IMPLICIT COORDINATION TECHNIQUES FOR WIRELESS COMMUNICATIONS

BY SANGHO OH

A dissertation submitted to the

Graduate School—New Brunswick

Rutgers, The State University of New Jersey

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

Graduate Program in Electrical and Computer Engineering

Written under the direction of

Prof. Marco Gruteser

and approved by

New Brunswick, New Jersey

May, 2012

ABSTRACT OF THE DISSERTATION

Implicit Coordination Techniques for Wireless Communications

by Sangho Oh
Dissertation Director: Prof. Marco Gruteser

In distributed networks with a large number of network nodes, direct coordination of communication nodes for performance optimization is an inefficient and difficult task that demands global knowledge of the network status. Hence, implicit coordination techniques, that indirectly infer the network status from the delay and loss of the packets that are received, transmitted, or overheard, have been developed for network performance improvement. Implicit coordination can be accomplished while preserving the valuable network bandwidth resource that can be easily exhausted during the coordination processes. Well-designed implicit coordination techniques, such as TCP in IP protocols or CSMA in 802.11 systems, can make the communication system more efficient and reliable by eliminating or reducing overheads and latency for coordination.

In this paper, implicit coordination techniques are designed and implemented for a number of practical cooperative communication protocols in wireless networks. Firstly, an implicit coordination technique is applied for vehicular networks where adaptability and scalability are major concerns owing to dynamically varying network conditions. For efficient and reliable dissemination of life-safety messages, packet relay nodes are implicitly coordinated for their cooperative relay of the packets received. Next, a joint power control and scheduling problem is discussed in wireless peer-to-peer to networks. Implicit coordination technique is applied to solve complicated resource allocation problems. The resulting coordination algorithm is fully distributed and improves both throughput efficiency and user fairness to the network, relying only on the local information of individual nodes. Lastly, implicit coordination techniques are used to protect the location privacy of the wireless nodes that are collaborating for their location privacy. Two novel cooperative location privacy protection methods, Location Cloaking and Location Cloning, are designed in the communication physical layer. Then, implicit coordination techniques are applied to protect the location privacy of cooperator nodes whose location information may be threatened while they are cooperating with another node. Implicit coordination also minimizes the risks caused from extra packet transmissions during cooperative operations.

Table of Contents

Abstract ii

List of Tables v

List of Figures vi

1. Introduction 1

1.1. Outline of the paper 3

2. Implicit Coordination for Reliable Routing 5

2.1. Introduction 5

2.1.1. Related Work 7

2.2. Background 8

2.3. Zero-Coordination Opportunistic Routing (ZCOR) Algorithm 13

2.3.1. Slot Reservations for LSM 15

2.3.2. Opportunistic Relayer (Relay Node) Selection 17

2.3.3. Implicitly Coordinated Opportunistic Multi-hop LSM Relay 18

2.3.4. The Size and Location of CoT 20

2.3.5. Multi-CoT Against Spatially-correlated Shadowing Effects 23

2.4. Performance Evaluation 25

2.4.1. Baseline Message Dissemination Protocols 26

CFG (Controlled Flooding-based Geocast) 26

MRG (Multicast Relay-based Geocast) 26

2.4.2. VANET Simulation Model 27

2.4.3. NS-2 Parameters and Evaluation Metrics 29

2.5. Result 30

2.5.1. Reliability and Overhead Comparison 30
2.5.2. The Performance of ZCOR in VANET Conditions 32
2.5.3. The Performance of Multi-CoT Against Shadow Fading 34
2.6. Conclusion 35

3. Implicit Coordination for Resource Allocation 38
3.1. Introduction 38
3.1.1. Related Work 39
3.2. System Model and Problem 41
3.2.1. Implicitly Coordinated Transmission Power Control 43
3.3. Joint Power Control and Scheduling Algorithm 44
3.3.1. Power control with a staircase utility function 45
3.3.2. Joint power control and scheduling 47
3.4. Simulation Result 49
3.4.1. Power control only versus Scheduling only 50
3.4.2. Performance of JPSA: Comparison with fair scheduling algorithm . . . 51
3.4.3. Performance of JPSA: Comparison with optimal scheduling algorithm . 52
3.5. Conclusions 53

4. Implicit Coordination for Cooperative Location Privacy Protection 55
4.1. Introduction 55
4.1.1. Related Work 57
4.2. Cooperative Cloaking: Jamming for Location Privacy Protection 59
4.2.1. The Positive Role of Jamming in Location Privacy 59
4.2.2. Single- and Multi-node Jamming 61
4.2.3. Multi Cooperator Power Control (*MCPC*) Jamming for Location Privacy 62
4.2.4. Performance of Multi-node Implicitly Coordinated Jamming Method . 65
4.3. *Phantom* : Location Cloning for PHY-Location Privacy Protection System . . 68
4.3.1. Location Privacy Protection through Ghosts Creation 69
4.3.2. Advanced adversary models 71

4.3.3. Implicit Coordination for Packet Synchronization 72

4.3.4. Implementation Using GNU Radios 74

Experiment Setup 75

Time and Frequency Synchronization 76

Effect of Synchronized Transmissions 78

4.3.5. Performance Evaluation on Indoor Test-bed 78

Power combinations for a cluster of ghosts 79

4.3.6. Privacy performance over various adversary locations 80

Adversary using scene analysis technique 80

Adversary using spectrum analysis tools 83

4.4. Conclusion 83

5. Conclusion 85

Appendix A. Location Privacy Measure using CRLB 86

References 91

List of Tables

2.1. Event-driven Life Safety Messages (LSM) : NHTSA & VSCC (USDOT 2006) 9

2.2. Protocol Parameter 36

2.3. Simulation Parameter 37

3.1. 802.11a radio reception thresholds: Receiver performance requirements ($PER = 10^{-3}$) 49

4.1. Simulation Parameters. 76

A.1. Simulation Parameters. 89

List of Figures

2.1. Three classes LSMs categorized into three classes. 10

2.2. VANET key attributes. 12

2.3. The overview of ZCOR in multi-hop LSM dissemination; $P_i^{(j)}$ is jth hop LSM packet with a sequence number i. 14

2.4. Transmission slot reservation in each class of LSMs ($L = 5$); MTMF geocast has 2-hop range ($h = 2$). 15

2.5. LSM relayer j selects a next-hop relayer based on its neighbor knowledge collected from heartbeat packets. 18

2.6. Implicitly coordinated opportunistic LSM relay. 19

2.7. Two-hop LSM relay scenario for the analysis and simulation of the implicit coordination method. 21

2.8. LSM relay rate in two-hop scenario. 23

2.9. Multi-CoT to cope with spatially-correlated shadow fading effects. 24

2.10. VANET simulation channel models and scenarios. 28

2.11. Reliability and overhead under various vehicle density conditions. 31

2.12. The reliability of MTMF and HTLF LSMs under various VANET conditions; vehicle density is 55 [vehicle/coverage]. 33

2.13. Gains from multi-CoT against shadow fading; vehicle density is 55 [vehicle/coverage]. 34

3.1. Peer-to-peer communications model (Unicast mode) 41

3.2. Staircase Utility function 43

3.3. Target SINR: Calculate utility and set the target SINR based the staircase utility function 46

3.4. Joint power control and scheduling algorithm 48

3.5. Distance and data rate: Maximum communication range is set as $200\mathrm{m}$ with maximum transmission power set as $\bar{p_i} = 18\mathrm{dBm}$ 50

3.6. Example topology: Five links 51

3.7. Power control with a rate adaptation 52

3.8. Performance comparison with Time division access (TDMA) : 5 Links topology 52

3.9. Performance comparison with an optimal scheduling algorithm: 5 Links topology 53

3.10. Performance comparison with a fair channel scheduling algorithm (TDMA): 5 Links topology 54

4.1. Cooperative jamming for location privacy protection 60

4.2. Example of cooperative jamming scenario; path-loss exponent:$\eta = 3$, Receiver noise floor:$N = -101\mathrm{dBm}$, Bandwidth:$f_b = 10\mathrm{MHz}$. 62

4.3. NUM-based distributed jamming power control method; $p_{TX} = 20\mathrm{dBm}$, $\alpha = 0.25$, Ricean fading. 63

4.4. Privacy performance measured by complementary cumulative distribution function; Jamming power for *SCFP* and *MCFP* are fixed as $9\mathrm{dBm}$ and $6\mathrm{dBm}$. . . . 66

4.5. Adversary localization systems tracking users. 69

4.6. Adversary localization system tracking ghost instead of real users. 70

4.7. Implicitly coordinated dummy packet transmissions 73

4.8. Synchronization test on GNURadios. 76

4.9. Time and frequency synchronization test using GNU Radios. 77

4.10. Demodulation of the synchronized packets. 78

4.11. Privacy performance in the experiment test-bed 81

4.12. Advanced adversaries using scene analysis technique 82

4.13. Advanced adversaries using spectrum analysis tools 84

A.1. Transmitter (TX), receiver (RX) and adversary sensors ($\boldsymbol{s}$). 86

Chapter 1

Introduction

The evolution of wireless technology provides a broadband and reliable connectivity to mobile users. High resolution video streaming applications and rapidly growing mobile computing network environments, however, are demanding high bit-rate services over large coverage areas for seamless support of mobile users. To fulfill such demands, the concepts of wireless mesh networks [1,2,3] and cooperative communication techniques [4] are actively researched to build more efficient and reliable wireless networks.

Cooperative communications in wireless systems, which exploit diversity gains from multiple radios, have advantages of efficiency and reliability in network protocols. However, cooperative communications presumes the coordination of nodes, which induces protocol overheads for coordination among the network entities in the network. For example, wireless nodes need to keep exchanging their status information for a proper coordination with other nodes to avoid collisions among them. Unless their status information is precisely updated, the gains from cooperation may significantly degrade. In such a case, the overhead from status information exchange should be carefully considered along with the efficiency and reliability of the protocol. On the other hand, the overhead in coordination also affects the privacy of wireless users. This is because the more wireless device transmit signals there are, the easier it is for malicious eavesdroppers to trace the user locations.

In this research, we design a number of wireless protocols based on implicit coordination techniques, which further enhances the efficiency of the existing networking protocols. Firstly, we highlight the benefits from implicit coordination techniques for various applications in Ad-Hoc networks where a central coordinator does not exist. Secondly, we review the difficulties in designing reliable protocols based on implicit coordination techniques when networks are dynamic and then we suggest a solution for reliable coordination among node, which restricts the rage of implicit coordination. Thirdly, we show how implicit coordination technique can be applied in solving very complicated distributed network coordination problems. Optimal resource allocation problems are known to be an NP complete problem in Ad-Hoc networks [5, 6, 7, 8]; however, we show that by applying dual-primal decomposition methods, the network utility maximization problem can be solved by a distributed algorithm employing an implicit coordination technique. Lastly, we propose a novel cooperative location privacy protection mechanism for mobile wireless users, which exploits implicit coordination of peer nodes.

We provide an overview of implicit coordination techniques, and then we provide the outline of the paper introducing each chapter, whereupon we discuss implicit coordination techniques for various objectives of the protocols in wireless networking. In wireless communications, protocols and network functions are defined to achieve more efficient and reliable networks. Although cooperative communication improves efficiency and overall network performances through the coordination among the network entities, such cooperation demands each node to update the status information of other network entities connected directly or indirectly to. Examples of such status information are locations, connectivity, hierarchical network structure, available resources, channel status, congestion status [9, 10].

Typical communication protocols rely on explicit coordination to exchange status information among network entities and to control their functions. In most cellular networks, base stations centrally coordinate mobile nodes associated with them using a globally collected knowledge through explicit coordination message exchanges. For example, in Time Division Multiple Access (TDMA) type radio systems, medium access is centrally coordinated by the base stations using explicit control messages. In some cases, the overhead for coordination may not be trivial, hence the overhead induced for coordination should be properly managed in order not to degrade the network performance too much.

In decentralized systems, such as Ad-Hoc network systems and IP networks where centralized coordinators are not available, implicit coordination techniques are already widely used. One good example is Carrier Sensing Multiple Access/Collision Avoidance (CSMA/CA) in Wi-Fi networks [11], which exploits random access delay to avoid collision among nodes. Using CSMA/CA protocol, each node adjusts its contention window size depending on the congestion status of the network that is implicitly inferred from the timeout of acknowledgement packet [12, 13]. TCP congestion control [14] is another good example that handles network congestion problems through an indirect rate control mechanism using congestion windows in both transmitter and receiver nodes. The network congestion status is inferred (i.e., implicitly measured) from the latency and packets losses of packets [15].

The property of wireless protocol that is properly designed for implicit coordination can be summarized as follows

- Locality: Since the nodes are coordinated based on their local information, the protocol functions can coordinated in a distributed way
- Efficiency: Low overhead from the elimination or reduction of coordinating messages
- Adaptivity: The protocol is more scalable over the variety of network conditions such as node density and network congestions
- Robustness: Since nodes are relying on local information, they can quickly adapt to the dynamic environmental changes networks

1.1 Outline of the paper

In this research, implicit coordination techniques are applied for various applications in wireless communications. In chapter 2, the *Zero-Coordination Opportunistic Routing (ZCOR)* algorithm is proposed for rapid and reliable road-emergency message disseminations in vehicular networks. Disseminating mission-critical life safety-messages reliably over multi-hop geocast areas is a very difficult task in dynamic and capacity limited vehicular networks. Without a coordinator, vehicular networks need a self-organizing architecture; moreover, nodes in the network are cooperating for reliable message dissemination over large geocast areas. Hence, solving the difficulties of coordination among nodes and of overhead control are key issues owing to the band-limited control channel in vehicular networks. By employing implicit coordination techniques, we solve the overhead and latency problems that are typically raised in such conditions. We also review the problems in implicit coordination techniques that are raised by imperfect state estimation due to the channel and topology dynamics. Then we provide a solution improving the coordination reliability by restricting the range of status information exchange.

In chapter 3, we apply implicit coordination technique for optimal resource allocation in Ad-Hoc networks. Network optimization using network utility maximization methods typically improves network throughput efficiency; however, they easily lose the balance for user fairness. By jointly considering time scheduling with power control, we can improve both efficiency and fairness. In this research, we propose a novel *Joint Power control and Scheduling Algorithm (JPSA)* to enhance network throughput without sacrificing fairness among users. We show that implicit coordination techniques can be applied to solve such complicated network utility maximization problems by introducing primal-dual decomposition methods. The resulting coordination algorithm is fully distributed and improves both throughput efficiency and user fairness of the network in a distributed way relying only on the local information of individual nodes. Our proposed *JPSA* also significantly alleviates the latency and overhead in coordinating nodes by employing an implicit coordination technique, which infers the local interference level from Received Signal Strength to Noise-Interference (RSSI) level.

In chapter 4, we discuss implicit coordination techniques in the context of location privacy. Wireless users are vulnerable to attacks from adversaries using various passive localization techniques. Adversaries can easily infer the location of wireless users by measuring Time Of Arrival (TOA) or Received Signal Strength (RSS) [16, 17, 18] from the user transmitted signals at the physical layer. Although such passive and indirect localization mechanisms are easy to implement, techniques securing location information at the physical layer of the wireless communication systems has not yet been actively studied. Such lack of an efficient location protection scheme at the physical layer that works seamlessly with commercial wireless infrastructure has motivated our two novel techniques of *Location Cloaking* and *Location Cloning*, in which wireless nodes cooperate to obfuscate user transmission signal preventing adversaries from precisely locate them. However, such cooperative location privacy protection methods can risk the location privacy of cooperative nodes [19]. Hence, we employ an implicit coordination technique to minimize the privacy risk of cooperator nodes from the threat of adversaries.

Chapter 2

Implicit Coordination for Reliable Routing

2.1 Introduction

Communications between Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) have been extensively studied during the last decade to guarantee human safety and road-network efficiency. The avoidance of accidents by disseminating safety messages at intersections or highways is considered as a basic element for safety-related applications in Vehicular Ad-hoc NETworks (VANETs). Therefore, issues on the reliability and latency in disseminating safety messages over VANET environments have been thoroughly investigated by many research projects [20, 21, 22, 23, 24, 25, 26].

Most research work to enable emergency applications such as pre-crash warning relies on single-hop broadcasts of critical Life Safety Messages (LSM). Such single-hop message broadcasting, however, does not always achieve the necessary coverage for various safety applications [27]. Consider, for example, low visibility conditions on wet/icy roads and overtaking-assist applications. If it were possible to track or query the positions and speeds of the vehicles ahead, the drivers could be informed of whether or not it would be safe to pass. In such cases, the geocast range of LSMs should be extended from several hundred meters up to a kilometer depending on vehicle speed. However, even with the boosted signal strength that is allowed by current Wireless Access in Vehicular Environments (WAVE) standards [20], the necessary transmission ranges cannot be reliably obtained through single-hop communications. In urban areas, some experimental measurements data indicate a maximum range of $100 - 150\,\mathrm{m}$ even with 33 dBm boosted transmission power [28]. Furthermore, the range is further reduced when transmission power is lowered to improve spectrum spatial reuse.

In addition, there are a number of technical challenges to consider in designing protocols for emergency applications. Adaptation to VANET specific network environments, such as high mobility, severe channel fading, and a wide range of vehicle density, including extremely high node-density owing to rush-hour traffic in metropolitan areas, are another important aspects to consider. Typically, congested common Control CHannel (CCH) is another problem to solve. In accordance with current standards, every wireless node in VANET shares a single CCH for the exchange of various safety-related messages [29]. Therefore, this bandwidth-limited CCH is easily congested as node density grows. Although rebroadcast-suppression and message-aggregation methods are able to alleviate such congestion problems [30], these approaches come with other undesirable drawbacks, such as the loss of reliability owing to the reduced number of rebroadcasts and the latency and security problems that arise when messages are aggregated.

In this chapter, we propose a Zero-Coordination Opportunistic Routing (ZCOR) algorithm for VANET that aims to deliver latency-sensitive LSMs over a broader target warning area efficiently and reliably. The ZCOR algorithm exploits implicit coordination techniques in coordinating a number of possible relay nodes with minimum overhead for conflict-free coordination. Also by implicitly reserving slot time, latency-bounded transmissions for LSM packets is achieved. Moreover, the reserved slots are not tied to a particular node; instead, they utilize opportunism in relaying packets via multi-node diversity. The coordination problem for opportunistic routing under dynamic and unstable vehicular channel conditions is solved by the novel concept of *Circle of Trust (CoT)*. The CoT is defined as the range of reliable communication needed to build accurate neighbor knowledge, which is subsequently used to determine the next relay node. Hence, ZCOR does not rely on a time-consuming pre-coordination process nor on extra overhead except for low-rate heartbeat packets.

The remainder of this chapter is organized as follows. In Section 2.2, we identify the characteristics of VANET. In Section 2.1.1, we review the existing protocols for life safety message dissemination. In Section 2.3, we present the details of the ZCOR algorithm. Simulation setups and scenarios are explained in Section 2.4 with simulation results following in Section 2.5. Finally, conclusions are drawn in Section 2.6.

2.1.1 Related Work

Existing prior works on safety message disseminations in VANET can be largely categorized as flooding-based protocols or as relay-based protocols [31]. In flooding-based broadcast protocols, the decision for packet forwarding relies on individual nodes. Each node makes a decision based on its own conditions such as location, distance, Random Access Delay (RAD) timer, neighbor knowledge, or combinations of them [26, 32, 33, 34]. Depending on the decision metric, overheads from rebroadcasting and reliability are determined. Flooding-based protocols are more suitable for short-range LSM dissemination; however, they usually produce larger overheads, which induce latency problems in dense network conditions due to contentions and collisions.

Compared to distributed flooding-based protocols, in relay-based protocols, the decision for packet relay is not distributed to receiver nodes, but given to sender nodes that relay packets [35, 25, 36, 37]. Packet forwarders use their neighbor knowledge and select a reliable and efficient next hop relay node. These protocols usually produce less redundancy than flooding-based protocols, but they are vulnerable to channel errors and node mobility, especially in sparse network conditions [38].

Many broadcast and geocast protocols use RAD timers to control rebroadcast redundancies, which are primarily built on a contention based CSMA MAC protocol. This randomness in channel access and packet routing induces not only delays but also collisions in dense network conditions [39, 40]. Therefore, a few reservation-based channel access protocols, such as Reservation-ALOHA (R-ALOHA) and Location Division Multiple Access (LDMA), have been proposed for VANET environments [41, 42, 43, 44]. R-ALOHA is robust over packet collisions through a channel reservation process [45, 46, 47, 48, 49]. However, they are mainly designed for single-hop broadcasts; therefore, reserving conflict-free slots for multi-hop delivery still remains an extremely difficult task in VANETs. LDMA was introduced for multi-hop bounded latency alerting [44], however, it still relies on out-of-band control channel for slot scheduling.

Under fading channel conditions, opportunistic routing algorithms can increase robustness and efficiency in multi-hop packet broadcasting scenarios by exploiting spatial diversity gains [50, 51]. Hence, opportunistic routing mechanisms have been applied to VANET in [52, 40], which are still relying on RAD-based timers. Recently, a time-space opportunistic routing algorithm has been proposed using a binary signaling technique to coordinate the candidates for relay nodes. However, such one-bit signaling technique is not appropriate for packet based communication systems. On the contrary, ZCOR does not require extra message exchange besides regular heartbeat packets for node coordinations in multi-hop packet relay, which can significantly reduce latency and overhead in LSM dissemination.

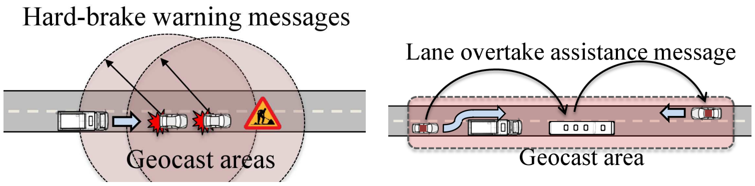
2.2 Background

Road safety messages in VANET can be classified into latency-tolerant Public Safety Messages (PSM) and latency-sensitive Life Safety Messages (LSM) [27]. PSMs are periodic advisory messages with less stringent requirements on their range and delivery latency. Examples of PSMs are neighbor finding heartbeats, GPS correction messages, service announcements, lane coordination, visibility enhancements, and Cooperative Adaptive Cruise Control (CACC) messages [53].

Table 2.1: Event-driven Life Safety Messages (LSM) : NHTSA & VSCC (USDOT 2006)

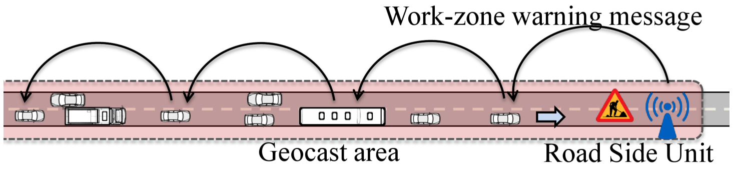
Class	**Latency**	**Frequency**	**Range**	**Application**	**Transmitter**
Low laTency High Frequency (**LTHF**)	$\leq 100\,\mathrm{ms}$	$10 - 20\,\mathrm{pkt/s}$	$\leq 150\,\mathrm{m}$	Pre-crash warning, post-crash warning, rollover warning, hard-brake and control loss warning, cooperative collision warning	Vehicle
Medium laTency Medium Frequency (**MTMF**)	$\leq 200\,\mathrm{ms}$	$5 - 10\,\mathrm{pkt/s}$	$\leq 100 - 300\,\mathrm{m}$	Curve speed assistance, stop light assistance, intersection collision warning, traffic signal violation warning	RSU (Road Side Unit)
				Left turn assistance, lane overtake assistance, extended brake signaling	Vehicle
High laTench Low Frequency (**HTLF**)	$\leq 1000\,\mathrm{ms}$	$1 - 2\,\mathrm{pkt/s}$	$\leq 1000\,\mathrm{m}$	Work-zone warning, low bridge warning, road condition warning	RSU (Road Side Unit)
				Emergency vehicle signal preemption	Vehicle

On the other hand, LSMs typically have higher priority than PSMs, as LSMs are generated for human-safety applications. In Table 2.1, we list and characterize the VANET applications that rely on LSMs, and subsequently categorize them into three subclasses according to their latency requirements, transmission frequencies, and ranges. As further illustrated in Fig. 2.1, Low laTency High Frequency (LTHF) LSMs convey time-critical messages, which have short-range geocast area that can be covered by single-hop transmissions. However, HTLF LSMs are not strictly sensitive to delay targeting vehicles in longer geocast ranges up to $1-2$ km. When compared to HTLF, MTMF LSMs have a medium latency requirement of several hundreds of milliseconds for the vehicles $2-3$ hops away from the LSM source. Particularly, the messages from the latter two categories require multi-hop dissemination to achieve their desired ranges.



(a) Low laTtency High Frequency (LTHF) LSM.

(b) Medium laTtency Medium Frequency (MTMF) LSM.



(c) High laTtency Low Frequency (HTLF) LSM.

Figure 2.1: Three classes LSMs categorized into three classes.

In this chapter, we focus on reliably disseminating latency-sensitive LSMs in the presence of background traffic packets (including PSMs) that share the same CCH. We assume that the destination of LSM is geographically defined and that their transmissions are directed along a roadway. However, reliable LSM dissemination is particularly challenging owing to a number of VANET attributes depicted in Fig. 2.2(a), that are summarized as follows:

Channel Dynamics: Similar to most mobile wireless communication channels, the vehicular communication channel suffers from reflections and signal scattering, which degrade signal strength and quality. Also, vehicular mobility adds more dynamic fading conditions combined with spatially correlated shadow fading effects. In urban areas, the correlation distance of the shadowing, caused by buildings and large vehicles, has been experimentally measured as $20\,\mathrm{m}$ [54]. In addition, strong ground reflections also produce deeply faded outage-areas between transmitters and receivers [55]. Such spatially and temporally correlated channels significantly affect the performance of wireless communications when their scale is larger than small scale fading and antenna diversity techniques are not helpful. Therefore, retransmission techniques assuring packet delivery combined with ACK (or NAK) feedback messages are widely used, although they induce more overhead and delay.

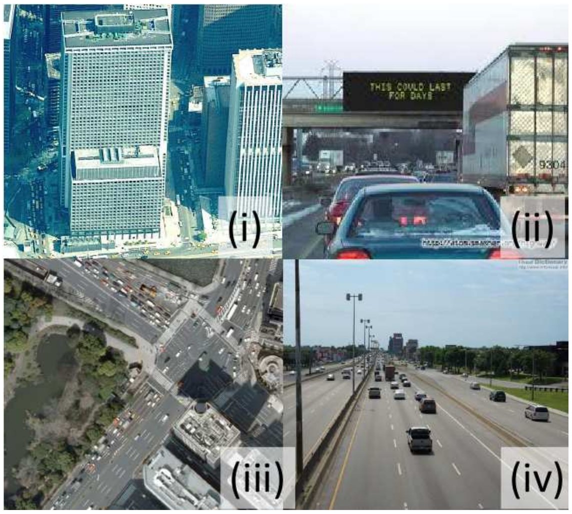
Mobility Dynamics: Although the mobility of vehicles is constrained by roadways, their velocity, density, and direction change dynamically over time and space. For example, a sparse road segment with a few fast running vehicles can be suddenly overcrowded with more vehicles. In such dynamically varying networks, LSM dissemination algorithms should be adaptive and scalable enough to cope with such abrupt changes of network conditions [39]. In addition, under such dynamic network conditions, nodes cannot obtain accurate neighbor knowledge. In VANETs, vehicles transmit low-rate periodic heartbeat packets to broadcast their positions and movement information for basic neighborhood discovery, which are widely used for various VANET applications designed to improve the efficiency, safety, and comfort of road traffic [58]. However, the rapidly changing topology of VANETs easily renders neighbor knowledge obsolete, which may degrade the performance of LSM dissemination protocols utilizing the neighbor knowledge in controlling the size of rebroadcast overhead [35, 36, 59].

Limited Control Channel Resource: The channel structure of current WAVE standards is shown in Fig. 2.2(b). Since conventional radios only allow one channel access at a time, nodes have to be synchronized to a Synchronization Interval (SI)[1] to make time-multiplex access between the Service CHannel (SCH) and the Control CHannel (CCH) [30]. Since CCH is shared by all the wireless nodes in VANETs and is used for most safety related message transmissions (including both LSMs and PSMs), the channel is easily congested in dense traffic areas[2]. Such

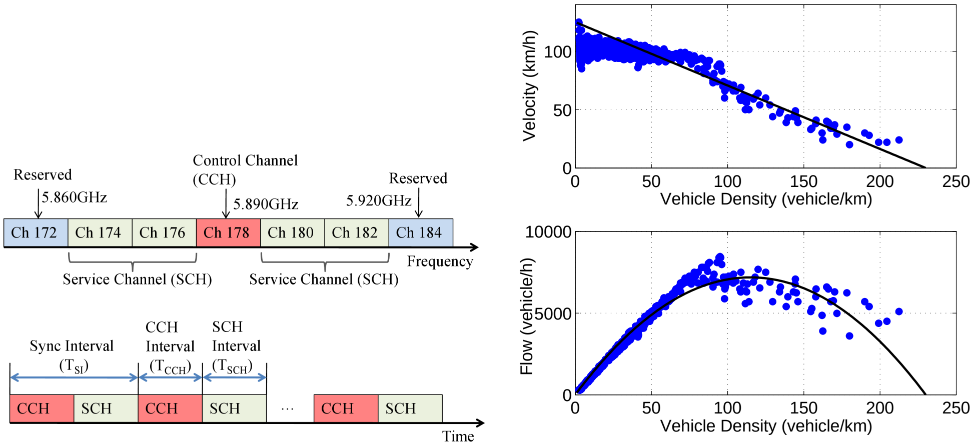
---

[1] Using GPS with pulse-per-second signals (available under ten dollars) is one of the cheapest methods to synchronize nodes

[2] Note that the vehicle density easily grows to hundreds of vehicles per one-hop communication range in rush-hour traffic, and CCH typically uses the lowest data rate for reliable packet delivery (i.e., $3\,\mathrm{Mb/s}$ in WAVE). For example, 200 vehicles would need $1.6\,\mathrm{Mb/s}$ bandwidth just for $100\,\mathrm{B}$ heartbeat packets with $10\,\mathrm{pkt/s}$ heartbeat rate, which already exceeds the CCH capacity (assuming CCH uses 50% of slots in SI).



(a) VANET key attributes: (i) Shadowing due to roadside buildings. (ii) Shadowing due to on road vehicles. (iii) Dynamic mobility changes in an intersection. (iv) Velocity-density correlation of vehicles.



(b) Multi-channel structure in WAVE standards.

(c) Vehicle flow model: Greenshield linear traffic model [56], which is one of widely used microscopic traffic models, is compared with sample traffic flow data collected in I-4 Orlando, Florida [57].

Figure 2.2: VANET key attributes.

CCH congestion easily degrades the performance of LSM dissemination protocols. Particularly, although background packets, such as heartbeats and other PSMs, are treated with lower priority [60], background packets can still interfere with LSM transmissions inducing collisions and channel access delays.

Difficulties in Adaptation: The design of LSM dissemination protocols in VANET should consider the peak amount of heartbeat transmissions in relation to the accuracy of neighbor knowledge, which varies depending on road traffic conditions. However, vehicle density is strongly correlated with vehicle velocity as shown in Fig. 2.2(c). Vehicles in VANET typically adjust their heartbeat transmission rate or power according to their velocity to alleviate the congestion in CCH from heartbeat packets [61, 62]. In such a case, traffic flow, that is vehicle density multiplied by vehicle velocity, equals the required bandwidth for heartbeat packets; since vehicle velocity is proportional to the heartbeat transmission rate. It is notable that nodes in VANET still experience CCH congestion at particular density conditions even when vehicles try to adapt their heartbeat transmission rate according to its velocity. Since such dynamic heartbeat transmission rate control incurs a drawback of inaccurate neighbor knowledge collection for the nodes, it is very difficult to design an adaptive algorithm incorporating all the different aspects of VANET conditions.

2.3 Zero-Coordination Opportunistic Routing (ZCOR) Algorithm

In this chapter, we propose Zero-Coordination Opportunistic Routing (ZCOR) algorithm for efficient and reliable LSM dissemination along a linear application-determined geocast zone. ZCOR follows the multi-channel structure of the WAVE standards. Although WAVE standards are currently based on CSMA-based MAC protocols, ZCOR can be seamlessly integrated with WAVE standards since it allows non-LSM packet transmissions as low-priority messages transmitted in the same CCH. However, to avoid collisions between high-priority ZCOR packets and low-priority non-LSM (background) packets, the backoff windows for channel access are exclusively assigned to each priority type.

To reduce collisions among the packets transmitted and to improve scalability over a wider range of vehicle densities, ZCOR relies on a slot reservation mechanism. Specifically, ZCOR employs an R-ALOHA style channel reservation method; where a slot reserved by one of LSM source nodes remains reserved until they are idle again. Differently from R-ALOHA, however, as shown in Fig. 2.3, the reservation of slots is spatially extended over multi-hop.

To implement such reservation based MAC access, ZCOR needs just a few microseconds level time synchronization assuming 8 μs of backoff access-slot size is applied. Such microseconds level synchronization can be easily achieved either by using Network Time Protocol (NTP) disciplined clocks from RSU beacons [63] or by using commodity GPS modules.[3] Assuming the scenarios that RSUs are not widely deployed, vehicles located outside of RSU's beacon range need to rely on GPS PPS signal to synchronize their internal clocks in order to prevent the clocks from drifting. ZCOR radio modules, which are directly fed with GPS PPS signals, can lock their internal clocks to the PPS reference clocks to control their packet transmission properly. Also, such time critical tasks are needed to be implemented in firmware/hardware level in radio transceivers to minimize the latency and jitters across network protocol layers.

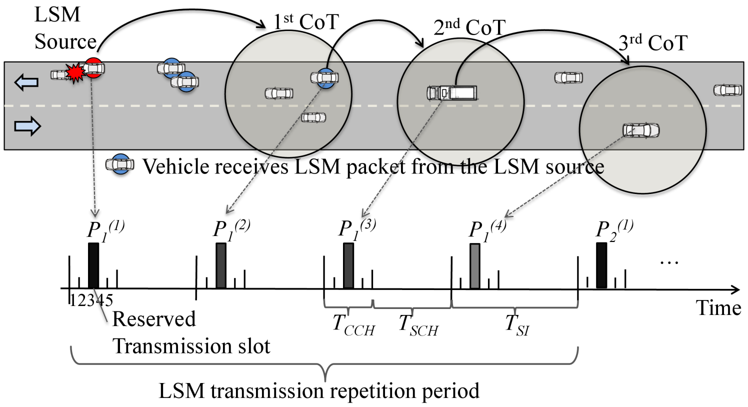


Figure 2.3: The overview of ZCOR in multi-hop LSM dissemination; $P_i^{(j)}$ is jth hop LSM packet with a sequence number i.

For reliable multi-hop LSM dissemination under dynamic vehicular mobility and fading channels, ZCOR exploits multi-node diversity in receiving and relaying packets. Every packet includes coordination information for the next relayers, denoting the next-hop relay nodes. Each relayer designates an area (rather than a node) for implicit coordination, which is called

---

[3] We experimentally measured the time offsets in PPS signals from a number of Garmin GPS 18x devices [64]. Their time precisions are within $500ns$, which can be further reduced when GPS modules are integrated with radio transceiver circuits with less expensive implementation cost.

Circle-of-Trust (CoT), to enable opportunistic relay to exploit multi-node reception diversity in packet receptions in each hop. However, the coordination is implicitly made without coordination-overhead besides beacon-type heartbeat packets that are considered as a basic protocol element in VANETs. The efficient and reliable multi-hop relay mechanisms of ZCOR make the protocol robust over the various VANET conditions even without relying on additional adaptive techniques.

In the following subsections, we first detail the slot reservation mechanism for LSM packets, and then explain CoT concept, which enables coordination-free opportunistic packet relay. Lastly, we extend ZCOR for multi CoTs to overcome spatially correlated shadowing effects.

2.3.1 Slot Reservations for LSM

As in current WAVE standards [65], we assume that nodes are time synchronized and simultaneously monitor CCH for a time interval T_{CCH}. After this interval, nodes access SCH until the next CCH interval begins. The time interval between the beginnings of two CCH intervals is called as a synchronization interval T_{SI}, which is typically set to $100 - 200$ ms. We propose that T_{CCH} is further divided into L transmission slots, and L is customizable to the size of a LSM packet. The transmission slots are accessed through reservations as in R-ALOHA mode. LSM source nodes randomly access any of the slots that were idle during the previous T_{CCH}. Only idle slots can be reserved, since slots that are used by other nodes are implicitly considered as reserved for the same LSM source node in the next control channel interval.

Figure 2.4 shows how LSMs are periodically transmitted with different periodicities according to their classes in Table 2.1. The figure illustrates the repeat-cycle and slot assignment for each LSM class. Because the relay of each LSM packet is completed within the duration of $h \cdot T_{SI}$, where h refers to the number of hops from the source node, the reception latency is bounded by $h \cdot T_{SI}$. To avoid collisions between LSM packets and non-LSM packets, access-backoff slots are exclusively assigned; low order (from 0 to $K - 1$) access-backoff slots are assigned for LSM packets for implicit coordination, while high order (from K to $2K - 1$) access-backoff slots are used by non-LSM packets to avoid collisions among them.

A LSM source reserves its slot using the first LSM packet, and considers its reservation a success if its first packet is overheard in the next transmission slot. However, due to channel

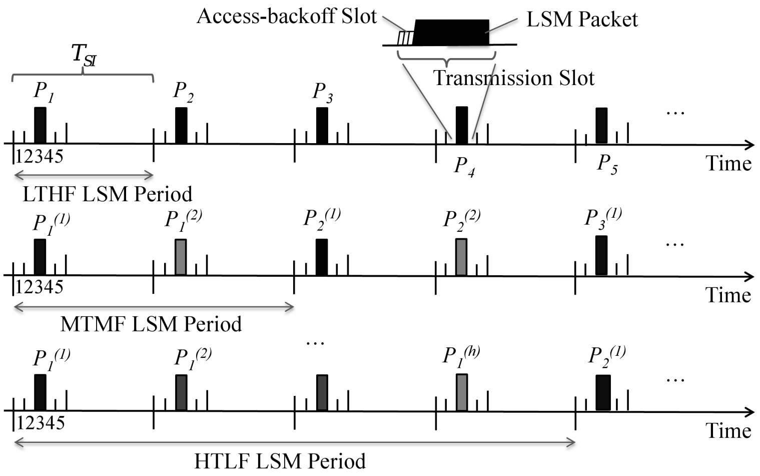


Figure 2.4: Transmission slot reservation in each class of LSMs ($L = 5$); MTMF geocast has 2-hop range ($h = 2$).

fading, the relayed LSM packet may not be overheard in the next transmission slot. In such a case, the node will sense busy channel status, but the node cannot demodulate the received packet; then the node cannot properly judge if its reservation has succeeded or failed due to a collision. Therefore, the source node can take a conservative choice: when the node has either received another node's LSM packet in the next transmission slot or cannot demodulate the received packet, the node considers that its reservation has failed due to a collision and therefore switches to another slot.

However, ZCOR is designed to minimize possible collision scenarios in reserving slots. We firstly consider the situation that more than two LSM sources try to reserve an identical idle slot during the same T_{CCH}. Note that such collisions rarely occur thanks to the randomness in emergency-event detections and in sensing delays in each node. However, the probability of such initial collisions can be further minimized, by exploiting the initial K random backoff slots in each transmission slot for the first LSM packets. On the other hand, LSM packets can collide with any packet transmitted from nodes in interference range. Therefore, it is necessary to sufficiently lower the carrier sensing range to avoid the transmission from the nodes in interference range; which means extending carrier sensing range to guarantee the reception of LSM packets at possible next hop relay locations (denoted as CoT in ZCOR) exploiting power capture effect [45].

After a successful hop-by-hop relay to the destination geocast area along the LSM path, the slot at each hop remains reserved. Thus, the reservation is spatially extended along the entire geocast path. By reserving packet transmission slots, LSM packets are much less interfered by background traffic in the same CCH. Moreover, such spatial and temporal slot reservation on a one-dimensional geocast area can be easily expanded over a 2-dimensional space through copying-and-forwarding multiple LSM packets to each directional road segment; however, such an expansion consumes additional transmission slots.

2.3.2 Opportunistic Relayer (Relay Node) Selection

The location of relayers significantly affects the efficiency and the reliability of multi-hop dissemination of LSM packets. However, selecting the best relayer, which usually is the farthest reachable node from the previous relayer, is a very difficult task in dynamic VANET conditions. That is because previous relayers typically have inaccurate reachability information on their edge neighbor nodes due to channel fading and mobility of nodes. Also typical velocity adaptive heartbeat rate control algorithms, which are used to alleviate heartbeat congestions, can further decrease the accuracy of neighbor knowledge.

One such problem is the *false-relayer selection problem*, which refers to the case in which a previous relayer selects a node that already moved out of its coverage range as its next hop relayer. Figure 2.5 illustrates an example of a two-hop LSM relay, where the current relayer node j relays packets to its relayer candidates. In this figure, node j may still falsely consider node b as its relayer candidate, because b is still in its neighbor list although b has moved away from its reachable range. Another such problem is the *hidden-neighbor problem*, which refers to the case in which better positioned nodes are not considered as candidates until their location is updated to the previous relayer. In the same figure, if j selects node c as its next relayer, then the relay fails when node c does not receive the packet to relay owing to channel fading. However, until the existence of node a is updated to node j, node a, which is a hidden-neighbor to j, cannot be used in the relay process.

Therefore, determining a relayer relying entirely on the neighbor knowledge of a single node is neither reliable nor efficient. The reliability of neighbor knowledge in VANETs, in fact, degrades rapidly according to the distance between nodes due to severe channel fading. Increasing the heartbeat packet transmission rate or power, however, easily congests CCH. To

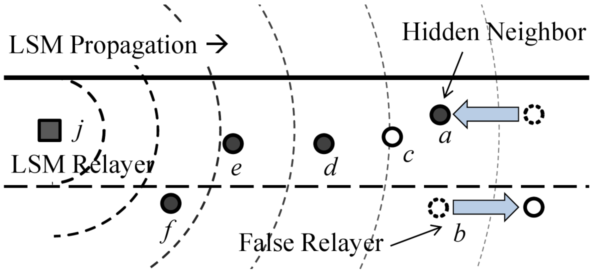


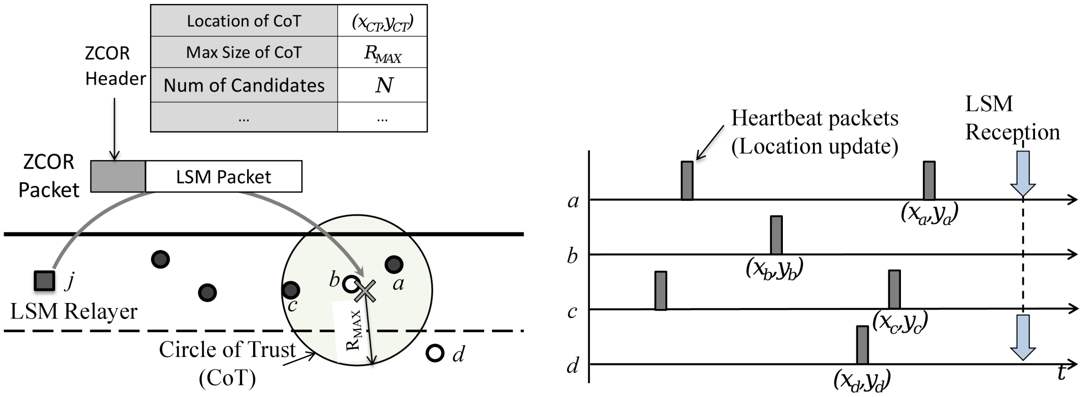
Figure 2.5: LSM relayer j selects a next-hop relayer based on its neighbor knowledge collected from heartbeat packets.

address these challenges, the LSM relayers in ZCOR select a geographic area incorporating a number of relayer candidates (instead of selecting a single node) allowing opportunistic forwarding to exploit multi-node diversity. The geography-based opportunistic relaying algorithm in ZCOR is designed to prevent both the *hidden-neighbor problem* and the *false-relayer selection problem*, which are mainly caused by imprecise neighbor knowledge.

2.3.3 Implicitly Coordinated Opportunistic Multi-hop LSM Relay

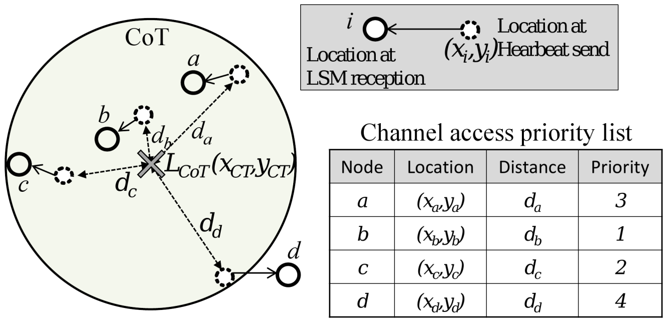
The opportunistic relaying mechanism improves reliability in the packet relay process [50, 51] since the relay succeeds when any candidate node receives the packet from the previous relayer. Typical opportunistic algorithms, however, rely on a rather complicated coordination processes to avoid collisions among relayer candidates. Such coordination typically induces not only delay in packet transmissions, but also overhead for negotiations, which degrades the overall efficiency of the protocol. Therefore, ZCOR seeks to minimize the overhead in coordination for opportunistic relay by integrating the relayer selection mechanism with slot-based channel reservations, which virtually enables coordination-free opportunistic routing.

ZCOR exploits implicit coordination technique and obviates the need for such coordination by applying deterministic backoff on reserved slots for LSM relay. Relayer candidates receiving LSM packets access the channel according to their channel access priorities (k), which are translated into the number of access-backoff slots. Note that candidates do not need to know which other nodes have also received the LSM packets for relaying, since they can overhear higher-priority transmissions; then they cancel their own relay transmissions if the same message was already forwarded by another node. In the example scenario in Fig. 2.6(a), LSM relayer j adds ZCOR header containing information on the next-hop (e.g., the location and the maximum size of CoT, as well as the number of candidates) to LSM packets. The nodes receiving ZCOR packets decode the headers and determine their rebroadcast priority to relay the packet. In the example figure, among the three candidates $\{a, b, c\}$ in CoT, two candidates $\{a, b\}$ received the LSM packet from node j. If the candidates have uniquely assigned access priority, e.g, $k = \{2, 1, 3\}$ for $\{a, b, c\}$, then the node with highest priority that received LSM becomes the next relayer.



(a) Transmission of ZCOR packet; packet header contains information for implicit coordination.

(b) Neighbor knowledge update through heartbeat packets among the candidates in CoT.


CoT
a
b
c
d
d_a
d_b
d_c
d_d
$L_{CoT}(x_{CT}, y_{CT})$
i
Location at LSM reception
(x_i, y_i)
Location at Hearbeat send
Channel access priority list

Node	Location	Distance	Priority
a	(x_a, y_a)	d_a	3
b	(x_b, y_b)	d_b	1
c	(x_c, y_c)	d_c	2
d	(x_d, y_d)	d_d	4

(c) Implicit coordination exploiting local neighbor knowledge.

Figure 2.6: Implicitly coordinated opportunistic LSM relay.

However, the access priority value should be uniquely assigned to each candidate to avoid collision among the relayer candidates. Also, the priority list should be immediately available to those candidates whenever LSM packets are received for relay. The candidates in CoT exploit their neighbor knowledge acquired from heartbeat packets, shown in Fig 2.6(b). Hence, the latency in establishing CoT is trivial, and LSM relayers can immediately select the location of the next CoT wherever they need to. Moreover, the candidate nodes can immediately determine their access priority using their neighbor knowledge that is previously acquired from heartbeat packets. Their access priority, k, can be simply calculated by comparing their distances to the center of CoT, L_{CoT}, with the distances of other candidates. As shown in Fig 2.6(c), nodes simply convert their distance rank into channel access priority, k, using the most recent location information updated from their neighbor nodes in CoT[4].

Assuming that the size of CoT is small enough to guarantee the reliable exchange of heartbeat packets, candidates can maintain identical neighbor knowledge, and then they can build an identical priority list to avoid collisions among them. Also the level of granularity in coordination outputs from current GPS modules are sufficiently fine (submillimeter levels) to avoid multiple candidates with identical distance values. Considering their typical measurement accuracy is of several meters, the digits in the coordination outputs beyond the measurement accuracy are nothing but random values, which can be used to provide enough randomness to prevent collisions among the candidates at similar distance to L_{CoT}.

2.3.4 The Size and Location of CoT

In the previous section, we simply assumed that the candidates in CoT can build reliable neighbor knowledge from heartbeat packets. However, we admit that node can collect incorrect neighbor knowledge due to errors in packet receptions caused by channel fading and the mobility of vehicles. In this section, we analyze the probability of successful packet relay (P_s) considering the heartbeat delivery rate (p_h), LSM packet delivery rate (p_r), and the number of candidates used (N).

Each LSM relayer sets the size and the location of the CoT for the next hop relay, and stores that information in the ZCOR packet header. The location of CoT is set as the location of the farthest reachable neighbor that contains N candidates in the circle of radius R. However, if the size of CoT R is too large, heartbeats cannot be exchanged reliably ($p_h < 1$). Then the candidates in CoT may no longer have a synchronized priority list, which may result in

---

[4] The location information used for priority determination is not the actual current location of candidates but the last location updated by heartbeat message; because the location information in heartbeat message is the common information all nodes within the CoT are sharing.

collisions among them. On the other hand, a smaller R may reduce spatial-diversity gains. A further tradeoff exists with respect to the distance between the CoT and the previous relayer. Let the probability of LSM delivery from the current relayer j to the next-hop candidates be denoted as p_r. If the CoT is located too far from j ($p_r \ll 1$), the relaying process may fail when none of the candidates successfully receive the LSM. If the CoT is located too close, it can increase the hop count along the path and result in additional delay. Therefore, ZCOR can flexibly trade off reliability with efficiency in LSM dissemination by controlling the location of CoT. By putting CoT away from the previous relayer, the area covered by each hop can be extended; however, the reliability can be degraded in fading channel conditions. Also, the maximum size of the access backoff, K, should be chosen considering that it limits the number of candidates used ($N \leq K$).

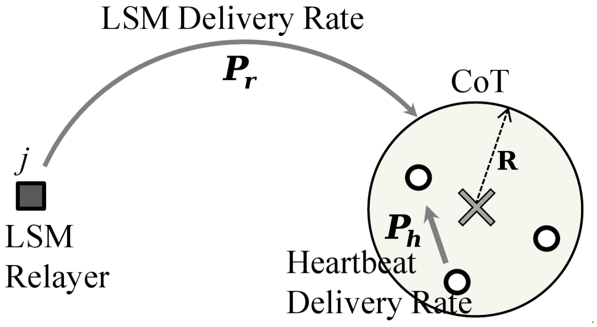


Figure 2.7: Two-hop LSM relay scenario for the analysis and simulation of the implicit coordination method.

To characterize reasonable parameter ranges for the size and location of CoT, using the two-hop relay scenario in Fig. 2.7, we analyze their interactions with successful relay probability, P_s. Using MATLAB, we also simulate the same scenario using a Monte Carlo method [66]. We consider that a LSM relay fails either when more than two candidates have the identical highest priority values owing to incorrect neighbor knowledge, or when the LSM packet is not delivered to any of the candidates.

The LSM forwarding success probability for N nodes in CoT, $P_s(N)$, can be derived from the following equation,

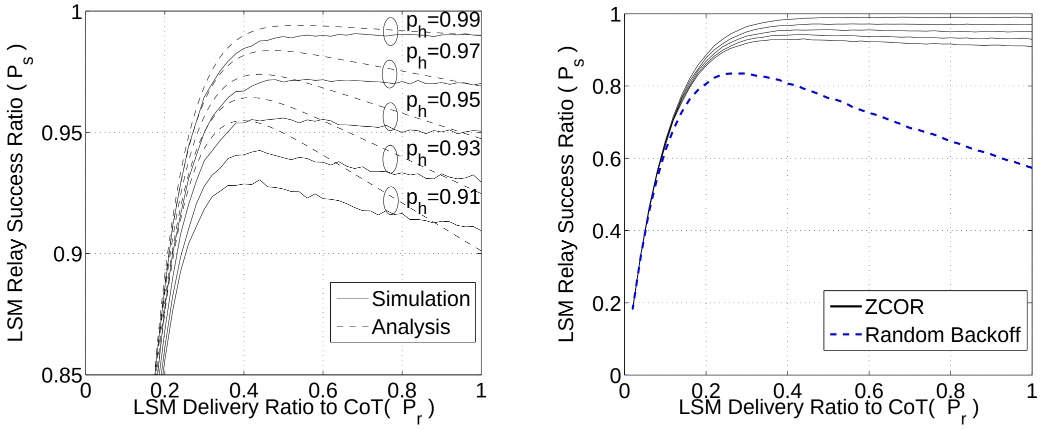
$$P_s(N) = \sum_{m=1}^{N} P_r(N, m)(1 - P_c(N, m)). \tag{2.1}$$

Here $P_r(N, m)$ is the probability that m out of N candidates in the CoT successfully receives LSM from node j, and $P_c(N, m)$ is the probability of any collision occurs in such a condition. Then, $P_r(N, m)$ can be computed by (2.2) from LSM delivery rate to the CoT, p_r.

$$P_r(N, m) = \binom{N}{m} p_r^m \cdot (1 - p_r)^{N-m}. \tag{2.2}$$

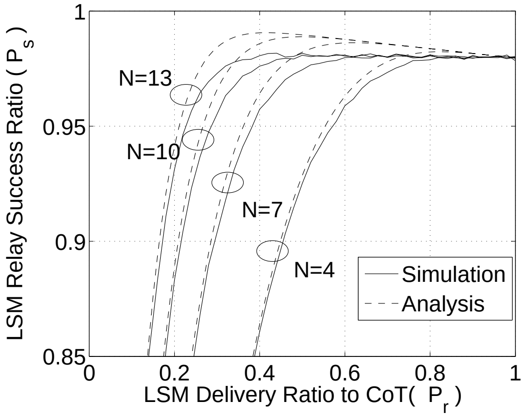
Also, the probability of any collision occurring when m out of N candidates in the CoT successfully receive LSM, $P_c(N, m)$, can be calculated by considering all possible priority collision cases over different combinations of receptions for N nodes. For example, when five nodes, a, b, c, d, e, have priorities of $\{1, 2, 3, 4, 5\}$ in CoT, and three of them receive LSM ($N = 5, m = 3$). One possible scenario is that node $\{a, c, d\}$ receives LSM, and node a has the highest priority. However, a collision occurs if either node c or d has the same probability as a, which is caused by any of $\{c, d\}$ having missed the heartbeat packet from a. In that case, the probability of collision can be approximated by $P_c(5, 3) \approx (1-p_h)^2 + (1-p_h)^4$ assuming $p_h \ll 1$.

Figure 2.8(a) shows the results on the LSM relay success rate, P_s, over the reliability of heartbeat messages. The figure indicates that the size of CoT should be chosen to allow $p_h > 0.95$ to achieve more than 95% reliability in LSM relays. Note that P_s decreases in high P_r conditions owing to increased collision probability among the candidate nodes when more of them have received the packet to relay while having inconsistent neighbor knowledge. On the other hand, we compared the performance of ZCOR's deterministic priority decision method with a simple random method that each candidate randomly select its own priority. Figure 2.8(b) shows the CoT based method significantly reduces the probability of collision compared to the random method. In Fig. 2.8(c), we change the number of candidates in CoT and determine the required number of nodes in CoT for reliable LSM relays. A larger N (the number of nodes in CoT) can enhance the reliability, however, which requires large K (backoff window size) to assign unique priority value to all candidates. From the figure, we can determine that $K = 10$ is large enough even for $p_r < 0.3$ assuming $p_h = 0.98$.



(a) LSM relay rate in fixed Number of relayer candidate ($N = 10$).

(b) Comparision with random backoff method.

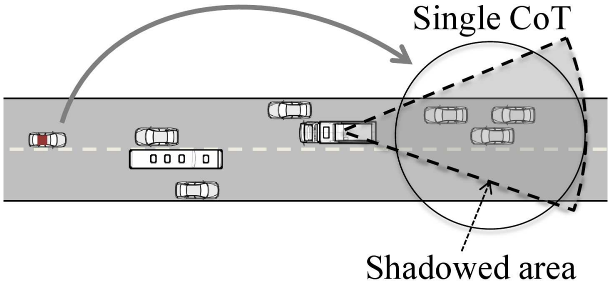


(c) LSM relay rate in fixed heartbeat delivery rate ($p_h = 98\%$).

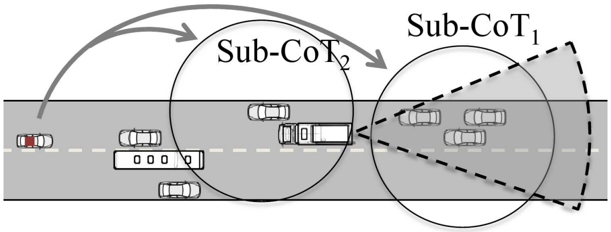
Figure 2.8: LSM relay rate in two-hop scenario.

2.3.5 Multi-CoT Against Spatially-correlated Shadowing Effects

For reliable LSM disseminations, the effects from spatially correlated shadow-fading also needs to be addressed, which is problematic when the entire area of the CoT is shadowed as shown in Fig. 2.9(a). The figure illustrates an example scenario where the LSM relay fails due to showing-fading caused by a large truck blocking the signal from the previous LSM relayer. Since such shadow fading in VANET is dynamic, estimating and responding to shadowing is difficult. Enlarging the size of CoT could alleviate such a problem; however, the enlarged CoT incurs undesirable tradeoffs that produce collisions among the candidates owing to low heartbeat delivery rate. The foregoing discussion shows that, for reliable LSM relay, the size of the CoT should be smaller than the range of reliable heartbeat exchange (e.g., $p_h > 0.95$).



(a) Single CoT.



(b) Multiple CoTs.

Figure 2.9: Multi-CoT to cope with spatially-correlated shadow fading effects.

We address this problem by splitting a single CoT into a number of sub-CoTs, as shown in Fig. 2.9(b), to further exploit spatial diversity gains. The sub-CoTs have a smaller number of candidate nodes, which are separated by more than the channel correlation distance. Thus, each CoT remains sufficiently small, but owing to their spatial separation, we can still overcome shadow fading effects (each sub-CoT likely experiences independent fading). Although sub-CoT$_1$ suffers from severe shadow-fading, LSM packets can still be relayed by candidates in sub-CoT$_2$. Even if any node in sub-CoT$_1$ receives LSM, the node receiving the packet can be the next relayer. However, when all the nodes in sub-CoT$_1$ fail to receive LSM, then the candidates in sub-CoT$_2$ are automatically involved in the relay process. Therefore, the decision for the LSM relay is made dynamically for each LSM packet depending on LSM packet receptions either in sub-CoT$_1$ or in sub-CoT$_2$, which is more efficient than relying on a single CoT.

To incorporate all sub-CoTs into the relay process, channel access priorities ($\{1, 2, \cdots, K\}$) are split into a number of access priority subsets by the previous relayer, then each subset is assigned to each sub-CoT. For example, when $K = 10$ and the number of sub-CoTs is 3, three exclusive priority subsets of $\{\{1, 2, 3, 4\}, \{5, 6, 7\}, \{8, 9, 10\}\}$ can be assigned to each sub-CoT, thereby, all the nodes in the three sub-CoTs are involved in the forwarding process. Sub-CoT$_1$ is set to cover the first 3 farthest neighbor nodes from the previous relayer within a circle or radius R. Then the sub-CoT$_2$ is set to cover the next 3 nodes outside of sub-CoT$_1$ (non-overlapping over sub-CoT$_1$), and sub-CoT$_3$ is set to cover the rest 4 nodes. If the network is sparse and cannot find a sufficient number of nodes in a circle of radius R, then the CoT is split until the sub-CoTs include a total of K nodes. Initially, node j finds the farthest neighbor node l_k and sets the center of the first sub-CoT (sub-CoT$_1$) at the location of its neighbor node, which puts node l_k within the range R, and the first n_1 priorities are assigned to sub-CoT$_1$. Then, the second sub-CoT is located at least $2R$ away from the sub-CoT$_1$, and the next n_2 priorities are assigned to sub-CoT$_2$. The process continues until all K priories are assigned to all sub-CoTs.

Besides the gains from additional spatial diversity, using multiple CoTs brings several additional benefits. In sparse network conditions, using multiple CoTs prevents the size of CoT from growing too large to incorporate enough number of relayer candidates, which may result in inaccurate neighbor knowledge collection among the candidates. Also, in dense network conditions, the multi-CoT algorithm prevents all candidates from being selected at the edge of the previous relayer node, which results in a high delivery failure rate caused by low LSM reception rate (p_r) for the candidates in the CoT.

2.4 Performance Evaluation

We implement ZCOR using Network Simulator (NS) 2 version 2.33 [67]. In this section, we explain the details of the simulation setup, channel models, and two baseline protocols to be compared with ZCOR.

2.4.1 Baseline Message Dissemination Protocols

Many broadcasting protocols for safety message dissemination have been developed to meet the various requirements for on-road human safety applications. However, it is virtually impossible to compare all broadcasting protocols side by side under the same network conditions, since each protocol is optimized assuming different scenarios under heterogeneous network conditions. Hence, we pick two representative baseline protocols for LSM dissemination, which are typically addressed as short-to-medium range geocast protocols in Ad-hoc networks.

CFG (Controlled Flooding-based Geocast)

CFG is based on a controlled flooding type broadcasting protocol. To prevent the "broadcasting storm" problem [68], CFG uses Scalable Broadcast Algorithm (SBA) algorithm [69] that suppresses redundant rebroadcast using two-hop neighbor knowledge. In the SBA algorithm, the nodes receiving LSM packets, put the received packets in their transmission queues, then set their RAD timers and observe channel. However, the packets in the queues for rebroadcast are discarded if their two-hop neighbors are already covered by other nodes' rebroadcast. Such a distributed decision mechanism in CFG increases reliability in severely faded channels by inducing large rebroadcast overhead. Moreover, in dense network conditions, such RAD-timer based redundancy suppression mechanisms cannot efficiently work owing to the latency between the decision on the rebroadcast and the actual attempt of rebroadcast of the packet [70]. Since SBA does not consider the directivity of message propagation, for a fair comparison, RAD values are weighted according to the distance from the previous relayer to give higher priority to edge nodes [70].

MRG (Multicast Relay-based Geocast)

MRG is based on a relay-based routing protocol, and next-hop relayers are deterministically selected by previous relayers. Compared to most flooding-based broadcasting algorithms, such centralized deterministic methods are more efficient since the amount of redundant rebroadcast can be easily controlled by the previous relayers depending on the network conditions. Considering the reliably in LSM disseminations, we choose Double Cover Algorithm (DCA) [71], which selects one next relayer covering the target geocast region twice at least. Moreover, to cope with erroneous channel conditions, ACK-based retransmission scheme is adopted with seven maximum retransmission attempts.

Compared to slot-based access in ZCOR, both baseline protocols use contention-based

802.11 CSMA MAC. For a fair comparison, however, 802.11e style prioritized transmission is applied to penalize low priority background PSM packets that share CCH with LSM packets. Hence, queues in MAC, the size of contention windows (CW_{min}), and backoff slots are differentiated according to the priority of the packet. Similarly, ZCOR uses exclusively differentiated backoff slots for LSM packets ($0 \leq k \leq K-1$) and PSM packets ($K \leq k \leq 2K-1$).

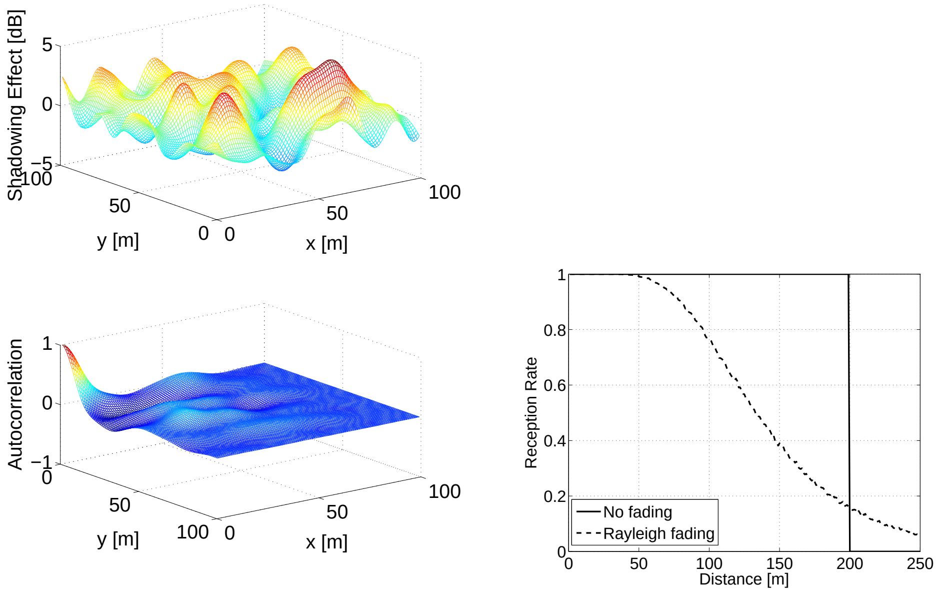
2.4.2 VANET Simulation Model

Path-loss in wireless communications is usually decomposed into distance-based path-loss, terrain dependent shadow-fading X_σ, and small-scale fading Y_r due to multi-path and mobility of mobile nodes. The aggregate path-loss L is represented in (2.3) at transmitter-receiver distance d with path-loss exponent γ. In V2V communications, where both transmitter and receivers have high mobility, shadow-fading is more dynamic [72], and spatially correlated [54], which is implemented by a 2-D shadowing model [73] using Sum-Of-Sinusoids (SOS) functions as shown in Fig. 2.10(a). The autocorrelation value for spatial correlation is set as $20\,\mathrm{m}$ according to the empirically measured value for peer-to-peer communications in urban areas [54]. We used the Rayleigh channel model for small scale fading considering the frequent non-line-of-sight conditions in VANET, and the packet receptions rate over distance due to small scale fading is shown in Fig. 2.10(b).

$$L = L_0 + 10\gamma log_{10}\frac{d}{d_0} + X_\sigma + Y_r \text{ [dB]}. \tag{2.3}$$

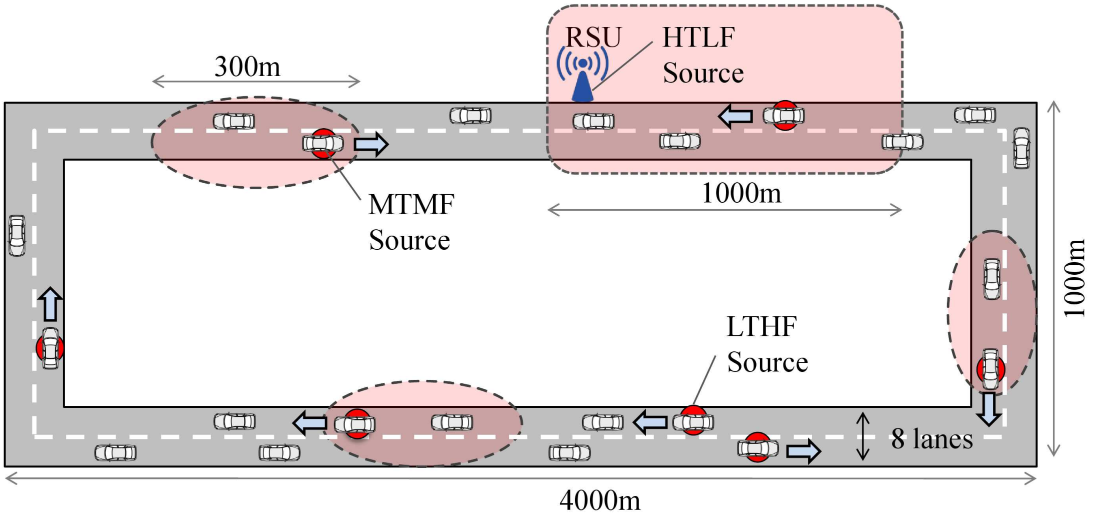
NS-2 simulation scenarios are created by using *VanetMobiSim* [74] with *Intelligent Driver with Intersection Management model* to model realistic car-chase and lane-changing behaviors of vehicles. Figure 2.10(c) depicts the road network where vehicles are running total $10\,\mathrm{km}$ track of 8 bi-directional lanes. For analytical simplicity, the locations of HTLF and MTMF sources (e.g., RSUs) are fixed, but single-hop LTHF sources are randomly selected among running vehicles.

We consider two types of PSM packets which are sharing CCH with LSM. They are heartbeat packets and various types of background PSM packets that are transmitted upto $25\,\mathrm{pkt/s}$ depending on the vehicle's speed [75]. These PSM packets are basically velocity (v) adaptive



(a) 2-Dimensional shadow channel model: $d_{corr} = 20\,\mathrm{m}$, maximum shadow effects: ± 5[dB]

(b) Communication range: log-distance path-loss model ($\gamma = 4$) and Rayleigh fading



(c) Highway scenario, 8-lane bi-directional roads

Figure 2.10: VANET simulation channel models and scenarios.

to prevent the CCH congestion problem. Considering that the accuracy of most GPS-based location finding devices installed in vehicles are around $5\,\mathrm{m}$, vehicles update their location in every $5\,\mathrm{m}$ movement by transmitting heartbeat packets ($0.2v\,\mathrm{pkt/s}$), and the background PSM packets transmission is also set as ($0.2vq\,\mathrm{pkt/s}$) for a background congestion factor q. The details of configuration are shown in Table. 2.2.

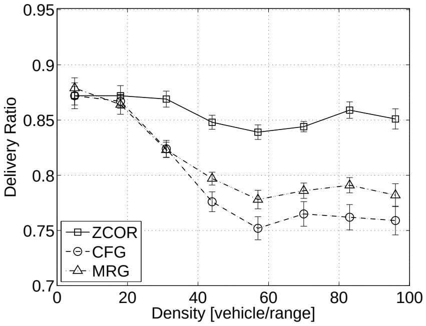
2.4.3 NS-2 Parameters and Evaluation Metrics

A number of parameters in NS-2 are adjusted to set the communication range without channel fading as $200\,\mathrm{m}$ when considering field measured data on the communication range for 802.11g based radio systems in [76]. Vehicle density is measured by the number of vehicles in a $200\,\mathrm{m}$ circular communication range. To minimize interference from the nodes out of carrier sensing range, the carrier sensing threshold is set to guarantee packet receptions at $200\,\mathrm{m}$ distance from the transmitter even when another packet transmitted outside of the carrier sensing range interferes with the packet. Because path-loss in vehicular networks is high, in actual network environments, throughput loss due to enlarged carrier sensing range will be small. Other parameters for simulation are presented in Table 2.3.

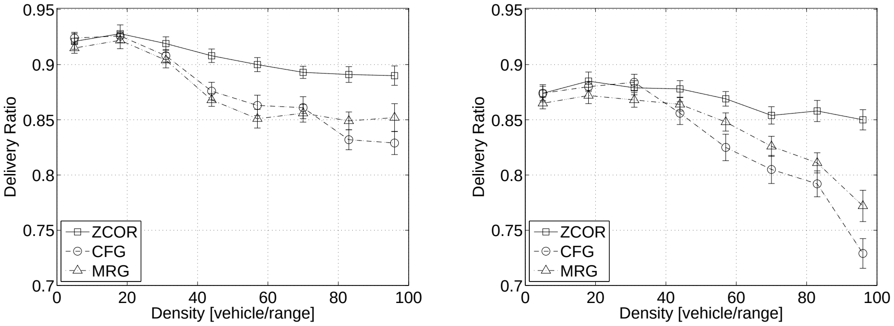
In evaluating the performance of protocols, we use reliability and overhead. Reliability is measured by LSM delivery ratio for the nodes in the geocast area. Since LSMs have strict latency requirement, packets arriving later then the latency requirement of each LSM class are silently discarded along with out-of-sequence packets. Overhead is measured by the number of rebroadcast packets for each LSM covering its geocast area. We do not consider heartbeat packets as protocol overhead because the heartbeat transmission is considered as a basic network protocol element in VANETs which is widely used for many applications.

2.5 Result

For simulations, fifty topologies are created with random initial positions of vehicles. The reliability and the size of the overhead are then measured for each protocol.

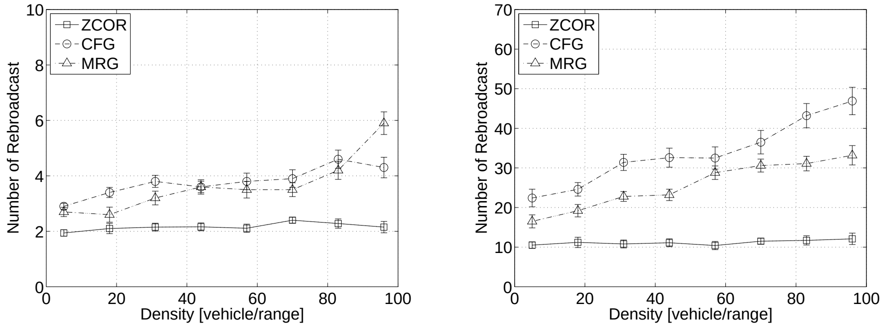


(a) Reliability of LTHF: LSM Delivery ratio.



(b) Reliability of MTMF: LSM Delivery ratio.

(c) Reliability of HTLF: LSM Delivery ratio.



(d) Overhead of MTMF: Rebroadcast overhead.

(e) Overhead of HTLF: Rebroadcast overhead.

Figure 2.11: Reliability and overhead under various vehicle density conditions.

2.5.1 Reliability and Overhead Comparison

In Fig. 2.11, we show the reliability and overhead of ZCOR compared with CFG and MRG under different vehicle density conditions. The number of LSM sources for MTMF and HTLF are fixed as 10 vehicles while $20\,\%$ of the vehicles in the networks are randomly selected as single-hop LTHF LSM sources.

Figure 2.11(a)−2.11(c) compares the reliability of each protocol. As vehicle density increases, the reliability of CFG and MRG degrades owing to packet collisions and transmission delays caused by the increased amount of background packets (including heartbeat packets), rebroadcast LSM packets, and the number of LTHF LSM sources. In congested networks, although LSM packets have higher priority for channel access over background packets in MAC layer, collisions and interference are unavoidable for CFG and MRG in congested networks. When compared to those protocols, ZCOR achieves a higher delivery ratio under overall vehicle density conditions by reserving channels for the duration of the LSM transmission. ZCOR only experiences minor reliability degradation in high density conditions owing to the interference from outside the carrier sensing rage.

Although all three protocols adopted the velocity-adaptive heartbeat rate adaptation method, CCH can still be congested in mid-density network conditions where the number of background packet transmission per unit area peaks as discussed in Section 2.2. Hence, as shown in Fig. 2.11(a), the reliability degrades at mid-density conditions. Figure 2.11(b) and 2.11(c) show the delivery ratio of MTMF and HTLF LSMs respectively. Compared to LTHF, MTMF LSM shows better reliability thanks to the rebroadcast LSM packets from the second-hop relay nodes. However, the reliability of HTLF LSMs is lower than MTMF as the target geocast region extends over a large area, because target nodes many hops away from LSM sources are easily disconnected.

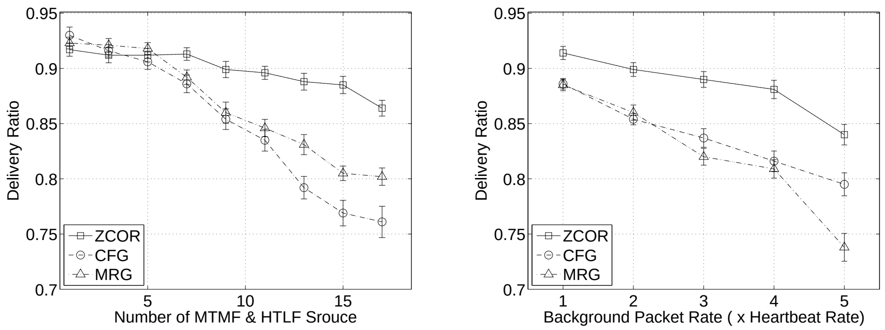
Figures 2.11(d) and 2.11(e) compare the rebroadcast overhead for LSM dissemination to cover $300\ \mathrm{m}$ (MTML) and $1\ \mathrm{km}$ (HTLF) geocast area. As discussed in Section 2.4, we find that as the network is congested, CFG relying on RAD based rebroadcast suppression mechanism, cannot suppress redundant rebroadcast enough, which further congests the network. Compared to flooding based CFG, ZCOR prevents the channel from being extremely congested even in high vehicle density conditions by limiting the number of rebroadcast packets at each hop.

On the other hand, although MFG can efficiently control the rebroadcast overhead by selecting a single next-hop relay node, the overhead from packet retransmission usually increases in unreliable fading channel conditions. Since the centralized next-hop selection method of MFG is inefficient and unreliable in erroneous VANET channel conditions, ZCOR overcome such a problem through the opportunistic LSM forwarding mechanism. Compared to those two protocols, the overhead in ZCOR is scalable over the number of hops and the ranges of geocast as a result of the gains from multi-node diversity. We can find that ZCOR can efficiently eliminate redundant rebroadcast, which in turn produces reliable message dissemination in congested network conditions.

2.5.2 The Performance of ZCOR in VANET Conditions

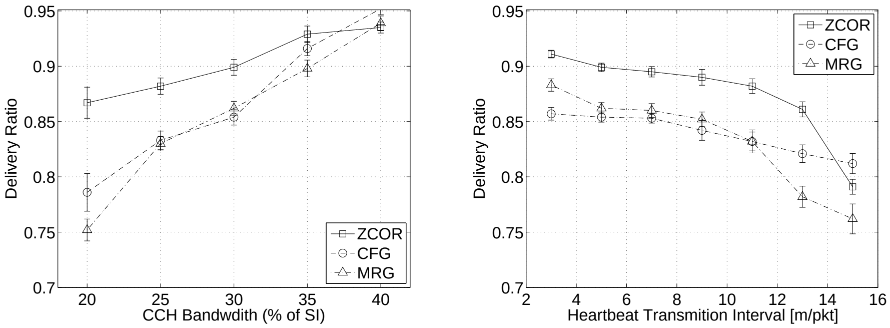
We measured the reliability of MTMF and HTLF LSMs under various VANET conditions considerable in real-road conditions. Figure 2.12 shows the results over four different network configurations. Firstly, Fig. 2.12(a) shows the result when we changed the number of MTMF and HTLF LSM sources. As the number of LSM source increases, CCH is more congested and the reliability of CFG and MRG degrades quickly. In Fig. 2.12(b), we can also find similar results when we increase the amount of non-emergency background packets sharing CCH with LSM. Compared to CFG and MRG, as long as CCH has enough slots for assignment to each LSM source, the reliability of ZCOR is not significantly affected by the network congestion status. However, the capacity of reservation-based MAC is hard bounded, which is limited by the number of slots. Therefore, when the number of LSM sources exceeds the number of available slots for a given CCH bandwidth, the LSM sources must reduce their LSM transmission rate by increasing their LSM update cycle; otherwise, a new LSM source cannot find its transmission slot until one of the existing LSM sources finishes its transmission. Hence, LSM source nodes need to monitor the occupied number of slots in CCH to adjust its LSM period according to CCH utilization.

Therefore, the bandwidth saved by ZCOR can be used to increase the utility of SCH, which is useful for various applications designed for VANET. In Fig. 2.12(c), we measure reliability under various CCH over SI ratio conditions. Because the rebroadcast redundancy in ZCOR is



(a) Various number of sources (MTMF & HTLF LSMs) conditions.

(b) Various background packet transmission rate conditions.



(c) Various CCH bandwidth conditions.

(d) Various heartbeat packet rate conditions.

Figure 2.12: The reliability of MTMF and HTLF LSMs under various VANET conditions; vehicle density is 55 [vehicle/coverage].

small, its reliability does not degrade much even with small CCH over the SI ratio as long as transmission slots are not fully occupied by LSM sources.

In Fig. 2.12(d), we increase the interval between heartbeat packet transmissions to measure the impact from the accuracy of neighbor knowledge. As the interval between heartbeat packets increases, the overhead from heartbeat packets reduces, but the information on neighbor nodes' existence and location becomes incorrect. As MRG mainly relies on neighbor knowledge to select the next forwarder, its performance is more vulnerable to the change of heartbeat transmission rate compared to CFG. As the update from heartbeat packets is delayed owing to network congestions, relayers tend to have incorrect neighbor knowledge, and relayers are likely to fail in choosing the best next-hop relayer. However, CoT based ZCOR is less dependent on neighbor knowledge, and is more resilient to the change of heartbeat transmission rate.

2.5.3 The Performance of Multi-CoT Against Shadow Fading

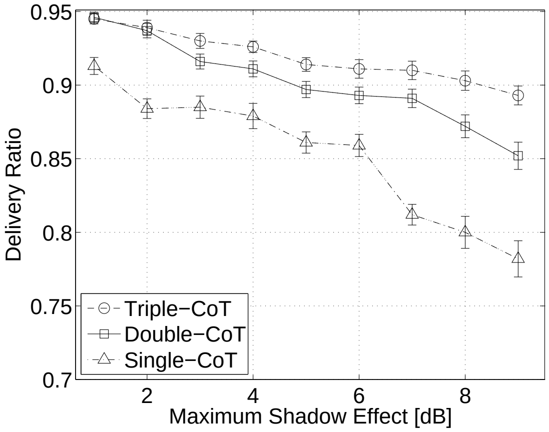


Figure 2.13: Gains from multi-CoT against shadow fading; vehicle density is 55 [vehicle/coverage].

In Fig. 2.13, we show how much the multi-CoT algorithm improves the reliability of LSM dissemination in severe shadow fading conditions. In the simulation, we fix the number of candidates at 10 and increase the maximum shadow-fading level up to 9 dB. We then compare the reliability of ZCOR when different numbers of sub-CoTs are used. The results show that it is important to increase the number of sub-CoTs in severe shadowing conditions, since reliability severely degrades when Single-CoT is used. However, using three CoTs (Triple-CoT) does not significantly improve the performance of ZCOR. As the nodes in the network experience deeper shadow-fading, which is spatially correlated over several tens of meters, using only a single CoT is less reliable since the nodes in a single CoT will experience similar fading. Therefore, in such conditions, it is important to use multiple CoTs to fully exploit spatial diversity gains.

2.6 Conclusion

We proposed *ZCOR* , an algorithm for mission-critical safety-related message dissemination in VANETs, which are characterized by dynamically changing network environments. *ZCOR* is a novel location-based opportunistic packet relay algorithm based on implicit coordination technique. Although *ZCOR* requires tight time-synchronization among nodes, it enables efficient and scalable multi-hop packet dissemination with significantly reduced overhead for the coordination of relayer candidates for opportunistic relay. Through extensive simulations, the performance of *ZCOR* is proved to meet the strong latency restrictions of safety-related messages over a wide variety of network conditions in VANET. Compared to the existing message dissemination algorithms, *ZCOR* showed similar or better reliability with much less rebroadcast overhead (up to 55% reduction). Such a bandwidth saving can be exploited to increase the utility of the service channel from 50% to 80% by reducing the size of control channel.

Table 2.2: Protocol Parameter

Protocol Parameters: Common	
T_{SI}	100 ms
T_{CCH}	30 ms
Number of Tx slots in T_{CCH}	30
LSM packet size	300 Bytes
Heartbeat packet size	250 Bytes
Heartbeat transmission interval	$5\,\mathrm{m/pkt}$
LTHF LSM (150 m) latency bound	100 ms
MTMF LSM (300 m) latency bound	200 ms
HTLF LSM (1000 m) latency bound	1000 ms
Protocol Parameters: ZCOR	
Transmission slot size	1 ms
Access-backoff slot size	$8\,\mu$s
First LSM access-backoff	$[0-9]$
Heartbeat packet access-backoff	$[10-19]$
The size of CoT: R	20 m
Protocol Parameters: CFG and MRG	
CWmin for LSM	7
CWmin for heartbeat packet	31
Random backoff slot size	$8\,\mu$s
Maximum RAD (CFG)	10 ms
Maximum number of retry (MRG)	7

Table 2.3: Simulation Parameter

Transmission power	$20\,\mathrm{dBm}$
Reception threshold	$-87\,\mathrm{dBm}$
Carrier sensing threshold	$-102.3\,\mathrm{dBm}$
Capture threshold	$6\,\mathrm{dB}$
Path loss exponent γ	4
Data rate	$3\,\mathrm{Mbps}$
Frequency	$5.89\,\mathrm{GHz}$
Shadow channel correlation distance: d_{corr}	$20\,\mathrm{m}$
Maximum shadow effect	$\pm 5\,\mathrm{dB}$
CCH duration	$30\,\%$ of SI
Minimum number of CoTs in splitting: M	2
Background congestion factor: q	2

Chapter 3

Implicit Coordination for Resource Allocation

3.1 Introduction

Wireless Mesh Network (WMN) [2, 3] is a communication network created by mesh style Ad-Hoc connections among wireless nodes to provide network services to mobile and stationary users even without infrastructure networks. WMNs are more reliable and can provide wider coverage since nodes are distributed, which exploit many redundant connections of mobile and stationary nodes. Since WMNs are resilient to partial break down of networks and is implementable using relatively low cost devices, their application can be easily extended to disaster networks [77, 78] and alternative Internet access service in underdeveloped countries [79, 80].

In WMNs, nodes are typically connected to peer nodes and cooperate to deliver packets to other nodes over multi-hop connections. However, such uncoordinated Ad-Hoc connections can cause server interference problems to each other. Although power control techniques can alleviate such interference problems in dense network conditions, they are not widely used in Ad-Hoc networks due to the difficulties in coordination. In wireless communication systems, power control has been thoroughly studied over decades aiming to enhance the network efficiency and the quality of service. Through the proper assignment of transmitting powers of wireless devices, it is possible to increase network throughput by reducing the level of mutual interference among devices. From the perspective of network throughput optimizations, power control is identical to the resource allocation by solving network-wide utility maximization (NUM) problems [5, 6, 7, 81, 8]. Although utility based power control methods produce optimal network throughputs, it requires frequent message exchange between nodes and also easily produce severe unfairness to individual node's throughput [82] depending on the topological conditions of the network. Also power control methods maximizing aggregate throughput may cause severe unfairness problems, as a number of transmitters inducing larger interference need to be shut down to improve overall network throughput.

Such fairness problems can be solved by joint scheduling and power control methods that guarantee minimum resource allocations by scheduling the nodes penalized in the power control process. By orthogonalizing the communication links – the transmitting and receiving node pairs – that produce high interference to other nodes, the rate region becomes convex achieving better network throughput. In this research, we propose a *Joint Power control and Scheduling Algorithm (JPSA)* to achieve better efficiency of the network throughput without sacrificing fairness among users. The joint scheduling and power control is known to be a NP-complete problem [83] which requires global knowledge of the network in order to find the optimal power values, which cannot be easily applied to Ad-Hoc networks where a central coordinator does not exist. In this research, we apply implicit coordination technique to achieve both efficiency and fairness while minimizing the overhead for coordination.

JPSA is a distributed coordination technique based on network utility maximization technique. We tackle the complexity issues related to joint scheduling and power control, *JPSA* employs implicit coordination technique, which infers the local interference level from Received Signal Strength to Noise-Interference (RSSI) level, *JPSA* significantly reduces latency and overhead in the coordination process. To schedule links for a better network fairness, *JPSA* autonomously groups links into a number of subgroups for scheduling for different time-slot access. Although its performance is not optimal, *JPSA* has the advantage of linear complexity compared to other NUM based joint power control and scheduling algorithms which have exponential complexity over the number of rate sets and number of nodes.

The remainder of this chapter is organized as follows: In section.3.2, we introduce the system model and identify the problems. Then, in section.3.3, we explain the the detailed explanation of our proposed *JPSA*. The simulation set-up and the results are presented in section.3.4. Conclusions are made in section.3.5.

3.1.1 Related Work

Utility based power control methods have been widely studied in cellular systems that are characterized by centralized base stations and mobile nodes connected to them. One of the key power control algorithm was developed in [84] where authors show that the utility-maximization problems for an optimal cell throughput can be implicitly solved in a distributed mechanism by introducing a shadow price function. For multi-cell environments, Ji et al. solved power control problems based on a convex utility function [7], and a distributed power control algorithm based on load-spillage is provided in [81]. Han et al. solved the power control problem by using a non-linear price function [85] for the uplink CDMA system. However the convergence of the proposed algorithm is only achieved when power values converge either to zero or to the maximum because price values converge only for those cases. They made a centralized approach that a base station broadcast system information to mobile stations. However, these papers do not discuss the fairness issue between users. In [5], Xiao et al. proposed an algorithm that adaptively modifies the price function to increase the fairness of users using a non-convex Sigmoid like utility function. Allowing soft SINR thresholds the authors alleviate the fairness problem. However, this scheme requires a tuning process of the parameters. These works attempt to design distributed coordination algorithms to enhance network efficiency in infrastructure-based networks.

In Ad-hoc networks, power control has mainly been applied for interference mitigation on a per-link basis to increase both the energy efficiency of nodes and the network capacity [86, 87, 88, 89, 90]. In [91, 92, 93], adaptive rate control is jointly considered with power control methods on a per link basis. In terms of per-network basis power control methods that primarily maximize network throughput, Vivek et.al. propose a cross-layered approach by jointly optimizing carrier sensing range and power control [94], and Narayanaswamy combines a power control algorithm with a routing protocol for network wide coordinations [95]. Coping with the fairness issues raised in network throughput maximization [82], the joint power control and scheduling approach is made by solving network-wide utility maximization (NUM) problems in [96, 83]. However, these algorithms not only require global knowledge of the networks, but also the complexity of the algorithms increases exponentially with the size of discrete rate set and the number of nodes. Compared to these works, by applying implicit coordination techniques, the proposed *JPSA* has a linear complexity that grows linearly with the number of nodes, which is independent of the size of rate sets. Also, the algorithm is fully distributed and requires very limited message exchange between nodes.

3.2 System Model and Problem

In Ad-hoc peer-to-peer networks, as shown in Fig 3.1, transmitter nodes and receiver nodes make a communication link pair. In our unicast communication model, each communication link, l_i, is assumed to have one transmitter node s_i and one receiver node r_i, which are not shared by other links, and G_{ii} is wireless channel gain for the connection.

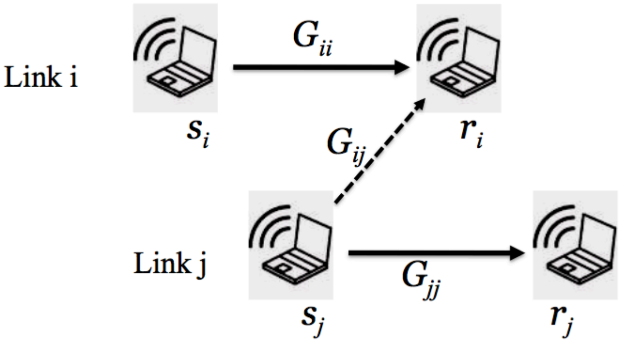


Figure 3.1: Peer-to-peer communications model (Unicast mode)

In interference limited communication systems such as CDMA and OFMDA systems, more than one communication pair is allowed to transmit data simultaneously. In such cases, a link capacity is limited by the interference caused by transitions from its neighboring links. The Signal to Interference and Noise Ratio (SINR), γ_i, at node r_i can be represented by the standard interference model in (3.1), which is a function of M interfering nodes' transmission power vector $\boldsymbol{p} = [p_1, \cdots, p_i, \cdots, p_M]^t$, where the transmission power is limited by a maximum value of $\bar{p}$. The amount of interference to r_i is related to the network channel gain matrix denoted by G_{ij} from the transmitter node s_j from link j to r_i. N_i is the thermal Gaussian noise component at r_i.

$$\gamma_i(\boldsymbol{p}) = \frac{G_{ii}p_i}{\sum_{j \neq i} G_{ij}p_j + N_i} \tag{3.1}$$

We can rewrite (3.1) as follows with the normalized channel gain matrix F_{ij} and the normalized thermal Gaussian noise η_i for $F_{ij} = \frac{G_{ij}}{G_{ii}}$, $\eta_i = \frac{n_i}{G_{ii}}$. R_i is the total amount of interference to node r_i.

$$\gamma_i(\boldsymbol{p}) = \frac{p_i}{\sum_{j \neq i} F_{ij} p_i + \eta_i} = \frac{p_i}{R_i} \tag{3.2}$$

We apply a network utility maximization (NUM) technique to solve the power control problem which can implicitly coordinate individual nodes to control their transmission power for the global network utility maximization. There are number of ways of defining utility functions depending on the applications of the service. Voice quality, data rates, network efficiency, and network throughput are examples of utility functions. In this research, we define the utility of the network as the sum of data rates of individual links, then the utility maximization problem can be described as following equations:

$$\text{maximize} \quad \sum_i U_i(\gamma_i(\boldsymbol{p})) \tag{3.3}$$

$$\text{subject to} \quad 0 \leq \boldsymbol{p} \leq \bar{\boldsymbol{p}} \tag{3.4}$$

Here, the optimization variable is the power of each node, p_i. By controlling p_i, we can maximize the network throughput. However, not all power assignments are feasible due to the mutual interference in the networks. Because the change of power in one the link affects all other links and their data rates, nodes are required to coordinate to maximize the network throughput.

Applying NUM methods for Ad-hoc networks for maximizing network throughput using minimum transmission power, the utility U_i is defined as the data rate of Wi-Fi radios. To allow the variable rates of Wi-Fi systems depending on SINR values, we set the utility function as a staircase function of γ as shown in Fig. 3.2 according to the 802.11a specifications. However, it is hard to directly apply NUM methods to the multi-rate Wi-Fi radios as NUM is based on convexity of the utility function while stair-case multi-rate function is a non-convex function which is discontinuous at each of the rate transitions. Approaches made in [96, 83] for this discrete utility function increase the algorithm complexity exponentially with the size of the rate set.

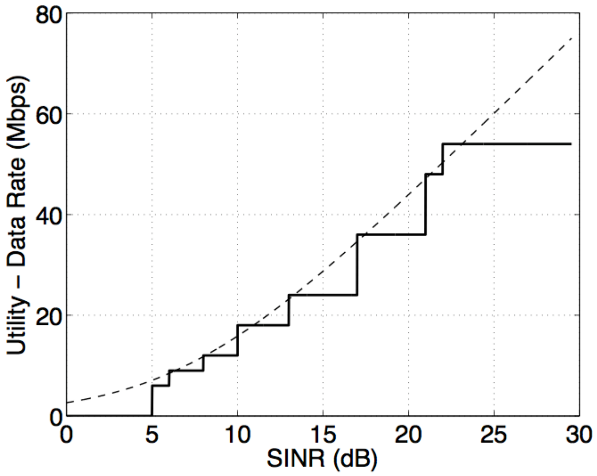


Figure 3.2: Staircase Utility function

3.2.1 Implicitly Coordinated Transmission Power Control

Solving a standard NUM problem in assigning powers to each transmitters, the utility maximization problem (3.4) can be rewritten as the following dual decomposition problem [85], which can be implicitly solved by individual nodes in a distributed way.

$$D(\lambda) = \max_{\boldsymbol{p}} \sum_i (U_i(\gamma_i(\boldsymbol{p})) - \lambda_i p_i) + \sum_i \lambda_i \bar{p_i} \tag{3.5}$$

Using gradient update method, the shadow price λ_i, which is used to implicitly coordinate nodes, is updated by the following equation.

$$\lambda_i^{(n+1)} = [\lambda_i^{(n)} + \alpha(p_i^{(n)} - \bar{p_i})]^+ \tag{3.6}$$

Depending on the interference conditions, each node has a different shadow price value that reflects its interference to other receiver nodes. Hence, transmitter nodes control the transmitter based on the price value updated by the receiver node. In the system of a convex utility function, powers only converge to either zero or to the maximum power, which is referred as a bang-bang type power control that either turns off nodes or makes nodes transmit in full power. The is due to the fact that the price, λ, converges only when power approaches to the maximum value, $\bar{p_i}$, and utility function monotonically increase with p_i unless the node is turned off ($p_i = 0$).

This causes serious fairness issues as nodes under large interference are forced to be turned off as it is hard to increase their utility for the same price of λ. There are a number of approaches to alleviate this unfairness problem. One method is to adjust the price function and adaptively adjust the price values as in [5]. However, this method requires calibration of the parameters, and cannot be a fundamental solution for the fairness issue.

Simple NUM based power control algorithms maximize network throughput, however, nodes will experience severe unfairness as the links that produce large spillage are turned off by the algorithm to maximize the network throughput [81]. Considering fairness issues, when the size of the network is large and their inter-distances are close enough to generate large mutual interference, it is necessary to schedule the transmissions of nodes in order to maximize the network throughput. Link scheduling is needed to orthogonalize links in time domain or in frequency domain to increase both the fairness and the aggregate throughput of the network simultaneously.

We are considering a scheduling method that orthogonalizes links in time domain without the need for extra frequency. By separating the links into more than one groups, it is possible to increase the total aggregate throughput by alleviating mutual interference. However, scheduling the transmission while simultaneously power controlling each link is a NP-complete problem, which is difficult to solve even in a centralized system.

For the link set $L = \{l_1, l_2, \cdots, l_M\}$, we can divide the links into more than two subgroups of links, $C_1 \cup C_2 \cup \cdots \cup C_k = L$ for the channel access in different time slots. Thus the scheduling problem is reduced to assigning links to each subgroup while applying the power control algorithm to each group maximizing the aggregate network throughput.

3.3 Joint Power Control and Scheduling Algorithm

We propose a Joint Power control and Scheduling Algorithm (JPSA) based on Utility maximization, which can provide a significantly improved throughput without sacrificing the fairness of users.

In Wi-Fi systems, applying convex optimization techniques for the distributed power control, the first problem is the complexity of the algorithm caused by the discrete utility function of Wi-Fi multi-rate systems. The complexity increases exponentially with the size of rate set. In addition to this, we cannot apply a gradient method to solve the maximization problem because the utility function is non differentiable due to its discontinuity at its rate transition SINR thresholds. Although we can apply a sigmoidal function instead of a staircase function in approximating the utility functions [5], the sigmoidal function is still a non-convex function, which is difficult to solve by standard methods used for general convex optimizations problems.

3.3.1 Power control with a staircase utility function

Because there is no central coordinator in Ad-hoc networks, scheduling and power control should be made with minimum exchange of information among nodes in the networks. We are assuming zero message exchange for power control. However, for scheduling, we need to allow a minimal information sharing between nodes to control the slots numbers and the timing of slots to avoid collisions between nodes.

Although the utility function is non-convex and is not differentiable, we can still exploit the concept of social welfare based on the price of the resource usage in the standard utility maximization problems. In (4.5), the distributed algorithm uses price, λ, in coordinating nodes to socially maximize the network throughput. This price prevents each node from selfishly exhausting air resources by increasing their transmission power to the maximum value.

Applying the staircase utility function of Wi-Fi radios, nodes do not need to increase their transmission power to the maximum as their utility does not linearly increase with their transmission power. Once the transmission power reaches a certain threshold for a data rate, its utility does not increase until the power reaches to the next threshold. This is problematic as λ always diverge to infinity, and the power never converges to any value. Thus, we modified the update algorithm of λ to the following equation in order to suppress its divergence problem. λ decreases as the number of iterations increase when divided by iteration step k.

$$\lambda_i^{(n+1)} = [\lambda_i^{(n)} + \frac{\alpha}{k}(p_i^{(n)} - \bar{p_i})]^+ \tag{3.7}$$

In each node, with the updated price λ_i, the utility is calculated and the power is adjusted to increases its own utility value U_i, which is affected by the interference from other transmitter's

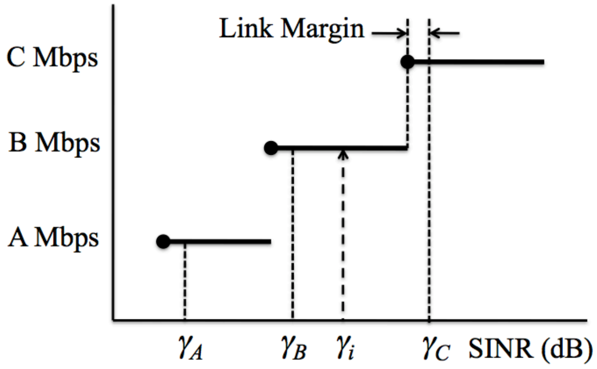


Figure 3.3: Target SINR: Calculate utility and set the target SINR based the staircase utility function

transmissions power $\boldsymbol{p_{i-}}$.

$$p_i^{(n+1)} = [arg \max_{p_i} U_i(\gamma_i(p_i, \boldsymbol{p_{i-}^{(n)}})) - \lambda_i^{(n)} p_i]^+ \tag{3.8}$$

Rather than setting the power value to an optimal point causing abrupt change in the utility value, in each iteration, power p_i is only slightly adjusted by the amount of Δp according to the direction that each node achieves higher utility value. Figure. 3.3 shows how p_i is determined based on the current SINR value, γ_i. With current γ_i between γ_B and γ_C, each node calculates its utility value assuming the γ_i equals to γ_A and γ_C. Then they compare their utility values to the current utility value, and determine the direction of power adjustment.

This utility calculation can be made without exchanging any information with other nodes as the problem is decomposed in a standard way using Lagrangian methodology. The utility is only dependent on the individual node's transmission power, p_i, of the link i. The aggregate interference from all other transmitting nodes, $R_i = \sum_{j \neq i} F_{ij} p_i + \eta_i$ can be calculated from known p_i, G_{ii}, and the amount of the thermal noise component.[2] Algorithm 1 shows the outline of the power control process assuming that the receiver node runs the power control algorithm and updates the power information to the transmitter node.

Assuming dynamic channel variations, the link margin is added to each SINR threshold for the reliable reception of packets. This margin is an environmentally dependent value, which

---

[2] The information on p_i is delivered to the receiver node in each packet header, and channel gain G_{ii} can be estimated from RSSI information

```
1) Measure $\gamma_i$
2) Find $R_i$
3) Find $\max U_i^-$, $U_i$, and $U_i^+$

4) Update $p_i$
if $U_i+$ is the $\max$ then
    $p_i^{(n+1)} = p_i^{(n)} + \Delta p$
$U_i-$ is the $\max$ $p_i^{(n+1)} = p_i^{(n)} - \Delta p$ $p_i^{(n+1)} = p_i^{(n)}$
5) receiver node $r_i$ feedback $p_i^{(n+1)}$ to transmitter node $s_i$
6) Update $\lambda^{(n+1)}$
$\lambda_i^{(n+1)} = [\lambda_i^{(n)} + \frac{\alpha}{k}(p_i^{(n+1)} - \bar{p_i})]^+$

$k = k + 1$
```

Algorithm 1: Receiver node feedback: updated power value to the transmitter node

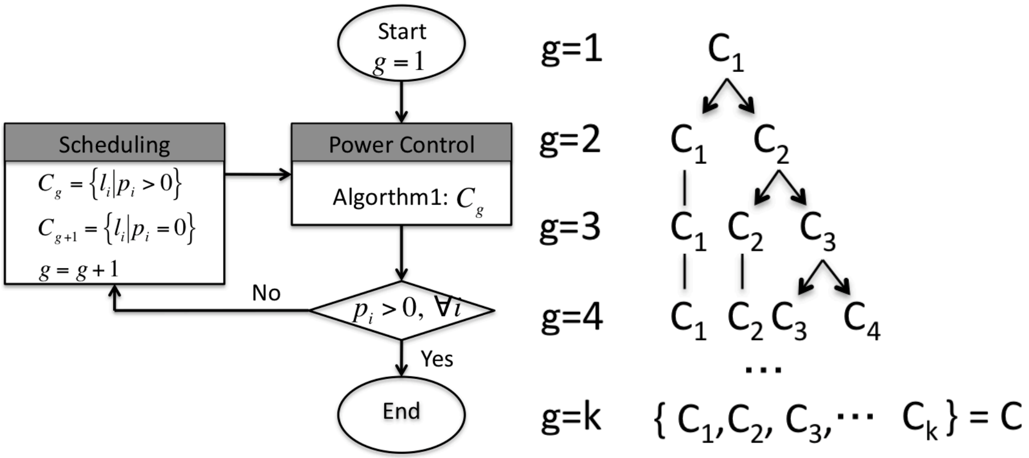
should be adjusted according to the amount of the small scale channel fluctuations. For the utility function, it is possible to apply a softly varying Sigmoidal function instead of the threshold based staircase function that abruptly switches the data rate. However, given the abruptly changing packet error rate at SINR thresholds for small changes in SINR, the impact on total utility values from Sigmoidal utility function is marginal.

3.3.2 Joint power control and scheduling

We solve the fairness issue discussed in Sect. 3.2.1 by jointly scheduling the transmission timing of nodes with power control algorithm simultaneously. As mentioned in the previous section, the problem of jointly scheduling transmissions and power control is a well-known NP-complete problem, which cannot be easily solved in a distributed way even with the full exchange of information on each node's status.

JPSA groups nodes into power control subgroups to reduce mutual interference between nodes so that each subgroup has a feasible solution for their power allocation. The algorithm is designed according to the following principles.

- The message exchange between nodes should be minimized
- The convergence of the power control algorithm should be fast, regardless of number of nodes



(a) Scheduling algorithm split groups until all the nodes have positive transmission power ($p_i > 0, \forall i$)

(b) Number of groups increase at each scheduling step

Figure 3.4: Joint power control and scheduling algorithm

- The complexity of the algorithm should be independent from the size of the rate set
- Each power control subgroup should have a convex rate region
- None of the nodes should suffer from severe unfairness

We exploit convergence of a Lagrangian based power control algorithm in grouping nodes and splitting the channels. Figure 3.4 show the scheduling algorithm; how nodes are grouped and where we split the channel in time domain. The power control process starts from the entire node group C. When the power control algorithm converges, the nodes in active transmission are grouped to C_1, and the nodes turned off after the power control process initiates the scheduling process. The scheduling process splits the time slot in half by broadcasting a channel split request message. Then the second node subgroup C_2 is organize. The power control algorithm continues to run on subgroup C_2 and produces another subgroup C_3 when any node in C_2 converges to zero transmission power. The scheduling process continues until none of the nodes have zero transmission power, and the channel is equally divided into k channels in time domain.

In the power control process, links under high interference from transmitters of other links are usually turned off as their utility function is hard to grow compared to other links, and the

Table 3.1: 802.11a radio reception thresholds: Receiver performance requirements ($PER = 10^{-3}$)

Data rate	Modulation	Coding rate	Threshold
6 Mbps	BPSK	1/2	-82 dBm
9 Mbps	BPSK	3/4	-81 dBm
12 Mbps	QPSK	1/2	-79 dBm
18 Mbps	QPSK	3/4	-77 dBm
24 Mbps	16QAM	1/2	-74 dBm
36 Mbps	16QAM	3/4	-70 dBm
48 Mbps	64QAM	2/3	-66 dBm
54 Mbps	64QAM	3/4	-65 dBm

system recovers its feasibility by turning a number of links off. This is not an optimal solution because the amount of utility is not considered in the process of the decision for scheduling. However, the scheduling algorithm is simple and fully distributed. The algorithm operates in each node without any coordination among nodes, and it performs reasonably well compared to the optimal scheduling cases requiring global knowledge of the networks. By allowing time division multiplex and power control simultaneously, we can efficiently increase both the fairness and the network throughput of the Wi-Fi Ah-hoc system.

3.4 Simulation Result

The channel model used in the simulation is the log-distance path model in (3.9) with a path-loss exponent value of $\zeta = 4$.

$$L = L_0 + 10\zeta \log_{10} \frac{d}{d_0} \tag{3.9}$$

Thermal Gaussian noise on the receiver antenna front-end can be found by the Boltzmann equation, $N = kTB$, where k stands for the Boltzmann's constant equals to $1.38065 \times 10^{-8} [J/K]$, T is the effective temperature in Kelvin, and B is the Bandwidth.

Table 3.1 shows the reception threshold of 802.11a radios for each data rate. Depending on

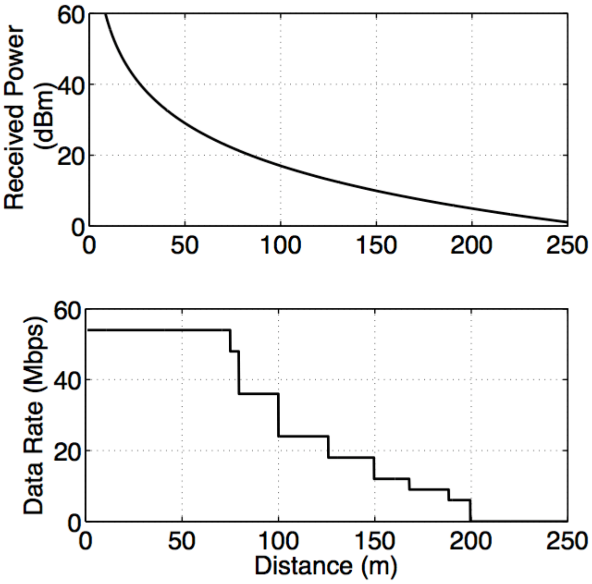


Figure 3.5: Distance and data rate: Maximum communication range is set as $200\mathrm{m}$ with maximum transmission power set as $\bar{p}_i = 18\mathrm{dBm}$

the modulation schemes and convolutional coding rate, the sensitivity over noise and interference is determined. The thermal Gaussian noise N_i in each receiver incorporates $10\mathrm{dB}$ noise figure and $9\mathrm{dB}$ loss margin, which adds up to $-87\mathrm{dBm}$. Based on the channel model in (3.9), the resulting distance and data rate relationship of ideal 802.11a radios is shown in Fig. 3.5.

In this chapter, we demonstrate the performance of the proposed JPSA through simulations. Because both the network throughput and the fairness of user are important, we uses a new metric in quantifying the performance of the proposed algorithm. The performance of the algorithm, P, is measured by multiplying the fairness of user throughput and the aggregate network throughput. The fairness is the average value of the Jain's fairness index over the link throughputs, t_i, in a network of total L links.

$$\text{Performance}(P) = \sum_{i}^{L} t_i \times \frac{(\sum_i^L t_i)^2}{L \sum_i^L t_i^2} \tag{3.10}$$

3.4.1 Power control only versus Scheduling only

Figure 3.7 shows the simulation result for the example of 5-link topology illustrated in Fig. 3.6. The transmission powers of l_1, l_2, and l_4 converge to the value that maximizes the sum of data rates of all links. However, l_3 and l_5 experience serious unfairness as they are completely turned off. If the deactivated nodes are turned on to alleviate the fairness problem, then the system becomes unstable and the power control algorithm diverges to the maximum values resulting in a situation where none of the links get any reasonable throughput.

In this topology, the throughput of a simple power control method is 84Mbps, and the ideal throughput of the contention based CSMA MAC of 802.11 system is 49.2Mbps. The ideal CSMA MAC is identical to the ideal TDMA system as it assumes zero overhead from collisions and back-off processes. In terms of aggregate throughput, TDMA based MAC that only schedules transmission of nodes performs much worse than a power control mechanism with a rate adaptation. However, the system based on the power control mechanism has a serious problem in the fairness as some of links are simply turned off to increase the aggregate network throughput.

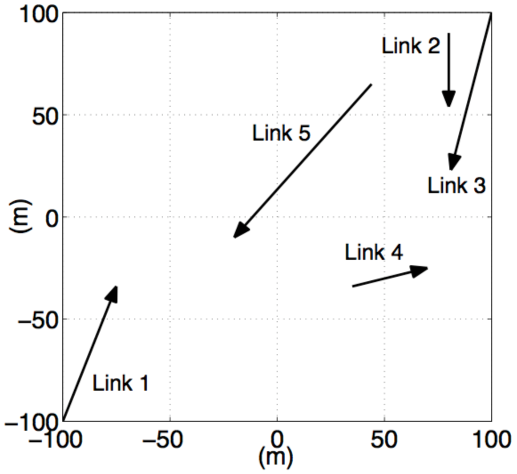


Figure 3.6: Example topology: Five links

3.4.2 Performance of JPSA: Comparison with fair scheduling algorithm

The proposed JPSA can solve the fairness problem caused by the feasibility issue in the utility based power control algorithm. By grouping links to reduce mutual interference and by assigning different slots for each of groups while simultaneously controlling the transmission powers of the links, it is possible to achieve gains in both the aggregate network throughput and the fairness in each individual throughout of the users.

In Fig. 3.8, we compare the performance of JPSA over the TDMA, which provides fair time

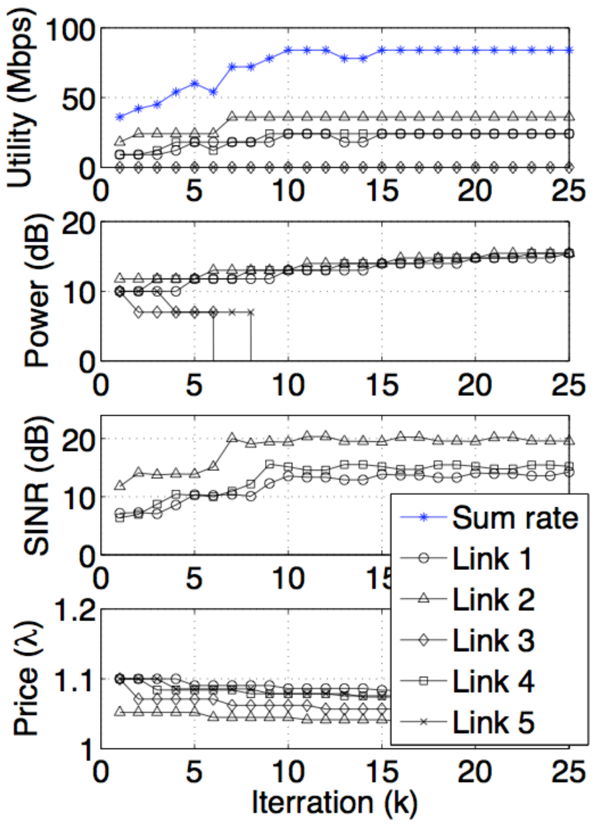


Figure 3.7: Power control with a rate adaptation

sharing of the channel without power control to all nodes. We generated $5,000$ random topologies in $1000 \times 1000\text{m}$ space, and the s_i - r_i distance is limited at $50 - 150\text{m}$. As discussed in the previous section, JPSA shows better performance in aggregate network throughput while TDMA shows better fairness. However, in terms of the joint performance P, which is a combined performance of both the network throughput and fairness, JPSA performs far better than TDMA especially for the topologies that JPSA converges to small number of subgroups.

Figure 3.8: Performance comparison with Time division access (TDMA) : 5 Links topology

3.4.3 Performance of JPSA: Comparison with optimal scheduling algorithm

Depending on the topological conditions and mutual interference levels, the optimal number of subgroups maximizing the network aggregate throughput varies. In JPSA, the selection of the number of subgroups and the node assignment for each group is made in a greedy way until all the nodes in the network have positive transmission power. As JPSA is a suboptimal algorithm, there exists a performance gap in the optimal scheduling method that ideally selects the group size and subsequently assigns nodes to each groups for maximum throughput. In this research, the optimal performance is determined by an exhaustive search algorithm that runs the power control algorithm for all the different combinations of group assignment cases, which assumes a central coordinator with a global knowledge of the network.

In Fig. 3.9 the performance of JPSA is compared with the optimal performance that can be achieved. This figure is drawn from $1,200$ cases that JPSA converges into 3 subgroups, and its performance is then sorted according in a descending order of the optimal performance. This figure shows the gap between the optimal scheduling performance and JPSA. We also compare the performance of JPSA to the fair time sharing TDMA performance without power control in Fig. 3.10, which is sorted in descending order of TDMA performance.

JPSA performs lower than the optimal scheduling algorithm. However, considering the complexity of algorithms and the amount of message exchanges required, JPSA performs reasonably well when compared to TDMA MAC.

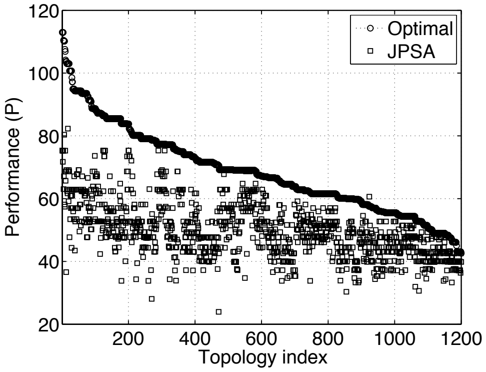


Figure 3.9: Performance comparison with an optimal scheduling algorithm: 5 Links topology

3.5 Conclusions

In this chapter, we introduce a joint scheduling and power control algorithm for Wi-Fi Ad-Hoc systems. Considering the need for peer-to-peer communications among mobile devices and the popularity of Wi-Fi radios, it is meaningful to increase the network throughput for users in a peer-to-peer mode by a relatively simple and distributed power control algorithm based on

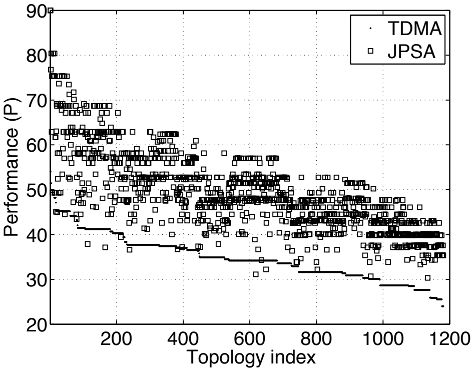


Figure 3.10: Performance comparison with a fair channel scheduling algorithm (TDMA): 5 Links topology

implicit coordination technique. To solve the fairness problems that arise in the power control mechanism, we introduce a simple greedy scheduling algorithm,*JPSA*, which is non-optimal, but performs reasonably well even without the need for information exchange on the mutual status between nodes. The proposed *JPSA* has a linear complexity with a number of nodes and is independent from the number of rate set. Through the proposed coordination algorithm, in addition to the gains of network throughput, individual users can extend their battery usage time, especially for energy constrained wireless devices.

Our contribution can be summarized as follows.

- We show that the potential capacity expansion of Wi-Fi radios in Ad-Hoc mode is highlighted, which can be enabled by coordination of transmit time and power scheduling.
- We show that the complicated joint power and scheduling problem can be efficiently solved by applying primal-dual decomposition methods that exploits implicit coordination technique.

Chapter 4

Implicit Coordination for Cooperative Location Privacy Protection

4.1 Introduction

Technology trends are leading to an increasing number of wireless transmitters that move around with us as we go about our daily lives. Many of these transmitters are virtually always on—they send messages for push email, handoffs, or sensor status updates even without any explicit user action. At the same time, widely available radio hardware is becoming increasingly flexible and openly programmable. Such hardware significantly lowers the bar for an adversary to intercept and decode wireless signals.

While message content can usually be protected through encryption, any transmitted signal will expose information about the location of the transmitter. Even without decoding, any of the transmitted bits, adversaries can use a variety of well-known localization techniques to determine the position and track the movements of a user. Examples of such techniques are Received Signal Strength (RSS) Fingerprinting [18, 97], Time-Of-Arrival (TDOA) [16], or Angle-Of-Arrival (AOA) [98] localization. Thus, emitting wireless signals can be misused to cause significant threats to people, property, or might be a nuisance to individuals in form of unwanted and bothersome activities.[1] In such cases, even a relatively small amount of confusion (tens of meters) about a position can sometimes lead to significant privacy gains—it would hide which store a person entered, or which room a VIP is located in, for example. Moreover, even if identifiers are removed or encrypted, such tracking still creates privacy risks since identity can often be inferred if a device can be tracked over longer period of time (for example, through face recognition on video surveillance cameras). Even a relatively small amount of confusion (tens of meters) about a persons position can sometimes lead to significant privacy gains—it

---

[1] FootPath system reportedly allows tracking the movement of cell phones in shopping malls [99].

would hide which store a person entered, or which room a VIP is located in, for example.

However, existing techniques can only provide very limited protection against such attacks on location privacy at the physical layer. Transmit power randomization [100] can throw off standard localization systems, but localization algorithms can easily filter out such changes by applying differential RSS techniques [101]. Although using directional antenna can improve user location privacy by changing RSS information on adversary sensors [102], its physical size and the requirement for antenna steerability pose design problems in portable mobile devices. In military communications, frequency hopping or code spreading techniques [103] are widely used to prevent jamming and eavesdropping on signals. These are not compatible with most commercial radios and are less effective for protecting location privacy, since it is not necessary to follow the hopping sequence of the transmitter. Receiving any part of a transmission on any one frequency is usually sufficient for localization.

In this chapter we propose two cooperative location privacy protection techniques in radio physical layer. We consider that coordination for locational privacy can induce overhead communications among the coordinated nodes, which can, on the contrary, threaten their location privacy inducing counter attack from adversaries. Hence, we apply implicit coordination technique to allow more secured coordination between coordinated nodes while minimizing the communication overhead.

Cooperative Location Cloaking We design a simple but robust noise injection technique that utilizes friendly neighboring nodes as cooperative jammers. Users cloak their location through the jamming signals transmitted from cooperators to obfuscate RSS or TOA information used by adversary sensors. While this jamming technique is quite intuitive, in-depth analysis should be made to consider the impact on radio link performance. We firstly identify the trade-offs relationship between throughputs and location privacy in wireless communication channels using Cramer-Rao Lower Bound (CRLB), which determines the theoretical limits on the accuracy of localization attacks from adversaries. We identify the tradeoff relationship between location-privacy and performance in wireless communications. Moreover, for to minimize the risks due to communications for coordination, we introduce a novel Multi Cooperator Power Control (MCPC) technique exploiting an implicit coordination technique based on primal-dual decomposition technique. In MCPC, users can set a threshold for throughput loss, and then cooperative jammers implicitly control their jamming signal strength within the threshold level, thereby maximizing their aggregate jamming power. The algorithm is fully distributed and secure since jammers do not transmit any message packet, which might possibly disclose their locations.

Cooperative Location Cloning: *Phantom* provides physical layer location privacy protection by creating a number of phantom locations around the true locations of users. Contrary to cooperative cloaking that drives adversaries have noisy estimation on the user location, *Phantom* protects the location privacy by creating a larger number of ghost locations. The cooperating nodes in *Phantom* synchronizes their transmissions so that their signals arrive at adversary receivers within normal multipath delay spreads and are hard to distinguish from regular multipath effects. Thus, intuitively, this technique creates stronger multipath effects that affect the accuracy of localizations techniques. One important part of *Phantom* is a collaboration protocol that allows multiple nodes in proximity—for example a VIP's phone and additional devices carried by the personal security detail—to transmit such simultaneous messages. We apply a implicit coordination technique using pseudo random generators to allow cooperating nodes to synchronize their transmission time and control transmission power.

The remainder of this chapter is organized as follows: In section 4.1.1, we review existing related work on location privacy protection at the physical layer. In section 4.2 we propose a multi-node cooperative jamming technique, and present simulation results. In section 4.3, we introduce *Phantom* and its collaboration protocol, and we explain our experiments in creating dummy locations using actual radio modules. Finally, we draw conclusions in section 4.4.

4.1.1 Related Work

A great deal of research effort on location privacy has been expended in the past decade. However, most efforts have focused on techniques preventing unintended disclosure of user location information collected at the MAC layer and above by filtering or obfuscating the true position data (e.g., [104, 105, 106]). Attacks to location privacy through passive location estimation techniques using physical layer RSS [97, 107], TOA [16], or angles from AOA [98] information have received less attention.

Such low level attacks on user location privacy are hard to protect against since manipulating the signal at the physical layer directly affects the radio performance. Conventional secure communications techniques are also not effective in protecting the location privacy of users from such attacks. For example, the frequency hopping technique cannot prevent the adversary from measuring needed information (such as RSS or TOA) from user transmitted signal, since the adversary only needs to keep monitoring a fraction of frequency to obtain a short signal useful for location estimation. In code spreading methods, using pseudo-random code is no longer secure due to various attack algorithms exploiting its auto-correlation properties [108, 109, 110, 111]. We review a number of existing techniques based on direct signal obfuscation methods, which mainly focus on lowering the accuracy of adversary location estimations.

Jiang et. al. [112] suggest a method that forces wireless nodes to reduce transmission power in order to minimize the number of adversary sensors detecting their RSS values. On the other hand, El-badry et. al. have introduced a protocol where anchor nodes dynamically change their transmission powers to prevent unauthorized nodes localizing their locations [113]. They have also proposed a method where transmitters add noise to their transmitting signal to prevent the precise adversaries' RSS measurements while sacrificing their own link throughput. These approaches are simple but not effective when adversaries install a sufficient number of sensors for the detection and estimation of the signal transmitted from the target nodes.

Beamforming technique [114] using an array antenna can be an alternate solution for such a mechanical steering problem, However, the gains on location privacy protection from beamforming antennas is not yet proved, since its directional antenna gains can be easily averaged out in mobile environments where the phases of the transmitted signal from an antenna array dynamically change over time and space. Using directional antennas can improve user location privacy by forging RSS information on adversary sensors [102]. However, directional antennas need to be physically steered to the direction of receiver nodes, which requires a mechanical steering module. Also the size of directional antenna can pose design problems in portable mobile devices.

4.2 Cooperative Cloaking: Jamming for Location Privacy Protection

When an adversary localization system tries to find the location of the sensors nodes, the attacks from the adversary can be made in a completely passive manner using the information measured from the received signal. However, it is difficult to obfuscate PHY information without degrading the quality of wireless communications. Transmitting noise-like jamming signals from a third cooperative node can obviously help nodes obfuscate the PHY information, by inducing estimation errors to the adversary's localization systems. However, such a jamming technique has the problem of interfering with the communication between transmitters and receivers, thereby reducing the overall communication throughput of the network. Although applying beamforming antenna techniques or adding filterable pseudo-random noise can alleviate such interference problems, those techniques generally induce coordination problems or require encryption of the entire signal including pilots and preambles, which also degrade the radio performance.

4.2.1 The Positive Role of Jamming in Location Privacy

Self-jamming techniques, such as the transmitters randomly changing transmission power or lowering transmission power to minimum, can be easily detected or estimated by adversaries since all of their sensors are uniformly affected by the change of transmission power of a target transmitter node (TX). Hence, we propose a cooperative jamming method that exploits neighbor nodes of TX as cooperative jamming nodes (COP). Figure 4.1 shows an example scenario of cooperative jamming. In the figure, TX obfuscates its TOA and RSS information through the transmission of a jamming signal from one of its COPs. The jamming noise can be either white Gaussian noise like wide-band signal or low power dummy data packets, which decreases the received signal quality on adversary sensors $\mathbf{s} = \{s_1, s_2, \cdots, s_8\}$. Specifically for the adversaries using TOA information (TOA adversary), jamming noise from COPs lowers the estimation accuracy on the adversaries' TOA estimation since TOA estimations are largely dependent on the received signal quality. Also, the jamming noise induces estimation errors for RSS adversaries, who are localizing TX based on the measured RSS values from TX, by inducing errors to the adversaries' RSS measurements.

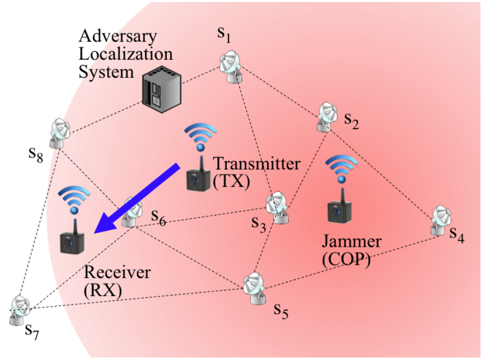


Figure 4.1: Cooperative jamming for location privacy protection

We briefly explain how the jamming noise affects the location privacy of nodes, which is measured by the accuracy that the adversary can achieve on the location of target nodes. The accuracy of location estimations of adversary localization systems using TOA measurements depends on the Signal to Interference and Noise Ratio (SINR) of the received signal and Non-Line Of Sight (NLOS) signal components [115]. Hence, we use the CRLB, $||\sqrt{\sigma_{\hat{u}}}||[\mathrm{m}]$, on the target location, $u = \{x, y\}$, as a privacy measure at given topology and SINR conditions where $\sigma_{\hat{u}}$ is the CRLB on u. The *Fisher Information Matrix (FIM)*, J_u is used to find $\sigma_{\hat{u}}$, which can be induced from the probability density function, $f_u(r)$, on the observation, r, in (4.2) [116].

$$\sigma_{\hat{u}} \geq J_u^{-1}, \tag{4.1}$$

$$J_u = E_u \left\{ \frac{\partial}{\partial u} \log f_u(r) \cdot \left(\frac{\partial}{\partial u} \log f_u(r) \right)^T \right\}. \tag{4.2}$$

The FIM, J_u, depends on the precision of time estimation whose variance is bounded by the SINR, γ, of the received signal ($\sigma_{\tau^2} \geq \frac{1}{8\pi^2 f_b^2 \cdot \gamma}$) [115]. Jammers lower the SINR conditions at the adversary sensors, thereby inducing errors to their localization system. Compared to the typical NLOS multi-path components which can be filtered out through extensive calibration in the training process, our approach using jamming noise can be easily filtered out unless the locations of COPs and the their jamming powers are known to adversary.

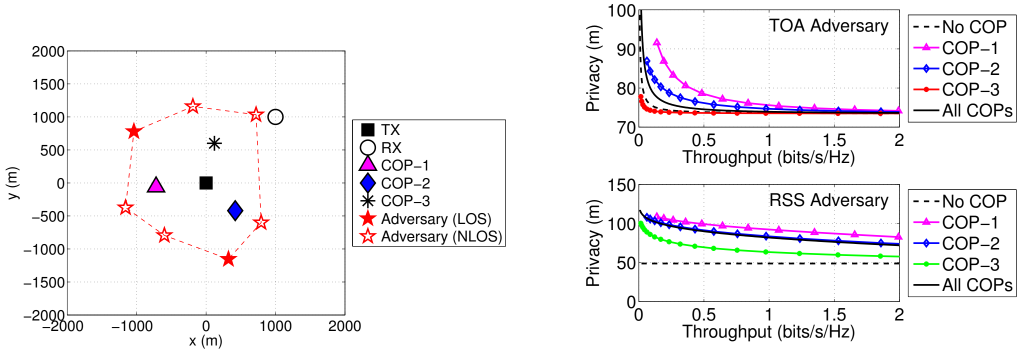
The jamming noise from COPs also affects the RSS measurement of the adversary sensors. Typical radios find RSS by subtracting background noise power from the measured aggregate signal power, where the background noise power is measured in a calibrating process [117]. Therefore, the jamming noise increases RSS estimation values at adversary sensors since the energy of the received signal increases due to the added noise power. When adversary sensors measure wrong RSS information, their estimation on the location of TX will be incorrect. For RSS adversaries, FIM, J_u, depends on the variation of the RSS measurement which is heavily dependent on the channel variations due to fading. Typically small scale fading can be averaged out, hence shadowing is a major factor that affects the accuracy of localization systems. The shadowing from terrain can be overcome by calibrating accurate RSS maps in the target area. However, the RSS variation induced from unknown COPs is hard to be filtered out. We define the level of location privacy using CRLB on the location estimation from the adversary. The details on the analysis method based on CRLB and the parameter values used in our simulations are presented in the Appendix.

4.2.2 Single- and Multi-node Jamming

Next, we explain the tradeoff relationship between throughput and location privacy, then show how single or multiple cooperative jamming technique improves the location privacy of wireless nodes. An example topology with 7 adversary sensors is shown in Fig. 4.2(a). Depending on the transmission signal power of TX and the jamming power of COPs, throughputs and location estimation errors from the adversary localization system change. The throughput of TX, $C = \log_2(1+\gamma)\,[bits/Hz/s]$, is determined from the SINR between TX and RX,$\gamma_0(\boldsymbol{p}) = \frac{p_{TX}h_{TX}}{\sum_i^M p_i h_i + N}$. We denote the transmission power of TX as p_{TX}, TX to RX channel gain as h_{TX}, the jamming powers from M COPs as $\boldsymbol{p} = \{p_1, p_2, \cdots, p_M\}$, i_{th} COP to RX channel gain as h_i, and noise floor as N.

We first assume only one out of three COPs transmits jamming noise signal. In such a case, the location privacy of TX is dependent on the location of the COP transmitting a jamming signal.

In Fig. 4.2(b), we can find that using COP-1, which is close to adversary sensors and away from RX node, is the best strategy maximizing the privacy gain, which is measured by the location estimation error from the adversary. On the other hand, the performance of using all three COPs at the same time is not as good as using a single best COP. However, using multiple COPs can be more reliable since it can provide consistent location privacy gain, when the location of adversary sensors is unknown. Also, relying on a single COP may enable the



(a) Example topology.

(b) Throughput and Privacy Tradeoff.

Figure 4.2: Example of cooperative jamming scenario; path-loss exponent:$\eta = 3$, Receiver noise floor:$N = -101\mathrm{dBm}$, Bandwidth:$f_b = 10\mathrm{MHz}$.

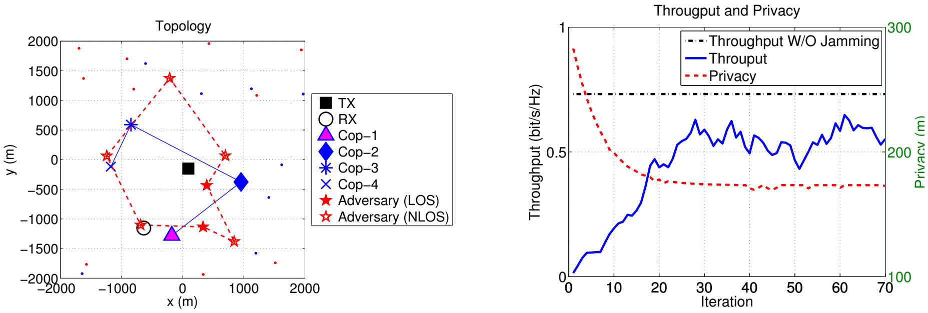
adversary to trace back the location of the jamming signal source.

To minimize exposure to adversary sensors, all COPs have to know the precise transmission time and duration of message transmission of TX. We assume that the transmission time is pre-scheduled, and neighboring node lists are previously determined so that TXs and COPs synchronize their transmission time. Such information can be pre-configured before the nodes are deployed in the area, or it can be broadcast through a secured channel. During the time assigned, each node continuously transmits its message packets to its receiver node while its pre-assigned COPs transmit jamming signals.

4.2.3 Multi Cooperator Power Control (*MCPC*) Jamming for Location Privacy

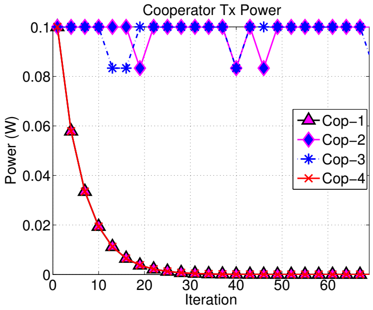
The locations and jamming signal powers of COPs determine both the TX-RX link throughput, and the location privacy of TX. Although multiple low power jammers are used, some of them might be located at the positions inducing too much interference to the RX node. However, it is not possible to determine the proper jamming signal strength without exchanging messages explicitly for coordination, since transmitting coordination messages can expose the location of both the TX and COPs to the adversary.

We, therefore, propose the Multi Cooperator Power Control (*MCPC*) algorithm for the protection of location privacy of COPs nodes while ensuring their control of jamming power power. Using a one-way single broadcast feedback channel from RX, COPs adjust their jamming power to guarantee a certain level of link throughout for TX while maximizing their



(a) Example topology

(b) Throughput and privacy tradeoff



(c) Jamming power change at each COP

Figure 4.3: NUM-based distributed jamming power control method; $p_{TX} = 20\text{dBm}$, $\alpha = 0.25$, Ricean fading.

jamming efficiency to the adversary sensors. Although the feedback channel from RX can expose the location of RX, we can minimize the risks of revealing the location of RX through an asymmetrical feedback channel that is low rate and low power. One example scenario is that RX has a mobility, therefore less sensitive to the localization attacks from adversaries, e.g., RX is a ferry node collecting data from scattered stationary nodes.

For better location privacy protections, the jamming powers of COPs should be maximized while the link throughput C is guaranteed at certain level. To that end, a manually tunable parameter α, with ($\alpha < 1$), is introduced to allow COPs flexibly trade throughput for privacy. Specifically, α is a user-defined threshold for acceptable throughput degradation due to jamming. We formulate this problem as a Linear Programing (LP) problem in (4.3), then apply the primal dual decomposition method to solve the problem in a distributed way [85].

$$\begin{aligned} \text{maximize} \quad & \sum\nolimits_{i=1}^{M} p_i \\ \text{subject to} \quad & \gamma_0(p_{TX}, \boldsymbol{p}) \geq (1-\alpha) \cdot \gamma_0(p_{TX}, \boldsymbol{p}=0), \\ & 0 \leq \boldsymbol{p} \leq \bar{\boldsymbol{p}}. \end{aligned} \tag{4.3}$$

Using M cooperative jammers, the optimization variables are the jamming powers of COPs, $\boldsymbol{p}$, which are limited by maximum jamming signal transmission power $\bar{\boldsymbol{p}}$. We assume the transmission power of TX, p_{TX} is fixed, but the M COPs control their jamming power $\boldsymbol{p}$ to ensure that the SINR condition between TX-RX is larger than a certain throughput threshold set by α and SNR without a jamming signal ($\gamma_0(p_{TX}, \boldsymbol{p}=0)$). Then the constrain on SINR in (4.3) can be rewritten as $\sum_{i=1}^{M} p_i h_i \leq \alpha'$ for $\alpha' = N(\frac{\alpha}{1-\alpha})$.

We apply a Lagrangian multiplier λ and rewrite (4.3) as (4.4)

$$L(\boldsymbol{p}, \lambda) = \sum\nolimits_{i=1}^{M} p_i - \lambda \left(\sum\nolimits_{i=1}^{M} p_i h_i - \alpha' \right). \tag{4.4}$$

Then the dual problem can be solved by finding the minimum of $D(\lambda)$ in (4.3)

$$\begin{aligned} D(\lambda)_{(\lambda \geq 0)} &= \max_{\boldsymbol{p}} \left\{ \sum\nolimits_{i=1}^{M} (1 - \lambda h_i) p_i \right\} + \alpha' \lambda \\ &= \sum\nolimits_{i=1}^{M} \left\{ \max_{\boldsymbol{p_i}} (1 - \lambda h_i) p_i \right\} + \alpha' \lambda. \end{aligned} \tag{4.5}$$

Now the problem is decomposed into M sub-problems in (4.5), which are implicitly solved by each COP using the shadow price λ that is updated by RX using a feedback control channel. The shadow price λ is updated at each iteration by (4.6) using a gradient value $\frac{D(\lambda)}{\partial \lambda} = \sum_{i=1}^{M} h_i p_i - \alpha'$ where $[z]^+ = max\{0, z\}$ and δ is a small number adjusts the speed of convergence.

$$\lambda^{(n+1)} = [\lambda^{(n)} \left(1 + \delta (\sum\nolimits_{i=1}^{M} h_i p_i - \alpha' \right)]^+. \tag{4.6}$$

Using the updated price λ, each COP determines its jamming power p_i.

$$p_i^{(n+1)} = [arg\max_{p_i} (p_i - \lambda h_i p_i)]^+. \tag{4.7}$$

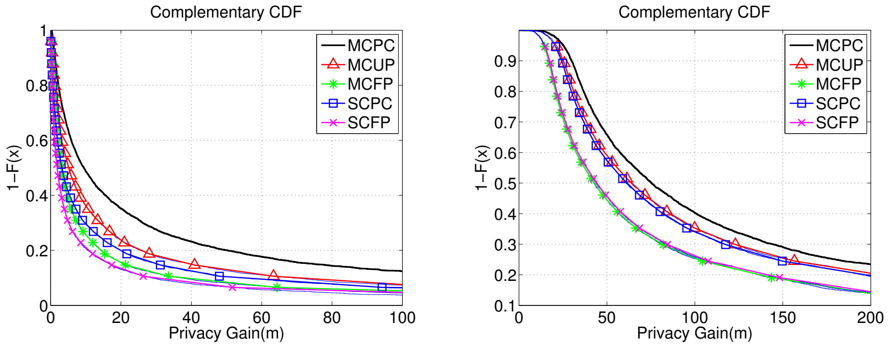
At each iteration, since each COP makes a greedy choice to maximize its own utility value $(p_i - \lambda h_i p_i)$, its transmission power abruptly changes between 0 and $\bar{p_i}$. Hence, we only allow a small power change of Δp in each iteration for slow but reliable convergence of power value considering unstable channel conditions due to fading.

Note that this distributed power control algorithm does not need any feedback from COPs. Since COPs passively estimate their channel gain to RX, h_i, from the feedback channel (from RX), their location privacy is preserved. In updating λ, RX only needs to know the sum of interference from COPs ($\sum_{i=1}^{M} h_i p_i$), which can be calculated from its SINR measurement, $\gamma_0(\boldsymbol{p}) = \frac{p_{TX} h_{TX}}{\sum_i^M p_i h_i + N}$. TX sends the values of p_{TX} and h_{TX} to RX, which can also be measured from the feedback channel from RX. Although RX has a mobility, the algorithm is fast (only 20 iteration is needed in the simulation) enough to catch up the variation of the channel.

We show in Fig. 4.3 an example topology when $M = 4$ (4 COPs). COPs start with transmitting maximum jamming noise signal to protect the location privacy of TX in the initial stage of the algorithm, then gradually reduce their power at each iteration according to (4.7). Due to small scale channel fading, the channel conditions dynamically change over time, but as shown in Fig. 4.3(c), the jamming power in each COP gradually converges to a point that maximizes the sum of jamming powers while satisfying the constraints on the throughput loss. Note that the proposed distributed jamming power control algorithm automatically penalizes the jammers close to RX (COP-1 and COP-4) since their interference to RX is much stronger than other COPs (COP-2 and COP-3), which is better to achieve higher throughput. Therefore, in general cases where adversary locations are unknown, the proposed distributed power control algorithm performs better than other methods, such as randomly selecting a COP or uniformly changing jamming powers.

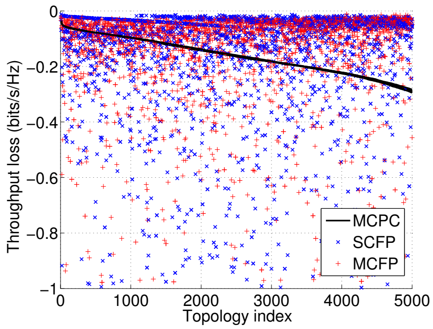
4.2.4 Performance of Multi-node Implicitly Coordinated Jamming Method

Through simulations, we compare a number of jamming-based location privacy protection methods with the proposed *MCPC* jamming method. We run simulations for 5000 random



(a) Privacy performance for TOA adversary.

(b) Privacy performance for RSS adversary.



(c) Throughput comparison with fixed transmission power methods.

Figure 4.4: Privacy performance measured by complementary cumulative distribution function; Jamming power for *SCFP* and *MCFP* are fixed as $9\mathrm{dBm}$ and $6\mathrm{dBm}$.

topologies created with the sizes of $10\mathrm{km}$ by $10\mathrm{km}$ network. 100 nodes are uniformly located in every $1\mathrm{km}$ by $1\mathrm{km}$ grid with 2-dimensional random offset of $500\mathrm{m}$, and 100 adversary sensing nodes are also co-located in the same manner. TX is selected as the closest node to the center of the network, and its RX is randomly selected from the 5 closest nodes to TX, and the rest 4 nodes become COPs. Adversary sensors are the 7 closest nodes to TX among the 100 adversary sensors in the network, and 2 of them are assumed to have LOS link to TX. The throughput loss threshold set to be $\alpha = 0.25$.

The jamming-based location protection algorithms we simulated are summarized as follows;

- Multi Cooperator Power Control (*MCPC*): The jamming power of COPs are controlled by the proposed distributed multi-node power control algorithm satisfying the link throughput loss threshold α.

- Multi Cooperator Uniform Power (*MCUP*): The jamming power of COPs are uniformly adjusted according to the feedback from RX to guarantee the link throughput loss threshold α.
- Multi Cooperator Fixed Power (*MCFP*): The jamming power of COPs are fixed regardless of the link throughput.
- Single Cooperator Power Control (*SCPC*): Use a single COP. The closest node to TX is RX, and the next closest node is COP. The jamming power of COP is adjusted according to the feedback from RX to guarantee the link throughput loss threshold α.
- Single Cooperator Fixed Power (*SCFP*): RX and COP are same as *SCPC*. However, the jamming power of COP is fixed regardless of the link throughput condition.

For a fair comparison, the fixed transmission powers for *SCFP* and *MCFP* are selected as a value that provides the same average TX-RX link throughput with *MCPC* for overall topology conditions. We measure the privacy gain by calculating how much location privacy is improved compared with the cases without jammers. Figure 4.4 shows the simulation results. The performance is measured by a complementary cumulative distribution function $(1-F(x))$, which indicates the probability that the privacy gain is above a particular privacy gain level. the proposed *MCPC* outperforms other baseline techniques. We can find that simple uniform power control methods marginally improve location privacy compared to fixed jamming power methods; even the fixed power values are reasonable well chosen to provide similar throughputs with *MCPC*. We can also find that multi-node jamming methods does not perform significantly better than single-node jamming methods for overall network environments. In the simulation result, the gains against TOA adversary is not significant compared to the scenarios for RSS adversary. However, note that the results we have shown through simulations are lower bound of the estimation errors that we can additionally introduce to adversary localization systems using cooperative jamming technique. The actual privacy gain we can obtain in real networks is mainly dependent on the radio environmental situation, such as path-loss, multi-paths, and obstacles, of the networks. Hence, the expected amount of privacy gains in real networks will be much higher than lower bound we measured in our results.

Figure 4.9(c) shows the throughputs in fixed power methods compared to *MCPC*. Since fixed jamming methods do not consider the link throughputs, their throughput loss and privacy gain is very unstable depending on topological conditions. Therefore, they should be carefully calibrated before nodes are deployed in the target area considering the channel conditions and the distances between nodes.

4.3 *Phantom* : Location Cloning for PHY-Location Privacy Protection System

In this chapter, we design, implement and evaluate Phantom, which provides physical layer location privacy protection by creating a number of fake ghost locations around the true locations of users. The key insight behind *Phantom* is that a group of collaborating nodes mislead a location inferencing system. It achieves this by having the cooperating nodes transmit the same signal simultaneously that make the inferencing system believe that the actual nodes are located in certain ghost locations. We design a coordinating protocol that allows cooperating nodes are implicitly coordinated for their synchronized transmissions arrive at receivers within normal multipath delay spreads are indistinguishable from regular multipath components. Thus, intuitively, *Phantom* creates stronger multipath effects that affect the accuracy of localizations techniques. We demonstrate that multi-transmitter cooperative transmission is possible using software-defined radios within the 802.11g radio standard that is currently widely used. Using an indoor test-bed, we show how ghost nodes are created in adversary localization systems and evaluate the location privacy gain that can be achieved depending on the selection of transmission power levels from two cooperative transmitters.

We show in Fig.4.5 an example scenario where *Alice* is accessing the Internet through a wireless access point (AP) and the adversary *Eve* is trying to determine her location using a RSS-based fingerprinting technique [18]. We focus on RSS-based localization systems in this chapter since they are easily implemented and outperform TOA- or AOA-based techniques in multi-path environments [118].[2]

---

[2] Although we do not discuss the details on TOA and AOA-based localization techniques in this chapter, *Phantom*

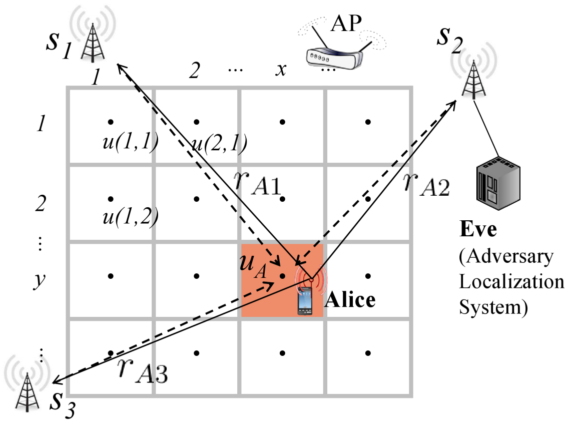


Figure 4.5: Adversary localization systems tracking users.

As typical in RSS fingerprinting techniques, we assume that the adversary *Eve* has obtained a RSS signature database. This database contains the RSS values, $R_u = \{r_1, r_2, r_3\}$, received at *Eve's* radio signal sensors, $S = \{s_1, s_2, s_3\}$, for target transmissions from each of the reference locations $u(x_i, y_i), i \in C$, where C is reference location set. During actual localization, *Eve* measures the signal strength from *Alice's* radio transmission at each of the sensors in S, yielding $R_A = \{r_{A1}, r_{A2}, r_{A3}\}$. She then estimates the location of *Alice*, (u_A), as the reference location that minimize the square error $(arg\ min_i ||R_A - R_u(x_i, y_i)||^2, i \in C)$. The accuracy of *Eve's* location estimation is affected by the granularity of the grid reference points and RSS variations due to shadow and small scale fading, among other factors. Note, that *Alice* could simply change her transmission power to cause errors in the mean square error estimation, but *Eve* can easily compensate the change power value by searching for a best match over several possible scaled value of R_A. We now describe a countermeasure that cannot be circumvented with this simple scaling technique, since it does not uniformly affect the signal at all sensors.

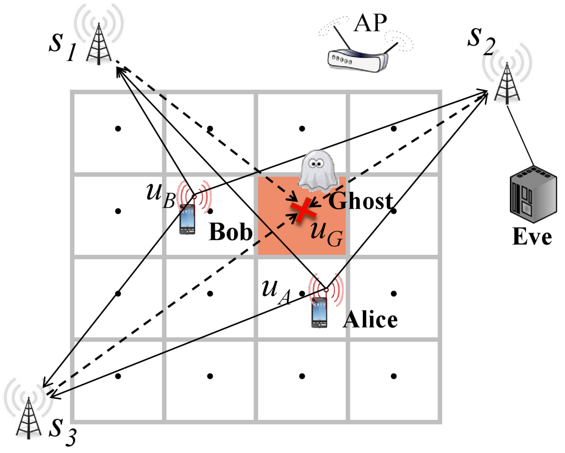
4.3.1 Location Privacy Protection through Ghosts Creation

Phantom protects the location privacy of wireless users by jointly transmitting signals from multiple cooperating nodes, say *Alice* and *Bob*. By creating many ghost locations to adversary localization systems thorough paired cooperators, *Phantom* improves the location privacy from adversary tacking systems. Figure 4.6(a) illustrates two users, *Alice* and *Bob*, jointly transmit

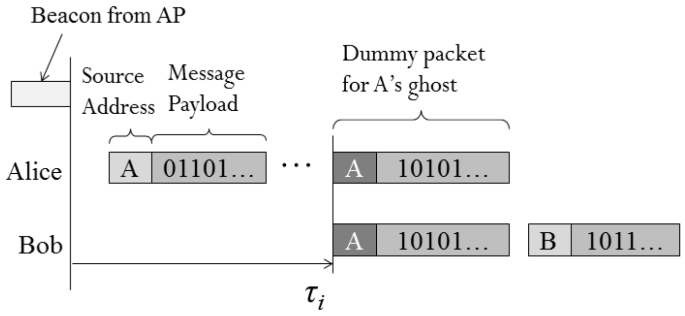
---

can also create ghosts against those adversary techniques by obscuring their TOA and/or AOA measurements.

signals and the combined signal is interpreted by the adversary, *Eve*, as if the signal is transmitted from another node, ghost, at different location. The signal received at an adversary sensor creates a different shift in the RSS at each sensor. Thus, the adversary cannot simply rescale all sensor values by a common factor—the best match is likely to somewhat randomly fall on a different reference location. This creates the appearance that a transmitter is located at other locations, which we refer to as a ghost location. By modulating their transmit powers *Alice* and *Bob* can create different ghost locations and thus cause confusion about the number of real transmitters and their locations. Note that compared to other anonymization techniques using cooperators (e.g., MAC masquerading in 802.11 networks), the performance of *Phantom* is not limited by the number and the mobility of cooperators.



(a) *Alice* and *Bob* cooperate for ghost creation



(b) Dummy packet transmission for ghost creation

Figure 4.6: Adversary localization system tracking ghost instead of real users.

When the cooperator *Bob* transmits the same packet as *Alice*, then the measured signal energy at the adversary sensors, $\{s_1, s_2, s_3\}$, is a combination of received signals from both nodes

($p_r \approx p_{w1} + p_{w2}$). As the result, the dummy packets that they simultaneously transmitted from the two nodes induce the adversary to measure different signal vector R_G, which will lead the adversary to a ghost location, u_G, that minimize $||R_G - R_u(x_i, y_i)||^2$. In *Phantom* , by switching the transmission power of each node, it is possible to create multiple ghost locations from two stationary nodes. Therefore, the number of ghost locations that are visible to the adversary is in control of the coordinating users. *In other words, users can increase the uncertainty of location prediction and location-to-identity mapping performed by the adversaries, which in turn improves their privacy level.*

Figure 4.6(b) shows dummy packets transmitted from two nodes are synchronized at τ_i. To properly create a ghost to adversary, these two packets needs to be indistinguishable from regular packets from *Alice*, which means the headers and preambles should be demodulated to adversary nodes. Therefore, not only the transmission time, but also every bit of the dummy packets should be identical. This includes all header information such as source and destination addresses as well as the payload. The dummy packets need to arrive at each adversary sensor within a delay spread that is indistinguishable from the naturally occurring multipath delay spreads. It furthermore requires that the transmitter hardware is precise enough so that there are no noticeable differences in center frequency or other radiometric features that can be used to distinguish the transmitters.

4.3.2 Advanced adversary models

Adversaries, who are aware of *Phantom* , are likely to detect dummy packets to filter out ghost locations. Unless the dummy packet transmissions are not properly synchronized between the two cooperative transmitters, their receptions at adversary sensors are destructive and fail to pass the packet integrity check from the adversaries - in such a case, adversaries simply detects noisy energy rather than forged packets. Besides such a simple attackers, we now address a number of possible advanced attack models.

Scene analysis attack: Adversaries can detect dummy packets by characterizing the received signals. They will consider that dummy packets are created by the sum of signals from two transmitters at different locations. Especially for RSS-based adversaries, the received signal is likely to be a linear sum of signal powers from two transmitters at different locations.

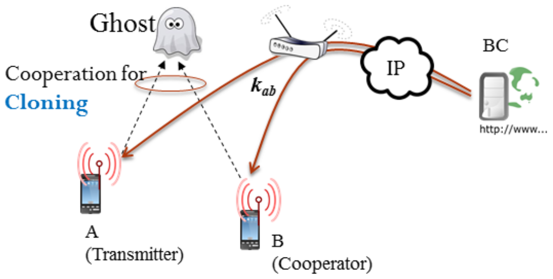
Then they can try to decompose the received signal to find whether the received signal power is sum of two signals powers from two different locations. However, the adversary need to consider that the received signals are easily distorted by multi-path or shadow fading, which lowers their confidence level of detection.

Spectrum analysis attack: Radio devices have radiometric signatures such as Error Vector Magnitude (EVM), I/Q offset, and synch errors, which can be used for the identification of device module [119]. Even so, unless the adversary has the full knowledge on the radiometric signatures from all radio devices, he cannot exploit such a device identification technique for dummy packet filtering. Therefore, the adversary will try to detect the difference in frequency offsets (f_{off}) and transmission time offset (τ_{off}) from two transmitters using spectrum analysis tools such as vector signal analyser (VSA). The precision of his measurement is limited by the number of samples, the bandwidth of the user signal, the sampling rate of VSA, and channel conditions such as delay spread (and Doppler spread in mobile environments). Hence, *Phantom* can thwart such attacks by calibrating their radios within the level of precision that protection can be maximally achieved.

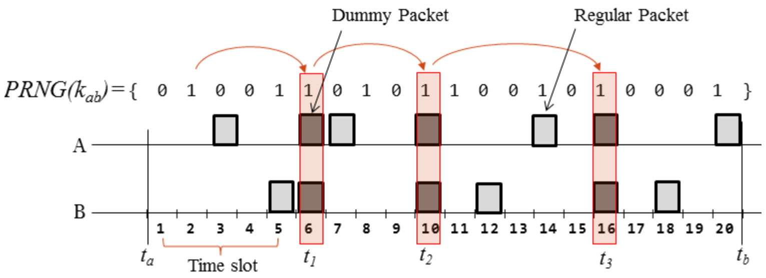
4.3.3 Implicit Coordination for Packet Synchronization

Realizing a practical system for ghost creation poses several challenges. First, the cooperating nodes should transmit the same bitstrings using the same transmission parameters. The frequency and content of dummy messages should be chosen so that it is difficult for the adversary to distinguish these dummy message from those used to transmit real messages. This requirement is difficult to meet if the nodes do not have access to an out-of-band communication channel and cannot agree on the content of all future messages before they are separated. We therefore explore an implicit coordinating technique exploiting a Pseudo-Random Number Generator (PRNG) to synchronize their transmissions. Figure 4.7(a) illustrates the overall coordination approach, where a Back-end Coordinator (BC) is indirectly coordinates two cooperating nodes.

Phantom nodes take four steps to enable *Phantom* service. In *registration*, nodes register their locations and BC authenticate their identity. In *association*, nodes synchronize their time to global clocks and prepare for *Phantom* service request. When a node needs to transmit



(a) Coordination message from BC



(b) Time synchronized dummy packet transmissions

Figure 4.7: Implicitly coordinated dummy packet transmissions

packets under the protection of *Phantom* , the node sends *service request* message to BC to receive a coordination key, k_{ab}, from BC for implicit coordination. The service request message contains information on when ($t_{ab} = (t_a, t_b)$), and how many packets (n) are going to be transmitted from the node. When another *Phantom* node is available in the nearby location of the node who requested *Phantom* service, then BC responds to both nodes with a configuration message contains k_{ab} and their network addresses so that they go into *implicit coordination* mode.

In *implicit coordination* mode, nodes synchronize their transmissions for dummy packets for ghost creation without an explicit or direct communication between the two cooperating nodes. Figure 4.7(b) shows an example scenario of node A and B synchronizing their transmission time using PRNGs. Using the coordination key, k_{ab}, for time duration t_{ab}, two nodes can generate identical bit-stream. Let us assume that the t_{ab} is divided into M fixed (pre-determined) time slots, and the node A requested to transmit n packets, then the number of dummy packets need to be transmitted should be approximately same number to n to avoid possible detection from adversaries on dummy packets. *Phantom* nodes can easily synchronize their transmit time for dummy packets using pseudo-random number sequence, $C_{ab} = \{c_1, c_2, ..., c_m, ...c_M\}$, which is mapped to the time slots for time duration t_{ab}. Time slot t_i for i_{th} dummy packets is selected as the slot number u that satisfies (4.8). For example, when $M = 20, n = 3$, the time slots for 3 dummy packets become slot numbers $u = \{6, 10, 16\}$ that satisfies the condition $\sum_{m=1}^{u} c_m = 3i, i \in \{1, 2, 3\}$ when $C_{ab} = \{0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1\}$. In the similar way, the packet header and payload of dummy packets can also be generated using PRNG and the network address information provided by BC.

$$\sum_{m=1}^{u} c_m = i\left\lfloor \frac{M}{2n} \right\rfloor \tag{4.8}$$

However, this n dummy packet transmission can create only a single ghost node. Hence, to create K ghost nodes, K times of dummy packets need to be transmitted with transmission slots selected from the same rule as (4.8) with a simple modification as follows, $\sum_{m=1}^{u} c_m = i\lfloor \frac{M}{2nK} \rfloor$. Transmitting K time more dummy packet can significantly increases the overhead for ghost creation since dummy packets cannot be used for communications, which are pure protocol overhead to achieve location privacy.

4.3.4 Implementation Using GNU Radios

In this section, we experiment with multi-node cooperative transmissions using software defined radio systems, and demonstrate their combined transmissions are demodulated like regular packets by 802.11g network cards. Although multi-transmitter signal combining techniques have already been developed as a concept of Single Frequency Networks (SFN) in OFDM networks, we are not aware of prior experiments using software defined radios for actual OFDM packets. We investigate the technical feasibility of *Phantom* through proof-of-concept experiments using GNU software defined radios (GNU Radio) [120], which are used to have better control over timing and frequency than in commodity radio devices such as Wi-Fi.[3] We chose Orthogonal Frequency Division Multiplexing (OFDM)-based 802.11g Wi-Fi protocols

---

[3] Specifically, we use the Universal Hardware Driver (UHD) for Ettus Research products instead of the standard GNU Radio software to enable sub-microsecond transmission time control [121]

for *Phantom* implementation to demonstrate an implementation with a real-world, popular protocol. The Cyclic Prefix (CP) [122] of the OFDM symbols also alleviates the level of time synchronization required for dummy packets.

Recall that both time and frequency synchronization are critical to make dummy transmissions indistinguishable from regular ones (and even to just pass a regular CRC packet integrity check). The timing offset (t_{off}) between two radios should be smaller than the CP of 802.11g symbols. Hence, nodes need to synchronize their local clocks to a common reference clocks, which can be achieved by exploiting Pulse Per Second (PPS) signal from GPS (Global Positioning System) receivers or beacons from APs. A frequency offset between two OFDM transmissions can induce severe inter-carrier interference and disturbs packet demodulation. Typically, 10% of sub-carrier space is allowed for frequency offsets [123]. The precision of typical oscillators used in commodity radios is $20 - 50\,\mathrm{ppm}$, which can produce up to 50-$-\ 100\,\mathrm{kHz}$ frequency offset in $2.5\,\mathrm{Ghz}$ bands. We use these values as a guide for required frequency synchronization.

Experiment Setup

Figure 4.8 shows the layout of the experiments using three GNU Radios. We use two of GNU Radios for cooperative transmission, which transmit regular 802.11g OFDM packets created by MATLAB codes developed in [124]. We use standard 802.11g packets, rather than creating custom OFDM symbols with extended CP size (which would simplify implementation of multi-node synchronization). This is to demonstrate that our scheme can be effective with Wi-Fi protocols and actually changes the RSS values on off-the-shelf Wi-Fi receivers. Hence, we use laptops with commodity 802.11g network cards as adversary sensors, specifically cards from two different vendors (Atheros and Broadcom).

The radio specification of 802.11g symbols is summarized in Table 4.1. The third GNU Radio acts as a monitor node for the analysis of the combined signal.

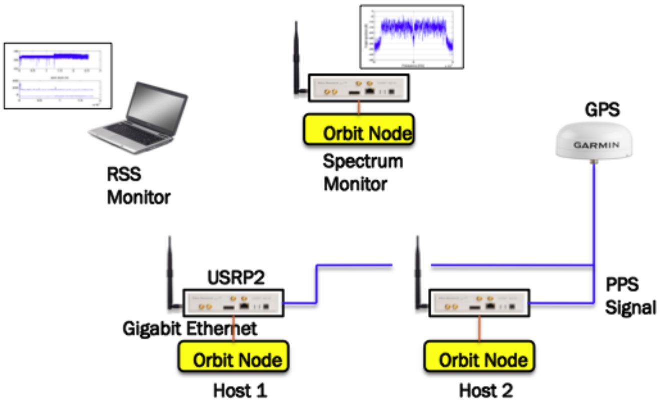


Figure 4.8: Synchronization test on GNURadios.

Table 4.1: Simulation Parameters.

802.11g Radio Specifications	
Bandwidth (Baseband sample rate)	20 MHz
FFT size	64
Number of sub-carrier	52
Number of pilot sub-carriers	4
OFDM symbol period	4 μs (80 samples)
Cyclic prefix (CP) length	0.8 μs (16 samples)
Frequency band	2.4 GHz
Preamble length	8 μs (160 samples)

Time and Frequency Synchronization

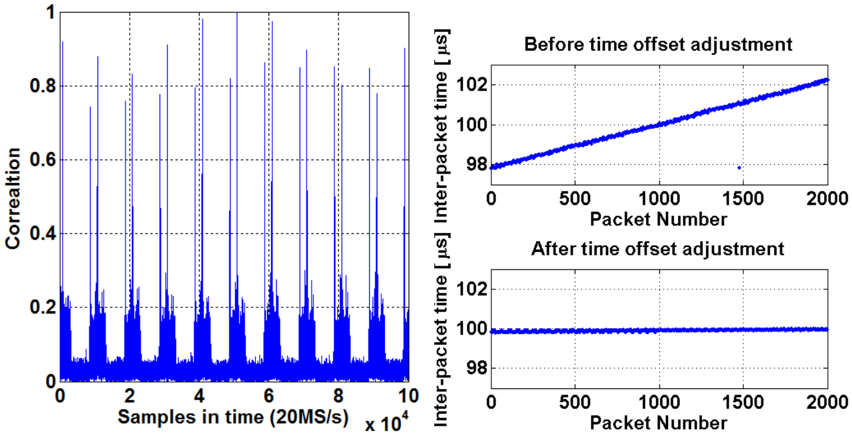
Assuming GPS PPS is available[4], we demonstrate synchronizing two independent GNU Radios using a low-cost GPS module (Garmin 18V) [125, 126][5]. Although the two radios synchronize their clocks to the PPS signal every second, differences in clock drifts still create time offsets between them (this difference also grows during the synchronization interval). Figure 4.9(a)

---

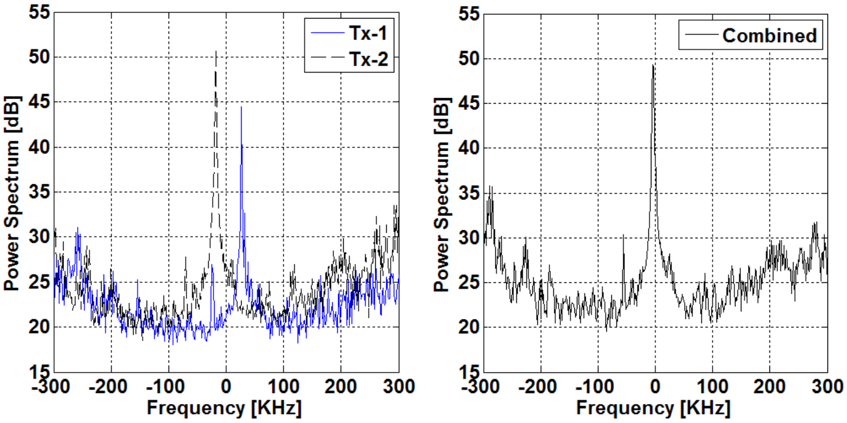
[4] Even indoors, a common PPS can be provided by devices such as GPS repeaters or Pseudolites

[5] We split the signal from a single GPS clock for use in both radios due to restrictions in our test-bed environment. However, we found the maximum time offset among 6 GPS modules was less than 500 ns, which is sufficient to synchronize multi-radios within the size of OFDM symbol CP duration.

shows the correlation value between the received signal and a 802.11g preamble. Both transmitters transmit 2000 packets for 1 s (each packet is 230 μs length). In Fig. 4.9(b), we can find that the initial time offset of 100 μs linearly increases up to 4 μs. Considering the size of CP of 802.11g symbols, which is 0.8 μs, this amount of clock offset should not be ignored. Therefore, *Phantom* nodes should calibrate such time offsets existing in their radio module beforehand. We demonstrate how such time offset can be calibrated in sub-microseconds level using GNU Radios. By adding more baseband samples to the packet data of the radio running a faster clock, as shown in the bottom graph in Fig. 4.9(b), less than 100 ns time synchronization is achieved over 1 s intervals.



(a) Correlation with 802.11g preamble. (b) Fine time synchronization.



(c) Before frequency synchronization. (d) After frequency synchronization.

Figure 4.9: Time and frequency synchronization test using GNU Radios.

The center frequencies of two radios also have offsets due to their oscillators' difference, but can be overcome through similar calibration efforts. Figure 4.9(c) shows the measured spectrum of two radio signals before calibration, which are then calibrated to within $3\,\mathrm{KHz}$ (less than 1% of inter-carrier space) in Fig. 4.9(d).

Effect of Synchronized Transmissions

Figure 4.10 shows the RSS measured from the combined signal while we gradually increased the transmission time offset between two radios by $10\,\mathrm{ns}$. The result shows that the combined signal is demodulated at the receiver nodes when they are time synchronized within $2\mu\mathrm{s}$. The measured RSS is increased by $2-3\,\mathrm{dB}$. Using a packet monitoring application, we also verified that no bit-errors occurred at the receiver node. Surprisingly, the measured synchronization margin of $2\,\mu\mathrm{s}$ is much larger than the $0.8\,\mu\mathrm{s}$ CP size of 802.11g radios. We assume that error correction codes in the 802.11g system help recover from inter-symbol interference errors due to the imperfect time synchronization.

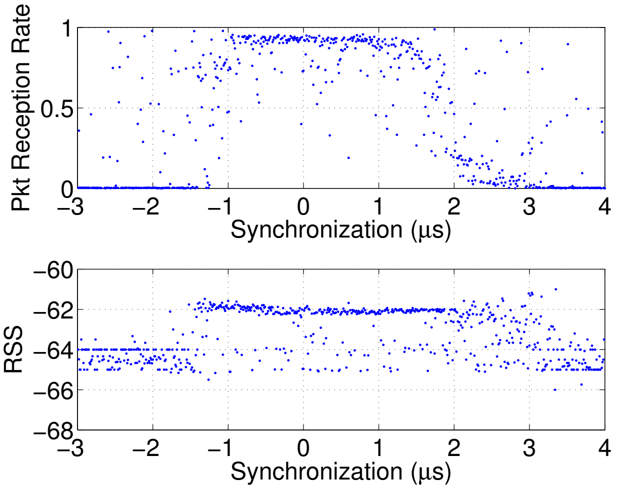


Figure 4.10: Demodulation of the synchronized packets.

4.3.5 Performance Evaluation on Indoor Test-bed

To evaluate our approach and see how the ghost packets in *Phantom* can induce forged ghost locations against adversaries using RSS fingerprinting technique, we conducted an extensive indoor experiment with a number of adversary sensors operating using Wi-Fi radios. We consider RSS-based localization systems more intensively since they are easy to implement and outperform other techniques in typical multi-path environments [118]. We used an isolated indoor test-bed, ORBIT [127], to exclude variables from external sources, e.g., interference, noise sources, and moving signal scatters and reflectors. The test-bed, shown in Fig. 4.11(a), is a grid of 400 (20×20) wireless nodes in $3600\,\mathrm{sq.ft.}$ area. Each node is equipped with Atheors 5212 Wi-Fi network cards, and they are separated by approximately $1\mathrm{m}$ spacing.

The adversary is assumed to build a RSS signature database at 400 reference points. We measure the performance of *Phantom* against various numbers and locations of adversary sensor nodes. We initially use 5 adversary sensors (A-Sensors) shown in Fig. 4.11(b), which is normally a sufficient number to precisely locate transmitters within $1\mathrm{m}$ accuracy on the test-bed. We implement the transmitter portion of *Phantom* using two GNU Radios, which are fixed at grid coordinates $(3, 8)$ and $(8, 3)$. The adversary system localizes the target node by comparing the measured RSS with the radio fingerprints database, as described in section 4.3. The dummy packets that they simultaneously transmitted from A and B induce the adversary to measure a different signal vector R_G, which will lead the adversary to a ghost locations u_G

Power combinations for a cluster of ghosts

Since the RSS measured from adversary sensor on dummy packets are mainly affected by the transmission powers from two transmitters, the locations of ghost node dynamically change according to the power configuration of the transmitter node pair. We found that the transmission power difference between two transmitters heavily affects the location of the ghost, hence we put power index $k \in \{1, 2, \cdots, 19\}$, which sets the power on two transmitters as $(p_A, p_B) = (k, 20 - k)$. Transmitting dummy packet with various power index values creates a cluster of ghosts, which improves the location privacy of users. However, we have to admit that such a clustering technique induces large overhead from the increased number of dummy packet transmissions.

4.3.6 Privacy performance over various adversary locations

We evaluate the performance of privacy protection using two metrics. The first metric is the sum of distance between the true location of the target nodes (Tx-1 and Tx-2) and ghost locations. The second metric is the entropy of the location information of the target nodes[6]. We change the numbers and locations of adversary sensors. Figure 4.11(c) shows the experiment results when adversary sensors are randomly selected from the nodes in a circle of radius $10\,\mathrm{m}$ around the target nodes. Figure 4.11(d) shows the result when the adversary sensors are randomly selected among 369 nodes in the test-bed. Both results indicate that as the number of adversary sensors increase, the location privacy gain decrease, however, with moderate number of adversary sensors (less than 7), *Phantom* well preserves the location privacy of users.

In our experiment, the privacy gains measured by the distance between ghost locations and true locations are actually limited by the size of the test-bed. Therefore, considering that signal attenuation is a log function of distance, the expected privacy gains in real networks will rapidly grow according to the size of the networks. In typical indoor localization systems, *Phantom* can easily achieve several tens of meters gain for moderate number of adversaries.

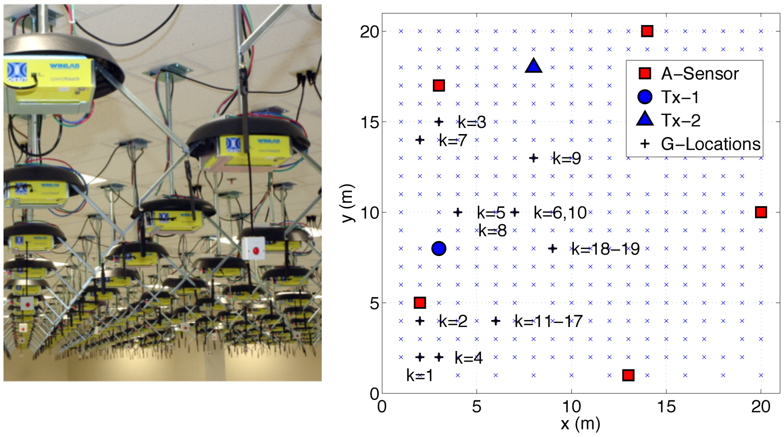
Adversary using scene analysis technique

As we addressed in section 4.3.2, adversaries who are aware of the existence of *Phantom* will try to detect dummy packets by characterizing the received signal. If the adversary uses RSS fingerprint technique, he will firstly try to decompose the received signal R_G, as shown in Fig. 4.12(a), to check if the signal is similar to a linear combination of two of his reference RSS fingerprints, i.e., $\alpha R_u(x_A, y_A) + \beta R_u(x_B, y_B)$. They can check the similarity by solving a linear estimation problem $Y = H\theta + W$, by putting $\theta = [\alpha\ \beta]^T$, where Y is the observation RSS, H is training data $[R_u(x_A, y_A)^T\ R_u(x_B, y_B)^T]$, and W is the observation noise. θ can be estimated by $(H^T H)^{-1} H^T B$, then it is possible to find the difference between the received signal and the linear sum of two fingerprints, $e_{Li} = min_{\{\alpha,\beta,A,B\}}\{R_G - (\alpha R_u(x_A, y_A) + \beta R_u(x_B, y_B))\}$, which indicates how likely the received signal is a dummy packet.

The adversary can also compare the observation error, e_{Ob}, between the received RSS and

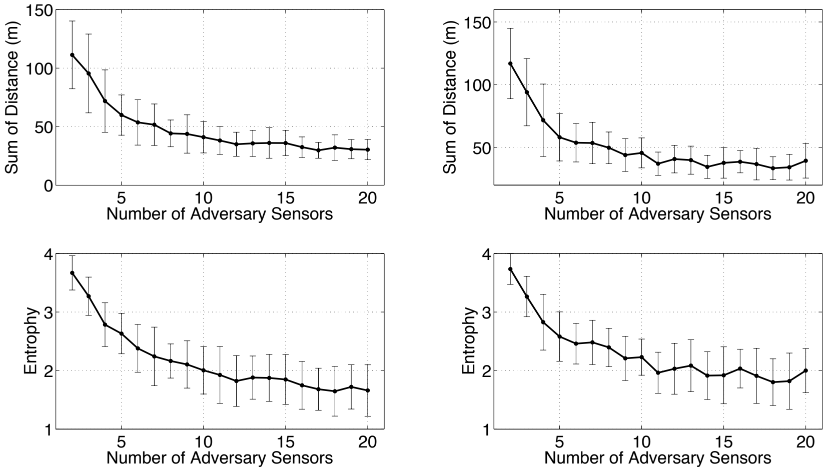
---

[6] For M ghost locations for node i, the entropy for node i is $P_i \cdot log_2(P_i)$, where $P_i = \frac{1}{M+1}$.



(a) ORBIT Test-bed

(b) Performance over different power combinations



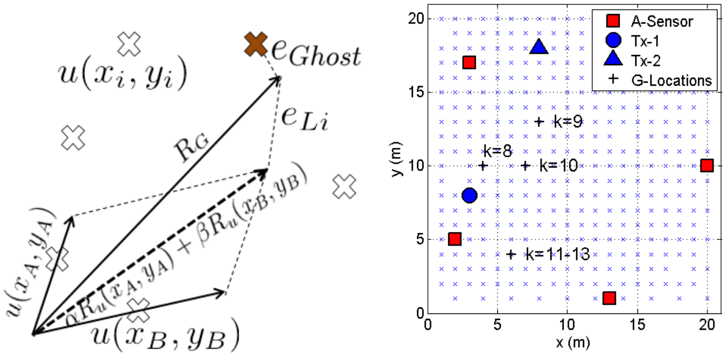
(c) Circularly positioned adversary sensors

(d) Randomly positioned adversary sensors

Figure 4.11: Privacy performance in the experiment test-bed

its closest reference value in the training data. Let the observation error for dummy packets, $e_{Ghost} = min_i||R_G - R_u(x_i, y_i)||^2, i \in C$ as shown in Fig. 4.12(a). If e_{Ghost} is significantly larger than the observation error from normal packets from a single transmitter, e_{Single}, then the adversary the observed RSS does not belong to any of the fingerprints and the adversary can easily identify dummy packets. Hence, the adversary will discard packets when the observation error in the received signal is larger than e_{Single}.

In Fig. 4.12(b), we consider adversary applies the scene analysis technique to filter out possible dummy locations. For each received dummy packet transmission, ghosts are assumed created when they only satisfy the condition, $e_{Ghost} \leq e_{Single}$, and $e_{Ghost} \leq e_{Li}$. The number of ghosts created is reduced from 10 to 4; however, *Phantom* still creates enough ghosts to provide location privacy for wireless users. In our indoor test-bed experiments we exclude the effects from shadowing,[7] which is difficult to calibrate since they are channel variations caused by reflections and detractions in the network environment. Note that in actual networks, observation errors are heavily affected by shadowing, which, in fact, obfuscates the precision of the adversaries' attacks using scene analysis techniques by characterizing the received signals. Hence the adversaries' attempt to filter dummy packets is likely to fail owing to the uncertainty of wireless channels.



(a) Signal decomposition attack

(b) Ghost locations created for the adversary using scene analysis technique

Figure 4.12: Advanced adversaries using scene analysis technique

---

[7] In typical indoor channel environments, RSS variation is normally $8 - 10$ dB [128].

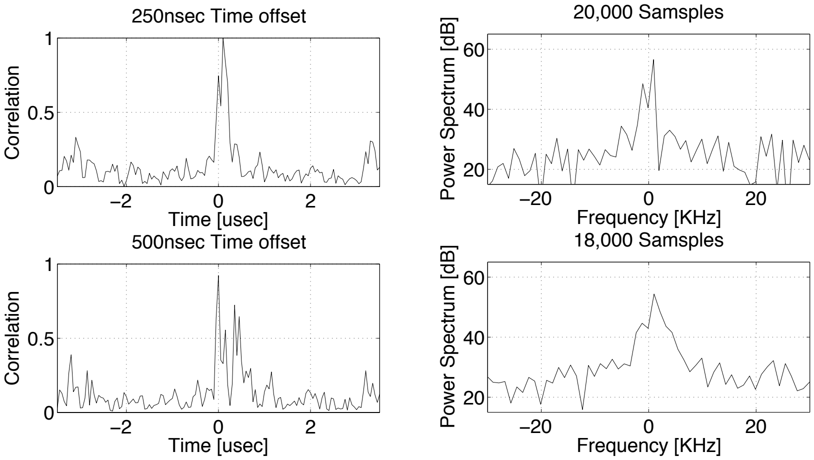
Adversary using spectrum analysis tools

Adversaries equipped with spectrum analysis will try to find dummy packets by measuring the residual difference in frequency offsets (f_{off}) and transmission time offsets (τ_{off}) between the two transmitters. Such attacks can be thwarted by further calibrating user radios within the level that the adversary cannot distinguish the difference between two radios. Figure 4.13 shows the level of synchronization needed for Wi-Fi radios in typical indoor environments. Firstly, Fig. 4.13(a) shows time correlation peak between 802.11g the preamble and the baseband samples collected by VSA at a sampling rate of $50M$ SPS. We can find that due to the delay spread from indoors and the time resolution limited by the bandwidth of the signal (20 MHz), the adversary cannot resolve the time offset between two transmitters for $\tau_{off} < 250\,\text{nsec}$. On the other hand, the resolution in spectrum analysis depends on the size of FFT and the number of baseband samples collected from VSA. Figure 4.13(b) shows at least $20,000$ samples are needed to properly identify 3 KHz frequency offset in two radios, which limits the size of packets transmitted for dummy packets. The smaller frequency offset the two radios have, the larger size of packets that can be transmitted.

Such high level of precision may require additional hardware (e.g., Ultra Stable TCXO can provide $0.1ppm$ accuracy) and software modules on existing radio devices. However, considering that high precision oscillators are currently available with a small additional cost, the implementation cost for *Phantom* devices is not high. Also, note that the required level of calibration is considerably alleviated in outdoor environments where the amount of delay spread and Doppler spread are much larger than in indoor environments.

4.4 Conclusion

The protection of user location privacy in PHY layer is a fundamental problem for secure communications. In this chapter, using theoretical analysis and simulations, we showed that the location privacy of wireless nodes and its communication throughput are negotiable parameters that can be traded off against one another. Moreover, we showed that by simply adding jamming noise from a third cooperator jamming node, it is possible to achieve better location privacy without sacrificing too much communication throughput. We also proposed an implicit



(a) Time offset analyse

(b) Frequency offset analyse

Figure 4.13: Advanced adversaries using spectrum analysis tools

jamming power control algorithm to find optimal jammers' transmission power in given topological conditions. The proposed algorithm significantly improves the location privacy while guaranteeing that the throughput is above a user-defined threshold. Furthermore, the proposed implicit coordination algorithm leaves the cooperative jammers location privacy intact.

We also proposed *Phantom* to protect location privacy of wireless users by creating a number of ghost locations that confuses adversaries for the true location of the users. Compared to other existing anonymization techniques, the performance of *Phantom* is not limited by the number and the mobility of cooperators. *Phantom* enables users to adjust their location privacy on-demand by creating ghost nodes, either with the same identity or anonymous. We introduced protocols for generating such ghost nodes through simultaneous transmissions from multiple nodes which are implicitly coordinated. We implemented a proof of concept using software defined radios as transmitters. Through experiments, we showed how such ghost nodes can improve user location privacy in indoor test-bed experiments and addressed several technical issues such as calibrating the radio parameters.

Acknowledgment

The authors would like to thank to Gayathri Chandrasekaran for the contribution of her RSS fingerprint data on ORBIT.

Chapter 5

Conclusion

In this paper, we designed protocols exploiting implicit coordination techniques for a number of practical applications in wireless communications. We demonstrated how implicit coordination techniques can improve efficiency and reliability while suppressing overhead for node coordination. Firstly, in chapter 2, we showed the noble design of the message dissemination method, *ZCOR* , which uses the frame of implicit coordination techniques to improve the scalability and performance of safety-message dissemination protocol in dynamic vehicular network environments. In chapter 3, we applied an implicit coordination technique for optimal power and transmission time allocation in Ad-Hoc networks. Nodes that are operated by *JPSA* can efficiently control their transmission power only using their specific local information without a global coordinator. We also extended the application of implicit coordination techniques to the area of user location privacy. In chapter 4, we proposed cooperative location protection techniques that preserve the location privacy of wireless users, and we developed node coordination protocols based on implicit coordination techniques. The proposed node coordination protocols minimize the coordination message transmission, which can significantly reduce the probability of detection of cooperating nodes from adversaries attacking their privacy.

Appendix A

Location Privacy Measure using CRLB

We use the CRLB to estimate the precision limit in adversary localization systems trying to find the location of wireless mobiles sensors. CRLB for TOA and RSS based localization systems in mixed LOS and NLOS conditions is discussed in [116].

CRLB for TOA-based localization methods The adversary localization system estimates the distance from target node TX by measuring TOA from the received signals, and then he applies triangulation techniques. Since the adversaries do not know the exact timing of the transmitted signal, they have to use Time Different Of Arrival (TDOA) values instead. We considered that the accuracy of TDOA-based localization method is basically the same as TOA-based system with doubled variances in time estimation [129].

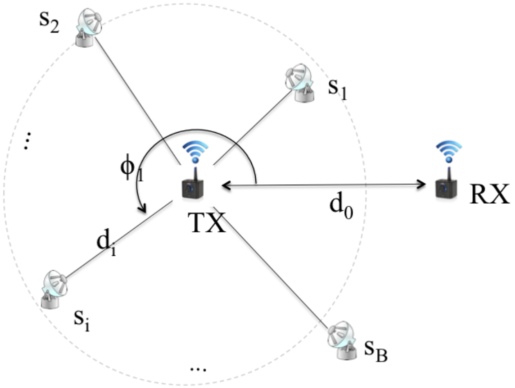


Figure A.1: Transmitter (TX), receiver (RX) and adversary sensors ($\boldsymbol{s}$).

Figure A.1 depicts the adversary system localizing the target node TX using total number of B sensors, $\boldsymbol{s} = \{s_1, s_2, \cdots, s_B\}$. Let us assume M sensors are in NLOS conditions, and the rest $(B - M)$ sensors are in LOS conditions. Then, the values to be estimated are $\mathbf{v} = (u, l)$ for the location of T,$\boldsymbol{u} = \{x, y\}$, and NLOS path lengths, $\boldsymbol{l} = (l_1, l_2, \cdots, l_M)$. The CRLB for

$\boldsymbol{v}$ is determined from *FIM* matrix $J_{\boldsymbol{v}}$ in (A.1),

$$Cov(\boldsymbol{v}) \geq J_{\boldsymbol{v}}^{-1}, \tag{A.1}$$

where $J_{\boldsymbol{v}}$ can be found from *FIM* for received signal delay τ in the following equation (A.2)

$$J_{\boldsymbol{v}} = H \cdot J_{\tau} \cdot H^{T}, \tag{A.2}$$

for H representing the geometric configuration of sensors in relation with the target transmitter location, where the angle to each sensor s_i is denoted as $\phi_{\mathbf{i}}$ referencing to the link to receiver RX.

$$H = \begin{pmatrix} \cos\phi_1, \cos\phi_2, \cdots, \cos\phi_M \\ \\ \sin\phi_1, \sin\phi_2, \cdots, \sin\phi_M \end{pmatrix}. \tag{A.3}$$

Then, $J_{\boldsymbol{v}}$ can be rewritten as the following equation

$$J_{\boldsymbol{v}} = \frac{1}{c^2} \begin{pmatrix} H_{NL}\Lambda_{NL}H_{NL}^{T} + H_{L}\Lambda_{L}H_{L}^{T} & H_{NL}\Lambda_{NL} \\ \\ \Lambda_{NL}H_{NL}^{T} & \Lambda_{NL} \end{pmatrix}, \tag{A.4}$$

where $c = 3 \times 10^{8}\mathrm{m/s}$. H can be decomposed into NLOS (denoted as ”NL”) and LOS (denoted as ”L”) components. Λ is a diagonal matrix of λ_i that represents the precision of time estimation for the TOA measurement at each sensor s_i. λ_i depends on the quality of the signal (SINR) and the delay spread of the channel, which can be expressed as (A.5).

$$\lambda = \frac{1}{\sigma_{\tau}^{2} + \sigma_{\text{rms}}^{2}}, \tag{A.5}$$

where σ_{rms} is the delay spread of the channel, and $\sigma_{\tau^2} = \frac{1}{8\pi^2 f_b^2 \cdot \gamma}$ is the precision of time delay estimation, which depends on SINR of the received signal, γ, and the bandwidth of the signal, f_b. For the sensors in NLOS conditions, the delay spread in the received signal $\sigma_{\text{rms-NL}}$ is much larger than that of LOS sensors, $\sigma_{\text{rms-L}}$. Matrix λ can be decomposed into NLOS and LOS components in the same way as H. When jammers transmit jamming signals, the precision of location estimation of adversary localization system decrease as the SINR conditions in the received signals degrades.

CRLB for TOA adversary can be calculated from $J_{\boldsymbol{v}}$ in (A.4)

$$J_{TOA}^{-1} = [J_{\boldsymbol{v}}^{-1}]_{2\times 2}. \tag{A.6}$$

CRLB for RSS-based localization methods

Adversaries can also measure RSS from the target node TX to estimate the distance from the node. RSS at the receiver s_i depends on the path-loss between the TX and adversary sensors $\boldsymbol{s}$. A typical path-loss model is presented in (A.7), where the aggregate path-loss between TX and s_i, $\hat{z_i}$, consists of log-distance path-loss (z_i), log-normal shadowing (ω_i) , and small scale fading (ξ_i) components.

$$\hat{z_i} = z_i + \omega_i + \xi_i \quad [\text{dB}]. \tag{A.7}$$

The impact from small scale fading can be averaged out by collecting large number of samples since its variance can be significantly reduced by averaging the channel over time. CRLB for RSS-adversary is mostly bounded by the amount of the shadowing component ω_i since its variance is quite large. However, RF fingerprinting techniques [18] significantly reduce the effects from shadowing through an extensive calibrating process that can also be applied to outdoor environments [130].

The path-loss z_i at distance d_i can be modeled by a log-distance path-loss model using a path-loss exponent η.

$$z_i = -10 \cdot \eta \cdot \log_{10} d_i \quad [\text{dB}]. \tag{A.8}$$

FIM for the location of TX can be found from

$$J_{\boldsymbol{v}} = \tilde{H} \cdot J_z \cdot \tilde{H}^T, \tag{A.9}$$

Table A.1: Simulation Parameters.

Parameter	Values
$\sigma_{\text{rms-L}}$	2×10^{-9} s
$\sigma_{\text{rms-NL}}$	2×10^{-8} s
$\sigma_{\omega-L}$	1 dB
$\sigma_{\omega-NL}$	3 dB

and

$$\tilde{H} = \frac{10\gamma}{\ln 10} \cdot \begin{pmatrix} \frac{\cos\phi_1}{d_1}, \frac{\cos\phi_2}{d_2}, \cdots, \frac{\cos\phi_B}{d_B} \\ \\ \frac{\sin\phi_1}{d_1}, \frac{\sin\phi_2}{d_2}, \cdots, \frac{\sin\phi_B}{d_B} \end{pmatrix},$$

where $\tilde{H}$ is the geometric configuration for adversary sensors in RSS-base localization systems.

For large enough number of samples, $\bar{\xi}_i \approx 0$, then J_z is a diagonal matrix of the variance of shadowing components $\sigma^2_{\omega_i}$, which is often modeled by log-normal distribution of $N(\mu, \sigma^2_{\omega_i})$. Sensors in NLOS conditions have larger $\sigma^2_{\omega_i}$ values that the sensors in LOS conditions.

$$J_z = \Lambda_B = [diag(\sigma^2_{\omega_1}, \sigma^2_{\omega_2}, \cdots, \sigma^2_{\omega_B}]^{-1}. \tag{A.10}$$

The RSS measurement value in adversary localization system interferes when jammers transmit jamming signals. We find σ_{c_i}, which is the variation of RSS induced by the jamming signal at adversary sensor s_i, from simulations for 5000 different locations of COPs and adversary sensors. We put Λ'_B as the sum of the RSS variance due to shadowing and jamming noise, which can be decomposed into NLOS ($\sigma^2_{\omega-NL}$) and LOS ($\sigma^2_{\omega-L}$) components.

$$\Lambda'_B = [diag(\sigma^2_{\omega_1} + \sigma^2_{c_1}, \sigma^2_{\omega_2} + \sigma^2_{c_2}, \cdots, \sigma^2_{\omega_B} + \sigma^2_{c_B}]^{-1}. \tag{A.11}$$

Then,

$$J_{\boldsymbol{v}} = \tilde{H} \cdot \Lambda'_B \cdot \tilde{H}^T. \tag{A.12}$$

CRLB in RSS adversary can be found from (A.13)

$$[J_{RSS}^{-1}] = [J_{\boldsymbol{v}}^{-1}]_{2\times 2}. \tag{A.13}$$

We summarize the parameter values used in the simulations in Table A.1.

References

[1] J. Jun and M. Sichitiu, "The nominal capacity of wireless mesh networks," *IEEE Wireless Communications*, vol. 10, no. 5, pp. 8 – 14, oct 2003.

[2] I. Akyildiz and X. Wang, "A survey on wireless mesh networks," *IEEE Communications Magazine*, vol. 43, no. 9, pp. S23 – S30, sept. 2005.

[3] R. Bruno, M. Conti, and E. Gregori, "Mesh networks: commodity multihop ad hoc networks," *IEEE Communications Magazine*, vol. 43, no. 3, pp. 123 – 131, march 2005.

[4] A. Nosratinia, T. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," *IEEE Communications Magazine*, vol. 42, no. 10, pp. 74 – 80, oct. 2004.

[5] M. Xiao, N. B. Shroff, and E. K. P. Chong, "A utility-based power-control scheme in wireless cellular systems," *IEEE Transactions on Networking*, vol. 11, no. 2, pp. 210–221, 2003.

[6] C. U. Saraydar, N. B. Mandayam, and D. J. Goodman, "Efficient power control via pricing in wireless data networks," *IEEE Transactions on Communication*, 2000.

[7] H. Ji and C.-Y. Huang, "Non-cooperative uplink power control in cellular radio systems," *Proc. of Wireless Networks*, vol. 4, no. 3, pp. 233–240, 1998.

[8] X. Lin and N. Shroff, "Joint rate control and scheduling in multihop wireless networks," in *Proc. of IEEE Decision and Control*, vol. 2, Dec. 2004, pp. 1484–1489 Vol.2.

[9] C. Prehofer and C. Bettstetter, "Self-organization in communication networks: principles and design paradigms," *IEEE Communications Magazine*, vol. 43, no. 7, pp. 78 – 85, july 2005.

[10] F. Stulp, H. Utz, M. Isik, and G. Mayer, "Implicit coordination with shared belief: A heterogeneous robot soccer team case study," *Advanced Robotics, the International Journal of the Robotics Society of Japan*, 2010.

[11] P. Brenner, "A technical tutorial on the ieee 802.11 protocol," Whitepaper from Breezecom Wireless Communication, 1997.

[12] S. Venkateswaran, S. Singh, U. Madhow, and R. Mudumbai, "Distributed synchronization and medium access in wireless mesh networks," in *Information Theory and Applications Workshop (ITA)*, feb. 2011, pp. 1 –8.

[13] A. Zvikhachevskaya and L. Mihaylova, "Self-organisation in wireless sensor networks for assisted living," in *Proc. of IET Assisted Living Conference*, feb. 2009.

[14] N. W. Group, "Architectural principles of the internet," Request for Comments: 1958, 1996.

[15] D. P. Palomar and M. Chiang, “A tutorial on decomposition methods for network utility maximization,” *IEEE Journal on Selected Areas in Communication*, vol. 24, pp. 1439–1451, 2006.

[16] P. Chen, “A cellular based mobile location tracking system,” in *Proc.of Vehicular Technology Conference*, vol. 3, jul 1999, pp. 1979–1983.

[17] L. Doherty, K. Pister, and L. El Ghaoui, “Convex position estimation in wireless sensor networks,” in *Proc. of IEEE Computer and Communications Societies (INFOCOM)*, vol. 3. Citeseer, 2001, pp. 1655–1663.

[18] P. Bahl and V. N. Padmanabhan, “RADAR: An in-building rf-based user location and tracking system,” in *Proc. of IEEE Computer and Communications Societies (INFOCOM)*, Tel Aviv, Israel, 2000.

[19] S. Oh and M. Gruteser, “Multi-node coordinated jamming for location privacy protection,” in *Proc. of IEEE Military Communications Conference MILCOM*. IEEE, Nov. 2011.

[20] “IEEE 1609 - Family of Standards for Wireless Access in Vehicular Environments (WAVE),” http://www.standards.its.dot.gov, 2007.

[21] “PReVENT: Preventive and active safety; 6th framework program integrated project,” http://www.prevent-ip.org.

[22] “Network on Wheels (NoW) project,” http://www.network-on-wheels.de/vision.html, 2007.

[23] S. Olariu and M. C. Weigle, *Vehicular Networks*. CRC Press, Dec 2009.

[24] G. Yan, S. Olariu, and M. C. Weigle, “Providing VANET security through active position detection,” *Computer Communications: Special Issue on Mobility Protocols for ITS/VANET*, vol. 31, no. 12, p. 2883 2897, Jul. 2008.

[25] E. Fasolo, A. Zanella, and M. Zorzi, “An effective broadcast scheme for alert message propagation in vehicular ad hoc networks,” *Proc of IEEE International Conference on Communications (ICC)*, vol. 9, pp. 3960–3965, Jun. 2006.

[26] H. Wu, M. Palekar, R. Fujimoto, J. Lee, J. Ko, R. Guensler, and M. Hunter, “Vehicular networks in urban transportation systems,” in *Proc. of the National conference on Digital Government Research*, 2005, pp. 9–10.

[27] H. Hartenstein and K. Laberteaux, *VANET Vehicular Applications and Inter-Networking Technologies (Intelligent Transport Systems)*, 1st ed. Wiley, 2010, vol. 1.

[28] K. Hong, D. Xing, V. Rai, and J. Kenney, “Characterization of DSRC performance as a function of transmit power,” in *Proc. of ACM international workshop on VehiculAr InterNETworking (VANET)*. Beijing, China: ACM, 2009, pp. 63–68.

[29] D. Jiang, V. Taliwal, A. Meier, W. Holfelder, and R. Herrtwich, “Design of 5.9 GHz DSRC-based vehicular safety communication,” *IEEE Wireless Communications*, vol. 13, no. 5, pp. 36 –43, Oct. 2006.

[30] Z. Wang and M. Hassan, "How much of DSRC is available for non-safety use?" in *Proc. of ACM International workshop on VehiculAr Inter-NETworking (VANET).* San Francisco, CA: ACM, 2008, pp. 23–29.

[31] M. M. I. Taha and Y. M. Y. Hasan, "A novel headway-based vehicle-to-vehicle multi-mode broadcasting protocol," in *Proc. of Vehicular Technology Conference*, Sep. 2008, pp. 1–5.

[32] H. Alshaer and E. Horlait, "An optimized adaptive broadcast scheme for inter-vehicle communication," in *Proc. of Vehicular Technology Conference*, vol. 5, May 2005, pp. 2840 – 2844 Vol. 5.

[33] K. Tokuda, M. Akiyama, and H. Fujii, "Dolphin for inter-vehicle communications system," in *Proc. of IEEE Intelligent Vehicles Symposium*, 2000, pp. 504 –509.

[34] A. Fukada, S. Matsuda, and H. Okada, "Multi-hop control scheme on vehicular information broadcasting relay (VIBROR)," in *Proc. of Vehicular Technology Conference*, 2001.

[35] G. Korkmaz, E. Ekici, F. Özgüner, and U. Özgüner, "Urban multi-hop broadcast protocol for inter-vehicle communication systems," in *Proc. of the workshop on Vehicular ad hoc networks (VANET '04).* New York, NY, USA: ACM, 2004, pp. 76–85.

[36] M.-T. Sun, W.-C. Feng, T.-H. Lai, K. Yamada, H. Okada, and K. Fujimura, "GPS-based message broadcast for adaptive inter-vehicle communications," in *Proc. of IEEE Vehicular Technology Conference*, 2002, pp. 101–110.

[37] M. Ashrafi, D. Taniar, and K. Smith, "ODAM: An optimized distributed association rule mining algorithm," *IEEE Distributed Systems Online, IEEE*, 2004.

[38] B. S. Chlebus, L. Gasieniec, A. Ostlin, and J. M. Robson, "Deterministic radio broadcasting," in *Proc. of International Colloquium on Automata, Languages and Programming (ICALP)*, Geneva, Switzerland, 2000, pp. 717–728. [Online]. Available: citeseer.ist.psu.edu/article/chlebus00deterministic.html

[39] T. Kosch, C. Adler, S. Eichler, C. Schroth, and M. Strassberger, "The scalability problem of vehicular ad hoc networks and how to solve it," *IEEE Wireless Communications*, vol. 13, no. 5, pp. 22–28, Oct. 2006.

[40] M. Li and W. Lou, "Opportunistic broadcast of emergency messages in vehicular ad-hoc networks with unreliable links," in *Proc. of International ICST Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness*, Hong Kong, 2008, pp. 1–7.

[41] D. Reichardt, M. Miglietta, L. Moretti, P. Morsink, and W. Schulz, "CarTALK 2000: safe and comfortable driving based upon inter-vehicle-communication," in *Proc of IEEE Intelligent Vehicle Symposium*, vol. 2, Versailles, France, Jun. 2002, pp. 545–550 vol.2.

[42] "Project: FleetNet - internet on the road," http://www.et2.tu-harburg.de/fleetnet/english/about.html.

[43] X. Chen, H. Refai, and X. Ma, "Broadcasting performance comparison among IVC MAC protocol candidates," in *Proc.International Symposium on Intelligent Control*, Singapore, Oct. 2007, pp. 19–22.

[44] R. Mangharam, R. Rajkumar, M. Hamilton, P. Mudalige, and F. Bai, "Bounded-latency alerts in vehicular networks," *Mobile Networking for Vehicular Environments*, pp. 55–60, May 2007.

[45] R. Verdone, "Multihop R-ALOHA for intervehicle communications at millimeter waves," *IEEE Transactions on Vehicular Technology*, vol. 46, no. 4, pp. 992–1005, Nov. 1997.

[46] T. Hatakeyama and S. Takaba, "A network architecture of the inter-vehicle packet communication system," in *Proc. of Vehicle Navigation and Information Systems Conference*, Yokohama, Japan, Aug. 1994, pp. 159–164.

[47] Y. Inoue and M. Nakagawa, "MAC protocol for inter-vehicle communication network using spread spectrum technique," in *Proc.of Vehicle Navigation and Information Systems Conference*, Yokohama, Japan, Aug. 1994, pp. 149–152.

[48] S. S. Lam, "Packet broadcast networks a performance analysis of the R-ALOHA protocol," *IEEE Transaction on Computers*, vol. 29, no. 7, pp. 596–603, 1980.

[49] S. Tasaka, "Stability and performance of the R-ALOHA packet broadcast system," *IEEE Transaction on Computers*, vol. 32, no. 8, pp. 717–726, 1983.

[50] M. Zorzi and R. R. Rao, "Geographic random forwarding (GeRaF) for ad hoc and sensor networks: Multihop performance," *IEEE Transactions on Mobile Computing*, vol. 2, no. 4, pp. 337–348, 2003.

[51] S. Biswas and R. Morris, "ExOR: Opportunistic multi-hop routing for wireless networks," in *Proc. of ACM Professional forum for discussing Communications and Computer Networks (SIGCOMM)*, Philadelphia, PA, 2005, pp. 133–144.

[52] B. Blaszczyszyn, A. Laouiti, P. Muhlethaler, and Y. Toor, "Opportunistic broadcast in VANETs (OB-VAN) using active signaling for relays selection," in *Proc. of ITST International Conference on Telecommunications*, Phuket, Thailand, Oct. 2008, pp. 384–389.

[53] SAEInternational, "Dsrc implementation guide: A guide to users of SAE J2735 message sets over DSRC," http://http://www.sae.org, 2010.

[54] Z. Wang, E. Tameh, and A. Nix, "Joint shadowing process in urban peer-to-peer radio channels," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 1, pp. 52–64, Jan. 2008.

[55] S. Oh, S. Kaul, and M. Gruteser, "Exploiting vertical diversity in vehicular networks channel environments," in *Proc. of Personal, Indoor and Mobile Radio Communications Symposium (PIMRC)*, 2009.

[56] R. D. Kuhne, "Foundations of traffic flow theory I: Greenshields' legacy highway traffic," in *Proc. of Symposium on the Fundamental Diagram*, Woods Hole, MA, Jul. 2008.

[57] "Traffic stream calibration software (Accessed on Jul. 1,2009)," http://filebox.vt.edu/users/hrakha/.

[58] R. Chen, W.-L. Jin, and A. Regan, "Broadcasting safety information in vehicular networks: issues and approaches," *IEEE Network*, vol. 24, no. 1, pp. 20 –25, Jan. 2010.

[59] M. Torrent-Moreno, P. Santi, and H. Hartenstein, "Distributed fair transmit power adjustment for vehicular ad hoc networks," in *Sensor and Ad Hoc Communications and Networks (SECON)*, vol. 2, Sep. 2006, pp. 479 –488.

[60] M. Torrent-Moreno, D. Jiang, and H. Hartenstein, "Broadcast reception rates and effects of priority access in 802.11-based vehicular ad-hoc networks," in *Proc. of International workshop on Vehicular ad hoc networks (VANET)*, 2004, pp. 10–18.

[61] R. K. Schmidt, T. Leinmüller, E. Schoch, F. Kargl, and G. Schäfer, "Exploration of adaptive beaconing for efficient intervehicle safety communication," *IEEE Network Magazine - Special Issue on "Advances in Vehicular Communications Networks"*, vol. 24, no. 1, Jan. 2010. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5395778

[62] C.-L. Huang, Y. Fallah, R. Sengupta, and H. Krishnan, "Adaptive intervehicle communication control for cooperative safety systems," *IEEE Network*, vol. 24, no. 1, pp. 6 –13, jan.-feb. 2010.

[63] J. E. Elson, M. Gerla, G. J. Popek, G. J. Pottie, M. Sarrafzadeh, and D. L. Estrin, "Time synchronization in wireless sensor networks," vol. 14, no. 3, 2003, pp. 1965–1970.

[64] "Technical specificatios of GPS 18x LCV OEM (part number:190-00879-08)," http://www.garmin.com/us/.

[65] "IEEE 1609 - Family of Standards for Wireless Access in Vehicular Environments (WAVE)," http://www.standards.its.dot.gov.

[66] I. Manno, "Introduction to the monte carlo method," Hungary: Akadmiai Kiad, 1999.

[67] "The network simulator, NS-2," http://isi.edu/nsnam/ns/.

[68] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen, and J.-P. Sheu, "The broadcast storm problem in a mobile ad hoc network," in *Proc. of ACM International conference on Mobile Computing and Networking (MobiCom)*, 1999, pp. 151–162.

[69] W. Peng and X.-C. Lu, "On the reduction of broadcast redundancy in mobile ad hoc networks," in *Proc. of ACM international symposium on Mobile ad hoc networking & computing (MobiHoc)*. IEEE Press, 2000, pp. 129–130.

[70] S. Oh, J. Kang, and M. Gruteser, "Location-based flooding techniques for vehicular emergency messaging," in *Proc. of Vehicle-to-vehicle Communication Workshop (V2VCOM)*, San Jose, CA, Jul. 2006, pp. 1–9.

[71] W. Lou and J. Wu, "Toward broadcast reliability in mobile ad hoc networks with double coverage," *IEEE Transactions on Mobile Computing*, vol. 6, no. 2, pp. 148–163, 2007. [Online]. Available: http://dx.doi.org/10.1109/TMC.2007.31

[72] J. Turkka and M. Renfors, "Path loss measurements for a non-line-of-sight mobile-to-mobile environment," in *Proc. of ITS Telecommunications (ITST)*, Pucket, Thailand, Oct. 2008, pp. 274–278.

[73] Z. Wang, E. Tameh, and A. Nix, "A sum-of-sinusoids based simulation model for the joint shadowing process in urban peer-to-peer radio channels," in *Proc. of IEEE Vehicular Technology Conference*, vol. 3, Dallas, TX, Sep. 2005, pp. 1732–1736.

[74] "Vanetmobisim," http://vanet.eurecom.fr/.

[75] M. E. van, W. Klein Wolterink, G. Karagiannis, and G. Heijenk, "Exploring the solution space of beaconing in vanets," in *Proc. of IEEE Vehicular Networking Conference (VNC)*. IEEE Communications Society, Oct. 2009. [Online]. Available: http://doc.utwente.nl/68265/

[76] "Final report: Vehicle infrastructure integration proof of concept results and findings summary," US Department of Transportation by The VII Consortium, May 2009.

[77] M. Iqbal, X. Wang, and X. Z. David Wertheim, "SwanMesh: A multicast enabled dual-radio wireless mesh network for emergency and disaster recovery services," *Journal of Communications*, vol. 4, no. 5, pp. 298–306, Jun 2009.

[78] T. Gao, T. Massey, L. Selavo, D. Crawford, B. rong Chen, K. Lorincz, V. Shnayder, L. Hauenstein, F. Dabiri, J. Jeng, A. Chanmugam, D. White, M. Sarrafzadeh, and M. Welsh, "The advanced health and disaster aid network: A light-weight wireless medical system for triage," *Biomedical Circuits and Systems, IEEE Transactions on*, vol. 1, no. 3, pp. 203 –216, sept. 2007.

[79] K. L. Kraemer, J. Dedrick, and P. Sharma, "One laptop per child: vision vs. reality," *Communications of ACM*, vol. 52, pp. 66–73, June 2009.

[80] D. L. Johnson, E. M. Belding, K. Almeroth, and G. van Stam, "Internet usage and performance analysis of a rural wireless network in macha, zambia," in *Proc. of ACM Workshop on Networked Systems for Developing Regions*, ser. NSDR '10, 2010, pp. 7:1–7:6.

[81] P. Hande, S. Rangan, and M. Chiang, "Distributed uplink power control for optimal sir assignment in cellular data networks," April 2006, pp. 1–13.

[82] B. Radunovic and J.-Y. Le Boudec, "Joint Scheduling, Power Control and Routing in Symmetric, One-dimensional, Multi-hop Wireless Networks," in *WiOpt'03: Modeling and Optimization in Mobile,Ad Hoc and Wireless Networks*, 2003.

[83] M. Cao, V. Raghunathan, S. Hanly, V. Sharma, and P. Kumar, "Power control and transmission scheduling for network utility maximization in wireless networks," in *Proc. of Decision and Control*, Dec. 2007.

[84] G. Foschini and Z. Miljanic, "A simple distributed autonomous power control algorithm and its convergence," *IEEE Transactions on Vehicular Technology*, vol. 42, no. 4, pp. 641–646, Nov 1993.

[85] S. wook Han, H. Kim, and Y. Han, "Distributed utility-maximization using a resource pricing power control in uplink ds-cdma," *Communications Letters, IEEE*, vol. 12, no. 4, pp. 286–288, April 2008.

[86] K. Ramachandran, R. Kokku, H. Zhang, and M. Gruteser, “Symphony: synchronous two-phase rate and power control in 802.11 wlans,” in *Proc. of Mobile systems, applications, and services (MobiSys)*. ACM, 2008, pp. 132–145.

[87] J. P. Monks, V. Bharghavan, and W. M. W. Hwu, “A power controlled multiple access protocol for wireless packet networks,” in *Proc. of IEEE INFOCOM*, vol. 1, 2001, pp. 219–228 vol.1. [Online]. Available: http://dx.doi.org/10.1109/INFCOM.2001.916704

[88] A. Muqattash and M. Krunz, “A single-channel solution for transmission power control in wireless ad hoc networks,” in *Proc. of Mobile ad hoc networking and computing (MobiHoc)*. New York, NY, USA: ACM, 2004, pp. 210–221.

[89] A. Sheth and R. Han, “Shush: reactive transmit power control for wireless mac protocols,” in *Proc. of Wireless Internet Conference (WICON*, July 2005, pp. 18–25.

[90] V. Shah and S. Krishnamurthy, “Handling asymmetry in power heterogeneous ad hoc networks: A cross layer approach,” *Proc. of Distributed Computing Systems*, vol. 0, pp. 749–759, 2005.

[91] A. Akella, G. Judd, S. Seshan, and P. Steenkiste, “Self-management in chaotic wireless deployments,” in *Proc. of Mobile computing and networking (MobiCom)*. ACM Press, 2005, pp. 185–199. [Online]. Available: http://dx.doi.org/10.1145/1080829.1080849

[92] T.-S. Kim, H. Lim, and J. C. Hou, “Improving spatial reuse through tuning transmit power, carrier sense threshold, and data rate in multihop wireless networks,” in *Procc of Mobile computing and networking (MobiCom)*. New York, NY, USA: ACM, 2006, pp. 366–377.

[93] D. Qiao, S. Choi, A. Jain, and K. G. Shin, “Miser: an optimal low-energy transmission strategy for ieee 802.11a/h,” in *Proc. Mobile computing and networking (MobiCom)*. ACM, 2003, pp. 161–175.

[94] V. Mhatre, K. Papagiannaki, and F. Baccelli, “Interference mitigation through power control in high density 802.11 wlans,” in *Proc. of IEEE INFOCOM*, May 2007, pp. 535–543.

[95] S. Narayanaswamy, V. Kawadia, R. Sreenivas, and P. Kumar, “Power control in ad-hoc networks: Theory, architecture, algorithm and implementation of the compow protocol,” in *Proc. of European Wireless*, 2002.

[96] M. Johansson and L. Xiao, “Cross-layer optimization of wireless networks using nonlinear column generation,” *Wireless Communications, IEEE Transactions on*, vol. 5, no. 2, pp. 435–445, Feb. 2006.

[97] P. Castro, P. Chiu, T. Kremenek, and R. R. Muntz, “A probabilistic room location service for wireless networked environments,” in *Procc of international conference on Ubiquitous Computing (UbiCom)*, 2001, pp. 18–34.

[98] S. Sakagami, S. Aoyama, K. Kuboi, S. Shirota, and A. Akeyama, “Vehicle position estimates by multibeam antennas in multipath environments,” *IEEE Transactions on Vehicular Technology*, vol. 41, no. 1, pp. 63 –68, Feb. 1992.

[99] FootPath system: http://www.pathintelligence.com/en/products/footpath/footpath-technology.

[100] T. Jiang, H. J. Wang, and Y.-C. Hu, "Preserving location privacy in wireless LANs," in *Proc. of the conference on Mobile systems, applications and services*, 2007, pp. 246–257. [Online]. Available: http://dx.doi.org/10.1145/1247660.1247689

[101] J. H. Lee and R. M. Buehrer, "Location estimation using differential rss with spatially correlated shadowing," in *Proc. of IEEE conference on Global telecommunications (GLOBECOM)*, 2009, pp. 4613–4618.

[102] K. Bauer, D. McCoy, E. Anderson, M. Breitenbach, G. Grudic, D. Grunwald, and D. Sicker, "The directional attack on wireless localization: how to spoof your location with a tin can," in *Proc. of IEEE conference on Global telecommunications*, 2009, pp. 4125–4130.

[103] R. Nikjah and N. Beaulieu, "On antijamming in general CDMA systems-part ii: Antijamming performance of coded multicarrier frequency-hopping spread spectrum systems," *IEEE Transactions on Wireless Communications*, vol. 7, no. 3, pp. 888 –897, march 2008.

[104] B. Hoh and M. Gruteser, "Preserving privacy in gps traces via uncertainty-aware path cloaking," in *In Proceedings of ACM CCS*, 2007.

[105] H. Polat and W. Du, "Privacy-preserving top-n recommendation on horizontally partitioned data," in *Proceedings of the 2005 International Conference on Web Intelligence*, 2005, pp. 725–731. [Online]. Available: http://dx.doi.org/10.1109/WI.2005.117

[106] M. Gruteser and D. Grunwald, "Enhancing location privacy in wireless lan through disposable interface identifiers: a quantitative analysis," *Mobile Networks and Applications*, vol. 10, pp. 315–325, June 2005. [Online]. Available: http://dx.doi.org/10.1007/s11036-005-6425-1

[107] P. Krishnan, A. S. Krishnakumar, W.-H. Ju, C. Mallows, and S. Ganu, "A system for LEASE: Location estimation assisted by stationary emitters for indoor rf wireless networks." in *Proc. of IEEE Computer and Communications Societies (INFOCOM)*, 2004.

[108] F. Hermanns, "Protection of the european space infrastructure ist project satnex ja2350 network security and management."

[109] E. Adams and P. Hill, "Detection of direct sequence spread spectrum signals using higher-order statistical processing," in *Proc. of IEEE Acoustics, Speech, and Signal Processing*, vol. 5, apr 1997, pp. 3849 –3852 vol.5.

[110] Z. Zhijin and P. Junjie, "A detection method of DS-CDMA signal based on the quadratic fourth-order moment chip," in *Proc. of Networks Security, Wireless Communications and Trusted Computing*, vol. 2, april 2009, pp. 759 –762.

[111] T. Zhang, S. Dai, W. Zhang, and G. Ma, "Blind estimation of the PN sequence for weak DSSS signals in dynamic environments," in *IEEE Singapore International Conference on Communication Systems*, nov. 2008, pp. 470 –474.

[112] T. Jiang, H. J. Wang, and Y. C. Hu, "Preserving location privacy in wireless lans," in *Proc. of Mobile systems, applications and services (MobiSys)*, New York, NY, USA, 2007.

[113] A. S. R. Elbadry and M. Youssef, "Hyberloc: providing physical layer location privacy in hybrid sensor networks," in *IEEE Ad-Hoc, Sensor and Mesh Networking Symposium*, 2010.

[114] B. Van Veen and K. Buckley, "Beamforming: a versatile approach to spatial filtering," *IEEE ASSP Magazine*, vol. 5, no. 2, pp. 4 –24, april 1988.

[115] H. Urkowitz, *Signal Theory and Random Processes*. Artech House, 1983.

[116] Y. Qi, H. Kobayashi, and H. Suda, "Analysis of wireless geolocation in a non-line-of-sight environment," *IEEE Transactions on Wireless Communications*, vol. 5, no. 3, pp. 672–681, 2006.

[117] Y. Chen and A. Terzis, "On the mechanisms and effects of calibrating rssi measurements for 802.15.4 radios," in *Proc. of European Conference on Wireless Sensor Networks (EWSN)*, 2010, pp. 256–271.

[118] A. Hatami, K. Pahlavan, M. Heidari, and F. Akgul, "On RSS and TOA based indoor geolocation - a comparative performance evaluation," in *IEEE Wireless Communications and Networking Conference*, vol. 4, april 2006, pp. 2267 –2272.

[119] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proc. of Mobile computing and networking (MobiCom)*, 2008, pp. 116–127. [Online]. Available: http://doi.acm.org/10.1145/1409944.1409959

[120] "GNU Radio: the gnu software radio," www.gnu.org/software/gnuradio.

[121] http://ettus-apps.sourcerepo.com/redmine/ettus/projects/uhd/wiki.

[122] R. V. Ne, *OFDM for Wireless Multimedia Communications*. Artech House Universal Personal Communications, 1999.

[123] G. Malmgren, "Impact of carrier frequency offset, doppler spread and time synchronization errors in OFDM based single frequency networks," in *Global Telecommunications Conference*, vol. 1, Nov. 1996, pp. 729–733.

[124] https://www.cgran.org/wiki/ftw80211ofdmtx.

[125] H. Toyoizumi and M. Genda, "Precise 1PPS signal by GPS," *IEEJ Transaction on Electronics Information and Systems*, vol. 125, no. 8, pp. 1217–1222, 2005.

[126] P. Vyskocil and J. Sebesta, "Relative timing characteristics of GPS timing modules for time synchronization application," in *Proc. of Satellite and Space Communications*, Sep. 2009, pp. 230 –234.

[127] D. Raychaudhuri, I. Seskar, M. Ott, S. Ganu, K. Ramachandran, H. Kremo, R. Siracusa, H. Liu, and M. Singh, "Overview of the ORBIT radio grid testbed for evaluation of next-generation wireless network protocols," in *IEEE Wireless Communications and Networking Conference (WCNC)*, 2005.

[128] K. Kaemarungsi and P. Krishnamurthy, “Properties of indoor received signal strength for wlan location fingerprinting,” in *Mobile and Ubiquitous Systems: Networking and Services (MOBIQUITOUS)*, aug. 2004, pp. 14 – 23.

[129] J. Li, X. Sun, P. Huang, and J. Pang, “Performance analysis of active target localization using TDOA and FDOA measurements in WSN,” in *Proc. of the Advanced Information Networking and Applications - Workshops*, 2008, pp. 585–589.

[130] I. J. Quader, B. Li, W. Peng, and A. G. Dempster, “Use of fingerprinting in Wi-Fi based outdoor positioning,” in *Proc. of International Global Navigation Satellite Systems Society IGNSS Symposium*, 2007.