2020 IEEE 39th International Performance Computing and Communications Conference (IPCCC) | 978-1-7281-9829-3/20/$31.00 ©2020 IEEE | DOI: 10.1109/IPCCC50635.2020.9391560

REPROOF: Quantifying the Jam Resistance of REBUF

Joshua Groen
EECS Department
United States Military Academy
West Point, NY
joshua.groen@westpoint.edu

Peter Howell
EECS Department
United States Military Academy
West Point, NY
peter.howell@westpoint.edu

Michael Collins
Laboratory for Advanced Cybersecurity Research
Annapolis Junction, MD
mdcolli@tycho.ncsc.mil

***Abstract*—REPROOF analytically and experimentally quantifies a Jam Resistant BBC based Uncoordinated Frequency Division Multiplexing (FDM) system that does not require any shared secret.**

I. Introduction

Nearly all existing jam resistant communication systems require a pre-shared secret, typically exchanged through an out of band communication method [1]–[3]. Establishing a system for jam-resistant communication without the use of a pre-shared secret would ensure channel availability when this is not possible.

REBUF is the first known implementation of the BBC algorithm in an uncoordinated frequency division multiplexing system [4]. REBUF transmits marks as pure sinusoidal signals at a given frequency with a random phase. One of the key assumptions of BBC is that it is possible to create indelible marks. This simply means there is some way to change the transmission medium in such a way that an attacker cannot remove that change. Since REBUF operates by transmitting marks as pure sinusoidal signals with random phase, the conditions a potential attacker must meet in order to erase the existence of a signal at a given frequency are considered too sophisticated to be feasible in real time [5]. One of the key metrics of REBUF is a packet's mark density. Mark density is expressed as a fraction: the number of marks in a packet divided by the packet's length. As long as the packet density remains below the critical density point of 50%, the hallucination density remains steady and the decoding time stays linear for BBC decoding [6], [7]. While there are a variety of methods of jamming, we focus on the random mark attack because it is the most effective method against REBUF [4]. In this method, an attacker generates enough random marks to cause the total mark density to exceed the allowable threshold, overwhelming the system.

II. Background Theory

REBUF operates under the assumption that high bits (mark) can never be mistakenly interpreted as a low; this can be modeled as a Z-Channel system. The channel matrix for this model is $P[Y|X] = \begin{bmatrix} 1 & 0 \\ p & 1-p \end{bmatrix}$. The received probability vector, $P[Y]$, can easily be found if the transmission probability, $P[X]_R$, is known. A REBUF packet is always constructed with a specific mark density, i so $P[X]_R = \begin{bmatrix} i & 1-i \end{bmatrix}$. Solving for $P[Y]$ gives: $P[Y] = \begin{bmatrix} i + p(1-i) & (1-i)(1-p) \end{bmatrix}$. In order to keep the decode time linear, the total probability of receiving a mark (one) must be $\leq 50\%$. Applying these conditions to $P[Y]$ and simplifying gives equation 1, where p is the minimum mark density that an attacker must generate to overwhelm the decoder and i is the initial mark density of the encoded packet.

$$p \geq \frac{0.50 - i}{1 - i} \tag{1}$$

In its current configuration, REBUF sends messages with a mark density of approximately 11% meaning a jammer would have to fill 43.8% of the frequency spectrum using nearly four times the energy of the legitimate user.

REBUF uses Binary On/Off Keying (BO/OK) to determine the presence or absence of a mark. BO/OK works by interpreting signals as Gaussian distributions of one-dimensional standard deviations of μ, and is entirely insensitive to multipath effects [8]. Equation 2 describes the bit error rate for a given threshold, t, of detecting a transmitted 1 as a 0, essentially erasing a mark.

$$BER = 1 - \exp\left(-\frac{t^2}{2(1+\sigma^2)}\right) \tag{2}$$

While there are many possible methods of setting the threshold, REPROOF sorts the received frequencies by magnitude and keeps the top k%.

III. Implementation

We used USRP N310 software defined radios and GNU Radio to implement REPROOF. We use BBC to encode messages into vectors of 1024 bits with a mark density of about 11%. This bit vector is used to generate the frequency tones transmitted by taking the IFFT of the bit vector. The receiver uses the magnitude squared of the FFT to detect the energy peaks present. To determine which energy peaks represent a mark, we used the top $k = 50\%$ to ensure the decode time was reasonable. The result of the peak detection algorithm is a vector of 1's (mark present) and 0's (no mark). This bit vector is then passed to the BBC decoder which produces a list of all possible code words as the output.

978-1-7281-9829-3/20/$31.00 ©2020 IEEE

Authorized licensed use limited to: MIT Libraries. Downloaded on July 27,2022 at 12:36:31 UTC from IEEE Xplore. Restrictions apply.

We used a third SDR as a jammer with nearly identical implementation as the legitimate transmitter. Both sources used the same transmit power and the antennas were equidistant from the receiver. To empirically determine the effect of jamming, we repeatedly sent a 10.3 KB text file from the sender to the receiver. In all of our trials we defined success as decoding any valid code word and failure as decoding no valid code word.

The baseline packet loss rate with no jamming has a mean of 0.56%. We introduced jamming and incremented the mark density of the jammer by intervals of 5% up to 45% mark density with additional 1% increments between 35% and 40%. The complete results can be seen in Figure 1.

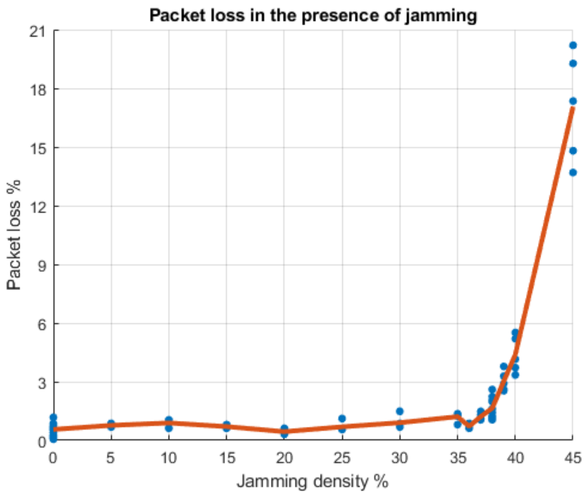

Fig. 1. Packet loss % in the presence of jamming

IV. Analysis

Our results demonstrates consistent jam-resistance up to about 39% mark density from the jammer. This means the malicious jammer had to use about 3.5 times more energy than the legitimate transmitter. The experimental results can be modeled as equation 3 where p is the minimum mark density a jammer must create to effectively interfere with REBUF.

$$p \geq 0.50 - i \tag{3}$$

This does not quite match the performance predicted by equation 1 where no marks should be lost up to a jamming mark density of 43.8%.

Understanding this discrepancy is crucial to developing an accurate model for analyzing the jam resistance of future systems. While both the z-channel model and BO/OK offer useful tools for modeling the REBUF system, neither completely account for the unique way REBUF encodes information. The Z-channel model fails to account for the true distribution of the marks described by the BO/OK model. The BO/OK model shows in equation 2 that the BER for 1s (marks) only goes to zero when the threshold is zero. On the other hand, the BO/OK analysis falls short because REBUF uses a top k% detection scheme. The threshold for ones is effectively zero until a significant number of zeros are incorrectly identified as a one. Then the threshold begins to increase as more frequency slots are filled.

It may be useful to treat equation 1 as the theoretical maximum for jam resistance and equation 3 as the practical implementation limit. It should be pointed out that taking the $\lim_{i\to 0}$, equation 3 converges with equation 1.

V. Conclusion

While No communications scheme is truly jam-proof [3], the true potential of a system based on REBUF is when the mark density is extremely low. A malicious jammer must expend at least $\frac{0.5-i}{i}$ times as much energy as the sender, where i is the legitimate sender's mark density. As i becomes very small, the relative energy the jammer must use increases exponentially. There are several possible methods to decrease the mark density including: using larger bandwidth, using a larger FFT, or utilizing time as another dimension.

REPROOF proves the feasibility of using the REBUF system, which does not require any pre-shared secret, to ensure the availability of communication systems even in the presence of malicious jamming.

Acknowledgment

The views expressed in this article are those of the authors and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

References

[1] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, pp. 42–56, 2009.

[2] L. B. Milstein, "Interference rejection techniques in spread spectrum communications," *Proceedings of the IEEE*, vol. 76, no. 6, pp. 657–671, 1988.

[3] W. L. Bahn, L. C. Baird III, and M. D. Collins, "Jam resistant communications without shared secrets," in *Proceedings of the 3rd International Conference on Information Warfare and Security (ICIW08)*, 2008, pp. 24–25.

[4] J. Ashley, J. Groen, and M. Collins, "REBUF: jam resistant BBC based uncoordinated frequency division multiplexing," in *2020 Wireless Telecommunications Symposium (WTS) (WTS 2020)*, Washington, USA, Apr. 2020.

[5] L. Baird, W. Bahn, and M. Collins, "Jam-resistant communication without shared secrets through the use of concurrent codes," *United States Air Force Academy, Tech. Rep. USAFA-TR-2007-01*, 2007.

[6] W. L. Bahn and L. C. Baird III, "Extending critical mark densities in concurrent codecs through the use of interstitial checksum bits," *US Air Force Academy, Academy Center for Cyberspace Research, Tech. Rep. USAFA-TR-2008-ACCR-02*, 2008.

[7] W. L. Bahn, *Concurrent code spread spectrum: theory and performance analysis of jam resistant communication without shared secrets.* University of Colorado at Colorado Springs, 2012.

[8] W. Press, W. Dally, D. Eardley, R. Garwin, and P. Horowitz, "An unconventional, highly multipath-resistant, modulation scheme," MITER, Tech. Rep., 1997. [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a331647.pdf

Authorized licensed use limited to: MIT Libraries. Downloaded on July 27,2022 at 12:36:31 UTC from IEEE Xplore. Restrictions apply.