PHYSICAL LAYER VOTING FOR SECURE AND FAST COOPERATION

by

Bocan Hu

A Thesis Submitted to the Faculty of the

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

In Partial Fulfillment of the Requirements
For the Degree of

MASTER OF SCIENCE

In the Graduate College

THE UNIVERSITY OF ARIZONA

2 0 1 5

STATEMENT BY AUTHOR

This thesis has been submitted in partial fulfillment of requirements for an advanced degree at The University of Arizona and is deposited in the University Library to be made available to borrowers under the rules of the Library.

Brief quotations from this thesis are allowable without special permission, provided that accurate acknowledgment of the source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the head of the major department or the Dean of the Graduate College when in his or her judgement the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

SIGNED: _____

APPROVAL BY THESIS DIRECTOR

This thesis has been approved on the date shown below:

_____ _____

Loukas Lazos
Associate Professor of
Electrical and Computer Engineering

Date

ACKNOWLEDGMENTS

I would like to take the opportunity to thank all the people that made this thesis possible. First and foremost, I would like to thank my academic advisor Dr. Loukas Lazos. His passion encouraged me to pursue my own goals, while his attention to detail instilled in me a unique perspective on which to approach problems. I am deeply grateful for taking me on as a student. Our academic work together has been a truly rewarding and enriching experience, while the lessons learned will help guide me throughout the course of my life in whatever avenue I pursue.

I would also like to thank the members of my defense committee, Dr. Roman Lysecky and Dr. Jonathan Sprinkle for both supporting my degree goals and providing valuable feedback to my research. I am deeply indebted to my family for being there with me through thick and thin and their unconditional love and support that has inspired me to strongly pursue my goals.

Finally, I would like to acknowledge the US National Science Foundation (NSF) and the US Army Research Office (ARO) for the financial support provided to conduct the research needed for this Thesis. This research was supported in part by the NSF under grants CNS-1409172, CNS-0844111, and CNS-1016943 and ARO grant W911NF-13-1-0302. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the NSF and the ARO.

To my parents for their unconditional love

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Distributed wireless networks often employ voting to perform critical network functions such as fault-tolerant data fusion, cooperative sensing, leader election, and others. The voting process involves the exchange of messages between the network participants and a fusion center (centralized voting) or just between the participants (distributed voting). However, the messaging and delay overheads associated with reaching consensus can be prohibitive when voting is frequent. If secure voting is required, additional overheads for voter authentication and vote integrity verification are incurred.

In this thesis, *we investigate distributed voting mechanisms for secure and fast cooperation*. We develop a fast PHY layer voting scheme called PHYVOS which significantly reduces the communication overhead for reaching consensus. In PHYVOS, wireless devices transmit their votes to a fusion center simultaneously, by exploiting the subcarrier orthogonality in OFDM systems. By implementing the voting process at the PHY layer, no explicit messaging is necessary between the wireless devices and the fusion center. The voting process is completed with the transmission of just a few symbols. This significantly reduces the delay until the voting is completed, thus making PHYVOS ideal in application scenarios where voting occurs frequently.

We show that PHYVOS is secure against attackers that attempt to manipulate the tallying result. Security is achieved without employing cryptography-based authentication and message integrity schemes. We rely on the difficulty of erasing energy from a subcarrier to ensure the voting robustness to attacks. We analyze various practical implementation challenges related to received power variation, transmitter synchronization, frequency offset estimation, and interference from co-existing wireless systems. Finally, we present results from a prototype implementation of PHYVOS on an experimental platform.

CHAPTER 1

INTRODUCTION

1.1 Motivation and Scope

Distributed wireless networks rely on the principle of user's cooperation. Network participants often share information to coordinate network functions or improve the fault tolerance of distributed operations. As an example, cooperative spectrum sensing is known to improve the detection of licensed user activity in cognitive radio networks (CRNs) in multi-path fading and shadowing environments [2, 5]. The so called cooperative gain comes from exploiting the spatial diversity of the RF sensing operation, when sensing observations are fused. Similarly, data fusion is widely used in wireless sensor networks (WSNs) for improving the performance of target detection, target tracking, and distributed sensing [3].

For many cooperative functions, binary consensus algorithms increase fault-tolerance at relative low cooperation overhead. In binary consensus, a community of distributed entities shares binary decisions ("yes" or "no") on a parameter of interest (e.g., channel idle/busy state, presence of a target) [4, 5, 11]. A combining decision rule is applied to collectively determine the parameter value. This rule is based on some form of majority voting, plurality or threshold, to achieve the desired level of reliability. Binary votes are casted using a messaging scheme, in which 1-bit votes are carried by messages. For wireless networks, 1-bit votes require the transmission of a preamble, a PHY header and a MAC layer header. This communication and delay overhead can be prohibitive for applications where voting is applied frequently. As an example, in CRNs, channel state observations are fused every 2 seconds [19]. For control applications in networked multi-agent systems, the consensus time requirement could be even more stringent [43].

The voting delay is amplified by the application of medium access control on

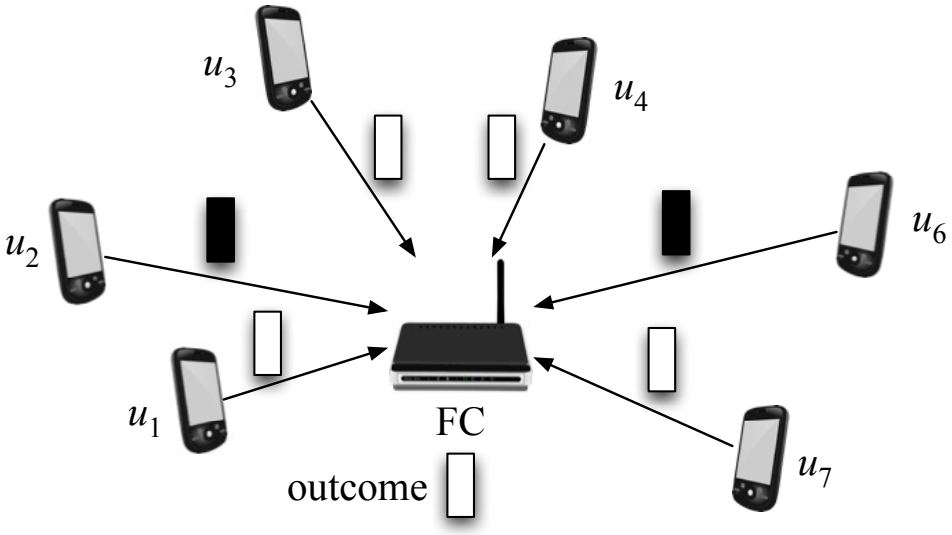


Figure 1.1: The PHYVOS voting scheme.

the wireless medium. Moreover, for applications where secure voting is required, additional overheads are incurred. To prevent an attacker from altering the voting outcome by inserting fake votes or modifying legitimate ones, cryptographic methods for user authentication and message integrity are applied. Verifying the voter authenticity and protecting the integrity of binary votes using digital signatures and message authentication codes could further increase the cooperation cost by several orders of magnitude.

To address the limitations of message-based voting, we present a secure voting scheme called PHYVOS that implements voting at the PHY layer. The basic principle of PHYVOS is shown in Figure 1.1. A set of wireless devices acting as voters exploit the subcarrier orthogonal in the widely adopted orthogonal frequency division modulation (OFDM), to simultaneously cast their votes to a fusion center (FC) within just a few symbols. The FC receives the superposition of all transmissions and tallies all votes to compute the voting outcome, without demodulating the received signal. Implementing secure voting at the PHY layer involves new security and implementation challenges.

- Voting at the PHY layer is susceptible to false vote insertion and vote modification attacks, similarly to message-based voting. An adversary can alter the voting outcome by exploiting the open nature of the wireless medium and manipulating the transmitted signals at the PHY layer. Without access to cryptographic primitives such as digital signatures and message authentication codes, securing the voting process is particularly challenging.

- The superposition of simultaneous transmissions from spatially-separated senders (voters) to a combined OFDM signal at a single receiver (fusion center) requires intricate transmitter and receiver designs [12, 37]. Senders must be synchronized in frequency and time to achieve symbol alignment at the receiver. Maintaining distributed synchronization in time and frequency could incur prohibitive coordination overheads [37], to be useful for fast voting.

1.2 Main Contributions

We design PHYVOS, a PHY-layer majority voting scheme that reduces the cooperation cost by several orders of magnitude compared to message-based voting. In PHYVOS, participants simultaneously cast their votes by exploiting the subcarrier orthogonality of OFDM. Wireless devices simultaneously cast their votes to a fusion center using orthogonal subcarriers. The fusion center tallies all votes and computes the voting outcome.

To overcome the challenges related to decoding simultaneous transmissions from multiple senders, binary votes are casted by adding energy to designated subcarriers. Therefore, no transmission of preambles and headers is required, as the receiver does not demodulate the OFDM signal. Simple energy detection suffices. Moreover, relying on energy detection rather than the decodable of message for vote casting strengthens the security of our scheme, as it is generally hard to "erase" energy from a channel. An attacker could still attempt to modify votes by inserting his own energy into various subcarriers. We reduce the probability of voting

outcome manipulation by executing multiple voting rounds. Since a voting round only lasts for a few OFDM symbols, executing multiple rounds is still far more efficient than applying message-based voting. We analytically evaluate the voting robustness as a function of the number of voting rounds. We further discuss practical implementation challenges of PHYVOS related to frequency and time synchronization. Finally, we present a prototype implementation of PHYVOS on the NI USRP platform.

1.3 Thesis Organization

In Chapter 2, we describe the basics of OFDM. We further present the state-of-the-art in voting schemes for wireless networks. In Chapter 3, we state the system and adversary models and develop the PHYVOS scheme for implementing physical layer voting. We describe the method for the simultaneous vote casting by the wireless devices, the reception of the superimposed signals at the fusion center, and the tallying of the voting outcome. The security of PHYVOS to vote insertion, deletion, and modification attacks is analyzed in Chapter 4. We show that PHYVOS is robust to an adversary who attempts to manipulate the tallying result. In Chapter 5, we provide details on practical considerations on the implementation of PHYVOS, such as the frequency offset estimation at the fusion center, time synchronization between the voters, and selection of the power threshold for tallying a vote. We also evaluate the communication and time efficiency of PHYVOS compared with message-based voting schemes. Finally, we present the results from the experimental implementation of PHYVOS. We summarize the contributions of this thesis and present future research directions in Chapter 6.

CHAPTER 2

PRELIMINARIES AND RELATED WORK

In this chapter, we present the basic operational details of OFDM systems. We further highlight prior art in voting mechanisms applied to wireless networks.

2.1 OFDM Basics

Orthogonal frequency-division multiplexing (OFDM) is a multi-carrier modulation method for encoding data over multiple carrier frequencies. It has developed as a popular system for wide band digital communications and it is used in many contemporary wireless technologies including digital television and audio broadcasting, DSL Internet access, WiFi networks, power line networks, and 4G mobile communications [1, 20, 34, 39]. OFDM is primarily adopted due to its high spectral efficiency and its ability to combat frequency-selective fading without complex equalization filters [6, 31]. Channel equalization is simplified due to the encoding of the information over many slow-modulated narrowband signals rather than one rapid-modulated wide band signal. The low symbol rate makes it possible to eliminate inter-symbol interference (ISI) through the use of short guard intervals.

In wireless communications, the power spectrum is not consistent over the entire frequency band. This frequency selectivity can cause significantly high bit error rates due to deep fading in some parts of the spectrum. In OFDM, frequency selectivity is mitigated by dividing the available bandwidth to overlapping frequency bands centered around a set of subcarriers. The subcarrier spacing is carefully selected so that subcarriers remain orthogonal. The orthogonal principle eliminates inter-carrier interference. That means that the cross-talk between the sub-channels is eliminated and inter-carrier guard bands are not required. This design simplifies both the transmitter and the receiver and significantly improves the spectral effi-

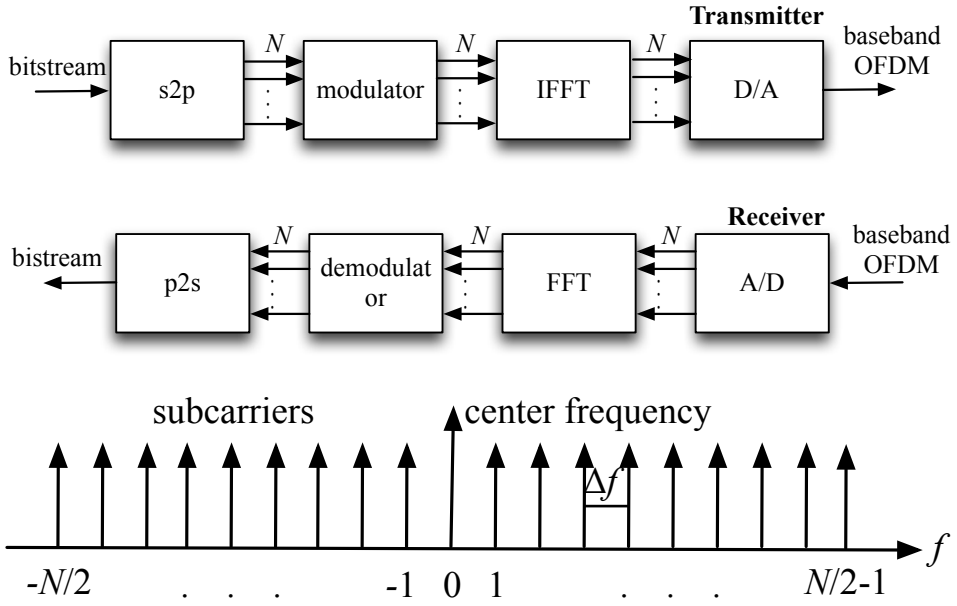


Figure 2.1: Block diagram of OFDM.

ciency of the system. Unlike conventional frequency division multiplexing (FDM), a separate filter for each subcarrier is not required. The orthogonal requires that the subcarrier spacing is set to

$$\Delta f = \frac{k}{T_s}, \tag{2.1}$$

where T_s denotes the duration of each symbol, and k is a positive integer, typically equal to 1. Hence, the subcarrier frequency of each sub-channel is determined by

$$f_k = \frac{k}{NT_s}, \tag{2.2}$$

where N denotes the total number of subcarriers. For N sub-carriers, the total passband bandwidth utilized by OFDM is

$$B = N\Delta f. \tag{2.3}$$

The main idea of OFDM is to divide the data stream to sub-streams, which are independently modulated in closely separated, orthogonal subcarriers. A basic block diagram of an OFDM system is shown in Figure 2.1. The data steam is transmitted through a serial-to-parallel (s2p) converter to generate N bit streams.

The N streams are modulated by digital modulation such as BPSK, QPSK, etc. An N-point inverse Fourier transform (IFFT) is applied on the complex symbols. The IFFT output is fed to a parallel-to-serial (p2s) converter and further processed by a D/A converter to compose the baseband OFDM signal. At the receiver, after the down conversion to the baseband frequency, the analog signal is digitized by the A/D converter. The Fourier transform is used to recover the complex constellation symbols. The N sub-streams are combined by the parallel to serial converter to recover the original data stream. The discrete time domain representation of the baseband OFDM signal $x(n)$ is given by [38]:

$$x(n) = \sum_{k=0}^{N-1} x_k(n) * e^{\frac{j2\pi nk}{N}} \tag{2.4}$$

where $x_k(n) \in \{\alpha_1, \alpha_2, ..., \alpha_q\}$ is the complex modulated symbol at each of the N subcarriers transmitted during at time n, and $\alpha_1, \alpha_2, ..., \alpha_q$ are the possible modulation symbol values (q denotes the modulation order). By selecting $x_k(n)$, we can control the energy that is injected at each of the N subcarriers. This energy is detected at an OFDM receiver by passing the time domain signal through an FFT. The energy detection at each subcarrier is the basic PHY-layer function exploited by PHYVOS for implementing the voting process.

2.1.1 OFDM Transmitter

The block diagram of an OFDM transmitter is shown in Figure 2.2. A binary input sequence $s(n)$ is split into N parallel streams when passed through a serial-to-parallel converter. Each sub-stream is modulated according to a given modulation scheme such as BPSK, QAM, QPSK, etc. Note that different modulations can be applied on individual sub-streams. After the constellation mapping, the N complex symbol data points are passed through an N-point IFFT. The IFFT output is fed to a p2s converter to form a single data stream. This data stream is then converted to the baseband OFDM signal by passing through a digital-to-analog converter (DAC). Finally, the baseband signal is raised to the carrier frequency f_c

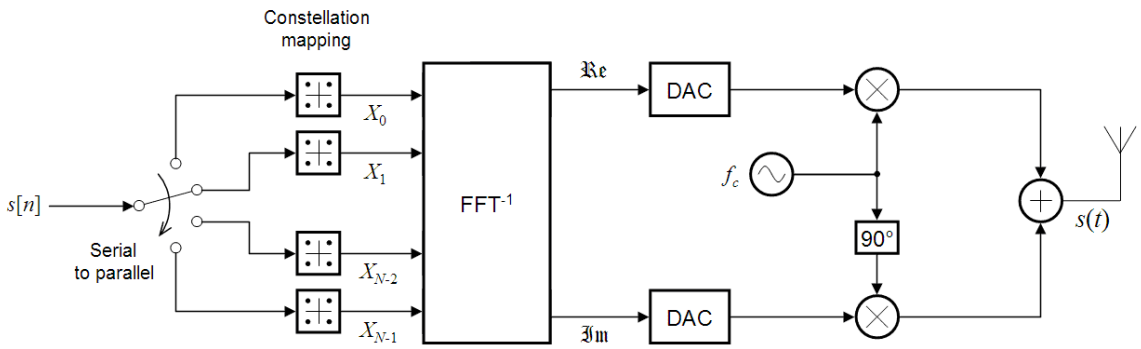


Figure 2.2: Block diagram of an OFDM transmitter

and transmitted into the channel.

2.1.2 OFDM Receiver

The receiver applies the reverse steps to recover the original data stream $s(n)$. These steps are outlined in Figure 2.3. Initially, the received signal is multiplied by the sine and cosine waves raised to the carrier frequency, in order to bring the received signal to baseband. The baseband signal is sampled in an analog-to-digital converter (ADC) to discretize it. The data corresponding to the cyclic prefix guard interval are removed from the sample sets. The sample stream is passed through an N-point FFT to recover the N constellation symbols sent by the transmitter. These constellation symbols are corrupted by the channel and the frequency offset between the transmitter and the receiver. To compensate for such distortions, channel and frequency offset estimation processes are applied. The N constellation symbols are then passed via N symbol detectors to be converted into N data sub-streams. Finally, the parallel-to-serial converter recovers the original data stream $s(n)$.

For a comprehensive review of the operational details of the OFDM system, interested readers are referred to the following books [6, 31].

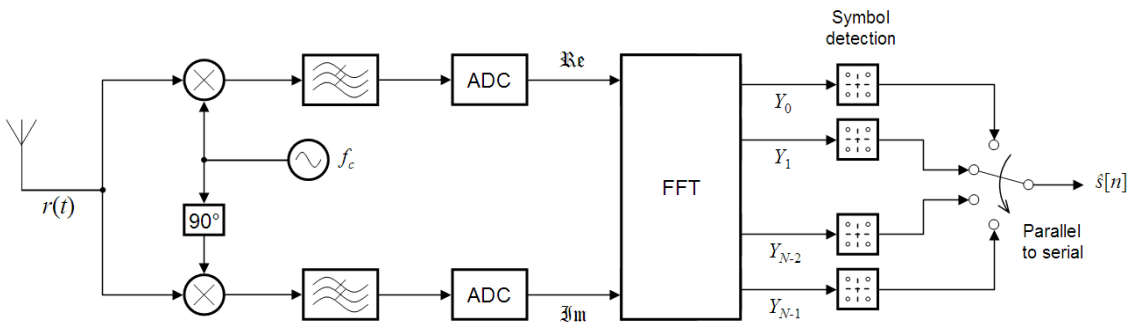


Figure 2.3: Block diagram of an OFDM receiver

2.2 Adoption of OFDM in Standards

Many standards have adopted an OFDM design for transmitting data due to its high spectral efficiency. In this section, we give a brief overview of the OFDM use in those standards. We categorize the standards into two classes; those used for wireless communications and those used for wired ones.

2.2.1 Wireless OFDM Standards

In this section, we give a brief overview of the OFDM implementation in different wireless standards. The IEEE 802.11 family provides the MAC and PHY layer specifications for implementing wireless local area networks (WLANs) [17]. The 802.11a protocol was the first one to adopt the OFDM modulation at the PHY layer. The standard operates over the 2.4GHz and 5GHz bands and uses 52 orthogonal subcarriers including 48 data subcarriers and 4 pilot subcarriers. All data subcarriers use same modulation type. Pilot subcarriers always use BPSK modulation and transmit known symbols. The basic structure of an 802.11a frame contains the preamble field, the signal field, and data fields. The preamble signal is used for synchronization and channel equalization. The signal field contains information such as the packet length, the modulation type and the data rate. The data field contains the packet payload. Depending on the modulation type, 802.11a

supports multiple data rates. The maximum data rate is capped at 54Mbps. Table 2.1 lists some parameters associated with OFDM in 802.11a.

Table 2.1: OFDM parameters in 802.11a.

Parameter	:	Value
Total number of subcarriers	:	52
Data subcarriers	:	48
Pilot subcarriers	:	4
Subcarrier frequency spacing	:	312.5KHz
Symbol length	:	4 μs
Data field length	:	3.2 μs
Guard interval	:	0.8 μs
FFT/IFFT period	:	3.2 μs
Preamble length	:	16 μs
FFT sample size	:	64 point

OFDM is also part of newer 802.11 standards which support higher data rates, including 802.11g, 802.11n, and 802.11ac. Moreover, OFDM is part of the IEEE 802.15 group of standards, which is targeted for wireless personal area networks (WPANs). The IEEE 802.15.3a protocol specifies the MAC and PHY operations for WPANs and supports a data rate up to 55Mbps. In 2002, the FCC liberated the framework for the unlicensed use of approved ultra wide band (UWB) devices over the 3.1-10.6GHz bands. To achieve a wide bandwidth signal with a low level of complexity and adaptability to different spectrum regulatory environments, multi-band OFDM UWB radios divide the available spectrum into fourteen sub bands. Each sub band is 528MHz wide. The first twelve bands are grouped into band groups 1 to 4 and the last two bands belong to the fifth group. Currently, only the first band group is mandatory. A total of 128 subcarriers are designed in each band including 10 pilot subcarriers and 100 data subcarriers. A 60.6ns cyclic prefix is pre-pended in each OFDM symbol, which is also followed by a 9.5ns guard

interval [52].

IEEE 802.16 is a group of broadband wireless communication standards for metropolitan area networks (WMANs), which is designed to operate in the 2GHz - 11GHz range. IEEE 802.16, which is typically referred to as WiMax, defines three standards for the PHY interface: WirelessMAN-SCa, WirelessMAN-OFDM and WirelessMAN-OFDMA. In IEEE 802.16d, 128 subcarriers are used in the WirelessMAN-OFDM PHY interface, which includes 96 data subcarriers, 28 null subcarriers as guard-bands, and 4 pilot subcarriers [14]. Up to 2048 subcarriers can be used in the WirelessMAN-OFDMA interface. OFDMA is a multiple user version of OFDM. In OFDMA, multiple access is achieved by assigning subsets of subcarriers to individual users. WiBro (IEEE 802.16e) is a wireless broadband internet technology is developed by South Korea which adopts OFDMA for multiple access [25]. In WiBro, the numbers of subcarriers are flexible and can be set to 128, 256, 512, or 1024 to achieve a desired level of scalability. The channel bandwidth is set to 10MHz.

IEEE 802.20, or Mobile Broadband wireless access (MBWA), is a group of standards for mobile wireless Internet access. IEEE 802.20 works below 3.5GHz and has an efficient packet-based air interface that is optimized for supporting IP-based services [9]. The standard includes an OFDMA wide-band mode and a 625 k-multi carrier mode. The numbers of subcarriers in IEEE 802.20 are 512, 1024, or 2048. The varying number of subcarriers provide a flexible channel bandwidth which can vary from 1.25MHz to 40MHz [16]. IEEE 802.20 can support up to 100 users per cell although not all of them may be active at once [18].

Digital Video Broadcasting (DVB) is an international open standard for digital television, which adopt the OFDM design at the PHY layer in the specification of the DVB-T (terminal) and DVB-H (handheld) [53]. The DVB-T OFDM signal has either 2K, 4K, or 8K subcarriers, depending on the operating mode [21]. The DVB-H system is defined based on the existing DVB-T standard for fixed and in-car reception of digital TV. DVB-H permits transmission of very large files and

can operate on 5, 6, 7 or 8MHz bandwidth. Compared to DVB-T, the 4k OFDM mode in DVB-H is adopted for trading off mobility and single-frequency network (SFN) cell size, allowing single-antenna reception in medium SFNs at very high speeds [15].

Digital Audio Broadcasting (DAB) is a digital radio technology for broadcasting radio stations. It is currently deployed in several countries, primarily in Europe. DAB adopts OFDM for carrier modulation. This particular coded multi carrier system is referred to as COFDM. The COFDM frame contains a null symbol for signaling the start of a frame, a phase reference symbol with fixed magnitude and phase in each subcarrier, and data symbols [48]. Digital Radio Mondale (DRM) is a OFDM-based standard used for short, medium, and long range communication. The maximum bandwidth of a DRM signal is less than 95kHz and the number of carriers is 40 [45]. Terrestrial-Digital Multimedia broadcasting (T-DMB) is based on Eureka 147. In T-DMB, 256 subcarriers are used in OFDM and the channel bandwidth is 1.536MHz [36]. ISDB-TSB is the terrestrial digital sound broadcasting specification for ISDB-T, which was first designed by Japan [47].

2.2.2 Wireline OFDM Standards

Due to the high spectral-efficiency, many wire line standards use OFDM as a modulation at the PHY layer, including ADSL/VDSL, MoCA and PLC. The digital subscriber line (DSL) standard achieves high data rates (for ADSL up to 6Mbps and for VDSL up to 100Mbps) based on OFDM running over copper wires. In DSL, OFDM is called discrete multi tone modulation (DMT). Uplink is operated from 26KHz to 138KHz. DMT is used in ADSL connections that follow the ANSI T1.413 and G.dmt (ITU G.992.1) standards. In ADSL, 138KHz are provided for uplink and 1.1MHz are provided as downlink. The frequency band is divided into 256 subcarriers with bandwidth 4.3125KHz [35]. The very-high-bit-rate digital subscriber line (VDSL) achieved data transmissions faster than ADSL downstream due to its higher bandwidth and the use of 4096 orthogonal subcarriers [35].

The Multimedia over Coax Alliance (MoCA) is a standard specification that allows the distribution of multimedia and data over coaxial cable infrastructures. MoCA operates from 850MHz to 1500MHz for the downlink and supports a raw data rate of 270Mbps. At the physical layer, OFDM subcarriers are modulated using a 256 QAM modulation and Reed Solomon forward error correction [10]. Finally, power line Communication (PLC) is a communication technology that enables the transmission of modulated data over power cables. PCL uses OFDM at the PHY layer and supports up to 4096 subcarriers [42].

2.3 Related Work

The use of voting for improving reliability has been studied since the 1950s [50], with a long literature on various reliability and efficiency aspects [7]. In the context of wireless networks, voting finds wide application to data fusion, intrusion detection and secure localization in WSNs [3,22–24,54], [27], real time coordination in multi-agent systems [43], fault-tolerant protocols [29, 32], and distributed spectrum sensing in CRNs [2]. The de facto voting mechanism adopted in these works is message-based voting, in which votes are casted through messaging. Message-based voting also facilities the integration of security measures for preventing the manipulation of the voting outcome. Voters can be authenticated, and vote integrity can be verified using standard cryptographic primitives such as digital signatures, message authentication codes, and digital certificates [2]. Compared to message-based voting, PHYVOS requires significantly less communication overhead, without sacrificing robustness to vote manipulation.

The messaging overhead for implementing majority voting has primarily been a concern in distributed consensus protocols. A wealth of prior works on gossip algorithms have been devoted to fine-tuning tradeoffs between the voting outcome accuracy, the messaging overhead, and the time until a consensus is reached [44]. The majorityiesof gossip algorithms were not designed with security in mind and

are susceptible to manipulation by internal and external entities. Our setup differs from that of gossip algorithms in that we consider a centralized, one-hop topology. This topology can arise in infrastructure based networks following a client-base station model, and in distributed networks where majority voting is used for taking local decisions or performing aggregation [33].

In [13], the authors established an electronic voting scheme using GSM. The voters were authenticated based on the credentials of their GSM cellphone and votes are sent through GSM network. Voters and their votes cannot be linked and votes remain secret until the final counting. Through GSM authentication infrastructure, a public-key-based solution is avoided.

Form an implementation standpoint, the most relevant works to ours are presented in [12, 37]. In [12], Dutta et al. proposed SMACK, an acknowledgment scheme for implementing a reliable broadcast service. Similar to PHYVOS, SMACK exploits the subcarrier orthogonality of OFDM to allow the simultaneous submission of acknowledgements in response to a broadcast message transmitted by a single source. The authors outline system implementation details related to the concurrent symbol transmission over different subcarriers and the reception of a combined OFDM symbol. To combat the problems of frequency and time synchronization, the detection of individual ACKs is based on energy and not demodulation, similar to our scheme. However, verification of the ACK integrity is beyond the scope of the SMACK design. A single attacker could emulate ACK responses for all broadcast receivers, by transmitting an OFDM symbol with energy on all subcarriers.

In [37], Rahul et al. propose SourceSync, a distributed wireless architecture that explores sender diversity in OFDM. SourceSync enables the reception and demodulation of OFDM symbols composed of symbol transmissions over individual subcarriers by a diverse set of senders. Contrary to SMACK and PHYVOS, SourceSync can demodulate the combined OFDM symbol and retrieve the individual data streams of each sender. This capability comes at the expense of complex symbol-

level synchronization and channel estimation at the senders, performed through the transmission of preambles. This additional communication overhead for maintaining tight synchronization and continuously estimating the channel makes the SourceSync solution inadequate for our purposes.

CHAPTER 3

PHYVOS: A PHYSICAL LAYER VOTING SCHEME

In this chapter, we state the network and adversary model assumptions. We then describe the operational details of PHYVOS, a physical-layer voting scheme that achieves robust voting with just a few symbol durations.

3.1 Network Model

We suppose a system that consists of a set $\mathcal{U} = \{u_1, u_2, \ldots, u_M\}$ with M voting participants. The participants cast M binary votes $v_1, v_2, \ldots, v_M$ with $v_i \in \{0, 1\}$ to a FC. The FC tallies all votes received from $\mathcal{U}$ and computes the voting outcome according to the following rule:

$$\mathcal{T} = \begin{cases} 1, & \text{if } \sum_{i=1}^{M} (-1)^{v_i} \leq \gamma \\ 0, & \text{if } \sum_{i=1}^{M} (-1)^{v_i} > \gamma. \end{cases} \tag{3.1}$$

In (3.1), if $\mathcal{T}$ is below a threshold value γ, the voting outcome is considered to be positive (a "yes" vote). Otherwise, the voting outcome is considered to be negative (a "no" vote). The value of γ is application-dependent. As an example, by setting $\gamma = 0$, a plurality rule is implemented. Other values of γ allow for more relaxed or stricter consensus rules. We emphasize that we are only interested in the robustness of the voting outcome. Well-known electronic voting requirements such as voter privacy, receipt-freeness, universal and individual verifiability, coercion-resistance and others are beyond the scope of our fast voting scheme. [41]. To this end, we define the following voting requirement.

Definition 1 (Robustness)**.** *A cooperative voting scheme is said to be robust against active attacks and faults if the voting outcome T reflects the true outcome when the votes of all honest participants are tallied.*

Note that the robustness requirement is different than the accuracy requirement, in which all votes must be tallied correctly. For the former, it is sufficient to reach the correct voting outcome, even if some votes are incorrectly tallied.

The participants cast their votes to the FC using an OFDM system with N orthogonal subcarriers, denoted by $f_1, f_2, \ldots f_N$. All participants can directly reach the FC (within one hop), but could be located at varying distances from the FC. Moreover, participants and the FC are loosely synchronized to a time-slotted system with a maximum synchonization error equal to δ_t. The FC shares a pairwise secret seed s_i with each participant u_i. The secret seed can be used to extract pairwise secret sequences between FC and u_i. These sequences are generated by the application of a cryptographically-secure pseudo random number generator [8, 49]. We note that these sequences are not used for encryption.

3.2 Adversary Model

We consider an external adversary who launches active attacks on the voting process, by injecting OFDM signals of his own choosing. The adversary aims at modifying the voting outcome $\mathcal{T}$ at the FC to a desired value. This model is also equivalent to an internal adversary who launches active attacks on the remaining honest participants. However, the adversary is not interested in launching denial-of-service attacks that will prevent the computation of a voting outcome at the FC. For instance, the adversary could inject energy on all subcarriers to deny the computation of any vote. Such an adversary is easily detectable and can be physically removed from the network.

The adversary is loosely synchronized to the FC with the same synchronization error as the rest of the participants. Moreover, he can observe the transmissions of the participants for long periods of time to observe the channels over which votes are casted. However, the adversary is not aware of the pairwise secret seeds shared between the FC and each participant. Without access to the individual

seeds, the adversary cannot infer the pseudo-random sequences generated by the cryptographically-secure pseudo random number generator.

We consider two models with respect to the secrecy of the votes.

Secret vote model: In the secret vote model, the adversary is unaware of the voting intent of each participant before votes are casted. That is, the vote values v_i remain secret. This model applies to general voting procedures in which the voting intent cannot be inferred ahead of time by observing some physical phenomena.

Open vote model: In the open vote model, the adversary knows the voting intent a priori. That is, the vote values v_i are known to the adversary for every $u_i \in \mathcal{U}$, before the votes are casted. This model is relevant when the vote intent is correlated to some observable phenomenon. As an example, if participants vote on the state of a channel (idle or busy), the adversary can predict the votes of the participants by sensing the channel ahead of time. Knowledge of the vote intent can assist the adversary in deciding which participants it should attack to modify the voting outcome.

3.3 Notation

The notation used in the remaining of the thesis is summarized in Table 3.1.

3.4 The PHYVOS scheme

In this section, we describe the operational details of the PHYVOS scheme. The key principle of PHYVOS is to simultaneously cast the votes by injecting energy on designated subcarriers. Energy detection is robust to active attacks and unintentional interference compared to vote decoding. An adversary attempting to modify a vote on subcarrier f_j, would have to "erase" the signal received by the FC on f_j and simultaneously inject energy on some other subcarrier. This is generally a hard problem that requires knowledge of the signal transmitted at

Table 3.1: Notation

$\mathcal{U}$:	set of voting participants
$u_1, u_2 \ldots, u_M$:	the M voting participants
v_i:	vote submitted by the i^{th} participant u_i
$v_i(n)$:	the symbol vote submitted by u_i during the n^{th} symbol transmission
$f_1, f_2, \ldots, f_N$:	the N subcarriers of the OFDM system
s_i:	random seed shared between u_i and the FC.
$R_i(s_i)$:	cryptographically-secure pseudo random binary sequence shared between u_i and FC
$\mathcal{T}$:	vote tally if all votes are correctly received
$\hat{\mathcal{T}}$:	estimated vote tally at the FC
γ:	vote threshold
μ:	vote margin
γ_D:	the vote detection threshold at the FC

f_j, the precise time that the signal was transmitted, the signal propagation delay, and precise channel state information. This information needs to be collected and synchronized for all voters.

The PHYVOS scheme consists of three phases; *the vote request phase, the vote casting phase, and the tallying phase*. In the vote request phase, the FC asks participants to cast their votes. In the vote casting phase, participants cast their votes by simultaneously transmitting over orthogonal subcarriers. In the tallying phase, the FC simultaneously receives OFDM symbols from participants and computes the voting outcome $\mathcal{T}$. We now describe each phase in detail.

3.4.1 Vote Request Phase

In the vote request phase, the FC signals to the participants for a vote. This phase is necessary to ensure that overhead gains are achieved by the simultaneous vote casting. Two mechanisms can be employed for requesting a vote: (a) periodic voting and (b) on-demand voting. In periodic voting, participants exploit their synchronization to a common time-slotted system to cast their votes at fixed intervals without an explicit request from the FC. This operation mode is suitable for periodic network operations. Take as an example the spectrum sensing operation at a CRN. The cognitive radios periodically sense the state of the channels and report their results to the FC. FC determines the idle portion of the spectrum to coordinate plectrum access

In on-demand voting, the FC broadcasts a vote request message to all participants to initiate the voting process. This operation mode is suitable for voting that is initiated as a response to some event. As an example, on-demand voting can occur if an application places an explicit request about the state of a parameter that is determined by distributed sensing. In both voting modes, the purpose of the vote request phase is to synchronize the participants, so that votes are casted simultaneously. The vote request phase is followed by the vote casting phase.

3.4.2 Vote Casting Phase

During the vote casting phase, participants simultaneously cast their votes to the FC. Each participant u_i is assigned two subcarriers f_1^i and f_2^i for casting his vote v_i. One subcarrier is used to cast a "yes" vote, while the other is used to cast a "no" vote. We note that in the absence of an adversary, a single subcarrier is sufficient to cast a binary vote (through the presence or absence of energy on that subcarrier). However, the adversary could easily modify the vote that corresponds to energy absence by injecting energy on the designated subcarrier. Therefore, we adopt a two-subcarrier solution.

Moreover, the subcarriers f_j^i and f_{j+1}^i assigned to u_i are not statically mapped to vote values. We use a secret pseudorandom binary sequence $R_i(s_i)$, shared between u_i and the FC, to randomize the mapping of vote values to subcarriers. This prevents the adversary from guessing the subcarrier where energy has to be injected to spoof a desired vote. Finally, we randomly select the transmitted symbol on the selected subcarrier to harden the nullification of the transmitted signal at the FC. Formally, vote casting involves the following steps.

1. Each u_i is assigned two subcarriers f_j^i and f_{j+1}^i.

2. Each u_i and the FC use a cryptographically-secure pseudorandom bit generator (PRBG) to individually generate a pairwise secret binary sequence, using s_i as a seed.

$$R_i(s_i) = \{r_i(n) = PRBG(n, s_i),\ n = 1, 2, \ldots\} \tag{3.2}$$

   In (3.2), the time n is quantized to the OFDM symbol duration.

3. Let voting be initiated at time n_0. To cast a vote $v_i \in \{0, 1\}$, a participant u_i casts ℓ *symbol votes* $v_i(n_0) = \ldots = v_i(n_0 + \ell - 1) = v_i$. Each $v_i(n)$ is represented by an OFDM symbol, with the following symbol values per subcarrier.

$$x_k(n) = \begin{cases} \alpha_y, & k = j + v_i \oplus r_i(n) \\ 0, & \text{otherwise,} \end{cases}, \quad n_0 \leq n < n_0 + \ell. \tag{3.3}$$

   where α_y is a randomly selected modulation symbol.

The vote casting phase for a set of M participants is depicted in Figure 3.1. Participant u_1 is assigned subcarriers f_1 and f_2, participant u_2 is assigned subcarriers f_3 and f_4, etc. Participants transmit $\ell = 4$ symbol votes to cast a vote. The votes for the individual participants are $v_1 = 1$, $v_2 = 0, \ldots,$ $v_M = 1$. Each participant u_i XORs his vote with the pseudorandom bit sequence $R_i(s_i)$ to determine

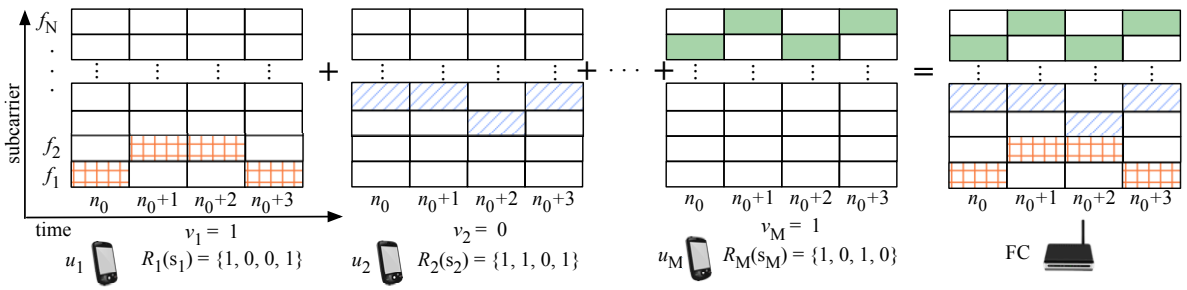


Figure 3.1: The vote casting phase for M participants voting over N subcarriers (here $N = 2M$) .

the subcarrier index where a symbol vote will be transmitted at each time slot n. The binary sequence $R_1(s_1)$ for u_1 is $1, 0, 0, 1$ and the binary sequence $R_2(s_2)$ is $1, 1, 0, 1$. Corresponding to the binary sequence, participant u_1 transmits symbol votes in f_1, f_2, f_2, f_1, participant u_2 transmits symbols votes in f_4, f_4, f_3, f_4, etc. The symbol votes arrive at the FC such that OFDM symbols are formed. The vote casting phase is followed by the vote tallying phase.

3.4.3 Vote Tallying Phase

In the vote tallying phase, the FC computes the voting outcome $\mathcal{T}$ according to (3.1). To infer the votes of each participant, the FC computes the FFT of the digitized baseband OFDM signal to separate the spectral components to each of the subcarriers. The FC then uses an energy detector at each output of the FFT block to detect the transmitted symbol votes. Note here that *no symbol demodulation is necessary to determine the presence of energy.* This process lasts for the duration of ℓ symbols that are used to submit the ℓ symbol votes. At time n, a symbol vote $v_i(n)$ is computed only if the detected average power is beyond a threshold γ_D on only one of the two designated subcarriers. If both subcarriers have an average power higher than γ_D (due to intentional or unintentional interference), or both have low power, the symbol vote is recorded in error. Formally, for a participant u_i, the recovery of v_i at the FC is performed as follows.

1. Sample the FFT output of subcarriers f_1^i and f_2^i assigned to u_i and compute the average received power over K samples:

$$p_j(n) = \frac{1}{K}\sum_{i=1}^{K}|y_j(i)|^2, p_{j+1}(n) = \frac{1}{K}\sum_{i=1}^{K}|y_{j+1}(i)|^2, \tag{3.4}$$

with $n_0 \leq n < n_0 + \ell$.

2. The symbol votes $v_i(n)$ are computed as:

$$v_i(n) = \begin{cases} 0 \oplus r_i(n), & \text{if } p_j(n) > \gamma_D, \quad p_{j+1}(n) \leq \gamma_D \\ 1 \oplus r_i(n), & \text{if } p_j(n) \leq \gamma_D, \quad p_{j+1}(n) > \gamma_D \\ e, & \text{otherwise.} \end{cases} \tag{3.5}$$

with $n_0 \leq n < n_0 + \ell$.

3. The final vote v_i is computed as:

$$v_i = \begin{cases} 0, & \text{if } \sum_{n=n_0, v_i(n)\neq e}^{n_0+\ell-1}(-1)^{v_i(n)} > 0 \\ 1, & \text{if } \sum_{n=n_0, v_i(n)\neq e}^{n_0+\ell-1}(-1)^{v_i(n)} < 0 \\ e, & \text{otherwise.} \end{cases} \tag{3.6}$$

In (3.5), we XOR the output with the pseudorandom sequence $R_i(s_i)$ shared between u_i and the FC to correctly map the subcarrier index to the vote value. Moreover, in (3.6) we discard all inconclusive symbol votes with value $v_i(n) = e$. Such votes could be the result of unintentional interference from systems operating over the same spectrum, or an active attack.

The tallying operation at the FC is shown in the example of Figure 3.1. For participant u_1, the FC detects an average power over γ_D on subcarriers f_1, f_2, f_2, and f_1. By XORing the output $\{0, 1, 1, 0\}$ with the random sequence $R_1(s_1) = \{1, 0, 0, 1\}$, it obtains the symbol votes $v_1(n_0) = 1$, $v_1(n_0 + 1) = 1$, $v_1(n_0 + 2) = 1$, and $v_1(n_0 + 3) = 1$, indicating a final vote $v_1 = 1$. Similarly, participant u_2 uses random sequence $R_2(u_2) = \{1, 1, 0, 1\}$ to compute $v_2 = 0$. The vote computation proceeds in parallel for all participants.

CHAPTER 4

SECURITY ANALYSIS

In this chapter, we evaluate the robustness of PHYVOS to an active adversary that attempts to flip the voting outcome $\mathcal{T}$. We first analyze the adversary's ability to modify a single vote v_i. After that, we extend our analysis to modifying the summary voting results $\mathcal{T}$ at the FC.

4.1 Modifying a Single Vote

To modify a vote v_i casted by u_i, the adversary can attempt to modify the ℓ symbol votes used in the computation of v_i. Let u_i select subcarrier f_1^i for transmitting $v_i(n)$, based on v_i and $r_i(n)$. Without knowledge of $r_i(n)$, determining the subcarrier used by u_i to cast $v_i(n)$ before $v_i(n)$ is transmitted, is equivalent to a random guess. The probability of a successful guess is equal to 0.5. Even if the adversary correctly guesses f_1^i, he cannot "erase" energy from f_1^i, in order to flip the value of $v_i(n)$. Erasure of the modulation symbol a_y transmitted by u_i requires the a priori knowledge of a_y, knowledge of the channel between the voter and the FC as well as the adversary and the FC, and precise synchronization between the voter and the adversary. We note that u_i randomly selects a_y for each symbol vote. Moreover, the channel between u_i and FC rapidly de-correlates with the distance from u_i. Unless the adversary is within a very short distance from u_i (within half a wavelength), the channel between u_i and FC becomes unpredictable [30].

The adversary can inject energy to f_2^i to nullify $v_i(n)$ (i.e., change the value of $v_i(n)$ from $v_i(n) = v_i$ to $v_i(n) = e$). According to (3.6), to nullify $v(i)$, all symbol votes $v_i(n_0), v_i(n_0+1), \ldots, v_i(n+0+\ell-1)$ must be nullified. This is equivalent to guessing the subcarrier index used by u_i to cast each of the ℓ symbol votes. As the subcarrier carrying each symbol vote is selected randomly (based on $R_i(s_i)$) and

independently, the probability of nullifying v_i becomes:

$$\begin{aligned} \Pr[v(i) = e] &= \Pr[v_i(n_0) = e, \ldots, v_i(n_0 + \ell - 1) = e] \\ &= 0.5^{\ell}. \end{aligned} \tag{4.1}$$

Note that (4.1) is true even if the value of v_i is known a priori, because v_i is XORed with $R_i(s_i)$ (see eq. (3.3)). From (4.1), we can select ℓ to drive $\Pr[v(i) = e]$ to any desired level.

4.2 Modifying the Voting Outcome

Let the vote tally used to compute the voting outcome $\mathcal{T}$ be equal to

$$\sum_{i}^{M} (-1)^{v_i} = \gamma + \mu.$$

Here, μ denotes the margin by which the tally exceeds the decision threshold γ (the case of $\sum_i^M = (-1)^{v_i} = \gamma - \mu$ is treated similarly). We analyze the probability of successfully modifying the voting outcome for the two adversary models defined in Section 3.2.

Proposition 1. *Under the secret vote model, an adversary can modify the voting outcome $\mathcal{T}$ for a decision threshold γ and a margin μ with probability*

$$\Pr[\hat{\mathcal{T}} \neq \mathcal{T}] = \sum_{i=\mu}^{\delta} HG(n_1, M, i, \delta) \sum_{z=\mu}^{i} \sum_{x=z}^{\min\{i, \frac{\delta+z}{2}\}} \frac{\binom{i}{x}\binom{\delta-i}{x-z}}{\binom{\delta}{2x-z}} B(2x - z, \delta, p),$$

where $n_1 = \frac{M+\gamma+\mu}{2}$ denotes the number of votes in favor of T_0, HG denotes the probability mass function of the hypergeometric distribution

$$HG(K, N, k, n) = \frac{\binom{K}{k}\binom{N-K}{n-k}}{\binom{N}{n}}, \tag{4.2}$$

B denotes the probability mass function of the binomial distribution

$$B(j, i, p) = \binom{i}{j} p^j (1-p)^{i-j}, \tag{4.3}$$

δ denotes the number of votes that the adversary attempts to nullify and $p = \Pr[v(i) = e]$ denotes the probability of nullifying a singe vote, which is given by equation 5.1.

Proof. For a voting outcome $\mathcal{T}$ selected with a margin μ, there are $n_1 = \frac{M+\gamma+\mu}{2}$ votes in favor of $\mathcal{T}$ and $n_2 = \frac{M-\gamma-\mu}{2}$ votes against T. Let the in favor votes be "yes" votes. To flip $\mathcal{T}$, the adversary must nullify at least μ more "yes" votes than "no" votes and drop the vote tally at or below γ. For an adversary that attempts to nullify a total of δ votes, the probability that i of them are "yes" votes is given by a hypergeometric distribution.

$$\Pr[I = i] = HG(n_1, M, i, \delta), \tag{4.4}$$

where I is an RV denoting the number of attacked "yes" votes when a total of δ votes are attacked. Each vote is successfully nullified with probability $p = \Pr[v_i = e] = 0.5^\ell$. Let X be an RV denoting the number of votes successfully nullified, when i are attacked. Because the nullification of each vote is an independent Bernoulli trial, X follows the binomial distribution

$$\Pr[X = x] = B(x, i, p), \quad p = 0.5^\ell. \tag{4.5}$$

Similarly let Y be an RV denoting the number of "no" votes that are successfully nullified. For Y, it also follows the binomial distribution

$$\Pr[Y = y] = B(y, \delta - i, p), \quad p = 0.5^\ell. \tag{4.6}$$

The probability that the number of successfully nullified "yes" votes exceeds the number of nullified "no" votes by exactly z votes is given by random variable $Z = X - Y$. The probability mass function of Z can be computed using the

convolution formula.

$$\begin{aligned}\Pr[Z=z] &= \sum_{x}\Pr[X=x,Y=x-z]\\ &= \sum_{x}\Pr[X=x]\Pr[Y=x-z]\\ &= \sum_{x}B(x,i,p)B(x-z,\delta-i,p)\\ &= \sum_{x=z}^{\min\{i,\frac{\delta+z}{2}\}}\frac{\binom{i}{x}\binom{\delta-i}{x-z}}{\binom{\delta}{2x-z}}B(2x-z,\delta,p). \end{aligned} \tag{4.7}$$

Summing over all $z \geq \mu$ yields,

$$Pr[Z\geq\mu] = \sum_{z=\mu}^{i}\sum_{x=z}^{\min\{i,\frac{\delta+z}{2}\}}\frac{\binom{i}{x}\binom{\delta-i}{x-z}}{\binom{\delta}{2x-z}}B(2x-z,\delta,p). \tag{4.8}$$

Using (4.4) and (4.8), we compute

$$\begin{aligned}\Pr[\hat{T}\neq\mathcal{T}] &= \sum_{i=\mu}^{n_1}\Pr[I=i]Pr[Z\geq\mu]\\ &= \sum_{i=\mu}^{n_1}HG(n_1,M,i,\delta)\sum_{z=\mu}^{i}\sum_{x=z}^{\min\{i,\frac{\delta+z}{2}\}}\frac{\binom{i}{x}\binom{\delta-i}{x-z}}{\binom{\delta}{2x-z}}B(2x-z,\delta,p).\end{aligned}$$

□

Proposition 2. *Under the open vote mode, an adversary with a priori knowledge of v_i, $\forall i$ can modify the voting outcome $\mathcal{T}$ for a decision threshold γ and a margin μ with probability*

$$\Pr[\hat{T}\neq\mathcal{T}] = \sum_{i=\mu}^{n_1}B(i,n_1,p), \quad n_1 = \frac{M+\gamma+\mu}{2}. \tag{4.9}$$

Proof. For a voting outcome $\mathcal{T}$ selected with a margin μ, there are $n_1 = \frac{M+\gamma+\mu}{2}$ votes in favor of T and $n_2 = \frac{M-\gamma-\mu}{2}$ votes against T. Let the in favor votes $n_1 = \frac{M+\gamma+\mu}{2}$ be "yes" votes. When the adversary is aware of the vote intent of each participant, he can target only "yes" votes. The voting outcome $\mathcal{T}$ is flipped if at least μ "yes" votes are nullified. For an adversary that attempts to nullify a

total of δ "yes" votes, the number of successfully nullified votes follows the binomial distribution.

$$\Pr[X = x] = B(x, \delta, p), \quad p = 0.5^{\ell}. \tag{4.10}$$

Summing over all values of $x \geq \mu$ yields,

$$\Pr[\hat{T} \neq T] = \sum_{i=\mu}^{\delta} B(i, \delta, p), \quad p = 0.5^{\ell}. \tag{4.11}$$

The δ is equal or smaller to the number of "no" votes n_1.

□

4.3 Selecting the Security Parameter ℓ

Propositions 1 and 2 allow us to select the number of symbol votes ℓ to guarantee robustness with a desired probability. Suppose we want to limit $\Pr[\hat{T} \neq \mathcal{T}] \leq p_0$. Then, we can select ℓ according to the following corollaries.

Corollary 1. *For an adversary unaware of the voting intent of each of participant,* $\Pr[\hat{T} \neq T] \leq p_0$ *if*

$$\ell > \left\lceil \frac{1}{\log 2} \log \frac{\delta \sum_{i=\mu}^{\delta} HG(\frac{M+\gamma+\mu}{2}, M, i, \delta) \sum_{z=\mu}^{i} \frac{1}{z}}{p_0} \right\rceil.$$

Proof. We wish to determine the value of ℓ for which $\Pr[\hat{T} \neq T] \leq p_0$. From the probability mass function of Z, it follows that

$$\begin{aligned} \Pr[Z = z] &= \sum_{x} \frac{\binom{i}{x}\binom{\delta - i}{x - z}}{\binom{\delta}{2x - z}} B(2x - z, \delta, p) && \text{(4.12a)} \\ &< \sum_{x} B(2x - z, \delta, p) && \text{(4.12b)} \\ &< \frac{\delta p}{z} && \text{(4.12c)} \end{aligned}$$

In (4.12b), we used the fact that $\binom{N}{n}\binom{M}{m} < \binom{N+M}{n+m}$. In (4.12c), we used the Chernoff bound to limit the tail sum of the Binomial distribution. Substituting to

(4.2) yields,

$$\Pr[\hat{T} \neq T] < \sum_{i=\mu}^{n_1} HG(n_1, M, i, \delta) \sum_{z=\mu}^{i} \frac{\delta p}{z}. \tag{4.13}$$

Limiting the right hand side of (4.13) by p_0 and solving for p results in

$$p < \frac{p_0}{\delta \sum_{i=\mu}^{n_1} HG(n_1, M, i, \delta) \sum_{z=\mu}^{i} \frac{1}{z}}. \tag{4.14}$$

Substituting $p = 0.5^{\ell}$ and solving for ℓ completes the proof.

□

Corollary 2. *For an adversary with a priori knowledge of v_i $\forall i$, the probability* $\Pr[\hat{T} \neq T] \leq p_0$ *if*

$$\ell \geq \left\lceil \frac{1}{\log 2} \log \frac{n_1}{\mu p_0} \right\rceil.$$

Proof. The proof follows by using the Chernoff bound to limit the tail probability of the binomial distribution in (4.11). □

Form corollaries 1 and 2, we observe that the required number of symbol votes ℓ drops linearly with the logarithm of p_0. This is also attested by the plots in Figure 4.1, Figure 4.2, and Figure 4.3, which show the required ℓ as a function of p_0, for various margins μ and number of attacked votes δ (to demonstrate the linear relationship of ℓ with the logarithm of p_0, the ceiling function has not been applied). Figure 4.1 considers the open vote model. A total of 20 participants are considered and the voting threshold γ is set to zero (plurality rule). Finally, δ is set to the number of positive votes. Exact values of ℓ can be computed using numerical methods. We observe that the margin μ has a small impact on the required ℓ. This is because the adversary only attacks participants that intend to cast "yes" votes.

Figure 4.2, shows ℓ as a function of p_0 for the secret vote model. As μ increases, fewer symbol votes are necessary to provide the same robustness compared to the model in Figure 4.1. This is because the adversary corrupts both "yes" and "no" votes, thus making it harder to close the margin. In Figure 4.3, we plot ℓ as a

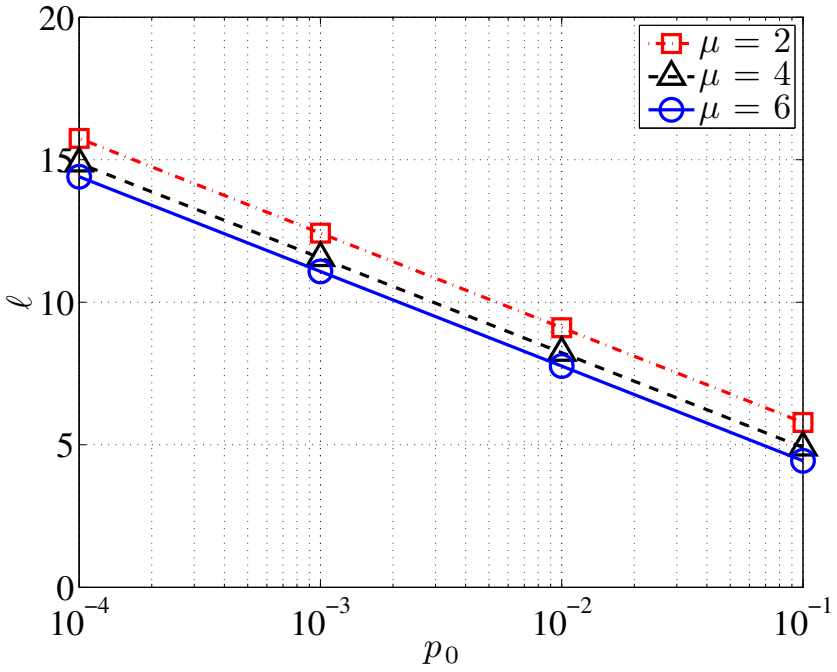


Figure 4.1: Minimum number of symbol votes ℓ to guarantee robustness p_0 for the secret vote model.

function of p_0 for different δ and for $\mu = 4$. If few votes are attacked (small δ), the achieved robustness is high for relatively small ℓ. Moreover, the adversary gains diminish with the increase of δ beyond a certain threshold. This threshold is located at the number of "yes" votes (for $\mu = 4$ and $\gamma = 0$, $n_1 = 14$).

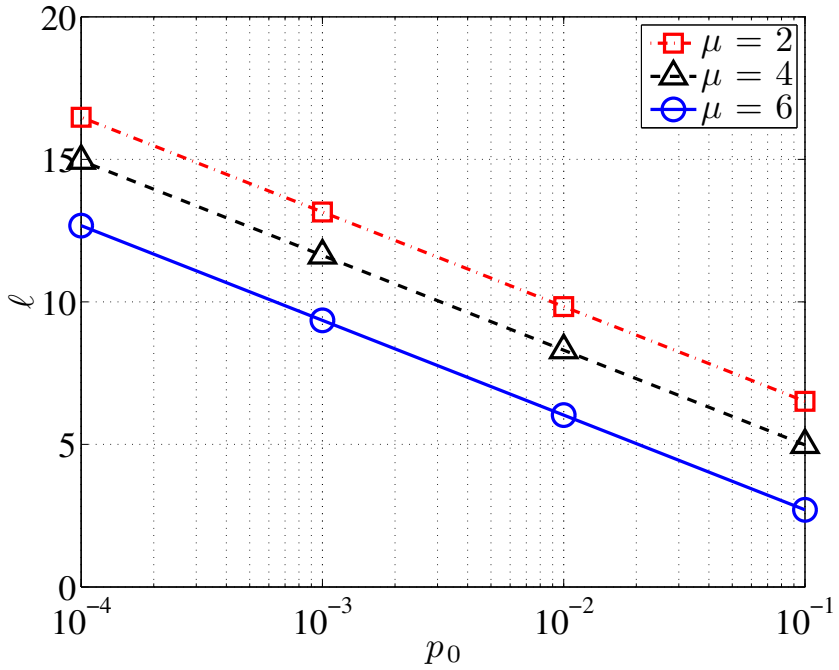


Figure 4.2: Minimum number of symbol votes ℓ to guarantee robustness p_0 for the open vote model.

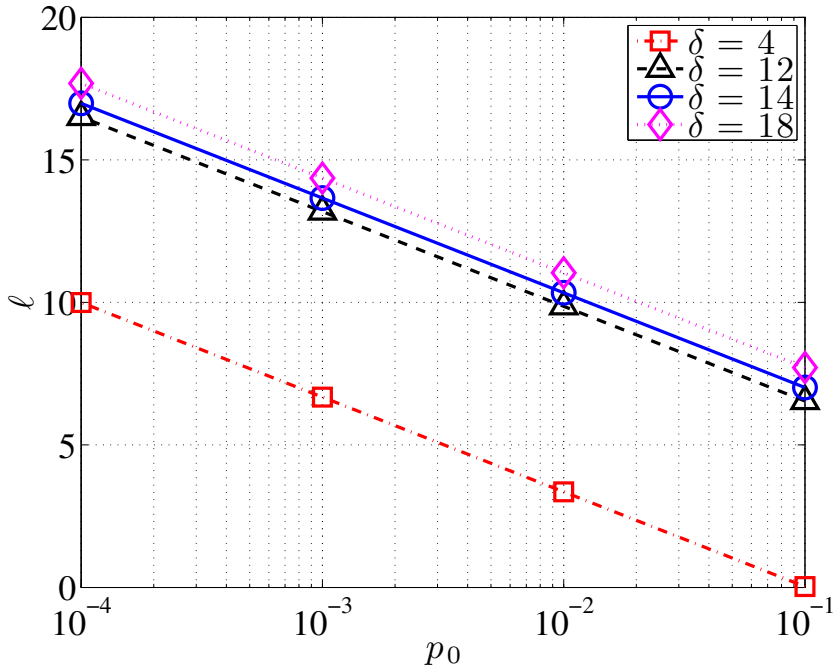


Figure 4.3: Minimum number of symbol votes ℓ to guarantee robustness p_0 for $\mu = 4$ and various δ, for the secret vote model.

CHAPTER 5

PRACTICAL CONSIDERATIONS AND IMPLEMENTATION

In this chapter, we compare the voting overhead of PHYVOS with the overhead of message-based voting schemes. The overhead is compared in terms of the time delay until a single vote is completed. As the symbol duration is constant, the delay overhead is proportional to the communication overhead. Hence, the analysis of the latter is omitted. We further present practical system implementation details of PHYVOS.

5.1 Voting Overhead

In this section, we compare the delay overhead of PHYVOS with the overhead of message-based voting. Suppose a popular OFDM-based protocol such as 802.11g is used for message-based voting (MV). Each 802.11g packet consists of a 20μsec preamble (5 OFDM symbols), a 30-Byte MAC header and a 4-Byte CRC code. Moreover, the vote integrity is protected by a message authentication code based on a secure hash function such as SHA-256 [46]. The message digest size for SHA-256 is 32 Bytes. Assuming the highest possible transmission rate for 802.11g, each OFDM symbol can carry 6 bits per subcarrier, times 48 data subcarriers = 36 Bytes. Therefore, one vote can be transmitted in 7 OFDM symbols. Ignoring any contention for capturing the wireless medium, participants must wait at least a DCF inter frame space (DIFS) between transmitting messages, For 802.11g, DIFS = 13 OFDM symbols. The total delay required to cast M votes becomes

$$D_{MV} = 20M - 13 \text{ OFDM symbols.} \tag{5.1}$$

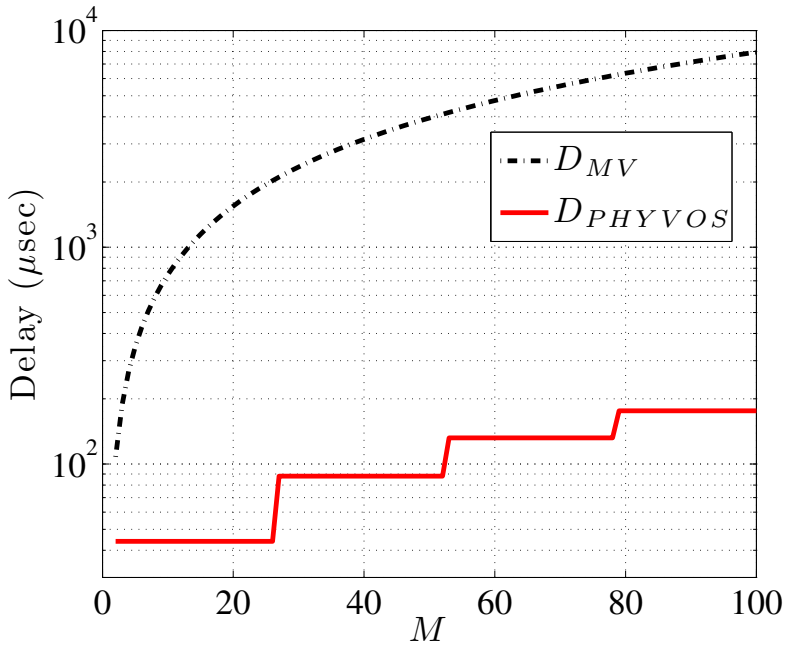


Figure 5.1: The voting overhead as a function of M for message-based voting (MV) and PHYVOS.

In PHYVOS, up to 26 participants can simultaneously cast their votes using ℓ OFDM symbols (2 subcarriers assigned per participant, no pilots necessary). For $M > 26$, a second voting round is required. The value of ℓ is based on the analysis presented in Section 4.3. For our comparison, we set $\ell = 11$ symbols, which yields a robustness level of 10^{-3}. The total delay required to cast M votes becomes,

$$D_{PHYVOS} = \left\lceil \frac{M}{26} \right\rceil \text{ OFDM symbols.} \tag{5.2}$$

Figure 5.1 shows the voting delay as a function of the number of participants M, assuming a typical OFDM symbol duration of 4μsec. PHYVOS reduces delay by one order of magnitude for $M = 11$ and two orders of magnitude for $M = 50$. Note that for $M = 26$, the MV incurs a delay of at least 2sec (this delay increases if contention is taken into account), which makes it unsuitable for time-critical applications (e.g., spectrum sensing in CRNs [19]).

5.2 Frequency Synchronization

Radio oscillators do not operate at the same nominal frequency due to manufacturing imperfections. The frequency misalignment which is known as carrier frequency offset (CFO), is amplified in mobile scenarios by the Doppler shift phenomenon. OFDM systems are particularly sensitive to CFO, due to the subcarrier orthogonality requirement [31]. The CFO has two critical effects on the demodulation process. First, subcarriers are no longer orthogonal causing inter-carrier interference (ICI) and reducing the SNR. Second, symbols at each subcarrier appear with arbitrary rotation in the constellation map. Finally, in the extreme case, a large CFO can cause a shift of the subcarrier bins at the receiver, whereby a symbol transmitted over subcarrier f_i is mapped to subcarrier f_j. This shift occurs if the CFO is larger than the subcarrier spacing [31].

To mitigate the impact of CFO in practical systems, receivers estimate the CFO using the preamble transmitted with every packet. In PHYVOS, no preamble is present with the transmission of votes to save on messaging overhead. However, the lack of frequency synchronization does not impact the correct vote estimation, because *no demodulation is performed.* Any symbol rotation in the constellation map does not affect the energy estimation on a given subcarrier. After all, the symbol transmitted to realize a vote is selected at random and does not convey any information. Furthermore, for a CFO that does not cause a subcarrier bin shift, the strongest ICI component comes from adjacent subcarriers. To limit ICI, the subcarriers assigned to each participant can be spaced as far as the number of participants allows. For instance, for 10 voters and 64 subcarriers, every 3rd subcarrier is used to cast a vote.

Finally, in typical OFDM systems, the subcarrier spacing is much larger than the expected CFO. As an example, the subcarrier spacing in 802.11g is 312.5KHz, while the expected device frequency misalignment is in the order of 10s of KHz [28]. In addition, the Doppler shift due to mobility is in the order of 10s of Hz (at 2.4GHz, 80Hz of Doppler shift equals a moving speed of 36Km/hr). Thus the

compounded CFO due to oscillator imperfections and the Doppler effect are not sufficient to cause a shift of the subcarrier bins. This is also observed in the experimental implementation of PHYVOS, where energy was detected primarily in the designated subcarriers.

5.3 Time Synchronization

Another practical problem for PHYVOS is that symbol votes do not reach the FC perfectly synchronized. Differences in propagation delay and device clock drifts can cause a time misalignment between the symbol votes casted by each device. This misalignment will affect the set of samples that fall within the FFT window of the Fourier transform applied at the receiver for extracting the spectral components of the OFDM signal. This is similar to *symbol bleeding* caused in OFDM systems when delayed copies of OFDM symbols arrive at the receiver due to multipath effects. The solution applied in OFDM is to append a cyclic prefix (CP) to every symbol, which is in the order of 0.8μsec.

For PHYVOS, the time misalignment Δt between symbols at the receiver can be greater than 0.8μsec. For a typical WiFi range of 300m, the propagation delay difference between two devices can by up to 1μsec. Moreover, the typical clock error for modern clocks is well below 5ppm [28]. If clock synchronization is performed every 100msec (typical beacon transmission period for WiFi base stations), the expected clock error between two devices can be up to 1μsec, making the total time misalignment $\Delta t \leq 2\mu$sec.

To cope with the symbol misalignment, we can extend the CP duration to 2μsec to account for the maximum expected Δt. The increase in CP comes at the expense of a higher overhead to cast a symbol vote (5.2μsec vs. 4μsec). Note that the increased CP duration is adopted only for vote casting and is not part of the normal OFDM operation for data transmissions. Alternatively, to maintain compatibility with the current OFDM specifications, we can extend the symbol

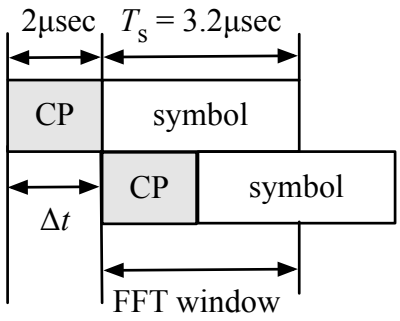


Figure 5.2: Increasing the CP to account for synchronization error.

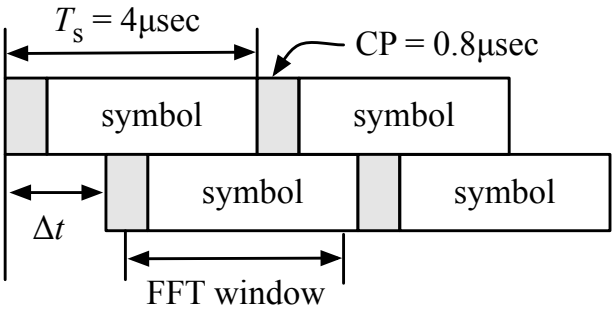


Figure 5.3: Casting a symbol vote in two symbol durations.

vote duration to two OFDM symbols, without increasing the CP duration. This solution comes at the expense of doubling the overhead for casting a symbol vote. A similar solution was adopted in [12]. The two solutions are shown in Fig. 5.3.

To cope with the symbol misalignment, we can extend the CP duration to 2μsec to account for the maximum expected Δt. The increase in CP comes at the expense of a higher overhead to cast a symbol vote (5.2μsec vs. 4μsec). Note that the increased CP duration is adopted only for vote casting and is not part of the normal OFDM operation for data transmissions. Alternatively, to maintain compatibility with the current OFDM specifications, we can extend the symbol vote duration to two OFDM symbols, without increasing the CP duration. This solution comes at the expense of doubling the overhead for casting a symbol vote.

A similar solution was adopted in [12]. The two solutions are shown in Figure 5.2 and Figure 5.3.

5.4 PHYVOS Implementation

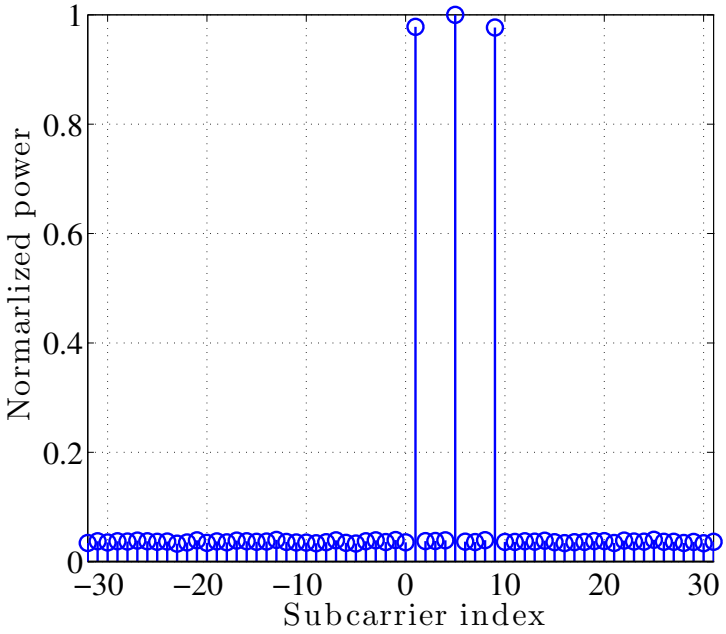
In this section, we report the results from the prototype implementation of PHYVOS on a USRP test bed.

5.4.1 Testbed Setup

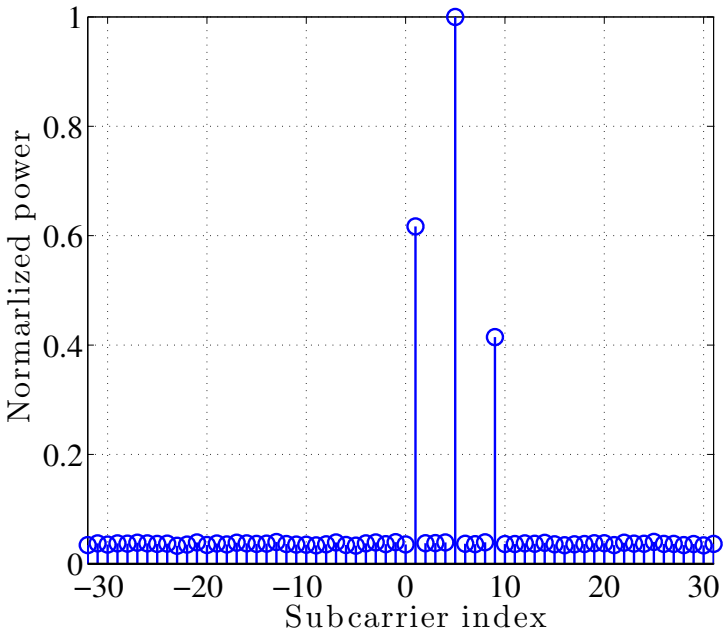
We implemented PHYVOS on NI USRPs 2921 devices, operating in the 2.4GHz band over a 39.6MHz spectrum. A total of four radios were at our disposal. Under normal operation, three radios operated as voters, while one radio operated as the FC. One radio was switched to an attacker role for adversarial scenarios. Voter radios were placed in a LoS configuration at varying distances from the FC within an office environment. We divided the 39.6MHz spectrum to 64 subcarriers. To cast a symbol vote, each radio used BPSK modulation to transmit a random symbol at the designated subcarrier. The CP value was set to 0.8μsec, as the time synchronization error between the different radios was relatively small. We used a 64-point FFT to collect the symbol votes from each subcarrier. The transmission power of each radio was set to 20dBm (0.1W).

5.4.2 Selection of Threshold γ_D

In the first experiment, we assigned the 1st, 5th, and 9th subcarrier to each of the three voter radios. Each voter radio casted 1,000 symbol votes at its designated subcarrier by transmitting 1,000 BPSK symbols. The rest of the subcarriers remained null. A time gap of 100msec was imposed between two consecutive votes. Figure 5.4(a) shows the normalized magnitude of the FFT output at the FC, averaged over the 1,000 transmitted symbols when the three voters are placed 5ft away



(a) Topology A



(b) Topology B

Figure 5.4: Normalized average received power per subcarrier

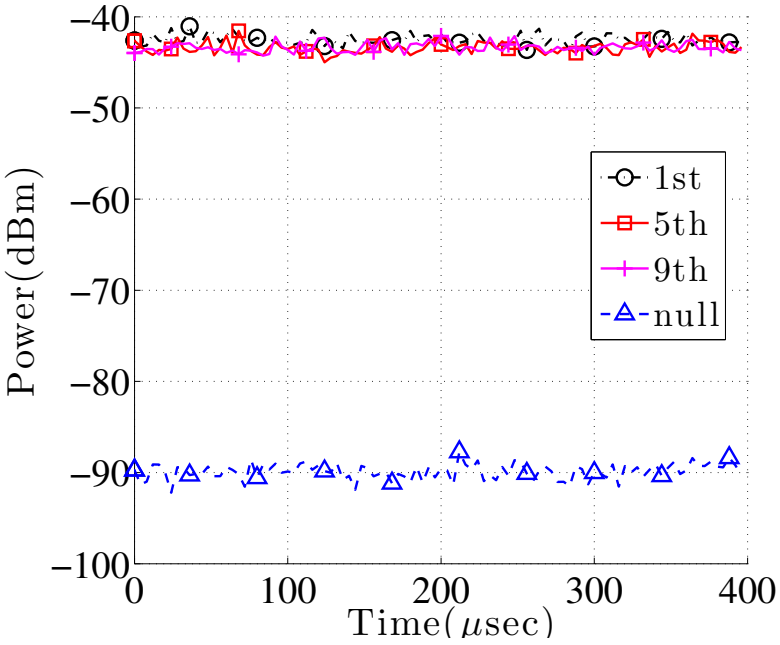
from the FC (topology A). Figure 5.4(b) shows the same results when the three voters are at 5ft, 10ft, and 15ft away from the FC (topology B). We observe that in both cases the magnitude of the FFT output is significantly higher for the active subcarriers.

Figures 5.5(a) and 5.5(b) show the received power as a function of time for 100 consecutive symbols. For topology A, the power of active subcarriers is approximately -42dBm, while the power of null subcarriers is -90dBm. The recorded -90dBm value for the null subcarriers is well above the noise floor due to the operation of nearby devices over the ISM band. For topology B, the received power from the farthest radio dropped to -49dBm. Based on the recorded values, we set the threshold γ_d for the detection of a symbol vote to -80dBm, which is well above the receiver sensitivity.

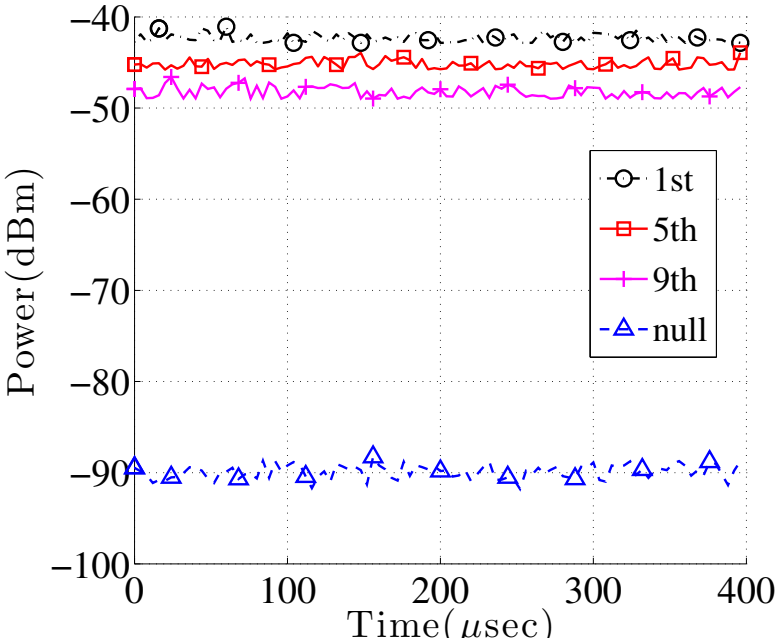
5.4.3 Voting in the Presence of an Adversary

In the second experiment, we implemented an adversarial scenario. One of the three voter USRPs was assigned the role of an attacker. Voter #1 was assigned the 1st and 2nd subcarrier while voter #2 was assigned the 5th and 6th subcarrier. For each symbol vote, the attacker randomly selected one subcarrier per voter and injected a random symbol in order to nullify or flip the casted vote. The experiment lasted for 10^6 symbol votes (no time gap). Figure 5.6 and Figure 5.7 show the probability of tallying the correct vote $v(i)$, having an inconclusive vote e, or flipping the vote to $\text{comp}(v(i))$, as a function of the security parameter ℓ and for topologies A and B, respectively. The theoretical values for tallying the correct vote $v(i)$, and having an inconclusive vote e are also shown (solid lines). The theoretical values are computed according to equation (4.1).

We observe that the experimental values are in close agreement with the theoretical ones. As expected, the probability of tallying the correct vote rapidly converges to 1 with the increase of ℓ, while the probability of an inconclusive vote becomes small (zero for $\ell > 8$). In our experiments, some votes were actually



(a) Topology A



(b) Topology B

Figure 5.5: Received power per subcarrier as a function of time.

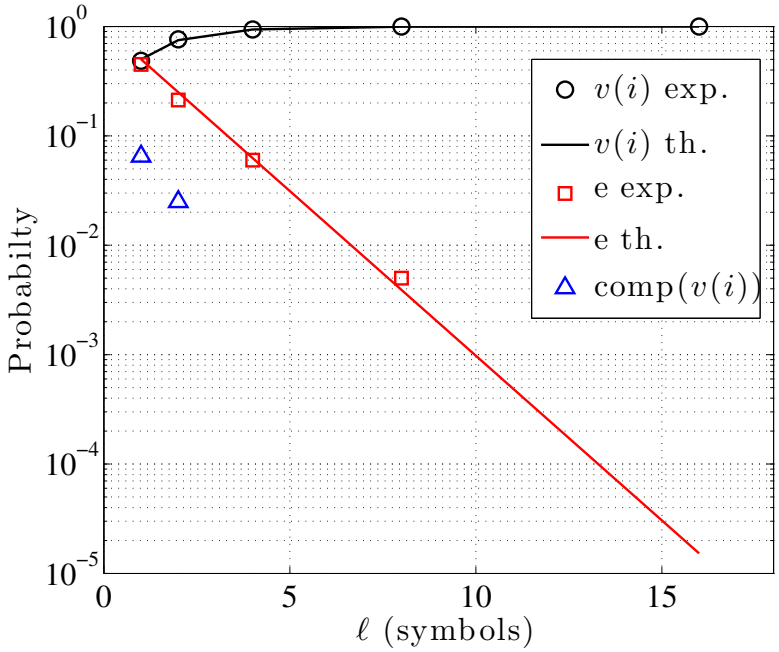


Figure 5.6: Probability of tallying the correct vote $v(i)$, having an inconclusive vote e, or flipping the vote to comp$(v(i))$ for Topology A.

flipped indicating a drop in the received power on a designated subcarrier to a value smaller than γ_D for ℓ consecutive symbol votes. However, this occurred with very low probability and was not observed at all when $\ell > 2$. The results were similar for topology B, with a slight increase in the probability of comp$(v(i))$. This was primarily observed due to the near-far effect for the most distant voter (placed at 15ft from the FC).

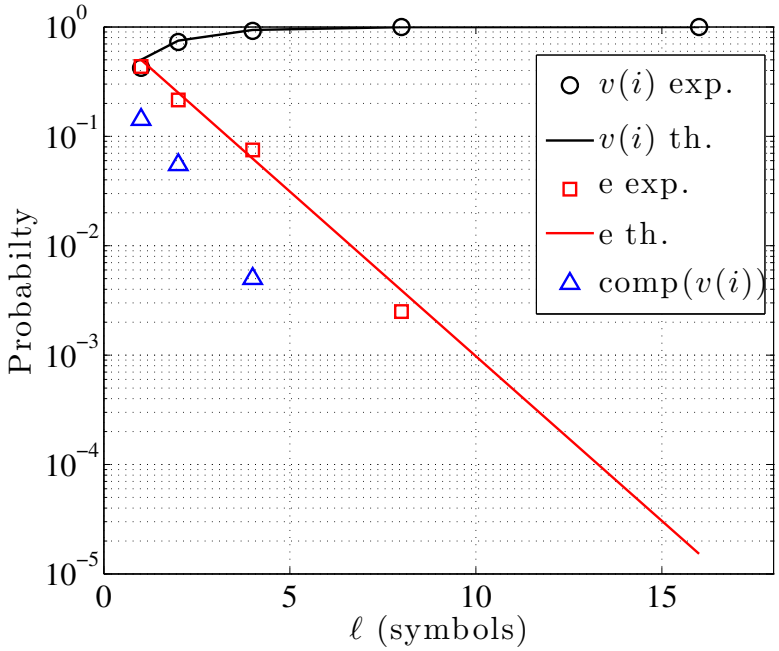


Figure 5.7: Probability of tallying the correct vote $v(i)$, having an inconclusive vote e, or flipping the vote to comp$(v(i))$ for Topology B.

CHAPTER 6

SUMMARY OF CONTRIBUTIONS AND FUTURE RESEARCH DIRECTIONS

6.1 Summary of Contributions

Although voting and reaching consensus are frequent operations in wireless networks, the problem of efficient and secure voting has received little attention. The majority of methods adopt message-based solutions that can incur prohibitive communication cost and delay for time-critical applications. To improve on the communication and delay efficiency, we presented PHYVOS, a secure and fast PHY-layer voting scheme for single-hop wireless networks. In PHYVOS, no explicit messaging is necessary. Participants exploit the subcarrier orthogonality of OFDM to cast their votes simultaneously by adding energy to designated subcarriers. Therefore, no transmission of preambles and headers is required, as the receiver does not demodulate the OFDM signal. Simple energy detection suffices. Moreover, relying on energy detection rather than message decoding for vote casting strengthens the security of our scheme, as it is generally hard to erase energy from a channel. An attacker could still attempt to modify votes by inserting his own energy into various subcarriers. We reduce the probability of voting outcome manipulation by executing multiple voting rounds. Since a voting round only last for a few OFDM symbols, executing multiple rounds is still far more efficient than applying message-based voting.

We showed that PHYVOS maintains the integrity of the voting outcome with high probability, without using cryptographic primitives. We analytically evaluated the voting robustness as a function of the number of voting rounds. We further discuss practical implementation challenges of PHYVOS related to frequency and time synchronization. Finally, we presented a prototype implementation of PHYVOS

on the NI USRP platform. Our implementation demonstrated that PHYVOS correctly computes the vote tally at the fusion center, in the presence of an adversary who inserts energy into the subcarriers. The proposed scheme was demonstrated for binary voting.

6.2 Future Research Directions

As future work, we aim at enriching the implementation scenarios for PHYVOS. In particular, we will study its resilience and correctness under varying channel conditions. We will further evaluate PHYVOS' performance when co-existing with other systems, which operate over the same frequency bands. Interference from co-existing systems could cause the incorrect tally of a vote fraction. Moreover, we intend to extend PHYVOS to accommodate x-ary voting. We will further explore methods for accommodating a larger number of votes over the same spectrum by allowing two or more participants to simultaneously cast votes over the same subcarriers. Finally, we will investigate the application of PHY-layer voting to fully distributed consensus algorithms.

REFERENCES

[1] A. N. Akansu and X. Lin. A comparative performance evaluation of DMT (OFDM) and DWMT (DSBMT) based DSL communications systems for single and multitone interference. In *Proceedings of the 1998 IEEE International Conference on Acoustics, Speech and Signal Processing*, volume 6, pages 3269–3272, 1998.

[2] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan. Cooperative spectrum sensing in cognitive radio networks: A survey. *Physical Communications*, 4(1):40–62, 2011.

[3] N. Al-Nakhala, R. Riley, and T. Elfouly. Distributed algorithms in wireless sensor networks: an approach for applying binary consensus in a real testbed. *Computer Networks*, 2015.

[4] N. Al-Nakhala, R. Riley, and T. Elfouly. Distributed algorithms in wireless sensor networks: An approach for applying binary consensus in a real testbed. *Computer Networks*, 79:30–38, 2015.

[5] S. Ashrafi, M. Malmirchegini, and Y. Mostofi. Binary consensus for cooperative spectrum sensing in cognitive radio networks. In *Proceedings of the Global Telecommunications Conference (GLOBECOM 2011)*, pages 1–6, 2011.

[6] A. R. Bahai, B. R. Saltzberg, and M. Ergen. *Multi-carrier digital communications: theory and applications of OFDM*. Springer Science & Business Media, 2004.

[7] M. Barborak, A. Dahbura, and M. Malek. The consensus problem in fault-tolerant computing. *ACM Computer Surveys*, 25(2):171–220, 1993.

[8] L. Blum, M. Blum, and M. Shub. A simple unpredictable pseudo-random number generator. *SIAM Journal on computing*, 15(2):364–383, 1986.

[9] W. Bolton, Y. Xiao, and M. Guizani. Ieee 802.20: mobile broadband wireless accesl. *Wireless Communications, IEEE*, 14(1):84–95, 2007.

[10] J. Cave. Moca enable home: Introduction and overview. In *Proc. of Sooner State Chapter SCTE Meeting - Tulsa*, 2009.

[11] M. Draief and M. Vojnovic. Convergence speed of binary interval consensus. *SIAM Journal on Control and Optimization*, 50(3):1087–1109, 2012.

[12] A. Dutta, D. Saha, D. Grunwald, and D. Sicker. SMACK: a SMart ACKnowledgment scheme for broadcast messages in wireless networks. *ACM SIGCOMM Computer Communications Review*, 39(4):15–26, 2009.

[13] Y. Feng, S. Ng, and S. Grosche. An electronic voting system using GSM mobile technology. *Technical Report RHUL-MA-2006-5*, 2006.

[14] A. Ghosh, D. Wolter, G. Andrews, and R. Chen. Broadband wireless access with wimax/8o2.16: Current performance benchmarks and future potential. *IEEE Communications Magazine*, 43(2):129–136, 2011.

[15] A. Greenspan, M. Klerer, J. Tomcik, and R. Canchi. Dvb-h: Digital broadcast services to handheld devices. *Proceedings of the IEEE*, 94(1):194–209, 2006.

[16] A. Greenspan, M. Klerer, J. Tomcik, and R. Canchi. Ieee 802.20: Mobile broadband wireless access for the twenty-first century. *IEEE Communications Magazine*, 46(7):56–63, 2008.

[17] I. . W. Group. Part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications high-speed physical layer in the 5 ghz band. http://standards.ieee.org/about/get/802/802.11.html, 2003.

[18] I. . W. Group. System requirements for IEEE 802.20 mobile broadband wireless access systems version 14. http://www.ieee802.org/20/P_Docs/IEEE%20802.20%20PD-06r1.doc, 2004.

[19] I. . W. Group. IEEE 802.22 WRAN standards. http://www.ieee802.org/22/, 2011.

[20] S. Hara and R. Prasad. *Multicarrier techniques for 4G mobile communications*. Artech House, 2003.

[21] A. Harms, L. Davis, and J. Palmer. Understanding the signal structure in dvb-t signals for passive radar detection. In *Radar Conference, 2010 IEEE*, pages 532–537, 2010.

[22] N. Katenka, E. Levina, and G. Michailidis. Local vote decision fusion for target detection in wireless sensor networks. *IEEE Transactions on Signal Processing*, 56(1):329–338, 2008.

[23] N. Katenka, E. Levina, and G. Michailidis. Robust target localization from binary decisions in wireless sensor networks. *Technometrics*, pages 448–461, 2008.

[24] W. Kim, K. Mechitov, J. Choi, and S. Ham. On target tracking with binary proximity sensors. In *Proc. of the IPSN*, pages 301–308, 2005.

[25] T. Kwon, H. Lee, S. Choi, J. Kim, D. Cho, S. Cho, S. Yun, W. Park, and K. Kim. Design and implementation of a simulator based on a cross-layer protocol between mac and phy layers in a wibro compatible.ieee 802.16e ofdma system. *IEEE Communications Magazine*, 43(12):136–146, 2005.

[26] R. Laroia. flash-ofdm — mobile wireless internettechnology. In *Proc. of IMA workshop on wireless network*, 2001.

[27] L. Lazos and R. Poovendran. SeRLoc: robust localization for wireless sensor networks. *ACM Transactions on Sensor Networks*, 1(1):73–100, 2005.

[28] LitePoint. Practical manufacturing testing of 802.11 OFDM wireless devices. http://www.litepoint.com/whitepaper/Testing%20802.11%20OFDM%20Wireless%20Devices_WhitePaper.pdf, 2012.

[29] X. Luo, M. Dong, and Y. Huang. On distributed fault-tolerant detection in wireless sensor networks. *IEEE Transactions on Computers*, 55(1):58–70, 2006.

[30] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In *Proc. of the MOBICOM Conference*, pages 128–139. ACM, 2008.

[31] R. v. Nee and R. Prasad. *OFDM for wireless multimedia communications*. Artech House, Inc., 2000.

[32] E. Ould-Ahmed-Vall, B. H. Ferri, and G. F. Riley. Distributed fault-tolerance for event detection using heterogeneous wireless sensor networks. *IEEE Transactions on Mobile Computing*, 11(12):1994–2007, 2012.

[33] S. Ozdemir and Y. Xiao. Secure data aggregation in wsns: A comprehensive overview. *Comp. Nets*, 53(12):2022–2037, 2009.

[34] E. Perahia and R. Stacey. *Next Generation Wireless LANS: 802.11 n and 802.11 ac*. Cambridge University Press, 2013.

[35] H. G. Perros. *An introduction to ATM networks*. WILEY, 2002.

[36] M. Poggioni, L. Rugini, and P. Banelli. Dvb-t/h and t-dmb: Physical layer performance comparison in fast mobile channels. *IEEE TRANSACTIONS ON BROADCASTING*, 55(4):719–730, 2009.

[37] H. Rahul, H. Hassanieh, and D. Katabi. SourceSync: a distributed wireless architecture for exploiting sender diversity. *ACM SIGCOMM Computer Communications Reviews*, 41(4):171–182, 2011.

[38] M. Ran., D. Falconer., and A. Seeyar. A mixed OFDM downlink and single carrier uplink for the 2-11 ghz licensed bands. Technical report, IEEE 802.16 Broadband Wireless Access Working Group, August 2002.

[39] U. Reimers. *DVB: the family of international standards for digital video broadcasting*. Springer, 2013.

[40] A. Sahai, R. Tandra, and M. Mishra. Spectrum sensing: Fundamental limits. In *Cognitive radios: System Design Perspective*, 2009.

[41] K. Sampigethaya and R. Poovendran. A framework and taxonomy for comparison of electronic voting schemes. *Computers & Security*, 25(2):137–153, 2006.

[42] J. Sanchez-Martnez, J. Cortes, L. Diez, F. Canete, and L. Torres. Performance analysis of ofdm modulation on indoor plc channels in the frequency band up to 210 mhz. In *Proc. of the IEEE International Symposium on Power Line Communications and its Applications (ISPLC)*, pages 38–43, 2010.

[43] J. Sanchez-Martnez, J. Cortes, L. Diez, F. Canete, and L. Torres. Distributed event-triggered control for multi-agent systems. *IEEE Transactions on Automated Control*, pages 1291–1297, 2012.

[44] D. Shah. *Gossip algorithms*. Now Publishers Inc, 2009.

[45] E. Shim, K. Lee, K. Kwoni, and Y. You. Synchronization receiver design for ofdm-based fm broadcasting systems. *Wireless Personal Communications*, 58(2):355–367, 2011.

[46] D. R. Stinson. *Cryptography: theory and practice*. CRC press, 2005.

[47] M. Takada and M. Saito. Transmission systems for isdb-t. In *Proc. of IEEE, Special Issue on Global Digital Television: Technology and Emerging Services*, pages 251–256, 2006.

[48] L. Thibault, D. Taylor, L. Zhang, J. Chouinard, and R. Boudreau. Advanced demodulation technique for cofdm in fast fading channels. In *Proc. of International Broadcasting Convention*, pages 416–422, 2003.

[49] U. V. Vazirani and V. V. Vazirani. Efficient and secure pseudo-random number generation. In *Advances in cryptology*, pages 193–202. Springer, 1985.

[50] J. Von Neumann. Probabilistic logics and the synthesis of reliable organisms from unreliable components. *Aut. studies*, 34:43–98, 1956.

[51] X. Wang. *Performance evaluation of the ISDB-T standard for multimedia services*. The university of British Columbia, 2002.

[52] M. Wylie-Green, P. Ranta, and J. Salokannel. Multi-band ofdm uwb solution for ieee 802.15.3a wpans. In *Advances in Wired and Wireless Communication, 2005 IEEE/Sarnoff Symposium on*, pages 102–105, 2005.

[53] Z. Zheng, Z. Yang, C. Pan, and Y. Zhu. Cutoff rate and outage probability performance comparisons between dvb-t and dmb-t systems under mobile multipath channels. *Broadcasting, IEEE Transactions on*, 49(4):390–397, 2003.

[54] M. Zhu, S. Ding, Q. Wu, R. R. Brooks, N. S. V. Rao, and S. S. Iyengar. Fusion of threshold rules for target detection in wireless sensor networks. *ACM Transactions on Sensor Networks.*, 6(2):181–187, 2010.