Final Report

W15QKN-05-D-0011, Task Order 43

(September 15, 2009)

Submitted by S. Tewksbury

Contract Number: W15QKN-05-D-0011, Task Order 43

Contract Name: Embedded Intelligent Sensor Network Systems

Task 1

Cognitive & Network Centric Military Communications

Subtask 1

Collaborative Spectrum Sensing

Prof. Hongbin Li
Department of Electrical and Computer Engineering
Stevens Institute of Technology
Hoboken, NJ 07030
Tel: (201) 216 5604
E-mail: Hongbin.Li@stevens.edu

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
05-06-2010	Final Report	08-30-2008 – 09-15-2009

4. TITLE AND SUBTITLE
Cognitive & Network Centric Military Communications

5a. CONTRACT NUMBER
W15QKN-05-D-0011

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Prof. Honghin Li

5d. PROJECT NUMBER

5e. TASK NUMBER
43

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Department of Electrical and
Computer Engineering
Stevens Institute of Technology
Hoboken, NJ 07030

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
DoD-ARDEC
ACOE
Building 407, Picatinny
07806

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A Unlimited Distribution

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This report is final report which is a compilation of reports for subtasks of the project. Each of the subtask sections has an individual abstract associated with it in the report.

15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSO Shafik Quoraishee
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(include are code)* 9737249463

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

Abstract

In this report, we examine distributed estimation of the average power of a random signal in wireless sensor networks. Due to stringent bandwidth/power constraints, each sensor quantizes its observation into one bit of information and sends the quantized data to a fusion center, where the signal power is estimated. We firstly introduce two fixed quantization (FQ) schemes, with the first using a single threshold and the second employing a pair of symmetric thresholds. The maximum likelihood (ML) estimators associated with the two FQ schemes are developed and their corresponding Cramer-Rao bounds (CRBs) are analyzed. We show that the FQ approach, especially the second one, can achieve an estimation performance close to that of a clairvoyant estimator using unquantized data, if the optimum quantization threshold is available; however, the optimum threshold is dependent on the unknown signal power and as the threshold deviates from its optimum value, the performance degrades rapidly. To cope with this difficulty, we propose a distributed adaptive quantization (AQ) approach by which the threshold is dynamically adjusted from one sensor to another, in a way such that the threshold converges to the optimum threshold. Our analysis shows that the proposed AQ approach is asymptotically optimum, yielding an asymptotic CRB equivalent to that of the FQ approach with optimum threshold.

1. Introduction

Wireless sensor networks (WSNs) have attracted much attention over the past few years. Composed of a large number of small, low-cost sensors with integrated sensing, processing, and communication abilities, WSNs can accomplish a variety of tasks including environment monitoring, battlefield surveillance, target localization and tracking, and many more [1], [2]. Bandwidth and power constraints are two primary issues that need to be addressed in network design and algorithm development, as limited communication bandwidth is shared across the entire network and, meanwhile, the sensors are often powered by irreplaceable batteries. As such, a major challenge of the WSN research is to design bandwidth and power efficient signal processing algorithms for network processing tasks such as estimation, detection and tracking.

In this report, we consider distributed estimation of the signal power from one-bit quantized data. This problem arising from other applications such as spectrum sensing whose objective is energy detection and estimation. The problem is to estimate a *scale* parameter associated with the sensor observations. Specifically, suppose we have N spatially distributed sensors, each sensor making an independent and identically distributed (i.i.d.) observation x_n from a certain distribution, $p_X(x)$, with zero mean and unknown variance σ^2.

The problem of interest is to design one-bit quantization strategies, $\{Q_n(\cdot)\}$, to convert $\{x_n\}$ into binary data $\{b_n\}$ which are forwarded to a fusion center (FC), and to find an effective estimate of the standard deviation or scale parameter, σ, from $\{b_n\}$ at the FC. Such a problem finds important applications, for example, in cognitive radios where a group of secondary users collaboratively measure the power of a primary user signal for opportunistic spectrum usage [3]–[5], and in many other sensor network applications such as detection and estimation which need to collect the statistics of a signal/observation noise for the algorithm design, e.g. [6], [7]. When

a quantization strategy is given, maximum likelihood (ML) estimation of σ using quantized data was considered in [8]. In this paper, we consider joint quantization and estimation, examine the impact of quantization on the estimation performance, and develop a new adaptive quantization (AQ) approach for the estimation of σ.

Specifically, two fixed quantization (FQ) schemes are firstly introduced in this report, where a single threshold and a pair of symmetric thresholds are employed, respectively. Theoretical analysis shows that the FQ scheme using dual thresholds has a better estimation performance, yielding a Cramer-Rao bound (CRB) that is about one half of that of the FQ scheme with a single threshold. Also, by choosing an optimum quantization threshold, both FQ schemes are able to achieve an estimation performance close to that of a ML estimator using unquantized data (also referred to as "clairvoyant estimator" in this paper). Specifically, for Gaussian distribution, the estimation variance of the FQ with a single threshold is within about 3 times that of the clairvoyant estimator, and the estimation variance of the FQ with a single threshold is within about 1.5 times that of the clairvoyant estimator.

Although the FQ approach provides a comparable performance to the clairvoyant estimator while requiring only one bit information from each sensor, its problem lies in that the optimum quantization threshold is dependent on the unknown parameter to be estimated, which is not usable in practice. Also, as the threshold deviates from its optimum value, its performance drops rapidly. To cope with this difficulty, we propose an adaptive quantization (AQ) approach which, with sensors *sequentially* broadcasting their quantized data, allows each sensor to adaptively adjust its quantization threshold. We design our AQ scheme by resorting to the ML estimator and a relationship between the optimum threshold and the unknown parameter found by an analysis. Our analysis shows that our proposed AQ scheme is asymptotically optimum, which yields an asymptotic CRB equivalent to that of the FQ approach with optimum threshold.

2. Approaches Taken

We firstly discuss the fixed quantization approach for distributed estimation, followed by the distributed adaptive quantization approach.

2.1 Distributed Estimation - Fixed Quantization with Single Threshold

We employ a common threshold τ for all sensors to quantize the observations into one-bit information:

$$b_n = \mathrm{sgn}\{x_n - \tau\} \tag{1}$$

To facilitate our analysis, we express x_n as

$$x_n = \sigma v_n \tag{2}$$

where v_n denotes a random variable having the same distribution as x_n but with zero mean and *unit* variance, σ is the unknown *scale* parameter to be estimated. It can be readily shown that the

probability mass function (PMF) of b_n is given by

$$P(b_n;\sigma) = (1 - F_V(\tau/\sigma))^{b_n} (F_V(\tau/\sigma))^{1-b_n} \tag{3}$$

where $p_V(x)$ and $F_V(x)$ denote the probability density function (PDF) and the cumulative distribution function (CDF) of v_n, respectively. Since $\{b_n\}$ are i.i.d., the log-PMF or loglikelihood function is

$$L_{FQS}(\sigma) = \sum_{n=1}^{N} \{b_n \log[1 - F_V(\tau/\sigma)] + (1 - b_n)\log[F_V(\tau/\sigma)]\} \tag{4}$$

The ML estimate and CRB associated with this scheme are given in the following proposition.

Proposition 1: For the FQS scheme, the ML estimate of σ is given by

$$\hat{\sigma} = \frac{\tau}{F_V^{-1}(1 - B/N)} \tag{5}$$

where F_V^{-1} denotes the inverse of the CDF, $B = \sum_{n=1}^{N} b_n$. Furthermore, the CRB for any unbiased estimator based on $\{b_n\}$ is

$$CRB_{FQS}(\sigma) = \frac{1}{N}\frac{\sigma^4}{\tau^2}\frac{F_V(\tau/\sigma)(1 - F_V(\tau/\sigma))}{p_V^2(\tau/\sigma)} \tag{6}$$

We see that the CRB depends on the quantization threshold τ. Specifically, for the Gaussian distribution, the optimum quantizationthreshold is $\circ 1.57\sigma$. To betterevaluate the performance of the FQS scheme, we compare itwith the ML estimator using *unquantized* data (also referred toas "clairvoyant estimator"), which provides a lower bound onthe achievable estimation performance of all rate-constrainedmethods, and serves as a benchmark for evaluating the efficiencyof the proposed quantization schemes. It is easy toderive (the derivation is straightforward and hence omittedhere) that for the Gaussian observations, the CRB for any unbiased estimator based on the unquantized data $\{x_n\}$ is given as

$$CRB_{NQ}(\sigma) = \frac{\sigma^2}{2N} \tag{7}$$

where we use the subscript NQ to stand for no quantization. Clearly, we see that the minimal CRB achieved by the FQS scheme using the optimum quantization threshold is only about 3 times that of the clairvoyant estimator using unquantized data. Nevertheless, from Fig. 1, we observe that the performance of the FQS scheme degrades rapidly as the thresholddeviates from its optimum value 1.57σ. Note that without any prior information of the true σ, the optimum

choice of the quantization threshold is arbitrary because the optimum threshold minimizing the CRB is dependent on the unknown parameter σ.

2.2 Distributed Estimation - Fixed Quantization with Dual Thresholds

Our previous analysis for FQS (i.e., the CRB is an even function of the threshold) motivates us to consider a symmetric quantization scheme using a pair of symmetric thresholds $\circ\tau$, which is defined as

$$b_n = \mathrm{sgn}(|x_n| - \tau) = \begin{cases} 0 & \text{if } \tau \le x_n \le \tau \\ 1 & \text{otherwise} \end{cases} \tag{8}$$

Intuitively, this quantization scheme is able to achieve a better performance as compared with the FQS scheme because the quantized bit, b_n, reveals more information about the signal variance by locating the absolute value of the observation. For this dual thresholds based quantizer, the PMF of b_n is given as

$$P(b_n;\sigma) = (2 - 2F_V(\tau/\sigma))^{b_n} (2F_V(\tau/\sigma) - 1)^{1-b_n} \tag{9}$$

It follows that the log-likelihood function is

$$L_{FQD}(\sigma) = \sum_{n=1}^{N} \left[b_n \log[2 - 2F_V(\tau/\sigma)] + (1 - b_n)\log[2F_V(\tau/\sigma) - 1] \right] \tag{10}$$

where the subscript FQD (Fixed Quantization with Dual thresholds) represents the current scheme. We have the following result regarding its ML estimate and CRB.

Proposition 2: For the FQD scheme, the ML estimate of σis given by

$$\hat{\sigma} = \frac{\tau}{F_V^{-1}(1 - B/(2N))} \tag{11}$$

The CRB for any unbiased estimator based on $\{b_n\}$ is given by

$$CRB_{FQS}(\sigma) = \frac{1}{2N} \frac{\sigma^4}{\tau^2} \frac{(2F_V(\tau/\sigma) - 1)(1 - F_V(\tau/\sigma))}{p_V^2(\tau/\sigma)} \tag{12}$$

For the Gaussian distribution, the optimum threshold τ is 1.48σ and the corresponding minimal CRB achieved is only about 1.5 times that of the clairvoyant estimator. Also, from Fig. 1, we can see that the FQD scheme outperforms the FQS scheme at all thresholds. This can be intuitively justified since the FQD scheme produces a binary bit that contains more information about the observation and the unknown parameter associated with the observations.

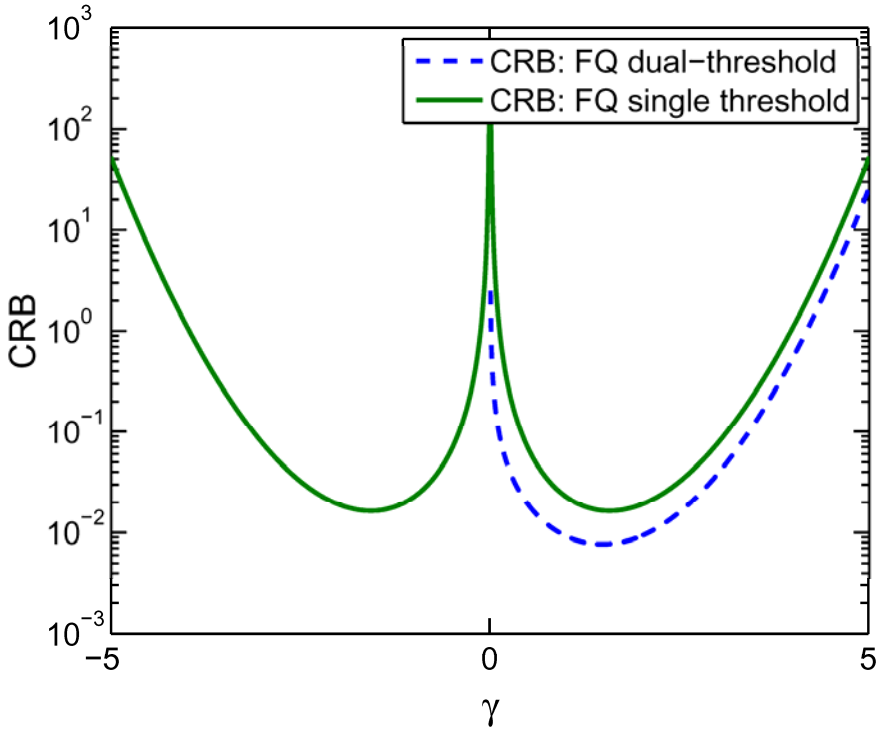


Fig.1: CRBs of the FQS and FQD schemes vs. $\gamma = \tau / \sigma$, $N = 100$.

2.3 Distributed Estimation - Adaptive Quantization

As we can see from previous analyses, both FQ schemes are very sensitive to the choice of the quantization threshold τ: the estimation performance of the FQ schemes degrades sharply as τ deviates from their optimum values. However, the optimum threshold is dependent on the unknown parameter σ to be estimated, which is not usable in practice. To cope with this difficulty, we propose a data-dependent distributed adaptive quantization (AQ) approach by which the threshold is dynamically adjusted from one sensor to another, in a way such that the threshold converges to the optimum threshold.

We adopt the following assumptions for the AQ approach:

A1 We assume each sensor sends its quantized data to the FC sequentially with the help of a scheduling algorithm.

A2 While each sensor transmits, the other sensors can listen to the transmission due to the broadcasting nature of the wireless channel. To focus on the quantization problem, we assume that the quantized data are received without errors (by using, e.g., a strong error correction code).

For the AQ approach, each sensor, say sensor n, finds its quantization threshold, τ_n, by using the

quantized data $\{b_k\}_{k=1}^{n-1}$ received from previous sensors. We firstly employ the ML estimator to compute $\hat{\sigma}_n$, where $\hat{\sigma}_n$ denotes an estimate of σ at sensor $n$based on $\{b_k\}_{k=1}^{n-1}$. The threshold τ_n is then calculated according to the $\tau_{opt} \propto \sigma$ relationship established by the FQ analyses, e.g., for Gaussian observations, $\tau_{opt} = 1.57\sigma$ if a single threshold quantization scheme is adopted or $\tau_{opt} = 1.48\sigma$ if a pair of symmetric thresholds are adopted. In this section, we only consider the AQ approach employing a pair of symmetric thresholds, i.e. each sensor quantizes its observation using the form of (8), as it yields better estimation performance. The details of the AQ scheme is described as follows.

We firstly generate two quantized bits b_1 and b_2 for initialization. For sensor 1, we use an arbitrary positive threshold, say $\tau_1 = 1$, to generate b_1:

$$b_1 = \text{sgn}(|x_1| - \tau_1) \tag{13}$$

Then, b_1 is sent to the FC and all other sensors. Upon receiving b_1, sensor 2 computes $\tau_2 = \tau_1 \Delta^{b_1} \Delta^{b_1 - 1}$, that is, $\tau_2 = \tau_1 \Delta$ if $b_1 = 1$ and $\tau_2 = \tau_1 / \Delta$ if $b_1 = 0$, and uses it to generate b_2, where Δ is a stepsize whose choice will be discussed shortly. Also, we assume that the initial threshold τ_1 and the stepsize Δ are known to all sensors. Based on the received b_1 and b_2, sensor 3 finds the ML estimate of σ as

$$\hat{\sigma}_3 = \arg\max_{\sigma} L_3(\sigma; b_1, b_2, \tau_1, \tau_2) \tag{14}$$

where

$$L_3(\sigma; b_1, b_2, \tau_1, \tau_2) = \sum_{k=1}^{2} [b_k \log[2 - 2F_V(\tau_k / \sigma)] + (1 - b_k) \log[2F_V(\tau_k / \sigma) - 1]] \tag{15}$$

denotes the log-likelihood function of σ given binary observations b_1, b_2 and the associated thresholds τ_1 and τ_2, where τ_2 can be recovered from $\tau_2 = \tau_1 \Delta^{b_1} \Delta^{b_1 - 1}$. The stepsize Δ used by sensor 2 should be large enough such that b_1 and b_2 have different discrete values. Otherwise, it can be shown that σ_3 obtained above is either infinity or zero (depending on the values of b_1 and b_2), which should be avoided. Although there is always a non-zero probability for b_1 and b_2 to have identical values, the probability can be made practically small by choosing Δ sufficiently large. In addition, if for a chosen Δ, the first two quantized bits are still of an identical value, the following sensors can keep adjusting the threshold by $\tau_{n+1} = \tau_n \Delta^{b_n} \Delta^{b_n - 1}$ until a binary bit of a different value is generated, at which point the quantization process is switched to use the ML estimator.

The threshold τ_3 is then computed as

$$\tau_3 = \mu\hat{\sigma}_3 \tag{16}$$

where μ is the coefficient of the relationship between the optimum threshold τ_{opt} and the unknown parameter σ for the corresponding FQ approach. In general, for sensor n, it first recovers the previous thresholds $\{\tau_k\}_{k=1}^{n-1}$ from the received quantized data $\{b_k\}_{k=1}^{n-2}$, which can be computed straightforwardly in a recursive manner. After obtaining $\{\tau_k\}_{k=1}^{n-1}$, sensor $n$computes its current threshold $\tau_n = \mu\hat{\sigma}_n$, where $\hat{\sigma}_n$ is given by

$$\hat{\sigma}_n = \arg\max_\sigma L_n(\sigma; \{b_k\}_{k=1}^{n-1}, \{\tau_k\}_{k=1}^{n-1}) \tag{17}$$

where

$$L_n(\sigma; \{b_k\}_{k=1}^{n-1}, \{\tau_k\}_{k=1}^{n-1}) = \sum_{k=1}^{n-1} [b_k \log[2 - 2F_V(\tau_k/\sigma)] + (1-b_k)\log[2F_V(\tau_k/\sigma) - 1]] \tag{18}$$

is the log-likelihood function of σ given $\{b_k\}_{k=1}^{n-1}$.

The ML estimator at the FC to find the final estimate of σ from the received quantized data $\{b_1, b_2, \ldots, b_N\}$ is given by

$$\hat{\sigma} = \arg\max_\sigma L_{AQ}(\sigma; \{b_k\}_{k=1}^{N}, \{\tau_k\}_{k=1}^{N}) \tag{19}$$

Note that unlike the FQ schemes, the ML estimators generally admit no closed-form solution, and a searching algorithm has to be utilized. Nevertheless, the computational complexity is moderate since only one-dimensional search is involved. We have the following result regarding the CRB of the proposed AQ approach.

Proposition 3: For continuous noise distribution $p_V(x)$, as *N*increases, the CRB of the proposed AQ scheme converges to the CRB of the FQ scheme using the optimum threshold, i.e.

$$NCRB_{AQ}(\sigma) \to NCRB_{FQD}(\tau_{opt}; \sigma) \tag{20}$$

Note that we multiply the CRBs on both sides by a factor *N*because we have to properly normalize the CRBs, otherwise both terms vanish with an increasing *N*, and the claim loses its meaning. This result indicates that our AQ scheme adaptively finds the best threshold by learning from prior transmissions. Without any prior knowledge of the unknown parameter, the proposed AQ scheme is able to asymptotically achieve a CRB which is attained by the FQD scheme with an optimum threshold.

3. Results

We firstly examine the information loss of the FQ and AQ schemes relative to the ML estimator using unquantized data. The concept "information loss" is defined as the ratio (in dB) of the CRB for the proposed scheme to the CRB for the clairvoyant estimator using unquantized data:

$$IL = 10\log\frac{CRB_{Q-based}(\sigma)}{CRB_{NQ}(\sigma)}$$

where we use the subscript Q-based to represent any quantization scheme. Note that although, for the AQ scheme, an exact computation of the CRB is impossible, nevertheless, it can still be evaluated numerically by Monte Carlo integration.

We set $\sigma = 1$. Fig. 2 shows the information loss of the FQ and AQ schemes as a function of the number of sensors, *N*. It can be seen that the information loss of the FQ schemes is independent of the number of sensors, *N*. Also, when the optimum thresholds are used, i.e. $\tau = 1.57$ for FQS and $\tau = 1.48$ for FQD, the FQ schemes incur a moderate information loss, which is about 5dB for FQS and 2dB for FQD. However, the FQ schemes are very sensitive to the value of τ; as the threshold τ becomes more apart from the optimum value (even not too far apart), the performance of the FQ schemes degrades significantly. As for the AQ scheme, the information loss decreases with an increasing *N*. This is because the AQ scheme benefits from the previous transmissions by adaptively choosing a proper quantization threshold. Also, we observe that the information loss of the AQ scheme approaches that of the FQD scheme with optimum threshold, i.e. $\tau = 1.48$, which corroborates our previous claim in Proposition 3.

The mean square errors (MSEs) of the ML estimators for the FQD and AQ schemes are included and compared with the corresponding CRB in Fig. 3, where we set $\sigma = 1$. For the AQ scheme and the FQD scheme with optimum threshold $\tau = 1.48$, it is observed that the MSEs approach the CRBs within a moderate number of sensors, *N*. However, this is not true for the FQD scheme with a non-optimum threshold $\tau = 3$. In this case, the ML estimator needs much more sensors to converge to its corresponding CRB. As we also see from this figure, the performance of the AQ scheme approaches that of the FQD with optimum threshold ($\tau = 1.48$) while without knowing any prior information of the unknown parameter σ.

We plot the MSEs of the ML estimators for the FQ schemes as a function of $\gamma = \tau/\sigma$ in Fig. 4, where we set $N = 100$ and $\sigma = 1$. It is seen that the ML estimators achieves its asymptotic performance with moderate number of sensors ($N = 100$) when the ratio γ is around its optimum value.

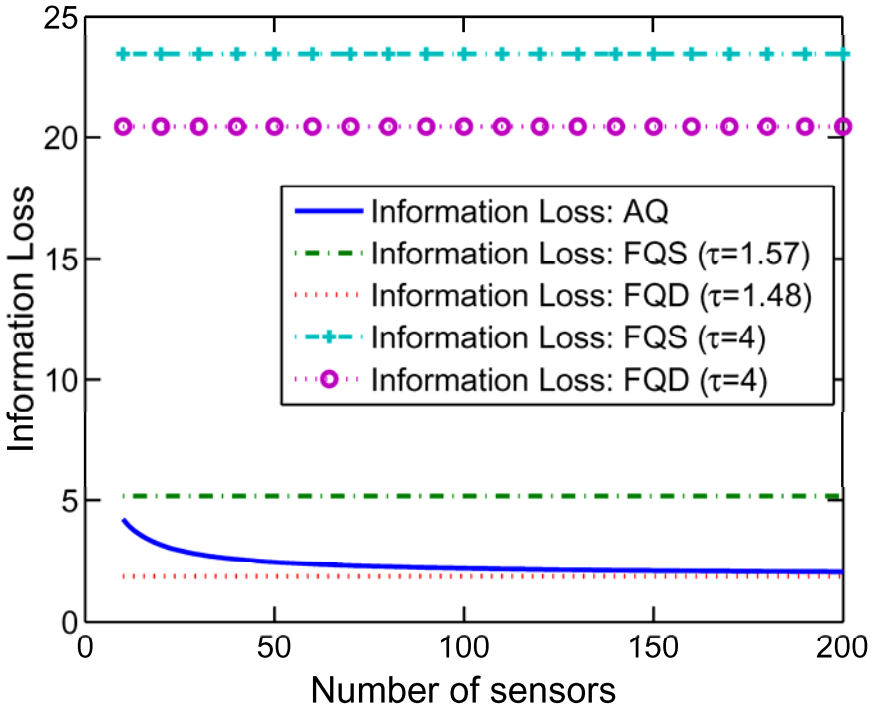


Fig. 2 Information loss of the FQ and AQ schemes relative to the ML estimator using unquantized data.

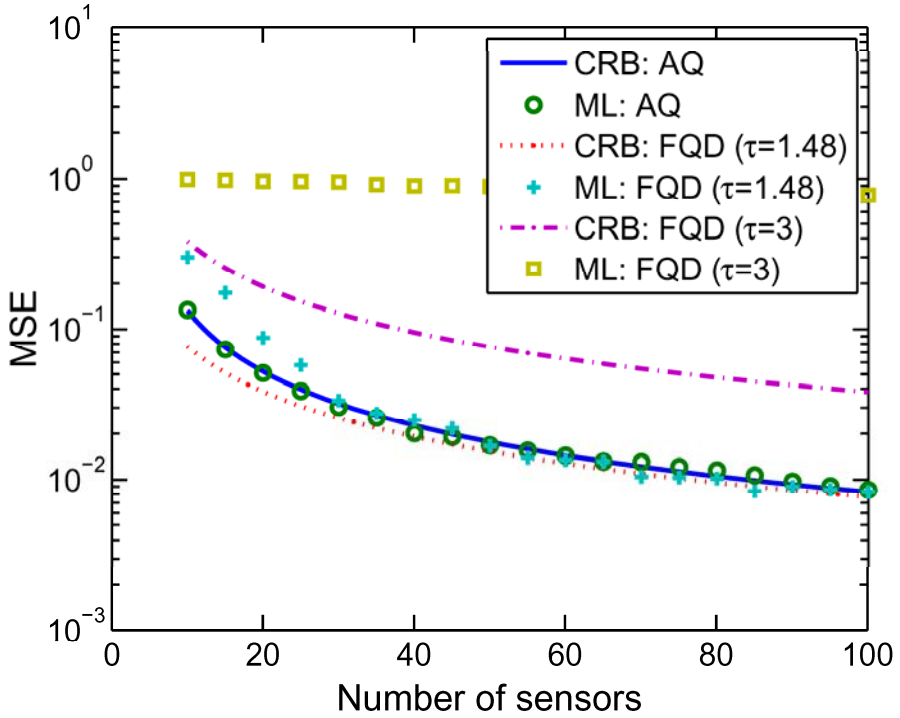


Fig. 3: MSEs and CRBs of the FQD and AQ schemes.

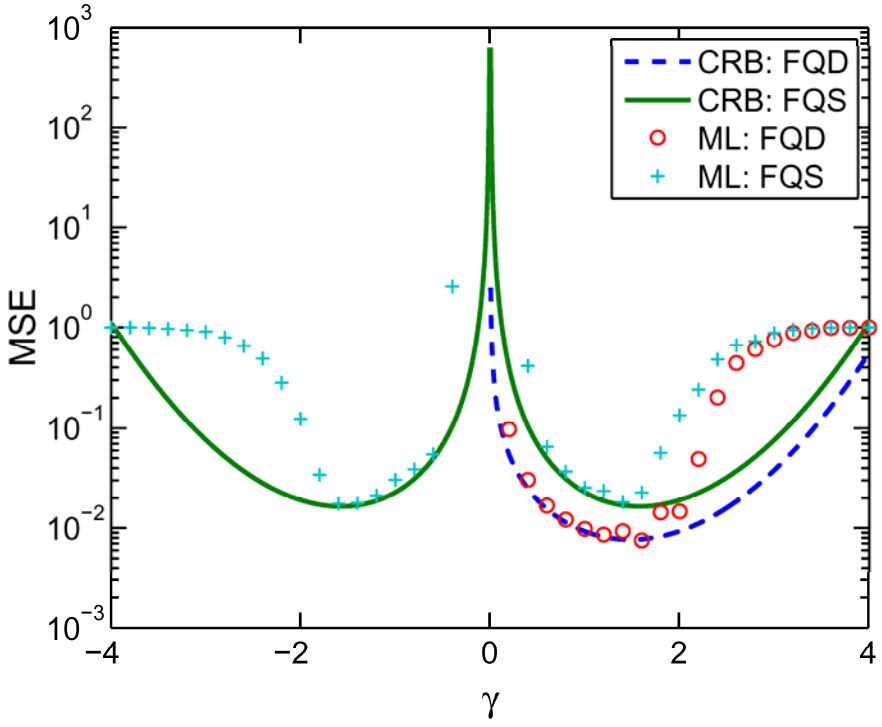


Fig. 4: MSEs and CRBs of the FQ schemes versus γ, $\sigma = 1$, $N = 100$

4. Potential Applications

The problem of power estimation from multi-sensors' observations was considered in the paper. In particular, we assume each sensor makes an independent observation from a certain distribution with zero mean and unknown variance. The objective is to estimate the standard deviation associated with the distribution in bandwidth/power constrained wireless sensor networks (WSNs). Two fixed quantization (FQ) schemes and an adaptive quantization (AQ) scheme were proposed and their corresponding MLEs were developed. CRB analyses show that the FQ schemes are able to achieve an estimation performance close to that of the clairvoyant estimator using unquantized data when the optimum quantization thresholds are employed. A drawback of the FQ approach is that its estimation performance is sensitive to the quantization threshold, whose choice is always tricky in practice since the optimum thresholds are dependent on the unknown parameter. The proposed AQ scheme, in contrast to the FQ approach, can effectively address this problem. Our analysis shows that the proposed AQ approach is asymptotically optimum. Without any prior knowledge of the unknown parameter, it yields an asymptotic CRB equivalent to that of the FQ approach with the optimum threshold. Simulation results were presented to corroborates our claims.

While we considered only the 1-bit (per sample) quantization case, our AQ approach can be extended for multi-bit quantization. Consider, for example, AQ-FS. Instead of using a 1-bit quantizer to just take the sign of the difference between the current observation x_n and quantization threshold τ_n, a multi-bit quantizer (either uniform and non-uniform) can be used to

quantize $x_n - \tau_n$ and provide finer adjustment of the subsequent quantization threshold. This multi-bit AQ-FS effectively uses a number of stepsizes (as opposed to a fixed stepsize in 1-bit AQ-FS) determined by the number of bits used for quantization. Extensions of AQ-VS are also possible and will be reported elsewhere.

5. Project Assessment

We have completed the major work for the proposed tasks, namely, low-rate quantizer design, collaborative signal estimation of signal power for intelligent wireless sensor networks. The developed techniques and methods are ready to be delivered.

6. Reference List

1. D. Li, K. D. Wong, Y. H. Hu, and A. M. Sayeed, "Detection, classification, and tracking of targets," *IEEE Signal Processing Magazine*, vol. 19, no. 2, pp. 17–29, March 2002.

2. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, pp. 102–114, August 2002.

3. A. Ghasemi and E. S. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," in *Proceedings of the IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Network*, November 2005, pp. 131–136.

4. G. Ganesan and Y. G. Li, "Cooperative spectrum sensing in cognitive radio: Part I: two user networks," *Transactions on Wireless Communications*, vol. 6, no. 6, pp. 2204–2213, 2007.

5. ——, "Cooperative spectrum sensing in cognitive radio: Part II: multiers networks," *Transactions on Wireless Communications*, vol. 6, no. 6, pp. 2214–2222, 2007.

6. A. Dogandˇzi´c and B. Zhang, "Distributed estimation and detection for sensor networks using hidden markov random field models," *IEEE Trans. Signal Processing*, vol. 54, no. 8, pp. 3200–3215, Aug. 2006.

7. K. Zhang and X. R. Li, "Optimal sensor data quantization for best linear unbiased estimation fusion," in *IEEE Conference on Decision and Control*, Atlantis, Paradise Island, Bahamas, 2004.

8. A. Ribeiro and G. B. Giannakis, "Bandwidth-constrained distributed estimation for wireless sensor networks - Part II: unknown probability density function," *IEEE Transactions on Signal Processing*, vol. 54, no. 7, pp. 2784–2796, July 2006.

Appendix: Statement of Work

Collaborative Spectrum Sensing and Signal Processing (Li)

Power constraint is an important design objective since cooperating CUs are often mobile and powered by battery. On the other hand, cooperation requires message exchange among the cooperating CUs. This causes additional bandwidth overhead that needs to be minimized; otherwise, it will eat up the bandwidth gain provided by dynamic spectrum access. To address these issues, we consider collaborative sensing, where each CU quantizes its measurement of the spectrum usage, by employing a specially designed low-rate quantizer (e.g., 1 to a few bits per measurement), before sharing it with the other CUs. Our proposed approach will build on the adaptive quantization (AQ) technology, our recent research result funded by the ARDEC, originally introduced for distributed estimation in a wireless sensor network. At 1 bit per measurement, our AQ approach has been found to yield nearly identical performance to the case where the cooperating nodes share unquanitzed observations, therefore providing a compelling solution in power- and bandwidth-constrained environments. Specific research subtasks to be addressed in this work include the following.

1.1 Adaptive quantization for power estimation: While we will build on our previous research on AQ, existing AQ techniques were developed for the estimation of a position parameter (i.e., the mean of the random observation) and, therefore, cannot be directly applied to the estimation of the power, which is a scale parameter that requires a symmetric quantizer (in contrast, our previous AQ techniques are all asymmetric). As the quantizer structure is different, we have to develop different schemes to adaptively change the quantizer thresholds from one CU to another.

1.2 Distributed estimation algorithms: A most general spectrum sensing approach (without requiring excessive prior knowledge of the PU, e.g., its modulation format, waveforms, etc.) is to obtain an accurate estimate of the power within a given frequency band and compare it with a threshold (i.e., the power or energy detector). We will develop distributed and collaborative power estimation techniques using quantized observations for reliable spectrum sensing. We will consider both high-performance parametric estimators, which require knowledge of the statistical distribution of the measurements, and robust non-parametric estimators, which require no such information and are more versatile (though some performance loss is expected).

1.3 Collaborative spectrum sensing algorithms: The power estimates as obtained in the previous task need to be processed by a detection algorithm which functions based on some detection criterion, e.g., the Neyman-Pearson criterion. We will develop effective distributed detectors for collaborative spectrum sensing in the Neyman-Pearson sense, which minimizes the probability of *missing* (i.e., the event of declaring no spectrum "white space" when there is one) for a given probability of *false alarm* (the event of claiming the presence of spectrum white space when there is none). We will also consider in the detection process the effects of fading and interference, which are ubiquitous in a wireless environment.

Final Report

W15QKN-05-D-0011, Task Order 43

(September 15, 2009)

Submitted by S. Tewksbury

Contract Number: W15QKN-05-D-0011, Task Order 43

Contract Name: Embedded Intelligent Sensor Network Systems

Task 1

Cognitive & Network Centric Military Communications

Subtask 2

Adaptive Architecture and Access Protocols

Prof. Yu-Dong Yao and Dr. Hongbing Cheng
Department of Electrical and Computer Engineering
Stevens Institute of Technology
Hoboken, NJ 07030
E-mail: yyao@stevens.edu

Abstract

In this project, we propose to use a cross-network cognitive relay technique to mitigate the co-channel interference (CCI) in infrastructure communication networks. In the proposed network, relay stations (RS) equipped with cognitive radio are deployed near the boundary of an infrastructure network to construct a complementary ad hoc network. Specifically, cellular network is selected as an example of infrastructural network. The base station (BS) and RS in each cell operate in the same spectrum band as primary and secondary transmitters, respectively. Once an interference limited mobile station (MS) requests an RS for assistance, the RS senses the spectrum band and accesses a spectrum hole to forward its received signal (and interference) to the MS. At the receiver of the MS, optimum combining is employed to combine the original signal received from the BS and the relayed signal to cancel the CCI. The system performance is analyzed in terms of the outage capacity and the average capacity considering the impact of the availability of cognitive relay channels and the link quality between RS and MS. The location and coverage radius of RS are designed based on the requirement of the RS-MS link quality. Finally, simulation results are given to validate the theoretical analysis and to show the capacity improvement due to the CCI cancellation with the assistance of cognitive relay.

In addition, we conduct network performance analysis for cognitive radio network with two different access protocols. One is TDMA for the primary network and slotted ALOHA for the secondary network. The other is slotted ALOHA for both primary network and secondary network. Simulation results are shown to validate the theoretical analysis.

INTRODUCTION

In a network centric environment, a great challenge is to accommodate and manage different network architectures and access protocols for different quality of service (QoS) requirements. Cognitive communication is a promising technology to sustain the coexistence of multiple networks devoid of comprehensive frequency planning. This research will focus on the hybrid network architecture in the cognitive and network centric communication systems.

Infrastructure networks and ad hoc networks are two most popular network architectures in both military and commercial communications. In an infrastructure network, there is a central node, which centrally control the resource allocation and all the subscriber nodes only communicate with the central node. Since the transmit power of the central node is limited, the cover area of an infrastructure network is limited. Many infrastructure networks must be deployed and frequency reuse is used for the seamless coverage. Therefore, the cross-network co-channel interference (CCI) is unavoidable in infrastructure networks. Cellular network is a typical infrastructure network and its performance is degraded a lot due to the CCI, also known as inter-cell interference (ICI).

In ad hoc networks, there is no central node and each pair of nodes communicated with each other through one or more hops. Since the communication range of each node is very small, ad hoc network is suitable for high-density small-range communications. In this project, we will

propose a hybrid network, which use some ad hoc networks as complement cognitive radio networks to help a cellular network cancel the ICI.

As has been known, many techniques were proposed to mitigate the ICI. However, the conventional methods usually compromise spectral efficiency in order to reduce the ICI, such as reducing the frequency reuse factor, spreading spectrum and frequency hopping [1]–[3]. To mitigate the ICI without reducing the the spectral efficiency of cellular systems, single input and multiple output (SIMO) or multiple input and multiple output (MIMO) techniques with optimum combing was proposed [4], [5]. The performance improvement obtained in SIMO and MIMO systems through optimum combining has been analyzed and simulated by many researchers [6], [7]. However, the space and resource limit is a major obstacle in practice for the deployment of multiple antennas at an MS.

Multi-hop relay is a promising technique for cellular systems to enhance throughput and extend coverage [8]. Its basic idea is to employ relay stations (RS) between base stations (BS) and MS to improve the performance of signal transmissions. The RS communicate with MS through an ad hoc network. A hybrid cellular-ad hoc network is thus constructed [9][10]. Two types of relay schemes have been proposed for cellular systems. One is the conventional relaying scheme without cooperative diversity, where the MS can only received the signal forwarded by the RS. This type of scheme is used only for path loss compensations, or to divert traffic from possibly congested areas to lower traffic areas. The other is the cooperative relay scheme, where the MS can receive both the signals originally transmitted by the BS and forwarded by the RS [11]. When the BS and the RS transmit in orthogonal channels (different time slots or frequency bands), the MS can combine the two signals to obtain the diversity gain. It is interesting to notice that the combination of the received signals from BS and RS can also be used to cancel the ICI, which is similar to the SIMO system with two receive antennas. However, the use of relay generally requires additional time or frequency resources for the communications between RS and MS.

As have been reported, most radio systems do not utilize all the assigned frequency bands all the time [12]. The unused frequency bands are called spectrum holes. Cognitive radio technique is recently proposed to improve the spectrum utilization by allowing secondary users to access the spectrum holes [13]. The concept of cognitive relay is proposed by several researchers for different scenarios [14]–[16]. The primary idea is to use cognitive radio nodes as relay to assist the communications of primary nodes. Since the relay nodes cognitively utilize the spectrum assigned to but unused by the primary nodes, it doesn’t incur additional resource consumption. The use of cognitive relay in cellular systems was considered in [17] and the paper only considered a noise-limited environment without ICI. It assumes that the RS utilizes the spectrum hole in ultra-high frequency (UHF) band or industry, industrial, scientific and medical (ISM) bands and no interference exists between the RS-MS link and BS-MS link.

In this project, we propose a cognitive-relay based hybrid cellular-ad hoc network by applying the cognitive radio technique in the relay network to mitigate the ICI. In the proposed scheme, several RS equipped with cognitive radio are deployed around each cell’s boundary. The RS and MS both receive the signal from the home cell BS and ICI from other co-channel BS in the downlink channel. Instead of using other bands as in [17], we assume that the cognitive RS in each cell operate in the spectrum band assigned for the primary downlink communications (i.e., BS-MS links) in the cell. If an interference-limited MS requires relay from RS, the RS will sense the spectrum band and find an unutilized channel to amplify and forward its received signal and

interference to the MS. The MS combines the received signals and interferences from BS and RS to perform the ICI mitigation. We study the outage capacity of the MS in the proposed hybrid network and identify two parameters which impact the system performance. One is the availability probability of the cognitive relay channel and the other is the link quality between the RS and MS (determined by path loss and ICI). Theoretical models are formulated to quantify and derive the two parameters. The locations and coverage of RS are designed based on the requirement of the link quality between the RS and MS. Theoretical and simulation results are provided to show the effectiveness of the proposed scheme.

In addition, at the end of the project, we analyzed the network throughput of cognitive radio networks. Media access control (MAC) issue plays a critical role in the cognitive radio network design. We considered cognitive radio networks with two different access protocols. One is TDMA for the primary network and slotted ALOHA for the secondary network. The other is slotted ALOHA for both primary network and secondary network. Simulation results are shown to validate the theoretical analysis.

APPROACH TAKEN

1. System Model

We consider a downlink fading channel in a multi-cell network, where each cell is interfered by N_I co-channel cells. Different users in one cell are allocated with orthogonal channels to avoid intra-cell interference, such as using time division multiple access (TDMA), code division multiple access (CDMA) or orthogonal freqeuncy division multiple access (OFDMA). However, the use of the same channel in different cells may cause ICI. The home cell is denoted as Cell

0 and the interference cells are from Cell 1 to N_I. Correspondingly, the base stations (BS) are denoted as BS 0 to N_I.

To help MS against the ICI, several RS are deployed around the cell boundary of each cell. RS and MS are equipped with two types of radio functionalities. One is the primary radio to communicate with BS. The other is the secondary radio, or called cognitive radio, for opportunistically communications between RS and MS. For the downlink transmission, RS and

MS receive signals from all BS through the primary radio. If a MS suffers from strong ICI and has a low quality link with BS, it will need the assistance from RS. One of the RS is selected to be the MS' associated RS and it will relay its received signal to the MS through cognitive radio. Specifically, it will first sense the spectrum band allocated to the primary radio to detect a spectrum hole (vacant channel). Many existing spectrum sensing techniques, such as energy detection, likelihood detection and so on, can be applied for the detection [18], [19]. Once a spectrum hole is detected, the RS will cognitively adjust its radio parameters to communicate with the MS through the spectrum hole. This is called cognitive relay. Fig. 1 illustrates our proposed cellular network with cognitive relay.

A MS may operate in noise-limited regime or interference-limited regime. Generally, the

operation condition is quantified in terms of the interference-to-noise ratio (INR), $\psi = P_{ICI} / \sigma^2$, where P_{ICI} is the power of the ICI and σ^2 is the power of the background noise [20]. If $\psi > 1$, the ICI dominates over noise. When $\psi >> 1$, the system is regarded as interference limited. In this paper, we assume that all the BS have the same transmit power. The ICI power of a MS is totally determined by its location and increased with the increase of its distance to the home cell BS. Therefore, we simply classify the MS with $r \le r_0$ as noise-limited MS and the MS with $r > r_0$ as interference-limited MS, respectively, where r is the distance between the MS and its home BS and r_0 is a given threshold.

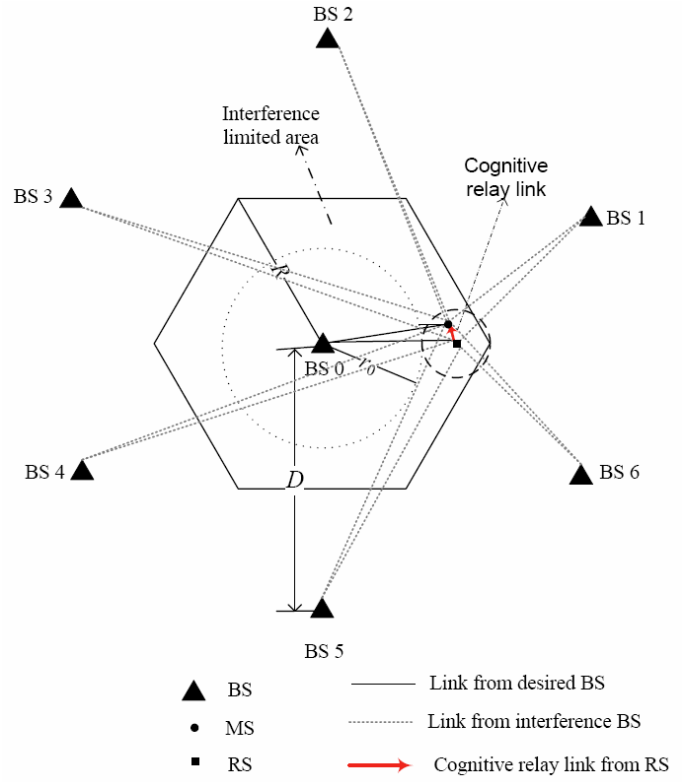


Fig. 1 The cellular system model with cognitive relay

We assume that only interference-limited MS will request the cognitive relay and all the RS are interference-limited since they are deployed near the cell boundary. The RS should be appropriately deployed so that each interference-limited MS is covered by at least one RS. The location and coverage of RS will be discussed in the next section.

To simplify the model, the background noises at the interference-limited MS and RS are assumed to be negligible. The received signals of an interference-limited MS and its associated RS through the primary radio are written as

$$y_{\mathrm{b,m}} = \sqrt{P_{\mathrm{tb}}} g_{\mathrm{b}_0,\mathrm{m}} h_{\mathrm{b}_0,\mathrm{m}} x_0 + \sum_{i=1}^{N_I} \sqrt{P_{\mathrm{tb}}} g_{\mathrm{b}_i,\mathrm{m}} h_{\mathrm{b}_i,\mathrm{m}} x_i \quad (1)$$

$$y_{\mathrm{b,r}} = \sqrt{P_{\mathrm{tb}}} g_{\mathrm{b}_0,\mathrm{r}} h_{\mathrm{b}_0,\mathrm{r}} x_0 + \sum_{i=1}^{N_I} \sqrt{P_{\mathrm{tb}}} g_{\mathrm{b}_i,\mathrm{r}} h_{\mathrm{b}_i,\mathrm{r}} x_i \quad (2)$$

respectively, where P_{tb} is the transmit power of each BS. x_0 is the desired signal transmitted from the BS of the home cell to the MS and x_i, with $i = 1, 2, \cdots, N_I$, is the ICI signal from the BS of Cell i, i.e., the ith BS. $h_{\mathrm{b}_i,\mathrm{m}}$ and $h_{\mathrm{b}_i,\mathrm{r}}$ are complex Gaussian-distributed random variables to represent the flat fading channels of the ith BS-MS link and BS-RS link, respectively , which are assumed to have unit power, i.e., $E[|h_{\mathrm{b}_i,\mathrm{m}}|^2] = 1$ and $E[|h_{\mathrm{b}_i,\mathrm{r}}|^2] = 1$. $g_{\mathrm{b}_i,\mathrm{m}}$ and $g_{\mathrm{b}_i,\mathrm{r}}$ are the propagation path losses of the ith BS-MS link and BS-RS link, respectively, which are calculated as

$$g_{\mathrm{b}_i,\mathrm{m}} = \sqrt{|g_0|^2 \, d_{\mathrm{b}_i,\mathrm{m}}^{-n}} \quad (3)$$

$$g_{\mathrm{b}_i,\mathrm{r}} = \sqrt{|g_0|^2 \, d_{\mathrm{b}_i,\mathrm{r}}^{-n}} \quad (4)$$

for $i = 0, 1, 2, \cdots, N_I$, where $|g_0|^2$ is the reference channel gain at the distance of 1 m. $d_{\mathrm{b}_i,\mathrm{m}}$ and $d_{\mathrm{b}_i,\mathrm{r}}$ are the communication distances of the ith BS-MS link and BS-RS link, respectively. Notice that $d_{\mathrm{b}_i,\mathrm{m}} = r$. n is the path loss factor.

After receiving the signal with ICI, the MS sends a relay request to its associated RS. The RS then detects the spectrum band to sense if there is a vacant channel. If no channel is found, the request is discarded. Otherwise, the RS amplifies and relays its received signal, including the desired signal and ICI, to the MS through the vacant channel following AF relay protocol. The received signal at the MS through this cognitive relay channel is

$$y_{\mathrm{r,m}} = \sqrt{\alpha P_{\mathrm{tb}}} g_{\mathrm{r,m}} h_{\mathrm{r,m}} g_{\mathrm{b}_0,\mathrm{r}} h_{\mathrm{b}_0,\mathrm{r}} x_0 + I_{\mathrm{r,m1}} + I_{\mathrm{r,m2}} \quad (5)$$

with

$$I_{\mathrm{r,m1}} = \sqrt{\alpha P_{\mathrm{tb}}} g_{\mathrm{r,m}} h_{\mathrm{r,m}} \sum_{i=1}^{N_I} g_{\mathrm{b}_i,\mathrm{r}} h_{\mathrm{b}_i,\mathrm{r}} x_i \quad (6)$$

$$I_{\mathrm{r,m2}} = \sqrt{P_{\mathrm{tb}}} \sum_{i=1}^{N_I} g_{\mathrm{b}_i,\mathrm{m}} \tilde{h}_{\mathrm{b}_i,\mathrm{m}} \tilde{x}_i \quad (7)$$

where α is the power amplify factor of the RS, which is assumed to be fixed over small-scale channel fading (i.e., fixed-gain relay) and calculated as [21], [22]

$$\alpha = \frac{P_{\text{tr}}}{P_{\text{tb}} \sum_{i=0}^{N_I} | g_{\text{b}_i,\text{r}} |^2} \tag{8}$$

where P_{tr} is the transmit power of the RS. $g_{\text{r,m}}$ and $h_{\text{r,m}}$ are the propagation path loss and small-scale channel fading between the RS and the MS. Similarly,

$$g_{\text{r,m}} = \sqrt{| g_0 |^2 \, d_{\text{r,m}}^{-n}} \tag{9}$$

where $d_{\text{r,m}}$ is the distance between the MS and its associated RS. The received signal in (5) contains two parts of ICI, $I_{\text{r,m1}}$ and $I_{\text{r,m2}}$. $I_{\text{r,m1}}$ is the ICI intentionally transmitted from the RS to the MS, which will be used to cancel the ICI at the MS and $I_{\text{r,m2}}$ is the inevitable ICI transmitted by other BS over the relay channel. $\tilde{h}_{\text{b}_i,\text{m}}$ is the small scale fading of the relay channel between the ith BS and the MS. $\tilde{x}_i$ is the signal transmitted by the ith BS over the relay channel. Notice that $\tilde{h}_{\text{b}_i,\text{m}}$ and $\tilde{x}_i$ are independent to $h_{\text{b}_i,\text{m}}$ and x_i, respectively, since the cognitive relay channel is orthogonal to primary channels.

The ICI, $I_{\text{r,m2}}$, exists in the cognitive relay channel because that the RS can only detect if a channel is occupied by primary radios in its own cell, but cannot detect if it is occupied in neighboring co-channel cells. Correspondingly, the transmission of RS will also cause ICI to MS in neighboring co-channel cells. To protect the primary communications in neighboring cells, we have to constraint the transmit power of RS so that its interference to neighboring cells is tolerable. This constraint is quantified in terms of the ratio between the maximum ICI power caused by the RS and the minimum signal power in neighboring cells and written as

$$\frac{P_{\text{tr}} d_{\min}^{-n}}{P_{\text{tb}} R^{-n}} \le \lambda \tag{10}$$

where $d_{\min}$ is the minimum distance from the RS to MS in neighboring cells and R is the cell radius. λ is the allowed interference-to-signal ratio (ISR) at the MS. Assuming that each RS always transmits with the maximum power, we have

$$\alpha = \lambda \frac{R^{-n}}{d_{\min}^{-n} \sum_{i=0}^{N_I} | g_{\text{b}_i,\text{r}} |^2} \tag{11}$$

The received signals of the MS from BS and RS, i.e., (1) and (5), can be represented in a vector form as

$$\mathbf{y} = \sqrt{P_{\text{tb}}}(\mathbf{c}_0 x_0 + \sum_{i=1}^{N_I} \mathbf{c}_i x_i) + \mathbf{I} \tag{12}$$

with $\mathbf{y} = [y_{\text{b,m}}, y_{\text{r,m}}]^T$, $\mathbf{c}_i = [g_{\text{b}_i,\text{m}} h_{\text{b}_i,\text{m}}, \sqrt{\alpha} g_{\text{b}_i,\text{r}} h_{\text{b}_i,\text{r}} g_{\text{r,m}} h_{\text{r,m}}]^T$ for $i = 0,1,2,\cdots,N_I$ and $\mathbf{I} = [0, I_{\text{r,m2}}]^T$.

At the receiver, the two received signals will be combined to cancel the ICI and improve the system performance. The combination output is

$$\mathbf{z} = \mathbf{w}^H \mathbf{y} \tag{13}$$

where $\mathbf{w}$ is the combining vector. To maximize the SIR, the optimum combining vector is given by [6]

$$\mathbf{w}_{opt} = \mathbf{\Omega}^{-1} \mathbf{c}_0 \tag{14}$$

where

$$\mathbf{\Omega} = \sum_{i=1}^{N_I} \mathbf{c}_i \mathbf{c}_i^H + \frac{E[\mathbf{I}\mathbf{I}^H]}{P_{\text{tb}}} \tag{15}$$

2. Outage Capacity Analysis

Outage capacity is an important measure of a communication system, especially in a slow fading channel environment, where the delay requirement is small compared to the coherent time. The definition of outage capacity is written as [23]

$$C_\varepsilon = \arg \max_{C_{\text{th}}} \{P_{\text{out}}(C_{\text{th}}) \le \varepsilon\} \tag{16}$$

where C_ε is the outage capacity, ε is the target outage probability. $P_{\text{out}}(C_{\text{th}})$ is the outage probability with a threshold capacity C_{th}, which is calculated as

$$P_{\text{out}}(C_{\text{th}}) = \Pr\{C(\gamma) \le C_{\text{th}}\} \tag{17}$$

where $C(\gamma)$ is the instantaneous capacity with a given SIR γ calculated as

$$C(\gamma) = \log_2(1+\gamma) \tag{18}$$

Considering an interference-limited MS in our cellular system model, if the MS fails to request the relay, the instantaneous SIR is

$$\gamma_{\text{norelay}} = \frac{|\, g_{\text{b}_0,\text{m}} h_{\text{b}_0,\text{m}} \,|^2}{\sum_{i=1}^{N_I} |\, g_{\text{b}_i,\text{m}} h_{\text{b}_i,\text{m}} \,|^2} \tag{19}$$

If the MS obtains the help of relay and conducts the optimum combining at the receiver, the instantaneous output SIR is

$$\gamma_{\text{oc}} = \mathbf{c}_0^H \mathbf{\Omega}^{-1} \mathbf{c}_0 = \hat{\mathbf{c}}_0^H \hat{\mathbf{\Omega}}^{-1} \hat{\mathbf{c}}_0 \tag{19}$$

where $\hat{\mathbf{c}}_i = [g_{\text{b}_i,\text{m}} h_{\text{b}_i,\text{m}}, g_{\text{b}_i,\text{r}} h_{\text{b}_i,\text{r}}]^T$ for $i = 0,1,2,\cdots,N_I$, $\hat{\mathbf{\Omega}} = \hat{\mathbf{C}}_I \hat{\mathbf{C}}_I^H + \begin{bmatrix} 0 & 0 \\ 0 & \delta \sum_{i=1}^{N_I} g_{\text{b}_i,\text{m}}^2 \end{bmatrix}$,

$\hat{\mathbf{C}}_I = [\hat{\mathbf{c}}_1, \hat{\mathbf{c}}_2, \cdots, \hat{\mathbf{c}}_{N_I}]$, where δ is defined as $\delta = \frac{1}{\alpha |\, g_{\text{r,m}} h_{\text{r,m}} \,|^2}$, which is the reciprocal of the RS-MS link gain (the power amplify factor at the transmitter of the link multiplied by the channel gain). We thus use δ to quantify the RS-MS link quality.

The outage probability of the MS with cognitive relay is

$$P_{\text{out}}(C_{\text{th}}) = (1-p) P_{\text{out1}}(C_{\text{th}}) + p P_{\text{out2}}(C_{\text{th}}) \tag{20}$$

where $P_{\text{out1}}(C_{\text{th}}) = \Pr(\gamma_{\text{norelay}} \le \gamma_{\text{th}})$, $P_{\text{out2}}(C_{\text{th}}) = \Pr(\gamma_{\text{oc}} \le \gamma_{\text{th}})$, $\gamma_{\text{th}} = 2^{C_{\text{th}}} - 1$ and p is the availability probability of the cognitive-relay channel, which will be discussed next section.

3. Availability Probability of the Cognitive-Relay Channel.

We establish a model to derive the availability probability of the relay channel, p, which is an important factor impacting the outage capacity. Assuming that there are N_c orthogonal channels allocated to each cell and the user number in each cell is N_u with $N_u \le N_c$. Each user is randomly allocated with one channel for communications with BS. Different users' channels are orthogonal. The loading factor is defined as the ratio between the user number and the available channel number,

$$\rho = \frac{N_u}{N_c} \tag{21}$$

It is worth noting that each user doesn't occupy the allocated channel all the time. In other words, there is an activity factor β for each user, which is the probability that the user is active.

Therefore, the probability that there are K vacant channels unoccupied by the primary communications is

$$p_{ch}(K)=\begin{cases}0 & K<(1-\rho)N_c \text{ or } K>N_c \\ \mathrm{C}_{\rho N_c}^{N_c-K}\,\beta^{N_c-K}(1-\beta)^{K-(1-\rho)N_c} & (1-\rho)N_c\le K\le N_c\end{cases} \tag{22}$$

where $\mathrm{C}_n^k=\dfrac{n!}{k!(n-k)!}$.

The number of interference-limited users is denoted as N_{ui}. If all the MS are uniformly distributed in the home cell, N_{ui} is calculated as

$$N_{ui}=\frac{S_i}{S}N_u=(1-\frac{2\pi}{3\sqrt{3}}\frac{r_0^2}{R^2})N_u \tag{23}$$

where S is the area of a whole cell and S_i is the area of the interference-limited part of the cell. r_0 is the interference-limited threshold distance and R is the cell radius. Notice that N_{ui} must be round to the nearest integer.

The probability that there are M active interference-limited users requesting cognitive relay channels is

$$p_{req}(M)=\begin{cases}\mathrm{C}_{N_{ui}}^{M}\,\beta^{M}(1-\beta)^{N_{ui}-M} & M\le N_{ui} \\ 0 & M>N_{ui}\end{cases} \tag{24}$$

The M active interference-limited users will compete for the K available vacant channels. Assuming that the K channels are randomly allocated to the M users, the probability that one relay channel is available for a given user is

$$p_a(K,M)=\begin{cases}1 & M\le K \\ K/M & M>K\end{cases} \tag{25}$$

By averaging over all K and M, the average availability probability of the cognitive-relay channel for a given user is

$$p=\sum_{K=(1-\rho)N_c}^{N_c}\sum_{M=0}^{N_{ui}}p_{ch}(K)\,p_{req}(M)\,p_a(K,M) \tag{26}$$

4. Interference Analysis and Avoidance: Location and Coverage of RS

As mentioned in Subsection III.A, the effectiveness of cognitive relay depends on the link quality between RS and MS. Therefore, we need to carefully determine the location and coverage of RS so that the RS-MS link quality is good enough. We assume that the RS-MS link can be regarded as perfect if

$$\Pr\{\delta > \delta_0\} \le \xi \tag{26}$$

where δ_0 is a threshold, which indicates the quality requirement of the RS-MS link.

Since $|h_{\mathrm{r,m}}|^2$ follows an exponential distribution, the above constraint is rewritten as

$$g_{\mathrm{r,m}}^2 \ge \frac{1}{\alpha \hat{\delta}_0} \tag{27}$$

where $\hat{\delta}_0 = -\delta_0 \ln(1-\xi)$.

The maximum transmit power of an RS is constrained by its interference. By inserting (11) to (27), we have

$$g_{\mathrm{r,m}}^2 \ge \frac{d_{\min}^{-n} \sum_{i=1}^{N_I} g_{\mathrm{b_i,r}}^2}{\lambda R^{-n} \hat{\delta}_0} \tag{28}$$

Therefore,

$$d_{\mathrm{r,m}} \ge \hat{\lambda} \frac{d_{\min}}{R} \left(\sum_{i=0}^{N_I} d_{\mathrm{b_i,r}}^{-4}\right)^{-1/4} \tag{29}$$

where $\hat{\lambda} = \sqrt[4]{\lambda \hat{\delta}_0}$. Notice that the value of the right-hand side in the above inequality is determined only by the location of the RS. Therefore, (44) gives the maximum distance a RS can reach if the RS' location is given. In other words, for an RS at a given location, its coverage radius is calculated as

$$R_c = \hat{\lambda} \frac{d_{\min}}{R} \left(\sum_{i=0}^{N_I} d_{\mathrm{b_i,r}}^{-4}\right)^{-1/4} \tag{30}$$

5. Performance analysis of cognitive radio networks with different access protocols

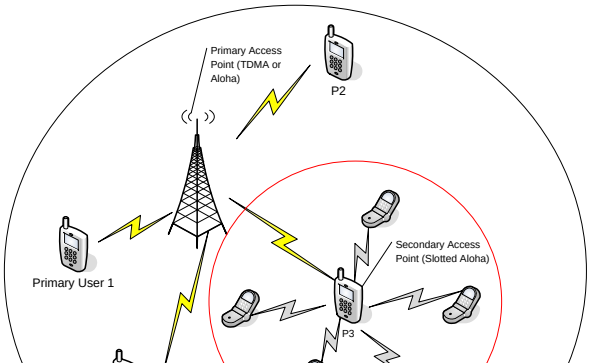


Fig 2. Cognitive radio network model

Besides the link performance analysis above, we also did network performance analysis for cognitive radio networks. In this part, we consider a cognitive radio network composed of a primary network and a secondary relay network, as shown in Fig. 2. This network model is abstracted from the above cognitive relay network. The performances of the cognitive radio network with two types of access protocols are analyzed. One access protocol is TDMA for primary network and slotted ALOHA for secondary network (TDMA/AlOHA). The other is slotted ALOHA for both primary network and secondary network (ALOHA/ALOHA).

We assume that there are N_p primary users and N_s secondary users in the network. The packet generation probabilities of each primary user and secondary user are σ_p and σ_s, respectively. In the TDMA/ALOHA network, we assume that secondary users can only access the network when the primary users are silent in a time slot. Therefore, the performance of TDMA primary network will not be impacted by the access of the secondary network. By using the Markov chain theory, we obtain the throughput of the secondary network as

$$\begin{aligned} S_{Aloha} &= P_{idle} \sum_{I_s=0}^{N_s} \binom{N_s}{I_s} \sigma_s^{I_s} (1-\sigma_s)^{N_s-I_s} \Pr(E_s|T_{I_s}) \\ &= (1-\sigma_p)^{N_p} \pi_0 \sum_{I_s=0}^{N_s} I_s \binom{N_s}{I_s} \sigma_s^{I_s} (1-\sigma_s)^{N_s-I_s} \\ &\quad \left(\frac{1}{R+1}\right)^{I_s-1} \end{aligned} \tag{31}$$

In ALOHA/ALOHA network, we assume that the primary users will emit a larger transmit power than that of the secondary users. The access of the secondary will inevitably reduce the throughput of the primary network. The throughputs of the primary network and the secondary network are

$$S_p = \sum_{i=0}^{N_P} \sum_{j=0}^{N_S} \binom{N_P}{i} \sigma_p^i (1-\sigma_p)^{N_P - i} \binom{N_S}{j} \sigma_s^j (1-\sigma_s)^{N_S - j} \tag{32}$$

(15)

$$\begin{aligned} &\Pr(E_P | T_{i,j}) \\ &= \sum_{i=0}^{N_P} \sum_{j=0}^{N_S} \binom{N_P}{i} \sigma_p^i (1-\sigma_p)^{N_P - i} \binom{N_S}{j} \sigma_s^j (1-\sigma_s)^{N_S - j} \\ &\quad i \left(\frac{1}{R+1}\right)^{i-1} \left(\frac{\gamma}{R+\gamma}\right)^j \end{aligned}$$

$$S_s = \sum_{i=0}^{N_P} \sum_{j=0}^{N_S} \binom{N_P}{i} \sigma_p^i (1-\sigma_p)^{N_P - i} \binom{N_S}{j} \sigma_s^j (1-\sigma_s)^{N_S - j} \tag{33}$$

(16)

$$\begin{aligned} &\Pr(E_S | T_{i,j}) \\ &= \sum_{i=0}^{N_p} \sum_{j=0}^{N_S} \binom{N_P}{i} \sigma_p^i (1-\sigma_p)^{N_P - i} \binom{N_S}{j} \sigma_s^j (1-\sigma_s)^{N_S - j} \\ &\quad j \left(\frac{1}{R\gamma+1}\right)^{i} \left(\frac{1}{R+1}\right)^{j-1} \end{aligned}$$

Simulation Results

Simulation results are presented in this section to validate the theoretical analysis and demonstrate the performance advantage of the cognitive-relay based cellular systems. In the simulations, we consider the ICI from six nearest interference cells using the same frequency band as the home cell, as shown in Fig. 1. Without loss of generality, we set the cell radius $R = 1$. We consider an urban area cellular network and assume that the path loss factor is $n = 4$. The reuse distance D, i.e., the distance between BS 0 and neighboring co-channel BS, is determined by the cluster size N and calculated as [25]

$$D / R = \sqrt{3N} \tag{34}$$

For convenience, we establish a polar coordinate system with BS 0 as the pole and the line from BS 0 to BS 1 as the polar axis. The location of BS 0 is thus represented as $(0,0)$ and the

location of BS i is $(D, \frac{(i-1)\pi}{3})$ for $i = 1, 2, \cdots, 6$. The location of a MS is represented as (r, θ) and the location of a RS is represented as (r', θ').

First, we investigate the system performance when the cognitive relay channel is always available, i.e., p = 1. Fig. 2 shows the outage probability of an MS at $(R,0)$ (the cell boundary) with different δ. It is noted that the case of $\delta \to \infty$ is equivalent to that no relay is available and the case of $\delta = 0$ represents that the RS-MS channel is perfect. Theoretical and simulation results are both illustrated for these two extreme cases and match very well. The results indicate that the use of cognitive relay improves the system performance significantly when the RS-MS link is perfect. Simulation results for $\delta = 1, 0.1, 0.01$ are also shown to compare with the two extreme cases. It is shown that the performance improvement is degraded with the increase of δ.

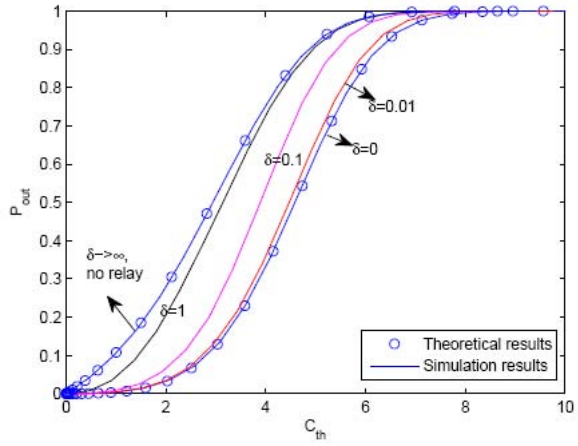


Fig. 2 Outage probability of a MS at the cell boundary when relay is available (δ indicates the RS-MS link quality. N = 3)

To quantify the impact of δ on the system performance, Fig. 3 and Fig. 4 illustrate the degrading factor of the outage capacity for MS at different locations ($r = R, 0.8R, 0.6R, \theta = 0$) when N = 3 and N = 7, respectively, where the degrading factor is quantified as

$$\eta(\delta) = \frac{C_\varepsilon|_{\delta=0} - C_\varepsilon|_\delta}{C_\varepsilon|_{\delta=0}} \times 100\% \tag{35}$$

The target outage probability is set to $\varepsilon = 0.1$. It is seen that when $\delta \le 0.01$, the decrease of outage capacity is less than 5% for any r and N. Therefore, we select $\delta_0 = 0.01$ in (26) so that the effect of δ is negligible.

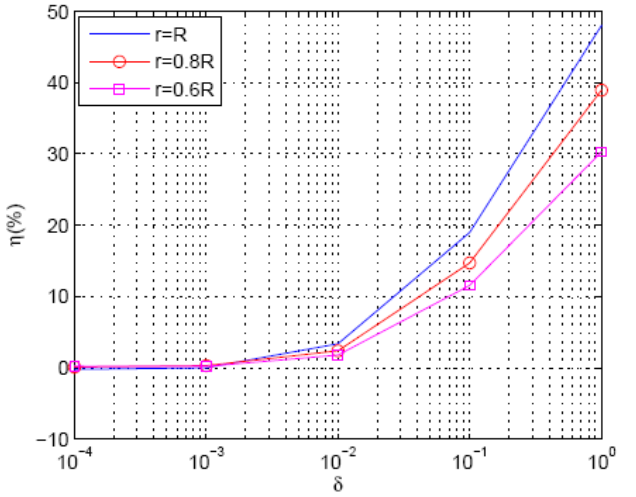


Fig. 3 Impact of δ on the outage capacity ($\varepsilon = 0.1, N = 3$)

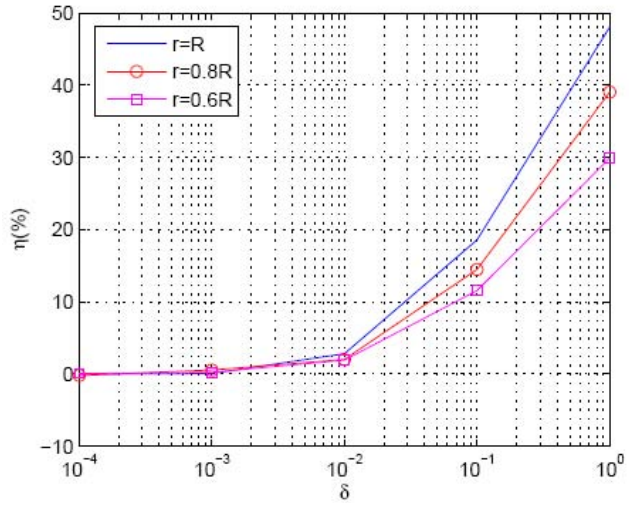


Fig. 4 Impact of δ on the outage capacity ($\varepsilon = 0.1, N = 7$)

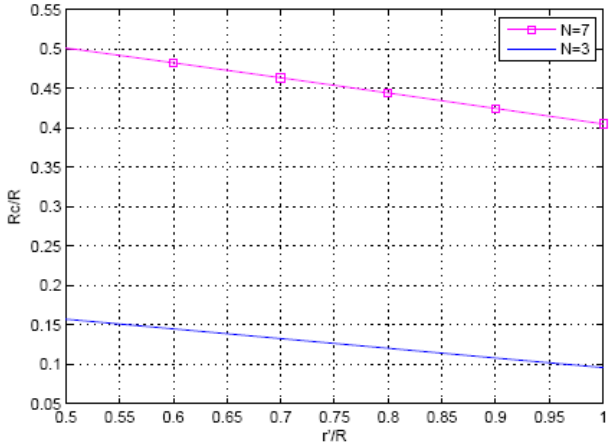


Fig. 5 Coverage radius of RS at different locations

Assume that the tolerable ISR of neighboring MS is $\lambda = -20\,\mathrm{dB}$ and the probability in (26) is $\xi = 0.1$. The coverage radius of RS at different locations (r', θ') can be calculated following (30). Since the variation of R_c for different θ' is small, we simply approximate that the RS with the same r' has the same coverage radius, which is set to

$$\tilde{R}_c(r') = \min_{\theta'} R_c(r', \theta') \tag{36}$$

Fig. 5 illustrates the numerical results of the coverage radius for different r' and cluster size N. It is seen that the coverage radius is increased with the decrease of r' and the increase of N. Appropriate RS' locations are selected according to Fig. 5 to cover the interference limited area. For example, assume that the interference limited distance threshold $r_0 = 0.8R$, i.e., all MS with $r > 0.8R$ require the assistance of RS. If the cluster size N = 3, to maximize the coverage area and make sure that the cell boundary is covered, we deploy RS at $r' = 0.9R$. The corresponding coverage radius is $R_c \approx 0.1R$. To cover all the interference limited area, the required RS number is about $\lceil 2\pi r' / 2R_c \rceil = 28$. If N = 7, we deploy RS at $r' = 0.8R$ to make sure that the RS is in the interference-limited region. The corresponding coverage radius is about $R_c \approx 0.45R$. The required number of RS is about 6.

Further, we illustrate the availability of the cognitive relay channel in cellular systems and its effect on the outage capacity. Assume that the number of channels allocated to each cell is 32. Fig. 6 shows the availability probability p as a function of the loading factor ρ with the activity factor $\beta = 0.9$ and Fig. 7 shows p as a function of β with $\rho = 1$. Different threshold distances for interference-limited operation ($r_0 = 0.6R, 0.7R, 0.8R$) are considered. It is seen that p is decreased with the increase of ρ, the increase of β or the decrease of r_0. The reason is that the increase of ρ and β both reduce the opportunity to have vacant channels and the decrease of r_0 increases the number of interference limited MS, which compete for the vacant channels.

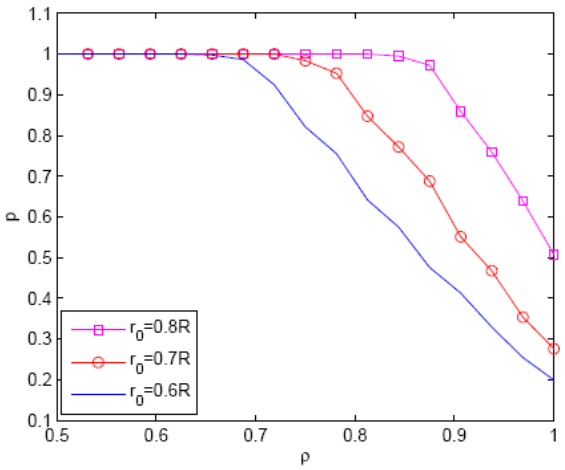


Fig. 6 Cognitive relay availability probability vs. loading factor

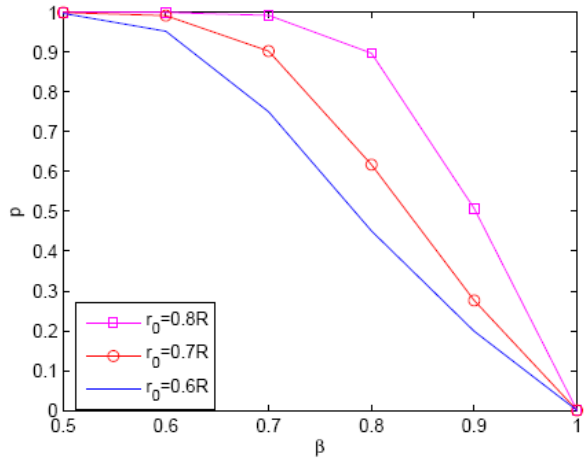


Fig. 7 Cognitive relay availability probability vs. activity factor

Fig. 8 shows the outage capacity of MS at different locations in a cognitive-relay based cellular network as a function of the channel availability probability p. The cluster size is N = 3 and the outage probability $\varepsilon = 0.1$. As described above, we assume that the considered MS are in the coverage area of an RS so that the RS-MS link can be regarded as perfect, i.e., $\delta = 0$. From Fig. 8, we see that if the relay channel is always available, i.e., $p = 1$, the cognitive relay improves the capacity of the MS at cell boundary by about three times compared with the system without relay, i.e., $p = 0$. The improvement is decreased with the decrease of p. However, even when p is decreased to 0.7, the improvement brought by the cognitive-relay based ICI cancelation still doubles the capacity of MS at cell boundary.

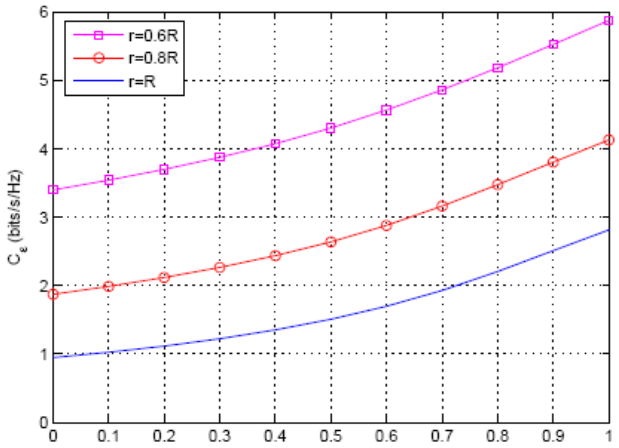


Fig. 8 Outage capacity of MS with cognitive relay as a function of *p*

Considering Fig. 6, Fig. 7 and Fig. 8, we conclude that the cognitive relay provides great opportunities to improve the capacity of cellular systems by mitigating the strong ICI near the cell boundary, especially for systems with relatively low traffic loads.

Finally, we show the throughput performance of cognitive radio networks with different access protocols. Fig. 9 shows the total network throughput of a TDMA/ALOHA networks. Since the secondary network will not impact the primary network, the employment of the cognitive radio increases the throughput of the overall network. Fig. 10 and Fig. 11 show the throughput of the primary network and secondary network in an ALOHA/ALOHA network, where the transmit power the primary users is 10 times larger than that of the secondary users. It is seen that the access of secondary users reduces the throughput network noticeably when the primary traffic load is high. Therefore, the ALOHA/ALOHA protocol is only suitable for cognitive radio network with a very low traffic load in primary networks.

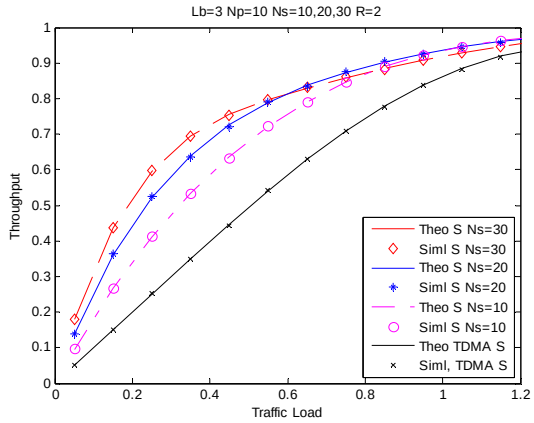


Fig. 9 Total network throughput of TDMA/ALOHA cognitive radio network

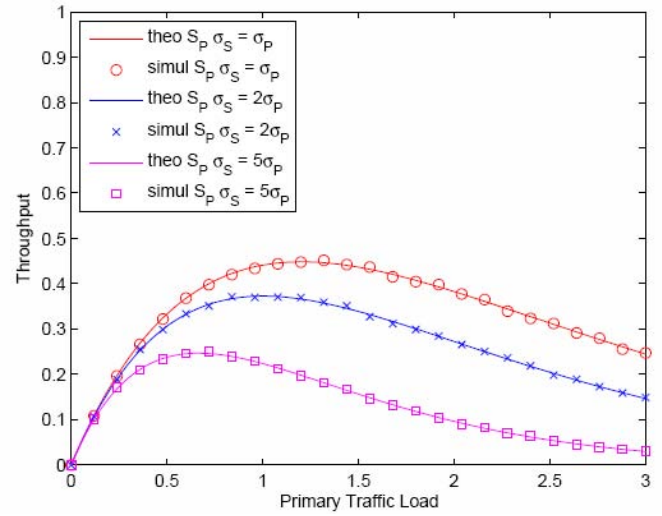


Fig. 10 Throughput of the primary network in an ALOHA/ALOHA network

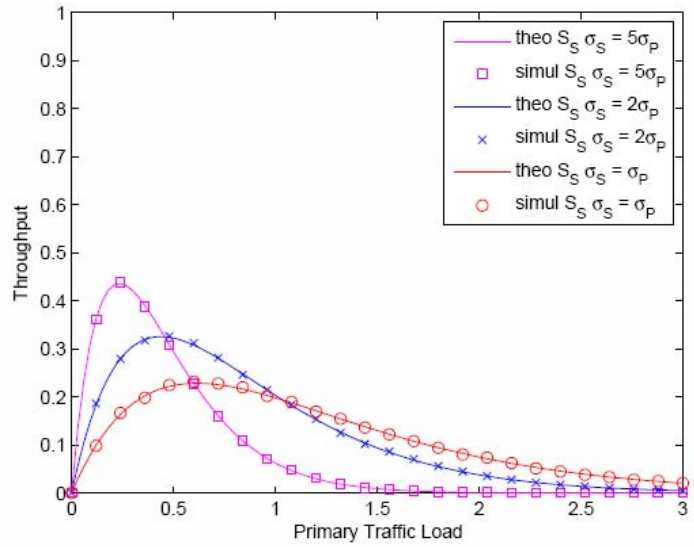


Fig. 11 Throughput of the secondary network in an ALOHA/ALOHA network

POTENTIAL APPLICATIONS

The proposed hybrid network with cognitive relay technique can be applied to various existing infrastructure networks, including commercial cellular networks and military networks to reduce the co-channel interference and improve the capacity.

.

PROJECT ASSESSMENT

This subtask (Adaptive architecture and access protocols) consists of several research steps and components.

1. QoS Comparison of different network architectures: We investigate and compare the QoS performance of infrastructure networks and ad hoc networks, as described in Section I.
2. Relay/cooperative communication across networks with different architectures: We proposed a hybrid network with cognitive relay. Specifically, an ad hoc relay network is deployed around the boundary of an infrastructure network to enable the cancellation of co-channel interference. The details are shown in Section II.1-3
3. Interference Analysis and Avoidance: The interference between the primary infrastructure network and secondary ad hoc network is analyzed. The details are shown in Section II.4
4. Adaptive channel access protocols: We analyzed the throughput of cognitive radio networks with different access protocols. The details are shown in Section II.5.

References List

[1] I. Katzela and M. Naghshineh, “Channel assignment schemes for cellular mobile telecommunication systems: A comprehensive survey,” IEEE Personal Commun. Mag., vol. 3, no. 3, pp. 10–31, June 1996.

[2] W. C. Y. Lee, “Overview of cellular CDMA,” IEEE Trans. Veh. Technol., vol. 40, no. 2, pp. 291–302, May 1991.

[3] M. Einhaus, O. Klein, and M. Lott, “Interference averaging and avoidance in the downlink of an OFDMA system,” in Proc. IEEE 16th International Symposium on Personal, Indoor and Mobile Radio Communications PIMRC 2005, vol. 2, 11–14 Sept. 2005, pp. 905–910.

[4] A. Shah and A. M. Haimovich, “Performance analysis of optimum combining in wireless communications with Rayleigh fading and cochannel interference,” IEEE Trans. Commun., vol. 46, no. 4, pp. 473–479, April 1998.

[5] K.-K. Wong et al., “Adaptive antennas at the mobile and base stations in an OFDMA/TDMA system,” IEEE Trans. Commun., vol. 49, no. 1, pp. 195–206, Jan. 2001.

[6] M. Kang, L. Yang, and M. S. Alouini, “Outage probability of MIMO optimum combining in presence of unbalanced co-channel interferers and noise,” IEEE Trans. Wireless Commun., vol. 5, no. 7, pp. 1661–1668, July 2006

[7] H. Kang et al., “Analytical framework for optimal combining with arbitrary-power interferers and thermal noise,” IEEE Trans. Veh. Technol., vol. 57, no. 3, pp. 1564–1575, May 2008.

[8] R. Pabst et al., “Relay-based deployment concepts for wireless and mobile broadband radio,” IEEE Commun. Mag., vol. 42, no. 9, pp. 80–89, Sept. 2004.

[9] H. Wu et al., “Integrated cellular and ad hoc relaying systems: iCAR,” IEEE J. Sel. Areas Commun., vol. 19, no. 10, pp. 2105–2115, Oct. 2001.

[10] J. Cho and Z. J. Haas, “On the throughput enhancement of the downstream channel in cellular radio networks through multihop relaying,” IEEE J. Sel. Areas Commun., vol. 22, no. 7, pp. 1206–1219, Sept. 2004.

[11] A. Sendonaris, E. Erkip, and B. Aazhang, “User cooperation diversity. Part I. System description; Part II. Implementation aspects and performance analysis,” IEEE Trans. Commun., vol. 51, no. 11, pp. 1927–1948, Nov. 2003.

[12] F. S. P. T. Force, “Report of the Spectrum Efficiency Working Group,” Nov. 2002. [Online]. Available: http://www.fcc/gov/sptf/reports.html.

[13] J. Mitola and G. Q. Macguire, “Cognitive radio: Making software radios more personal,” IEEE Personal Communications, vol. 6, no. 4, pp. 13–18, Aug. 1999.

[14] K. B. Letaief and W. Zhang, “Cooperative communications for cognitive radio networks,” Proc. IEEE, vol. 97, no. 5, pp. 878–893, May 2009.

[15] N. Devroye, P. Mitran, and V. Tarokh, “Achievable rates in cognitive radio channels,” IEEE Trans. Inf. Theory, vol. 52, no. 5, pp. 1813–1827, May 2006.

[16] K. Lee and A. Yener, “Spectrum-sensing opportunistic wireless relay networks: Outage and diversity performance,” in Proc. Fortieth Asilomar Conference on Signals, Systems and Computers ACSSC ’06, Oct. 29 2006–Nov. 1 2006, pp. 206–210.

[17] S. Kim et al., “Downlink performance analysis of cognitive radio based cellular relay networks,” in Proc. 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications CrownCom 2008, 15–17 May 2008, pp. 1–6.

[18] S. Haykin, D. Thomson, and J. Reed, “Spectrum sensing for cognitive radio,” Proc. IEEE, vol. 97, no. 5, pp. 849–877, May 2009.

[19] T. Yucek and H. Arslan, “A survey of spectrum sensing algorithms for cognitive radio applications,” IEEE Communications Surveys & Tutorials, vol. 11, no. 1, pp. 116–130, Quarter 2009.

[20] E. Larsson and M. Skoglund, “Cognitive radio in a frequency-planned environment: Some basic limits,” IEEE Trans. Wireless Commun., vol. 7, no. 12, pp. 4800–4806, December 2008.

[21] C. Patel and G. Stuber, “Channel estimation for amplify and forward relay based cooperation diversity systems,” IEEE Trans. Wireless Commun., vol. 6, no. 6, pp. 2348–2356, Jun. 2007.

[22] M. O. Hasna and M. S. Alouini, “A performance study of dual-hop transmissions with fixed gain relays,” IEEE Trans. Wireless Commun., vol. 3, no. 6, pp. 1963–1968, Nov. 2004.

[23] A. S. Avestimehr and D. N. C. Tse, “Outage capacity of the fading relay channel in the low-SNR regime,” IEEE Trans. Inf. Theory, vol. 53, no. 4, pp. 1401–1415, April 2007.

[24] H. Shin and M. Z. Win, “MIMO diversity in the presence of double scattering,” IEEE Trans. Inf. Theory, vol. 54, no. 7, pp. 2976–2996, July 2008.

[25] T. S. Rappaport, Wireless Communications: Principle and Practice, 2nd ed. Prentice-Hall inc., 2002.

Appendices

Appendix A. Statement of Work

Adaptive architecture and access protocols:

This task will focus on the adaptive network architecture and access protocols with scalable QoS in the cognitive and network centric communication systems. The

multiple objectives include the real-time network selection, adjustment of network architectures, and access protocols and the cooperation between networks. Specific subtasks of this research are listed below**.**

- Adaptive network architecture with scalable QoS: The contractor shall develop analytical models to characterize and classify network architectures, including infrastructure networks, ad hoc networks and mesh networks, for different QoS requirements and channel environments. Network selections and adaptive network reconfigurations will be investigated for different network architectures.

- Relay/cooperative communication across networks with different architectures: They contractor shall develop multi-network relay protocols to realize relay/cooperative communication across networks with different architectures. The contractor shall establish a model to analyze the performance of the multi-network relay, including utilization, delay, and reliability.

- Adaptive channel access protocols: The contractor shall explore and compare various multiple access techniques, including CDMA, TDMA, OFDMA techniques, fix and random access protocols for different network architectures. The coexistence problem of different access techniques resulted from different network architectures shall be investigated. Interference avoidance algorithms will be developed for access protocol designs. Interference modeling and modeling algorithms will be based on the research results from task of spectrum sensing and signal processing.

Appendix B. Proprietary Information

N/A.

Appendix C. Investigator-Sensitive Information

N/A.

Final Report

W15QKN-05-D-0011, Task Order 43

(September 15, 2009)

Submitted by S. Tewksbury

Contract Number: W15QKN-05-D-0011, Task Order 43

Contract Name: Embedded Intelligent Sensor Network Systems

Task 1

Cognitive & Network Centric Military Communications

Subtask 3

Ubiquitous service oriented network architecture

Prof. Yingying Chen
Department of Electrical and Computer Engineering
Stevens Institute of Technology
Hoboken, NJ 07030

Abstract

The broad deployment of wireless technologies has brought many opportunities to emerging ubiquitous services. In the mean while, in order for successful implementation of emerging ubiquitous services, new challenges are arising that need to be addressed. In this year's work, we focused on the following research tasks: (1) we developed a service oriented trusted framework for regulating the access of the network information; (2) we designed and developed both a centralized architecture as well as a fully decentralized enforcement mechanism; and (3) We designed an on-node trusted component and developed a fully decentralized position verification mechanism, NORM, utilizing neighbor node observation in decentralized architecture. Further, in NORM, we developed three schemes, namely, Neighbor Examination (NE) scheme, Neighbor Verification (NV) scheme, and Neighbor Localization (NL) scheme, to perform position verification for location-based service access and help to enhance the node verification for secure access. Finally, we introduced the concepts of communal policies to enforce the proper access of the network information. This trusted ubiquitous service-oriented network architecture, which utilizes a policy-based approach to access the network information, can provide situation-aware services of different networks.

1. Introduction

The broad deployment of wireless technologies has brought many opportunities to emerging ubiquitous service. In addition, the rapid development in wireless technologies such as GPS, GSM, WiFi (802.11), and RFID have enabled a host of new service-oriented applications. This opens up the opportunities for using services from different devices in different situations. However, extensive deployment of service-oriented applications without safeguards may be dangerous if misused by adversaries. Thus, one of the main challenges in ubiquitous service is sharing the right resources with the right party at the right time. In particular, it is desirable to develop mechanisms, which provide safeguard and only allow the network resources to be accessed by the right party at the right time.

We first developed a service oriented trusted framework for regulating the access of the network information. The proposed service oriented trusted infrastructure is generic and targets for any networks. We designed and developed both a centralized architecture as well as a fully decentralized enforcement mechanism. There are two phases in our access control model: verification and authorization. In a centralized architecture, a central server performs verification and authorization and stores the results in a centralized database, while in a decentralized approach, the verification and authorization are performed at each network device and the results are only available to the network device itself.

We then proposed an on-node trusted component and developed the Neighbor ObseRvation Mechanism (NORM), which performs position verification for location-based network resource access and helps to enhance the node verification for secure access. The traditional approach for position verification is to use a centralized server that contains all the location information and can thus verify the position of the client. This kind of approach inherently introduces an issue related to the location privacy. And consequently, network devices may be tracked by the central

server. In addition, due to environmental constraints, the deployment of a central verification server is not always possible, especially in military tactical fields. As opposed to the traditional centralized location verification methods, we propose NORM, which is a decentralized mechanism to perform position verification based on the observation from the neighboring nodes of the client. NORM is a software component deployed in each node, and can assist information processing and position verification in autonomous systems. We investigate NORM under two adversarial models, a naive adversary and a sophisticated adversary model. We further develop three schemes, namely, Neighbor Examination (NE) scheme, Neighbor Verification (NV) scheme, and Neighbor Localization (NL) scheme, to detect the abnormal location caused by both adversarial models.

Finally, we introduced the concept of communal policies to the service-oriented network architecture. In our proposed trusted framework, wireless devices must adhere to the communal policies when requesting services. We present trusted policies for communal access and regulations over the service-oriented architecture. We also describe the policy formalism for accessing the ubiquitous services.

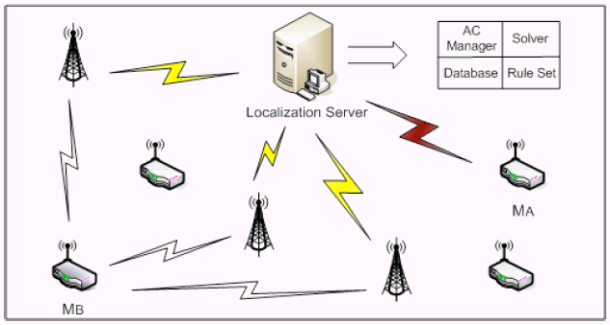


Fig.1 Centralized architecture

2. Approach Taken

2.1 Task 1: Development of a Trusted Infrastructure for Regulating the Access of the Network Information

We present an overview of our service oriented trusted infrastructure, which targets for any wireless networks. We first present a centralized architecture for network information access control. We then turn our focus to a decentralized policy enforcement approach. In our model, the information access control involves two phases, verification and authorization. The verification phase performs authentication of the client, i.e., the wireless device requests the location information. The location-based access of the network information will then be authorized based on communal policies.

Centralized Architecture: In a centralized approach, the wireless localization is performed in a central server. The localization process is conducted continuously and the results are stored in the database as depicted in Figure 1. In the area of interest, the base stations will report the signal readings of a wireless device back to a localization server. The localization server contains solver that has the data processing and analysis capabilities to estimate the positions of wireless devices. A management entity, namely the *Access Control Manager (AC Manager)*, performs verification and authorization before accessing the information stored in the database. The *AC*

Manager can reside within the localization server as shown in Figure 1 or operate separately in a centralized manner but can access the database remotely. A set of access control rules will be disseminated and stored in the *AC Manager*.

As illustrated in Figure 1 when a wireless device M_A wants to obtain the information of another wireless device M_B, first it sends a request message to the *AC Manager* with its ID and current position. As evidenced by the numerous possible security threats due to node ID compromise or identity based spoofing attacks [1], we note that it is not enough to verify a wireless device just based on its node ID. However, the position information is relatively harder to falsify without being detected. The advantage of the centralized architecture is that it can easily prevent identity-based attackers from accessing the information by comparing to the complete position information stored in the central database. If a match is found, then the wireless device M_A is authenticated. Next, based on the verification status, the *AC Manager* consults with the access control policies stored in the *rule set* and decides whether to send the exact information as requested (e.g., the real coordinates of the position) or adjust the resolution of the information (e.g., the room or floor level location resolution is returned.).

One drawback of the centralized approach utilizing *AC Manager* is that the server contains all the information and inherently introduces an issue related to the user's privacy. Consequently, wireless devices may be tracked by the central server. Next, we present our decentralized policy enforcement for location access control, which achieves user location privacy by not requiring interaction between a wireless device and a central server.

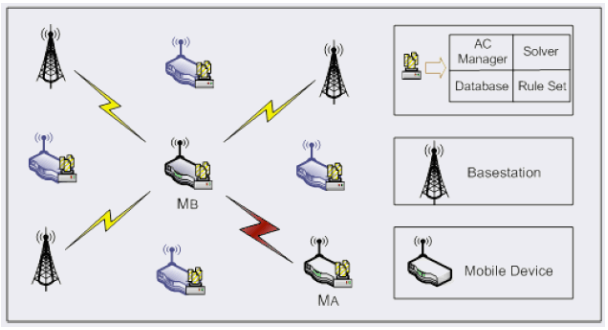


Fig. 2 Decentralized architecture.

Decentralized Architecture: In order to build a decentralized infrastructure, wireless devices are equipped with the localization capability. Various localization methods can be applied in the solver. One simple approach is to use the multilateration strategy. When a wireless device collects signals from three or more base stations, it can position itself by applying the multilateration calculation [2]. The location information will then be stored in the database within the wireless device. As shown in Figure 2 the functionalities of information access control will be distributed to each wireless device, which forms a decentralized trusted computing base. The access control policies will be disseminated to each wireless device and examined by the *AC Manager* that resides in each wireless device. Although we use the same name *AC Manager*, we replace the central entity of *AC Manager* with a distributed set of *AC Managers*. Structurally, all these *AC Managers* are generic, support the same set of communal policies, and all must be trusted to interpret correctly any rules they might operate under.

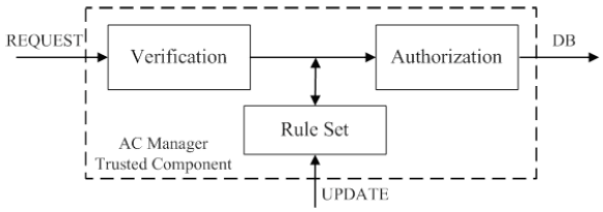


Fig. 3 Decentralized enforcement via AC Manager's trusted computing module

The access control policies need to be supported by enforcement mechanisms local to the wireless devices. It is therefore necessary to develop an on-node trusted computing base in each wireless device that enforces the policies. As depicted in Figure 3, the *AC Manager* implements the trusted component in each wireless device. It contains several logical components including *verification*, *authorization*, and *rule set*. Conceptually, the *AC Manager* can be viewed as a safeguard when the request first coming in.

When a wireless device receives a request for information, the *AC Manager* on the wireless device performs verification, which is the same as in the centralized approach. However, in the decentralized enforcement, the *AC Manager* does not have a central database that can be used to verify the client's ID and position. Instead of introducing the traditional cryptographic authentication methods on the wireless device [3], [4], we focus the node verification based on its location and propose a node location verification mechanism, Neighbor ObseRvation Mechanism **(NORM)**, which utilizes observations from neighboring nodes, to enhance the identity based authentication methods. Next, the *AC Manager* evaluates the request along with the verification results and checks it against the access control policies stored in the *rule set*. If the client's credentials don't permit the privilege level of the request, then the *AC Manager* will either try to find a permissible modification of the request that adapts to the access control policy and authorize the access of the granted location information, or reject the request if such a modification is not feasible.

2.2 Task 2: Neighbor ObseRvation Mechanism (NORM)

NORM is a software component deployed in each node. Comparing to prior position verification techniques[5,6], the main advantage of NORM is that it does not require special hardware, deployment knowledge, or a central verification center. NORM performs position verification of a node in a fully distributed way, depending on the spatial consistency relationship inherited between a node and its neighbors. We next describe three detecting schemes we developed in NORM. For illustration purpose, we use the example when a node S_B needs to verify the reported location of the node S_A.

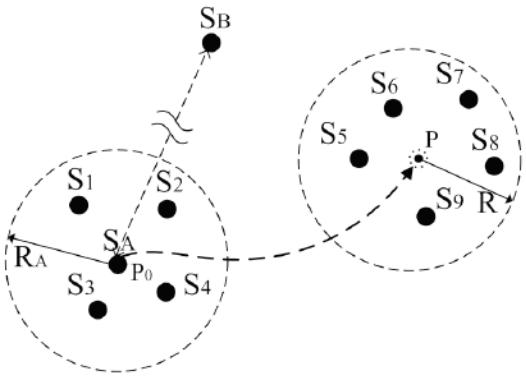


Figure 4: Illustration of two adversarial models: a naive adversary and a sophisticated adversary model.

Adversary Model: In our work, we consider two adversarial models, a naive adversary and a sophisticated adversary model. In both models, the adversary claims the position of the compromised at P, while its true position is at P_0, As shown in Figure 4, the compromised node S_A's true location is at P_0, but the adversary claims its position is at P.

For a naive adversary, it either sends an arbitrary neighbor list or reports neighbors of the compromised node consistent with their reported location P. Whereas for a sophisticated adversary, it reports the true neighbors around the compromised sensor's true position P_0 to trick the system. For instance, in Figure 4, the naive adversary at the node S_A reports P as the position of S_A and sends nodes $\{S_5, S_6, S_7, S_8, S_9\}$ around location P as neighboring nodes of S_A, whereas the sophisticated adversary sends the true neighbors of S_A, $\{S_1, S_2, S_3, S_4\}$, around location P_0.

If a node is compromised, it will not respond to any verification requests for confirming the observation of other nodes. Further, we define an *Anomaly Distance (AD)* as the distance between the reported location and the true location (i.e. $AD = ||P - P_0||$). We want to design position verification schemes that can detect the abnormal location when AD exceeds certain distances.

Neighbor Examination (NE) Scheme: The NE scheme performs position verification based on the direct response from neighbors of the node under verification, i.e., S_A. The node S_B issues a special verification request to each neighbor, S_i, with $i = 1, 2, ...N$ (N is the total number of neighbors), reported in the neighbor list of the client S_A, and asks whether it has S_A in its neighbor list. When the S_i receives the request, if S_i has S_A in its neighbor list, S_i confirms and reports its current position P_i back. If S_i is compromised by the adversary, based on our adversary model, S_i will keep silent and does not respond. We then define the neighbor examination probability P_{ex} as

$$P_{ex} = \frac{\sum_{i=1}^{K} S_i}{N}$$

where K is the total number of neighbors that responds to the request from SB. If $P_{ex} > \alpha$ where α is the confidence level, S_B determines that S_A passes the neighbor examination. A naive adversary, who sends an arbitrary neighbor list or reports neighbors around location P when lying about the location of the compromised node, will thus result in $P_{ex} < \alpha$ and fail the neighbor examination scheme.

Neighbor Verification (NV) Scheme: Like in the NE scheme, S_B first issues a special verification request to each neighbor, S_i with $i = 1, 2, ...N$, reported in the neighbor list of the client S_A, and asks whether it has S_A in its neighbor list. When the node S_i receives the request, if S_i has S_A in its neighbor list, S_i confirms and reports its current position P_i back. Based on the reported positions of the responded neighbors, S_B then needs to conduct further neighbor verification. Given that the neighboring nodes of S_A must be within the communication range R_A of S_A, the distance between the estimated locations of S_A and its neighbor $||P_A - P_i||$ should be within R_A for an honest node. S_B could complete the position verification of S_A if $||P_A - P_i|| < R_A$ for all $i = 1...K$.

However, since there are localization errors from the location estimation process, we define

$$||P_A - P_i|| < R_A + r,$$

where r is a random variable introduced by localization errors. We may assume localization errors are Gaussian. Under this assumption, r also follows a Gaussian distribution with mean μ and variance σ. Thus the probability that P_A and P_i are neighbors is given by

$$P_r(P_i) = P_r(r > (||P_A - P_i|| - R_A)) = 1 - F(||P_A - P_i|| - R_A),$$

with $F(r)$ as the Cumulative Distribution Function of r,

$$F(r) = \frac{1}{\sqrt{2\pi\delta^2}} \int_{-\infty}^{r} \exp(-\frac{(u-\mu)^2}{2\delta^2}) du.$$

Further, we define the neighbor verification probability P_{ve}, which is the joint probability that all P_i, $i = 1...K$, are the neighbors of P_A as:

$$P_{ve} = \prod_{i=1}^{K} P_r(P_i)$$

We then set a confidence level β such that if $P_{ve} > \beta$, we declare that S_A passes the Neighbor Verification scheme. Otherwise, the reported location information of S_A is declared as compromised.

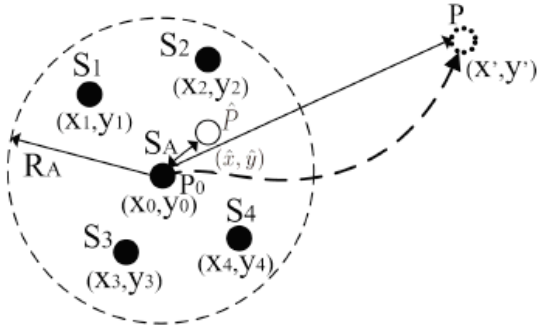


Figure 5: Illustration of the Neighbor Localization (NL) scheme.

Neighbor Localization (NL) Scheme: The NL scheme utilizes the location of S_A's neighboring nodes to estimate the position of S_A and further to verify the reported position of S_A. The estimated position $\hat{P}$ of S_A is expressed as:

$$\hat{P} = \frac{1}{K} \sum_{i=1}^{K} (X_i, Y_i)$$

where K is the total number of responded neighbors to S_B, (X_i, Y_i) is the position of the ith neighbor. Under the normal situation, the distance between the node S_A's true location P_0 and the

estimated location $\hat{P}$ from NL scheme should be small [11, 12]. However, if S_A is compromised, the distance between the reported location P of S_A and $\hat{P}$ should be large.

As illustrated in Figure 5, the distance between P_0 and $\hat{P}$ is much smaller than the distance between P and $\hat{P}$. Therefore, we define a *Maximum Tolerable Distance (MTD)* as the threshold of declaring the abnormal location in NL scheme. In particular, let $D = ||P - \hat{P}||$. If $D > MTD$, NL scheme declares the location reported by S_A is compromised.

2.3 Task 3: Authorization and Policy Formalism

In our proposed trusted framework, wireless devices must adhere to the communal policies when requesting information/service. In this section, we present the main functionality of the *AC Manager* to perform authorization, which evaluates the policy and authorizes the access of the location information. We also describe the policy formalism for accessing the information/service.

The *AC Manager* implements three main functionalities, namely *Matching*, *Adaptation*, and *Application*. First, *AC Manager* matches the request to the *rule set*. A location request may satisfy one or more policies in the rule set. The *AC Manager* will then return the information based on the matching that provides the finest granularity of the information/service that is permitted according to the client's credentials.

However, if the client's credentials do not permit the privilege level of the request. For example, if M_A requests for point-level location information of M_B, but its credentials only allows it to access the room-level location information of M_B based on current policies. The *AC Manager* modifies the request to adapt to the access control policy and authorize M_A to access the room-level location information of M_B. On the other hand, the available information may be in a finer granularity than the location request. One example is that M_A only needs to know at which floor that M_A is located. The *AC Manager* could then reduce the spatial accuracy, protect the location privacy, and meet the requirement of the location request. Finally, if an adaptation is not feasible, the location request is rejected at the authorization phase.

Moreover, the application function is used to impose the usage of the information/service returned to the client. Two important aspects are: *retransmission* and *retention*. The application of *retransmission* defines whether the client is permitted to share the obtained information with other wireless devices. *Retransmission* aims to prevent unauthorized usage of the information/service. Whereas the application of *retention* defines the duration that the returned information is valid. Further, in order to prevent frequent location requests from the same client, which may be used to derive the moving track of a wireless device, the *AC Manager* keeps a list of the clients and records their request time as part of the application function.

Turning to examine the policy formalism, the wireless devices should be able to interpret the policies and update them as needed. Hence, policies should be expressed in an easy to understand manner and can facilitate rule integration, consistency checking and conflict resolution.

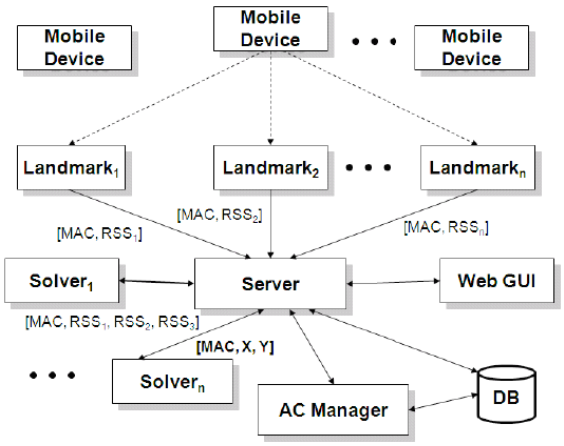


Figure 6: Prototype: system components in the centralized approach.

3. Results

3.1 Trusted Infrastructure for Regulating the Access of the Network Information

To evaluate the feasibility of our centralized architecture for policy enforcement, we integrated the *AC Manager* into a real-time indoor localization system [7]. The system components for the prototype is shown in Figure 5. During the localization process, a wireless device sends packets. Some number of Landmarks (i.e., traffic observers or base stations) observe the packets and record the RSS (Received Signal Strength) readings. Each landmark forwards the observed RSS from the wireless device to the Server. The Server collects the complete RSS vector for the wireless device and sends the information to a Solver instance for location estimation. The Solver instance performs the localization and returns the location estimate of the wireless device back to the Server. The Server stores the location estimate to the database and displays it in GUI.

When a wireless device sends a request to the Server to access the location information of another wireless device, the *AC Manager* performs *verification* and *authentication* before granting the access to the location information. Once the *AC Manager* grants the access, the requested location information is fetched from the database and sent back to the client device. We prototyped the centralized approach in both a 802.11 (WiFi) network as well as a 802.15.4 (ZigBee) network in a real office building environment.

3.2 Simulation Results of Neighbor ObseRvation Mechanism (NORM)

In our simulation setup, we deploy 200 to 500 sensors randomly in a *350m* × *350m* square field. The communication range of the node is modeled to follow a Gaussian distribution with mean at *30m* and standard deviation as *2m*. Under this setup each node can observe average number of neighbors ranging from 4 to 11. Further, we simulate the localization error of a node by modeling the localization errors of the *X* and *Y* coordinates to follow a Gaussian distribution with zero mean and standard deviation of 3m. This corresponds to the localization error with a median of *3m* and can range from 0 to *11m*, which is inline with previous experimental findings [8-10].

We then randomly choose nodes that are compromised by adversaries. The default percentage of compromised nodes is set to 0.1. Based on our adversary model, a compromised node will keep silent when receiving special verification requests. To evaluate the effectiveness of NORM, we vary *Anomaly Distance (AD)*, percentage of compromised nodes, network density and localization error in our simulation study.

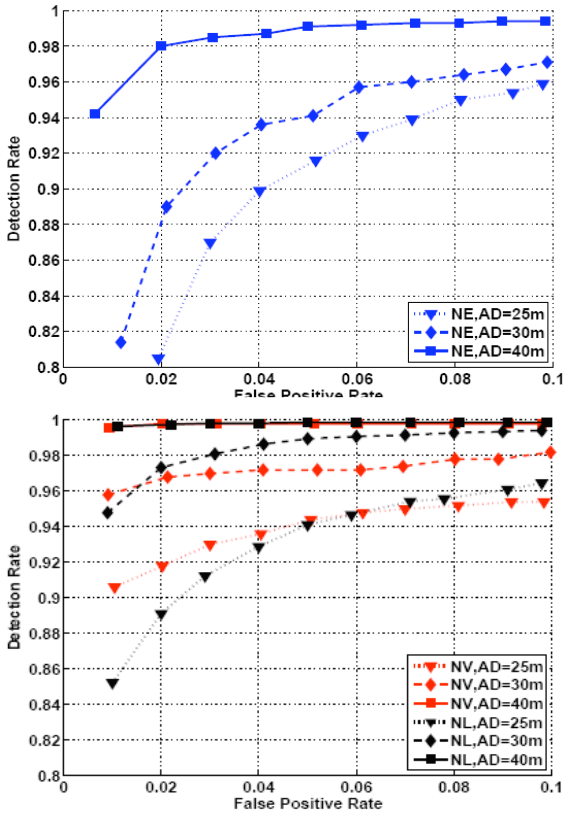


Figure 8: Sophisticated Adversaries: Receiver Operating Characteristic (ROC) curve for impact of Anomaly Distance.

Impact of Anomaly Distance (AD): Figure 7 presents the Receiver Operating Characteristic (ROC) curve under various *Anomaly Distance (AD)* when the Neighbor Examination (NE) scheme is used to detect abnormal locations caused by naive adversaries. We observed that NE scheme can achieve detection rates over 95%when the FPR is less than 10%. For the case of *AD = 25m*, which is less than the average communication range (i.e., 30m) of nodes, the detection rate *(DR)* is above 90% when the FPR reaches 5%. Further, the detection rate achieves 99%when the false positive rate is 5%for the case of *AD = 40m*. Moreover, we found that the larger the *AD* is, the higher the detection rate can achieve. Specifically, by examining the condition of *False Positive Rate(FPR) = 0.0*5 the detection rate increases from 91% to over 99% when *AD* increases from 25m to 40m.

Figure 8 presents the ROC curves under various *Anomaly Distance* when NV and NL schemes are used respectively to detect the abnormal locations caused by sophisticated adversaries. Both NV as well as NL schemes present similar detection performance to NE scheme when *AD* ranges from 25m to 40m: the detection rate increases with the increasing of the *Anomaly Distance*. In particular, the detection rates are above 92% when the FPR is 5% for both NV and NL schemes

under the case of *AD = 25m*. The detection rates are close to 100% when the FPR is 5% for both NV and NL schemes under the case of *AD = 40m*. This indicates our position verification schemes are effective in detecting abnormal locations caused by both naive as well as sophisticated adversaries. We further observed that NV scheme outperforms NL scheme when *FPR* is below 5%, whereas NL scheme outperforms NV scheme when *FPR* is above 5%. Therefore, we can choose proper detection schemes according to the application tolerance to the false positive rate.

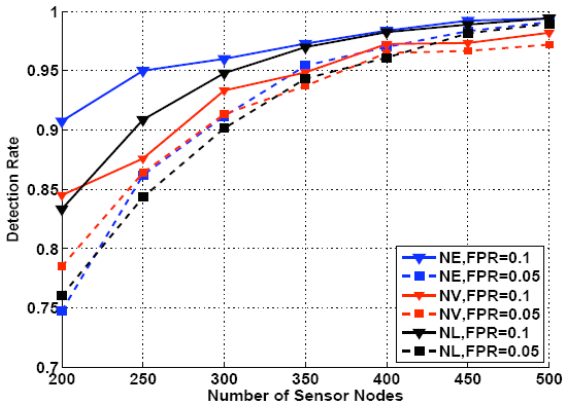


Figure 9: Impact of network density.

Impact of Network Density: By varying the number of nodes from 200 to 500 in our simulated networks, we evaluated how the network density impacts the performance of NORM. In this setup, each node can observe in average 4 neighbors for the deployment of 200 sensors and 11 neighbors for the deployment of 500 sensors in the network respectively. Figure 9 presents the detection rate versus number of nodes under all three schemes. We observed that the detection rate increases with the increasing of network density. In particular, when the number of sensors increases from 200 to 500, the detection rate increases from 85% to 98% for NV scheme, from 90% to 99% for NE scheme and from 83% to 98% for NL scheme respectively, under the condition of FPR less than 10%. Further, we found that NV scheme outperforms NL scheme when the number of sensors is small (e.g. 200), whereas the NL scheme outperforms NV scheme when the number of sensors is large (e.g. 500). Since NL scheme relies on positions of neighbors to estimate the location of a node, the denser the network, the more accurate the position estimation can become and thus the higher detection rate NL scheme can achieve. Hence, based on different network density, we can choose different schemes to perform position verification.

Impact of Percentage of Compromised Nodes: We vary the percentage of compromised nodes in the network to evaluate the robustness of NORM when large number of nodes is compromised in the network. Figure 10 presents the relationship between the detection rate and the percentage of compromised nodes. The false positive rate is set at 10% and the Anomaly Distance equals to 30m.

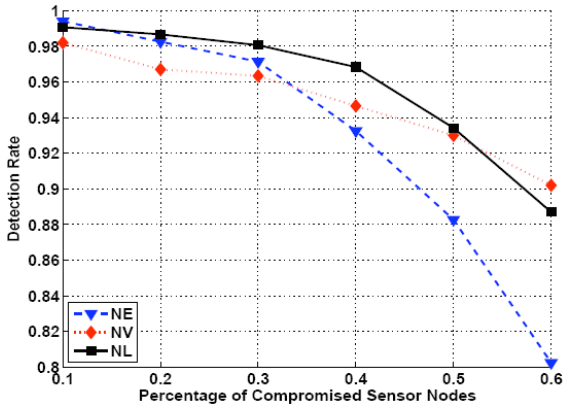


Figure 10: Impact of Percentage of Compromised Sensor Nodes in Network.

As shown in Figure 10, the detection rates of the three schemes drop gradually from above 98%to 80%as the percentage of compromised nodes increases from10%to 60%. A key observation of this experiment is that the performance of NORM is still over 80% even when the percentage of compromised nodes is extensively large (i.e. 60%), which indicates that NORM is robust in detecting abnormal locations under the situation when large number of nodes are compromised.

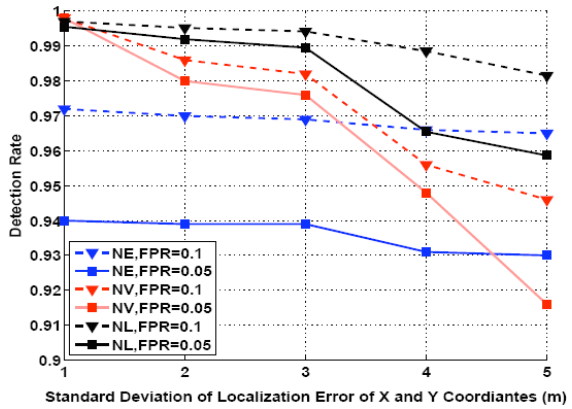


Figure 11: Impact of Localization Error of Sensor Nodes.

Impact of Localization Error of Nodes: We further examine how the localization error can impact the performance of NORM. In this experiment, we vary the standard deviation of the localization error of the X and Y coordinates of a node from 1m to 5m. We note that 1m standard deviation corresponds to a mean localization error of 1.3m, whereas 5m standard deviation corresponds to a mean localization error of 6.3m. The Anomaly Distance is maintained at 30m and the false positive rate is set to 5% and 10% respectively.

Figure 11 presents the detection rates of all three schemes versus the standard deviation. We observed that overall the detection rates are decreasing when the localization error is increasing for all three schemes. And the detection rates of NL and NV schemes can approach 100% no matter the FPR is 5% or 10% when the mean localization error is around 1.3m with a corresponding standard deviation of 1m. Interestingly, we found that NE scheme is not as sensitive as NV and NL schemes to the localization error. Specifically, the decreasing of the

detection rate of NE schemes is about 1%, whereas it is 4% for NL scheme and 8.5% for NV scheme when the mean localization error ranges from 1.3m to 6.3m. This is because NE scheme does not use the positions of nodes (i.e. neighboring nodes) directly, and thus the performance of NE scheme is more stable under various localization errors than other schemes that rely on the positions of nodes.

3.4 Policy Formalism

The following are two examples of rules to access the location information specified in plain English. The pseudo code implementation of R1 is presented in Figure 12.

- Rule 1: (1) allow access to both the current as well as the past 30 minutes location information, (2) the location accuracy is at room-level, (3) the location information is forbidden to be shared with other devices once obtained by a client device, (4) the location information is valid for 60 minutes, and (5) the access frequency of the location information is 30 minutes.

```
Bool Matching () {
    if (Request(location) == ROOM)
        return TRUE;
}
Permission () {
    Multi_Time () {FALSE};
    One_Time () {TRUE};
}
One_Time () {
    current_location = TRUE;
    past_location = TRUE;
    past_duration = 30 MIN;

    location_resolution = ROOM_LEVEL;
}
Bool Adaptation () {
    if (Matching ()) {
        // if the Request(request) is a subset
        // of the Permission, then no need to
        // perform adaptation.
        if (Request(request) <= Permission)
                Authorization = Request(request);
        else    Authorization = Modified_request();
        return TRUE;
    }
}
Modified_Request() {
    //Adapting the location resolution from
    //POINT_LEVEL to ROOM_LEVEL
    Request(request(resolution)) = ROOM_LEVEL;
}
Bool Application () {
    if (Adaptation()) {
        do Authorization;
        do Usage ();
        frequency = 30 MIN;
    }
}
Usage () {
    retransmission = FORBIDDEN;
    retention = 60 MIN;
}
```

Figure 12: Pseudo code implementation of *Rule 1*.

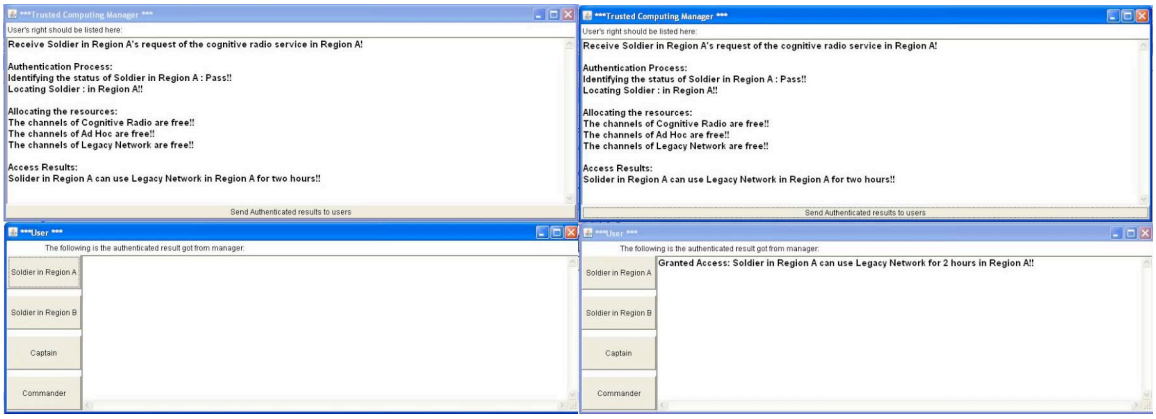
- Rule 2: (1) allow access to the current location trace and the duration of the trace is 1 hour, (2) the location accuracy is at point-level, (3) the location information is allowed to be shared with other devices once obtained by a client device, (4) the location

information is valid forever, and (5) the access frequency of the location information is 2 hours.

Figure 12 illustrates how the *AC Manager* performs authentication in terms of matching, adaptation, and application. To enforce *Rule 1*, *Matching()* is used to apply the room-level resolution, and *Adaptation()* adapts the location information from the point level to the room level. Finally, *Application()* enforces the usage of the location information with *retransmission* and *retention* setting to FORBIDDEN and 60 minutes respectively.

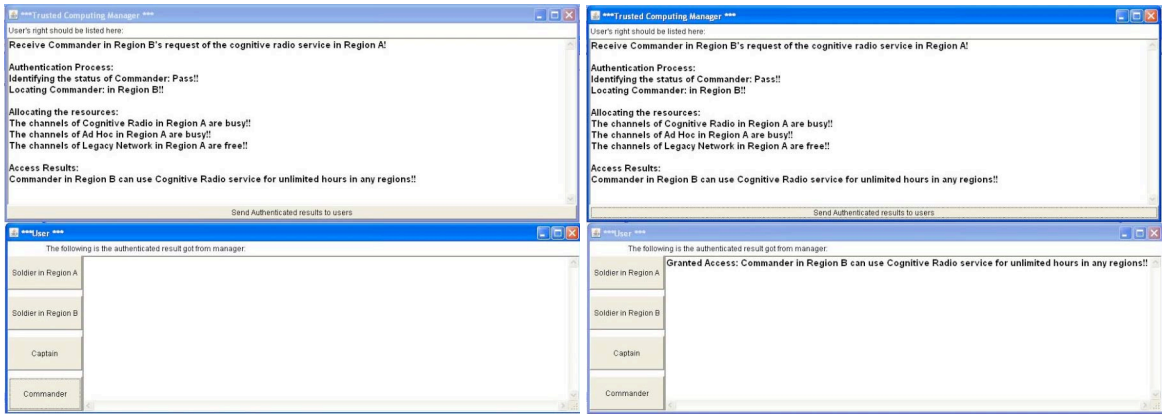
3.5 Demonstration

Figure 13 and 14 present the screen captures of our demonstration of a simulated ubiquitous service-oriented architecture by using communal policies. Figure 13 shows the service request and response of a soldier, while Figure 14 shows the service request and response from a commander. We can see that the commander who has a higher privilege is allowed to access all kinds of networks, whereas a solider can only access the legacy networks.



(a) Soldier in Region A (b) Soldier in Region A, Returned Results

Figure 13: The service request and response of a soldier



(a) Commander (b) Commander, Returned Results

Figure 14: The service request and response from a commander

4. Potential Applications

The proposed ubiquitous service-oriented architecture is flexible and scalable, and can be applied potentially in various Army applications using wireless networks to support Army's net-centric warfare environments.

5. Project Assessment

Our work in this year has met the SOW objectives. The following is the related publications for our subtasks:

- Yingying Chen, Konstantinos Kleisouris, Xiaoyan Li, Wade Trappe, Richard P. Martin, "A Security and Robustness Performance Analysis of Localization Algorithms to Signal Strength Attacks," ACM Transactions on Sensor Networks (ACM TOSN), Volume 5, Issue 1, February 2009.

- Yingying Chen, Jie Yang, Xiuyuan Zheng, Venkataraman Swaminathan, "NORM: A Decentralized Location Verification Mechanism for Wireless Sensor Networks", in Proceedings of 26th Army Science Conference, Orlando, FL, December 2008.
- Yingying Chen, Jie Yang, Fangming He, "A Trusted Infrastructure for Facilitating Access Control Location Information", in Proceedings of IEEE MILCOM, San Diego, CA, November 2008.

6. Reference List

[1] Y. Chen, W. Trappe, and R. P. Martin, “Detecting and localizing wireless spoofing attacks,” in Proceedings of the Fourth Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), May 2007.

[2] N. Patwari, J. N. Ash, S. Kyperountas, A. O. Hero, R. L. Moses, and N. S. Correal, “Locating the nodes,” IEEE Signal Processing Magazine, July 2005.

[3] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, “Secure and efficient key management in mobile ad hoc networks,” in Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS), 2005.

[4] T. Aura, “Cryptographically generated addresses (cga),” RFC 3972, IETF, 2005.

[5] S. Capkun and J. P. Hubaux, “Secure positioning of wireless devices with application to sensor networks,” in Proceedings of the IEEE International Conference on Computer Communications (INFOCOM), 2005, pp. 1917–1928.

[6] Y. Wei, Z. Yu, and Y. Guan, “Location verification algorithms for wireless sensor networks,” in Proceedings of the 27th IEEE International Conference on Distributed Computing Systems (ICDCS), 2007.

[7] Yingying Chen, Gayathri Chandrasekaran, Eiman Elnahrawy, John-Austen Francisco, Konstantinos Kleisouris, Xiaoyan Li, Richard P. Martin, Robert S. Moore, Begumhan Turgut, "GRAIL: A General Purpose Localization System," Sensor Review, special edition, Localisation Systems, Vol. 28, No. 2, pp.115-124, 2008.

[8] D. Madigan, E. Elnahrawy, R. Martin, W. Ju, P. Krishnan, and A. Krishnakumar, Bayesian Indoor Positioning Systems,” in Proceedings of the 24th IEEE International Conference on Computer Communications (INFOCOM), March 2005, pp. 324–331.

[9] Y. Chen, W. Trappe, and R. P. Martin, “Detecting and localizing wireless spoofing attacks,” in Proceedings of the Fourth Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), May 2007.

[10] P. Bahl and V. N. Padmanabhan, “RADAR: An In-Building RF-Based User Location and Tracking System,” in Proceedings of the 19th IEEE International Conference on Computer Communications (INFOCOM), March 2000.

[11] H. Lim, L. Kung, J. Hou, and H. Luo, “Zero-configuration, robust indoor localization: Theory and experimentation,” in Proceedings of the IEEE International Conference on Computer Communications (INFOCOM), March 2006.

[12] Y. Chen, K. Kleisouris, X. Li, W. Trappe, and R. P. Martin, “The robustness of localization algorithms to signal strength attacks: a comparative study,” in Proceedings of the International Conference on Distributed Computing in Sensor Systems (DCOSS), June 2006, pp. 546–563.

Appendices

Appendix A: Statement of Work

Task 1.3 Ubiquitous service oriented network architecture

This task aims to design and develop a ubiquitous service-oriented network architecture that can provide situation-aware services of different networks. This research task proposes a trusted service-oriented network architecture which utilizes a policy-based approach to access the network information.

1.3.1. Formalizing communal policies: to provide situation-aware services in ubiquitous computing, we propose a layered trusted architecture with service layer, virtualization layer (integrated network service layer), and data layer. We will develop algorithms and trusted policies for communal access and regulations over the service-oriented architecture. The access control policies will be prototyped in the central processing manager, sensor nodes (e.g. motes), and cognitive devices.

1.3.2. Development of a graphical user interface (GUI) and backend integration: We will develop a friendly GUI to demonstrate the usage of the trusted framework prototype with the implementation of communal policies at back end. The GUI needs to be integrated with the QoS network architecture layer and the spectrum sensing layer to get real-time feeding of data.