

REPORT DOCUMENTATION PAGE			Form Approved OMB NO. 0704-0188		
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA, 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 15-04-2014		2. REPORT TYPE Final Report		3. DATES COVERED (From - To) 14-Sep-2012 - 13-Sep-2013	
4. TITLE AND SUBTITLE Robust mobile tactical communications for video transmission				5a. CONTRACT NUMBER W911NF-12-1-0510	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER 611102	
6. AUTHORS Pamela Cosman, Larry Milstein				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAMES AND ADDRESSES University of California - San Diego 9500 Gilman Drive MC 0934 La Jolla, CA 92093 -0934				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES) U.S. Army Research Office P.O. Box 12211 Research Triangle Park, NC 27709-2211				10. SPONSOR/MONITOR'S ACRONYM(S) ARO	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S) 61838-NS.4	
12. DISTRIBUTION AVAILABILITY STATEMENT Approved for Public Release; Distribution Unlimited					
13. SUPPLEMENTARY NOTES The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.					
14. ABSTRACT This project is concerned with the cross-layer design of a video transmission system for use over tactical, mobile channels. The research is concerned with effects of signal modulation at the physical layer, including the use of spread spectrum and forward error control (FEC), to ensure reliable communications over channels that are dominated by both multipath/fading and intentional spoofing and jamming. We assume a cluster-head-based cognitive radio (CR) at the MAC layer, and unequal protection techniques at the application layer to allow for efficient video compression and reliability.					
15. SUBJECT TERMS cognitive radio, tactical environment, jamming, spoofing					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Pamela Cosman
a. REPORT UU	b. ABSTRACT UU	c. THIS PAGE UU			19b. TELEPHONE NUMBER 858-822-0157

Report Title

Robust mobile tactical communications for video transmission

ABSTRACT

This project is concerned with the cross-layer design of a video transmission system for use over tactical, mobile channels. The research is concerned with effects of signal modulation at the physical layer, including the use of spread spectrum and forward error control (FEC), to ensure reliable communications over channels that are dominated by both multipath/fading and intentional spoofing and jamming. We assume a cluster-head-based cognitive radio (CR) at the MAC layer, and unequal protection techniques at the application layer to allow for efficient video compression and reliability.

Much of our research, as described in detail in two publications which are included with this report, considers a generic source, and emphasizes the twofold vulnerability of a tactical CR system to a sufficiently intelligent intentional adversary, namely spoofing in the spectrum sensing mode, and jamming in the data transmission mode. We take the objective of the adversary to be the minimization of the throughput of the desired signal, and this leads naturally into the second phase of the research, in which the generic source is replaced with a video source.

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Received

Paper

TOTAL:

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

Received

Paper

TOTAL:

Number of Papers published in non peer-reviewed journals:

(c) Presentations

Number of Presentations: 0.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

<u>Received</u>	<u>Paper</u>
-----------------	--------------

TOTAL:

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

<u>Received</u>	<u>Paper</u>
-----------------	--------------

04/14/2014	3.00	Madushanka Soysa, Pamela C. Cosman, Laurence B. Milstein. Spoofing optimization over Nakagami-m fading channels of a cognitive radio adversary, 2013 IEEE Global Conference on Signal and Information Processing (GlobalSIP). 02-DEC-13, Austin, TX, USA. ; ,
------------	------	---

TOTAL: 1

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):

(d) Manuscripts

<u>Received</u>	<u>Paper</u>
-----------------	--------------

04/14/2014	2.00	Madushanka Soysa, Pamela C. Cosman, Laurence B. Milstein. Spoofing and jamming optimization over Rayleigh fading channels of a cognitive radio adversary, IEEE Transactions on Communications (05 2013)
------------	------	---

TOTAL: 1

Number of Manuscripts:

Books	
<u>Received</u>	<u>Paper</u>
TOTAL:	

Patents Submitted

Patents Awarded

Awards

Larry Milstein, IEEE Communications Theory Technical Committee Achievement Award, 2012.

Graduate Students

<u>NAME</u>	<u>PERCENT SUPPORTED</u>	Discipline
Madushanka Dinesh Soysa	0.21	
FTE Equivalent:	0.21	
Total Number:	1	

Names of Post Doctorates

<u>NAME</u>	<u>PERCENT SUPPORTED</u>
FTE Equivalent:	
Total Number:	

Names of Faculty Supported

<u>NAME</u>	<u>PERCENT SUPPORTED</u>	National Academy Member
Pamela Cosman	0.08	No
Larry Milstein	0.07	No
FTE Equivalent:	0.15	
Total Number:	2	

Names of Under Graduate students supported

<u>NAME</u>	<u>PERCENT SUPPORTED</u>
FTE Equivalent:	
Total Number:	

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: 0.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:..... 0.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):..... 0.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense 0.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields: 0.00

Names of Personnel receiving masters degrees

NAME

Total Number:

Names of personnel receiving PHDs

NAME

Total Number:

Names of other research staff

NAME

PERCENT SUPPORTED

FTE Equivalent:

Total Number:

Sub Contractors (DD882)

Inventions (DD882)

Scientific Progress

see attachment

Technology Transfer

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Service Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.					
1. REPORT DATE (DD-MM-YYYY) 07/04/2014		2. REPORT TYPE Final		3. DATES COVERED (From - To) 20120914 - 20130913	
4. TITLE AND SUBTITLE Robust mobile tactical communications for video transmission				5a. CONTRACT NUMBER W911NF-12-1-0510	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Cosman, Pamela Milstein, Larry				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) The Regents of the University of California; University of California, San Diego 9500 Gilman Drive, Mail Code 0934 La Jolla, California 92093-0934				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) US ARMY RDECOM ACQ CTR - W911NF 4300 S. MIAMI BLVD DURHAM NC 27703				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT N/A					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT This project is concerned with the cross-layer design of a video transmission system for use over tactical, mobile channels. The research is concerned with effects of signal modulation at the physical layer, including the use of spread spectrum and forward error control (FEC), to ensure reliable communications over channels that are dominated by both multipath/fading and intentional spoofing and jamming. We assume a cluster-head-based cognitive radio (CR) at the MAC layer, and unequal protection techniques at the application layer to allow for efficient video compression and reliability. Much of our research, as described in detail in two publications which are included with this report, considers a generic source, and emphasizes the twofold vulnerability of a tactical CR system to a sufficiently intelligent intentional adversary, namely spoofing in the spectrum sensing mode, and jamming in the data transmission mode. We take the objective of the adversary to be the minimization of the throughput of the desired signal, and this leads naturally into the second phase of the research, in which the generic source is replaced with a video source.					
15. SUBJECT TERMS cognitive radio, tactical environment, jamming, spoofing					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Pamela Cosman
U	U	U	UU	10	19b. TELEPHONE NUMBER (Include area code) 858-822-0157

I. INTRODUCTION

This project is concerned with the cross-layer design of a video transmission system for use over tactical, mobile channels. The research is concerned with effects of signal modulation at the physical layer, including the use of spread spectrum and forward error control (FEC), to ensure reliable communications over channels that are dominated by both multipath/fading and intentional spoofing and jamming. We assume a cluster-head-based cognitive radio (CR) at the MAC layer, and unequal protection techniques at the application layer to allow for efficient video compression and reliability.

Much of our research, as described in detail in [1] and [2], which are included in this report, considers a generic source, and emphasizes the twofold vulnerability of a tactical CR system to a sufficiently intelligent intentional adversary, namely spoofing in the spectrum sensing mode, and jamming in the data transmission mode. As will be seen below, we take the objective of the adversary to be the minimization of the throughput of the desired signal, which then leads naturally into the second phase of the research, in which the generic source is replaced with a video source. It is in this latter phase of the research that we emphasize a cross-layer design between the application and physical layers that emphasizes joint source and channel coding.

II. SYSTEM OVERVIEW

An adversary intending to disrupt the communication in a CR network has two ways to attack. The first way is to exploit the inherent vulnerability of spectrum sensing by transmitting a spoofing signal that emulates a primary user (PU) during the sensing interval. Here the secondary user (SU) might mistakenly conclude that the channel is occupied by a PU and not available for transmission. In this way, an intelligent attacker reduces the bandwidth available for the SU. Further, the adversary can disrupt communications using jamming techniques during the data transmission phase of the communication.

Consider a cluster based SU network, as shown in Figure 1. We denote the cluster head serving the SUs by CH_S , and we denote the adversary by A. We consider the downlinks from CH_S to the users of a multi-carrier direct sequence code division multiple access (MC-DS-CDMA) system with N_T bands (or subcarriers). The N_T bands are shared among PUs and SUs. *Allowed bands* are ones unoccupied by PUs. The cluster head periodically performs spectrum sensing, and uses a subset of allowed bands to transmit

data to the SUs. *Busy bands* are bands that the SU network cannot use due to PU activity. The cluster head uses power control to maintain constant average link signal-to-noise ratio (SNR) for all SUs. We denote the length of the sensing interval by T_0 and the length of the data transmission interval by T_1 .

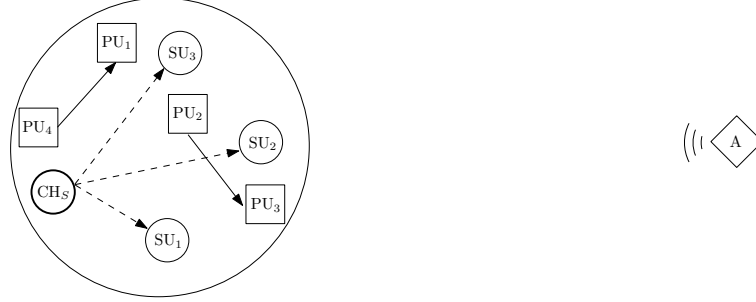


Fig. 1: The system network model

The adversary uses Gaussian noise signals when it spoofs or jams. The objective of the adversary is to disrupt the communication, and we use the average throughput as the performance metric. We assume that the adversary is aware of the basic characteristics of the system, including the receiver structure, type of spreading, bandwidth of the waveform, sensing and transmission times, background noise power spectral density (PSD), that all links undergo Rayleigh fading, and whether it is slow or fast fading. We also assume that the links from the adversary to the SUs in the cluster have equal average gain in each band, which is known by the adversary. Because a practical adversary cannot have all the assumed knowledge, such as the average channel gain, the work done here is a worst-case analysis, which gives a lower bound to the throughput with jamming and spoofing.

Let $B = \{1, 2, \dots, N_T\}$ be the set of bands, and $B_{su} \subseteq B$ be the subset of bands used by the SU network for communication in one transmission interval. The throughput (Γ) of the SU network during the data transmission interval is given by

$$\Gamma = \sum_{i \in B_{su}} \sum_{u=1}^{\Omega_i} L_P (1 - p_e^{(i,u)}) \log_2 M_{i,u} \quad (1)$$

where Ω_i is the number of SUs in the i -th band, L_P is the packet length in symbols, $p_e^{(i,u)}$ is the probability of packet error of the u -th user in the i -th band, and $\log_2 M_{i,u}$ is the number of bits per symbol in the alphabet used by the u -th user in the i -th band. The SUs use a single 4-QAM alphabet for fast fading, and may use either a single alphabet or adaptive modulation for slow fading. Spoofing reduces $|B_{su}|$, and jamming increases $p_e^{(i,u)}$ in (1), thus reducing Γ .

Our key analytical result is embodied in the following theorem:

Let $f : \mathbb{R}^+ \rightarrow \mathbb{R}^+$ be a function such that

P0: f is bounded above, i.e., $\exists M < \infty$, s.t. $f(x) \leq M \forall x \in [0, \infty)$

P1: f is an increasing function, i.e., $f'(x) \geq 0$, where $f'(x)$ is the first derivative of $f(x)$,

P2: $f''(x) = 0$ has at most one root in $x > 0$, where $f''(x)$ is the second derivative of $f(x)$. Also, define $g : \mathbb{R}^+ \rightarrow \mathbb{R}$, as $g(x) \triangleq f(x) - f(0) - xf'(x)$. Then, if $\sum_{i=1}^N x_i \leq X_T$ and $x_i \geq 0$,

$$\sum_{i=1}^N f(x_i) \leq \begin{cases} Nf\left(\frac{X_T}{N}\right), & \text{if } \frac{X_T}{N} \geq x^* \\ (N - n^*)f(0) + n^*f\left(\frac{X_T}{n^*}\right), & \text{if } \frac{X_T}{N} < x^* \end{cases} \quad (2)$$

where $n^* = \frac{X_T}{x^*}$ and x^* is the largest root of $g(x) = 0$. Also, the set of arguments, S_x , that correspond to the equality when n^* is an integer, is given by

$$S_x = \arg \max_{\sum_{i=1}^N x_i = X_T, x_i \geq 0} \left(\sum_{i=1}^N f(x_i) \right) = \begin{cases} \underbrace{\left\{ \frac{X_T}{N}, \dots, \frac{X_T}{N} \right\}}_{N \text{ elements}}, & \text{if } \frac{X_T}{N} \geq x^* \\ \underbrace{\left\{ \frac{X_T}{n^*}, \dots, \frac{X_T}{n^*} \right\}}_{n^* \text{ elements}}, \underbrace{\{0, \dots, 0\}}_{(N-n^*)}, & \text{if } \frac{X_T}{N} < x^* \end{cases} \quad (3)$$

Note that when $\frac{X_T}{x^*}$ is not an integer, we use the approximation $n^* = \arg \max_{n=\lfloor \frac{X_T}{x^*} \rfloor, \lceil \frac{X_T}{x^*} \rceil} (N - n)f(0) + nf\left(\frac{X_T}{n}\right)$, to arrive at a suboptimal set S_x .

In optimizing power allocation for spoofing, $f(x)$ is the probability of false detection in one band as a function of the spoofing power allocated for that band. A false detection is mistakenly detecting a vacant band as being occupied by the PUs. For jamming, $f(x)$ is the packet error rate per user in a band, as a function of the jamming power allocated for that band.

III. SPOOFING CONSIDERATIONS

During the sensing interval, the adversary attacks the system by spoofing to reduce the bandwidth available to the SUs. Let $B_{al} \subseteq B$ be the set of allowed bands in the current sensing interval. An allowed band may appear busy due to background noise and spoofing. This is called a *false detection*. The objective of the adversary in the spoofing mode is to minimize the number of allowed bands accessible to SUs. We can show that the expected number of allowed bands accessible to SUs is $\sum_{i \in B_{al}} (1 - p_{fd}^{(i)})$, where $p_{fd}^{(i)}$ is the probability of false detection of the i -th band, given that the i -th band is vacant. We assume that

the adversary has knowledge of the system false alarm probability, i.e., the probability of false detection caused only due to background noise with no spoofing. The average probability of false detection due to spoofing discussed here is an upper bound to the achievable probability of false detection, when the adversary does not have this knowledge.

At the start of the sensing interval, the adversary does not know which bands are allowed for SUs. Therefore, from the adversary's perspective, every band has an equal probability of being vacant. Hence, the objective of the adversary is to maximize $\sum_{i=1}^{N_T} p_{fd}^{(i)}$, under the constraint $\sum_{i=1}^{N_T} P_{S,i} = P_S$, where $P_{S,i}$ is the spoofing power allocated for the i -th band and P_S is the total spoofing power available.

IV. JAMMING CONSIDERATIONS

From (1), to minimize the throughput of the network by jamming, the adversary ideally aims to maximize $\sum_{i \in B_{su}} \sum_{u=1}^{\Omega_i} L_P p_e^{(i,u)} \log_2 M_{i,u}$. The probability of packet error, $p_e^{(i,u)}$, depends on the jamming power, the channel state, the FEC, and the alphabets and thresholds used in conjunction with adaptive modulation. We assume that the adversary senses and detects the bands used for transmission before jamming, and hence knows $B_{su} \cup B_{pu}$, where $B_{pu} \subseteq \{1, 2, \dots, N_T\}$ is the set of bands occupied by PUs. The average SNR of the SUs, maintained by the cluster head through power control, is assumed to be known by the adversary. We further assume that the adversary is aware of the type and rate of the FEC, the alphabet sizes, and the thresholds. However, the adversary is not aware of instantaneous system parameters, such as the instantaneous CSI, the instantaneous numbers of secondary users in the i -th band (Ω_i), and which alphabet each user is using. Further, the adversary cannot differentiate between the bands occupied by PUs and SUs through observations during the transmission interval. Therefore, to minimize the average throughput without this information, the objective function is changed to $\max \sum_{i \in B_{su} \cup B_{pu}} r_e(P_{J,i})$, under the constraint $\sum_{i \in B_{su} \cup B_{pu}} P_{J,i} = P_J$, where P_J is the total power available for jamming, $P_{J,i}$ is the jamming power allocated for the i -th band, $r_e(P_{J,i})$ is the expected value of $p_e^{(i,u)} \log_2 M_{i,u}$ and the expectation is taken over the fading gains of the links from CH_S to the SUs, and the adversary to the SUs.

V. TYPICAL RESULTS

We assume that, in each transmission and sensing interval, the PUs occupy $|B_{pu}| = \min(N_{pu}, N_T)$ bands at random, where N_{pu} is a Poisson random variable with mean parameter $\bar{N}_{pu}$. The number of SUs (Ω_{su})

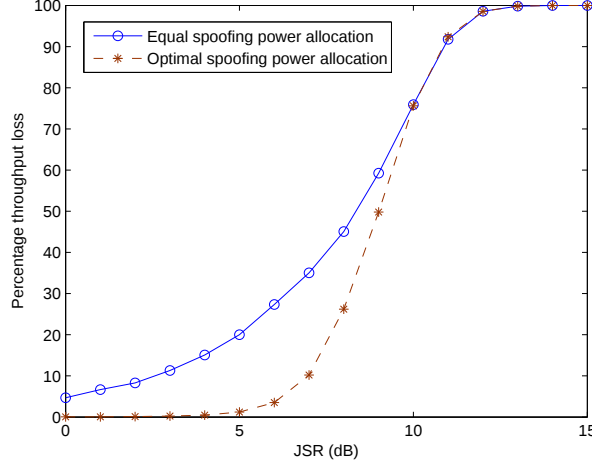


Fig. 2: Percentage loss of throughput under fast fading ($T_0 = 128T_s$, $N_T = 100$, $\frac{\bar{\Omega}_{su}}{\Omega_M} = 50$, $\bar{N}_{pu} = 50$)

in each transmission interval is modeled as an independent Poisson random variable with mean parameter $\bar{\Omega}_{su}$. The number of bands used by SUs in each transmission interval is $|B_{su}| = \min\left(\lceil \frac{\Omega_{su}}{\Omega_M} \rceil, |B - B_{pu}|\right)$, where Ω_M is the maximum number of SUs that can share a single band. We select the average SNR $\bar{\gamma}_S = 10$ dB, $\Omega_M = 8$, $T_0 = 128T_s$ and $T_1 = 1024T_s$, where T_s is the symbol time. For FEC, we use a rate $\frac{1}{2}$ LDPC code with block lengths varying from 1024 bits to 6144 bits. We define the jamming-to-signal power ratio (JSR) as the ratio of adversary-power-to-signal-power per user. That is, the adversary power J is taken to be the sum of the jamming and the spoofing power available in all bands, and the signal power S is taken to be the transmission power available for a single SU. When there is no knowledge of the system other than its operating frequency range, the adversary can perform equal power spoofing or jamming across the total bandwidth. We use this equal power spoofing and jamming strategy as a reference, with which the performance of the optimized strategy is compared.

V.1 Spoofing

Figure 2 shows the average throughput loss in the SU network due to spoofing, under fast fading. At a JSR of 7 dB, the optimal spoofing power allocation reduces the throughput by 35.1%, while the equal power allocation reduces the throughput only by 10.2%. As JSR is increased beyond 10dB, the optimal spoofing power allocation strategy shifts from partial-band spoofing to full-band spoofing, and hence the curves overlap at high JSR.

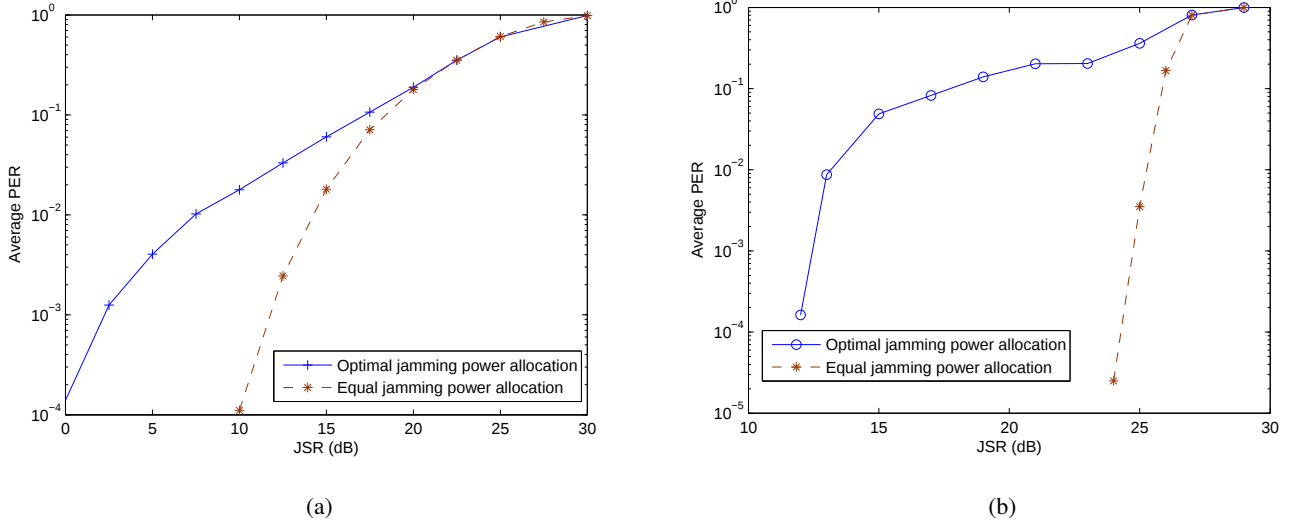


Fig. 3: Average packet error rate vs. JSR ($\bar{\gamma}_S = 12$ dB, $\frac{\bar{\Omega}_{SU}}{\bar{\Omega}_M} = 10$, $\bar{N}_{pu} = 10$, $N_T = 20$): (a) under slow fading (b) under fast fading.

V.2 Jamming

Figure 3(a) shows the average PER versus JSR, with total power put into jamming by the adversary, under slow fading. At a JSR of 7dB, the optimal jamming power allocation achieves a PER of 10^{-2} , while the PER at the same JSR with equal power jamming is below 10^{-4} . Figure 3(b) shows the average PER due to jamming under fast fading. The optimal jamming power allocation achieves a 10^{-2} average PER at a JSR more than 10 dB below the JSR required for the same average PER with equal jamming power allocation.

V.3 Joint optimization of spoofing and jamming

Figure 4(a) shows the SU throughput-per-transmission interval versus JSR when the adversary jointly optimizes the jamming and spoofing power allocation under slow fading. It is compared with the throughput if the adversary spoofed and jammed bands at equal power. Notice that for JSR in the vicinity of 25dB, the use of the optimization technique by the adversary reduces the CR throughput by a factor of 4 to 5, relative to an adversary who divides power equally across all bands. At low JSR, below about 18dB under simulated system parameters, spoofing is ineffective, as the system is lightly loaded. However, the optimized adversary is able to reduce the throughput slightly through increased packet error rate by jamming. Beyond a JSR of 18dB, the system throughput is significantly reduced, predominantly due to

successful spoofing. Figure 4(b) shows the SU throughput-per-transmission interval versus JSR under fast fading. We note that the optimal power allocation can significantly reduce the throughput of SUs at a JSR 10.5 dB lower than constant power allocation, under the simulated-system parameters.

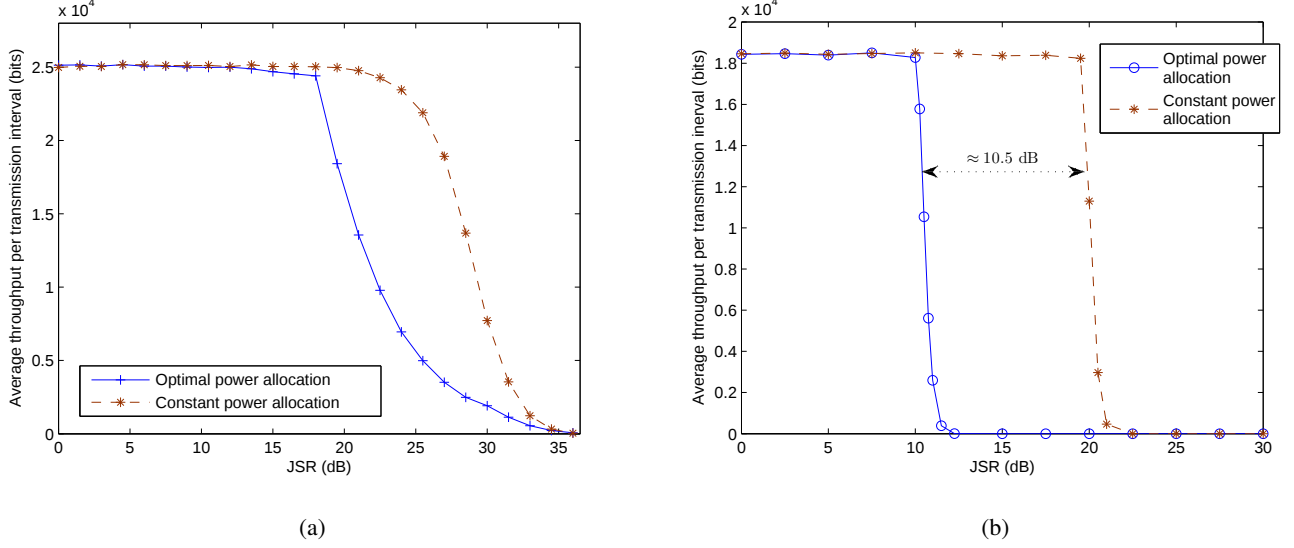


Fig. 4: Throughput vs. JSR ($T_0 = 128T_s$, $T_1 = 1024T_s$, $\frac{\bar{\Omega}_{su}}{\bar{\Omega}_M} = 10$, $\bar{N}_{pu} = 10$, $N_T = 100$): (a) under slow fading (b) under fast fading.

It is shown in [1] that it is generally optimal to attack with both spoofing and jamming, whereby the optimal energy allocation between the two methods of attack is dependent on system parameters and JSR. While successful spoofing has the most noticeable impact on SU throughput, we observe that when the system is not heavily loaded, spoofing is not effective at low JSR, and the optimal method of attack is jamming. An increase in the average number of subcarriers required by SUs, or a decrease in the sensing duration relative to the transmission duration, would lower the JSR, at which point the optimal strategy shifts from jamming to spoofing.

VI. SPOOFING CONSIDERATIONS FOR A VIDEO SOURCE

We now look at how the performance of the system is affected by a spoofing attack, when the generic source used to generate the results presented above is replaced by an actual video waveform. We use the normalized average distortion of the received video as the performance metric. The normalized average distortion is the mean square error, as a fraction of the source variance. Consider a H.264/AVC video

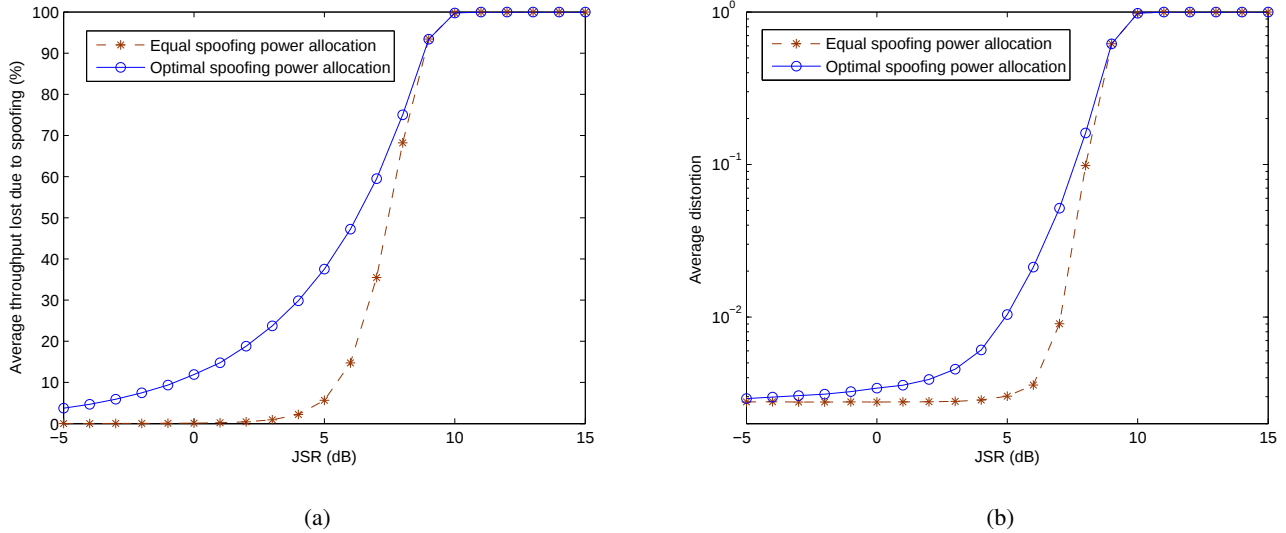


Fig. 5: (a) Average throughput loss due to spoofing attack (b) Average distortion due to spoofing attack ($N_T = 100$, $\bar{N}_{pu} = 20$, $\bar{\Omega}_{su} = 480$, $\Omega_M = 8$)

source at the cluster head, with both the quantization parameters and the length of the group-of-pictures (GoP) optimized to minimize average distortion under source rate constraints.

Figure 5(a) shows the average throughput lost due to spoofing attacks, for $N_T = 100$, $\bar{N}_{pu} = 20$, $\bar{\Omega}_{su} = 480$, $R_0 = 128\text{kbps}$ and $R_M = 1024\text{kbps}$, where R_0 is the average source rate per user per band, and R_M is the maximum information rate a single SU needs in a transmission interval. The average throughput loss due to equal power spoofing is 5% at 5 dB of JSR, while the optimal spoofing power allocation increases the average throughput loss to 37% at the same JSR. Note that the curves in Figure 5(a) for a video source are quite similar to those of Figure 2 for a generic source. Figure 5(b) shows the normalized average distortion of the spoofed SUs plotted against JSR. The normalized average distortion under optimal spoofing power allocation is higher than that under equal power allocation at low JSR. The distortion is a decreasing function of source rate, the average of which is proportional to the average throughput. Due to the reduction in throughput resulting by more effective spoofing, as seen in Figure 5(a), optimal spoofing power allocation results in higher average distortion.

REFERENCES

- [1] M. Soysa, P. Cosman, and L. Milstein, "Spoofing and jamming optimization over Rayleigh fading channels of a cognitive radio adversary," *submitted to IEEE Trans. Commun.*

- [2] —, “Spoofing optimization over Nakagami- m fading channels of a cognitive radio adversary,” in *IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, 2013, Dec 2013, pp. 1190–1193.

List of Illustrations

Fig. 1: The system network model

Fig. 2: Percentage loss of throughput under fast fading ($T_0 = 128T_s, N_T = 100, \frac{\bar{\Omega}_{su}}{\bar{\Omega}_M} = 50, \bar{N}_{pu} = 50$)

Fig. 3: Average packet error rate vs. JSR ($\bar{\gamma}_S = 12$ dB, $\frac{\bar{\Omega}_{su}}{\bar{\Omega}_M} = 10, \bar{N}_{pu} = 10, N_T = 20$): (a) under slow fading (b) under fast fading.

Fig. 4: Throughput vs. JSR ($T_0 = 128T_s, T_1 = 1024T_s, \frac{\bar{\Omega}_{su}}{\bar{\Omega}_M} = 10, \bar{N}_{pu} = 10, N_T = 100$): (a) under slow fading (b) under fast fading.

Fig. 5: (a) Average throughput loss due to spoofing attack (b) Average distortion due to spoofing attack ($N_T = 100, \bar{N}_{pu} = 20, \bar{\Omega}_{su} = 480, \bar{\Omega}_M = 8$)

REPORT OF INVENTIONS AND SUBCONTRACTS
(Pursuant to "Patent Rights" Contract Clause) (See Instructions on back)

Form Approved
OMB No. 9000-0095
Expires Jan 31, 2008

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services Directorate (9000-0095). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR COMPLETED FORM TO THE ABOVE ORGANIZATION. RETURN COMPLETED FORM TO THE CONTRACTING OFFICER.

1.a. NAME OF CONTRACTOR/SUBCONTRACTOR The Regents of the Univ of CA; San Diego		c. CONTRACT NUMBER W911NF-12-1-0510	2.a. NAME OF GOVERNMENT PRIME CONTRACTOR US ARMY RDECOM ACQ CTR - W911N		c. CONTRACT NUMBER W911NF-12-1-0510	3. TYPE OF REPORT (X one) ☐ a. INTERIM ☒ b. FINAL	
b. ADDRESS (Include ZIP Code) 9500 Gilman Dr. La Jolla, CA 92093-0934		d. AWARD DATE (YYYYMMDD) 20120914	b. ADDRESS (Include ZIP Code) 4300 S. MIAMI BLVD DURHAM NC 27703		d. AWARD DATE (YYYYMMDD) 20120914	4. REPORTING PERIOD (YYYYMMDD) a. FROM 20120914 b. TO 20130913	

SECTION I - SUBJECT INVENTIONS

5. "SUBJECT INVENTIONS" REQUIRED TO BE REPORTED BY CONTRACTOR/SUBCONTRACTOR (If "None," so state)

NAME(S) OF INVENTOR(S) (Last, First, Middle Initial) a.	TITLE OF INVENTION(S) b.	DISCLOSURE NUMBER, PATENT APPLICATION SERIAL NUMBER OR PATENT NUMBER c.	ELECTION TO FILE PATENT APPLICATIONS (X) d.				CONFIRMATORY INSTRUMENT OR ASSIGNMENT FORWARDED TO CONTRACTING OFFICER (X) e.	
			(1) UNITED STATES		(2) FOREIGN			
			(a) YES	(b) NO	(a) YES	(b) NO	(a) YES	(b) NO
None								

f. EMPLOYER OF INVENTOR(S) NOT EMPLOYED BY CONTRACTOR/SUBCONTRACTOR			g. ELECTED FOREIGN COUNTRIES IN WHICH A PATENT APPLICATION WILL BE FILED	
(1) (a) NAME OF INVENTOR (Last, First, Middle Initial)	(2) (a) NAME OF INVENTOR (Last, First, Middle Initial)	(1) TITLE OF INVENTION	(2) FOREIGN COUNTRIES OF PATENT APPLICATION	
(b) NAME OF EMPLOYER	(b) NAME OF EMPLOYER			
(c) ADDRESS OF EMPLOYER (Include ZIP Code)	(c) ADDRESS OF EMPLOYER (Include ZIP Code)			

SECTION II - SUBCONTRACTS (Containing a "Patent Rights" clause)

6. SUBCONTRACTS AWARDED BY CONTRACTOR/SUBCONTRACTOR (If "None," so state)

NAME OF SUBCONTRACTOR(S) a.	ADDRESS (Include ZIP Code) b.	SUBCONTRACT NUMBER(S) c.	FAR "PATENT RIGHTS" d.		DESCRIPTION OF WORK TO BE PERFORMED UNDER SUBCONTRACT(S) e.	SUBCONTRACT DATES (YYYYMMDD) f.	
			(1) CLAUSE NUMBER	(2) DATE (YYYYMM)		(1) AWARD	(2) ESTIMATED COMPLETION
None							

SECTION III - CERTIFICATION

7. CERTIFICATION OF REPORT BY CONTRACTOR/SUBCONTRACTOR (Not required if: (X as appropriate))		☐ SMALL BUSINESS or ☒ NONPROFIT ORGANIZATION	
I certify that the reporting party has procedures for prompt identification and timely disclosure of "Subject Inventions," that such procedures have been followed and that all "Subject Inventions" have been reported.			
a. NAME OF AUTHORIZED CONTRACTOR/SUBCONTRACTOR OFFICIAL (Last, First, Middle Initial) Michael Brown	b. TITLE Contract and Grant Officer	c. SIGNATURE 	d. DATE SIGNED 4102014