Northeastern University
College of Computer and Information Science

Proposal for Thesis Research in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Title: Dynamic Discovery in Wireless Networks

Date of Submission: October 23, 2013

SUBMITTED BY: Abhishek Samanta
#208, 440 Huntington Ave
Boston, MA-02115
samanta@ccs.neu.edu

COMMITTEE: Prof. Ravi Sundaram (Advisor)
Prof. Rajmohan Rajaraman
Prof. Guevara Noubir
Dr. Ram Ramanathan, Raytheon BBN Technologies (External Member)

Abstract

In today's world, wireless technology is widely employed because of its various benefits, such as mobility, low-cost deployment, scalability etc. But, at the same time, it suffers from a variety of issues ranging from speed and stability to security. In this thesis, we identify three major challenges and propose efficient solutions to mitigate them. First, the broadcast nature of wireless communication makes it inherently vulnerable to eavesdroppers. This makes it very difficult for a participant in a wireless network to discover and access services without also disclosing their identity and need for service. We develop a protocol based on partial (additive) homomorphic functions for private service discovery. Second, wireless networks are inherently ad hoc, with participants dynamically entering and leaving the network at different times. This asynchrony complicates the task of finding shared channels of communication. We present near-optimal schemes for asynchronous channel discovery. The third problem relates to the energy-efficiency of wireless transmissions. A typical wireless agent uses power from an on-board battery with limited power supply. In a multi-hop network it is a non-trivial problem to find relays and schedule non-interfering transmissions which conserve energy. We develop energy-efficient schemes for discovering next-hop relays.

Contents

1 Introduction **4**

2 Private service discovery **5**

2.1 Motivation 5

2.2 Related Work 5

2.3 Our Contributions 6

2.4 System Design 6

2.4.1 System Model 6

2.4.2 Attack Model 7

2.5 Protocol 7

2.5.1 Correctness 9

2.5.2 Security 10

2.6 Evaluation 11

3 Asynchronous channel discovery **12**

3.1 Motivation 12

3.2 Related Work 12

3.3 Model 12

3.4 Bounds on time to rendezvous among synchronous agents 13

3.5 Proposed Research 14

4 Energy efficient relay discovery **14**

4.1 Energy efficient relay selection by accumulating energy at relays 14

4.1.1 Motivation 14

4.1.2 Related work 14

4.1.3 Model 15

4.1.4 Bug in NP-completeness proof described in [1] 15

4.1.5 Proposed Research 15

4.2 Stochastic multi-relay routing 16

4.2.1 Motivation 16

4.2.2 Related work 17

4.2.3 Model 17

4.2.4 Proposed Research 17

5 Plan **18**

1 Introduction

Over the last few decades, wireless communication proved to be an enabling technology to an increasingly large number of applications. Starting from wireless capable consumer devices used day-in day-out to wireless sensor nodes deployed in hard to reach places; wireless technologies have affected human life in many different ways. Now-a-days almost all kinds of devices communicate via some kind of wireless technology, viz. WiFi, Bluetooth, Radio Frequency Identification (RFID), Near-Field Communication (NFC) etc. This prolific dependency on wireless communication is ushered by wide variety of opportunities offered by this technology. Although mobility is the most touted benefit perceived by wireless communication, under different circumstances this technology has found its application because of its simplicity and practically no deployment overhead. For example, pacific tsunami warning center deploys many sensor nodes in several parts of Pacific Ocean to gather data on underwater earth-quakes. Although these sensor nodes are relatively stationary, wireless communication is used, because wired communication is highly impractical in this scenario. But, as with any other prevalent technology, a major lacuna in most of the wireless networks is its inability to utilize sophistications of this technology to the fullest. This thesis work proposes following new techniques to solve some of the existing problems.

Private service discovery: Since, the advent of online social networks (OSNs) people have started sharing small pieces of their life, online. Moreover, location based services (LBS) require users to provide with their location and other sensitive informations. Leakage of these personal informations to an adversary might prove fatal for the user. Most of these information sharing happens with an intention to find nearby service(s). It has been seen that, in recent years, a major part of this information sharing is initiated from mobile platforms. But, a much less appreciated facet of mobile networks is its more vulnerability toward security leakage than any other form of communication. This is because of what is termed as "wireless broadcast advantage" (WBA) [2] of wireless transmission. When a wireless agent transmits a packet using omni-directional antenna all its neighbors receive the message. This effect is advantageous if the transmitted message is intended for all neighbors. Otherwise, this might cause a potential security breach. Highly dynamic nature of wireless network lends the problem of finding near neighbor difficult to solve. The security risk adds one more dimension to the problem. Here, we propose a technique to securely and efficiently avert security risk by using additive homomorphic encryption system.

Asynchronous channel discovery: Tremendous development of mobile technology has put wireless devices as one of the major tools for communication in recent years. More and more wireless devices are brought to life every day to support ever increasing demand for mobile connectivity. But, due to this enormous deployment, the unlicensed frequency bands (mostly, ISM band) is over crowded which essentially results in poor working efficiency of devices using these bands. In contrast, licensed frequency bands have been found to be sparsely used by their primary users. Thus, to increase the efficiency of wireless devices, dynamic spectrum allocation (DSA) techniques have been developed with cognitive radio network (CRN) to utilize unlicensed frequency bands (ISM) along with licensed spectrum opportunistically, when these spectrums are not actively used by its primary users. Although this opens up the opportunity for utilizing a large amount of frequency band, but the agents are capable of accessing only a small fraction of these channels at a time. Thus, for efficient DSA protocols, earliest rendezvous is of prime concern of nodes. Although, randomized protocols exist for probabilistic rendezvous among nodes. But, in some mission critical situations, guaranteed rendezvous within bounded time is of absolute necessity. For example, let us consider a scenario where CRN is deployed by a disaster relief authority for communication during an effort of distributing basic utilities. Each team has their own share of utilities for distribution. A team asks for resupply when the storage nears empty. Under this scenario, it is absolutely necessary that, wireless agents being used by the teams and relief redistribution body rendezvous deterministically within a bounded time. Otherwise, some of the teams might run out of relief due to lack of resupply. Moreover, to add up to the problem, dynamic nature of wireless networks makes individual wireless nodes potentially asynchronous.

Energy-efficient relay discovery: Sensor networks are deployed in hard to reach geographic locations. These networks form an essential part of calamity prediction or disaster recovery systems. Individual sensor nodes are inexpensive and use power from on-board battery with limited amount of power. Most of the times, recharging or changing the power source is not feasible. So, to increase the longevity of network, each sensor node should use available source of power as efficiently as possible. It has been observed that, wireless communication subsystem is one of the most power hungry module in a wireless agent [3,4]. So, it is imperative that, sensor nodes forward packets to its neighbors in energy efficient way, to live long. Energy accumulation at nodes and stochastic routing has been proposed for energy efficiency.
Energy accumulative routing: In traditional wireless communication technique, a packet is only accepted by an agent if the reception power is more than a pre-defined threshold. This threshold is set to much higher level than noise floor of the wireless medium. This technique guarantees successful decoding of received packet. But, on the other hand lots of energy is wasted by discarding unreliable packets received with energy less than the threshold. In contrast, energy accumulation technique enables agents to store multiple unreliable transmissions of same packet and decode it when the accumulated

energy crosses the threshold. We are working towards developing energy efficient protocol with this technique. **Stochastic multi-hop routing:** Wireless medium is inherently very dynamic and error prone in nature. For this reason, selecting the next hop deterministically before sending real message might not yield optimal results. To avoid this problem, we propose a stochastic model for wireless network. Our work would yield distributed routing protocol, based on the solution to stochastic shortest path problem.

2 Private service discovery

2.1 Motivation

People often have the need for assistance from strangers in remote locations. Consider the following requests: please tell the marathon runner with bib #123 I will wait at the finish line; did I leave my key-chain on campus? Is there a brown puppy roaming in the playground? In this article we propose, not just a new architecture, but, in fact, a new cloud based service - the goal is to provide a way for people to connect with others (possibly strangers) in a remote location and obtain (physical) help from them. The new system is deployed as cell phone application, users submit their requests to the cloud which coordinates users' requests and efficiently find possible candidates to respond to the request. Such a service will require efficient technical solutions to problems such as scalability, privacy, reputation etc to overcome the social barriers of soliciting help from strangers. We focus primarily on the technical aspects of scalability and privacy (matching people with strangers in a secure and private way) so that the need for help and the ability/desire to assist are disclosed safely.

Since the emergence of online social networks (OSNs), people have sought help from their social contacts. The most common method to seek for help on social network sites, e.g, Facebook, Twitter, or "strangers helping strangers" [5], is post - an user posts his/her question or request on his/her social network page or a relative group page and waits for response, which is very similar to subscribing to an email list and broadcast questions except exposing more privacy. This method is simple but suffers from three major drawbacks.
High/unpredictable response latency: Popular OSNs, e.g., Facebook, Twitter own worldwide users, who live in different locations and have different schedules. A post on a group page could not reach all the members in a short time and may be overwhelmed by other posts soon.
Limited range of request subjects: Groups on OSNs are typically centered around interests, occupations, genders, ages. So, it is hard to elicit response for time-restricted and location sensitive questions. Most online requests focus on recommendations, suggestions and people do not make off-line offer before they build trust on each other.
Privacy loss: Users requesting help on OSNs could end up exposing themselves to a large group, including friends they know in real life, as well as users, who are not willing/able to offer help. Moreover, when these OSNs are accessed from a wireless device chance of security leakage increases because of WBA. These unnecessary privacy leaks may affect user's personal life and should be avoided.

2.2 Related Work

Geo-social networking [6–9] offers location based services (LBS) to users to interact relative to their locations. LBS typically is an information or entertainment application that is dependent on location of user. By these services users are offered possibilities to find other people, machines and location-sensitive resources. Some applications [10] match users with locations of interest. These services are used for finding a physically proximal social contact or for crowd sourcing. Many of such public LBS provide no privacy while some offer limited protection on an opt-in or opt-out basis. Here we briefly categorize the different approaches to providing privacy, as well as the associated shortcomings.

Middleware: Geopriv [11] and LocServ [12] are policy-based privacy management approaches for secure location transfer that employ a trustworthy middleware mediating between location-based applications and location tracking servers. Geopriv [11] describes an approach to securely transferring location information and associated privacy data by creating "location objects" that encapsulate user location data and associated privacy requirements. Once "location generator" (e.g. user device) creates an "location object", it sends it to a middle server which forwards the object to "location recipient" based on different kinds of rules. LocServ [12] is a middleware service that lies between location-based applications and location tracking servers. It offers a general framework of components that allows users to apply general policies to control release of their location information. However, the practicality of such systems have yet to be determined, as the trustworthiness of middleware is hard to guarantee.

Dummies or Anonymity: Instead of sending out the exact location, a client sends multiple different locations to the server with only one of them being true [13]. The drawback of such schemes is that over the long run the adversary is able to figure out the client's location by comparing the intersection of uploaded locations. Some other schemes [14, 15] separate location information from other identifying information and report anonymous locations to the server. However, guaranteeing anonymous usage of location-based services requires that the precise location information transmitted by a client cannot be easily used to re-identify the subject.

Location hiding: Clients define sensitive locations where they do not want to be tracked, and the location-based application stops tracking when the user gets close to those areas [16].

Location perturbation: These schemes "blur" the exact location information to a spatial region [17–20] or send a proxy landmark instead [21] and hence, are not suitable for applications that require accurate locations.

The scheme presented in this article uses *client-specific*, *personalized* and *global* blurs that are random elements in a finite field to guarantee perfect accuracy and cryptographic security; more on this in the sections to follow.

To complete our review of related work we briefly survey the literature on homomorphic encryption. Homomorphic encryption is a type of encryption scheme that provides ability to perform arithmetic operation on cipher text and get the encrypted result which is equivalent to the encryption of the result by applying the same arithmetic operation on the plain text. The encryption systems of Goldwasser and Micali [22], and El Gamal [23] are known to support either addition or multiplication among encrypted cypher texts, but not both operation at the same time. In a breakthrough work, Gentry [24] constructed a fully homomorphic encryption scheme (FHE) capable of an arbitrary number of addition and multiplication on encrypted data. Fully homomorphic encryption schemes are very powerful as it computes any function on an encrypted cipher text. But, Lauter et al [25] showed that fully homomorphic encryption schemes till date are very resource consuming and are impractical to be used for most of practical purposes.

2.3 Our Contributions

To overcome the above mentioned drawbacks, we propose a location-based cyber-physical network allowing people to reach friends or strangers in desired locations for help. Our system is easily deployed as a location-based cell phone application; the server coordinates client requests and efficiently finds candidates who are able/willing to offer help, even possibly physical help, in real-world life-threatening emergencies.

From a technical standpoint our primary contribution is to show how partially homomorphic encryption can be adapted to a distributed setting so as to guarantee cryptographic security without sacrificing efficiency gains. The resulting protocol finds near-neighbors in constant-time thus providing efficient and private match of help-seekers and help-givers.

Proposed system preserves efficiency and privacy while calculating near neighbor, by employing different blurring techniques and partially homomorphic encryption.

2.4 System Design

2.4.1 System Model

A network consists of n clients and one server. Clients are represented by $i \in [1 \dots n]$. We call a client asking for help a querying client and we reserve the notation q for that. Each client has a mobile device with enough computation power to efficiently encrypt-decrypt using additive homomorphic functions. Clients are assumed to share a common key with which they exchange private messages that are denied to the server. The server is efficient in simple arithmetic computations (viz. addition, subtraction). It is also capable of broadcasting request to f clients, efficiently. On the other hand, a client can efficiently talk to the server or a small group of other clients. The server is used to authenticate clients and to initiate distributed near-neighbor computation. Once the querying client knows the set of near neighbors, it sends out the help request. Each client is associated with an user-name, password and profile. A client uses user-name and password for authentication. A profile is a collection of d variables and their respective values (or, range of values). Variables are drawn from a metric space and for the purposes of this article are assumed to take real numbers. For sake of notation, we say that profile of a client $i \in [1 \dots n]$ is p_i. p^q is the profile of a querying client. To minimize dependencies on itself, the server delegates all computationally extensive operations, viz. distance computations, encryption-decryption process, to the clients.

2.4.2 Attack Model

We consider both external and internal attack models. The goal of an adversary is to extract profile informations from the messages seen so far.

External attack: Under external attack model, adversary does not have access to secrets used by the protocol. The only way for the adversary to get hands on a message is by overhearing data transmissions among different parts of the system.

Internal attack: Adversary compromises the server or, n_a number of clients. When the server or, a client is compromised it works as an attacker and launches attack against rest of the system. We classify these attacks as follows,

Rogue server: In this scenario, the server goes rogue and tries to retrieve profile information of at-least one good client from messages stored in its memory.

Rogue client: We assume that there are n_a rogue clients (attackers) present in the network and launch attack to leak profile information of at-least one good client. All the attackers share informations among themselves to make the attack successful. Rogue clients can launch two types of attacks as follows,

- *Passive Attack:* The compromised client passively tries to extract profile information of at-least one good client.
- *Active attack:* A compromised client sends a fake Help-Request to server. After receiving the request, the server disseminates its response to the network. With help of this response, other attackers try to retrieve profile information of a good client successfully.

We present some definitions we will need later on

Distance: The distance between two profiles p_1, p_2, represented as d-dimensional vectors, is defined as:

$$\|p_1 - p_2\| = (\Sigma_i(|p_{i1} - p_{i2}|)^2)^{(1/2)},$$

where p_{i1} and p_{i2} are the values of the i^{th} dimension of p_1 and p_2, respectively.

Near-neighbor: Given a querying client q, a set of clients C, and a distance value $dist$, $i \in C, q \notin C$, is said to be a near-neighbor of q if the distance between p^q and p_i is at most $dist$, i.e. if,

$$\|p^q - p_i\| \leq dist,$$

where p^q and p_i are profile data of c^q and c_i, respectively.

Blur: Blur is a random number which is used to blur data. e.g. data p is blurred with a random blur r as follows,

$$\beta_r^{\pm}(p) = (p \pm r) \mod P,$$

where $r \in [1, P]$ and P is a large public prime number.

Tolerance-value: Tolerance value is the maximum distance between profile of a client j and profile requested by q, within which j receives help request from q.

Our scheme builds on prior work on confidential publish/subscribe schemes. In the confidential publish/subscribe process, when a client wishes to send a request, it retrieves a random number from the server and encrypts this number and sends it back to the server. But, one problem with this scheme is that, the server uses a common random number for all the clients. If the random number changes in server between the time the client retrieves it and the time the client sends the encrypted random number back to the server, the whole process of near-neighbor computation fails. For detailed discussion please refer to Section II-D in [26].

2.5 Protocol

The central idea of the proposed protocol lies in the solution of the following puzzle.

Puzzle 1. *Two agents A and B have two numbers a and b, respectively. How can a third agent C securely compute the sum* $(a + b) \mod P$*, where P is a public prime, without the individual knowledge of a or b.*
Assumption: Both A and B have access to a random number r which is kept secret from C.

Solution 1. *A sends $(a+r) \mod P$ to C. B sends $(b-r) \mod P$ to C. C adds the two messages received from A and B.*

Although our scheme is based on the solution stated above. We use different techniques to synchronize random blurs among different clients. Also, we use a number of random blurs to avert security leakage. Here, we present a brief overview of the proposed protocol.

At the startup time, the server generates client specific blur for each client and a global blur, which are kept secret from clients.

When profile of a client changes, it blurs the changed profile with a random personalized blur and sends it to the server along with encrypted blur. Since, the profile data is blurred with a random blur and the blur is encrypted, no profile information leaks from the blurred profile. The server re-blurs the already blurred profile with global and client-specific blur of the client and distributes among a set of randomly selected clients.

When a client wants help, he/she blurs request-profile with his/her personalized blur and sends to the server which in turn re-blurs the already blurred profile and distributes to all clients. Along with these re-blurred profiles, the server also forwards sum of encrypted client specific and personalized blurs to all clients in the network. With these informations, a client computes the set of near-neighbors of requesting client. Server uses both client specific blur and global blur, because without these blurs under certain attack scenarios, an attacker can deterministically compute profile information of a requesting client.

Now, we present the proposed protocol in detail.

Initialization: In this phase, server assigns client-specific blur ${}^{cs}r_i$ to each client i. The server also generates a global blur r^g. Both client-specific and global blurs are kept secret from clients. These are used by the system to blur client profiles.

ProfileUpdate-Request: This phase is invoked by a client i, when its profile data p_i is changed.
In this phase, i updates the server with its blurred profile data. Server forwards blurred p_i among selected set of clients. The data transfer is thus composed of two sub-phases as follows,
Update: In *Update* phase, a client i blurs its profile data p_i by blurring each dimension separately as follows,

$$\begin{aligned} \beta^-_{r_i}(p_{ji}) &= (p_{ji} - r_i) \mod P, \forall j \in [1,d] \\ \beta^-_{r_i}(p_i) &= (\beta^-_{r_i}(p_{1i}), \beta^-_{r_i}(p_{2i}), ..., \beta^-_{r_i}(p_{di})) \end{aligned} \tag{1}$$

where, p_{ji} is j^{th} dimension of p_i, and r_i is the personalized blur used by i. The client also encrypts its personalized blur, using the additive-homomorphic encryption $\xi^h_{sk}(r_i)$, and sends the pair $(\xi^h_{sk}(r_i), \beta^-_{r_i}(p_i))$ to the cloud.
Redistribution: The server invokes this phase when it receives an update request from a client i. Client-specific blur ${}^{cs}r_i$, and the global blur r^g are used to blur already blurred profile of i. We call this process re-blurring.

$$\begin{aligned} p^{rblur}_{ji} =& (\beta^-_{r_i}(p_{ji}) -^{cs} r_i + r^g) \mod P = (p_{ji} - r_i -^{cs} r_i + r^g) \mod P \\ & p^{rblur}_i = (p^{rblur}_{1i}, p^{rblur}_{2i}, ..., p^{rblur}_{di}) \end{aligned} \tag{2}$$

The server saves the encrypted blur $\xi^h_{sk}(r_i)$ and distributes re-blurred profile values computed in equation (2) along with the address of i to k random clients. These clients are selected in k rounds. In each round two clients are chosen randomly. The client which is less loaded is selected.

Help-Request: When a client (q) is in need of help, it invokes Help-Request phase. In this phase, q sends blurred requested-profile along with a tolerance value to the server. On reception of a request, the server broadcasts the blurred requested-profile and delegates the near-neighbor computation to all clients. Clients compute distance between the requested profile and saved blurred-profiles and send back the result directly to the querying client, q. Thus, this phase is composed of 3 sub-phases as follows,
Request: The requesting client q blurs the requested-profile p^q with a randomly generated personalized blur (r^q) by blurring each dimension of p^q separately.

$$\begin{aligned} \beta^+_{r^q}(p^q_i) &= (p^q_i + r^q) \mod P, \forall i \in [1,d] \\ \beta^+_{r^q}(p^q) &= (\beta^+_{r^q}(p^q_1), \beta^+_{r^q}(p^q_2), ..., \beta^+_{r^q}(p^q_d)) \end{aligned} \tag{3}$$

q encrypts its personalized blur and tolerance value (tol) and sends the tuple $(\xi^h_{sk}(r^q), \xi_{sk}(tol), \beta^+_{r^q}(p^q))$ to server.

Redistribution: The server invokes this phase on reception of a request from q. Without loss of generality, let us assume that a client i has blurred profile information of t other clients each of which is represented by j. Server builds a set (R_i) of t 6-tuples (T_j) and sends it to i. Each of these 6-tuples contains informations to determine near neighbor of the requesting client.
1^{st} and 2^{nd} entries of T_j are addresses of q and j, respectively.

$$^1T_j = q, ^2T_j = j$$

3^{rd} entry is built by reblurring the blurred profile of q, with the clients-specific blur assigned to q and the global blur, as follows.

$$^3T_{lj} = (\beta^+_{r^q}(p^q_l) + {^{cs}r^q} + r^g) \mod P = (p^q_l + r^q + {^{cs}r^q} + r^g) \mod P, \tag{4}$$

where $^3T_{lj}$ is l^{th} dimension of 3^{rd} entry of T_j, $^{cs}r^q$ is client specific blur of q and r^g is the global blur.
The server adds encrypted personalized random blur of q and j to build 4^{th} entry of the tuple. This is where we use additive homomorphic nature of encryption scheme.

$$^4T_j = (\xi^h_{sk}(r^q) + \xi^h_{sk}(r_j)) \mod P \tag{5}$$

5^{th} entry is built by adding the client specific blur of q and j. Since, both the client-specific blurs are not known to clients, the individual value of either $^{cs}r^q$ or $^{cs}r_j$ is not leaked by this entry.

$$^5T_j = ({^{cs}r^q} + {^{cs}r_j}) \mod P \tag{6}$$

6^{th} entry is the encrypted tolerance value sent by q. This tolerance value is used in the near-neighbor computation.

$$^6T_j = \xi_{sk}(tol) \tag{7}$$

The tuple T_j is then forwarded to all clients in the network.
Distance-Computation: In this phase clients compute distance between the blurred requested-profile and saved blurred profile data of other clients. Let us assume that after redistribution phase, a client i receives a set R_i. Let us also assume that i has blurred profile informations of t clients, $j \in [1, \ldots, n]$. Let $T_j \in R_i$ be the tuple containing data to compare with j and p^{rblur}_j be the re-blurred profile of j.
Since, i has the shared secret sk, it decrypts the encrypted blur and tolerance value in T_j. c_i informs requesting client (q) about clients whose re-blurred profile satisfy the following condition.

$$(\sum_{l=1}^{d}(^3T_{lj} - p^{rblur}_j - \delta^h_{sk}(^4T_{lj}) -^5 T_{lj})^2)^{1/2} < \delta^h_{sk}(^6T_j), \tag{8}$$

where $\delta^h_{sk}(\cdot)$ decryption using key sk.

2.5.1 Correctness

After stating the newly proposed scheme, here we prove that, the scheme calculates distance correctly between requested profile data q and blurred profile of a candidate client j. The fact that blurring according to our proposed scheme preserves distance is captured by the following lemma.

Lemma 1. *Given, T^q_j is the tuple containing data to compare with j and p^{rblur}_j is the blurred profile of j*

$$(\sum_{i=1}^{d}(^3T^q_{ij} - p^{rblur}_j - \delta^h_{sk}(^4T^q_{ij}) -^5 T^q_{ij})^2)^{1/2} = \|p^q - p_j\|$$

Proof. As described in ProfileUpdate-Request protocol, blurred profile stored on the server is calculated using equation (2).

$$p^{rblur}_{ij} = (p_{ij} - r_j - {}^{cs}r_j + r^g) \mod P \tag{9}$$

Since, $\xi^h_{sk}(\cdot)$ is an additive homomorphic encryption, from equation (5),

$$^4T^q_j = (\xi^h_{sk}(r^q) + \xi^h_{sk}(r_j)) \mod P = \xi^h_{sk}(r^q + r_j) \mod P$$

So,

$$\delta^h_{sk}(^4T^q_j) = \delta^h_{sk}(\xi^h_{sk}(r^q + r_j) \mod P) = (r^q + r_j) \mod P \tag{10}$$

So, combining equations (4), (6), (9), and (10),

$$\begin{aligned}
&(^3T^q_{ij} - p^{rblur}_j - \delta^h_{sk}(^4T^q_{ij}) -^5 T^q_{ij}) \\
&= ((p^q_i + r^q + {}^{cs}r^q + r^g) \mod P - (p_{ij} - r_j - {}^{cs}r_j + r^g) \mod P - (r^q + r_j) \mod P - ({}^{cs}r^q + {}^{cs}r_j) \mod P) \\
&= (p^q_i - p_{ij}) \mod P
\end{aligned}$$

Thus, according to the definition,

$$(\sum_{i=1}^{d}(^3T^q_{ij} - p^{rblur}_j - \delta^h_{sk}(^4T^q_{ij}) -^5 T^q_{ij})^2)^{1/2} = (\sum_{i=1}^{d}((p^q_i - p_{ij})^2)^{1/2}) \mod P = \|p^q - p_j\|$$

□

2.5.2 Security

We measure security of the proposed protocol with following metric,
Probability of Information Leak per Comparison (PILC): PILC is defined as the probability of an adversary successfully computing the profile data of a client by single comparison.

Security against external attacker and rogue server : In the proposed protocol ProfileUpdate-Request and Help-Request are blurred with random personalized blur of a client and then these already blurred profiles are further blurred with client specific and global blurs. So, only way for an external attacker and rogue server to retrieve client profile from a blurred profile is by guessing the blur correctly. Since, all the blurs are selected uniformly at random from $[1, P]$,

$$PILC_{external} = PILC_{rogue-server} = \frac{1}{P}$$

Security against passive rogue client : A passive rogue client tries to retrieve client profile data from their respective reblurred profiles data. According to the proposed protocol, the profile data of a client j is reblurred with its client-specific blur and the global blur as follows,

$$p^{rblur}_{ji} = (\beta^-_{r_i}(p_{ji}) - {}^{cs}r_i + r^g) \mod P = (p_{ji} - r_i - {}^{cs}r_i + r^g) \mod P$$

where, r_i and ${}^{cs}r_i$ are the personalized and client-specific blur, respectively. r^g is the global blur.

$$p^{rblur}_i = (p^{rblur}_{1i}, p^{rblur}_{2i}, \dots, p^{rblur}_{di})$$

The adversary retrieves the blurred profile suucessfully, if it guesses $(r^g - {}^{cs}r_i - r_i) \mod P$ correctly. Since, all the blurs are selected uniformly at random, chance of that happending is $\frac{1}{P}$. Thus,

$$PILC_{passive-rogue-client} = \frac{1}{P}$$

Security against active rogue clients : Now let us consider attacks launched by active rogue clients. According to active attack model, a rogue client a sends a fake Help-Request to the server. The server then builds a set of tuples R_i with T_j as follows for all clients ($i \in C$) and forwards it.

- ${}^{1}T_j = a$
- ${}^{2}T_j = j$, where j is a client whose blurred profile data is stored by i.
- The third dimension of T_j is reblurred request-profile of the requesting attacker (a). The request-profile (p^a) blurred with personalized blur of a (r^a) is further reblurred by using client specific blur of a (${}^{cs}r^a$) and global blur (r^g). This process of reblurring is shown below,

  $${}^{a}p_l^{rblur} = (\beta^{+}_{r^a}(p_l^a) + {}^{cs}r^a + r^g) \mod P = (p_l^a + r^a + {}^{cs}r^a + r^g) \mod P,$$

  where ${}^{a}p_l^{rblur}$ is l^{th} dimension of reblurred requested profile of a.

  $${}^{3}T_j = \{{}^{a}p_1^{rblur}, {}^{a}p_2^{rblur}, \ldots, {}^{a}p_d^{rblur}\}$$

- ${}^{4}T_j = \xi^{h}_{sk}(r^a + r_j) \mod P$, where r^a is the random personalized blur used by a and r_j is the random personalized blur used by client j
- ${}^{5}T_j = ({}^{cs}r^a + {}^{cs}r_j) \mod P$
- ${}^{6}T_j = \xi^{h}_{sk}(tol)$, where tol is the tolerance value requested by a.

Since, all the attackers share informations, a knows the profile requested by a (p^a) and the random personalized blur used by a (r^a). With these informations, a retreives $(({}^{cs}r^a + r^g) \mod P)$ and personalized blur (r_j) used by j whose reblurred profile is stored by a. If a guesses either global blur (r^g) or the client specific blur of a (${}^{cs}r^a$) correctly, it retrieves client specific blur of j and also the global blur. Thus, q retrieves the profile information of j from its blurred profile. Since, both the client-specific and global blurs are selected uniformly at random from $[1, P]$,

$$PILC_{active-rogue-client} = \frac{1}{P}$$

2.6 Evaluation

Implementation: The implementation of the proposed system includes two parts — client side application and the server. We implemented the client side application with a prototype mobile application running on iOS 5.0, allowing users to

- log in or register with unique user name and password.
- choose time interval to update profile; by setting a fixed update time interval, exact profile change time is not exposed to the server.
- input request location (either latitude and longitude coordinates or zip code) and request content.
- get notification when the client is close to a requested location; response willingness to offer help.
- get notification if anyone offers help to the client's request.

We implemented the server using Python Twisted library. The major concerns of the performance of the proposed system are client application battery consumption and server scalability.

Mobile application: We first examine the proposed system on mobile devices. Our application registers itself as a background VoIP service allowing it to (1) maintain a persistent connection with the server, (2) periodically fetch location information, even if the app is running on background. Battery consumption results are shown in Table 1.

Server Scalability: For server side performance we are primarily interested in understanding the rate of *requests* that a single server can handle, as this serves as the dominating factor controlling the number of on-line users that the server can support. Table 2 shows computational complexity of each phase in our system.

Please refer to [26] for detailed evaluation.

Table 1: Impact of proposed system as iOS application on battery life in ProfileUpdate-Request

network	standard (GPS)	standard (WiFi/cellular)	significant-change location service
3G	10h	12h 8mins	12h 10mins
WiFi	11h 14mins	16h 14mins	16h

Table 2: Runtime of different phases of proposed system on servicing client

ProfileUpdate-Request	Help-Request
$O(1)$	$O(d \cdot loglogn)$

3 Asynchronous channel discovery

3.1 Motivation

Given the ever-increasing demand for all things wireless, spectrum has become a scarce resource. Historically, regulators around the world have employed a command and control philosophy towards managing spectrum [27]: Some channels were statically licensed to particular users (for certain periods and in certain geographies) while others were kept aside for community use. Cognitive radio networks have emerged as a modern, dynamic approach to spectrum allocation [28, 29]

3.2 Related Work

Rendezvous problems have a long history in mathematics - an early example is Rado's famous "Lion and Man" problem [30]. Over time a variety of problems and solutions have evolved in both adversarial [31] and cooperative settings [32]. Rendezvous in networks has been extensively studied in the computer science community [33]. Though the study of rendezvous in cognitive radio networks is relatively recent there already exists a comprehensive survey [34] that contains a detailed taxonomy of the different models including the specific one relevant to this work. The problem of guaranteed blind rendezvous in the asymmetric, asynchronous and anonymous case was first considered in [35] and subsequently in [36, 37]. The use of prime numbers and modular algorithms was initiated in [38]. However, the general case of the problem withstood attack until [39, 40]. The current state of the art is [41] which achieves $O(n^2)$ algorithm for the asymmetric case and $O(n)$ for the symmetric case.

3.3 Model

We work in the blind model where a collection of agents A_i wish to discover each other with no dedicated common control channel or other shared infrastructure. Time is divided into discrete slots and spectrum is divided into discrete channels, [n] = 1, 2, . . . , n. Each agent may access (or, hop on) a single channel in a single time slot and two agents rendezvous when they hop on the same channel in the same time slot. When more than 1 agents hop onto the same channel, the channel contention is resolved by CSMA/CA MAC protocol. Challenge is to design a channel-hopping schedule for each agent so that they discover each other. As stated thus far, the problem has the trivial solution where all agents can hop on a specific channel, say channel 1, in the very first time slot. However, reality is complicated by three additional requirements: asymmetry, asynchrony and anonymity.

Asymmetry: Different agents may have access to different subsets of channels as a result of local interference or variations in radio capabilities. Let $S_i \subseteq [n]$ be the subset of channels to which agent A_i has access. Thus the challenge is to create for each agent A_i a channel-hopping schedule $\sigma_i : \{0, 1, \ldots\} \to S_i$ which guarantees that $\exists t, \sigma_i(t) = \sigma_j(t)$ for any two agents $A_i, A_j, s.t. S_i \cap S_j \neq \phi$. (In the symmetric setting all agents have access to the identical subset of channels.)

Asynchrony: Different agents may not share a common notion of time. They may commence at different wake-up times inducing a relative shift in their progress through their schedules. Note that agents do possess a common understanding of slot duration. The goal, therefore, is to ensure rendezvous between a pair of agents in the shortest possible time once they have both woken up. (In the synchronous setting all agents share a common notion of absolute time.)

Anonymity: In our setting an agent's schedule must depend only on the subset of channels available to, and not on a distinct identity of, the agent i.e., σ_i must depend only on S_i . Note that S_j is unknown to A_i for $i \neq j$ and it is allowed for two different agents to have the same set of accessible channels, i.e., $S_i = S_j$ for $i \neq j$.

Now, the problem has the naive randomized solution, in which each agent, at each time step, selects a channel uniformly and independently at random from its subset. It is not hard to see that this provides a high-probability guarantee of rendezvous for agents A_i, A_j in time $O(|S_i||S_j| \log n)$. However, the deterministic setting is the gold-standard in the cognitive radio networking community: it makes the weakest assumptions about the devices, which need not have an available source of randomness, and provides absolute guarantees on rendezvous time.

3.4 Bounds on time to rendezvous among synchronous agents

We reserve the notation i' for bitwise negation of i. Also, i_2 is used to represent the binary representation of i.

Definition 1. *$\chi(a, b)$ is defined to be the location of first difference between the binary representation of a and b.*

Definition 2. *A* **schedule** *(s) is a binary sequence, $s \in \{0, 1\}^{\mathbb{N}}$, with the convention that 0 calls for hopping on the smaller channel and 1 calls for hopping on the larger channel.*

The following 2 theorems capture the upper and lower bound on time to rendezvous for the case when each agent has access to 2 channels.

Theorem 1. *Synchronous agents having access to 2 channels each, are guaranteed to rendezvous within $O(\log \log n)$ time.*

Proof. Since, there are n channels, $\chi(\cdot, \cdot)_2 < \log \log n$. Thus the hopping sequence from Lemma 2 is of length $O(\log \log n)$. □

Lemma 2. *In synchronous setting, hopping sequence $S = 01\chi(\cdot, \cdot)_2\chi'(\cdot, \cdot)_2$ guarantees rendezvous among all nodes having access to 2 channels.*

Proof. Let us consider two agents A and B. Set of channels available to A and B are $S_A = \{a_l, a_h\}$ and $S_B = \{b_l, b_h\}$, respectively. Moreover, without loss of generality, let us assume that $a_l < a_h$ and $b_l < b_h$. Also, $S_A \cap S_B \neq \phi$. One of the following 4 scenarios may happen,

- **Scenario 1 ($a_l = b_l$):** By dint of 0 at the beginning of the schedule, rendezvous under this situation is achieved.
- **Scenario 2 ($a_h = b_h$):** Rendezvous is guaranteed, because of presence of 1 in the schedule.
- **Scenario 3 ($a_l = b_h$):** It is to be noted that, to make guaranteed rendezvous in this scenario, A must choose 0 in some time-slot and B must choose 1 in that same time-slot. According to the definition, $\chi(a_l, a_h) \neq \chi(b_l, b_h)$. So, $\chi(a_l, a_h)_2 \neq \chi(b_l, b_h)_2$. Thus, there is a location where binary string $\chi(a_l, a_h)_2\chi'(a_l, a_h)_2$ contains 0 but $\chi(b_l, b_h)_2\chi'(b_l, b_h)_2$ contains 1.
- **Scenario 4 ($a_h = b_l$):** Similar to Case 3.

Combining above mentioned scenarios, the hopping sequence $S = 01\chi(\cdot, \cdot)\chi'(\cdot, \cdot)$ guarantees rendezvous between agents A and B.

□

Theorem 2. *Rendezvous requires at least $\Omega(\log \log n)$ time, even in the synchronous model when agents are promised to have sets of channels of size 2.*

Proof. Let us consider the complete graph κ_n, with the interpretation that each vertex represents a channel and each edge represents a set of size two. Moreover, each edge has a direction from the node with lower index to the node with higher index.

Let σ be a schedule which guarantees rendezvous in time T. In this case, we treat a schedule as a finite length string in $\{0, 1\}^T$, with the understanding that rendezvous is guaranteed before any schedule is exhausted. Let us treat every schedule as a coloring of the edges of κ_n. So, the size of the palette is 2^T. According to a variant of Ramsey's theorem, any m-coloring of the edges of the complete graph, κ_n, must have a monochromatic triangle when $n \geq em!$. However, it is to be noted that, a monochromatic triangle yields an ordered triple $i < j < k$ for which the schedules associated with (i, j) and (j, k) are identical: such schedules never rendezvous. It follows that $e(2^T)! \geq n$. Thus, $T = \Omega(\log \log n)$. □

3.5 Proposed Research

- Extend the upper and lower bounds shown in Section 3.4 to more general case, where each synchronous agent has access to more than two channels.
- In asynchronous settings, agents start hopping channels at different points in time. This relaxes the unnatural assumption of synchronicity among agents. It would be interesting to compute similar bounds for asynchronous agents.

4 Energy efficient relay discovery

Sensor nodes are small inexpensive devices running on on-board battery power. Most of the times it is impractical to change or recharge the battery. This makes sensor nodes very short lived compared to other wireless devices, e.g. consumer wireless devices. Although, several different approaches have been proposed to harvest ambient energy (e.g. solar energy, electro magnetic energy etc.) periodically to recharge battery. But, these energy scavenging techniques require building complex systems and also are not efficient. Moreover, even with on-board energy harvesting techniques, continuous use of a sensor node lends the device inaccessible for regular work for long period of time. It has been shown that wireless communication module is the most power hungry subsystem in a mobile device. So, it is absolutely imperative that mobile devices use energy efficient routing protocols for longer lifetime. It has been seen that, wireless transmissions over longer distance fade more quickly than in shorter distance and thereby wasting more power. To work around this problem cooperative routing protocols have been developed. In such protocols, instead of transmitting to a far away destination, an agent transmits to a relatively closer neighbor (relay) which in turn forwards the message to the original destination. Energy efficiency of a cooperative network depends on the selection of relay nodes. Two techniques called ”Energy accumulation” and ”Stochastic routing” have been devised to increase the energy efficiency of cooperative networks. Energy accumulation provides more energy saving over stochastic routing with a cost of sophisticated hardware.

4.1 Energy efficient relay selection by accumulating energy at relays

4.1.1 Motivation

In traditional wireless communication system, agents only keep packets which have been received with a power higher than a predefined threshold value, otherwise the packet is dropped. This threshold value is set much higher than noise level, to ensure successful decoding of packets. But, in reality if the reception power of a packet is more than noise level of the medium (but, less than the threshold), the agent can retrieve some partial information about the packet. Energy accumulative routing protocols save energy over traditional form of wireless communication by storing partially heard packets. In these protocols, partially overheard signals of previous transmissions for the same packet are aggregated by nodes and decoded using a maximal ratio combiner technique.

4.1.2 Related work

Cooperative routing protocols have received lots of attentions to increase the efficacy of message transfer protocols in wireless networks. Kailas et. al. [42] have proposed a technique called opportunistic large array (OLA) to increase network life time. In OLA technique several relay nodes synchronize their transmissions to amplify the power at receivers placed outside their individual coverage area. But, one disadvantage with this technique is the requirement of high level of synchronization. To avoid this problem, energy accumulation routing is employed. In a wireless network, because of broadcast nature of a wireless transmission, every node is able to listen to several transmissions of a packet. A node might not be able to decode each of such transmissions because of low reception power. But over time, a node can successfully decode the packet by aggregating accumulated energy from multiple transmissions using maximal ratio combiner technique. Energy accumulating routing protocols have been used to increase the efficiency of several different aspects of wireless networks. Sharma et. al. [43] have used energy accumulation technique to increase capacity of a network. Girici et. al. [44] have proposed heuristics to minimize outage probability in the network. "Wireless Multicast with HitchHiking"(WMH) proposed by Agarwal et. al. [45] is the first protocol that uses accumulative relay technique to save transmission energy. WMH starts by building a MST rooted at the source. Once the MST is built, the power level of each node is decreased without breaking the tree. Yang et. al. [46] have proposed heuristics similar to WMH to minimize energy consumption of packet transmission. Authors of [47–49] have proposed several other heuristics to solve minimum energy problem. Maric et. al. [1] have proven that minimum energy broadcast problem with energy accumulation technique is NP-complete and proposed a heuristic. Baghaie et. al. [50] have shown that delay constrained energy efficient broadcast in cooperative networks is not only NP-complete, but also $o(\log n)$-inapproximable. Chen et. al. [51] showed that, not only broadcast but also minimum energy unicast with energy accumulation is NP-complete and proposed a heuristics called "MEAR". Baghaie et. al. [52] proved that, energy efficient transmission in multi-flow wireless network is NP-hard and also $O(n^{1/7-\epsilon})$-inapproximable.

4.1.3 Model

We consider a static wireless network with n nodes. Radio propagation is modeled by a given symmetric AWGN channel, with a channel gain h_{ab} (sometimes, we use the notation $h(a,b)$, instead) from node b to a. The network has enough bandwidth resources to enable each transmission to occur in an orthogonal channel, thus causing no interference to other transmission. Each node has both transmitter and receiver capable of operating over all available channels.

We assume that appropriate coding (e.g., repetition coding, space-time coding etc.) is used to enable nodes to accumulate power. Every node is capable of transmitting packets with different power levels selected from $W = \{w_1, w_2, \ldots\}$. Every node is capable of storing all transmissions of a packet before the accumulative reception power for that packet is greater than a predefined threshold value (τ).

4.1.4 Bug in NP-completeness proof described in [1]

Example Scenario: Let us consider the network shown in Figure 1. Node 0 is the source node, that has a packet to broadcast. There are m other nodes $i, \forall i \in [1, m]$. Direction of edges represent direction of packet flow. Let us represent the network in Figure 1 by a graph $G = (V, E)$.

Construction of $G' = (V', E')$ from G: For each $k \in V$, cluster C_k is constructed. A cluster C_k includes a node $i_{j,k} \in V'$ for each incident edge $(j,k) \in E$ and a node $o_{k,l} \in V'$ for each outgoing edge $(k,l) \in E$. We define the function, $h(a,b)$, for each node $a, b \in V'$, as follows,

- $h(i_{j,k}, o_{j,k}) = 1, \forall (j,k) \in E$
- $h(i_{j,k}, i_{j',k}) = 1, \forall i_{j,k}, i_{j',k} \in C_k$
- $h(o_{k,l}, i_{j,k}) = 1, \forall o_{k,l}, i_{j,k} \in C_k$
- $h(a,b) = 0, otherwise$

An edge is constructed between two nodes $a, b \in V'$, if $h(a,b) = 1$.

It is to be noted that total energy consumed in a broadcast by node $o_{0,1}$ is $2 \cdot m$, which is a solution to the minimum energy accumulative broadcast problem of graph G'. But, it is clear that, G does not have a Hamilton path.

4.1.5 Proposed Research

I plan to achieve the following,

- Prove NP-completeness of minimum energy broadcast problem with energy accumulation.

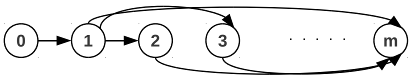

Figure 1: Example network for which the reduction proposed in [1] fails

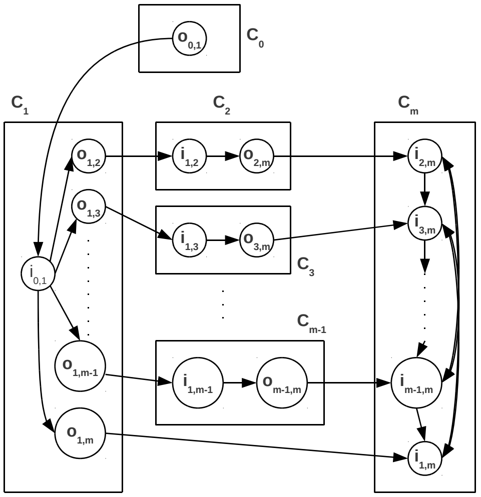

Figure 2: Graph G' constructed from network in Figure1

- Compute inapproximability result in minimum energy broadcast.
- Propose a polynomial time computable algorithm that solves the minimum energy problem within a finite bound of the optimal solution.

4.2 Stochastic multi-relay routing

4.2.1 Motivation

Wireless medium is inherently error prone and highly dynamic in nature. This renders traditional uni-path routing inefficient for wireless communication. A naive approach to increase efficiency of wireless transmission is to use multi-path routing instead of unipath routing. For better understanding let us consider the network in Figure 3. Node s is the source, t is the destination and $r_1, r_2, ..., r_{10}$ are relay nodes. Let us also assume that the communication channels between the source s and the relay nodes are highly error prone (10% error rate). But, the communication channels from the relay nodes to the destination node are reliable with 100% packet delivery rate. Since, the packet drop rate for the channels between s and relay nodes is 10%, using traditional routing protocol, each packet is required to be transmitted on an average 10 times to ensure successful reception by the selected relay node. So, to transfer 10 packets from s to t successfully, on an average 100 transmissions by s are required. On the other hand, with multi-path routing protocol, where each packet is broadcasted to all its neighboring nodes, each packet transmitted by s is received by at-least one relay node with very high probability. So, a multi-path routing protocol can transfer 10 packets from s to t with 10 transmissions by s.

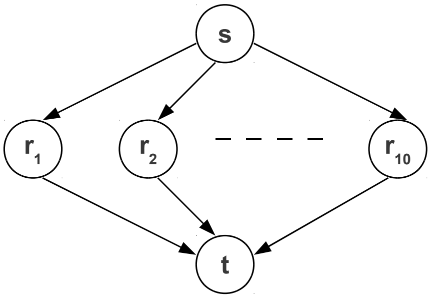

Figure 3: Each communication lines originating at s have error rate 10%, all the communication lines terminating at t have 0% error rate

But, without proper relay scheduling, multi-path routing can have negative impact. viz., in the network in fig3, let us consider that relay nodes r_1 and r_3 both receive a packet transmitted by s. After receiving, if both nodes r_1 and r_3 try to transmit a packet to t, there would be collision, which would eventually decrease the efficiency of the network.

4.2.2 Related work

Most of the wireless routing protocols [53–56] mimic wired counter parts. But, these protocols yield poor performance in many scenarios as they do not consider the highly dynamic nature of wireless medium. This has attracted several researches [57–61] to model wireless network as a stochastic process. Chen et. al. [57] have considered the problem of maximizing life time of a network where sensor nodes directly sends their collected data to the access point (AP). Authors have modeled the network as a stochastic Markov decision process to select sensors for data transmission. Li et. al. [58] have researched with 3 agent networks (1 transmitter, 1 relay and 1 destination). Every agent in the network is capable of communicating with each other with varying transmission power. Authors have proposed a solution to the minimum energy routing problem by modeling the wireless network as MDP and selecting a transmitter and receiver for each packet. Singh et. al. [60] have used MDP modeling to maximize the flow problem of wireless network. The work proposed in this article is very similar to the work done by Shirazi et.al. [59]. Authors [59] have worked with a network consists of several agents capable of communicating with a fixed transmission power. Since, the transmission power is fixed for all agents, the minimum energy transmission problem is derived to problem of finding minimum transmissions required to reach destination. Authors have modeled the network as a MDP and used dynamic programming to solve the minimum-hop problem for optimal result. Work proposed in this article differs in two ways. Firstly, in the current work, agents are capable of communicating with each other with multiple transmission power levels. Secondly, I wish to come up with the dynamic index (similar to "Gittins index") to solve the MDP for efficiency.
To complete our review of related work we briefly survey work done on "Gittins index". Gittins [62, 63] has proven the existance of an index, maximizing which yields the optimized solution to multi-armed bandit problem. Gittins have stated dynamic allocation index (DAI) theorem (similar to his original statement) in [64]. The DAI theorem states that, in a multi-armed bandit problem, if all the bandit processes are independent of each other and at a time only one bandit is selected, "Gittins index" yields optimal solutions. Original proof by Gittins have been followed by several other proofs [65–68] of the same theorem with more and more insight to the problem. Dimitriu et. al. [69] have derived a variation of "Gittins index" for finite horizon games.

4.2.3 Model

Wireless network is composed of N nodes. Time is divided into discrete slots. A node starts with an energy source with ξ_0 power. Every node is capable of transmitting at a power level selected from the set $W = \{w_1, w_2, \dots w_f\}$. We also assume that $w_1 < w_2 < \dots < w_f$. After each transmission, a node loses energy depending on the transmission power. Energy of a node i in t time-slot is represented by ξ_{it}. A node is said to be dead if residual energy of that node is less than minimum power required to reach its nearest neighbor. Every node has 3 modes of operation. A node is in **sleep** mode, if it does not have any message to transfer. In **active** mode, a node transmits a message to its neighbors. A node is in **stand-by** mode, when it has message to transfer, but it is not transmitting. Wireless channel between nodes are symmetrical. Bit error rate of the channel between nodes i and j is e_{ij}.

Stochastic model of network: Each node of the network corresponds to a Markov decision process (MDP). Let us consider that a node i corresponds to a MDP M_i. For simplicity, we say that a MDP M_i is in state s when the corresponding node i is in the same state.
State space: A state of MDP contains the residual energy of the node, the MDP belongs to. Moreover, every state of M_i contains the MDPs of neighbors of i.
Action space: The action space of a node i is $\Lambda(i) \in [0, f+1]$. When the node i is not selected for transmission, $\Lambda(i) = 0$. Otherwise, $\Lambda(i)$ is the index of power level for transmission.

4.2.4 Proposed Research

Gittins has shown that, dynamic allocation index ("Gittins index") yields optimal solution if each bandit process is independent of each other. Is it possible to find such index among several non-independent semi-markov processes potentially with more than 2 possible actions? If such index exists, then is it possible to propose a distributed protocol based on such index? On the other hand, if such index does not exist, I would propose heuristics computing routing protocols with energy requirement comparable to dynamic programming solution.

5 Plan

Oct, 2013	Proposal defense
Nov, 2013 - March, 2014	Work detailed in sections 3, 4 and 5
March, 2014 - April, 2014	Final thesis writing
May, 2014	Tentative defense data

References

[1] I. Maric, R. Yates, Efficient multihop broadcast for wideband systems, in: In DIMACS Workshop on Signal Processing for Wireless Transmission, American Mathematical Society, 2002.

[2] A. Banerjee, C. H. Foh, C. K. Yeo, B. S. Lee, Exploiting wireless broadcast advantage as a network-wide cache, in: Fourth IEEE International Workshop on Selected Topics in Mobile and Wireless Computing, IEEE, 2011, pp. 490–497.

[3] V. Raghunathan, C. Schurghers, S. Park, M. Srivastava., Energy-aware wireless microsensor networks., IEEE Signal Processing Magazine 19 (2) (2002) 40–50.

[4] G. Pottie, W. Kaiser, Wireless integrated network sensors., Communication of the ACM 43 (5) (2000) 51–58.

[5] Strangers helping strangers, `http://www.facebook.com/SHStrangers`.

[6] Yelp, `http://www.yelp.com/`.

[7] Facebook places, `http://www.facebook.com/facebookplaces`.

[8] Gowalla, `http://gowalla.com/`.

[9] Foursquare, `https://foursquare.com/`.

[10] Q. Huang, Y. Liu, On geo-social network services, Geoinformatics.

[11] A. Cooper, T. Hardie, Geopriv: creating building blocks for managing location privacy on the internet, IETF Journal.

[12] G. Myles, A. Friday, N. Davies, Preserving privacy in environments with location-based applications, Pervasive Computing, IEEE.

[13] H. Kido, Y. Yanagisawa, T. Satoh, An anonymous communication technique using dummies for location-based services, in: Proceedings of IEEE International Conference on Pervasive Service, 2005.

[14] A. R. Beresford, F. Stajano, Location privacy in pervasive computing, IEEE Pervasive Computing.

[15] K. P. Tang, P. Keyani, J. Fogarty, J. I. Hong, Putting people in their place: An anonymous and privacy-sensitive approach to collecting sensed data in location-based applications, in: Proceedings of the SIGCHI conference on Human Factors in Computing Systems, 2006.

[16] M. Gruteser, X. Liu, Protecting privacy in continuous location-tracking applications, IEEE security and privacy.

[17] M. Duckham, L. Kulik, A formal model of obfuscation and negotiation for location privacy, Pervasive.

[18] M. Gruteser, D. Grunwald, Anonymous usage of location-based services through spatial and temporal cloacking, in: Proceedings of the International Conference on MobiSys, 2003.

[19] B. Gedik, L. Liu, A customizable k-anonymity model for protecting location privacy, in: Proceeding of the International Conference on Distributed Computing Systems, 2005.

[20] M. F. Mokbel, C.-Y. Chow, W. G. Aref, The new casper: a privacy-aware location-based database server, IEEE 23rd International Conference on Data Engineering.

[21] J. I. Hong, J. A. Landay, An architecture for privacy-sensitive ubiquitous computing, in: Proceedings of the International Conference on Mobile Systems, 2004.

[22] S. Goldwasser, S. Micali, Probabilistic encryption & how to play mental poker keeping secret all partial information, in: Proceedings of the fourteenth annual ACM symposium on Theory of computing, STOC '82, ACM, 1982.

[23] T. Elgamal, A public key cryptosystem and a signature scheme based on discrete logarithms, Information Theory, IEEE Transactions on 31 (4) (1985) 469 – 472. doi:10.1109/TIT.1985.1057074.

[24] C. Gentry, Fully homomorphic encryption using ideal lattices, in: Proceedings of the 41st annual ACM symposium on Theory of computing, STOC '09, ACM, 2009.

[25] K. Lauter, M. Naehrig, V. Vaikuntanathan, Can homomorphic encryption be practical?, in: Proceedings of the 3rd ACM workshop on Cloud computing security workshop, CCSW '11, ACM, 2011.

[26] A. Samanta, F. Zhou, R. Sundaram, Samaritancloud: Secure and scalable infrastructure for enabling location-based services, in: Networking, IFIP, 2013.

[27] Spectrum management, `http://en.wikipedia.org/wiki/Spectrum_management`.

[28] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, S. Mohanty., Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey., COMPUTER NETWORKS JOURNAL 50 (2006) 2127 – 2159.

[29] Q. Zhao., A survey of dynamic spectrum access: signal processing, networking, and regulatory policy., IEEE Signal Processing Magazine (2007) 79–89.

[30] B. Bollobas, J. E. Littlewood., Littlewoods miscellany, Cambridge University Press.

[31] R. Isaacs, Differential Games., John Wiley and Sons, 1965.

[32] S. Alpern, S. Gal., The theory of search games and rendezvous., Springer.

[33] A. Pelc., Deterministic rendezvous in networks: A comprehensive survey., Networks 59 (3) (2012) 331–347, iSSN 0028-3045.

[34] H. Liu, Z. Lin, X. Chu, , Y.-W. Leung., Taxonomy and challenges of rendezvous algorithms in cognitive radio networks., in: Computing, Networking and Communications (ICNC), 2012, pp. 645–649.

[35] L. A. DaSilva, I. Guerreiro., Sequence-based rendezvous for dynamic spectrum access., in: IEEE DySPAN, 2008, pp. 1–7.

[36] H. Liu, Z. Lin, X. Chu, , Y.-W. Leung., Ring-walk based channel-hopping algo-rithms with guranteed rendezvous for congnitive radio networks., in: IEEE/ACM Intl Conference on Green Computing and Communications & Intl Conference on Cyber, Physical and Social Computing (GREENCOM-CPSCOM 10), IEEE, 2010, pp. 755–760.

[37] D. Yang, J. Shin, C. Kim., Deterministic rendezvous scheme in multichannel access networks, Electronics Letters.

[38] C. N. Theis, R. W. Thomas, L. A. DaSilva., Rendezvous for cognitive radios., IEEE Transactions on Mobile Computing.

[39] D. Yang, J. Shin, C. Kim., A channel rendezvous scheme for cognitive radio networks., Communication Letters 14 (10) (2010) 954–956.

[40] H. Liu, Z. Lin, X. Chu, , Y.-W. Leung., Jump-stay based channel-hopping algorithm with guaranteed rendezvous for cognitive radio networks., in: Proceedings of INFOCOM 2011, IEEE, 2011, pp. 2444–2452.

[41] Z. Gu, Q.-S. Hua, Y. Wang, F. Lau., Nearly optimal asynchronous blind rendezvous algorithm for cognitive radio networks., in: SECON, 2013.

[42] A. Kailas, M. ann Ingram, Alternating opportunistic large arrays in broadcasting for network lifetime extension., IEEE transactions on wireless communications 8 (6) (2009) 2831–2835.

[43] S. Sharma, Y. Shi, Y. T. Hou, H. D. Sherali, S. Kompella, S. F. Midkiff, Joint flow routing and relay node assignment in cooperative multi-hop networks, IEEE journal on selected areas in communications 30 (2) (2012) 254–262.

[44] T. Girici, G. D. Kurt, Minimum-outage broadcast in wireless networks with fading channels, IEEE communications letters 14 (7) (2010) 617–619.

[45] M. Agarwal, J. H. Cho, L. Gao, J. Wu, Energy efficient broadcast in wireless ad hoc networks with hitch-hikingks, in: Proceedings of IEEE INFOCOM, IEEE, 2004, pp. 2096–2107.

[46] Z. Yang, J. Liu, A. Host-Madsen, Cooperative routing and power allocation in ad-hoc networks., in: Proceedings of IEEE GLOBECOME, IEEE, 2005, pp. 2730–2734.

[47] B. Maham, A. Hjorungnes, Minimum power allocation for cooperative routing in multihop wireless networks, in: Proceedings of IEEE SARNOFF, IEEE, 2009, pp. 1–5.

[48] B. Sirkeci-Mergen, A. Scaglione, On the power efficiency of cooperative broadcast in dense wireless networks, IEEE journal on selected areas in communications 25 (2) (2007) 497–507.

[49] J. Si, Z. Li, Z. Liu, X. Chen, Energy efficient cooperative broadcasting in wireless networks, in: Proceedings of IEEE ICC, IEEE, 2009.

[50] M. Baghaie, B. Krishnamachari, Delay constrained minimum energy broadcast in cooperative wireless networks, in: Proceedings of IEEE INFOCOM, IEEE, 2011, pp. 864–872.

[51] J. Chen, L. Jia, X. Liu, G. Noubir, R. Sundaram, Minimum energy accumulative routing in wireless networks, in: Proceedings of IEEE INFOCOM, IEEE, 2005, pp. 1875–1886.

[52] M. Baghaie, D. S. Hochbaum, B. Krishnamachari, On hardness of multiflow transmission in delay constrained cooperative wireless networks, in: Proceedings of IEEE Globecom, IEEE, 2011.

[53] S. Murthy, J. Garcia-Luna-Aceves, An efficient routing protocol for wireless networks, Journal of mobile networks and applications 1 (2) (1996) 183–197.

[54] C. Perkins, P. Bhagwat, Highly dynamic destination sequenced distance-vector routing (dsdv) for mobile computers, in: SIGCOMM, ACM, 1994, pp. 234–244.

[55] C. E. Perkins, E. M. Royer, Ad-hoc on-demand distance vector routing, in: IEEE WMCA, IEEE, 1999, pp. 90–100.

[56] D. B. Johnson, D. A. Maltz, Dynamic source routing in ad hoc wireless networks, in: Mobile Computing, Kluwer Academic Publishers, 1996, pp. 153–181.

[57] Y. Chen, Q. Zhao, V. Krishnamurthy, D. Djonin, Transmission scheduling for optimizing sensor network lifetime: A stochastic shortest path approach, IEEE transaction on signal processing 55 (5) (2007) 2294–2309.

[58] H. Li, N. Jaggi, B. Sikdar, Relay scheduling for cooperative communications in sensor networks with energy harvesting, IEEE transaction on wireless communications 10 (9) (2011) 2918–2928.

[59] G. N. Shirazi, P.-Y. Kong, , C.-K. Tham, Markov decision process frameworks for cooperative retransmission in wireless networks, in: Proceedings of IEEE WCNC, IEEE, 2009.

[60] J. P. Singh, T. Alpcan, P. Agrawal, , V. Sharma, A markov decision process based flow assignment framework for heterogeneous network access, Wireless networks 16 (2010) 481–495.

[61] E. Altman, Applications of markov decision processes in communication networks: a survey, in: in Markov Decision Processes, Models, Methods, Directions, and Open Problems, E. Feinberg and A. Shwartz (Editors) Kluwer, 2001, pp. 488–536.

[62] J. C. Gittins, D. M. Jones, A dynamic allocation index for the design experiments, Progress in statistics 9.

[63] J. C. Gittins, Multi-armed bandit allocation indices, Wiley, 1989.

[64] J. C. Gittins, Bandit processes and dynamic allocation indices, Journal of the Royal Statistical Society. 41 (2) (1979) 148–177.

[65] P. Varaiya, J. Walrand, C. Buyukkoc, Extensions of the multi-armed bandit problem: The discounted case, IEEE transactions on automatic control (1985) 426–439.

[66] J. Walrand, An introduction to queueing networks, Prentice-Hall, 1988.

[67] R. Weber, On the gittins index for multiarmed bandits, The annals of applied probability 2 (1992) 1024–1033.

[68] P. Whittle, Multi-armed bandits and the gittins index, Journal of the Royal Statistical Society. 42 (1980) 143–149.

[69] P. W. Iona Dimitriu, Prasad Tetali, On playing golf with two balls, Journal of discrete mathematics 16 (4) (2003) 604–615.