International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.07, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Performance Evaluation of Satellite Communication under Jamming Environment

Tarun Varma[1],Dr. Akhilesh R. Upadhyay[2]

[1]*Research scholar ECE,MewarUniversity,Raj.*

[2] *Director SIRTS Bhopal(MP)*

ABSTRACT

A major challenge in securing wireless applications and services is the inherent vulnerability of radio transmissions to communication jamming Denial-of-Service (DoS) attacks. This vulnerability gains in significance the more one takes the ubiquity of these applications and services for granted and becomes a crucial factor in the context of safety-critical applications. At best, failures of safety-critical systems can result in substantial financial damage at worst, in loss of life.We tackle the problem of how devices that do not share any secrets can establish a jamming-resistant communication over a wireless radio channel in the presence of a satellite communication jammer.[1] We address the dependency between anti-jamming spread-spectrum communication and pre-shared keys that is inherent to this problem, and propose Uncoordinated Frequency Hopping (UFH), a novel anti-jamming technique, as a solution to break this dependency. In particular, we illustrate how UFH enables the jamming-resistant execution of (group) key agreement protocols in order to bootstrap common (coordinated) frequency hopping. Prompted by this deficiency, we discuss alternative jamming mitigation techniques and present a novel jamming detection scheme to counter advanced (reactive single bit) jamming attacks. We also present reactive jamming We perform an evaluation of the proposed schemes and validate our findings analytically.[2] The results show that our solution effectively detects sophisticated jamming attacks and enables the formation of robust sensor networks for the dependable delivery of alarms messages.[1][2][3]

Keywords:-Jamming,frequency hopping, shared codes,UHF,radio channel

I.INTRODUCTION

There are three ways to counter communication jamming, jamming avoidance, jamming detection, and jamming mitigation.[3] The arguably most evident and most effective way is to avoid the jammer by moving out of its range or by switching to a different communication medium (such as a wire) that is not affected by the jamming. But in spite of its effectiveness, avoiding the jammer is almost never possible, most wireless applications and services must be available at a specific location and entirely replacing the wireless communication infrastructure with a wired one is hardly ever a feasible option. The efficiency of jamming detection and localization as a means to counter jamming heavily depends on what the network entities can cause with the obtained information, that is, on whether effective and immediate countermeasures (e.g., the quick

deactivation/destruction of the jammer) can be taken.[4] This limits the application of jamming detection to settings where physical intervention is possible or where no intermediate actions are required (i.e., where detection of the attacker is sufficient)[5].The third and most common measure against jamming is to mitigate its impact by means of anti-jamming communication techniques that can resist the attack. Possible mitigation techniques include highly directional antennas, forward error- correcting codes, and spread-spectrum communication. Common spread-spectrum anti-jamming communication such as frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS) enables the sender to spread a signal (in time and/or frequency) such that its transmission becomes unpredictable for the attacker. Provided that the attacker cannot physically isolate a device, her ability to alter or erase a message is restricted to interfering with the message transmission and is hence limited by the achieved processing gain of the spread-spectrum communication.[6][7]

II.IMPACT OF REACTIVE JAMMING AND MITIGATION STRATEGIES

Before we present our solution for the detection of reactive jamming, we first want to highlight the importance of such a detection scheme by demonstrating how a reactive jammer can block communication in current wireless sensor networks with minimal exposure. We additionally present two techniques based on forward error correction and limited node wiring, respectively, that help to alleviate the impact of jamming attacks but do not suffice to adequately counter them in practice.[8][9]

III. IMPACT OF REACTIVE JAMMING

In order to enable the jamming of single bits without having to use expensive hardware, the transmission rate of the sender and receiver was reduced. We then implemented the jammer using an additional BT node sending random data.If the jamming was targeted at the sync-byte, the jammed packet transmissions were not even recognized as such by the network stack and were thus completely ignored by the nodes and not counted as packet losses.[10][11]

As a first step towards a better jamming resistance, we introduce a technique that significantly increases the minimal duration during which the jammer must interfere with a packet to block it. In case of jamming mitigation technique that harnesses limited node wiring in the form of wired node chains to forward messages out of the jammed region. Although schemes present here help to diminish the impact of the jammer but they cannot entirely counter jamming attacks. In the absence of (broadband) anti-jamming communication, an effective jamming detection thus remains an essential countermeasure against such attacks.[2]

Uncoordinated Frequency HoppingCommunication

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. 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). Messages in 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.

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 bandwidth 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.[5]

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.[13]

IV.JAMMING DETECTION TECHNIQUES

There are three technique present as jammingresistance, which also consider reactive jamming, Anti-jamming Communication without Shared Secrets,Robust Packet Detection, Interference Detection, Beam forming detection[14][11][16]

V.ANTI-JAMMING COMMUNICATION WITHOUT SHARED SECRETS

In the first part of this thesis, we address the major problem of jamming-resistant communication in scenarios in which the communicating parties (in this case communication through satellite) do not share secret keys. This

includes scenarios where the parties are not known in advance or where not all parties can be trusted (e.g., jamming-resistant key establishment or anti-jamming broadcast to a large set of unknown receivers). An inherent challenge in solving this problem is that known anti-jamming communication techniques such as frequency hopping or direct-sequence spread spectrum require that the devices share a secret spreading key (or code) *prior* to the start of their communication. This requirement creates a circular dependency between anti-jamming spread- spectrum communication and key establishment and generally precludes the unanticipated anti-jamming communication between unpaired devices. As a solution to break this dependency, we propose Uncoordinated Frequency Hopping (UFH), a new spread-spectrum anti-jamming technique that does not rely on shared keys. We present and discuss several UFH- based anti-jamming communication schemes and show their usage for various applications, including the establishment of pair wise or group keys in order to bootstrap common coordinated frequency hopping. We further demonstrate the feasibility of our UFH schemes, in terms of execution time and resource requirements, with MATLAB software based prototype implementation.[14]

VI.ADAPTIVE CHANNEL SELECTION

Achieving an optimal throughput with UFH requires the sender and receivers to accurately assessc_b and agree on a set of $c = c^*$ frequency channels. Especially in the absence of jamming, any selection of $c > 1$ channels will lead to a suboptimal performance. An optimal adaptive scheme in which both the sender and receiver(s) adapt their channels depending on the encountered jamming is, however, not practical. As jamming occurs at the receiver of a transmission, the sender would have to reliably obtain the feedback of the (maybe unknown) receiver(s),since different receivers are likely to observe different jamming strengths, this would further require to adapt to the worst case receiver. To avoid that the attacker can exploit this feedback, the feedback channel would have to be authentic. Providing the sender with the required feedback is therefore the same problem as the one we intend to solve with UFH in the first place.

VII.ROBUST PACKET DETECTION

Before a packet is transmitted, the sender applies error correcting codes to the header and shuffles the encoded bits according to a pseudo random sequence based on a secret key shared by the sender and the receiver. As we shall see, this process ensures that a substantial part of the packet header must be jammed to prevent being decoded.

Traditional approaches for the detection of jamming in wireless networks use the packet-delivery-ratio (PDR) and the received ambient signal strength as the main decision criteria.. Although these approaches are well-suited for the detection of proactive (long-term) jamming, they are not sufficient to protect the considered applications against targeted reactive jamming.

Jamming detection scheme does not suffer from these limitations. The central idea of our approach is to identify the cause of individual bit errors within a packet and to deduce therefrom whether the packet was jammed or just sent over a weak link,if the error was due to a weak signal (e.g., due to fast fading or shadowing), the RSS

value should be low. This additional information allows an accurate differentiation of packet errors that are caused by (un)intentional interference from errors that are caused by weak links.[15]

VIII.INTERFERENCE DETECTION

If a received packet contains at least one bit error, a node uses the measured RSS values to decide whether the identified errors are due to interference or due to a weak signal. If there was a bit error although the respective RSS value was high (i.e., although the link appeared to be strong), consider that the error must have been caused by external (intentional or unintentional) interference. If, on the other hand, the respective RSS value was low, we conclude that the error was most likely due to a low signal-to-noise ratio.[16]

IX.BLIND BEAMFORMING TECHNIQUE

This technique consist of 3 stages the very first stage has subspace stage in which strong interference is removed by applying input signal ,second stage is beamformer stage in which desire Received GPS signal is enhanced to desired level ,these two stages are added to GNSS receiver for anti jamming approach.

System model

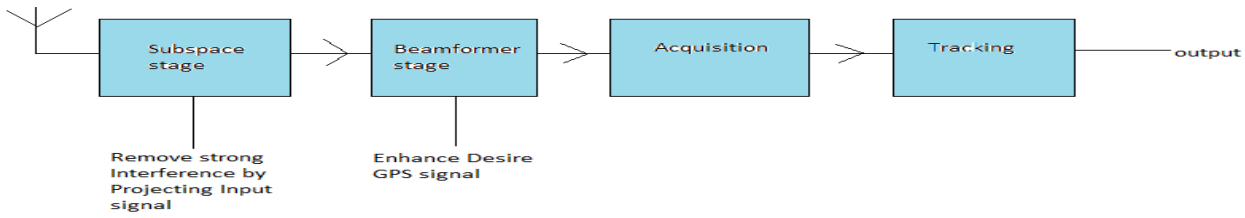

Fig.1 Proposed system using Blind Beamforming Techniques for Anti jamming

Simulation Result

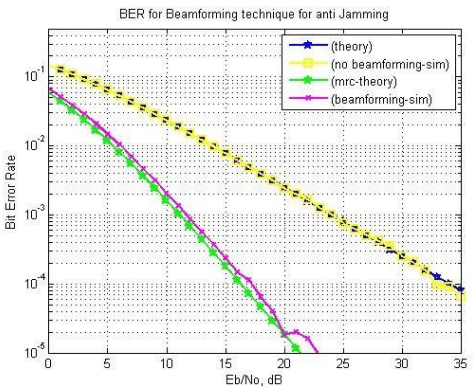

Fig 2:-Analytical and Simulated BER with jamming

X.CONCLUSION

A major challenge in reaching this goal is the inherent vulnerability of wireless communication to communication jamming DoS attacks. The problem becomes even more significant the more one takes the ubiquity of these emerging applications and services for granted. In this paper, we addressed this problem, focusing on scenarios where common anti-jamming techniques (such as FHSS and DSSS) are limited.More specificallywe tackled the problem of how devices that *do not share any secrets* can establish jamming-resistant communication over a wireless radio channel in the presence of a communication jammer. We addressed the dependency between anti-jamming spread-spectrum communication and pre-shared keys that is inherent to this problem, and proposed a novel anti-jamming technique called Uncoordinated Frequency Hopping (UFH) as a solution to break this dependency. We presented a number of UFH-based communication schemes and showed their use in several applications.we also present and mitigate reactive jamming to solve the problem.

REFERENCES

[1] - "*Global Positioning System* - Wikipedia, the free encyclopedia", http://www.wikipedia.org/wiki/GPS

[2] - P.L .N. Raju, "*Satellite Remote Sensing and GIS Applications in Agricultural Meteorology: Fundamentals of GPS"*, Proceedings of a Training Workshop, *7-11 July 2003, pp 121-150*

[3] - James Bao-Yen Tsui, "*Fundamentals of Global Positioning System Receivers : A Software Approach", 2nd ed. John Wiley & Sons, Inc, 2005*

[4] - Michael S. Braasch and A. J. Van Dierendonck, "*GPS Receiver Architectures and Measurements", Proceedings of the IEEE, vol. 87, no. 1, January 1999*

[5] - John Ruley, "*Global Positioning System Jamming*",http: //www.avweb.com/news/avionics/182754-1.html

[6] -Moeness G. Amin, "*Signal Processing Techniques for Antijamming GPS Receivers"*, Final Technical Report, *Villanova University, August 2005*

[7] - R.L. Fante and J.J. Vaccaro, "*Wideband Cancellation of Interference in a GPS Receiver Array*", IEEE Transactions on aerospace and electronic systems, vol. 36, no. 2, April 2000

[8] - Ronald L. Fante and John J. Vacarro, "*Cancellation of Jammers and Jammer Multipath in a GPS Receiver"*, IEEE AES Systems Magazine, *November 1998*

[9] -Yimin Zhang, Moeness G. Amin, and Alan R. Lindsey, "*Anti-jamming GPS Receivers Based on Bilinear Signal Distributions"*, Villanova University, IEEE, *2001*

[10] - Chung-Liang Chang and Bo-Han Wu, "*Analysis of Performance and Implementation Complexity of Array Processing in Anti-Jamming GNSS Receivers*", *Electrical and Electronic Engineering*, Copyright © 2011, pp 79-84

[11] - R. Sharma and B. D. Van Veen, "*Large Modular Structures for Adaptive Beamforming and the Gram-Schmidt Preprocessor"*, IEEE Transactions on signal processing, vol. 42, no. 2, February 1994

[12] -YaohuaZheng, "*Adaptive Antenna Array Processing for GPS Receivers"*, *Thesis submitted for the*

degree of Master of Engineering Science, University of Adelaide: Australia, July 2008

[13] - J. Litva and T. K.-Y. Lo., "*Digital Beamforming in Wireless Communications"*,Artech House, *Boston, 1996*

[14] - W. L. Myrick, J. S. Goldstein, and M. D. Zoltowski,***"Low complexity anti-jam space-time*** *processing for GPS," Proceedings of the 2001 IEEE International Conference on Acoustics, Speech, and Signal Processing, vol. 4, pp. 1332- 1336, 2001*

[15] D.G. Luenberger,*"Optimization by Vector Space Methods", New York: Wiley, 1969*

[16] BTnodes - *A Distributed Environment for Prototyping Ad Hoc Networks. http://www.btnode.ethz.ch/*.

[17] *GNU Radio Software. http://gnuradio.org/trac*.

[18] *ECRYPT Yearly Report on Algorithms and Keysize*. D.SPA.28, July 2008. IST-2002-507932.

[19] ImadAad, Jean-Pierre Hubaux, and Edward W. Knightly. *Denial of Service Resilience in Ad hoc Networks. In* Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom), *pages 202-215. ACM, 2004.*

[20] *David Adamy A First Course in Electronic Warfare. Artech House, 2001.*

[21] Ozgur B. Akan and Ian F. Akyildiz. *Event-to-sink Reliable Transport in Wireless Sensor Networks.* IEEE/ACM Transaction on Networking, *13(5):1003-1016, 2005.*

[22] ANSI. X9.63-2001: *Key Agreement and Key Transport Using Elliptical Curve Cryptography. American National Standards Institute, 2001*.

[23] International Loran Association. LORAN: *LOng Range Aid to Navigation.*http://www.loran.org.

[24] ParamvirBahl and Venkata N. Padmanabhan. *RADAR: An In-building RF-based User Location and Tracking System. In* Proceedings of the IEEE Conference on Computer Communications (INFOCOM), *pages 775-784. IEEE Communications Society, 2000.*

[25] Leemon C. Baird, William L. Bahn, Michael D. Collins, Martin C. Carlisle, and Sean Butler. *Keyless Jam Resistance. In* Proceedings of the IEEE Information Assurance and Security Workshop (IAW), *pages 143-150. IEEE, 2007.*

[26] Niko Bari and Birgit Pfitzmann. *Collision-Free Accumulators and Fail-Stop Signature Schemes Without Trees. In* Advances in Cryptology EUROCRYPT, *volume 1233/1997 of* Lecture Notes in Computer Science, *pages 480-494. Springer Berlin / Heidelberg, 1997*

[1] Michael Baron. *Probability and Statistics for Computer Scientists. Chapman & Hall/CRC, 2007.*