques

In a Frequency Hopping Spread Spectrum (FHSS) system the sender and the receiver rapidly switch the carrier frequencies of their radio transceivers among a (large) set of frequency channels according to a random hopping sequence. In the case of common, coordinated frequency hopping, this sequence is known to the sender and the receiver and is typically generated by means of a pseudo-random generator which was seeded with a shared secret key. The two main advantages of FHSS communication compared to single carrier communication are a high resistance to (narrowband) interference and a reduced probability of interception. FHSS communication can further be divided into fast frequency hopping and slow frequency hopping, based on the number of bits sent per

hop. The hopping is called fast if there are multiple frequency hops per bit transmission and is called slow if there are multiple bit transmissions per frequency hop. In both cases, the jamming resistance of the scheme is usually expressed by the achieved processing gain, given by the ratio of the width of the whole frequency band in which the channels are located to the bandwith of a single channel. If the channels are orthogonal (i.e., do not overlap) the processing gain is equal to the number of channels among which the sender and the receiver hop. **[6][7]**

A. *Uncoordinated Frequency Hopping*

With UFH, the sender and receiver hop among a set of known frequency channels in an uncoordinated and random manner. Information is transferred whenever the receiver happens to listen on the same frequency channel on which the sender is currently transmitting. In order for (coordinated or uncoordinated slow) frequency hopping to be effective against jamming, the time slots during which the sender is transmitting on a specific channel must be kept short (i.e., at most a few hundred bits). Messagesin particular if they are authenticated—thus do typically not fit into the sender's short transmission slots and are split into fragments by the sender and reassembled by the receiver. After the fragmentation, the sender encapsulates each fragment into a packet, encodes the packets with error correcting codes, and repetitively transmits the encoded packets one after another on randomly chosen frequency channels. Receiving a fragment with (coordinated or uncoordinated) frequency hopping requires the receiver to listen on the correct channel for the complete transmission of the fragment. If the sender's and receiver's hopping frequencies were identical (and with it the time that both stay on a channel before hopping to the next), the successful transmission of a fragment would require precisely synchronized transmission and reception slots to avoid partially received fragments. In UFH, we do not require the slots to be synchronized by permitting the receiver to switch the channels less often than the sender, thus reducing the number of partially received fragments.[8][9][10][11]

B. *UFH-based Communication Schemes*

For a given message size j*M*j (determined by the application) and a size *s* of the frequency hopping slots (usually given by the hopping rate of the radio device), the throughput/latency of UFH communication depends not only on the probability that a packet sent by the sender is successfully received by the receiver but also on the number of packets that the receiver must receive to reconstruct the message.[9][10][11][23]

IV. Error-correcting codes of reliable transmission of information on a noisy channel

A. *Reed-Solomon codes*

Reed-Solomon codes are an extremely important and well-studied family of linear codes. They are based on the properties of univariate polynomials over infite felds.

B. *Reed-Muller codes*

Reed-Muller codes are a generalization of Reed-Solomon codes obtained by taking for message space all `-variate polynomials over some finite field equation with total degree at most m, subject to the condition that no variable takes on a degree of q or more.

C. *Hadamard codes*

Of special interest are Reed-Muller codes of order 1, i.e., codes based on multilinear polynomials, also known as simplex codes. A variant of these, based on homogeneous polynomials with no constant term, are commonly referred to as Hadamard codes.

D. *Algebraic-geometric codes*

Algebraic-geometric codes (or AG-codes, for short) are also a generalization of Reed-Solomon codes. Reed-Solomon codes may be viewed as evaluations of certain functions at a subset S of points on the projective line over the functions are those that have a bounded number of poles at a certain point that is designated as the point at infinity and no poles elsewhere (this corresponds precisely to low-degree polynomials), and the code can be defined based on any subset S of points that does not include the point at infinity

E. *Concatenated codes*

The big advantage of concatenated codes for us is that we can get a good list decodable code over a small alphabet (say, binary codes) based on a good list decodable outer code (like a Reed-Solomon or AG-code) and a suitable binary inner code.[17][22][21]

V. Diversity techniques

Diversity technique is used to decreased the fading effect and improve system performance in fading channels. In this method, we obtain L copies of desired signal through M different channels instead of transmitting and receiving the desired signal through one channel. The main idea here is that some the signal may undergo fading channel but some other signal may not. While some signal might undergo deep fade, we may still be able to obtain enough energy to make right decision on the transmitted symbol from other signals.[18][25] There is a number of different diversity which is commonly employed in wireless communication systems. Some of them are following:

- Multipath/frequency diversity
- Spatial/space diversity
- Temporal/time diversity
- Polarization diversity
- Angle diversity
- Antenna diversity

VI. Intrusion detection by Hidden Markov model

Intrusion detection is the art of detecting inappropriate, incorrect, or anomalous activities. There are two types of Intrusion Detection Systems (IDSs) such as: misuse detection systems and anomaly detection systems. When used in a wireless system, IDS is designed to capture the malicious use of available services so that it protects availability and security for legitimate users. Several intrusion detection technologies such as calling patterns on application layer, Radio Frequency Fingerprinting (RFF) on physic layer, and detection on the network layer are designed to protect wireless networks. As a complement to the above technologies, employing User Mobility (UM) profiling, this thesis addresses the following open question:

how to identify abnormal users efficiently with low false alarm rate in the anomaly detection system.

This thesis provides a feasible solution to this question with two classification frameworks, Instance Based Learning (IBL) and Hidden Markov Models (HMMs). It also describes details of design and implementation of the frameworks. The performance of two frameworks were evaluated by simulating the IBL with location data, and the HMMs with both location data and other mobility features (e.g., transmission time, speed, and course). The True Detection Rate (TDR), True Acceptance Rate (TAR), and False Detection Rate (FDR) were examined. The IBL framework has better success rate and is easy to implement. The HMMs framework could produce precise results if it has enough data from profiled users. Moreover, this thesis analyzes a performance of the true detection rate and false alarm rate with authentic UM position data and other related mobility features.[18][19][24]

VII. CONCEPT OF ABSTRACT SIGNATURES TO IMPROVE DETECTION SYSTEM

Intrusion detection systems have to process incoming events at a very high speed to be able to detect all attacks against a system. Current intrusion detection systems compare incoming events in a serial way with the signatures, which results in a performance decrease when more signatures are used for detection. In the first part of this dissertation we present a new of way of processing events which applies clustering algorithms for parallelizing the task of comparing events to signatures. The clustering algorithm is used for finding signatures with commonalities which are then used for constructing a decision tree, that can then be used for efficient event processing. The worst-case timing behavior can be improved using this approach which makes decision-tree based systems more resistant against denial-of-services attacks. The approach has been implemented and evaluated on the open-source intrusion detection system Snort. The concept of abstract signatures is introduced, The concept of abstract signatures tackle the problem of signature-based intrusion detection systems that they cannot detect attacks that have not been modeled previously, i.e., for which a signature has been created. This is true even in the case that an attack is just a modification of an existing class of attacks. The defenders of networks therefore are always in disadvantage compared to attackers. Abstract signatures represent a whole attack-class by specifying the similarities of the instances of an attack- class. This enables abstract signatures to detect variations of existing attacks.[20][26]

VIII. CONCLUSION

In this paper, we addressed the problem of security risk in satellite communication, broadcast communication among entities that do not share secret keys. We proposed solutions for the MIJI to a group of (partially) unknown or potentially malicious receivers and for the bootstrapping of conventional anti jamming communication. Our solutions are based on uncoordinated spread spectrum communication, a novel class of anti-jamming techniques that does not rely on shared secrets, coding techniques, Intrusion improvement techn- -ique etc.

REFERENCES

[1] Thomas A. Groshong Sr, "Satellite Communications System Security Risk Analysis",LHT_Task4_2011-06 20.docx
[2] Don Wilcoxson, "Advanced Commercial Satellite Systems Technology for Protected Communications" 987-1-4673-0080-3/11 2011 IEEE.
[3] Christina P¨opper, Mario Strasser, and Srdjan Capkun, "Anti-Jamming Broadcast Communication using Uncoordinated Spread Spectrum Techniques" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 28, NO. 5, JUNE 2010
[4] Vidal, G.Verelst, J.Lacan, E.Alberty, J.Radzik, and M.Bousquet, "Next Generation High Throughput Satellite System" First International Ieee-Aess Conferenc In Europe On Space And Satellite Telecommunications, Rome, 02-05 Oct 2012
[5] Junghwan Kim, Chong Wang, and Mike Orra, "Performance Analysis of SDPSK and 1-Bit Differential GMSK Modems for FFH-FDMA Satellite Communications Under Jamming" 978-1-4244-4148-8/09 2009 IEEE.
[6] Ioannis A. Chatzigeorgiou, Miguel R. D. Rodrigues, Ian J. Wassell and Rolando Carrasco," A Comparison of Convolutional and Turbo Coding Schemes For Broadband FWA Systems" 2009
[7] Jaroslav , Jiří, "New Channel Coding Methods for Satellite Communication" RADIO ENGINEERING, VOL. 19, NO. 1, APRIL 2010.
[8] P.Thompson, B.Evans, L.Castanet, M.Bousquet, T.Mathiopoulos " Concepts and Technologies for a Terabit/s Satellite", SATCOM 2011.
[9] B. Devillers, A.Pérez-Neire, "Advanced Interference Mitigation Techniques for the Forward Link of Multi-beam Broadband Satellite systems", SatNex III, 2011.
[10] Sastri L.Kota, "Broadband Satellite Network Trend and Challenges" 0-7803-8966-2/05 2005 IEEE.
[11] Yi an Huang and Wenke Lee. A cooperative intrusion detection system for ad hoc networks. In SASN '03: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pages 135-147, New York, NY, USA, 2003. ACM Press.
[12] J A. Boukerche and M.S. M. A. Notare. Applications of neural networks to mobile and wireless networks. In Biologically Inspired Solutions to Parallel and Distributed Computing, A. Zomaya(Ed-). Wiley, New York, 2001.
[13] Azzedine Boukerche and Mirela Sechi M. Annoni Notare. Behavior-based intrusion detection in mobile phone systems. J. Parallel Distrib. Comput., 62(9): 1476-1490, 2002
[14] William W. Cohen. Fast effective rule induction. In Armand Prieditis and Stuart Russell, editors, Proc. of the 12th International Conference .
[15] Mechanisms to Implement Intrusion Response, http://www.sdsc.edu/DOCT/ Publi- cations/e2/e2.html, August 1998.
[16] Antivirus approaches. www.cs.bvu.edu/courses/cs565/slides/Ch9.pdf, January 2003.
[17] A. Aho and M. Corasick. Efficient String Matching: An Aid to Bibliographic Search. Communications of the

Association for Computing Machinery, 18:333-340, 1975.
[18] Edward Amoroso. Intrusion Detection - An Introduction to Internet Surveillance, Correlation, Trace Back, and Response. Intrusion.Net Books, New Jersey, USA, 1999.
[19] D. Anderson, T. Frivold, A. Tamaru, and A. Valdes, Next Generation Intrusion Detection Expert System (NIDES). SRI International, 1994.
[20] M. Asaka, A. Taguchi, and S. Goto. The Implementation of IDA: An Intrusion Detection Agent System. In 11th FIRST Conference, June 1999.
[21] Stefan Axelsson. Intrusion Detection Systems: A Survey and Taxonomy. Technical Report 99-15, Chalmers Univ., March 2000.
[22] C. A. Carver, J. M. D. Hill, and U. W, Pooch. Limiting Uncertainty in Intrusion Response. In Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, June 2001.
[23] Curtis Carver. Intrusion Response Systems - A Survey, 2000.
[24] William R. Cheswick and Steven M. Bellovin, Firewalls and Internet Security. Addison-Weslev, Reading, Massachusetts, USA, 1994.
[25] Ids245 smtp-email-buffer-overflow, http://www.whitehats.com/info/IDS245, January 2001.
[26] F. Cohen. Simulating Cyber Attacks, Defenses, and Consequences, http://all.net/ journal/ntb/simulate/simulate.html, May 1999.
[27] C. Jason Coit, Stuart Staniford, and Joseph McAlernev. Towards Faster String Matching for Intrusion Detection or Exceeding the Speed of Snort. In Proceedings of DISCEX 2001, 2001.

