ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL OF SCIENCE ENGINEERING AND TECHNOLOGY

SIMULTANEOUS TRANSMISSION BASED COMMUNICATION TECHNIQUES

M.Sc. THESIS

Ufuk ALTUN

Department of Electronics and Communications Engineering

Telecommunications Engineering Programme

JULY 2020

ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL OF SCIENCE ENGINEERING AND TECHNOLOGY

SIMULTANEOUS TRANSMISSION BASED COMMUNICATION TECHNIQUES

M.Sc. THESIS

Ufuk ALTUN
(0504171355)

Department of Electronics and Communications Engineering

Telecommunications Engineering Programme

Thesis Advisor: Prof. Dr. Güneş KARABULUT KURT
Co-advisor: Assoc. Prof. Dr. Enver ÖZDEMİR

JULY 2020

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

EŞZAMANLI İLETİME DAYALI HABERLEŞME SİSTEMLERİ

YÜKSEK LİSANS TEZİ

Ufuk ALTUN
(0504171355)

Elektronik ve Haberleşme Mühendisliği Anabilim Dalı

Telekomünikasyon Mühendisliği Programı

Tez Danışmanı: Prof. Dr. Güneş KARABULUT KURT
Eş Danışman: Doç. Dr. Enver ÖZDEMİR

TEMMUZ 2020

Ufuk ALTUN, a M.Sc. student of ITU Graduate School of Science Engineering and Technology 0504171355 successfully defended the thesis entitled "SIMULTANEOUS TRANSMISSION BASED COMMUNICATION TECHNIQUES", which he/she prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

Thesis Advisor :	**Prof. Dr. Güneş KARABULUT KURT** Istanbul Technical University	.....
Co-advisor :	**Assoc. Prof. Dr. Enver ÖZDEMİR** Istanbul Technical University	.....
Jury Members :	**Assoc. Prof. Dr. Sıddıka Berna Örs Yalçın** Istanbul Technical University	.....
	Asst. Prof. Dr. Tunçer Baykaş Medipol University	.....
	Assoc. Prof. Dr. Ali Emre Pusane Boğaziçi University	.....

Date of Submission : **01 July 2020**
Date of Defense : **17 July 2020**

FOREWORD

I am sincerely thankful to my Advisor Prof. Güneş KARABULUT KURT and Co-advisor Assoc Prof. Enver ÖZDEMİR. I simply learned everything from them that makes me in this profession in the past three years. Acknowledging only their scientific knowledge would not be fair. My appreciation for their teachings competes with my appreciation for their understanding, kindness and many other virtues. Lastly, I would like to thank the most important people in my life; my mother, my father and my beloved Kübs. Their existence is everything to me.

JULY 2020

Ufuk ALTUN
Electronics and Communication Engineer

TABLE OF CONTENTS

Page

ABBREVIATIONS

AF : Amplify and Forward
AFC : Analog Function Computation
AI : Artificial Intelligence
AWGN : Additive White Gaussian Noise
BER : Bit Error Rate
C-RAN : Cloud-Radio Access Network
CDMA : Code Division Multiple Access
CEE : Channel Estimation Error
CF : Compress and Forward
CFO : Carrier Frequency Offset
cMACr : Compound Multiple Access Channel with a relay
CoMAC : Computation over Multiple Access Channels
CPF : Compute and Forward
CPCF : Compute Compress and Forward
CSI : Channel State Information
DF : Decode and Forward
DFT : Discrete Fourrier Transform
DSGD : Distributed Stochastic Gradient Descent
FC : Fusion Center
i.i.d. : Independent and identically distributed
IA : Interference Alignment
IoT : Internet of Things
IPC : Individual Power Constraint
LDLC : Low Density Lattice Code
LDPC : Low Density Parity Check
LLR : Log-Likelihood Ratio
MAC : Multiple Access Channel
MAF : Modified Amplify and Forward
MAP : Maximum a Posteriori
MDF : Modified Detect and Forward
MIMO : Multiple-Input Multiple-Output
ML : Machine Learning
MMSE : Minimum Mean Square Error
MSE : Mean Square Error
MWRC : Multi-way Relay Channel
NC : Network Coding
NOMA : Non-orthogonal Multiple Access
OFDM : Orthogonal Frequency Division Multiplexing
PLNC : Physical Layer Network Coding
SDR : Software Defined Radio

SER : Symbol Error Rate
SIC : Successive Interference Cancellation
SIMO : Single-Input Multiple-Output
SNR : Signal to Noise Ratio
STAC : Simultaneous Transmitting and Air Computing
STANC : Space-Time Analog Network Coding
SVP : Shortest Vector Problem
TBMA : Type-Based Multiple Access
TDMA : Time Division Multiple Access
TPC : Total Power Constraint
UAV : Unmanned Aerial Vehicles
W-FMAC : Wireless Half Duplex Multiple Access Channel
W-HMAC : Wireless Half Duplex Multiple Access Channel
W-MAC : Wireless Ful Duplex Multiple Access Channel
WSN : Wireless Sensor Network
ZF : Zero Forcing

LIST OF TABLES

Page

LIST OF FIGURES

Page

SIMULTANEOUS TRANSMISSION BASED COMMUNICATION TECHNIQUES

SUMMARY

Any interference between two communicating point is regarded as unwanted noise in conventional communication networks, since it distorts the received signal. In the last two decades, allowing simultaneous transmission and intentionally accepting the interference of signals has been taken into consideration as opposed to the conventional perspective. Joint source-channel coding and the computation codes are one of the first paradigms that allow simultaneous transmission at the same time and frequency and benefit from it. Joint source-channel coding later inspired many other fundamental work from network coding to consensus algorithms, from distributed detection applications to the emerging machine learning. In this thesis, the simultaneous transmission techniques are investigated and two security methods are proposed based on the simultaneous transmission. The chapters of this thesis can be placed under two titles.

In the first part, the readers will find a thorough map of the wireless communication literature that benefits from the superposition of signals. The studies are grouped together depending on their purpose and application area. Later, they are presented along with the details such as their contributions and performance metrics. These studies show that the simultaneous transmission can bring scalability, security, low-latency, low-complexity and energy efficiency for certain wireless distributed networks. This part of the thesis emphasizes how the physical layer can be beneficial for unconventional network structures. Especially, the internet of things (IoT) requires unconventional designs to support large networks where the nodes are often resource limited. Simultaneous transmission-based techniques show great opportunities in these scenarios. Also, the attention on the simultaneous transmission applications is expected to grow larger since the application areas of the IoT are constantly spreading.

In the second part, an authentication method and a key generation method is presented for multi-user networks. These methods are inspired by the analog function computation (AFC) studies that reduce the computational load of the receiver by computing functions over the air. In essence, AFC methods use signal processing at the transmitters and receivers to invert the fading effect such that the channel model matches with summation operation. After this point, the signal processing is extended to compute any other function. However, existing AFC methods always lose the individual channel inputs over the channel and the receiver only obtains a function of these inputs. In the authentication method, a novel signal processing is developed to harness the individual data from the channel and authenticate it against spoofers. For this purpose, Gaussian prime integers are involved in the signal processing. The pre-processing function encodes the messages at the signal amplitudes in the logarithmic forms. Also the messages are encoded as the exponents of the Gaussian prime "identifiers" which is unique to each user. These prime identifiers enable the

extraction of individual data from the superimposed signals. Gaussian primes and the fading ensure the detection of spoofing attacks. For a successful detection, the spoofer is assumed to have larger channel estimation error than the legitimate users. The symbol error rate (SER) and the receiver operating characteristics (ROC) are investigated with simulations in order to verify the feasibility of the proposed approach.

In the key generation method, time and bandwidth efficiency of multi-user networks are improved and their dependency on a center node (or an external third party) is removed. Similar to the authentication method, channel model is adjusted with pre and post processing functions. However in this model, the channel is matched with a key generating function that outputs a shared key at each node. The key is assumed to be the combination of multiple key components that are taken from each node. Half duplex and full duplex communication scenarios are considered for the key generation purpose. In the half-duplex scenario, key components are pre-processed and simultaneously transmitted. The pre-processing functions make sure that only the targeted receiver obtains the meaningful information after post-processing. Repeating this process for every node completes the key generation process without leaking the key to the eavesdroppers. This scenario especially removes the dependency on a center node which is required in many traditional method to distribute prior information to each node. This scenario is investigated with simulations and the error probability results are presented. Moreover, the full-duplex scenario is considered where each node simultaneously transmits and receives key components. This model manages to provide a secret key to multiple nodes in a single communication.

EŞZAMANLI İLETİME DAYALI HABERLEŞME SİSTEMLERİ

ÖZET

Geleneksel haberleşme sistemlerinde, haberleşmenin iki uç arasında olduğu varsayılır. Harici işaretlerin bu uçlardan gönderilen işaretler ile girşimi gürültü olarak değerlendirilir ve istenmeyen bir durumdur. Son 20 yılda, bu düşüncenin aksine, eş zamanlı iletime izin veren ve işaretler arası girişimi kasten kabul eden çalışmalar yapılmıştır. Ortak kaynak-kanal kodlama (Joint source-channel coding) ve hesaplamalı kodlar (computation codes), aynı zaman ve frekans aralığında iletime izin veren ve bu durumdan faydalanan ilk paradigmalardır. Ortak kaynak-kanal kodlama daha sonra eş zamanlı iletimin ağ kodlama (network coding), oy birliği (consensus) algoritmaları, dağınık tespit (distributed detection) algoritmaları, makina öğrenmesi (machine learning) gibi bir çok alanda kullanılmasına öncülük etmiştir. Bu tezde de, eşzamanlı iletim teknikleri (simultaneous transmission techniques) incelenmiş ve iki özgün güvenlik methodu (security methods) tanıtılmıştır. Tezi oluşturan bölümleri iki başlık altında değerlendirmek mümkündür.

Tezin ilk kısmında, işaretlerin girişiminden faydalanan literatürdeki çalışmaların kapsamlı bir haritası sunulmuştur. Çalışmalar; hedeflerine ve uygulama alanlarına göre derlenmiş, sonrasında literatüre katkıları, başarım kriterleri ve benzeri detaylarla birlikte tanıtılmışlardır. Böylece bu tezde, eşzamanlı iletimin dağınık ve telsiz ağlara alışılagelmiş yöntemlerin aksi bir yapı ile; ölçeklenebilirlilik, güvenlik, enerji verimliliği, daha az gecikme süresi ve daha az karmaşıklık kazandırabileceği ortaya koyulmuştur. Özellikle nesnelerin interneti (IoT), kısıtlı kaynaklara sahip düğümlerden oluşan büyük ağlardaki çok sayıda düğümü destekleyebilmek için sıradışı yöntemlere açık bir oluşumdur. Bu sebeple eş zamanlı iletime dayalı yöntemler nesnelerin interneti uygulamalarında verimliliği artırmak adına büyük fırsatlar sunmaktadır. Ayrıca; nesnelerin internetinin yaygınlaşmasıyla birlikte telsiz ve dağınık ağların kaçınılmaz olduğu ve bu sebeple eşzamanlı iletimin öneminin artacağı aşikardır.

Eşzamanlı iletime dayalı çalışmaların, literatürde birçok telsiz haberleşme uygulamasında var olduğu görülmektedir. Ancak bu çalışmaların literatürdeki yaygınlığı ve popüleritesi oldukça kısıtlıdır. Eş zamanlı iletimin izin verildiği en bilinen uygulama alanı olarak çoklu erişim (multiple access) amaçlı yöntemler gösterilebilir. Bu alandaki Code Division Multiple Access (CDMA), Non-orthogonal Multiple Access (NOMA) gibi yöntemler literatürde kabul görmüştür; ancak bu yöntemler işaretlerin birleşiminden doğrudan faydalanmamaktadır. Bir ağ kodlama yöntemi olan Compute and Forward (CPF), çoklu erişim yöntemlerinden sonra bilinirliği en yüksek eş zamanlı iletim yöntemi olarak gösterilebilir. Bu yöntem özellikle ağ kodlama amacı ile literatüre sunulmuş olsa da güvenlik ve çoklu erişim amaçları için de genişletilmiştir. Kanalda hesaplama (Computation over MAC, CoMAC) ise bir diğer popüler eş zamanlı iletim uygulama alanıdır. Bu alanda yapılan çalışmalar başka bir çok uygulama alanı için genişletilmiştir. Analog fonksiyon hesaplama (Analog Function

Computation, AFC) yöntemleri özellikle consensus uygulamalarında (bu uygumalarda kullanıcıların bir değer üzerinde hem fikir olması amaçlanmaktadır), federated learning uygulamalarında (kullanıcıların dağınık olduğu ağlarda özelleşen makine öğrenmesi yöntemleridir) ve spectrum sensing uygulamalarında (kanalda birincil kullanıcıların kullanmadığı frekansların tespit edilerek ikincil kullanıcılara atanması ve frekanstan tarassufu edilmesi amaçlanmaktadır) kullanılmıştır. Bu tez içerisinde eş zamanlı iletimin kullanıldığı uygulamalar ve bu uygulama alanlarındaki literatürde bulunan çalışmalar detaylı bir şekilde incelenmiş ve gruplandırılmıştır. Bu inceleme sonucunda elde edilen fikirler, eş zamanlı iletimin desteklendiği iki güvenlik sistemine esin kaynağı olmuştur. Özellikte kanalda hesaplama çalışmalarının genişletilmesi sonucu elde edilen bu yöntemler, eş zamanlı iletimin güvenlik uygulamalarındaki kullanılabileceğini göstermektedir.

İkinci kısımda, çok kullanıcılı ağlar için bir kimlik doğrulama (authentication) yöntemi ve bir anahtar oluşturma (key generation) yöntemi sunulmuştur. Bu yöntemler, fonksiyonları havada (kanalda) hesaplayarak alıcının iş yükünü azaltan analog fonksiyon hesaplama (AFC) çalışmalarından esinlenmiştir. AFC yöntemleri temelde, alıcı ve verici uçlarda işaret işleme kullanarak kanalın sönümlemesini (fading) tersine çevirip kanal modelini toplama işlemi ile eşleştirmeye (matching) dayalıdır. Sonrasında işaret işleme tekniği ilerlerilerek başka fonksiyonların hesaplanması da mümkündür. Ancak mevcut AFC yöntemlerinde, gönderilen bireylsel verilere alıcıda ulaşmak mümkün değildir. Alıcı sadece iletilen bilginin bir fonksiyonuna erişmektedir. Kimlik doğrulama yönteminde, bu verilere alıcı tarafında tek tek ulaşılmasını sağlayan, hatta vericilerin kimliğinin doğrulanmasını mümkün kılan bir işaret işleme şeması geliştirilmiştir. Bu amaçla, işaret işleme şemasında Gauss asal (prime) sayıları kullanılmıştır. Ön-işlem fonksiyonları (pre-processing functions), iletilecek bilgileri işaretlerin genliklerine logaritmik formda kodlamaktadır. Ayrıca mesajlar, her düğüm için özel olan asal kimliklerin (identifier) üsteli şeklinde kodlanmaktadır. İşaretler eş zamanlı gönderildiği için kanalda birleşmiş (superimposed) olsa da, asal kimlikler sayesinde bireysel mesajların alıcıda tek tek elde edilmesi mümkündür. Ayrıca, asal sayılar ve kanalın sönümlemesi sonrasında sahte işaretlerin tespit edilmesini (spoofing detection) de sağlamaktadır. Başarılı bir tespit için saldırganın resmi kullanıcılardan daha büyük kanal kestirim hatasına (channel estimation error) sahip olduğu varsayılmaktadır. Bu yöntemin bilgisayar ortamında benzetimlerle işaret hata oranı (symbol error rate, SER), alıcı çalışma karakteristiği (receiver operating characteristics, ROC) eğrileri oluşturulmuş ve uygulanabilirliği sınanmıştır.

Anahtar üretme yönteminde ise, çok kullanıcılı ağların anahtar üretme sürecindeki zaman ve bant genişliği verimliliği artırılmış; ayrıca merkezi bir düğüme (veya harici bir üçüncü partiye) olan ihtiyaç ortadan kaldırılmıştır. Anahtar üretim yöntemi, kanal modelini kimlik doğrulama yöntemine benzer bir şekilde ön ve son işlem fonksiyonları ile değiştirmektedir. Ancak bu sefer kanal, her bir düğümde ortak anahtar oluşturacak bir fonksiyon ile eşlenmiştir. Üretilen anahtarın, her düğümden bileşenler içerdiği varsayılmıştır ve yarı çift yönlü ve tam çift yönlü iletişim senaryoları için incelenmiştir. Yarı çift yönlu iletimde, anahtar parçaları ön-işlem fonksiyonundan geçirilim eş zamanlı şekilde iletilmektedir. Buradaki ön-işlem fonksiyonu, gönderilen işaretlerin sadece hedeflenen alıcıda anlam ifade etmesini sağlayacak şekilde tasarlanmıştır. Bir alıcıda anahtar oluşmasını sağlayan bu yöntemin tüm düğümler için tekrar edilmesi ile tüm düğümlerin aynı anahtara sahip olduğu bir ağ elde edilmesi mümkündür. Bu yöntem sayesinde gizli dinleyicilerin anahtarı doğru bir şekilde elde

etmesi engellendiği gibi, merkezi bir düğümün varlığına olan gereksinim de ortadan kaldırılmaktadır.

Yarı çift yönlü iletimin uygulanabilirliği ve hata performansı benzetimlerle incelenmiştir. Elde edilen hata oranları yarı çift yönlü iletime dayalı anahtar üretim yönteminin uygulanabilirliğini göstermiştir. Sunulan yöntemin ideal olmayan durumlardaki uygulanabilirliğinin sınanması ve performansının incelenmesi için benzetimler genişletilmiştir. Öncelikle sadece gürültünün bulunduğu senaryoda, elde edilen anahtarın gerçek anahtardan sapması MSE (Mean Squared Error) kullanılarak hesaplanmıştır. Sonrasında anahtar üretim başarımını iyileştirmek için alıcılara kod çözme işlemi eklenmiştir. Alınan işaretlerin en yakın olası noktaya eşlendiği bu kod çözme sayesinde performans metriği olarak hata olasılığına geçilmiştir. Kod çözmeli durum için, öncelikle gizli dinleyicinin kanalının gerçek alıcının kanalından farklı olduğu gerçekçi senaryo benzetimler ile incelenmiştir. Bu senaryoda alıcının yüksek SNR değerlerinde hata oranını düşürebildiği görülürken, gizli dinleyicinin hata olasılık alt sınırının %50'nin olduğu görülmüştür. Sonrasında, resmi vericilerin kanal kestirim hatası yaptığı senaryo hesaba katılmış ve kanal kestirim hatasının anahtar üretim performansı üzerine etkisi incelenmiştir. İnceleneme sonucunca kanal kestirim hatasının hem resmi alıcı için hem de gizli dinleyici için yıkıcı bir etkiye sahip olduğu görüşmüştür. Tam çift yönlü iletim senaryosunda ise tüm düğümlerin eş zamanlı iletim yaptığı ve kanalı dinlediği varsayılmıştır. Bu senaryoda, tek bir eş zamanlı iletim ile tüm düğümlerde aynı gizli anahtarı üretmek mümkündür. Tek bir denklem içerisinden (tek bir iletişim ile) çok sayıda kullanıcı için gizli anahtar üretiminin ancak çoklu-doğrusal haritalar (multi-linear maps) ile mümkün olacağı literatürde gösterilmiştir. Ancak daha çoklu-doğrusal harita şartlarını sağlayabilen bir fonksiyonun varlığı tespit edilmemiştir. Tam çift yönlü senaryoda ise, düğümlerin kanal ile etkileşimi metamatiksel olarak çoklu-doğrusal haritaların gereksinimlerini sağlamaktadır. Böylece tek iletişimde (tek bir denklem ile) tüm düğümlerin gizli anahtara sahip olması sağlanmaktadır. Bu durumda telsiz kanal doğal bir çoklu-doğrusal harita işlevi görmektedir veya bir başka deyişle telsiz kanal işaret işleme kullanılarak çoklu-doğrusal haritaya eşlenmiştir.

1. INTRODUCTION

The theory of communication, as given in [2] by Shannon, considers the mathematical relation between two points. Since the objective of the communication is to reconstruct a message at another point, the theory identifies anything between the source and the destination as noise. This assumption is still valid in the advanced communication systems, especially in the wireless communication networks that introduce the most destructive, as well as limited, medium to its users. On the other hand, its mobility feature attracts more and more users at each generation and its limited resources present extreme design challenges since the wireless medium is shared by all the participants.

Some of the most critical design challenges can be listed as providing security, low latency, and high communication rates and supporting a large number of users. In any of those aspects, the solution is sought, designed and tested for the Shannon's pairwise communication model. Hence, the first step of the network design generally starts with virtually dividing the limited channel resources to each user and considering the crowded wireless channel as a combination of multiple subchannels between the pairs of nodes. For example, assigning orthogonal frequencies to different users is an elegant approach to solve these challenges.

It is needless to say that all the aspects listed above are important for a wireless network, however their importance and the priority depends on the objective of the application. With the emergence of the internet of things (IoT), other design considerations can be added to the design challenge list such as the energy consumption or the system complexity. More importantly, the IoT enables an immense range of wireless applications such that these aspects (and many more) are required in different and particular orders in these applications. For instance, for a banking-related application, security criteria would have higher importance whereas another criteria, i.e. complexity, would have less, while mass sensor networks can require low energy consumption and high bandwidth efficiency instead.

This diversity of wireless applications attracts the researchers' attention to the beyond of the traditional perspective. The physical layer based studies have already gained attention on this matter to help with the wireless communication problems. One peculiar idea is related to the physical layer and the interference of signals. In the last two decades, the researchers have sought an answer to the question if the interference of signals can be beneficial. Many studies in the literature considered this question and positive answers were given under certain scenarios. In this thesis, firstly a survey is presented on these scenarios and secondly, two security methods are presented to improve the resource efficiency with simultaneous transmission.

1.1 The Scope of the Thesis

The multiple user networks and the ways of accessing the wireless channel is the major interest of this thesis. The answers that are given to the question of if the interference of the signals can be beneficial, directly violates the Shannon's communication model regarding the inference policy. As a result, the answers to that question also skip the first design step that divides the wireless channel into pairwise subchannels and distributes the resources among the users. Here, the scope of the thesis is argumentative because there are certain techniques in the literature, that accept the inference of other signals, however still interested in the pairwise communication and not benefit from the inference.

The general resources of a wireless network is the time and the frequency spectrum that is suitable for distribution among the users. However, the communication technologies found other resources such as code or energy to be distributed among the users. The users of these studies occupy the same time and frequency dimensions, yet the users are distinguished from another resource. The Code Division Multiple Access (CDMA) is an example that enables interference and use the code dimension for the multiple access. In another example, the spatial diversity of the MIMO networks can be given that enables the interference. However, the MIMO technology should be considered under the pairwise communication since its interference comes from the signals that are known and managed by a single user.

These examples raise the question of whether the scope of this thesis is limited to any technique that enables the interference of signals (i.e. uses the same time and frequency

slots) or limited to a more narrow scenario. The first option would draw an incomplete map on the main idea and the latter would be too extensive to cover and also include unrelated parts. For this reason, this thesis loosely includes the major techniques (e.g. CDMA, MIMO) that enable the interference of signals and not directly benefit from it. However, the surface on their relation to the interference are illustrated and the readers are referred to more detailed resources on the subject.

The major interest of this thesis is the techniques that intentionally exploit the interference of signals and directly benefit from it. The multi-user techniques that is presented here use the same time and frequency dimensions for communication and do not aim to distinguish the individual information. Instead, these methods are only interested with the superimposed form of the signals. Before giving a general map of these techniques, it is beneficial to clarify some of the phrases used in the thesis to avoid any ambiguity.

The Wireless Multiple Access Channel (W-MAC) model that is given in Fig. 1.1 is considered throughout the thesis and the multiple access term states the fact that the simultaneously transmitted electromagnetic waves combine with each other. In general, this statement only covers the time dimension, i.e. the waves from other frequencies also merge over the W-MAC. However, it is straightforward to separate the superimposed waves in the frequency dimension at the receiver. For this reason, the definition of the simultaneous transmission also includes the frequency dimension. The simultaneous (concurrent) refers to transmissions at both time and frequency domain, i.e. signals are transmitted at the same time and frequency band. Similarly, the simultaneously transmitted signals are referred as *superpositioned* or *superimposed*.

1.2 A Map of the Communication Techniques That Uses Simultaneous Transmission

There are several application areas of *simultaneous transmission* based techniques for different purposes. Each application has its own design parameters and performance metrics, e.g. distributed detection problems usually require a high detection probability while the security applications are interested in the secrecy rates. As a result, this thesis assumes an extraordinary point of view that connects various problems and application

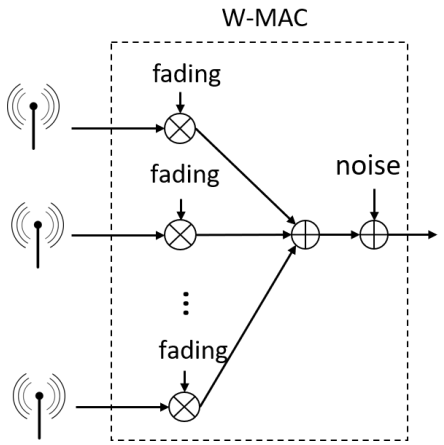


Figure 1.1 : An illustration of the Wireless Multiple Access Channel.

areas of the wireless communication networks. However, the *superposition* property of the W-MAC implies several common grounds as;

- Distributed nature: All applications include decentralized multiple nodes. As a result, scalability, energy efficiency and complexity is often a design concern.
- Wireless nature: The users communicate over the wireless channel and the amount of channel state information (CSI) knowledge at the users and the channel characteristics (e.g. fading) are important concerns.

The application areas of the simultaneous transmission-based techniques are listed in Fig. 1.2. The multiple access and the multiple antenna applications are the early examples that the simultaneous transmission is enabled. The CDMA and the NOMA techniques are essentially interested in the pairwise communication. For this reason, the transmitters use a third resource (other than the time and frequency) to distinguish the individual messages, e.g. the CDMA or NOMA users uniquely encode their messages as a function of a code block or a power level respectively. On the other hand, the traditional MIMO applications benefit from the superimposed signals to gain diversity although the network is not distributed.

The joint source-channel coding proposed in [3] created a paradigm shift on the multi-user communication models by considering the joint optimization of communication and computation aspects. This paradigm is later shaped into several core models such as TBMA [4], CoMAC [5], CPF [6] and AFC [7]. These studies influenced novel techniques in the past decade and appeared at various application

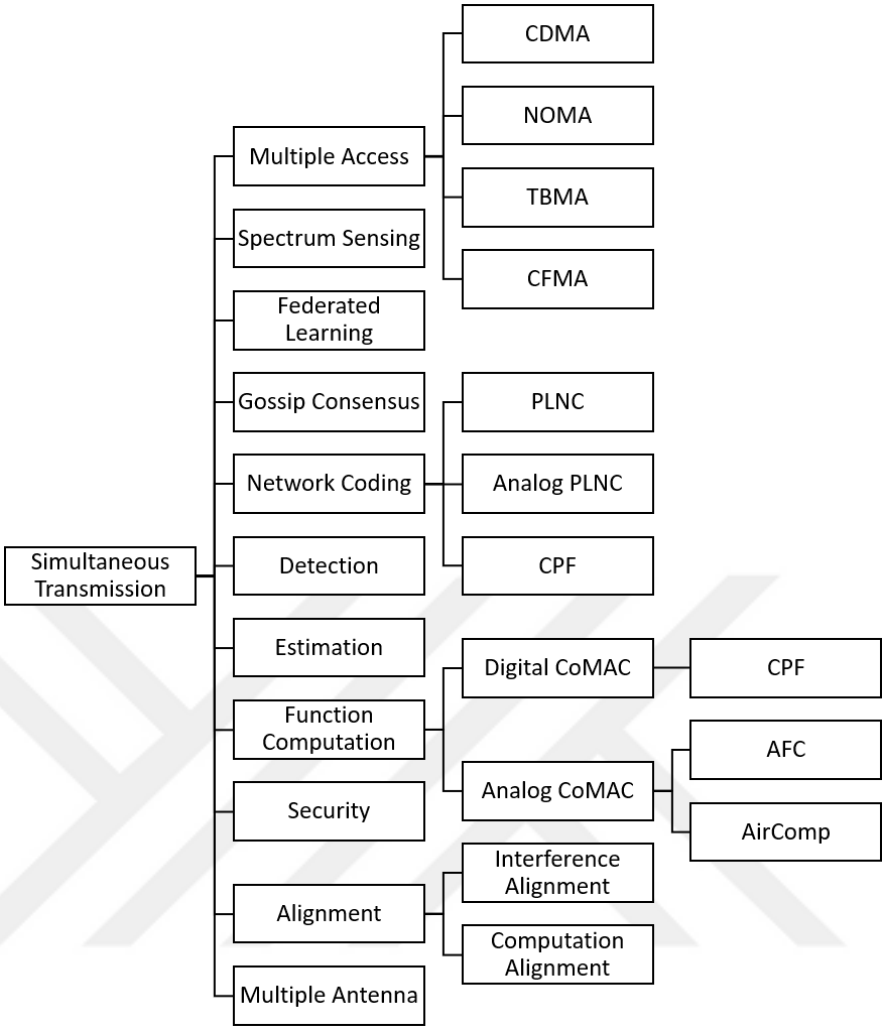


Figure 1.2 : A list of the application areas where the simultaneous transmission techniques are implemented.

areas from network coding to the federated learning. An illustration of these techniques and their general application areas can be seen at Fig. 1.3.

The CPF is mainly investigated for the relaying and network coding purposes to improve the network capacity (i.e. computation rate), however, it also extended to multiple access applications (CFMA [8]) to reduce complexity and security applications [9] to improve secrecy rate. Also, the computation alignment and the function alignment studies which are influenced by the CPF and CoMAC are proposed to reach the computing capacity in multiple antenna networks.

The CoMAC inspired various digital and analog function computation methods that aim to allow low-latency and low-bandwidth computations in distributed wireless networks. The main idea behind the CoMAC is later implemented in spectrum sensing,

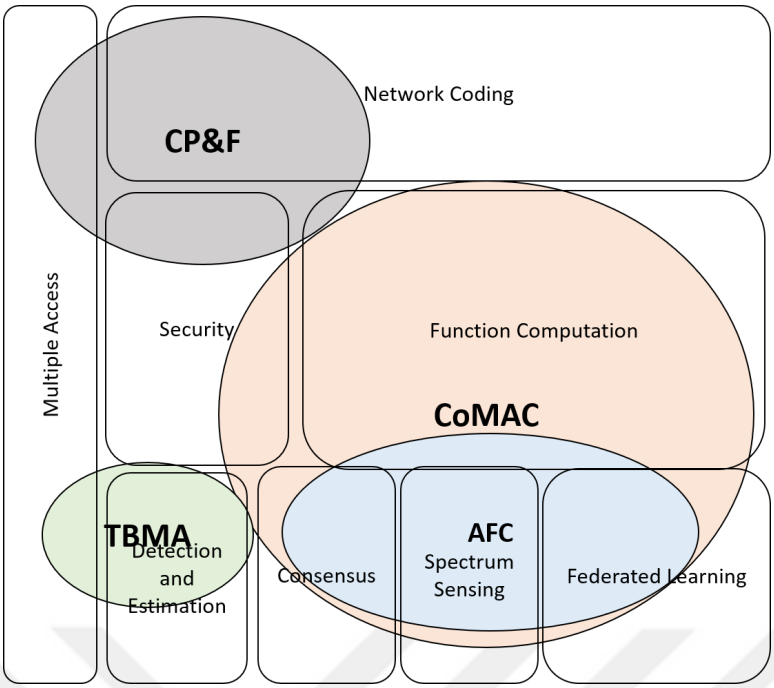


Figure 1.3 : A map of the featured methods and their applications.

federated learning, and consensus algorithms to improve network efficiency. The TBMA is primarily used for the distributed detection and estimation applications to design scalable and energy-efficient models.

From an intriguing perspective, all these models and applications can be viewed as a particular function that manipulates the wireless channel to perform a given task. For example, multiple access algorithms aim to transfer the transmitted data to a destination. Eventually, the simultaneous transmission manipulates the channel to perform a function which both inputs and the outputs are the transferred data. However in the detection algorithms, the outputs are not the data, instead the output of the function is the test statistics. Hence, it can be said that a detection algorithm that use simultaneous transmission manipulates the wireless channel to perform a function that inputs are the sample set and the output is the test statistics. These input-output relationships are illustrated in Fig. 1.4.

The security applications consider transferring data to the receiver without leaking information to the eavesdroppers. This approach manipulates the W-MAC to transfer the initial data to the receiver such that the received signal is only meaningful at the destination. Network coding applications considers transferring data in layered networks structures. The simultaneous transmission models propose a cascade of functions (composite functions) (relays) that both the initial inputs and the final

outputs are the data. Function computation, federated learning, spectrum sensing etc. algorithms match the W-MAC with particular functions that is unique to the purpose of the application. Moreover, gossip and consensus algorithms also consider the topology of the network by using subgroups or subfunctions in the network, i.e. composite functions.

1.3 Contributions

Contributions of this thesis can be listed in three categories. Firstly, the simultaneous transmission-based communication techniques are investigated and classified regarding their application purposes. Also, a map of the existing literature is given with introductory information on each application. Major studies are investigated in more detail and their contributions are highlighted.

Secondly, an authenticated data transmission method is proposed. The method brings time and bandwidth efficiency to multi-user uplink networks. Simultaneous transmission is used to reduce the required time slots as in AFC. However, authenticated data transmission also allows the reconstruction of the individual data at the receiver. Furthermore, the uniqueness of the fading is exploited to authenticate the data at the Fusion Center (FC).

Lastly, a key generation method is proposed for wireless sensor networks (WSN). The method brings scalability and does not require a trusted third party or a center node to distribute keys to the nodes. As a result, the energy and complexity burden of the network and the duration of the key generation process can be reduced. If the communications between the nodes are half duplex, the method can reduce the key agreement duration proportional to the number of nodes. In the scenario of full-duplex communications, the method is able to reduce this duration to a constant scale. The method provides weak security against passive eavesdroppers.

The research outputs that are presented in this thesis are also submitted in the following publications.

- U. Altun, S. T. Basaran, G. Kurt and E. Ozdemir, "Authenticated Data Transmission Using Analog Function Computation," in *IEEE Communications Letters*, doi: 10.1109/LCOMM.2020.3007636.

- U. Altun, S. T. Başaran, G. K. Kurt and E. Ozdemir, "Scalable Secret Key Generation for WSNs," in *IEEE Internet of Things Journal*, *in review*.
- U. Altun, G. K. Kurt and E. Ozdemir, "A Survey on the Simultaneous Transmission based Communication Techniques," in *IEEE Communications Surveys & Tutorials*, *in review*.
- U. Altun, S. Tedik Basaran, G. Karabulut Kurt, and E. Ozdemir, “A Joint Data Transmission and Authentication Technique over the Wireless Multiple Access Channel,” applied to Turkish Patent Institute, 2018/ 11274, August 2018

1.4 Outline

In Chapter 2, multiple access methods that benefit from the simultaneous transmission is presented. Chapter 3 is dedicated to the network coding algorithms and the digital and analog function computation studies are investigated in Chapter 4. The detection, estimation and spectrum sensing studies are listed and examined in Chapter 5. The contributions and the performance metrics of various simultaneous transmission applications are presented in Chapter 6 and the security studies are presented in Chapter 7. In Chapter 8, a simultaneous transmission based data transfer model is proposed. Its authentication mechanism is also investigated and verified with simulations. The Chapter 9 is dedicated to the secret key generation model that provides a key to multiple nodes without the need of a center node or a third party. Lastly, the thesis is concluded in Chapter 10.

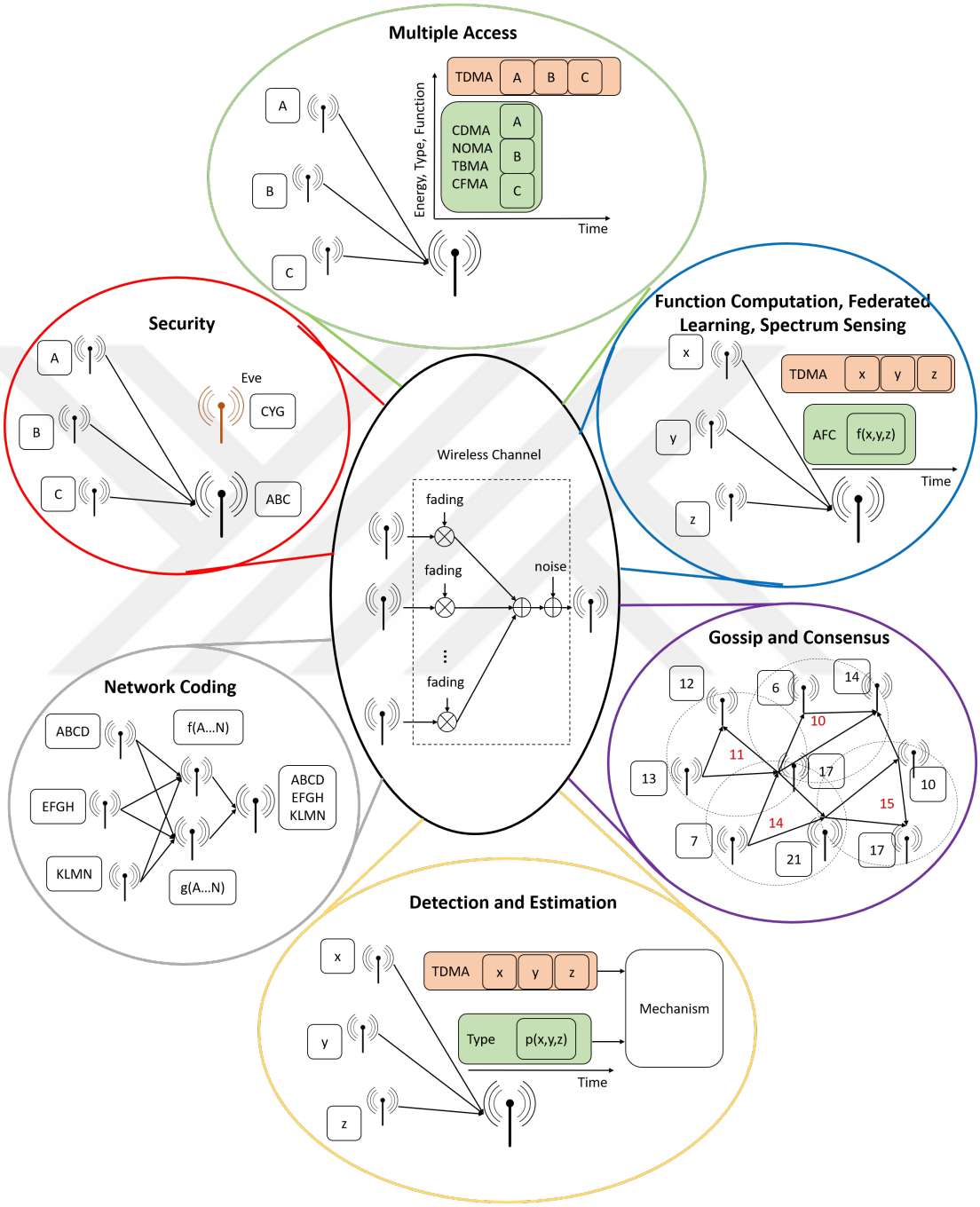


Figure 1.4 : An illustration of relationship between the applications and their network model.

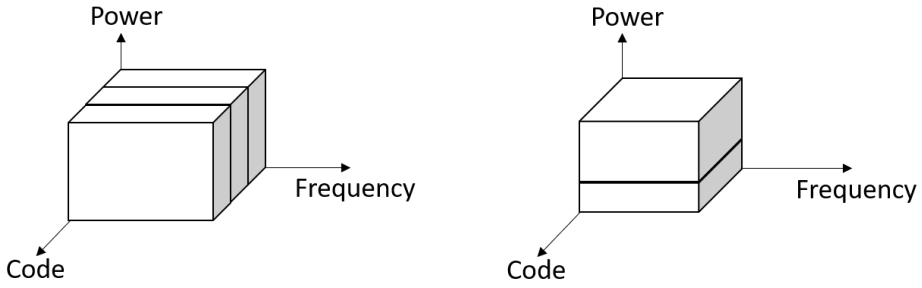
2. MULTIPLE ACCESS

Wireless channel has limited resources (signaling dimensions) such as frequency, time or space, and accessing the channel requires a portion of each resource. Multiple access methods aim to allocate these resources to multiple users efficiently [10]. The simultaneous transmission enables the dedication of all frequency and time domains to a single user. However, known multiple access methods such as CDMA and NOMA divide another dimension to its users rather than exploiting the superposition of the signals. For this reason, elementary information on these methods will be given and the reader will be referred to proper references.

2.1 Code Division Multiple Access

In Code Division Multiple Access (CDMA) method, users are assigned a spreading code to separate users from each other. Therefore, channels can be used by all users in the same period and bandwidth. Especially in the uplink scenario, in which multiple users transmit simultaneously, the base station receives a combination of signals from all users. If the codes are orthogonal, despreading the received signal with the corresponding code outputs the information signal of the corresponding user. Fig. 2.1 illustrates the resource distribution of the CDMA technique. As seen, each user occupies a large and equal bandwidth and usually, a power balance is required. Non-orthogonal codes are also used in CDMA to flex the synchronization problem and support more users, however removing orthogonality adds interference to the system.

In [11] and [12], extensive information is given about the working principles of the CDMA and various versions of the CDMA are classified. Complementary code based MIMO CDMA methods that aim to revive CDMA in the next-generation systems are investigated in [13].



(a) CDMA (b) NOMA

Figure 2.1 : Distribution of the resources in CDMA and NOMA methods.

2.2 Non Orthogonal Multiple Access

Non Orthogonal Multiple Access (NOMA) is an emerging multiple access method that is based on the distribution of power domain.[1] NOMA can be viewed as a complementary method for the existing multiple access techniques since the power domain is not suitable to support more than two or three users. As a result, the distribution of another resource is required. However, NOMA based systems still fall under the category of our interest since NOMA enables the transmission of two users simultaneously. Resource distribution of NOMA is given in Fig. 2.1b. Power is intentionally distributed to users with a level difference. The model depends on interference cancellation such that the receiver can distinguish the higher level and lower level signals and cancel it.

NOMA is a new and rapidly emerging multiple access method and attracts attention for the next generation communication systems. Comprehensive information on NOMA can be found in [14] and [15]. In [16] general information on the current challenges of NOMA (also the rejection of NOMA in 5G standards) and possible solutions are analyzed. Additionally, performance of NOMA is investigated with computer simulations.

[1]NOMA is usually referred for power domain distribution. However, the name also suggests a category that includes any non-orthogonal method (i.e. two categories; orthogonal and non-orthogonal multiple access methods). Only the power domain NOMA is considered in the thesis.

2.3 Type-Based Multiple Access

The Type-Based Multiple Access is a unique method by means of channel-user relationship since the users in the TBMA does not aim to reach to their destination individually. Instead, data statistics (type) of all the users are transferred to their destination [17]. It should be noted that the individual data is not reconstructed at the receiver and the TBMA is not suitable for mobile communication. However, it reduces the network latency and shows huge potential in sensor networks that require only the total data statistics. Specifically, TBMA is widely used for detection and estimation purposes.

The TBMA is not widespread in the literature and requires a broader explanation of its working mechanism. For this reason, this section is dedicated to the explanation, and the literature review of the TBMA is given in the detection and estimation chapter.

Consider a network that consists of n users that aims to transfer messages (e.g. sensor readings) $X_i, X_2, ..., X_n$ to an FC. The i^{th} user in the network assigns its message X_i to a waveform s_{x_i} that is chosen from an orthonormal waveform set $\{s_1, s_2, ...s_k\}$. When each user in the network simultaneously transmit its data with energy E, the FC obtains the following expression [18],

$$z = \sum_{i=1}^{n} h_i \sqrt{E} s_{x_i} + w \tag{2.1}$$

where h_i and w are the channel and fading coefficients respectively. Assuming the channel gains are inverted, the signal at the FC becomes,

$$z = \sum_{j=1}^{k} \sqrt{E} N_j s_j + w \tag{2.2}$$

where $N_j = \sum_{i=1}^{n} 1 \; \forall (X_i = j)$. Note that the same messages are transmitted with the same waveforms and superimposed over the channel. As a result, the FC receives the count of the messages for each waveform (e.g. the histogram (type) of the messages).

2.4 Compute-and-Forward Multiple Access (CFMA)

The Compute-and-Forward (CPF) is a relaying and network coding method that is based on the simultaneous transmission of signals. The objective of the CPF is to efficiently transfer the messages of multiple sources to a receiver by using multiple relay nodes. Essentially, CPF transfers a function of the source messages to each

relay by exploiting the superposition property. The relays are unable to decode the individual messages since each of them obtains a single function that contains multiple messages (unknown parameters). The relays forward their functions to the receiver and the receiver can reconstruct the individual messages by solving the functions for the unknown parameters. Contrary to other network coding algorithms, the communication phase between the sources and the relays takes place at the same time slot and the bandwidth in the CPF, hence it offers efficiency on the spectrum and latency.

The Compute-and-Forward Multiple Access (CFMA) is inspired by the CPF and instead of relaying the messages, it enables direct access to the channel by exploiting the superposition property. The CFMA is proposed in [19] by Zhu and Gastpar for the networks that two users aim to access to a single receiver. The main idea behind the CFMA is based on the same coding and decoding structure as the CPF which yields a function of the messages at the receiver. However, two users directly communicate towards a receiver without multiple relays and two functions are required at the receiver to solve the messages. For this reason, CFMA also uses successive cancellation decoding to obtain the coefficients of the second function. The writers also examine the more than two users scenario in [19] and they consider the LDPC coded CFMA in [8, 20].

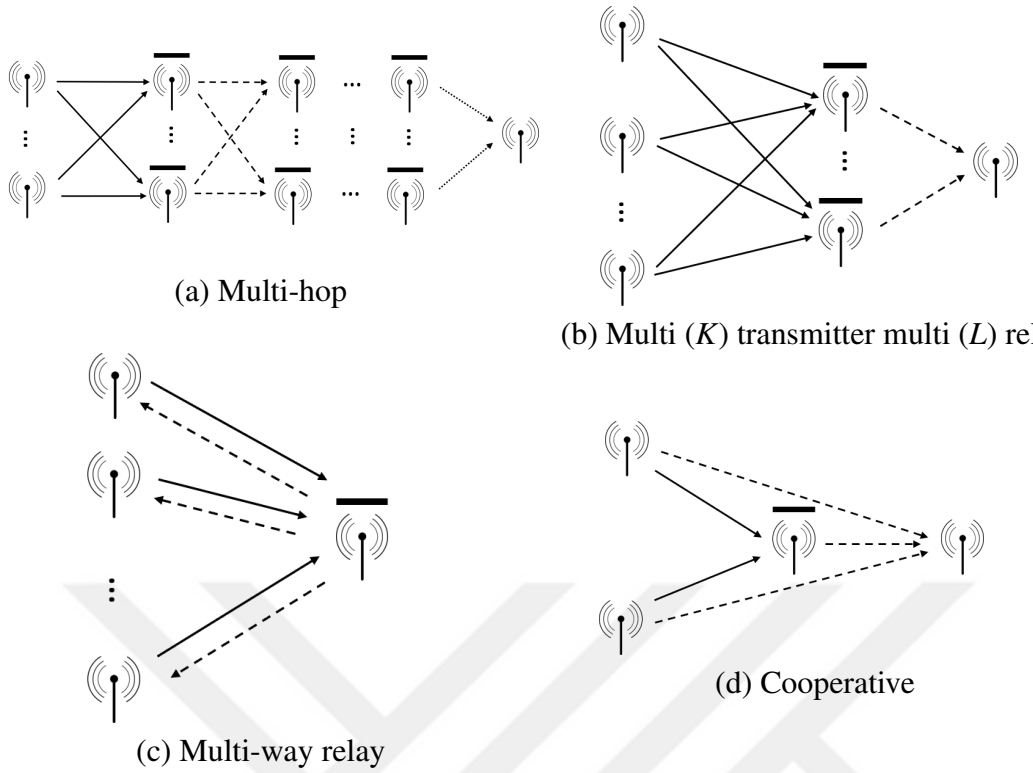
The multiple access methods eventually match the wireless channel with a function that transfers data from multiple sources to a single destination. Inputs and the outputs in this function are the transferred data. In the following Chapter, network coding algorithms are presented. The network coding considers layers of nodes between the sources and the destination. As a result, these methods consider composite functions that the initial inputs and the final outputs are the transferred data.

3. NETWORK CODING

The source and channel coding are essentially concerned with the communication between two nodes. Specifically, they improve the capacity and error performance of pairwise communication respectively. On the other hand, network coding benefits from the architecture of the network in order to improve its capacity, efficiency, or security [21]. The network coding is interested in the information flow between the nodes, and the fundamental idea behind the network coding is illustrated in Fig. 3.2a. n_1 and n_3 aims to exchange information through an in-between node n_2 in the given network. Without network coding, the messages S_1 and S_3 of the nodes n_1 and n_3 would require a total number of four pairwise hops, hence four-time slots. A simple network coding algorithm can be applied, as given in Fig. 3.2a, to reduce the required time slots. After obtaining S_1 and S_3 sequentially, the relay node n_2 computes $S_2 = S_1 \oplus S_3$ and broadcasts it. Since the nodes know their initial messages, n_1 and n_3 can extract the unknown message from S_2. As a result, the network gains a time slot with the broadcast of the relay node.

Network coding is one of the most effective and intriguing applications of the simultaneous transmission since the multiple access nature of the channel presents unique opportunities for the code design. These studies are specifically named Physical Layer Network Coding (PLNC) and they outperform the traditional network coding in certain scenarios [22]. The PLNC is considered in two sections since one study, the Compute-and-Forward (CPF) [6], made a name for itself and requires special attention.

The network architecture is an important parameter in the investigation of these studies and some commonly used architectures are illustrated in Fig. 3.1. Also, the studies are classified for their network architecture in Table 3.1 along with their performance metrics. In this section, the main ideas behind these methods are briefly explained and the literature is investigated.



(a) Multi-hop

(b) Multi (K) transmitter multi (L) relay

(c) Multi-way relay

(d) Cooperative

Figure 3.1 : Common network models where the lines over the nodes represent the relays.

3.1 Physical Layer Network Coding

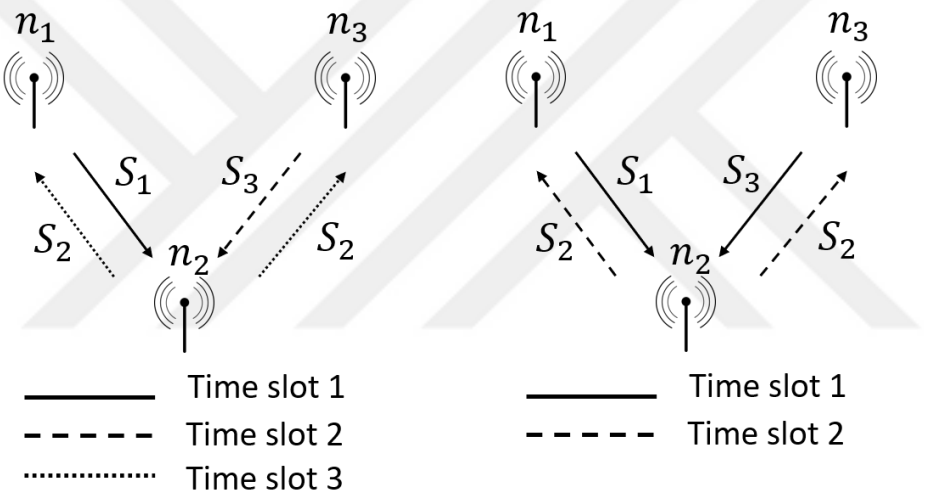
The PLNC is proposed in 2006 by Zhang *et al* [1]. The proposed network is based on the superposition principle to reduce the required time slots. A simple three-node example of the PLNC is given in Fig. 3.2b. Without the conventional network coding, it is obvious that the uncoded scheme requires a time slot for each transmission and the conventional network coding reduces the required number of transmission by enabling the broadcast of the relay.

The PLNC further improves this situation by accepting the superposition of the messages from n_1 and n_3 to the relay node as seen in 3.2b. In the PLNC scenario, relay node receives the superimposed message and can not extract S_1 and S_3. However PLNC allows n_1 and n_3 to decode the superimposed message after n_2 broadcasts it. Later, this basic example is extended to larger networks and different coding schemes as in [23] that a packet-based PLNC architecture is proposed and implemented. The study uses a testbed of computers and establishes a proof of concept for the PLNC.

Analog version of the PLNC [1] is proposed in [24]. The writers simply consider the superposition of the signals instead of packets. Also, the relay uses AF to transfer the

Table 3.1 : PLNC studies.

Author	Year	Network model	Contribution	Performance metric
Zhang *et al* [1]	2006	Two-way (multi-hop)	Traditional PLNC introduced.	BER
Katti *et al* [23]	2008	Multi-way	Throughtput improved with PLNC.	Throughtput gain
Katti *et al* [24]	2007	Two-way	Analog PLNC introduced.	Network throughput
Amah and Klein [25]	2011	Multi-way	STANC introduced.	Sum rate
Wie and Chen [26]	2013	Cooperative	STANC adapted to multi-way cooperative networks.	Sum rate
Gündüz *et al* [27]	2010	Cooperative (cMACr)	Lattice codes used for PLNC in cooperative networks.	Achievable rate region
Xu *et al* [28]	2012	Multi-hop	PLNC implemented to multi-hop networks with a cross-layer design.	Network throughput
Burr and Fang [29]	2014	Multi-hop	Algebraic constructs are used in the network design.	Network throughput
Al-Rubaie *et al* [30]	2013	Two-way	LDPC and Turbo codes are compared.	BER
Hayashi [31]	2019	Cooperative (Butterfly)	PLNC and NC is compared.	Number of time spans



(a) Traditional Network Coding (b) Physical Layer Network Coding

Figure 3.2 : Information flow comparison between the traditional NC and PLNC [1].

superimposed signal. After presenting their results, the study also verifies them by implementing the proposed method with SDR modules.

Another analog PLNC scheme, space-time analog network coding (STANC), is proposed in [25]. The study considers a non-regenerative multi-way relay network that multiple nodes (equipped with single antenna) exchange information through a single relay (equipped with multiple antennas) in the scenarios of stationary and non-stationary channels. The STANC is proposed for the stationary case and an alternative solution, the repetition transmission, is suggested for the non-stationary channels. Achievable sum rates of these two models are calculated and verified with

simulations. The simulations also included a comparison with the Zero Forcing (ZF) and maximization of SNR beamforming models and it is shown that the STANC outperforms the other models regarding the sum rates. In [26], this study is customized to the networks where multiple nodes transfer information to a single receiver both directly and with the help of a relay node (equipped with multiple antennae). The sum-rate performances and the error rate performances are evaluated with simulations for the cases of direct transmission, analog network coded transmission, and the STANC transmission.

In [27], a network that consists of a single relay, two transmitters and two receivers (compound multiple access channel with a relay (cMACr)) is considered. The relay node is assumed to have cognitive capabilities and able to include its own message to the received message before forwarding. The study investigates the achievable rate regions of three relay methods; Decode-and-Forward (DF), Compress-and-Forward (CF) and lattice coded (CPF) schemes. Also, a special case is examined where the cMACr network does not allow cross-reception (i.e. one of the sources always connects to the receiver via the relay, not directly). In this scenario, the modulo sum of the source messages is computed with the lattice codes and compared with the DF and CF schemes.

A multi-hop network includes multiple layers of relay nodes between the transmitters and the receiver as illustrated in Fig 3.1a. In [28], a cross-layer strategy is followed for a multi-hop PLNC network to design the efficient routing paths. In [29], algebraic frameworks are considered for the design of multi-hop PLNC networks.

The compatibility and the performance of the PLNC with error correction codes are investigated in [30]. Turbo codes, LDPC codes and bit-interleaved coded modulation with iterative decoding (BICM-ID) are simulated in a PLNC based network. The results showed that the PLNC reduces the BER performance of the all three channel coding schemes.

In [31], a secure PLNC scheme is designed. The method is inspired by the forwarding algorithm given in [32] (based on CPF). The study analyzes two networks with a butterfly topology and a three source topology. Also, it is shown that the secure PLNC outperforms the secure network coding such as given in [33].

3.2 Compute-and-Forward

The Compute-and-Forward (CPF) is proposed by Nazer and Gastpar in [6] as a relaying method and draw the attention of numerous researchers throughout the years. The CPF is inspired from the lattice codes (structured codes) that is previously used in [5, 34, 35]. A lattice is a group of real number that is denoted by Λ and for any $t_1, t_2 \in \Lambda$, their summation is also $t_1 + t_2 \in \Lambda$. This property makes the lattice codes the building blocks of CPF as for many simultaneous transmission techniques.

In a fundamental CPF network as given in Fig. 3.3, N nodes encode their message $t_n \in \{1, ..., N\}$ to the lattices as

$$x_n = \mathscr{E}(t_n) \tag{3.1}$$

and simultaneously transmit their message x_n to the channel. Then a relay obtains the superimposed signal

$$y = \sum_{n=1}^{N} h_n x_n + z \tag{3.2}$$

where h_n is the channel coefficient and z is the AWGN. The CPF decoder ($\mathscr{D}$) scales the received message as,

$$\alpha y = \sum_{n=1}^{N} \alpha h_n x_n + \alpha z \tag{3.3}$$

and then quantizes the scaled signal to the closest lattice as follows,

$$\alpha y = \underbrace{\sum_{n=1}^{N} \beta_n x_n}_{\text{approximation of } \alpha y} + \underbrace{\sum_{n=1}^{N} (\alpha h_n - \beta_n) x_n \beta z}_{\text{effective noise}}. \tag{3.4}$$

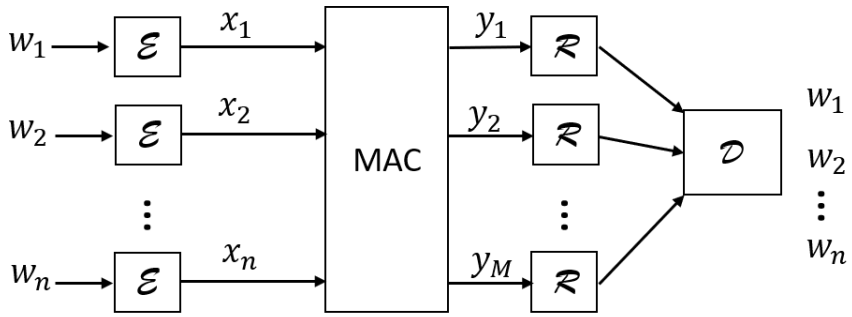


Figure 3.3 : Compute-and-Forward (CPF) network model.

Here, the receiver uses αy to approximate the appropriate coefficients β_n and obtains the following function of the codewords,

Table 3.2 : Compute-and-Forward (CPF) studies.

Study	Year	Network	Contribution	Performance metric
Nazer and Gastpar [6]	2011	$K \times K \times 1$	CPF is proposed.	Achievable rates
Nazer and Gastpar [36]	2011	Two-way	Considered for PLNC.	Achievable rates
Huang *et al* [37]	2013	Multi-way	Rate optimization is investigated.	Sum rates
Tan and Yuan [38, 39]	2015	$K \times L \times 1$, multi-hop	CPCF is proposed.	Sum rates
Nokleby and Nazer [40]	2013	$2 \times 2 \times 1$	Amplify-and-Compute model proposed.	Sum rate
Ntranos *et al* [41], Tan *et al* [42]	2013,4	$K \times 1$, $K \times L \times 1$	Asymmetric power allocation case is considered.	Sum rate
Pappi *et al* [43]	2015	C-RAN	Investigated from coalition game perspective.	Sum rate
El Soussi *et al* [44]	2014	$2 \times 1 \times 1$ cooperative	Rate optimization is investigated.	Symmetric rates
Ordentlich *et al* [45]	2014	$K \times K$	Interference channel considered.	Symmetric rate, sum rate
Zhu and Gastpar [46]	2015	Two-way	Input distributions are investigated.	Symmetric computation rate
Wang *et al* [47]	2012	Multi-way	Outage prob. investigated.	Outage prob.
Song *et al* [48, 49]	2011,3	$2 \times 2 \times 1$, $3 \times 3 \times 1$	Inverse CPF model proposed.	Rate region
Huang *et al* [50]	2013	Two-way	Capacity bounds investigated.	Rate region
Zhu and Gastpar [51]	2013	$K \times 1$	Considered for cognitive radios.	Rate region
Nazer and Gastpar [52]	2014	$K \times 1$	Adapted to DMC.	Rate region
Lim *et al* [53–56]	2016-9	$K \times L \times 1$	Joint typicality decoder proposed.	Rate region
Pappi *et al* [57]	2013	$K \times L \times 1$	CEE investigated.	Computation rate
Ordentlich *et al* [58]	2015	2×1	Feedback included.	Computation rate
Hong and Caire [59–61]	2011-3	$K \times L$	A low complexity design presented.	Computation, sum rate
Liu [62]	2014	Two-way	Channel inversion precoding considered.	Achievable rates, SER
Tunali *et al* [63, 64]	2012,5	$K \times L \times 1$	Eisenstein integer lattices considered.	Outage prob., SER
Wang and Burr [65]	2014	$2 \times 1 \times 2$	Coding gain improved with LDLC.	SER
Mejri *et al* [66, 67]	2012,5	$K \times 1 \times 1$, $K \times 1$	Decoding schemes compared.	Error probability
Wei and Chen [68]	2012	Two-way	Fincke-Pohst code search implemented	Average rate, zero entry prob.
Niesen and Whiting [69]	2012	$2 \times 2 \times 1$	Degrees of freedom investigated.	Degrees of freedom
Feng *et al* [70, 71]	2013	$K \times 1$	Blind CPF (without CSI) presented.	Throughput, complexity
Najafi *et al* [72]	2013	$K \times L \times 1$	Synchronisation problems investigated.	Outage rate, average rate
Sakzad *et al* [73]	2014	$K \times L \times 1$	Phase precoding included.	Equation error rate
Wen *et al* [74]	2015	$K \times L \times 1$	SVP considered with sphere decoding.	Average computation rate
Nokleby and AAzhang [75]	2016	$K \times L \times 1$	Node cooperation case investigated.	Computation rate, outage prob.
Goldenbaum *et al* [76]	2016	$2 \times 2 \times 2$	Designed for OFDM and 5G.	Message rate
Zhu and Gastpar [77]	2016	2×1	Typical sumsets of lattices investigated.	Density of the sets
Huang and Burr [78–80]	2016,7	$K \times L \times 1$, $K \times 1 \times 1$	A low complexity coefficient selection design suggested.	Cumulative distribution func.
Goseling *et al* [81, 82]	2013,4	$K \times L$	Random access included.	Throughput

$$\sum_{n=1}^{N} \beta_n x_n. \tag{3.5}$$

A single relay in the given scenario only obtains an integer function of the messages which gives no information on the individual messages. However, the receiver can solve the messages as long as it obtains independent functions as much as the number of unknown messages. This idea inspired many studies in the literature and several aspects of the CPF have been investigated. The CPF is extended to various channels and network models. Also, various design challenges (e.g. CSI estimation) of the CPF are addressed in the literature. A portion of these studies is collected in Table 3.2 and classified for their network topology, contribution and performance metrics.

In [36], Nazer and Gastpar propose a PLNC scheme based on the nested lattice codes and CPF. It has been shown that the lattice codes are an efficient choice to transfer a polynomial of inputs to a sink node and the receiver can recover the messages if an adequate amount of functions are obtained. The study considers a two-way relay channel and provides an introduction to the existing PLNC approaches. Later, the study proposes the lattice code based PLNC and compares it with other schemes for the transfer rates.

In [48], a complimentary scenario to the CPF scheme, inverse compute-and-forward, is proposed. The CPF scheme computes a function of the transmitted messages at the relay nodes. The proposed network aims to recover the computed functions of the CPF at the receiver. In this network model, two CPF relays send their computed functions to a sink node. The inverse CPF is considered as a cascade to the traditional scheme and the rate region of the cascade network is investigated. It is shown that the proposed cascade network outperforms the traditional pairwise communication-based relay networks on the rate region. In [49], the writers extend their previous inverse CPF study to the three transmitters scenario and investigate the rate region. Their findings show that transmitting equations that have a correlation between them is more optimal than transmitting independent equations.

Challenges of the CPF on lattice decoding is investigated in [66]. The study analyzes the lattice decoders that are suitable for practical scenarios. Specifically, the performance of the maximum likelihood decoder, Diophantine Approximation, and the Sphere Decoder are investigated. The computer simulations are used to compare the decoders and to verify the previous theoretical results. Also, the performance of the one and two-dimensional lattice codes is investigated and it is shown via simulations that the performance degrades for larger constellations. This study is later extended to provide an overall base on the decoding of the CPF in [67]. In addition to the previous study, [67] involves a novel maximum a posteriori (MAP) decoder and a Diophantine approximation based maximum likelihood decoder.

A two-way relay channel with CPF is considered in [68] and [62]. The study in [68] proposes a Fincke-Post strategy based code search algorithm to find the appropriate coefficients. In [83], the writers consider a multi-source multi-relay network to maximize the network flow with CPF. In contrast to the traditional CPF which

optimizes the network coefficients separately for each relay, the proposed design jointly optimizes the coefficient matrix for all relays. The method utilizes a candidate set search algorithm based on the Fincke-Post strategy (as in [68]) to choose the coefficients. The performance of the proposed method is investigated with simulations. In [62], a channel inversion precoding is proposed. The achievable rates of the channel inversion precoded CPF are calculated and it is stated that the proposed precoding approach improves the performance of the CPF.

The communication between the nodes of a hexagonal lattice network is analyzed in [84]. Four communication models are derived depending on the broadcast and superposition communications between the nodes. The two models that are applicable to CPF are investigated on the subject of network capacity. The study achieves an improved lower bound compared to the previous studies. The results reveal that the minimum transport capacity of the broadcast or superposition enabled case $(3/7)$ is larger than the maximum capacity of the not enabled cases $(2/5)$.

In [63] and [64], the alphabet of the lattice codes that is used in CPF is restricted to the Eisenstein integers [1]. The traditional CPF (as in [6]) uses integer-based lattice codes and the study exploits the Eisenstein integers to obtain a better pair of a nested lattice (the coarse and the fine lattice). It is shown that the outage performance and the error-correction performance of the proposed codebooks are superior to the integer-based lattice codebooks.

In traditional CPF, received signals at the relays are scaled up in order to ensure that the coefficients are close to an integer. This is a result of the lattice codes that involve only integer codebooks and scaling the signals up also amplifies the noise at the receiver [6]. Eventually, scaling the signals up establishes a Diophantine trade-off between the amplified noise level and the approximation performance. The Diophantine trade-off of the CPF scheme is investigated in [69] and it is stated that the asymptotic rate of the scheme in [6] is below the MIMO schemes. The writers design a novel compute-and-forward model that benefits from the IA in [69]. The proposed model is shown to reach the same degrees of freedom with the MIMO scheme.

[1] Eisenstein integers are the complex numbers in the form of $z = a + b\exp[2\pi i/3]$ where $a, b \in \mathscr{Z}$

In [38] and [39], the Compute-Compress-and-Forward (CPCF) method is proposed to establish an efficient multi-hop design of the CPF. The main idea behind the CPCF is the fact that relay forwarding rates can exceed the information rate of the sources. For this reason, CPCF includes a compressing phase to improve network efficiency (e.g power gain). The compressing and the recovering algorithms of the CPCF is designed and verified with numerical results. Later, the writers generalize the CPCF method in which the compression algorithm includes more operations and shows better compression performance as demonstrated with simulations. The same problem that results from the redundant forward rate is also considered in [85]. However, in [85], the compression is applied at the symbol level rather than the message level and introduces a mapping to the system.

In [44], a cooperative relay network is considered where two nodes are able to send their messages to a receiver via both directly and over a relay. The study examines two coding methods (CPF and CF) that are based on lattice codes and it aims to optimize the symmetric rate. The writers propose an iterative coordinate descent method that focuses on the power allocation and integer coefficient selection processes for the optimization problem. The results state that the CPF shows better performance than the lattice-based CF. This work is later extended to a multi-user multi-relay cooperative scenario in [86]. Cooperative networks are also considered in [87–91]. The writers in [88, 89, 91] propose an CPF method for the two transmitter singe relay two receiver networks. The CPF is considered for the same scenario with single receiver in [87, 90].

The pairwise CPF model is applied to multi-way relay channels in [37]. The pairwise structure of the network is accomplished with the broadcast and the multiple access transmission of the nodes in two phases. The sum rates of the pairwise CPF and the pairwise successive transmission cases are derived for the multi-way relay channel and compared with each other.

The outage probability of the CPF scheme is derived in [47] for multi-way relay channels. Also the CPF is compared with the non-network coding scheme with respect to the outage probabilities. The results show that in a canonical two-way relay channel, CPF achieves 7 dB gain against the non-network coding at the outage probability of 10^{-2}.

In [40], amplify-and-compute method is proposed which combines the CPF and AF methods. The relays in the network receive the superpositioned lattice codes from the sources as in the CPF and transmit to the next network layer as in the AF.

A CPF scheme that allows asymmetric power allocation to the nodes is proposed in [41] and [42]. The method in [41] is based on the lattice codes in which a fine lattice and a coarse lattice provide codebooks that are decodable and under the power limit respectively. The method maps the messages to the codebooks depending on the power and noise tolerance. Specifically, the top of the message vector is set to zero depending on the power of the codebook and the bottom of the message vector is set to zero depending on the noise tolerance.

A bi-directional relay network in which two nodes exchange information through a relay node under an inter-symbol interference channel is considered in [50]. The proposed model is separated into a multiple access phase and a broadcast phase and the capacity region is derived. The inner bound of the capacity region is computed with the help of the CPF method and the outer bound is computed with the cut-set argument given in [92]. The numerical results revealed that the proposed CPF scheme has a better exchange rate than the DF.

A low-complexity CPF is proposed in [59] which only involves scaling, offset and scalar quantization at the receivers. The method aims to reach the same capacity of the CPF with the low-complexity, low-power decentralized antenna networks. For this purpose, the method considers quantization at the receivers as a part of the wireless channel. The simulations revealed that the computation rate of the quantized CPF outperforms traditional CPF of [6]. The writers extended their work to the downlink scenario of the quantized CPF in [60]. The study derives the computation rate of the proposed scheme and compares it with the downlink CPF via simulations. The reverse CPF is generalized and extended in [61] to cover additional scenarios and to include comprehensive simulation results and comparisons.

Another low-complexity CPF scheme is given in [93]. The outage probability of the proposed model is derived and compared with the standard CPF scheme in the study. Additionally, the channel estimation error (CEE) is introduced to the system and its effect is investigated. The results showed that the proposed simple method is also more

resistant to the CEE than the traditional CPF. In [94], authors extend their scope and propose two CPF based methods. The first method is designed to lower the required computation load while the latter shows better performance compared to the traditional CPF which is verified via simulations.

The complexity of the coefficient selection of the CPF is considered in [78–80, 95]. The writers propose a low-complexity algorithm to optimize the integer coefficients that are essential for the CPF performance in [95]. This work is later improved and generalized to cover CPF and integer-forcing algorithms in [96]. The same problem is studied in [78, 79]. An exhaustive search algorithm and a lattice reduction algorithm is proposed in [78, 79] to reduce the hardness of the coefficient selection problem. Also in [80], a low-complexity coefficient method is proposed for the massive MIMO enabled CPF networks.

The effect of the channel estimation error to the performance of the CPF scheme is analyzed in [57]. The computation rate region for the imperfect channel estimation case is derived and the expression is closely approximated for the Gaussian distributed channel estimation error. Additionally, the distribution of the rate loss is given in the closed-form. The simulations are used to demonstrate the vulnerability of the CPF to the CEE.

The traditional CPF requires CSI to decide the appropriate scale factors which are essential in the decoding of the integer lattices. Otherwise, the non-integer channel coefficients increase the symbol error. In [70, 71], a practical CPF scheme is proposed that does not require the CSI to compute the most suitable scale factors. Instead, the proposed method chooses sub-optimal however sufficient scaling factors to gain from the system complexity. The simulations show that in some cases, the computation complexity can be reduced ten times compared to the CPF of [6].

The synchronisation problem of the CPF is evaluated in [72]. The CPF networks can exhibit synchronization of the nodes as a result of the decentralized node structure of the network. The study proposes a solution to the symbol synchronization problem with an equalizer by converting the nature of the network from asynchronous to synchronous. The frame synchronization is solved by eliminating the delays with

multiple antennas at the relay node. Also, it is shown that the achievable rate can be maximized for all SNR regions by applying a linear filter.

A phase precoding method for the CPF scheme is proposed in [73] for multi-user multi-relay networks. The objective of the method is to reach higher computation rates than the traditional CPF, however it requires an optimal precoding matrix and an optimal network equation matrix to fulfill that objective. For this reason, the study introduces a partial feedback channel between the relays and the nodes since the precoding matrix is needed at the nodes and the network equation matrix has to be computed at the relays. The relays compute the optimal precoder and the network equations, then forward the precoder information to the nodes through the feedback channel. With the simulations, the study shows that the proposed phase precoding can improve the equation error rate.

Another feedback enabled CPF method is given in [58]. The method aims to design the optimal CPF model to achieve the maximum computation rates for the scenario that transmitters have access to an ideal feedback channel towards the relay. The method is designed for two users (and a relay) networks and it is demonstrated that the proposed scheme attains better computation rates than the CPF without feedback.

The CPF is considered for the Gaussian multi-user interference channels in [45]. A comprehensive study is given on the approximate sum capacity and the capacity bounds. In [52], the CPF is investigated for the discrete memoryless channels. The lattice codes are considered for the complex modulo arithmetics in [97]. It is shown that only five lattice code families are capable of complex modulo arithmetics over the Euclidean geometry and their coding gains are calculated. In [43], the CPF scheme is considered for the Cloud-Radio Access Networks. The study aims to maximize the information flow from the nodes to the FC of the network. For this reason, a coalition game is designed that maximizes the defined profits. Exploiting the interference of signals is considered for the fifth generation ($5G$) networks in [76]. The objective is to provide channel access to a massive number of nodes that are required by the IoT. For this purpose, the study combines the PLNC with the pulse shaped OFDM.

In [65], an Low Density Lattice Codes (LDLC) based CPF method is proposed in order to reach high coding gains. In [74], the writers propose a sphere decoding

method to maximize the computation rate by considering the problem in hand as an Shortest Vector Problem (SVP). The sumsets can be defined in simple terms as the set of received lattice points which is the sum of the transmitted lattice points. In [77], the typical sumsets are defined and analyzed for their size, distribution, and density. The study aims to obtain results that can improve the performance of the lattice decoding in the CPF.

Cooperation between the transmitters is considered in [75]. In this study, the meaning of cooperation differentiates from the cooperative networks that are given in Fig. 3.1d. Here, the nodes can partially hear the messages of the other nodes which resembles the diversity improvement of a multiple antenna network. The results reveal that the partial cooperation between the nodes can increase the computation rate almost to the capacity.

In [98], a CPF Transform is proposed in which the W-MAC is transformed to a modulo-lattice MIMO channel with the help of SIC. Joint typicality decoders are adopted to the CPF method in [53–56]. The CPF is also considered for random access channels in [81, 82, 99]. The impact of the input distribution to the computation rate of the CPF is considered in [46] for the Gaussian W-MAC. It is shown that the Gaussian input distribution is not optimal and the computation rates can be improved if the input distribution is wisely chosen. In [51], the CPF is extended to cognitive radio networks.

Network coding algorithms can be viewed as a composite function between the initial sources and the final destination. The inputs and the outputs of this function are the data of the initial sources. However, the relays only obtain a function of the transmitted data rather than the individual source information. In the following Chapter, function computation studies are presented. These studies are only interested in transferring a function of the data instead of reconstructing the individual data.

4. FUNCTION COMPUTATION

Function computation is one of the most striking applications of simultaneous transmission. The joint source-channel coding paradigm by Gastpar and Vetterli [3] and later Nazer and Gastpar [5] establish the basis for the function computation. This approach inspires a wide range of studies that often targets one of the two main aspects; computation or multiple access. The motivation behind the studies that focus on the multiple access aspect is generally to improve the network throughput as in CPF and considered in Chapter 3. Here, the studies that focus on the computation aspect as the digital function computation is given. The computation aspect later inspires the analog studies that purely focus on function computation. The motivation behind these studies is strictly computation related and presented as the analog function computation [7].

4.1 Digital Function Computation

A summary of the digital function computation studies is given in Table 4.1. Computation codes are the first examples that enable digital function computation. The computation codes are, inspired by lattices, proposed by Nazer and Gastpar in [5]. The objective of this study is to send a linear function of multiple users to a receiver with the simultaneous transmission. The study investigates the achievable rates with the proposed computation codes and compares them with the separation based methods. Computation of linear functions is also considered in [100] for a wireless network that consists of two correlated Gaussian sources. The paper investigates the optimum scheme that upper bounds the received signal distortion. The numerical results are given for the subtraction ($a-b$) and weighted addition ($a+2b$) functions as a function of the correlation coefficient of the two sources.

Golden Baum *et al* generalize the digital computation of nomographic functions with nested lattice codes in [105]. The model is based on the fact that the nomographic functions can be written in the form of *pre* and *post* processing functions as studied in the analog function computation studies. However, writers adopt a digital model

Table 4.1 : Digital function computation studies.

Author	Year	Network model	Contribution	Performance metric
Jeon *et al* [101, 102]	2013, 2014	$K \times L \times 1$	Extends the lattice code computable function set by considering orthogonal components and derives an approximation of computation capacity	Computation rate
Wu *et al* [103, 104]	2015, 2016		Proposes a low-bandwidth, low-energy SDR network architecture, STAC	SER, session rate
Nazer and Gastper [5]	2007	$K \times 1$	Proposes the computation codes and the CoMAC which enhance the communication performance by utilizing lattice codes and the joint source-channel coding	Computation rate
Goldenbaum *et al* [105, 106]	2013, 2015		Improves the reliability of nomographic function computation by adapting lattice codes to AFC based consensus methods	
Jeon and Jung [107, 108]	2015, 2016		Provides non-vanishing computation rates (asymptotically positive) by allowing only a subset of nodes with high gains to transmit	
Wu *et al* [109–112]	2019		Considers the wide-band implementation of CoMAC by allocating sub-functions to subcarriers	
Soundararajan and Vishwanath [100]	2012	2×1	Derives a lower bound on the distortion of CoMAC and considers correlated source scenario	Distortion rate
Zhan *et al* [113]	2011	Butterfly	Investigates the duality between computation and communication aspect of simultaneous transmission schemes	Distortion level
Zhu *et al* [114, 115]	2017, 2019	2×2		Capacity region

to reduce the destructive effects of the noise. The study also examines the required number of channel uses and the accuracy performance of the system. Lattice codes are used in [106] for the computation of nomographic functions. The study thoroughly analyzes the relation between the lattice codes and the nomographic functions and derive the computation rate performances. One of their results reveals that any continuous function can be computed over the channel.

In [101, 102], writers include orthogonal components to their coding scheme in a similar manner that the TBMA benefits from the orthogonal signals. The method is interested in calculating the arithmetic summation and the type functions. The type function computes the histogram of the transmitted signals as explained in TBMA. Then the resulting statistics can be used to obtain the mean, variance, maximum, minimum, and median functions. The W-MAC is firstly decomposed into multiple modulo sum subchannels with nested lattice codes and linear network codes. Then the linear Slepian–Wolf source coding is used to calculate the desired functions. It is shown that the joint source-channel coding provides better performance than the separate coding schemes in certain cases.

Simultaneous Transmitting and Air Computing (STAC) method is proposed in [103] and [104] to improve the function computation capability and the network efficiency of the data center networks. The proposed method is based on a traditional function

computation model that combines communication and computation. However, the model is also developed upon an enhanced SDR structure that provides side information to the nodes. Computer simulations demonstrate the spectrum and energy efficiency of the STAC in the data center networks.

Function computation problem is considered for the fading MACs in [107, 108]. The main idea behind the study is that only the nodes with high channel gains participate in the in-network computation rather than the whole network. The study investigates the computation rates of the proposed model for the fading channels.

A duality between the function computation problem and the multicast problem is considered in [113]. The function computation problem is interested in receiving a function (e.g. summation) of the transmitted messages. In the multicast problem, the objective is to receive individual messages. After defining the duality relation for the deterministic networks, Gaussian MACs are considered. The achievable distortion levels are derived for the summation of two Gaussian sources in these networks. The results revealed that there is a constant gap between the cut-set bound and the distortion of the summation function of the independent Gaussian sources.

It is obvious that the superposition of the signals destroys the individual information of the transmitted messages. This can be interpreted as renouncing the capability of accessing to the receiver [114, 115]. However, computation codes benefit from this idea to improve the efficiency of the computations in the network. Here, access to the individual information is traded with improved computation efficiency and this can be highly beneficial if the network only requires a function of the transmitted signal. In other words, computation codes present a duality between the multiple access and computation. This duality is investigated in [114, 115] to check the existence of the computation codes that also allow the individual access to the receiver. The investigation results indicate that efficient computation codes prevent the individual access to the receiver.

The wideband Computation over Multiple Access Channels (CoMAC) schemes that is adopted for the frequency selective channels are proposed in [109–112]. These studies rely on the Non Orthogonal Multiple Access (NOMA) and Orthogonal Frequency Division Multiplexing (OFDM) models to use wideband frequencies. A

NOMA assisted function computation network is proposed in [109, 110]. As given in the following sections, NOMA is a multiple access method that is based on the superposition of signals. In [109], functions to be computed are intentionally divided into sub-functions and these sub-functions are computed simultaneously under different NOMA access slots. As a result, the computations can be made at the wideband frequencies where the fading is more challenging. The results reveal that the proposed NOMA assisted approach achieves higher computation rates and prevents vanishing computation. Additionally, expressions for the diversity order is obtained in [110]. In [111, 112], the sub-functions are allocated to the Orthogonal Frequency Division Multiplexing (OFDM) carriers and an optimization problem is considered for the power allocation.

4.2 Analog Function Computation (AFC)

The main idea behind the Analog Function Computation (AFC) is to match the W-MAC with desired functions. The superposition property of the W-MAC is a natural summation operation and the AFC aims to adjust the channel with proper signal processing at the transmitter and receiver ends. For this purpose, transmitters use *pre*-processing functions, $\varphi_k(.) : \mathbb{R} \to \mathbb{R}$, before transmitting their signals and the receiver applies a post processing function after receiving the superpositioned signal. This channel matching mechanism is illustrated in Fig. 4.1. The users simultaneously transmit their pre processed signals and the receiver obtains the following function output after the post process,

$$f(s_1, s_2, ..., s_K) = \psi\left(\sum_{k=1}^{K} \varphi_i(s_k)\right). \tag{4.1}$$

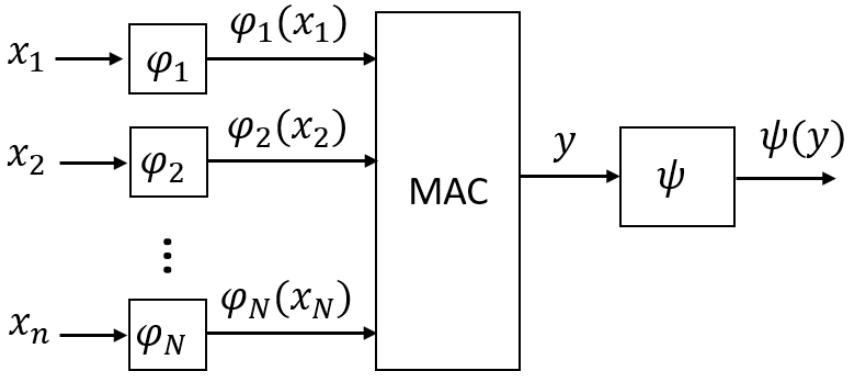


Figure 4.1 : Analog Function Computation (AFC) network model.

The functions that can be obtained by matching the summation operation is called nomographic functions. AFC was firstly proposed to compute nomographic functions, later it is proven that any function can be represented with nomographic functions and computed with AFC [7].

A collection of the AFC studies is given in Table 4.2. Goldenbaum and Stańczak are the pioneers of the studies that computes mathematical functions in the communication process. In [116], the communication system carries the information at the transmit powers which relieves the synchronization burden. Their method manages to compute a variety of functions which involve nonlinear functions. Writers lastly exhibit the error analysis of the arithmetic mean function. In [117], Goldenbaum and Stańczak extend their previous work by analyzing the geometric mean function. They also compare their method with TDMA via simulations and present their results that AFC outperforms the TDMA on the function computation time.

In their following works, Goldenbaum and Stańczak provide an extensive theory of Analog Function Computation in [7, 118]. They analyze the function sets and network topologies that are compatible with AFC. Their results show that every function can be computed with AFC as the *pre*-processing is independent of the computed function.

The error performance of the estimators that are used in the receivers of AFC is analyzed in [119] for arithmetic and geometric mean functions. Additionally, function computation simulations are performed for AFC, TDMA and CDMA models. The results showed that the AFC brings out better computation accuracy in less required time than time or code divided networks.

Dependency of the AFC to channel state information is investigated in [120]. The letter firstly shows that the transmitters only need the magnitude of the CSI rather than the full CSI. Then it is proven that any CSI knowledge requirement on the transmitters can be removed if the receiver is equipped with multiple antennas.

The computation of the l_p-norms with the AFC is investigated in [124]. The writers later propose an algorithm to approximate certain continuous multivariate functions by the nomographic function in [136]. In [78], the max function which aims to obtain the maximum value at the FC is implemented with the AFC and CDMA.

Table 4.2 : Analog Function Computation (AFC) studies.

Author	Year	Contribution	Performance metric
Goldenbaum *et al* [116]	2009	Computes functions (e.g. arithmetic mean) over the channel with low-complexity and low-energy consumption	Outage probability
Goldenbaum and Stańczak [117]	2010	Extends [116] to investigate the geometric mean	
Stańczak *et al* [118, 119]	2012,3	Provides a complete theory of AFC	
Goldenbaum and Stańczak [120]	2014	Investigates the AFC for different CSI assumptions	
Jeon and Jung [121]	2018	Improves the traditional AFC against fading environment by utilizing causal CSI	
Chen *et al* [122]	2018	Extends [123], considers the computation of multiple functions and investigates the method's performance	
Goldenbaum *et al* [7]	2013	Investigates and generalizes the functions that is computable with AFC	MSE
Limmer and Stańczak [124]	2014	Investigates the computation of l_p-norm functions with AFC	
Huang *et al* [125]	2015	Extends AFC to MIMO networks and includes imperfect CSI	
Zhu *et al* [126, 127]	2018	Introduces a multi-modal AirComp technique with MIMO and beamforming that minimizes distortion	
Farajzadeh *et al* [128]	2020	Removes the CSI requirement of AirComp	
Wen *et al* [129]	2019	Provides low-complexity and low-latency with MIMO AirComp	
Ang *et al* [130, 131]	2019	Reduce the complexity of the training process in massive CSI acquisition	
Li *et al* [132, 133]	2018,9	Considers an AirComp method that transfers power to the distributed nodes over the air to relax energy constraints	
Cao *et al* [134]	2019	Considers joint optimization of the transmit powers and the denoising factor to improve AirComp	
Basaran *et al* [135]	2020	Provides an energy efficient AirComp method by exploiting the correlation between the measurements	
Chen *et al* [123]	2018	Considers non-uniform fading scenario in the proposed AirComp method and brings robustness with the uniform-forcing transceiver design	
Limmer *et al* [136]	2015	Provides a method that computes certain multivariate functions with nomographic function approximation	Approximation error
Goldenbaum *et al* [137]	2015	Adapts computation codes to AFC to provide reliability and investigate its rates	Computation rate
Wang *et al* [138]	2015	Without channel estimation, reduces the required number of channel uses on the computation of mean function with free deconvolution	Relative error
Dong *et al* [139]	2020	Uses Wirtinger flow to provide a low-complexity, low-latency AirComp method that requires no CSI)	
Chen *et al* [140]	2019	Investigates and compares the computation based and communication based methods	Function rate
Jakimovski *et al* [141]	2011	Provides a testbed implementation	Average error
Sigg *et al* [142]	2012		Mean error
Kortke *et al* [143]	2014		Relative error
Abari *et al* [144]	2015		CFO
Altun *et al* [145]	2017		MSE

In [137], Goldenbaum and Stańczak investigate the relation between the reliability and efficiency of an AFC model from an information-theoretic point of view. The achievable computation rates are given for linear combination and special polynomial functions. The letter states that the computation rate is dependant on the required accuracy level and the number of transmitters as well as the function type.

An AFC method based on the free deconvolution theorem (see [146] for the further information on the free deconvolution) is proposed in [138]. The contribution of the study is that the mean function can be computed with fewer channel uses and without the channel estimation.

In [125], a MIMO AFC model is proposed that the FC and the multiples transmitting nodes are equipped with multiple antennas. The method allows channel estimation errors in the system model to consider realistic scenarios and design a non-convex optimization problem to achieve the optimum solution in this scenario. The optimization problem that minimizes the worst-case MSE is converted to a simpler version and solved.

In [126], a function computation method that can compute functions for multiple variables is proposed. For example, multi-model sensor measurements such as temperature, humidity, and pollution can be computed over the air simultaneously. This is possible with the utilization of beamforming technology over MIMO enabled nodes. The study aims to reduce the sum mean-squared error. The optimization problem is shown to be an NP-hard problem and an approximate version is solved with differential geometry. Also, the result of the optimization problem (based on Grassmann Manifold) is validated with computer simulations. This work is later extended to high-mobility sensing networks where an environment is monitored by unmanned aerial vehicles (UAV) [127]. In addition to [126], the study includes enhanced equalization and channel feedback methods to provide reliable information exchange between the sensors and the receiver.

Non-uniform fading in different nodes of an AFC network is a performance degrading problem. A transceiver design is proposed in [123] to mitigate the effects of fading that is not uniformly distributed.. The authors formulate a similar optimization problem as in [126]. Their results show that a semidefinite relaxation is necessary to solve the problem and successive convex approximation can further increase the accuracy of the solution. The proposed transceiver model in [123] is extended in [122] to compute multiple functions simultaneously. The nodes in the new network model are equipped with antenna arrays and zero-forcing beamforming technology. Beamforming technology is adopted to remove the interference of other functions that are computed simultaneously and multiple antenna arrays relieve the massive CSI knowledge requirement. Also as in [123], the method is resilient to the non-uniform fading problem. The performance of the proposed network is analyzed with both simulations and analytical expressions.

Another beamforming and MIMO enabled function computation method is given in [129]. The study proposes a receiver beamforming model design that reduces channel dimensions and equalizes channel covariances and small scale fading components. Additionally, the method uses a feedback scheme to accurately provide massive CSI knowledge to the network. The proposed approach mainly aims to reduce the computation error resulting from the discrepancy of the received function output. The simulations demonstrate the positive effect of the proposed model on error reduction.

A training model for the faster acquisition of the CSI is proposed in [130, 131]. The method is based on the effective CSI definition that is obtained with the simultaneous pilot transmission of the nodes. The method requires iterative broadcasts from FC to estimate the effective CSI and one last simultaneous transmission of pilots yield the CSI vector at the FC while the traditional AFC methods individually train each CSI. The study analytically obtains the computation complexity of both traditional and proposed methods. Also, an error improvement method is proposed to compensate for the larger estimation error of the novel approach.

Function computation is integrated with wireless power transfer in [132] for IoT networks. The framework aims to minimize the computation error that is seen at the aggregated data by jointly optimizing power transfer and function computation tasks. The framework is designed for networks that consist of MIMO beamforming capable nodes. The joint optimization problem in hand divided into two sections; wireless power control optimization and function computation optimization. As applied earlier in [123], the semidefinite relaxation method is implemented to solve the function computation section of the optimization problem while the wireless power control section is solved in closed form. The study also states that the integration of the wireless power transfer into the AFC network brings an additional design dimension which can increase the computation accuracy. A combination of function computation and wireless power transfer is also implemented for high-mobility sensing in smart cities where unmanned aerial vehicles are used to collect sensor readings [133].

Power control problem of the AFC systems are considered in [134]. Poor distribution of transmit powers in an AFC network can cause high computation errors as a result of channel distortion. The proposed method aims to find the optimum transmit power level design by solving the optimization problem that minimizes the computation error

at the FC. The definition of the problem involves the optimization of both transmit powers and the denoising factor of the FC. Moreover, the problem is solved for additional scenarios such as only one transmitter has power constraints instead of all devices. Lastly, the simulations reveal that the proposed power control scheme has a notable mitigating effect on the computation error of the AFC network.

The problem of energy consumption in function computation networks is considered in [135]. The method mainly benefits from the spatial correlations between the sensor readings to reduce energy consumption. For this purpose, a minimum mean square error (MMSE) estimator is designed to obtain estimations with less number of samples. The proposed estimator requires significantly less energy consumption to work, hence nearly doubles the lifetime of the network. In addition to the improved energy efficiency, the estimator also yields better MSE performance compared to the traditional methods as illustrated via simulations.

Wirtinger flow is an algorithm that is usually used in the solution of non-convex optimization problems such as phase retrieval from the received signal magnitudes. Dong *et al* use the Wirtinger flow method optimize the function computation without the knowledge of CSI in [139]. The proposed algorithm only requires data samples and randomly initialized Wirtinger flow iterations to reach a convex are in the optimization problem. As a result, the study can further reduce the latency of the function computation applications by removing the dependency on the pilot transmission process of the CSI estimation. Also, the study reveals that the estimation error of the Wirtinger flow-based function computation model is sufficiently small.

The power alignment is usually performed with *pre*-processing or precoding in traditional function computation networks. In [128], this problem is addresses with a backscatter framework instead of precoding. The proposed method is designed for mass density sensor networks where multiple UAVs are responsible for the collection of sensor measurements from their assigned area of nodes. The model consists of two phases; channel gain acquisition and data aggregation. In the first phase, the UAVs are the power emitters and the sensor nodes act as the backscattered object in which the nodes backscatter the ambient signal that comes from the UAV. As a result, the UAV collects the sum channel gain. In the second phase, the UAVs are the readers that

receive the aggregated sensor data. The results show that using the sum channel gain for the aggregation of the sensor readings can improve up to 10 dB MSE.

The function computation capability of the AFC is compared with the separate communication schemes in [140]. The achievable rates are obtained for the two cases and it is shown via simulations that the computation over the channel (AFC) is not always the optimum scenario for the function computation.

4.2.1 Test-bed implementations

The feasibility of the AFC is also investigated with testbed implementations in the literature. In [143], writers realise the model of [119] with SDRs. A network with 11 nodes and an FC is implemented to compute the arithmetic and geometric mean of the sensor readings of the nodes. In another implementation study [145], the summation of sensor readings over the channel is tested via software defined radio modules. The network that includes three transmitters and an FC is used to analyze the effect of distance and signal power level. Also, the error performance of the AFC network is compared with the TDMA scheme via computer simulations. The TDMA scheme requires communication slots for each node while the AFC completes the transmission in one slot. As a result, the simulation results of AFC displays less error since TDMA adds thermal noise to the system with each communication.

In [141], a simultaneous transmission method is proposed and implemented with software defined radio modules. The method is based on the hamming distance of the superimposed received signals that are affected by each transmit vector. The calculation of corrupted goods in a pallet via temperature readings is suggested as an example of an application. The testbed implementation of this system demonstrated the feasibility of the method and the success of computations over the channel. Another implementation study is given by Sigg *et al* in [142]. They suggested a computation model that carries information in the mean of Poisson distributions. Users transmit burst sequences that are Poisson distributed and the density of the bursts in a time interval represents the mean of the distribution. The model then extracts the mean value of the superimposed signal at the receiver. The proposed model is implemented with 15 sensor nodes and a receiver that is driven by microcontrollers. The realized scenario

successfully recovered the average temperature of the simultaneously transmitted sensor readings.

AirShare method is presented in [144] to improve the resistance of the distributed wireless applications against carrier frequency offset (CFO). The method uses a broadcast clock signal as a reference to other nodes that aim to transmit simultaneously. The paper firstly investigates the feasibility of the AirShare method and then implements the network via software defined radio modules.

Function computation studies focus on matching the channel with desired functions. These studies consider the general bounds and the set of functions that is possible with simultaneous transmission. Detection and estimation studies, on the other hand, focus on particular functions that take observation samples as input and statistics of these samples as output. These functions are used in detection, estimation and spectrum sensing algorithms and presented in the following Chapter.

5. DETECTION AND ESTIMATION

Detectors and estimators are essential parts of many engineering applications and their performance profoundly affects the performance of a system. While the detection and estimation theory is concerned with the optimal design of the decision mechanisms, the acquisition of the samples is another important parameter for the whole system. In general, larger sample sizes produce better decision performance, on the other hand, it requires more energy consumption and long computation times. For this reason, the response of the decision performance to the sample size is an important aspect to consider. The error exponent is a measure that indicates how fast the error changes with the increasing sample size and often used in the analysis of asymptotic behavior of the sample size. This aspect is particularly important in the IoT applications that can involve massive sensor networks in which the observations from multiple sensors create the sample set togetherly. For this reason, distributed detection and estimation strategies are developed to improve the performance of this process. In this chapter, distributed detection and estimation studies and the spectrum sensing studies are presented.

5.1 Detection

A selection of the simultaneous transmission-based detection studies is given in Table 5.1. As one of the first examples, the distributed detection problem of the wireless networks is considered in [147]. The network consists of spatially distributed sensors that aim to transfer the statistics of the sensor measurements to the FC. The method exploits the superposition of property of the W-MAC for this purpose by simultaneously transmitting their statistics. The study examines the detection performance of the proposed method from the perspective of the number of measurements and power consumption. Two sensor types are considered for the review; intelligent and dumb. The intelligent sensors are aware of the source statistics and transfers the log-likelihood ratio (LLR) to the FC. It is shown that the LLR based

detection is asymptotically optimal (i.e. can reach the performance of the centralized detection). The dumb sensors are unaware of the source statistics and transfer the histogram of their measurements to the FC, however, source statistics is required at the FC. The results show that the histogram transfer is also asymptotically optimal. The results are also verified with simulations that show the detection error as a function of the number of sensors.

Sensor measurements of a wireless sensor network are used for target detection in [18]. The sensor measurements are transferred to the test center via Type-Based Multiple Access. In TBMA, the receiver only accesses to the histogram of the transmitted data (see Section 2 for detailed information) and the detection mechanism is based on the histogram of the observations. The study focuses on the performance analyses of the TBMA based detection schemes (includes a large deviations approach). An asymptotically optimal detection mechanism is proposed and its detection error exponents are derived. Channels with ideally and not ideally distributed gains are considered. Also, the error probabilities of the TBMA scheme is compared with the Time Division Multiple Access (TDMA) via simulations.

Table 5.1 : Detection studies.

Author	Year	Contribution	Performance metric
Liu and Sayeed [147]	2007	A low-complexity distributed detection mechanism (based on type function) is proposed and investigated for the error exponent	Error probability
Mergen *et al* [18]	2007	Provides an asymptotically optimal detector and analyzes its error exponent performance	Error exponent
Li and Dai [148]	2007	Proposes a bandwidth and delay efficient method and compares with the separation based methods	
Li *et al* [149]	2011	Analyzes and compares the MDF and the MAF methods for error exponents under power constraints	
Banavar *et al* [150]	2012	Includes multiple antenna receivers and investigates different CSI scenarios	
Ralinovski *et al* [151]	2016	The anomaly detection method reduces the communication costs (energy, bandwidth) and investigate relation between accuracy and communication costs	Reliability, energy consumption
Raceala-Motoc *et al* [152]	2018	Gives the upper-bounds for the probability of mislabeling for [151]	Probability of mislabeling

In [148], the existence of a signal is checked with a binary hypothesis test where the observation samples are obtained from a decentralized sensor network. The sensor readings are collected in the FC via two-channel models; each sensor has its own dedicated channel or a single channel is dedicated to all sensors. The second model that dedicates a single channel to the sensors attracts allows the superposition of signals. The study focuses on the detection performance of these two-channel models and their

comparison with the centralized detection model. In the analyses, two Gaussian noise cases (correlated and independent) and two power constraint cases (average and total) are considered. Bayesian error exponents of the detection probabilities are derived for these scenarios (includes large deviations approach). Several results are shown in the study and verified via simulations that examine the effect of the number of sensors on the detection error probability and error exponent. The result for the average power constraint case is that the superimposed signals with the correlated Gaussian noise can reach the error performance of the centralized detection scenario; however, dedicating channels to each sensor always leads to error performance reductions. For the total power constraint case, an increasing number of sensors exponentially reduces the error exponent for the superimposed signals.

Two superposition based schemes are proposed in [149] for the distributed signal detection via binary hypothesis testing. The Modified Detect and Forward (MDF) scheme considers the signal detection at each distributed node and transfers the test results to the FC. The second scheme, Modified Amplify and Forward (MAF), transfers the observations to the FC before the hypothesis testing. The study examines the detection performance of these schemes under individual power constraint and total power constraint. The results show that the MAF is asymptotically (e.g. infinite number of sensors) optimal under the individual power constraint, whereas MDF is not.

In [150], multiple antennas at the FC is considered for the distributed detection problem. The error exponent is is investigated for the scenarios; AWGN and Rayleigh channels, full CSI, and phase-only CSI constraints at the sensors. It is shown that equipping the FC with multiple antennas presents a gain of $\pi/8$ for the scenario of Rayleigh channel and full CSI. Four algorithms are proposed for the design of the sensors' power allocation. Lastly, the error exponents of these algorithms are compared with the derived bounds via simulations.

An anomaly detection algorithm is proposed in [151] which is based on the AFC given in [119]. A supervised learning algorithm is used for the hypothesis testing and the classifier of the algorithm is generated at the FC with the sensor readings. Since the FC is only interested in a function of the sensor readings, the AFC is proposed for the classifier generation over the channel. The main contribution of the study is

energy efficiency and it is shown that the proposed scheme can significantly reduce the consumed energy compared to the TDMA scheme. Later, in [152], the previous study on anomaly detection is extended to include the upper bounds on the probability of mislabeling.

5.2 Estimation

A collection of estimation studies that use simultaneous transmission is presented in Table 5.2. The TBMA scheme given in [4] is the first method that is used for distributed estimation with simultaneous transmissions. The method benefits from the superposition of the sensor readings over the channel to gain from the bandwidth and the delay time. The study aims to design the optimum estimation process that includes the transfer of the samples to FC and the estimator. The study derives the Cramer-Rao bound of the estimation problem and designs the estimation process as the combination of TBMA and an ML detector. The results show that the TBMA based estimation is asymptotically optimal if the channel gains of all sensors are the same. Additionally, the proposed model is analyzed for the fading channels and compared with the TDMA based schemes via simulations.

Table 5.2 : Estimation studies.

Author	Year	Contribution	Performance metric
Mergen and Tong [4]	2006	Analyzes the asymptotic behaviour of TBMA based estimation	MSE
Xiao *et al* [153]	2008	Propose a bandwidth and power efficient method and , defines and solves an optimization problem for power scheduling	
Bajwa *et al* [154]	2007	Proposes a energy efficient joint source-channel based method and defines the relationship between its power consumption, error rate and latency	Power, distortion, scaling exponents
Wang and Yang [155]	2010	The method removes the CSI requirement by using more bandwidth	MSE, bandwidth
Banavar *et al* [156]	2010	Considers and investigates different fading models and their effect on the performance	Asymptotic variance

In [153], power and bandwidth limited networks are considered for the distributed estimation of unknown signals. The writers especially propose a power scheduling model and investigate the cases where the observations are scalar and vectorial. The optimization problem for power scheduling is shown to be convex and solved for the scalar observations. Additionally, it is shown via simulations that the proposed scheduling generates better MSE performance than the uniform scheduling. Optimal scenario to estimate the vectorial observations investigated for both noiseless and noisy channel models. The results for the noiseless channel model are given in closed

form; however, the solution of the optimization problem for the noisy channel required semidefinite relaxation methods.

A joint source-channel communication structure is considered for the distributed wireless sensor networks [154]. The objective is to build a communication infrastructure that reduces bandwidth and power consumption. For this purpose, optimization of the acquisition, communication, and processing of the measured data is considered collectively. The relationships between power consumption, error rate, and the latency of the network are derived for an increasing number of sensors and verified with simulations. It is shown that the efficient and healthy estimation of the unknown signals is possible for a large number of sensors if prior knowledge is allowed in the proposed approach. Moreover, the method still produces healthy estimation results with the power and latency constraints that are growing at most sublinearly with the number of sensors when partial or no prior knowledge is given.

A TBMA based estimation method is proposed in [155] for distributed WSNs. In traditional TBMA schemes; the fading of the wireless channel notably degrades the communication performance and providing CSI to each node via pilot transmission or feedback channel brings excessive burden for large sensor networks. The proposed method aims to provide robustness against these problems by partitioning additional bandwidth to the network. The main idea behind the model is to use multiple orthogonal waveforms for each message (type) where the traditional TBMA uses only one. The writers also designed a ML maximum likelihood estimator for the system and derived the Cramer-Rao lower bound expression. The simulations compare the MSE performance of the method with traditional TBMA and illustrate the relationship between the bandwidth, SNR and the number of nodes.

Fading characteristics of the channel and the amount of allowed CSI at the network is highly important for the performance of the distributed sensor networks that exploit the superposition of the signals. In [156], various fading models and different CSI amounts are tested for distributed estimation networks. The variance expression for the network's estimate is derived for the perfect and partial CSI cases. Also, different channel characteristics are considered and the corresponding variance expressions are derived for a large number of sensors. The study also includes the impact of the errors that occur at the feedback process in their evaluations. The convergence rates are

calculated for several scenarios. It is shown that the asymptotic results can be nearly reached with a practical number of sensor nodes. The results are also verified with computer simulations.

5.3 Spectrum Sensing

Supporting a high amount of users is one of the most important challenges of wireless communication since the frequency spectrum is limited. However, the distribution of the spectrum to the users is usually more challenging than the physical scarcity of the channel itself [157]. The cognitive radio is a delicate approach that aims to handle the spectrum access problem efficiently and it is designed to be aware of its surroundings with SDR capabilities, e.g. spectrum analysis or CSI estimation. The main objective of cognitive radio is to find the idle channels, that is dedicated to primary users, and utilize them to secondary users. The spectrum sensing problem is the first aspect of this objective and attracted distributed network solutions in the literature [158].

The spectrum sensing is a particular case of the detection problem (see Section 5) and involves certain network dynamics. A selection of the spectrum sensing studies is given in Table 5.3. In a distributed cognitive radio network, numerous nodes sense the spectrum and report back to an FC. A cooperative method that utilizes the simultaneous transmission for this problem is proposed in [159]. Instead of individual sensing, the method takes help from the decentralized nodes to detect the free frequency bands. The spectrum sensing mechanism is based on observed energy from the frequency channels. This energy information is carried simultaneously from the distributed nodes to the FC as encoded to the signal energies and the final decision is made at the FC. The detection probability and the false alarm probability of the proposed method are derived and used in order to optimize the detection performance. Also, the proposed scheme is compared with the traditional spectrum sensing methods with respect to the approximation error and network throughput via simulations. The writers later consider the energy efficiency of the spectrum sensing problem in [160]. For this reason, an optimization problem is derived that considers the sensing time, the detection threshold, and the symbol sequence length. The problem is simplified and solved and the results are verified with the simulations.

Table 5.3 : Spectrum sensing studies.

Author	Year	Contribution	Performance metric
Zheng *et al* [159]	2015	The method manages to transfer the sensing data in one time slot, analyze its detection and throughput performance	Approximation error, throughput
Zheng *et al* [160]	2017	Define an energy optimization problem and find the expression of optimal threshold	Energy efficiency, sensing time
Chen *et al* [161]	2018	Considers the effect of CFO in the sensing algorithm	Signal to aliasing and noise ratio

In [161], the proposed cognitive radio network focuses on the wideband spectrum. The objective of the method is to find the occupied wideband channels with low latency and high accuracy. The method utilizes a distributed network model to improve the sensing accuracy and benefits from the superposition of the signals to reduce the delay time. Specifically, the Discrete Fourier Transform (DFT) of the data is computed over the nodes and the air. The network is examined for the synchronization errors (e.g. synchronization phase offset) that occur between the nodes. Furthermore, a robust estimation and equalization technique is proposed to mitigate the effects of the imperfect synchronization. Lastly, theoretical investigations, simulations and SDR based implementations are conducted.

6. MISCELLANEOUS APPLICATIONS

Simultaneous transmission is extended to several other applications such as federated learning or computation alignment. This chapter is dedicated to the miscellaneous applications that present limited appearance in the literature.

6.1 Multiple Antenna

Multiple antenna techniques became beneficial in the communication networks as a result of the developments in both the antenna technology and the processing capacity. The MIMO structure is proven to improve the multiplexing capability of the single antenna networks as well as increasing their diversity gain [162]. The MIMO presents a unique case for the scope of this survey since the communication is between pairwise nodes, e.g. the antennas are controlled by the same source. The fundamental advantage of the MIMO is the diversity gain which results from the superposition of the signals that are transmitted from multiple antennas. As a result, MIMO networks exploit the superposition of signals to reduce the error rates or to improve the bit rates.

On the other hand, the conventional MIMO is an extensive topic and the superposition property is just a tool in the MIMO studies which leads to larger results [163]. Also, the connection between the MIMO and the superposition property can be better observed from the existing studies such as [164, 165]. Further reading on the MIMO can be found in [166] for its security applications and in [167] for its challenges and future. In addition to its conventional perspective, there also exists studies that exploit the superposition property in a unique way with multiple antennas. The integer-forcing receivers [168, 169] are an example of these studies and will be briefly explained in the following subsection.

6.1.1 Integer-forcing architecture

An effective channel matrix can be defined and used for the analysis of linear MIMO receivers. In the traditional sense, the effective channel matrix should be matched

with an identity matrix in order to recover the messages of each antenna. However, the integer-forcing receivers match the effective channel matrix with integer value matrices as proposed in [168]. Inspired by the CPF [6], the nested lattice codes are used for the communication in order to obtain functions with integer coefficients. After matching with integer values, the receiver can solve the effective channel matrix and obtain the messages.

The integer-forcing receiver is extended to mitigate external signal interference in [170]. In addition to the results given in [168] that the integer-forcing receivers obtain the inputs with integer coefficients, the writers later find in [170] that the integer values can be also controlled to mitigate the external interference by considering the interference space. The results show that the proposed receiver presents significant gain over the traditional linear MIMO receivers.

The SIC technique is adapted to the integer-forcing receivers in [171] as successive integer-forcing. The results indicate that the successive integer-forcing receiver can achieve the channel's sum capacity and outperform the traditional linear receivers with SIC in certain scenarios.

6.2 Interference / Computation / Function Alignment

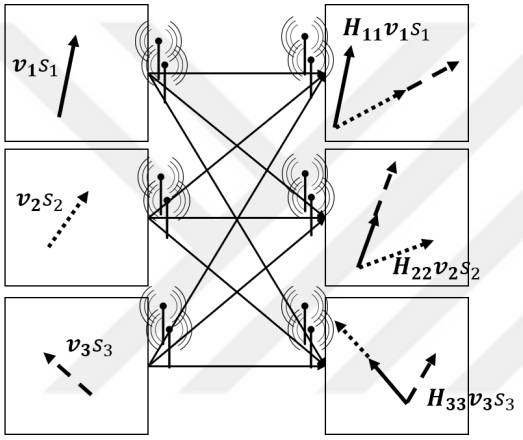
The interference alignment is an interference management technique and can be compared with the multiple access methods for their application purpose. The conventional multiple access methods divide the time, frequency, etc. resources to the users. In the IA, all users share the same resources, however, the IA algorithm affects the transmitted signals (a precoding) such that the received signals are aligned into two subspaces. As the algorithm aims, the unintended signals (the interference from the other users) fall under one subspace and the intended signal can be extracted from the other subspace. Although the traditional AI network model enables the interference, eventually it aims to discard the interference instead of benefiting from it.

On the other hand, the computation alignment method, inspired by the IA and the CPF, also benefits from the interference of signals. Similar to the IA, the computation alignment divides the signals into subspaces, however, the aligned signals are not discarded, instead, the interference is exploited for the computation. In this section,

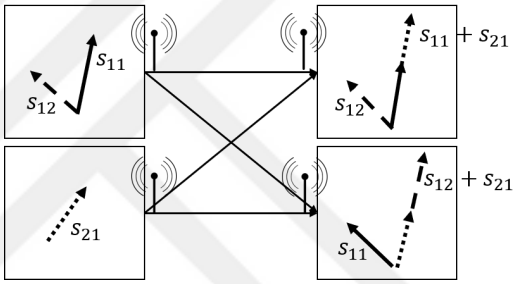
firstly an elementary description of the IA is given (see [172] and [173] for detailed information), later the computation and function alignment studies are presented.

The IA studies are mainly centered upon the space, frequency, or time dimensions to align the interference [172]. Here, a simple space dimension method (based on multiple antenna) is explained as an example. Consider a MIMO network that consists of three transmitters and three receivers all of which equipped with two antennas as shown in Fig. 6.1a. After the simultaneous transmission, the first receiver obtains the following signal,

$$\mathbf{y_1} = \mathbf{H_{11}}\mathbf{v_1}x_1 + \mathbf{H_{21}}\mathbf{v_2}x_2 + \mathbf{H_{31}}\mathbf{v_3}x_3 + \mathbf{n_1}. \tag{6.1}$$



(a) Interference Alignment [172]



(b) Computation Alignment [174]

Figure 6.1 : An illustration of the working mechanisms of IA and computation alignment methods.

The subscripts are used to indicate the users, $\mathbf{y_j}$ is the received signal of the j^{th} receiver, $\mathbf{H_{ij}}$ is the channel matrix from the i^{th} transmitter to the j^{th} receiver, $\mathbf{v_i}$ is the precoding of the i^{th} transmitter, x_i is the message of the i^{th} transmitter and the $\mathbf{n_j}$ is the Gaussian noise at the j^{th} receiver. The bold characters are two-element vectors that each raw corresponds to an antenna.

Assuming perfect CSI at the receivers, the MIMO algorithms require three antennas since each of the three users' inputs is an unknown variable. In the IA, the precoding vector ($\mathbf{v_i}$) elegantly aligns the two unknown vectors (the interference from the other users) such that (6.1) can be written with two unknown vectors. After that, the two unknown variables can be solved with the two equations. The vector representation of how the IA works is illustrated in Fig. 6.1a. Each node is represented with a square and the transmitted and received signals are given in the inside of these squares. The

precoding at the transmitter divides the three vectors (the number of users, can be more) into two subspaces; one of them is the intended vector and the other is the aligned (unintended) signals.

The perspective given above exploits the physical layer to suppress the interference. The computation alignment method is inspired from this perspective, however, it focuses on the unintended aligned vector for the function computation, which genuinely exploits the signal interference. A simple two transmitter two receiver network example of the computation alignment is given in Fig. 6.1b. In this example, the time dimension is used to create the subspaces. Assume that the first transmitter aims to send s_{11} and s_{12} while the second transmitter aims to sent s_{21}. In this scenario, the receivers obtain the following expressions,

$$\begin{aligned} \mathbf{y_1} &= \mathbf{H_{11}v_1}(s_{11}+s_{12}) + \mathbf{H_{21}v_2}(s_{21}) + \mathbf{n_1} \\ \mathbf{y_2} &= \mathbf{H_{12}v_1}(s_{11}+s_{12}) + \mathbf{H_{22}v_2}(s_{21}) + \mathbf{n_2}. \end{aligned} \tag{6.2}$$

where the subscripts indicate the users, $\mathbf{y_j}$ is the received signal of the j^{th} receiver, $\mathbf{H_{ij}}$ is the channel matrix from the i^{th} transmitter to the j^{th} receiver, $\mathbf{v_i}$ is the transmit vector of the i^{th} transmitter, s_{ij} is the message of the i^{th} transmitter and the $\mathbf{n_j}$ is the Gaussian noise at the j^{th} receiver. The network operates at two-time slots and each time slot is represented with a row of the matrices that are given with bold characters.

The design of the transmit vector enables the computation alignment. The vectorial illustration of the (6.2) is given in Fig. 6.1b. It should be noted that the illustration omits the representation of the transmit vectors and the channel gain vectors in the figure for better appearance. As a result of the computation alignment, the receivers obtain the summation of the messages in the aligned subspace. Specifically, the first receiver obtains $s_{11}+s_{21}$ aligned and s_{12} in the other subspace while the receiver two obtains $s_{12}+s_{21}$ and s_{11}.

A survey of the computation and function alignment methods is presented in Table 6.1. In a relay network, the CF method adds additional noise to the network in each layer. As a result, the approximation gap of the network capacity widens for the increasing number of network layers. The computation alignment scheme in [174] and [175] presents a relay network with an approximation gap that is independent of the layer depth. The computation alignment technique depends on the lattice codes and the CPF to be able to recover the integer-valued messages. However, the CPF scheme also

produce errors as a result of the non-integer channel gains. This problem is solved with the IA by partitioning the wireless channel into multiple sections and aligning. The results reveal that the approximation gap is not constant as opposed to CF results, it depends on the fading characteristics.

Table 6.1 : Ccomputation alignment and function alignment studies.

Author	Year	Network model	Contribution	Performance metric
Niesen *et al* [174, 175]	2011,3	$K \times K$	Provides a capacity approximation for multi-layer networks that is independent of network depth	Capacity approximation
Goela *et al* [176]	2012		Investigates coding schemes that reach computation capacity with network decomposition	Coding capacity
Suh *et al* [177, 178]	2012,6	2×2	Obtains the computing capacity bounds, propose a network decomposition theorem	Computing capacity
Suh and Gastpar [179]	2013		Considers feedback for function alignment	
Suh and Gastpar [180]	2013		Investigates the scenarios where network decomposition is optimal	Symmetric capacity

In [176], multiple transmitter multiple receiver summation networks are considered. The scalar and vectorial linear codes are investigated for these networks and it is stated that the computation alignment is essential to reach the computation capacity. For this purpose, the network is decomposed into sub-networks with the network equivalence theorems. Also, the linear coding capacity of the computation is derived for various channel parameters.

In the references [177, 178], 2×2 modulo-2 sum networks [1] are considered. The study is inspired by the IA and similar to the computation alignment given in [175], and named as the function alignment. A new upper bound is derived for the computing capacity of the two receiver CPF networks with linear codes in [177, 178]. Also, the studies define a network decomposition theorem to divide the network into elementary subnetworks. Using the theorem, the computing capacity is generalized for the N-transmitter N-receiver CPF networks. In [179], the writers extend their previous work, [177], to include feedback. The study derives the computing capacity of the feedback included system and compare it with the no-feedback schemes (as in [177]). It should be stated that network decomposition is crucial to create subnetworks. The writers also investigate the network decomposition and its importance in the CPF networks thoroughly in [180].

In [181], memoryless bivariate Gaussian sources are considered for a two-source one receiver network. The receiver aims to obtain the information of the two sources with

[1] In particular Avestimehr-Diggavi-Tse (ADT) network is considered.

the minimum distortion. In the paper, perfect causal feedback is assumed and the power-distortion relationship is investigated. The results are given as a function of the source correlation and SNR. Also, the sufficient and necessary conditions to reach the minimum distortion levels are derived. The study is later extended to two transmitter two receiver networks in [182].

6.3 Gossip and Consensus

The physical layer is generally exploited for many-to-one networks where an FC requires the message of multiple users ($K \times 1$). However, in consensus problems, all users in the network aim to agree upon a common value, e.g. average, which carries a much higher communication burden. Finding an efficient communication structure for the consensus problem that provides fast and reliable convergence, while requiring low-energy, is a challenging task [183]. Gossiping is a distributed form of consensus that the nodes locally communicate with their neighbors instead of sticking to a network-wide protocol. It has been shown that simultaneous transmission presents opportunities for the improvement of gossip and consensus algorithms. In this section, the consensus studies that exploit the wireless channel to provide energy and time efficiency are examined. A summary of the results can be found in Table 6.2.

Table 6.2 : Gossip and consensus studies.

Author	Year	Contribution	Performance metric
Kirti *et al* [184]	2007	Provides a scalable consensus algorithm that the convergence time is independent of the network size	MSE
Goldenbaum *et al* [185]	2012	The consensus of multiple nodes with respect to nomographic functions is established and analyzed	
Steffens and Pesavento [186]	2012	Provides a low-complexity and scalable consensus algorithm	
Nazer *et al* [187]	2009	Faster than the pairwise gossip and provides energy efficiency exponential to the network size	Number of gossip rounds
Nazer *et al* [188]	2011	Provides time and energy efficiency polynomial to the network size	
Nokleby *et al* [189]	2011	Based on full duplex communication and provides scalability to the network size	Averaging time
Molinari *et al* [190]	2018	Robust to fading and provides fast convergence	Convergence time
Agrawal *et al* [191]	2019	Provides robustness to noise and low SNR for max-consensus networks	Error rate, number of iterations

The average consensus problem of wireless networks is considered in [184]. The method exploits the physical layer with the simultaneous transmission in order to update the consensus algorithm. The results show that each node in the proposed network can obtain the average of the data under a sufficient MSE level. Since

the channel is accessed by the nodes simultaneously, the method presents better convergence performance compared to the conventional consensus algorithms as the number of nodes increase.

In [187], Nazer *et al* use the computation coding in a gossip algorithm that averages the sensor readings. The method is based on the simultaneous transmission of the nodes by exploiting the superposition property of the physical layer. The network is arbitrarily divided into local neighborhoods such that the average consensus is initially provided for each of them, later the global consensus is provided for the network. The results reveal that the energy efficiency of the network increases exponentially and the time efficiency increases polynomial as the number of nodes increase. In [188], the previous studies are extended and compared with the nearest neighborhood gossip algorithms via simulations. Also, it is shown that the proposed method converges in $O(n^2/m^2)$ rounds while the nearest neighborhood algorithm converges in $O(n^2)$ rounds where n and m are the network and local neighborhood sizes respectively.

The averaging gossip problem of a wireless network is extended to nomographic functions in [185]. The main idea behind the study is the analog computation of the nomographic consensus functions over the wireless channel with the concurrent transmission. The proposed model is cluster/neighborhood-based as in [187, 188] such that the consensus is initially provided for local clusters rather than the whole network. Different from the [187, 188], the global consensus is obtained with the existence of the common nodes which connect the clusters with each other. Two algorithms, deterministic and randomized, are proposed and shown that both of them significantly increases the convergence rate.

Another gossip algorithm that exploits the physical layer is proposed in [189]. The novelty of the study lies in the full-duplex communication model of the network which allows simultaneous transmission and reception of signals with special self-interference cancellation techniques. Each node in the network broadcasts to its neighbors and receives from them simultaneously and requires only synchronization. The theoretical results reveal that the gossip algorithm has a three times faster convergence rate compared to randomized gossip algorithms. Also, the study supports their theoretical results with computer simulations.

In [186], the average consensus of a wireless network is considered. Although many of the simultaneous transmission-based consensus algorithms are neighborhood/cluster-based (as in [185, 187, 188]), this study arbitrarily divides the network into two subgroups rather than many. In each iteration, all the nodes of a subgroup simultaneously broadcast their data while the nodes in the other subgroup receive the superimposed signal. After an iteration, the subgroups change roles such that the receiver subgroup becomes the transmitting subgroup and vice versa. The nodes in the transmitting subgroup create their new data as a weighted sum of the received signal and the original data. The proposed method offers energy efficiency and significant convergence performance as the simulations illustrate the comparison of the proposed method with the randomized and the broadcast gossip algorithms.

The superposition of the transmitted signals is also considered in [190]. The study uses similar grounds that are used in [185], however [190] also includes unknown channel coefficients in the design of the consensus method. Time variant and time-invariant cases are considered for the wireless channel model. A tuning parameter (a stubbornness index) is proposed to control the convergence rate. The results show that the smaller values of the tuning parameter (stubborn systems) reduce the effect of the time-variant channel coefficients and increase the convergence time. However, the tuning parameter only affects the convergence rate in the time-invariant systems. The study also verifies their results via simulations. A max consensus scheme (*ScalableMax*) is proposed in [191]. The method focuses on the dense networks where the nodes aims to find the maximum function. The main contribution of the proposed method is scalability. An error correction mechanism is added to increase the resilience to the low SNR region.

6.4 Federated Learning

Machine Learning (ML) is the rising technology of the last decade as a result of the increasing computational capabilities of the electronic devices (machines) (comprehensive information on the main contents of this section can be found in [192]). ML is based on the usage of massive data or data sets on the classification or prediction operations. Many aspects of a communication system such as modulation, demodulation, channel estimation, etc. can be considered as a classification or

prediction problem [193]. This observation brings out the relationship between ML and wireless communication. Although traditional communication systems use model-based solutions for their problems, ML based data-driven techniques have already started to show promising results in the wireless communication area [194]. In the following years, this relationship proved to be two ways such that the communication networks can also be beneficial in the learning area.

The data-driven nature of the ML requires the collection of massive data in centralized points before the learning process. However, data sources of today's technology are often at the wireless edges. As a result, collecting massive data from wireless devices to a center can cost a high amount of energy and bandwidth [195]. Collaborative machine learning or federated learning is a solution to the data collection problem which proposes the process of the data at the edge users or distributed centers instead of a local center [196, 197]. Superposition property of the wireless channel can further relieve some of the costs in the federated learning schemes by performing computations over the wireless channel. The summary of the federated learning studies is presented in Table 6.3.

Table 6.3 : Federated learning studies.

Author	Year	Contribution	Performance metric
Tran *et al* [196]	2019	The method provides a duality between learning time and energy efficiency	Time vs energy cost
Yang *et al* [197]		Overviews the existing federated learning studies and promotes its data aggregation aspect	Classification
Amiri and Gündüz [198]		Improve the error performance of [195] by compressing the gradient estimate	Accuracy
Amiri *et al* [199]		Removes the requirement on CSI for the distributed ML method	
Zhu *et al* [200]		The method is for broadband communications and reduces latency as well as promoting a trade-off between communication and learning performance	
Yang *et al* [201]		Reduces the convergence rate of the learning algorithm by considering device selection and beamforming	
Amiri and Gündüz [195, 202, 203]	2019,20	Analog and digital DSGD reduce the learning time in bandwidth and energy limited networks	

One fundamental example of this paradigm is given by Amiri and Gündüz [195, 202, 203]. The learning algorithm is based on the minimization of a loss function which is solved with the Distributed Stochastic Gradient Descent (DSGD) method. In this method, the learning parameters are updated with multiple iterations. Different from the traditional collaborative ML that uses DSGD, this study exploits the wireless channel for the parameter update. In other words, the function that updates the learning parameters are calculated over the air as a result of the superposition property. Two

models, digital and analog, are proposed to reduce the required number of iterations to reach an accuracy level. Simulations show that the analog model requires fewer iterations, hence saves both energy and bandwidth of the system.

In the following study [198], Amiri and Gündüz extend their previous model to fading channels. Writers propose the *compressed worker-wise scheduled analog DSGD* model in which the edge users accumulate the error from previous iterations and reduce the dimension of their transmit vector. The proposed model is also compared with the model of another study that does not reduce the transmit vector (without scheduling) and the results show that the *compressed worker-wise scheduled analog DSGD* model increases accuracy. In [199], writers remove the CSI knowledge assumption on the transmitters. Instead, the receiver is equipped with multiple antennas. Results show that the increasing number of antennas alleviate the destructiveness of the wireless channel such that the infinite antennas result in totally removed fading and noise.

Zhu *et al* takes the same approach on federated learning in [200]; error function is minimized with each iteration and the iterations are calculated over the air. Additional to other studies, tree performance metrics are defined to analyze the network performance and the relations between them are obtained in closed forms. Also, the network is implemented to compare the proposed model with OFDM. The results confirm the relations between the defined metrics and show the low latency contribution of the proposed method.

Yang *et al* considers the same approach which relies on the over-the-air computation in [201]. The study includes user selection as in [198] which schedules the users according to their channel state. As an addition, [201] considers the usage of beamforming to improve learning performance. Also, they define the optimization problems that govern the performance of the device selection model. Then, they proposed a method to approach the optimization problem.

7. SECURITY

Simultaneous transmission is also considered in security applications. The majority of these studies are either derived from the CPF and the lattice codes or investigated the security performance of an existing structure. Moreover, the simultaneous transmission is only considered against passive attacks such as eavesdroppers. Various artificial noise and cooperative jammer applications also promote the superposition of signals to prevent information leakage to the eavesdroppers. A summary of these studies is given in Table 7.1.

Table 7.1 : Security studies.

Author	Year	Contribution	Performance metric
Shashank and Kashyap [204]	2013	Achieves strong secrecy with lattice codes and randomized encoding	Achievable power-rate pair
Vatedka *et al* [9]	2015	Provides perfect or strong secrecy to two-way relay networks using CPF	
Babaheidarian and Salimi [205]	2015	Combines lattice alignment and asymmetric CPF to improve the secure sum rates	Achievable sum rate
Richter *et al* [206]	2015	Includes fading and provides weak secrecy for multi-way relay networks using CPF	Secrecy capacity
Karpuk and Chorti [207]	2016	Derive the secrecy rate upper bounds, investigates the effect of synchronization error and extends the proposed model to MIMO sceheme	
Ren *et al* [32]	2017	Investigates internet and external eavesdropper scenarios, includes two-hop channel, jammer and improves the secrecy rate	
Goldenbaum *et al* [208]	2016	Defines and derives the secrecy computation-capacity and shows that it can be achieved without sacrificing capacity	Secrecy computation-rate
Goldenbaum *et al* [209]	2016	Secure against the eavesdroppers that has good channel conditions and applicable with low-complexity	
Babaheidarian *et al* [210]	2017	Considers the scenario of malicious receiver and provides secrecy in this scenario with beamforming and jamming	Achievable secure rate
Hynek Sykora [211]	2015	Uses game theory to provide secrecy	Pay-off matrix
Negi and Goel [212]	2016	Provides secrecy by using artificial noise for networks with multiple antennae or helper nodes.	Secrecy Capacity, outage prob.

The CPF method is utilized for the security purposes in [204]. The study considers a two transmitter network that communicates with a curious relay using CPF over the AWGN channel. The security of the method is confirmed by investigating the mutual information between the individual messages and the superimposed signal at the relay. It is shown that the mutual information is significantly small for large block lengths and gives insufficient information to the relay. The study also derives the achievable rates and the necessary conditions for secure communication. Lastly, the network is generalized for the multi-hop networks.

Another secure communication scheme based on the CPF is given in [205]. In the study, an asymmetric CPF model (as in [41]) is considered which assumes asymmetric channel gains towards the eavesdropper and the secure sum rates are derived.

A comprehensive study on secure communication is given in [9] which is based on the CPF over bi-directional relay channels. Two nodes in the proposed model aim to communicate with the help of a relay without leaking information to the relay. Perfect and strong secrecy conditions are defined to evaluate the secrecy performance. It is shown that the proposed lattice coding and the CPF provide both strong and perfect secrecy even in a noiseless design. Also, the results reveal that the noise only affects the computation performance. Lastly, the computation rate under the Gaussian noise is derived. Another comprehensive secure communication study is given in [206]. In addition to [9], this study considers SIMO multi-user multi-way networks and includes fading to the channel model. The study derives the secrecy region under the weak secrecy condition. The results show that the securely achievable sum-rate is equal to the difference between the computation rate and the MAC capacity. The simulations verify the derived results and compare the proposed model with the traditional insecure CPF and the security schemes in [9] with respect to the secrecy rates.

Secure communication of two nodes through a relay node is considered in [207] with the help of PLNC. The study considers perfect secrecy conditions and defines the upper bounds on the achievable secrecy rate for noiseless channels. Different coding algorithms are designed for scenarios where the nodes are alone or they cooperate. Moreover, the achievable rates are calculated for these scenarios and it is shown that the given algorithms reach close to the calculated upper bounds. Lastly, the study is extended to multiple antenna equipped nodes.

In [208], the secure communication of multiple nodes is aimed at a modulo-2 adder network. The objective is to leak no information to the eavesdropper while the legitimate receiver obtains the modulo-2 sum of the transmitters. The study defines the secrecy computation communication capacity which is the maximum achievable secure computation rate and it is shown that the secrecy computation communication capacity is the same as the computation capacity under certain conditions. In other words, the proposed scheme can achieve security constraints without reducing the capacity.

Secure function computation based on the AFC over a wiretap channel is considered in [209]. The study aims to keep the eavesdropper ignorant and contributes to the complexity such that the method can provide security without the need for additional stochastic encoding. Also, the study assumes no advantage over the eavesdropper e.g. better channel quality.

In [32], a modified CPF given in [213] is exploited for the purpose of secure communication. Two scenarios where the adversary is external and internal (the relay) are considered. In the internal case, the relay is assumed to be curious that eavesdrops the received signal and the destination node is assumed to be cooperative by jamming the relay to prevent information leakage. The random binning and the lattice chain codes are used in the proposed scheme. It is shown that the proposed methods can achieve the secrecy capacity at the high SNR regions. Moreover, the results reviled that the obtained secrecy capacity is close to the channel capacity. Specifically, the security constraints only lower the insecure channel capacity by $1/2$ bits per channel use. Cooperative jamming is also applied in [210]. Secure communication from multiple sources to multiple receivers is aimed by using relay nodes. In contrast to [32], a relay is assumed to be trustworthy and cooperative in the way that the relays use beamforming to jam the malicious receivers.

The short note in [211] considers a scenario such that the relays of a PLNC network can be malicious and intentionally use a deceptive mapping. The study views this problem as an incomplete information game and aims to find an equilibrium as a function of the probability that a malignant relay exists.

Some studies aim to improve the security of the communication system by intentionally introducing noise. These studies are commonly classified under physical layer security methods. Negi and Goel [212] proposes a secure transmission model that uses artificial noise. The proposed model intentionally introduces AN to the wireless channel in order to degrade the eavesdropper's channel. Naturally, the added AN also degrades the legitimate receiver's channel. This problem is solved by separating the AN source from the signal source. Writers propose two methods for the separation; using other antennas (multiple antennae) or other users (helpers). In both methods, AN and signal source transmit simultaneously at the same time and frequency slot. However, AN source chooses the noise vector such that the noise and the channel

coefficient of the legitimate receiver cancel each other. In other words, AN lies in the null space of the channel coefficient of the legitimate receiver. The paper makes two critical assumptions. Firstly, transmitters perfectly know the receiver's channel. Secondly, legitimate receivers and the eavesdropper's channels are uncorrelated, which enables AN to degrade any channel other than the legitimate receiver's. Presented methods are also supported and compared with simulations.

The simultaneous transmission techniques are considered in the literature for security purposes as presented in this Chapter. However, these studies do not take active attacks, e.g. spoofing, into account. Also, the traditional simultaneous transmission models lose individual data at the receiver and only obtain a function of them. In the following Chapter, a unique AFC method is proposed to achieve the individual data at the receiver and also authenticate it.

8. AUTHENTICATED DATA TRANSMISSION

The expectations from next-generation wireless networks include higher rates and lower latency values with secure transmissions from numerous devices [214]. The traditional orthogonal multiple access schemes become insufficient to meet these targets [215]. AFC makes the simultaneous transmission of information possible for multiple nodes. In particular, the signal processing at the transmitting and receiving ends transforms the interference into computational power [116]. In other words, AFC manages to change the channel model in a way that received signals from the channel form the output of the target operation. As a result, the computational load on the receiver end is transferred to the channel. Also in the sense of transmission efficiency, the number of time slots required to collect information from multiple nodes is reduced to one transmission time slot with AFC [105].

Recent works about various applications of AFC target a variety of different objective functions [122, 126, 133, 135]. In [126], AFC is used in combination with a fusion center (FC) that can obtain multiple target functions of the different types of measurements (e.g. temperature, pressure, or light) through transmitting multi-modal data values from sensor nodes. Multi-input multi-output (MIMO) based AFC model with transmit and receive beamforming schemes is utilized in [126]. [122] proposes another approach to calculating different target functions with the MIMO-based AFC scheme by utilizing the zero-forcing beamforming scheme to reduce the interference and to alleviate the nonuniform fading effect. To alleviate the energy cost of the investigated AFC scheme, a minimum mean square error (MMSE) estimator based on exploiting spatial correlations among sensor observations is proposed in [135]. A unified architecture including AFC and wireless power transfer is introduced to control energy utilization and data aggregation by utilizing a beamforming technique in [133].

Although the conventional AFC schemes provide significant benefits, one of the drawbacks of the AFC is that its use is restricted to the applications, where only a function of the information from multiple nodes is required. Individual information

of nodes is lost over the channel due to simultaneous signal transmissions. Besides, conventional AFC schemes are also vulnerable to passive and active physical layer attacks due to the anonymity of the received signals. The resilience against spoofing attacks can be introduced by using authentication schemes, frequently applied at the upper layers of a communication system. However, classical authentication schemes are applicable to pairwise communications and they require a private key only known by the legitimate users to function [216]. Extending the use of such an algorithm to numerous users in an effective manner is not straightforward [216]. As a result, classical authentication methods restrict the time and communication efficiency of the system.

This chapter of the thesis considers the problem of secure information sharing in a wireless uplink data transmission system that is composed of a base station (BS), a spoofer and $N \in \mathbb{N}$ users, as illustrated in Fig. 8.1. The i^{th} user is denoted by U_i for $i = 1,\ldots,N$. h_i represents the channel coefficient between U_i and the BS. A unique prime number denoted by p_i is assigned to U_i as a unique identifier (key) to realize authenticated data transmission.

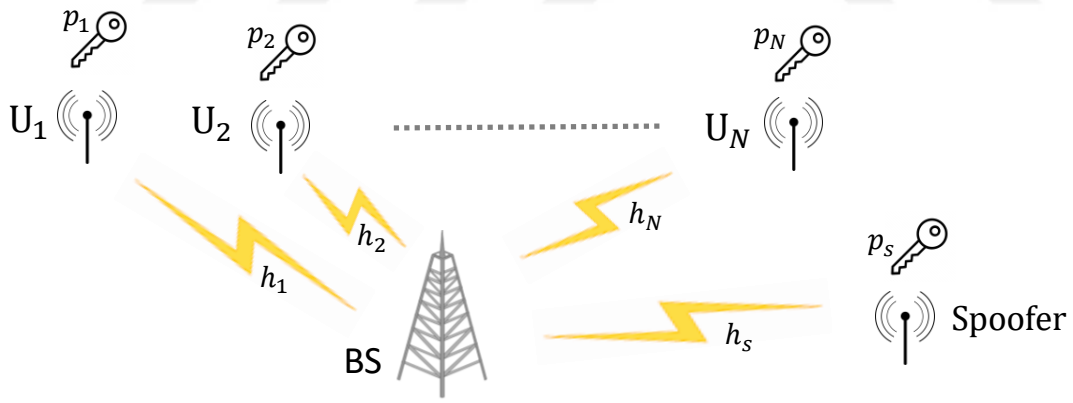


Figure 8.1 : Multi-user authenticated data transmission network model.

The first aspect of the considered model is the reduced number of required time slots to complete simultaneous communication in the uplink direction. As expected, the proposed technique offers the same efficiency with AFC and completes the overall transmission in a single time slot. Furthermore, the proposed method is not restricted to lose individual information at the BS like the AFC applications. It will be explained in the following sections that the information from all nodes is accessible and identifiable at the receiver.

The second aspect is the robustness of the system against active attacks that aim to imitate a legitimate user. In a traditional sense, authentication of the users requires previously distributed private keys [216] and pairwise communications that are proportional to the number of users. In this method, the fading characteristic of the channel is exploited to work as a natural secret key and distinguish malicious users from the legitimate ones at the BS while preserving the scalability of the AFC. In addition, the presented model enables simultaneous digital data transmission over W-MAC for multiple users.

8.1 System Model

The considered wireless uplink scenario consisting of the BS and N users is depicted in Fig. 8.1. All communications in the system are limited to be half-duplex. The set of all users are denoted by $\mathscr{U} = \{U_1, \ldots, U_N\}$, where U_i is the i^{th} user. A set of prime or Gaussian prime integers[1] are defined as $\mathscr{P} = \{p_1, \ldots, p_N\} \subset \mathbb{C}$ to be the set of identifiers assigned uniquely to each user and the set of information containing messages is denoted by $\mathscr{M} = \{m_1, \ldots, m_M\}$. The identifier and the message sets are under the power and complexity restrictions that the transmit power of the nodes and computation time of transmitters are under the allowable levels. The channel gains between the U_i and the BS is indicated by h_i and h_s represents the channel coefficient between the spoofer and the BS. Channel estimation errors of the U_i and the spoofer are modeled with two random variables, E_i and E_s, and their realizations are represented by e_i and e_s respectively. Any wireless link between the BS and any user is assumed to be uncorrelated [217]. The BS requires information from all users in a one-time slot, which is possible with simultaneous transmission of $\mathscr{U}$ over the wireless channel based on AFC. As a design goal, it is expected that the BS should be able to distinguish the interference of non-legitimate users (spoofing attacks) from the channel estimation error and the thermal noise. Communications in the system are modeled according to the W-MAC model defined as follows.

[1] Gaussian primes are complex integers that can not be written as a product of two non-units in the complex plane. Using complex domain instead of using only real increases our symbol set without significantly increasing the symbol energy, elegantly reducing the peak to average power ratio (PAPR) of the transmitters.

Definition 1. *Let y, x_i, h_i and ω be the received signal, transmitted signal, fading coefficient between two nodes and the additive noise, respectively. Then, the channel model W-MAC is defined as,*

$$y = \sum_{i=1}^{N} h_i x_i + \omega. \tag{8.1}$$

The summation operation given in (8.1) represents the superposition property of the W-MAC. This characteristic enables the simultaneous transmission of users; thus contributes to the scalability and time slot gain of the proposed network.

Functions computable over the ideal W-MAC is not limited to the summation operation when signal processing is applied at the transmitter and the receiver [119]. The following two functions define the application performed at the transmitter and the receiver, which is signal processing, respectively.

Definition 2. *A function is denoted with φ_i to describe $\varphi_i(x_i) = (\varphi \circ x_i)$ as the pre-processing function of the U_i where x is a real number.*

Definition 3. *A function is denoted with ψ to describe $\psi(y) = (\psi \circ y)$ as the post-processing function of the BS where x is a real number.*

Faithful to the AFC terminology [119], the ideal W-MAC ($\omega = 0$) is modified with pre and post-processing functions as a new channel model, matched W-MAC, and depicted in Fig. 8.2. The input and output of the matched W-MAC denote the signal processed inputs and output. By using these signal processing, computation of desired functions is possible over the matched W-MAC. In conventional AFC applications, the matched W-MAC model is used in sensor networks for only computational purposes, where individual inputs of the nodes are not required at the FC [218]. The total transmission of multiple sensor readings can be completed in a single transmission slot thanks to AFC. Hence, significant reductions in transmission duration are obtained for sensor networks.

Different from the rest of the AFC studies, matching the ideal W-MAC to transfer individual data of the users to the BS is evaluated in this chapter. As a design goal, obtaining each individual message of $\mathscr{U}$ at the output of the matched W-MAC is aimed while being able to detect any spoofing attack.

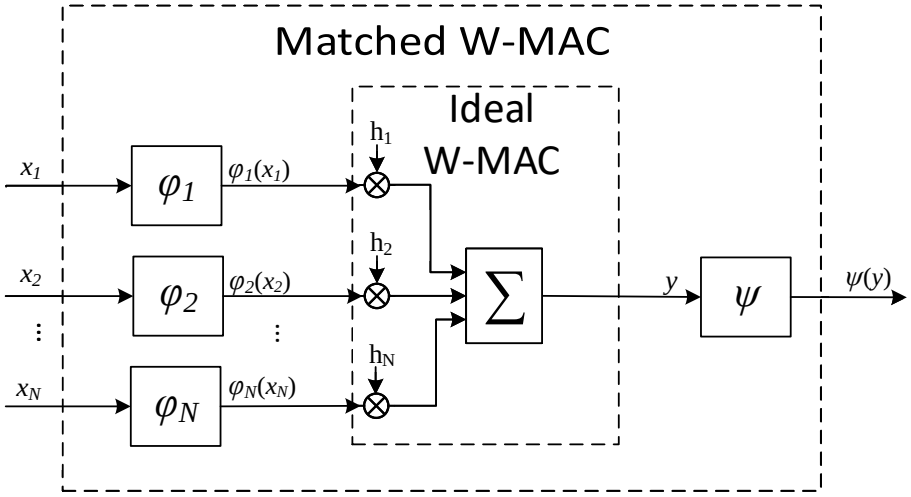


Figure 8.2 : Illustration of the matched W-MAC.

8.2 Authenticated Data Transmission

The main objective of this approach is to carry information from multiple users to one receiver (the BS) in a one-time slot. As mentioned before, the superposition property of the W-MAC naturally allows the transmission of information in a one-time slot since multiple users can transmit their information simultaneously. However, interference of signals with each other prevents the reconstruction of individual data of multiple users. In order to overcome this restriction, the use of a specific pre-processing function with specific inputs in the matched W-MAC is proposed.

Theorem 1. *A BS can receive individual information from N users in one time slot over the matched W-MAC using the signal processing as follows.*

$$\varphi_i(x_i) = \frac{1}{h_i} \ln {p_i}^{x_i}, \qquad \psi(y) = \exp(y) \tag{8.2}$$

where $\ln(\cdot)$ *and* $\exp(\cdot)$ *denote the natural logarithm and exponential functions respectively,* h_i *is the fading coefficient between the* U_i *and the BS,* $p_i \in \mathscr{P}$ *is the identifier of the* U_i *and* x_i *is the input of the matched W-MAC*

Proof. Let all users choose their input to the modified channel as $x_i = m_i$, where m_i is an integer number selected from a given set $\mathscr{M}$ at U_i. The utilization of the primes in the defined pre-processing function make the digital transmission over AFC structure possible. When all users broadcast their output of the pre-processing function, $\varphi_i(x_i)$,

the received signal at the BS can be given as

$$y = \sum_{i=1}^{N} \ln {p_i}^{m_i} = \ln \prod_{i=1}^{N} p_i^{m_i} \tag{8.3}$$

is expected to be received as the output of the matched W-MAC. The fading coefficient used in the pre-processing function cancels the destructive effect of the channel. Since the pre-processing function is in logarithmic base, the channel is matched to perform multiplication and inputs of the users are multiplied with each other.

After the simultaneous transmission of $\mathscr{U}$, the output of the matched W-MAC can be expressed as

$$\psi(y) = \exp\left[\ln \prod_{i=1}^{N} {p_i}^{m_i}\right] = \prod_{i=1}^{N} p_i^{m_i}. \tag{8.4}$$

The output given in (8.4) contains information of each user as exponents of each identifier. Since identifiers are prime, each identifier p_i can be extracted from $\psi(y)$ with factorization and the occurrence of each identifier gives the information m_i corresponding to that identifier. Prime numbers in multiplication are separable from each other, hence using prime identifiers as inputs would enable the reconstruction of individual information at the BS. □

As stated in the given theorem, information from multiple users can be carried to the BS in a single time slot without compromising the individual data recognition. Another observation from the Theorem 1 is the scalability aspect of the proposed method. Since the number of users, N, is not a variable of the matched W-MAC, increasing N does not change the total transmission time. Lastly, the computational complexity in the BS is an important detail to consider. Therefore, it should be noted that the elements of the identifier set, $\mathscr{P}$, and the message set, $\mathscr{M}$, are chosen such that the computations in the BS are feasible. In the following section, the given method is investigated against spoofing attacks in the presence of channel estimation errors and thermal noise with Monte Carlo simulations.

8.3 Authentication of the Transmitted Data

Messages carried over a broadcast channel is vulnerable to spoofing attacks. As a result, traditional authentication methods apply authentication codes to the messages

in order to prevent adversaries from modifying the original message without being detected [216]. However, authentication codes used in these algorithms require both users to have prior knowledge of the same private key. Sender modifies the message with an algorithm using the private key, hence only the receiver can decode the message with the same private key.

Unlike the traditional authentication approaches, the proposed method does not require a private key that is shared by the participants. Carrying information embedded to signal amplitudes over the matched W-MAC presents a unique advantage against spoofing attacks. The reason comes from the fading characteristic of the channel that can only be estimated by the original users. Each user in the proposed network uses the fading coefficient in the pre-process such that transmitted signal only has the intended value at the BS. Since illegitimate users are unable to accurately estimate their fading coefficient towards the BS, messages sent by the adversary would distort the post-processed output and this distortion acts as a natural authentication mechanism.

First consider the ideal condition that legitimate users have perfect channel state information (CSI), as in [219, 220], and the spoofer tries to estimate its own CSI. Assume that the spoofer makes an estimation error which is modelled with Gaussian distribution $E_s \sim \mathcal{N}(0, \sigma_s^2)$ with zero mean, σ_s^2 variance. Then the BS would obtain

$$\psi(y) = \exp\left(\underbrace{r_s \ln {p_s}^{m_s}}_{\text{spoofer}} + \underbrace{\sum_{i=1}^{N} \ln {p_i}^{m_i}}_{\text{legitimate users}} \right) = {p_s}^{(m_s r_s)} \prod_{i=1}^{N} {p_i}^{m_i} \tag{8.5}$$

as the output of the matched W-MAC, where p_s is the spoofer's identifier, m_s is the fraudulent message and $r_s = h_s/(h_s + e_s)$. The spoofer's input to the W-MAC is distorted as a result of the channel estimation error as shown in (8.5) and ${p_s}^{(m_s r_s)}$ is obviously not an integer. Since the BS only expects the multiples of the prime identifiers from the matched W-MAC, spoofing attacks can be successfully detected if $r_s \neq 1$.

Now the non-ideal conditions are considered by introducing Gaussian noise and imperfect CSI to the system model. With this goal, it is assumed that all legitimate users make estimation error and use imperfect CSI in their pre processing. The estimation error of the i^{th} legitimate user is defined as a random variable, $E_i \sim$

$\mathcal{N}(0,\sigma_i^2)$ with zero mean, σ_i^2 variance. The resulting post-processing function output becomes,

$$\begin{aligned}\psi(y) =& \exp\left(\underbrace{r_s \ln {p_s}^{m_s}}_{\text{spoofer}} + \underbrace{\sum_{i=1}^{N} r_i \ln {p_i}^{m_i}}_{\text{legitimate users}} + \omega\right) \\ =& e^{\omega} {p_s}^{(m_s r_s)} \prod_{i=1}^{N} {p_i}^{(m_i r_i)}\end{aligned} \tag{8.6}$$

where $r_i = h_i/(h_i + e_i)$ represents the distortion of legitimate users caused by the fading. A reasonable question at this point is whether the source of discrepancy at the BS is the non-ideal conditions or a spoofing attack. It is clear that the ideal conditions can be solved by simply integer checking since the signals other than the exponential of the prime identifiers are not expected at the BS. However, imperfect CSI also yields non-integers at the BS and triggers a false authentication alarm with a simple integer based detection.

The problem now becomes differentiating spoofing attacks from the impact of non-ideal conditions. It can be also given as a detection problem under the following hypotheses,

$$\begin{aligned} H_0 &: \psi(y) = e^{\omega} {p_s}^{(m_s r_s)} \prod_{i=1}^{N-1} {p_i}^{(m_i r_i)}, \\ H_1 &: \psi(y) = e^{\omega} \prod_{i=1}^{N} {p_i}^{(m_i r_i)} \end{aligned} \tag{8.7}$$

where the null hypothesis states the existence of a spoofer. A straightforward test to decide between the given hypotheses can be based on the distance between the post-processing functions of ideal and non-ideal cases. For this purpose, the following threshold-based test is defined as,

$$T(x) = \min_{y \in \mathscr{Y}} \left(\psi(y) - \psi(\tilde{y}) \right) \lesseqgtr \lambda \tag{8.8}$$

where $\tilde{y}$ is the received signal from the matched W-MAC under non-ideal conditions and $y \in \mathscr{Y}$ is the expected signal under ideal conditions. λ denotes the threshold and $\mathscr{Y}$ is the set of possible received signals under ideal conditions.

The detection mechanism that is given above relies on the deviation from the ideal conditions. In other words, the threshold limits the decision regions, that the signals

inside these regions are accepted and the larger deviations than the threshold are recognized as an attack. Therefore, the performance of the given system depends on the selected threshold. The identifier and the message sets, as well as the noise, have important impacts on the selection of a threshold which is pre-determined and not dependant on the current transmission. Utilizing (8.7) and (8.8), the successful detection rate, P_d, and the false alarm ratio, P_{fa} can be defined as

$$\begin{aligned} P_d &= P(T(x) > \lambda | H_0), \\ P_{fa} &= P(T(x) > \lambda | H_1). \end{aligned} \tag{8.9}$$

Receiver operating characteristics (ROC) are useful tools to decide the value of the threshold. A ROC curve can be obtained with simulations (as in the next section) that test the various threshold samples and output the detection performance of those thresholds. Once the corresponding ROC curve is obtained, the threshold can be determined to satisfy the maximum false alarm or the minimum successful detection rate conditions. The feasibility of this detection mechanism and the impact of the non-ideal conditions is investigated via simulations in the following section.

8.4 Numerical Results

The feasibility of the method is examined in two directions; data transfer performance and spoofing detection performance. For this purpose, two simulation scenarios are designed where the clean (not spoofed) scenario consists of N legitimate users, and the latter, spoofed scenario, consists of $N-1$ users and a single spoofer. The wireless channel among users and the BS are modeled as given in (8.1). Gaussian distributed channel estimation errors, i.e. imperfect CSI, are assumed for each legitimate user and the spoofer with $\sigma_i^2 = 10^{-5}$ and $\sigma_s^2 = 10^{-2}$, respectively. Here, the legitimate users' estimation process is assumed to be more accurate than that of the spoofer's, i.e. ($\sigma_i^2 < \sigma_s^2$). The prime identifiers, p_i, are selected from a Gaussian prime set such that $\mathscr{P} = \{a+bj\}$, $a \in (0,5)$, $b \in (-5,5)$ and $a,b \in \mathbb{N}$.

The data transfer performance is analyzed in the clean scenario in terms of symbol error rate (SER) as a function of the signal to noise ratio (SNR). Here, the received signals are mapped to the closest $y \in \mathscr{Y}$. The simulation results are given in Fig. 8.3 for $N,M = \{2,3,4\}$, where $N = |\mathscr{U}|$ and $M = |\mathscr{M}|$. The simulations demonstrate that the proposed method provides feasible operating points after SNR = 20 dB. Increasing

the number of users and using larger message sets deteriorate the SER performance and require higher transmission power levels to operate while presenting higher data rates.

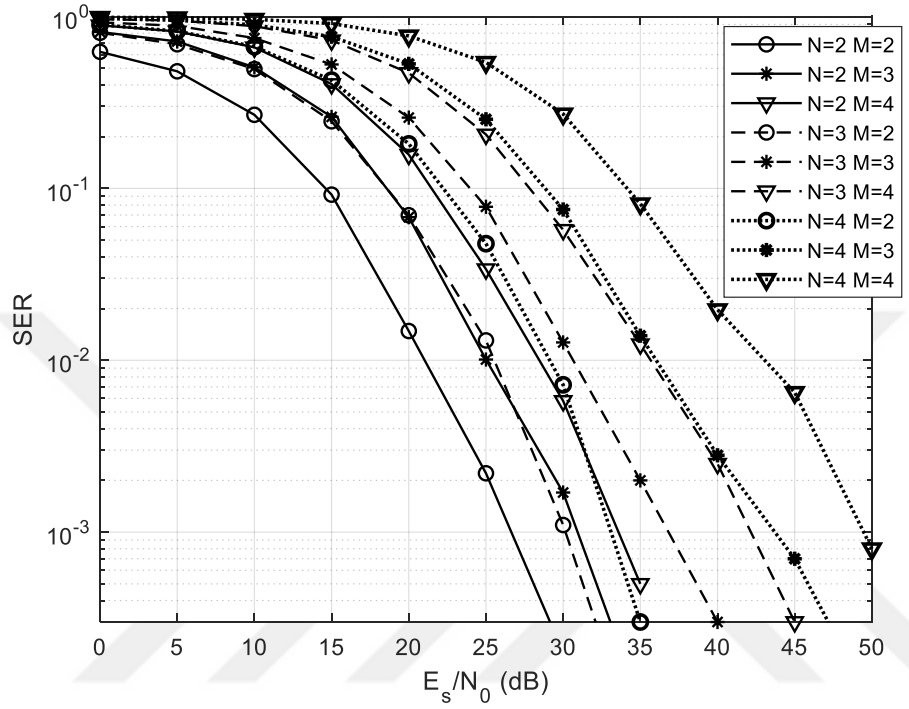


Figure 8.3 : Symbol error performance of the authenticated data transmission method.

The second aspect considered in this chapter is the spoofing detection performance where both clean and spoofed scenarios are compared with the hypothesis test given in (8.8). The detection performance is depicted in Fig. 8.4 with ROC curves for $N = 2,3,4$, $M = 2,3$ and SNR = $30,50$ dB. Each curve in Fig. 8.4 is obtained by testing 10^4 different thresholds and illustrates the successful detection rate, P_d, as a function of false alarm ratio, P_{fa}.

It can be observed from the figure that operating at very high SNR values such as 50 dB presents efficient detection performance. For example allowing $P_{fa} = 0.2$ enables the $N,M = 2$ networks to detect more than 99% of the spoofing attacks correctly and this rate only falls to 80% for $N = 4$. Note that under ideal conditions (i.e. in the absence of channel estimation errors and very high SNR values) the proposed method is expected to function ideally and support very high data rates (high N,M values) securely.

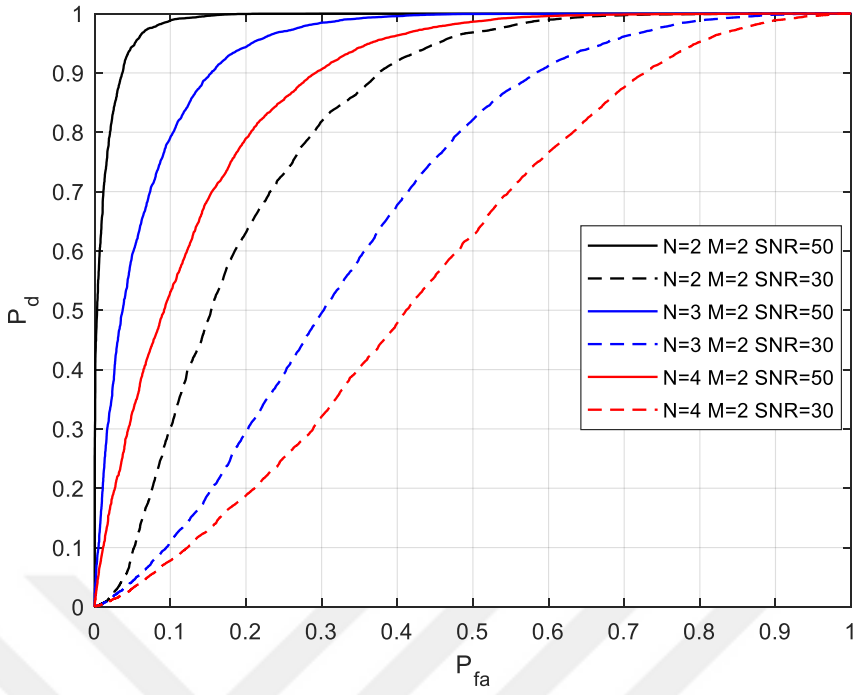


Figure 8.4 : Spoofing detection performance of the authenticated data transmission method.

The proposed method carries the information of multiple nodes to a single receiver with the simultaneous transmission. The objective of the method is to manipulate the wireless channel to obtain each individual data at the receiver from the superpositioned signal. The method is also investigated against active attacks and its robustness against spoofers is verified. In the following Chapter, a similar analog approach is considered for multi-node networks. However this time, the channel is matched with a function that generates secret keys to each node and the network is secure against eavesdroppers.

9. SECRET KEY GENERATION

The size of the wireless sensor networks (WSNs) that are connected with the IoT is expected to grow at massive scales in the future. For this reason, the IoT seeks communication technologies that are able to handle the limited wireless resources more efficiently than traditional methods. Providing security in these settings is a challenging task that costs network resources proportional to the network size with conventional security measures. Messages are usually processed at the upper layers to disguise the information from eavesdroppers. However, the distribution of the key to nodes is a vulnerable process that can be intercepted by adversaries and also requires the existence of a center node that is a large cost.

The physical layer security is an alternative that is proposed in [221] to prevent adversaries from obtaining the information. Instead of hiding the information with keys, the physical layer studies (as in [222, 223]) considered preventing the eavesdropper from correctly obtaining the signals. This point of view is later extended to the Gaussian wiretap channel [224]) and to several wireless technologies such as AN, beamforming [225, 226]) to improve the efficiency of the network.

Although these models consider the communication between two nodes, their perspective inspired the physical layer key generation methods [227, 228] which carry the resource efficiency of the encryption methods and eliminate the vulnerability of key distribution process. The key generation problem of multi-node networks is studied from two perspectives. In [229–231], a central node is assigned to distribute the secret key to multiple nodes by broadcasting it under the security of the physical layer. Instead of acting as a central node, the nodes in [232–234], sequentially broadcast their messages to agree on a secret key under the security of the physical layer.

Although the reciprocity and the fading of the W-MAC are exploited for security purposes, these characteristics have been also a ground for AFC studies, which are pioneered by Gastpar [3, 235] and Stańczak [7, 116, 119]. Contrary to security methods, AFC exploits these characteristics to improve network throughput with

function computation over the channel. In conventional networks, communication and computation processes are separated such that the receiver obtains the individual information and then computes the desired function using the obtained information. The AFC fundamentally transfers the computation process to the wireless channel and reduces the computation task of the receiver. In other words, the AFC *matching* the wireless channel to compute the desired function with the *pre* and post processing functions [116].

AFC is often considered in sensor networks to transfer the data of multiple sensor nodes to the receiver. The nodes in an AFC network simultaneously transmit their data to the receiver after applying a pre-processing function. The receiver obtains the superimposed signal which contains the weighted sum of the initial data. The signal processing enables the receiver to obtain the average of the initial data without explicitly computing the average function. The authors of [126] and [122] extended the AFC to MIMO channels and beamforming. Also, the AFC is used in consensus algorithms to reduce the convergence time of sensor networks [188, 236]. In [135], an energy-efficient AFC scheme is proposed for densely deployed IoT networks. In this chapter, two key generation methods are proposed for WSNs that N nodes agree upon a secret key. The important attributes and the contributions of these models can be listed as follows.

- Proposed method removes the need for a center node to distribute keys to the nodes, hence relieves some of the energy and complexity burdens of the key generation process.
- It has been proven that the key generation of multiple nodes with a single communication would require the existence of multi-linear maps [237]. Since the multi-linear maps have not been presented explicitly yet, pair-wise or broadcast communications are used to generate secret keys with sequential communications. In these methods, the multiple access nature is exploited with simultaneous transmissions to reduce the delay of the key generation process.
  - In the first method, a half-duplex network is considered for the key generation. The method manages to reduce the key agreement duration to a linear scale by providing secret keys to N nodes with N-to-1 concurrent transmissions.

  - The second method reduces the key generation duration to constant scale by enabling full-duplex communications (see [238, 239]) and N-to-N concurrent transmission. Although a multi-linear map is not used in the algorithm, the W-MAC imitates the effect of a multi-linear map on the channel inputs.

- The proposed methods provide security against eavesdroppers. The security aspect eventually comes from the network size and simultaneous transmission. A single node receives $N-1$ components of the secret key that consists of N components in a single communication. Then the node combines with its own component to reach the secret key. However, the eavesdropper needs to listen to every communication to obtain all of the N components. It is shown with simulations that the additive noise of each component eventually causes the eavesdropper to calculate the secret key with a 100% error.

- The method is also able to detect active eavesdroppers that aim to add false components to the secret key if a small channel estimation error is assumed at the eavesdropper's side. The key components are randomly chosen from a Gaussian prime set at each node and transmitted to the channel simultaneously. Since the nodes expect to receive the product of $N-1$ Gaussian primes, a distorted component can be detected by the nodes.

9.1 System Model

Consider a wireless sensor network that consists of N nodes as depicted in Fig. 9.1. It is assumed that an eavesdropper (Eve) is also present and monitors the transmitted signals. The purpose of this chapter is to provide each node with a secret key S using in-network communications without leaking S to Eve. The set of all nodes is denoted by $\mathscr{N} = \{n_1, \ldots, n_N\}$, where nodes are in an arbitrary order. The transmitting nodes are specified as $n_i \in \mathscr{N}$ and the receiving node as $n_j \in \mathscr{N}$, where $i \neq j < N$ are integers. The key components are randomly drawn from Gaussian prime integers such as $\mathscr{P} \subseteq \mathbb{N}$.

Two methods are presented to generate secret keys depending on the half-duplex or full-duplex communication capacity of the nodes. The communications that generate a secret key takes place over the W-MAC that is given in Definition 1. In [119]

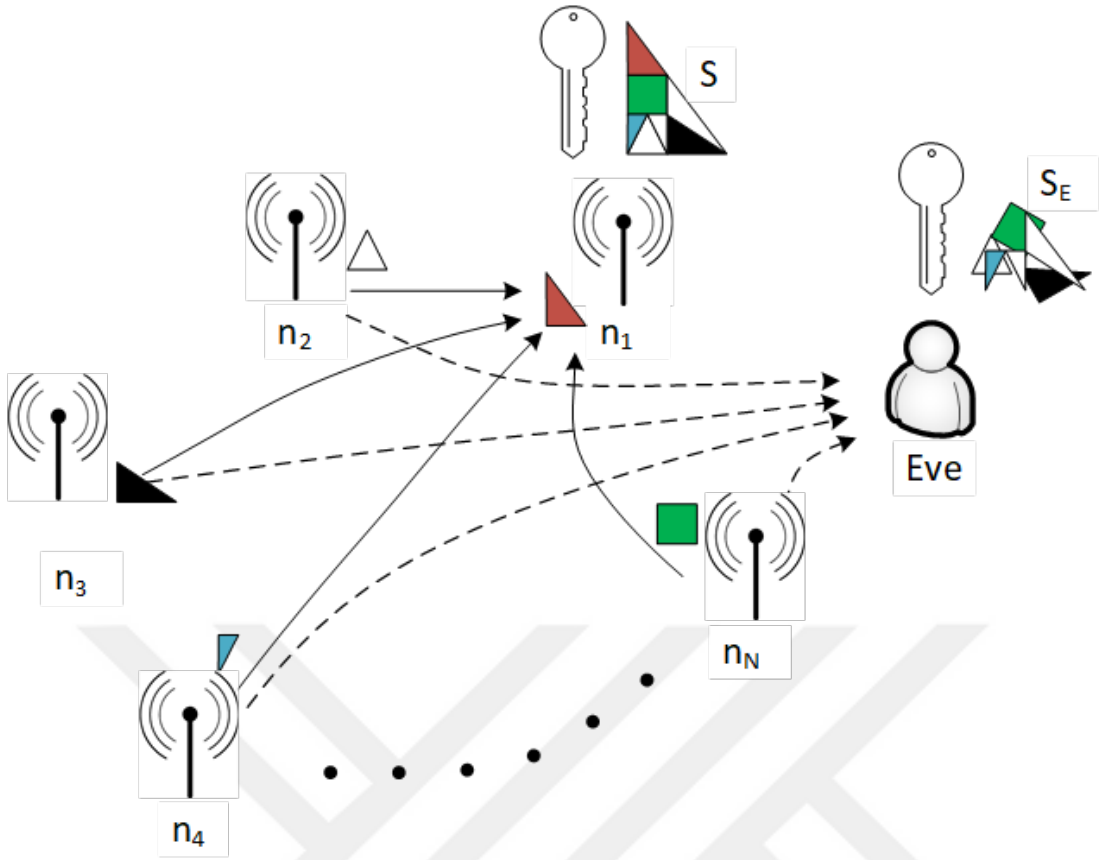


Figure 9.1 : Illustration of the secret key generation method.

it is proved that AFC can be used to compute any function over the channel. The pre-processing and the post-processing functions that compute any function are defined in Definition 2 and Definition 3, respectively.

The pre processing and post processing functions fundamentally alters the wireless channel to imitate mathematical functions. The key generation method is based on the multiplication operation of the AFC over the W-MAC which can be given as follows.

$$\varphi_i(x_i) = \frac{1}{h_{ij}} \ln(x_i). \tag{9.1}$$

Remark 1. *AFC methods consider noise-free channel models (ω=0) and invert the channel gain beforehand with the channel state information (CSI) (h=1). As a result, the channel fading coefficient h_{ij} is not given in the pre-processing functions. Here, the fading component is explicitly included in the pre-processing functions due to the full-duplex key generation model. Also, a more realistic scenario is considered where AWGN is added to the received signals.*

Logarithmic functions can be used to convert a summation operation into multiplication. However, the inputs of the logarithmic function later require an inverse

operation to obtain the product of the inputs. The post-processing function that satisfies this observation can be given as follows.

$$\psi_j(y_j) = \exp[y_j] \tag{9.2}$$

With pre processing function in (9.1) and the post processing function in (9.2), product of transmitted components can be obtained at the receiver node as follows.

$$\psi(\sum_{i=1}^{N} \varphi_i(x_i)) = \psi(\ln\left(\prod_{i=1}^{N} x_i\right)) = \prod_{i=1}^{N} x_i. \tag{9.3}$$

In the following section, the wireless channel is matched with novel pre and post processing functions in order to provide a key to all WSN nodes.

9.2 Secret Generation over W-HMAC

The half-duplex method involves $N-to-1$ communications that provide a secret key to a single node. Hence, N nodes can acquire the same secret key with N concurrent transmissions. The following definition presents the manipulated channel model that enables $N-to-1$ concurrent transmissions.

Definition 4 (W-HMAC)**.** *Let $\varphi_i(x_i)$ and $\psi_j(y_j)$ be the signal processing where $i, j \leq N, i \neq j$. The W-HMAC is defined as,*

$$\psi_j(y_j) = \psi_j\left(\sum_{\substack{i=1 \\ i\neq j}}^{N} h_{ij}\varphi_i(x_i)\right), \tag{9.4}$$

between n_i and n_j.

The W-HMAC is illustrated in Fig. 9.2 where a node $n_j \in \mathscr{N}$ obtain the data of other nodes $n_i \in \mathscr{N} \setminus n_j$. The key generation over the W-HMAC scheme can be presented in two steps as follows.

Initialization Nodes in the network take a Gaussian prime $p_i \in \mathscr{P}$ as a prime component for the shared key and transmit $x_i = p_i$ to the W-HMAC. The following functions are used over the W-HMAC, respectively.

$$\begin{aligned} \varphi_i(p_i) &= \frac{\ln x_i}{h_{ij}} \\ \psi_j(x_j, y_j) &= x_j \exp[y_j]. \end{aligned} \tag{9.5}$$

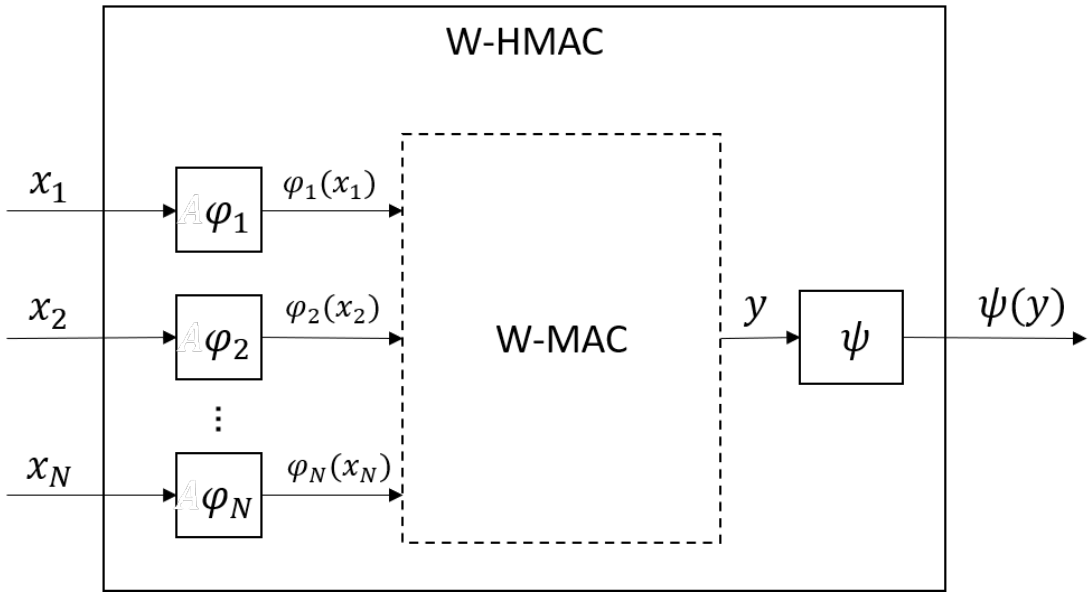


Figure 9.2 : An illustration of W-HMAC where $x_1, ..., x_n$ are inputs and $\psi(y)$ is output.

Key generation n_i in the WSN transmit their signals to the W-HMAC where an $n_j \in \mathcal{N}$ obtains the product of the prime components as

$$\psi(x_j, y_j) = \prod_{i=1}^{N} p_i. \tag{9.6}$$

After the post-processing function, y_j obtains (9.6) which contains the prime components of all nodes. The WSN should repeat the *Secret Generation* step N times where each node becomes the receiver node, i.e. j iterates from 1 to N. Shared key generation over the W-HMAC requires N sequential communications which is in linear scale as opposed to traditional pairwise secret generation methods. Also, it is highly bandwidth and energy-efficient since the nodes occupy the same frequency and time slot by simultaneously transmitting. In the following section, a full-duplex key generation method is presented which can provide a shared key in a single communication.

9.3 Secret Generation over W-FMAC

In this section, a novel approach is developed with full-duplex communication for the key generation problem. For this purpose, the W-MAC is matched with the following channel model.

Definition 5 (W-FMAC)**.** *Let $\varphi_i(x_i)$ and $\psi_j(y_j)$ be the pre processing and post processing functions where $i, j \leq N$. The W-FMAC is defined as,*

$$\psi_j(y_j) = \psi_j \left(\sum_{i=1}^{N} h_{ij} \varphi_i(x_i) \right), \tag{9.7}$$

between n_i and n_j.

The W-FMAC yields a function of the transmitted signals at the receiver nodes x_j as shown in Fig. 9.3. Contrary to the W-HMAC where a node can either transmit or receive ($i \neq j$), W-FMAC can provide a shared secret to all nodes in the WSN.

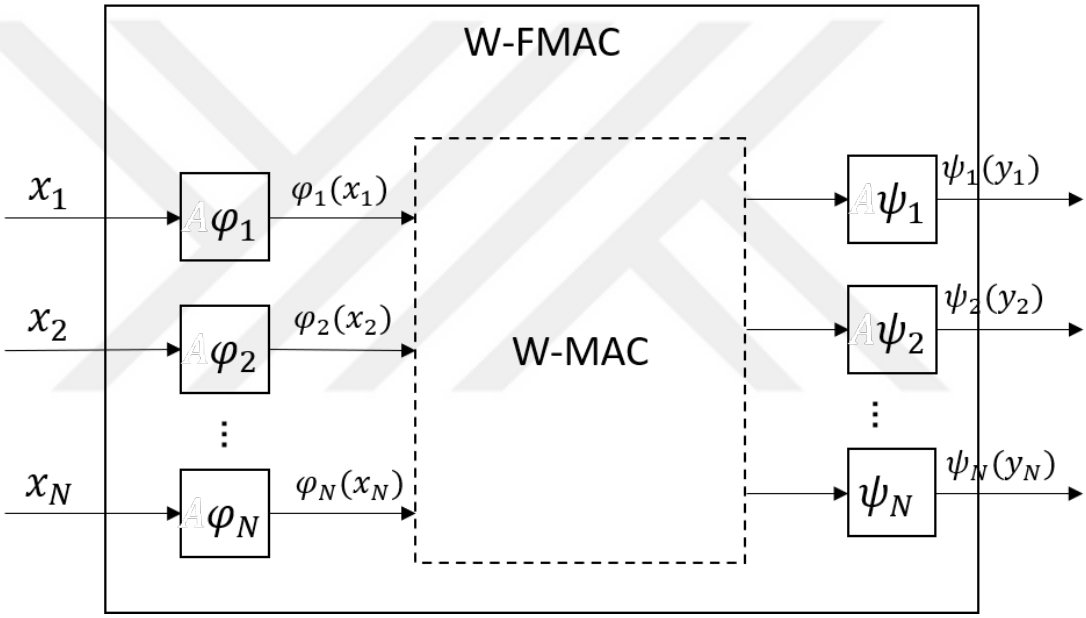


Figure 9.3 : An illustration of W-FMAC, full-duplex adaptation of the W-MAC for secret key generation, where $x_1, ..., x_n$ are inputs and $\psi_1(y_1), ..., \psi_N(y_N)$ are outputs.

Remark 2. *The AFC applications can compute functions given that the fading of the wireless channel is reversed. However, W-FMAC can not reverse the fading of the channel since a transmitter can only reverse its channel towards a single receiver. In W-FMAC, multiple nodes receive information from the channel concurrently. In other words, transmitting nodes in the W-HMAC targets a single receiver. An external receiver in W-HMAC would obtain an independent and meaningless function if it is at least spatially half wavelength away from the targeted receiver. As mentioned in the following section, this is also a security argument against Eve.*

Presenting a meaningful relationship between the received functions in this scenario is a major problem since the fading effects an input differently at each destination. For this problem, the existence of the *pre* and post-processing functions is investigated that can yield a consistent result for each node in the WSN. The results showed that with the following *pre* and post-processing functions, it is possible to salvage enough information to create a relationship between the received signals. The results are presented in the following two steps.

Initialization All nodes in $\mathscr{N}$ take a Gaussian prime $p_i \in \mathscr{P}$ as their input to the W-FMAC as $x_i = p_i$. The pre processing function of the W-FMAC is defined as,

$$\varphi_i(x_i) = \frac{\ln(x_i)}{h^*} \tag{9.8}$$

where h^* is defined such that $h_{ij}/h^* = c_{ij}, \forall i, j$ and $c_{ij} \in \mathbb{Z}^+$, i.e. h_{ij}/h^* becomes an integer. The following post processing function is used in the W-FMAC.

$$\psi_j(x_i, x_j) = \gcd\left(\mathscr{P}, \psi'_j(x_i, y_j)\right) \tag{9.9}$$

where gcd is defined as the greatest common divisor operation. $\psi'(x_i, y_j)$ is an auxiliary function as,

$$\psi'(x_i, y_j) = x_j \exp[\Theta(y_j)] \tag{9.10}$$

where $\Theta(y_j)$ is the self interference cancellation operation (as in [239, 240]). In a realistic scenario, $\psi'(x_i, y_j)$ operation is necessary to normalize the x_j in the post processing function output by firstly removing the self interference and then multiplying with x_j. The pre processing function include the fading coefficients of the W-MAC as integers in the W-FMAC. Therefore, the effect of the fading can be expressed as exponents of x_i. Since x_i only consists of Gaussian primes, the exponents can be removed by finding the gcd's of x_i over $\mathscr{P}$.

Key generation Nodes in $\mathscr{N}$ simultaneously transmit their signals to the W-FMAC. Output of the $\psi'_j(x_i, y_j)$ is

$$\begin{aligned}\psi'_j(x_i,y_j) &= \psi'_j\left(x_j, \sum_{i=1}^{N} h_{ij}\frac{\ln(x_i)}{h^*}\right) \\ &= \psi'_j\left(x_j \exp\left[\sum_{\substack{i=1\\ i\neq j}}^{N} c_{ij}\ln(x_i)\right]\right) \\ &= \psi'_j\left(x_j \exp\left[\ln\left(\prod_{\substack{i=1\\ i\neq j}}^{N} x_i^{c_{ij}}\right)\right]\right) = \prod_{i=1}^{N} x_i^{c_{ij}},\end{aligned} \tag{9.11}$$

which contains x_i with different exponents. Since all nodes know the set of possible prime components, transmitted components can be extracted by finding the elements of $\mathscr{P}$ that is present in (9.11) as follows.

$$\begin{aligned}\psi_j(x_i,y_j) &= \gcd\left(\mathscr{P}, \prod_{i=1}^{N} x_i^{c_{ij}}\right) \\ &= \prod_{i=1}^{N} x_i.\end{aligned} \tag{9.12}$$

The output of the post processing function in (9.12) is obtained at each node and contains the product of all transmitted prime components. At this point, nodes can directly use the product of prime components as S or further produce any desired key with this shared information.

9.4 Secrecy of the Proposed Approach

The security of the key generation methods relies on the size of the WSN and the fading of the W-MAC that is unique to the path between any two points. It is proposed that two-channel models in the previous sections that the nodes communicate over these models to obtain the shared key. As given in the *pre* and post-processing functions, the components of the shared key is carried at the amplitudes of the transmitted signals. In this thesis, it is argued that the proposed methods also show robustness against eavesdroppers that aim to obtain the shared key.

9.4.1 Analysis of W-HMAC

As stated previously, the W-HMAC carries the key components of the other nodes to the receiver. Then, n_j obtains the secret key with x_j and $\psi(y)$. The obtained key can

be used in security applications with the desired encryption algorithm. Eve can either obtain the secret key from the encryption algorithm or from sniffing the channel at the key generation process. The security of the encryption algorithms is not in the scope of this thesis and the security of the key generation process will be investigated in this section. Since W-HMAC uses CSI to invert the fading, Eve has to be physically present to the receiver to imitate the perfectly inverted channel. On the other hand, Eve does not know the initial key component of the receiver and requires another sniffing from the channel.

Eve requires sniffing at least two communications from W-HMAC by physically being present in order to generate the secret key. In this scenario, Eve obtains the following information from eavesdropping a single communication.

$$y_E = \sum_{\substack{i=1 \\ i \neq j}}^{N} r_{ij} \ln(x_i)$$

where $r_{ij} = {}^{h_{ij}}/_{h_{iE}}$. After applying the post processing function, Eve receives

$$\psi_E \left(\sum_{i=1, i \neq j}^{N} r_{ij} \ln(x_i) \right) = \prod_{i=1, i \neq j}^{N} x_i^{r_{ij}}$$

from the W-HMAC.

Theorem 2. *Let n_j obtain $\psi_j(y_j)$ from the W-HMAC and $r_{ij} = h_{ij}/h_{iE}$. The obtained secret key of Eve and n_j from W-HMAC is different given that $|1 - r_{ij}| \neq 0$.*

Proof. Assume that the Eve also knows the x_j. In this scenario, the difference of the received signals of n_j and Eve from the W-HMAC becomes,

$$\begin{aligned} |\psi_j(x_j, y_j) - \psi_E(x_j, y_E)| &= |x_j \exp[y_j] - x_j \exp[y_E]| \\ &= \left| \exp\left[\sum_{i=1}^{N} \ln x_i \right] - \exp\left[\sum_{i=1}^{N} r_{ij} \ln x_i \right] \right| \\ &= \prod_{i=1}^{N} p_i - \prod_{\substack{i=1 \\ i \neq j}}^{N} p^{r_{ij}} \\ &= \prod_{i=1}^{N} x_i \underbrace{\left(1 - \prod_{i=1}^{N} x_i^{r_{ij}-1} \right)}_{E_r}. \end{aligned} \tag{9.13}$$

Note that Eve will have a discrepancy once the error, E_r, is not 0 and it occurs When $|1 - r_{ij}|$ is not equal to 0, an error, E_r, occurs as shown in (9.13). As a result, a discrepancy between the received signals occur. □

Selecting high digit key components is effective against Eve since the error that Eve obtains increases with larger. The lemma given below presents the impact of the error that Eve obtains on the sniffed key.

Lemma 1. *Let m be the length of the decimal part of $s = 1.a_1a_2a_3\ldots a_m$. Let a_r be the first non-zero number of the decimal part. The multiplication n times s is the same as n for its r number of digits. However the rest of the expression is not expected to be the same.*

Proof. Let $n = n_1n_2\ldots n_d$ be a d digit number. The decimal expression:

$$n = n_1 \cdot 10^{d-1} + n_2 \cdot 10^{d-2} + \cdots + n_{d-1} \cdot 10 + n_d$$

and

$$s = 1 + a_1 \cdot \frac{1}{10} + a_2 \cdot \frac{1}{10^2} + \cdots + a_r \frac{1}{10^r} + a_{r+1} \frac{1}{10^{r+1}} + \ldots$$

where a_r occurs in the first digit that is not zero

$$a_1 = a_2 = \cdots = a_{r-1} = 0$$

and

$$s = 1 + a_r \frac{1}{10^r} + a_{r+1} \frac{1}{10^{r+1}} + \ldots$$

Then

$$\begin{aligned}
n \cdot s &= \left(n_1 \cdot 10^{d-1} + n_2 \cdot 10^{d-2} + \cdots + n_d\right) \cdot \\
&\quad \left(1 + a_1 \cdot \frac{1}{10^r} + a_2 \cdot \frac{1}{10^{r+1}} + \ldots\right) \\
&= n_1 \cdot 10^{d-1} + n_2 \cdot 10^{d-2} + \cdots + n_d \\
&\quad + n_1 \cdot 10^{d-r-1} + n_2 \cdot 10^{d-r-2} + \cdots + n_d \cdot \frac{1}{10^r} \\
&\quad + n_1 \cdot 10^{d-r-2} + n_2 \cdot 10^{d-r-3} + \cdots + n_d \cdot \frac{1}{10^{r+1}} \\
&\quad + . \\
&\quad + . \\
&\quad + . \\
&= n_1 \cdot 10^{d-1} + n_2 \cdot 10^{d-2} + \cdots + (n_{d-r-1} + n_1) \cdot \\
&\quad 10^{d-r-1} + (n_{d-r-2} + n_2 + n_1) \cdot 10^{d-r-2}.
\end{aligned}$$

Consequently, the output of the product is equal to n for its r number of digits. □

Example 1. *Assuming that each node has a prime component with a minimum of 5 digits and Eve achieves* $\psi_E(y_E)$ *with* $|r_{ij}| > 1.001$. *Lemma 1 states that the last two digits of the prime components that Eve receives will not be equal to the original components. As a result,* $\psi_E(y_E)$ *will be ultimately different from the legitimate signal* $\psi_j(y_j)$.

Example 1 gives the relation between the key generation model and the number of nodes. Since each key component exponentially increases the error, increasing the number of nodes increases the error of Eve.

9.4.2 Analysis of W-FMAC

The W-FMAC provides each node with N distinct functions of the key components. The only relation between these distinct functions is that every function contains the key components with various exponents. While the self-interference cancellation of the legitimate receiver eliminates the x_j, Eve obtains the self interferenced and distorted signal.

In addition to this statement, Eve is also unable to receive $\psi_j(y_j)$ as pointed out as follows. Assume Eve obtains

$$y_E = \sum_{\substack{i=1 \\ i \neq j}}^{N} r_{ij} \ln(x_i), \tag{9.14}$$

where $r_{ij} = {}^{h_{iE}}/_{h^*}$. Assuming that Eve knows x_j, the difference of the outputs of W-FMAC can be given as follows.

$$\begin{aligned} |\psi'_j(y_j) - \psi'_E(y_E)| &= |x_j \exp[y_j] - x_j \exp[y_E]| \\ &= \left| \exp\left[\sum_{i=1}^{N} c_{ij} \ln x_i \right] - \exp\left[\sum_{i=1}^{N} r_{ij} \ln x_i \right] \right| \\ &= \left| \prod_{i=1}^{N} x_i^{c_{ij}} - \prod_{i=1}^{N} x_i^{r_{ij}} \right|. \end{aligned} \tag{9.15}$$

Note that r_{ij} includes a dual component, c_{ij} as a whole number. If r_{ij} is substituted with $v_{ij}c_{ij}$ where $v_{ij} = r_{ij}/c_{ij}$, above expression becomes

$$= \prod_{i=1}^{N} x_i^{c_{ij}} \underbrace{\left(1 - \prod_{i=1}^{N} x_i^{c_{ij}(v_{ij}-1)} \right)}_{E_r}.$$

The above expression also satisfies Theorem 2 and it is stated that S that is generated by communication with W-FMAC is protected towards passive adversaries.

9.5 Numerical Results

The half-duplex key generation method is investigated with simulations in this section. Three realistic scenarios are considered for simulations. In the first scenario, AWGN is added to the received signal of both Eve and the legitimate nodes. Eve is assumed to have the same channel coefficient with the receiving node. In the second scenario, discrepancies are added to Eve's channel coefficient. In the third scenario, the channel estimation error is added to the transmitting nodes. The key components are selected from a Gaussian prime set $\mathscr{P} = \{a+bj\}$, $a \in (0,5)$, $b \in (0,5)$ and $a,b \in \mathbb{N}$.

Fig. 9.4 and Fig. 9.5 consider the first scenario where only Gaussian noise is added to the system. In Fig. 9.4, Mean Squared Errors (MSE) of the obtained keys are presented for $N = 3,5,7$ networks. Eve is assumed to listen to all communications in the network to generate the secret key since Eve can not obtain the legitimate receiver's key component from a single sniffing. The results show that Eve's key shows more error than the legitimate node's key. While increasing SNR reduces the MSE of the legitimate node's key, the MSE of Eve's key is not affected. Also, the MSE of both Eve and the legitimate node increase with larger N values since the size of the secret key increases for larger networks.

In Fig. 9.5, the received signals are decoded to the closest possible secret key. The figure illustrates the error probability that the obtained key is different from the actual key. Eve is assumed to generate the secret key by sniffing all communications. As seen from the figure, Eve obtains wrong secret keys with more than 80% probability for $N = 3$ and 95% probability for $N > 3$. However, legitimate nodes can successfully create secret keys with more than 95% probability at high SNR regions. The number of nodes increases the required SNR level for a constant success rate.

Fig. 9.6 considers the second scenario where discrepancies are added to Eve's channel coefficient. In the figure, the error probability of Eve and the legitimate nodes is illustrated for $N = 3$ networks. Eve is assumed to know the receiver's key component and it creates the secret key from a single sniffing since the scenario aims to investigate

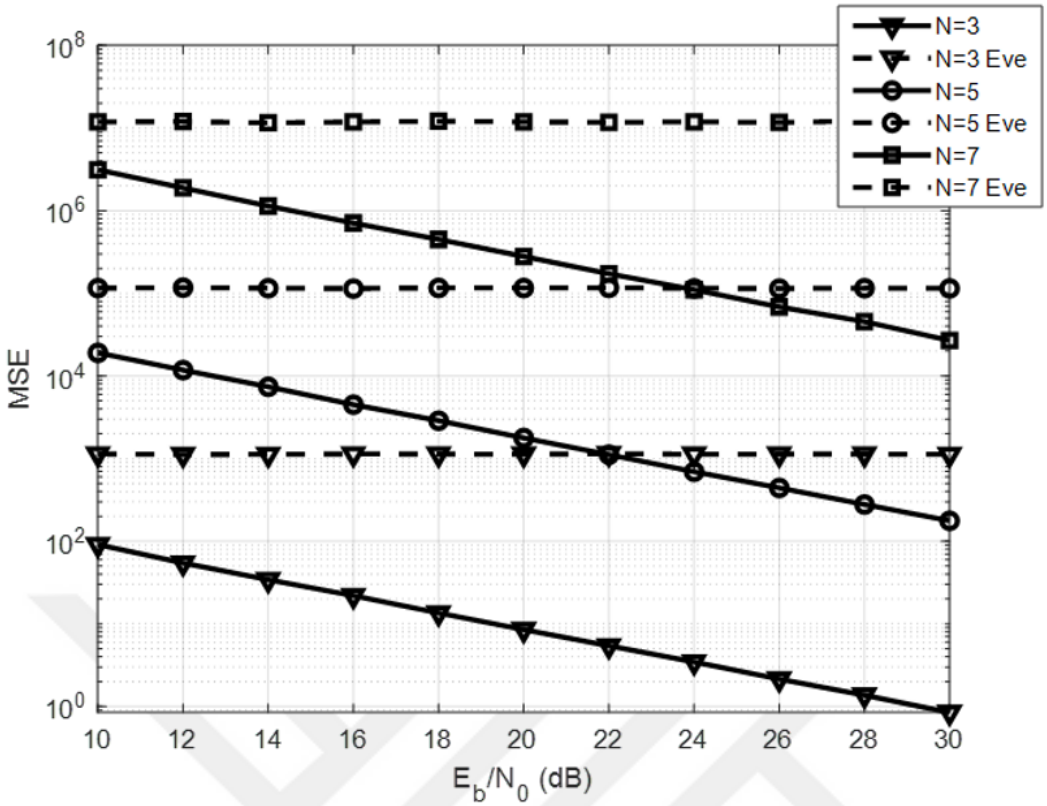


Figure 9.4 : MSE of Eve's and the legitimate node's secret key.

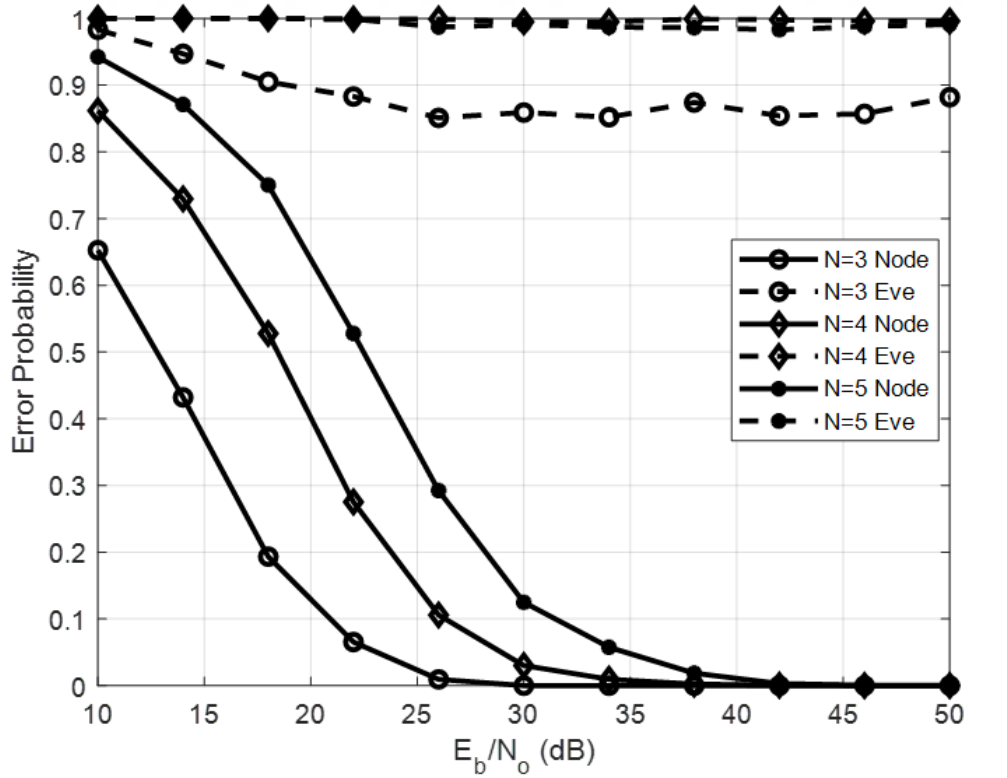


Figure 9.5 : Error probabilities of Eve and the legitimate nodes on the secret key generation with AWGN.

the effect of the channel coefficient. When a discrepancy with zero-mean $\sigma = 0.1$ Gaussian distribution is added, Eve stays above of 50% error level. However, when the energy of the discrepancy is reduced to $\sigma = 0.01$, the error floor of Eve reduces to 10%.

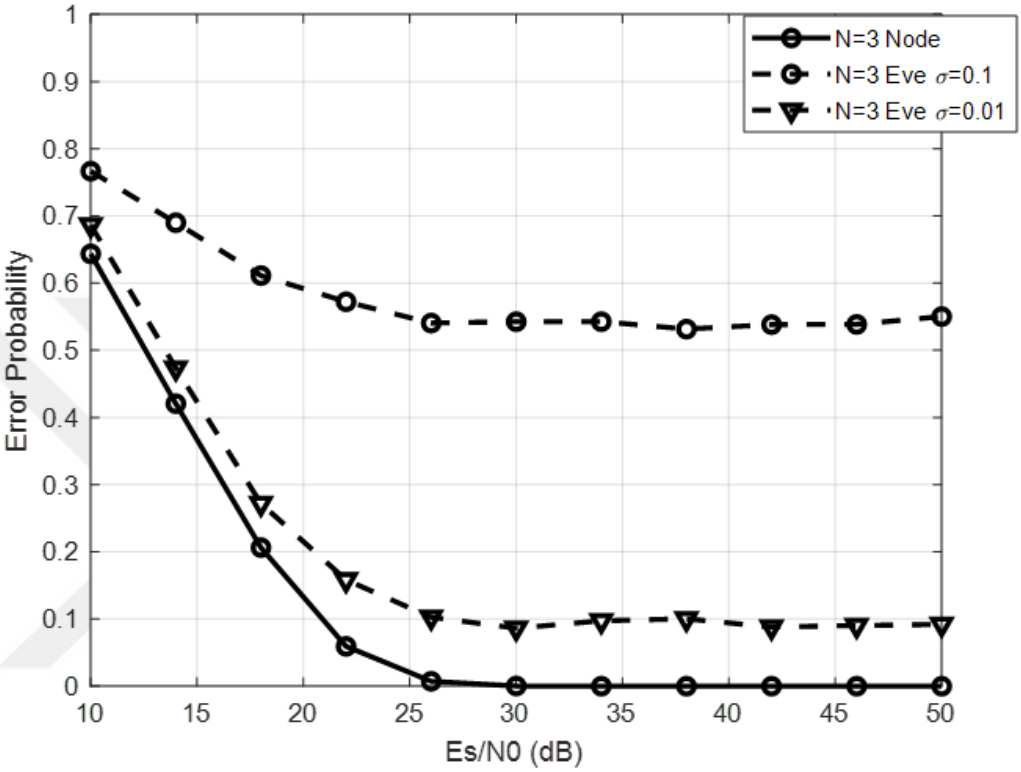


Figure 9.6 : Error probabilities of Eve and the legitimate nodes on the secret key generation with channel coefficient discrepancy.

The channel estimation error is added to the system in the third scenario. Fig. 9.7 shows the error probability of Eve and the legitimate receiver for $N = 3$. The legitimate transmitters are assumed to make a channel estimation error that is modeled with zero-mean $\sigma_{estimation}$ Gaussian distribution. The AWGN noise is added to all receivers and Eve is assumed to have $\sigma = 0.1$ discrepancy on its channel coefficient. Also, Eve is assumed to create the secret key from a single sniffing since the scenario aims to investigate the effect of the channel estimation error. When $\sigma_{estimation} = 0.01$ is added, error probability of the legitimate nodes reduces below 5% after 25 dB SNR. However, the feasibility of the proposed model is badly affected when $\sigma_{estimation} = 0.1$, since the error probability of legitimate nodes rises to 50% floor.

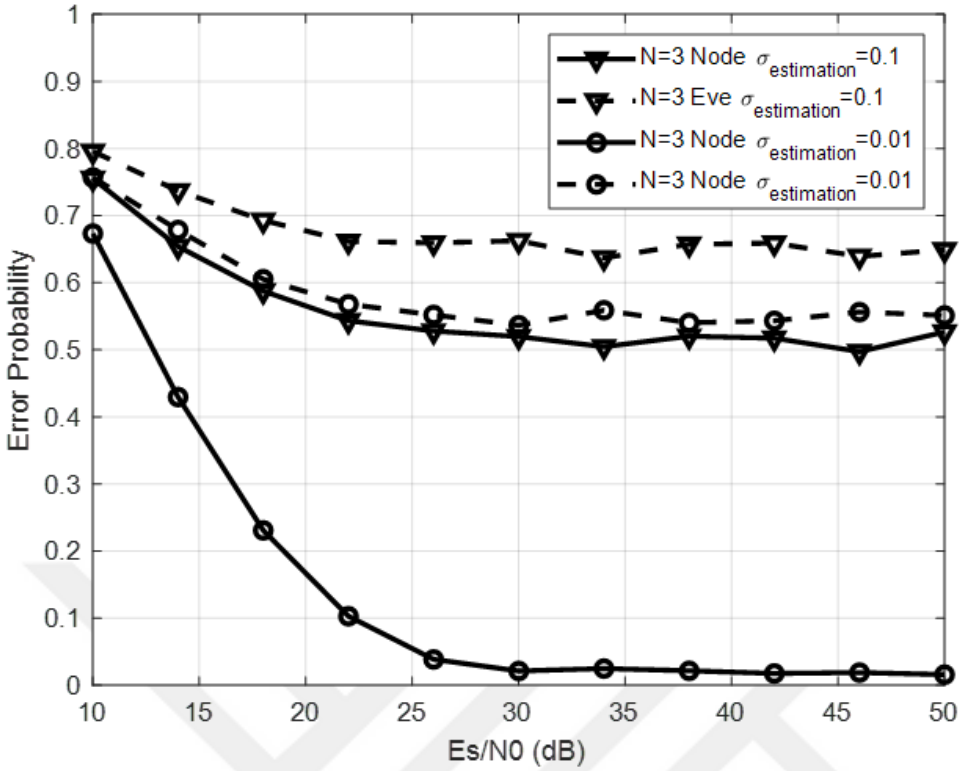


Figure 9.7 : Error probabilities of Eve and the legitimate nodes on the secret key generation with channel estimation error.

10. CONCLUSIONS

The simultaneous transmission based communication techniques are the main objective of this thesis. In the first part, an extensive literature overview is presented on the wireless applications that exploit the interference of signals. These methods are grouped depending on their applications areas and presented with detailed information. The wireless channel presents a natural weighted summation operation for the simultaneously transmitted inputs. This summation is exploited in various applications such as network coding and federated learning to perform desired tasks. From this perspective, simultaneous transmission techniques can be viewed as channel manipulations that performs a specific function over the channel. The thesis firstly investigated these functions and their applications such as multiple access, network coding, detection, security etc. The studies in each application listed along with their contributions and performance metrics.

In the second part, two network models, that is robust against active and passive attacks respectively, are presented. In the first model, a simultaneous transmission based uplink communication model is proposed. The method carries information of multiple nodes to a single receiver node. The transmission time of the network is independent of the number of nodes, since the wireless channel is used with simultaneous transmissions. The method is based on the AFC applications which lose individual information at the receiver. To overcome this problem, the wireless channel is adapted with pre and post processing functions at both ends. Gaussian prime integers are used as node identifiers to distinguish individual data at the receiver. Robustness of the proposed network against spoofing attacks is investigated in the presence of channel estimation error and thermal noise. Simulations are used to analyze the performance of the proposed methods. The results showed that the transmitted information can be successfully authenticated at the receiver without any prior secret communication or a trusted third party.

A key generation method is presented in the second model. The W-MAC is manipulated with signal processing to provide each node with a secret key without using a center node. The W-HMAC model and the W-FMAC model are given for the scenarios of half and full-duplex communication. The W-DMAC provides a secret key to N nodes by N concurrent transmission. In W-FMAC, multiple nodes agree on a secret key in a single concurrent transmission. Lastly, the secrecy of the proposed approach is investigated. The results showed that the proposed approach provides security against passive attacks.

REFERENCES

[1] **Zhang, S.**, **Liew, S.C. and Lam, P.P.** (2006). Hot topic: Physical-layer network coding, *Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM*, *2006*(Node 1), 358–365.

[2] **Shannon, C.E.** (1948). A mathematical theory of communication, *The Bell System Technical Journal*, *27*(July 1928), 379–423.

[3] **Gastpar, M. and Vetterli, M.** (2003). Source-Channel Communication in Sensor Networks, *In Information Processing in Sensor Networks Springer Berlin Heidelberg*, 162–177.

[4] **Mergen, G. and Tong, L.** (2006). Type based estimation over multiaccess channels, *IEEE Transactions on Signal Processing*, *54*(2), 613–626.

[5] **Nazer, B. and Gastpar, M.** (2007). Computation over multiple-access channels, *IEEE Transactions on Information Theory*, *53*(10), 3498–3516.

[6] **Nazer, B. and Gastpar, M.** (2011). Compute-and-forward: Harnessing interference through structured codes, *IEEE Transactions on Information Theory*, *57*(10), 6463–6486.

[7] **Goldenbaum, M.**, **Boche, H. and Stanczak, S.** (2013). Harnessing interference for analog function computation in wireless sensor networks, *IEEE Transactions on Signal Processing*, *61*(20), 4893–4906.

[8] **Sula, E.**, **Zhu, J.**, **Pastore, A.**, **Lim, S.H. and Gastpar, M.** (2019). Compute-Forward Multiple Access (CFMA): Practical Implementations, *IEEE Transactions on Communications*, *67*(2), 1133–1147.

[9] **Vatedka, S.**, **Kashyap, N. and Thangaraj, A.** (2015). Secure Compute-and-Forward in a Bidirectional Relay, *IEEE Transactions on Information Theory*, *61*(5), 2531–2556.

[10] **Goldsmith, A.** (2005). *Wireless Communications*.

[11] **Prasad, R. and Ojanpera, T.** (1998). An Overview of COMA Evolution Towards Wideband COMA, *IEEE Communications Surveys*, *1*(1), 2–29.

[12] **Prasad, R. and Ojanpera, T.** (1998). A Survey on CDMA: Evolution Towards Wideband CDMA, *IEEE*, 323–331.

[13] **Sun, S.Y.**, **Chen, H.H. and Meng, W.X.** (2015). A Survey on Complementary-Coded MIMO CDMA Wireless Communications, *IEEE Communications Surveys and Tutorials*, *17*(1), 52–69.

[14] **Islam, S.M.**, **Avazov, N.**, **Dobre, O.A. and Kwak, K.S.** (2017). Power-Domain Non-Orthogonal Multiple Access (NOMA) in 5G Systems: Potentials and Challenges, *IEEE Communications Surveys and Tutorials*, *19*(2), 721–742.

[15] **Dai, L.**, **Wang, B.**, **Jiao, R.**, **Ding, Z.**, **Han, S. and Chih-Lin, I.** (2018). A Survey of Non-Orthogonal Multiple Access for 5G, *5G Networks: Fundamental Requirements, Enabling Technologies, and Operations Management*, *20*(3), 135–203.

[16] **Makki, B.**, **Chitti, K.**, **Behravan, A. and Alouini, M.S.** (2020). A Survey of NOMA: Current Status and Open Research Challenges, *IEEE Open Journal of the Communications Society*, *1*(January), 179–189.

[17] **Jeon, H.**, **Hwang, D.**, **Member, S.**, **Choi, J. and Member, S.** (2011). Secure Type-Based Multiple Access, *6*(3), 763–774.

[18] **Mergen, G.**, **Naware, V. and Tong, L.** (2007). Asymptotic detection performance of type-based multiple access over multiaccess fading channels, *IEEE Transactions on Signal Processing*, *55*(3), 1081–1092.

[19] **Zhu, J. and Gastpar, M.** (2017). Gaussian Multiple Access via Compute-and-Forward, *IEEE Transactions on Information Theory*, *63*(5), 2678–2695.

[20] **Sula, E.**, **Zhu, J.**, **Pastore, A.**, **Lim, S.H. and Gastpar, M.** (2017). Compute-forward multiple access (CFMA) with nested LDPC codes, *IEEE International Symposium on Information Theory - Proceedings*, (2), 2935–2939.

[21] **Bassoli, R.**, **Marques, H.**, **Rodriguez, J.**, **Shum, K.W. and Tafazolli, R.** (2013). Network coding theory: A survey, *IEEE Communications Surveys and Tutorials*, *15*(4), 1950–1978.

[22] **Hu, P. and Ibnkahla, M.** (2010). A survey of physical-layer network coding in wireless networks, *2010 25th Biennial Symposium on Communications, QBSC 2010*, 311–314.

[23] **Katabi, D. and Katti, S.** (2007). XORS in the air: Practical wireless network coding, *Multi-Hop Ad Hoc Networks from Theory to Reality*, *16*(3), 225–240.

[24] **Katti, S.**, **Gollakota, S. and Katabi, D.** (2007). Embracing wireless interference: Analog Network Coding, *ACM SIGCOMM Computer Communication Review*, *37*(4), 397.

[25] **Amah, A.U.T. and Klein, A.** (2011). Non-regenerative multi-way relaying: Space-time analog network coding and repetition, *IEEE Communications Letters*, *15*(12), 1362–1364.

[26] **Wei, L. and Chen, W.** (2013). Space-time analog network coding for multiple access relay channels, *IEEE Wireless Communications and Networking Conference, WCNC*, 2961–2965.

[27] **Gündüz, D.**, **Simeone, O.**, **Goldsmith, A.J.**, **Poor, H.V. and Shamai, S.** (2010). Multiple multicasts with the help of a relay, *IEEE Transactions on Information Theory*, *56*(12), 6142–6158.

[28] **Xu, L.**, **Pan, P.**, **Wang, X. and Wu, W.** (2012). Physical-layer network coding and connected dominating set based routing protocol in wireless multi-hop network, *Proceedings of the 2012 4th International Conference on Intelligent Networking and Collaborative Systems, INCoS 2012*, 259–263.

[29] **Burr, A. and Fang, D.** (2014). Linear physical layer network coding for multihop wireless networks, *European Signal Processing Conference*, 1153–1157.

[30] **Al-Rubaie, A.A.**, **Tsimenidis, C.C.**, **Johnston, M. and Sharif, B.** (2013). Comparison of a physical-layer network coding system with iterative coding schemes, *Proceedings of 2013 6th Joint IFIP Wireless and Mobile Networking Conference, WMNC 2013*, 1–4.

[31] **Hayashi, M.** (2019). Secure physical layer network coding versus secure network coding, *2018 IEEE Information Theory Workshop, ITW 2018*, 1–5.

[32] **Ren, Z.**, **Goseling, J.**, **Weber, J.H. and Gastpar, M.** (2017). Secure Transmission on the Two-Hop Relay Channel with Scaled Compute-and-Forward, *IEEE Transactions on Information Theory*, *63*(12), 7753–7769.

[33] **Cai, N. and Chan, T.** (2011). Theory of secure network coding, *Proceedings of the IEEE*, *99*(3), 421–437.

[34] **Nazer, B. and Gastpar, M.** (2007). The Case for Structured Random Codes in Network Communication Theorems, 260–265.

[35] **Nazer, B. and Gastpar, M.** (2007). Lattice coding increases multicast rates for Gaussian multiple-access networks, *45th Annual Allerton Conference on Communication, Control, and Computing 2007*, *2*, 1089–1096.

[36] **Ning, H. and Ling, C.** (2011). Reliable Physical Layer Network Coding, *Heterogeneous Cellular Networks: Theory, Simulation and Deployment*, *9781107023*(3), 352–382.

[37] **Huang, T.**, **Yuan, J. and Sun, Q.T.** (2013). Opportunistic pair-wise compute-and-forward in multi-way relay channels, *IEEE International Conference on Communications*, 4614–4619.

[38] **Tan, Y. and Yuan, X.** (2015). Compute-compress-and-forward, *IEEE International Symposium on Information Theory - Proceedings*, 561–565.

[39] **Tan, Y. and Yuan, X.** (2016). Compute-compress-And-forward: Exploiting asymmetry of wireless relay networks, *IEEE Transactions on Signal Processing*, *64*(2), 511–524.

[40] **Nokleby, M. and Nazer, B.** (2013). Amplify-and-compute: Function computation over layered networks, *IEEE International Symposium on Information Theory - Proceedings*, 2314–2318.

[41] **Ntranos, V.**, **Cadambe, V.R.**, **Nazer, B. and Caire, G.** (2013). Asymmetric compute-and-forward, *2013 51st Annual Allerton Conference on Communication, Control, and Computing, Allerton 2013*, 1174–1181.

[42] **Tan, Y.**, **Yuan, X.**, **Liew, S.C. and Kavcic, A.** (2014). Asymmetric Compute-and-Forward: Going beyond one hop, *2014 52nd Annual Allerton Conference on Communication, Control, and Computing, Allerton 2014*, 667–674.

[43] **Pappi, K.N.**, **Diamantoulakis, P.D.**, **Otrok, H. and Karagiannidis, G.K.** (2015). Cloud compute-and-forward with relay cooperation, *IEEE Transactions on Wireless Communications*, *14*(6), 3415–3428.

[44] **El Soussi, M.**, **Zaidi, A. and Vandendorpe, L.** (2014). Compute-and-forward on a multiaccess relay channel: Coding and symmetric-rate optimization, *IEEE Transactions on Wireless Communications*, *13*(4), 1932–1947.

[45] **Ordentlich, O.**, **Erez, U. and Nazer, B.** (2014). The approximate sum capacity of the symmetric gaussian K -User interference channel, *IEEE Transactions on Information Theory*, *60*(6), 3450–3482.

[46] **Zhu, J. and Gastpar, M.** (2015). Compute-and-forward using nested linear codes for the Gaussian MAC, *2015 IEEE Information Theory Workshop, ITW 2015*, (3), 1–5.

[47] **Wang, G.**, **Xiang, W. and Yuan, J.** (2012). Outage performance for compute-and-forward in generalized multi-way relay channels, *IEEE Communications Letters*, *16*(12), 2099–2102.

[48] **Song, Y.**, **Devroye, N. and Nazer, B.** (2011). Inverse compute-and-forward: Extracting messages from simultaneously transmitted equations, *IEEE International Symposium on Information Theory - Proceedings*, 415–419.

[49] **Chen, Y.**, **Song, Y. and Devroye, N.** (2013). The capacity region of three user Gaussian inverse-compute-and-forward channels, *IEEE International Symposium on Information Theory - Proceedings*, 1476–1480.

[50] **Huang, Y.C.**, **Tunali, N.E. and Narayanan, K.R.** (2013). A compute-and-forward scheme for gaussian bi-directional relaying with inter-symbol interference, *IEEE Transactions on Communications*, *61*(3), 1011–1019.

[51] **Zhu, J. and Gastpar, M.** (2013). Lattice codes for many-to-one cognitive interference networks, *IEEE International Symposium on Information Theory - Proceedings*, 2234–2238.

[52] **Nazer, B. and Gastpar, M.** (2014). Compute-and-forward for discrete memoryless networks, *2014 IEEE Information Theory Workshop, ITW 2014*, 5–9.

[53] **Lim, S.H.**, **Feng, C.**, **Nazer, B. and Gastpar, M.** (2016). A joint typicality approach to compute-forward, *2015 53rd Annual Allerton Conference on Communication, Control, and Computing, Allerton 2015*, 1294–1301.

[54] **Lim, S.H.**, **Feng, C.**, **Pastore, A.**, **Nazer, B. and Gastpar, M.** (2017). Towards an algebraic network information theory: Simultaneous joint typicality decoding, *IEEE International Symposium on Information Theory - Proceedings*, 1818–1822.

[55] **Lim, S.H.**, **Feng, C.**, **Pastore, A.**, **Nazer, B. and Gastpar, M.** (2018). A joint typicality approach to compute-forward, *IEEE Transactions on Information Theory*, *64*(12), 7657–7685.

[56] **Lim, S.H.**, **Feng, C.**, **Pastore, A.**, **Nazer, B. and Gastpar, M.** (2019). Towards an Algebraic Network Information Theory: Distributed Lossy Computation of Linear Functions, *IEEE International Symposium on Information Theory - Proceedings*, 1827–1831.

[57] **Pappi, K.N.**, **Karagiannidis, G.K. and Schober, R.** (2013). How sensitive is compute-and-forward to channel estimation errors?, *IEEE International Symposium on Information Theory - Proceedings*, (1), 3110–3114.

[58] **Ordentlich, O.**, **Erez, U. and Nazer, B.** (2015). On compute-and-forward with feedback, *2015 IEEE Information Theory Workshop, ITW 2015*, 1–5.

[59] **Hong, S.N. and Caire, G.** (2011). Quantized compute and forward: A low-complexity architecture for distributed antenna systems, *2011 IEEE Information Theory Workshop, ITW 2011*, 420–424.

[60] **Hong, S.N. and Caire, G.** (2012). Reverse compute and forward: A low-complexity architecture for downlink distributed antenna systems, *IEEE International Symposium on Information Theory - Proceedings*, 1147–1151.

[61] **Hong, S.n. and Caire, G.** (2013). Compute-and-Forward Strategies for Cooperative, *59*(9), 5227–5243.

[62] **Liu, W.** (2014). Compute-and-forward for two-way relay, *2014 9th International Symposium on Communication Systems, Networks and Digital Signal Processing, CSNDSP 2014*, 465–468.

[63] **Tunali, N.E.**, **Narayanan, K.R.**, **Boutros, J.J. and Huang, Y.C.** (2012). Lattices over Eisenstein integers for compute-and-forward, *2012 50th Annual Allerton Conference on Communication, Control, and Computing, Allerton 2012*, 33–40.

[64] **Tunali, N.E.**, **Huang, Y.C.**, **Boutros, J.J. and Narayanan, K.R.** (2015). Lattices over Eisenstein Integers for Compute-and-Forward, *IEEE Transactions on Information Theory*, *61*(10), 5306–5321.

[65] **Wang, Y. and Burr, A.** (2014). Physical-layer network coding via low density lattice codes, *EuCNC 2014 - European Conference on Networks and Communications*, (Ldlc), 1–5.

[66] **Mejri, A.**, **Othman, G.R.B. and Belfiore, J.C.** (2012). Lattice decoding for the compute-and-forward protocol, *3rd International Conference on Communications and Networking, ComNet 2012*, 1–8.

[67] **Mejri, A. and Rekaya-Ben Othman, G.** (2015). Efficient decoding algorithms for the compute-and-forward strategy, *IEEE Transactions on Communications*, *63*(7), 2475–2485.

[68] **Wei, L. and Chen, W.** (2012). Efficient compute-and-forward network codes search for two-way relay channel, *IEEE Communications Letters*, *16*(8), 1204–1207.

[69] **Niesen, U. and Whiting, P.** (2012). The degrees of freedom of compute-and-forward, *IEEE Transactions on Information Theory*, *58*(8), 5214–5232.

[70] **Feng, C.**, **Silva, D. and Kschischang, F.R.** (2012). Blind compute-and-forward, *IEEE International Symposium on Information Theory - Proceedings*, 403–407.

[71] **Feng, C.**, **Silva, D.**, **Kschischang, F.R. and C, A.C.a.f.** (2016). Blind Compute-and-Forward, *64*(4), 1451–1463.

[72] **Najafi, H.**, **Damen, M.O. and Member, S.** (2013). Asynchronous Compute-and-Forward, *61*(7), 2704–2712.

[73] **Sakzad, A.**, **Viterbo, E.**, **Boutros, J. and Hong, Y.** (2014). Phase precoded compute-and-forward with partial feedback, *IEEE International Symposium on Information Theory - Proceedings*, 2117–2121.

[74] **Wen, J.**, **Zhou, B.**, **Mow, W.H. and Chang, X.W.** (2015). Compute-and-forward protocol design based on improved sphere decoding, *IEEE International Conference on Communications*, 1631–1636.

[75] **Nokleby, M. and Aazhang, B.** (2016). Cooperative Compute-and-Forward, *15*(1), 14–27.

[76] **Goldenbaum, M.**, **Jung, P.**, **Raceala-Motoc, M.**, **Schreck, J.**, **Stanczak, S. and Zhou, C.** (2016). Harnessing channel collisions for efficient massive access in 5G networks: A step forward to practical implementation, *International Symposium on Turbo Codes and Iterative Information Processing, ISTC*, 335–339.

[77] **Zhu, J. and Gastpar, M.** (2017). Typical sumsets of lattice points, *Conference Record - Asilomar Conference on Signals, Systems and Computers*, 1816–1820.

[78] **Huang, Q. and Burr, A.** (2016). Low complexity coefficient selection algorithms for compute-and-forward, *IEEE Vehicular Technology Conference*, 1–5.

[79] **Huang, Q. and Burr, A.** (2017). Low Complexity Coefficient Selection Algorithms for Compute-and-Forward, *IEEE Access*, *5*, 19182–19193.

[80] **Huang, Q. and Burr, A.** (2017). Compute-and-forward in cell-free massive MIMO: Great performance with low backhaul load, *2017 IEEE International Conference on Communications Workshops, ICC Workshops 2017*, 601–606.

[81] **Goseling, J.**, **Gastpar, M. and Weber, J.H.** (2013). Physical-layer network coding on the random-access channel, *IEEE International Symposium on Information Theory - Proceedings*, 2339–2343.

[82] **Goseling, J.** (2014). A random access scheme with physical-layer network coding and user identification, *2014 IEEE International Conference on Communications Workshops, ICC 2014*, 507–512.

[83] **Wei, L. and Chen, W.** (2012). Compute-and-forward network coding design over multi-source multi-relay channels, *IEEE Transactions on Wireless Communications*, *11*(9), 3348–3357.

[84] **Goseling, J.**, **Weber, J.H. and Gastpar, M.** (2012). Compute-and-forward on wireless lattice networks with local interference, *Proceedings of the International Symposium on Wireless Communication Systems*, 281–285.

[85] **Aguerri, I.E. and Zaidi, A.** (2016). Compute-remap-compress-and-forward for limited backhaul uplink multicell processing, *2016 IEEE International Conference on Communications, ICC 2016*, 1–6.

[86] **Soussi, M.E.**, **Zaidi, A. and Vandendorpe, L.** (2014). Compute-and-Forward on a Multi-User Multi-Relay Channel, *3*(6), 589–592.

[87] **Tseng, T.Y.**, **Lee, C.P.**, **Lin, S.C. and Su, H.J.** (2014). Non-orthogonal compute-and-forward with joint lattice decoding for the multiple-access relay channel, *2014 IEEE Globecom Workshops*, 924–929.

[88] **Jeon, S.W.**, **Choi, S.W.**, **Kim, J. and Shin, W.Y.** (2016). Cellular-Aided Device-to-Device Communication: The Benefit of Physical Layer Network Coding, *IEEE Communications Letters*, *20*(11), 2324–2327.

[89] **Jlassi, A.**, **Slama, L.B.H.**, **Zaidi, A. and Cherif, S.** (2016). Compute-and-forward on compound multiple access relay channel, *2015 5th International Conference on Communications and Networking, COMNET 2015 - Proceedings*, 1–8.

[90] **Hasan, M.N. and Kurkoski, B.M.** (2017). Practical compute-and-forward approaches for the multiple access relay channel, *IEEE International Conference on Communications*, 1–6.

[91] **Jlassi, A.**, **Slama, L.B.H.**, **Zaidi, A. and Cherif, S.** (2018). Compute-and-forward on Gaussian interference relay channel, *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*, 1–5.

[92] **Cover, T.M. and Thomas, J.A.** (2005). *Elements of Information Theory*.

[93] **Hejazi, M. and Nasiri-Kenari, M.** (2013). Simplified compute-and-forward and its performance analysis, *IET Communications*, *7*(18), 2054–2063.

[94] **Hejazi, M.**, **Azimi-Abarghouyi, S.M.**, **Makki, B.**, **Nasiri-Kenari, M. and Svensson, T.** (2016). Robust Successive Compute-And-Forward over Multiuser Multirelay Networks, *IEEE Transactions on Vehicular Technology*, *65*(10), 8112–8129.

[95] **Sahraei, S. and Gastpar, M.** (2014). Compute-and-forward: Finding the best equation, *2014 52nd Annual Allerton Conference on Communication, Control, and Computing, Allerton 2014*, 227–233.

[96] **Sahraei, S. and Gastpar, M.** (2017). Polynomially Solvable Instances of the Shortest and Closest Vector Problems with Applications to Compute-and-Forward, *IEEE Transactions on Information Theory*, *63*(12), 7780–7792.

[97] **Vázquez-Castro, M.A.** (2014). Arithmetic geometry of compute and forward, *2014 IEEE Information Theory Workshop, ITW 2014*, 122–126.

[98] **Ordentlich, O., Erez, U. and Nazer, B.** (2012). The compute-and-forward transform, *IEEE International Symposium on Information Theory - Proceedings*, 3008–3012.

[99] **Ashrafi, S., Feng, C. and Roy, S.** (2018). Compute-and-Forward for Random-Access: The Case of Multiple Access Points, *IEEE Transactions on Communications*, *66*(8), 3434–3443.

[100] **Soundararajan, R. and Vishwanath, S.** (2012). Communicating linear functions of correlated Gaussian Sources over a MAC, *IEEE Transactions on Information Theory*, *58*(3), 1853–1860.

[101] **Jeon, S.W., Wang, C.Y. and Gastpar, M.** (2013). Computation over Gaussian networks with orthogonal components, *IEEE International Symposium on Information Theory - Proceedings*, 2139–2143.

[102] **Jeon, S.w., Wang, C.y. and Gastpar, M.** (2014). Computation Over Gaussian Networks With Orthogonal Components, *60*(12), 7841–7861.

[103] **Wu, X., Zhang, S. and Ozgur, A.** (2016). STAC: Simultaneous Transmitting and Air Computing in Wireless Data Center Networks, *IEEE Journal on Selected Areas in Communications*, *34*(12), 4024–4034.

[104] **Zhang, S., Wu, X. and Ozgur, A.** (2016). STAC: Simultaneous transmitting and air computing in wireless data center networks, *2015 IEEE/CIC International Conference on Communications in China, ICCC 2015*, 1–7.

[105] **Goldenbaum, M., Boche, H. and Stanczak, S.** (2013). Reliable computation of nomographic functions over Gaussian multiple-access channels, *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, 4814–4818.

[106] **Goldenbaum, M., Boche, H. and Stanczak, S.** (2015). Nomographic functions: Efficient computation in clustered gaussian sensor networks, *IEEE Transactions on Wireless Communications*, *14*(4), 2093–2105.

[107] **Jeon, S.W. and Jung, B.C.** (2015). Opportunistic in-network computation for wireless sensor networks, *IEEE International Symposium on Information Theory - Proceedings*, (1), 1856–1860.

[108] **Jeon, S.W. and Jung, B.C.** (2016). Opportunistic Function Computation for Wireless Sensor Networks, *IEEE Transactions on Wireless Communications*, *15*(6), 4045–4059.

[109] **Wu, F.**, **Chen, L. and Wei, G.** (2019). Sub-function superposition for computation over NOMA, *2019 IEEE International Conference on Communications Workshops, ICC Workshops 2019 - Proceedings*, 1–6.

[110] **Wu, F.**, **Chen, L.**, **Zhao, N.**, **Chen, Y.**, **Yu, F.R. and Wei, G.** (2020). NOMA-Enhanced Computation Over Multi-Access Channels, *IEEE Transactions on Wireless Communications*, *1276*(c), 1–1.

[111] **Wu, F.**, **Chen, L. and Wei, G.** (2019). Sub-Function Allocation for Computation over Wide-Band MAC, *IEEE Wireless Communications and Networking Conference, WCNC*, 1–6.

[112] **Wu, F.**, **Chen, L.**, **Zhao, N.**, **Chen, Y.**, **Yu, F.R. and Wei, G.** (2019). Computation over wide-band multi-access channels: Achievable rates through sub-function allocation, *IEEE Transactions on Wireless Communications*, *18*(7), 3713–3725.

[113] **Zhan, J.**, **Park, S.Y.**, **Gastpar, M. and Sahai, A.** (2011). Function computation in networks: Duality and constant gap results, *2011 49th Annual Allerton Conference on Communication, Control, and Computing, Allerton 2011*, 1470–1477.

[114] **Zhu, J.**, **Lim, S.H. and Gastpar, M.** (2017). On the duality between multiple-access codes and computation codes, *2017 Information Theory and Applications Workshop, ITA 2017*, *2*(1).

[115] **Zhu, J.**, **Lim, S.H. and Gastpar, M.** (2019). Communication versus computation: Duality for multiple-access channels and source coding, *IEEE Transactions on Information Theory*, *65*(1), 292–301.

[116] **Goldenbaum, M.**, **Stańczak, S. and Kaliszan, M.** (2009). On function computation via wireless sensor multiple-access channels, *IEEE Wireless Communications and Networking Conference, WCNC*.

[117] **Goldenbaum, M. and Stańczak, S.** (2010). Computing the geometric mean over multiple-access channels: Error analysis and comparisons, *Conference Record - Asilomar Conference on Signals, Systems and Computers*, 2172–2178.

[118] **Stańczak, S.**, **Goldenbaum, M.**, **Cavalcante, R.L. and Penna, F.** (2012). On in-network computation via wireless multiple-access channels with applications, *Proceedings of the International Symposium on Wireless Communication Systems*, 276–280.

[119] **Goldenbaum, M. and Stanczak, S.** (2013). Robust analog function computation via wireless multiple-access channels, *IEEE Transactions on Communications*, *61*(9), 3863–3877.

[120] **Goldenbaum, M. and Stańczak, S.** (2014). On the channel estimation effort for analog computation over wireless multiple-access channels, *IEEE Wireless Communications Letters*, *3*(3), 261–264.

[121] **Jeon, S.W. and Jung, B.C.** (2018). Adaptive Analog Function Computation via Fading Multiple-Access Channels, *IEEE Communications Letters*, *22*(1), 213–216.

[122] **Chen, L.**, **Zhao, N.**, **Chen, Y.**, **Yu, F.R. and Wei, G.** (2018). Over-the-Air Computation for IoT Networks: Computing Multiple Functions with Antenna Arrays, *IEEE Internet of Things Journal*, *5*(6), 5296–5306.

[123] **Chen, L.**, **Qin, X. and Wei, G.** (2018). A uniform-forcing transceiver design for over-the-air function computation, *IEEE Wireless Communications Letters*, *7*(6), 942–945.

[124] **Limmer, S. and Stańczak, S.** (2014). On p-norm computation over multiple-access channels, *2014 IEEE Information Theory Workshop, ITW 2014*, (i), 351–355.

[125] **Huang, J.**, **Zhang, Q.**, **Li, Q. and Qin, J.** (2015). Robust parallel analog function computation via wireless multiple-access MIMO channels, *IEEE Signal Processing Letters*, *22*(9), 1297–1301.

[126] **Zhu, G.**, **Chen, L. and Huang, K.** (2018). MIMO Over-the-Air Computation: Beamforming Optimization on the Grassmann Manifold, *2018 IEEE Global Communications Conference, GLOBECOM 2018 - Proceedings*, 1–6.

[127] **Zhu, G.**, **Member, S.**, **Huang, K. and Member, S.** (2019). MIMO Over-the-Air Computation for High-Mobility Multimodal Sensing, *6*(4), 6089–6103.

[128] **Farajzadeh, A.**, **Ercetin, w.O. and Yanikomeroglu, w.H.** (2020). Mobility-assisted Over-the-Air Computation for Backscatter Sensor Networks, *IEEE Wireless Communications Letters*, *2337*(c), 1–1.

[129] **Wen, D.**, **Zhu, G. and Huang, K.** (2019). Reduced-Dimension Design of MIMO Over-the-Air Computing for Data Aggregation in Clustered IoT Networks, *IEEE Transactions on Wireless Communications*, *18*(11), 5255–5268.

[130] **Ang, F. and Chen, L.** (2019). An Efficient Training Scheme to Acquire Massive CSI in Analog Function Computation Networks, *IEEE Wireless Communications and Networking Conference, WCNC*, 1–6.

[131] **Ang, F.**, **Chen, L.**, **Zhao, N.**, **Chen, Y. and Yu, F.R.** (2019). Robust Design for Massive CSI Acquisition in Analog Function Computation Networks, *IEEE Transactions on Vehicular Technology*, *68*(3), 2361–2373.

[132] **Li, X.**, **Zhu, G.**, **Gong, Y. and Huang, K.** (2019). Wirelessly powered data aggregation for IoT via over-the-air function computation: Beamforming and power control, *IEEE Transactions on Wireless Communications*, *18*(7), 3437–3452.

[133] **Li, X.**, **Zhu, G.**, **Gong, Y. and Huang, K.** (2019). Wirelessly Powered Over-the-Air Computation for High-Mobility Sensing, *2018 IEEE Globecom Workshops - Proceedings*, 1–6.

[134] **Cao, X.**, **Zhu, G.**, **Xu, J. and Huang, K.** (2019). Optimal power control for over-the-air computation, *2019 IEEE Global Communications Conference, GLOBECOM 2019 - Proceedings*, 1–6.

[135] **Basaran, S.T.**, **Kurt, G.K. and Chatzimisios, P.** (2020). Energy-Efficient Over-the-Air Computation Scheme for Densely Deployed IoT Networks, *IEEE Transactions on Industrial Informatics*, *16*(5), 3558–3565.

[136] **Limmer, S.**, **Mohammadi, J. and Stanczak, S.** (2016). A simple algorithm for approximation by nomographic functions, *2015 53rd Annual Allerton Conference on Communication, Control, and Computing, Allerton 2015*, (1), 453–458.

[137] **Goldenbaum, M.**, **Stanczak, S. and Boche, H.** (2015). On achievable rates for analog computing real-valued functions over the wireless channel, *IEEE International Conference on Communications*, 4036–4041.

[138] **Wang, L.**, **Wang, X. and Jiang, G.** (2015). Computation over fading multiple-access channels based on free deconvolution, *IET Wireless Sensor Systems*, *5*(6), 283–289.

[139] **Dong, J.**, **Shi, Y. and Ding, Z.** (2020). Blind over-the-air computation and data fusion via provable wirtinger flow, *IEEE Transactions on Signal Processing*, *68*, 1136–1151.

[140] **Chen, L.**, **Zhao, N.**, **Chen, Y.**, **Yu, F.R. and Wei, G.** (2019). Communicating or Computing over the MAC: Function-Centric Wireless Networks, *IEEE Transactions on Communications*, *67*(9), 6127–6138.

[141] **Jakimovski, P.**, **Becker, F.**, **Sigg, S.**, **Schmidtke, H.R. and Beigl, M.** (2011). Collective communication for dense sensing environments, *Proceedings - 2011 7th International Conference on Intelligent Environments, IE 2011*, 157–164.

[142] **Sigg, S.**, **Jakimovski, P. and Beigl, M.** (2012). Calculation of functions on the RF-channel for IoT, *Proceedings of 2012 International Conference on the Internet of Things, IOT 2012*, 107–113.

[143] **Kortke, A.**, **Goldenbaum, M. and Stánczak, S.** (2014). Analog computation over the wireless channel: A proof of concept, *Proceedings of IEEE Sensors*, 1224–1227.

[144] **Abari, O.**, **Rahul, H.**, **Katabi, D. and Pant, M.** (2015). AirShare: Distributed coherent transmission made seamless, *Proceedings - IEEE INFOCOM*, *26*, 1742–1750.

[145] **Altun, U.**, **Başaran, S.T.**, **Alakoca, H. and Kurt, G.K.** (2018). A testbed based verification of joint communication and computation systems, *2017 25th Telecommunications Forum, TELFOR 2017 - Proceedings*, 1–4.

[146] **Anderson, G.W.**, **Guionnet, A. and Zeitouni, O.** (2009). *An Introduction to Random Matrices*, Cambridge Studies in Advanced Mathematics, Cambridge University Press.

[147] **Liu, K. and Sayeed, A.M.** (2007). Type-based decentralized detection in wireless sensor networks, *IEEE Transactions on Signal Processing*, *55*(5 I), 1899–1910.

[148] **Li, W. and Dai, H.** (2007). Distributed detection in wireless sensor networks using a multiple access channel, *IEEE Transactions on Signal Processing*, *55*(3), 822–833.

[149] **Li, F.**, **Evans, J.S. and Dey, S.** (2012). Design of distributed detection schemes for multiaccess channels, *IEEE Transactions on Aerospace and Electronic Systems*, *48*(2), 1552–1569.

[150] **Banavar, M.K.**, **Smith, A.D.**, **Tepedelenlioğlu, C. and Spanias, A.** (2012). On the effectiveness of multiple antennas in distributed detection over fading MACs, *IEEE Transactions on Wireless Communications*, *11*(5), 1744–1752.

[151] **Ralinovski, K.**, **Goldenbaum, M. and Stańczak, S.** (2016). Energy-efficient classification for anomaly detection: The wireless channel as a helper, *2016 IEEE International Conference on Communications, ICC 2016*.

[152] **Raceala-Motoc, M.**, **Limmer, S.**, **Bjelakovic, I. and Stanczak, S.** (2019). Distributed Machine Learning in the Context of Function Computation over Wireless Networks, *Conference Record - Asilomar Conference on Signals, Systems and Computers*, 291–297.

[153] **Xiao, J.**, **Cui, S.**, **Luo, Z.Q. and Goldsmith, A.** (2006). Linear coherent decentralized estimation, *GLOBECOM - IEEE Global Telecommunications Conference*, *56*(2), 757–770.

[154] **Bajwa, W.U.**, **Haupt, J.D.**, **Sayeed, A.M. and Nowak, R.D.** (2007). Joint source-channel communication for distributed estimation in sensor networks, *IEEE Transactions on Information Theory*, *53*(10), 3629–3653.

[155] **Wang, X. and Yang, C.** (2010). Type-based multiple-access with bandwidth extension for the decentralized estimation in wireless sensor networks, *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, (1), 2914–2917.

[156] **Spanias, A.** (2010). Feedback Using Distributed Sensing, *Channels*, *58*(1), 414–425.

[157] **Savage, N.** (2005). Cognitive radio: Brain-Empowered Wireless Communications, *Technology Review*, *109*(1), 61–62.

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

[159] **Zheng, M.**, **Xu, C.**, **Liang, W.**, **Yu, H. and Chen, L.** (2015). A Novel CoMAC-based cooperative spectrum sensing scheme in cognitive radio networks, *2015 IEEE International Conference on Communication Workshop, ICCW 2015*, 1009–1013.

[160] **Zheng, M.**, **Chen, L.**, **Liang, W.**, **Yu, H. and Wu, J.** (2017). Energy-Efficiency Maximization for Cooperative Spectrum Sensing in Cognitive Sensor Networks, *IEEE Transactions on Green Communications and Networking*, *1*(1), 29–39.

[161] **Chen, L.**, **Zhao, N.**, **Chen, Y.**, **Yu, F.R. and Wei, G.** (2018). Over-the-air computation for cooperative wideband spectrum sensing and performance analysis, *IEEE Transactions on Vehicular Technology*, *67*(11), 10603–10614.

[162] **Mietzner, J.**, **Schober, R.**, **Lampe, L.**, **Gerstacker, W. and Hoeher, P.** (2009). Multiple-antenna techniques for wireless communications - A comprehensive literature survey, *IEEE Communications Surveys and Tutorials*, *11*(2), 87–105.

[163] **Agiwal, M.**, **Roy, A. and Saxena, N.** (2016). Next generation 5G wireless networks: A comprehensive survey, *IEEE Communications Surveys and Tutorials*, *18*(3), 1617–1655.

[164] **Castañeda, E.**, **Silva, A.**, **Gameiro, A. and Kountouris, M.** (2017). An Overview on Resource Allocation Techniques for Multi-User MIMO Systems, *IEEE Communications Surveys and Tutorials*, *19*(1), 239–284.

[165] **Xu, C.**, **Sugiura, S.**, **Ng, S.X.**, **Zhang, P.**, **Wang, L. and Hanzo, L.** (2017). Two Decades of MIMO Design Tradeoffs and Reduced-Complexity MIMO Detection in Near-Capacity Systems, *IEEE Access*, *5*, 18564–18632.

[166] **Chen, X.**, **Ng, D.W.K.**, **Gerstacker, W.H. and Chen, H.H.** (2017). A Survey on Multiple-Antenna Techniques for Physical Layer Security, *IEEE Communications Surveys and Tutorials*, *19*(2), 1027–1053.

[167] **Yang, S. and Hanzo, L.** (2015). Fifty years of MIMO detection: The road to large-scale MIMOs, *IEEE Communications Surveys and Tutorials*, *17*(4), 1941–1988.

[168] **Zhan, J.**, **Nazer, B.**, **Erez, U. and Gastpar, M.** (2010). Integer-forcing linear receivers, *IEEE International Symposium on Information Theory - Proceedings*, 1022–1026.

[169] **Zhan, J.**, **Nazer, B.**, **Erez, U. and Gastpar, M.C.** (2012). Integer-forcing architectures: An overview, *5th International Symposium on Communications Control and Signal Processing, ISCCSP 2012*, 1–2.

[170] **Zhan, J.**, **Erez, U.**, **Gastpar, M. and Nazer, B.** (2011). Mitigating interference with integer-forcing architectures, *IEEE International Symposium on Information Theory - Proceedings*, 1673–1677.

[171] **Ordentlich, O.**, **Erez, U. and Nazer, B.** (2013). Successive integer-forcing and its sum-rate optimality, *2013 51st Annual Allerton Conference on Communication, Control, and Computing, Allerton 2013*, 282–292.

[172] **Zhao, N.**, **Richard Yu, F.**, **Jin, M.**, **Yan, Q. and Leung, V.C.** (2016). Interference Alignment and Its Applications: A Survey, Research Issues, and Challenges, *IEEE Communications Surveys and Tutorials*, *18*(3), 1779–1803.

[173] **Ayach, O.E. and Heath, R.W.** (2013). Interference alignment - Recent results and future directions, *IEEE Radio and Wireless Symposium, RWS*, 205–207.

[174] **Niesen, U.**, **Nazer, B. and Whiting, P.** (2013). Computation alignment: Capacity approximation without noise accumulation, *IEEE Transactions on Information Theory*, *59*(6), 3811–3832.

[175] **Niesen, U.**, **Nazer, B. and Whiting, P.** (2011). Computation alignment: Capacity approximation without noise accumulation, *2011 49th Annual Allerton Conference on Communication, Control, and Computing, Allerton 2011*, 1607–1612.

[176] **Goela, N.**, **Suh, C. and Gastpar, M.** (2012). Network coding with computation alignment, *2012 IEEE Information Theory Workshop, ITW 2012*, 507–511.

[177] **Suh, C.**, **Goela, N. and Gastpar, M.** (2012). Computation in multicast networks: Function alignment and converse theorems, *2012 50th Annual Allerton Conference on Communication, Control, and Computing, Allerton 2012*, 1049–1056.

[178] **Suh, C.**, **Goela, N. and Gastpar, M.** (2016). Computation in multicast networks: Function alignment and converse theorems, *IEEE Transactions on Information Theory*, *62*(4), 1866–1877.

[179] **Suh, C. and Gastpar, M.** (2013). Interactive function computation, *IEEE International Symposium on Information Theory - Proceedings*, 2329–2333.

[180] **Suh, C. and Gastpar, M.** (2013). Network decomposition for function computation, *IEEE Workshop on Signal Processing Advances in Wireless Communications, SPAWC*, 340–344.

[181] **Bross, S.I. and Laufer, Y.** (2016). Sending a bivariate Gaussian source over a Gaussian MAC with unidirectional conferencing encoders, *IEEE Transactions on Information Theory*, *62*(3), 1296–1311.

[182] **Song, L.**, **Chen, J. and Tian, C.** (2015). Broadcasting Correlated Vector Gaussians, *IEEE Transactions on Information Theory*, *61*(5), 2465–2477.

[183] **Olfati-Saber, R.**, **Fax, J.A. and Murray, R.M.** (2007). Consensus and cooperation in networked multi-agent systems, *Proceedings of the IEEE*, *95*(1), 215–233.

[184] **Kirti, S.**, **Scaglione, A. and Thomas, R.J.** (2007). A Scalable Wireless Communication Architecture for Average Consensus, *Proc. IEEE Conference on Decision and Control*, 32–37.

[185] **Goldenbaum, M.**, **Boche, H. and Sta, S.** (2012). Nomographic Gossiping for f -Consensus, 14–18.

[186] **Steffens, C. and Pesavento, M.** (2012). A physical layer average consensus algorithm for wireless sensor networks, *2012 16th International ITG Workshop on Smart Antennas, WSA 2012*, 70–77.

[187] **Nazer, B.**, **Dimakis, A.G. and Gastpar, M.** (2009). Neighborhood gossip: Concurrent averaging through local interference, *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, 3657–3660.

[188] **Nazer, B.**, **Dimakis, A.G. and Gastpar, M.** (2011). Local interference can accelerate gossip algorithms, *IEEE Journal on Selected Topics in Signal Processing*, *5*(4), 876–887.

[189] **Nokleby, M.**, **Bajwa, W.U.**, **Calderbank, R. and Aazhang, B.** (2011). Gossiping in groups: Distributed averaging over the wireless medium, *2011 49th Annual Allerton Conference on Communication, Control, and Computing, Allerton 2011*, 1242–1249.

[190] **Molinari, F. and Sta, S.** (2018). Exploiting the Superposition Property of Wireless Communication For Average Consensus Problems in Multi-Agent Systems, 1766–1772.

[191] **Agrawal, N.**, **Frey, M. and Stanczak, S.** (2019). A Scalable Max-Consensus Protocol for Noisy Ultra-Dense Networks, *IEEE Workshop on Signal Processing Advances in Wireless Communications, SPAWC*, *2019-July*, 2–6.

[192] **Zhang, C.**, **Patras, P. and Haddadi, H.** (2019). Deep Learning in Mobile and Wireless Networking: A Survey, *IEEE Communications Surveys and Tutorials*, *21*(3), 2224–2287.

[193] **Gunduz, D.**, **De Kerret, P.**, **Sidiropoulos, N.D.**, **Gesbert, D.**, **Murthy, C.R. and Van Der Schaar, M.** (2019). Machine Learning in the Air, *IEEE Journal on Selected Areas in Communications*, *37*(10), 2184–2199.

[194] **Simeone, O.** (2018). A Very Brief Introduction to Machine Learning with Applications to Communication Systems, *IEEE Transactions on Cognitive Communications and Networking*, *4*(4), 648–664.

[195] **Amiri, M.M. and Gunduz, D.** (2019). Machine Learning at the Wireless Edge: Distributed Stochastic Gradient Descent Over-the-Air, *IEEE International Symposium on Information Theory - Proceedings*, *2019-July*, 1432–1436.

[196] **Tran, N.H.**, **Bao, W.**, **Zomaya, A.**, **Nguyen, M.N. and Hong, C.S.** (2019). Federated Learning over Wireless Networks: Optimization Model Design and Analysis, *Proceedings - IEEE INFOCOM*, 1387–1395.

[197] **Yang, Q.**, **Liu, Y.**, **Chen, T. and Tong, Y.** (2019). Federated machine learning: Concept and applications, *ACM Transactions on Intelligent Systems and Technology*, *10*(2), 1–19.

[198] **Amiri, M.M. and Gunduz, D.** (2019). Over-the-Air Machine Learning at the Wireless Edge, *IEEE Workshop on Signal Processing Advances in Wireless Communications, SPAWC*, *2019-July*, 1–5.

[199] **Amiri, M.M.**, **Duman, T.M. and Gunduz, D.** (2019). Collaborative machine learning at the wireless edge with blind transmitters, *GlobalSIP 2019 - 7th IEEE Global Conference on Signal and Information Processing, Proceedings*.

[200] **Zhu, G.**, **Wang, Y. and Huang, K.** (2020). Broadband Analog Aggregation for Low-Latency Federated Edge Learning, *IEEE Transactions on Wireless Communications*, *19*(1), 491–506.

[201] **Yang, K.**, **Jiang, T.**, **Shi, Y. and Ding, Z.** (2020). Federated Learning via Over-the-Air Computation, *IEEE Transactions on Wireless Communications*, *19*(3), 2022–2035.

[202] **Amiri, M.M. and Gunduz, D.** (2019). Federated Learning over Wireless Fading Channels.

[203] **Mohammadi Amiri, M. and Gunduz, D.** (2020). Machine Learning at the Wireless Edge: Distributed Stochastic Gradient Descent Over-the-Air, *IEEE Transactions on Signal Processing*, (4), 1–1.

[204] **Shashank, V. and Kashyap, N.** (2013). Lattice coding for strongly secure compute-and-forward in a bidirectional relay, *IEEE International Symposium on Information Theory - Proceedings*, *2*, 2775–2779.

[205] **Babaheidarian, P. and Salimi, S.** (2015). Compute-and-forward can buy secrecy cheap, *IEEE International Symposium on Information Theory - Proceedings*, 2475–2479.

[206] **Richter, J.**, **Scheunert, C.**, **Engelmann, S. and Jorswieck, E.A.** (2015). Weak Secrecy in the two-way untrusted relay channel with compute-and-forward, *IEEE International Conference on Communications*, (6), 4357–4362.

[207] **Karpuk, D.A. and Chorti, A.** (2016). Perfect Secrecy in Physical-Layer Network Coding Systems from Structured Interference, *IEEE Transactions on Information Forensics and Security*, *11*(8), 1875–1887.

[208] **Goldenbaum, M.**, **Boche, H. and Poor, H.V.** (2016). On secure computation over the binary modulo-2 adder multiple-access wiretap channel, *2016 IEEE Information Theory Workshop, ITW 2016*, 21–25.

[209] **Goldenbaum, M.**, **Boche, H. and Poor, H.V.** (2017). Secure computation of linear functions over linear discrete multiple-access wiretap channels, *Conference Record - Asilomar Conference on Signals, Systems and Computers*, 1670–1674.

[210] **Babaheidarian, P.**, **Salimi, S. and Papadimitratos, P.** (2017). Preserving confidentiality in the Gaussian broadcast channel using compute-and-forward, *2017 51st Annual Conference on Information Sciences and Systems, CISS 2017*, 1–6.

[211] **Hynek, T. and Sykora, J.** (2015). Wireless physical layer network coding in potential presence of malicious relays - Incomplete information game approach, *Electronics Letters*, *51*(16), 1292–1294.

[212] **Negi, R. and Satashu, G.** (2005). Secret Communication using Artificial Noise, 1906–1910.

[213] **Zhu, J. and Gastpar, M.** (2014). Asymmetric Compute-and-Forward with CSIT.

[214] **Li, S.**, **Da Xu, L. and Zhao, S.** (2018). 5G Internet of Things: A survey, *Journal of Industrial Information Integration*, *10*, 1–9.

[215] **Dai, L.**, **Wang, B.**, **Yuan, Y.**, **Han, S.**, **I, C.L. and Wang, Z.** (2015). Non-orthogonal multiple access for 5G: Solutions, challenges, opportunities, and future research trends, *IEEE Communications Magazine*, *53*(9), 74–81.

[216] **Katz, J. and Lindell, Y.** (2008). *Introduction to Modern Cryptography*, Chapman & Hall/CRC.

[217] **Tse, D. and Viswanath, P.** (2005). *Fundamentals of Wireless Communication*, Cambridge University Press.

[218] **Zhang, F.**, **Liu, M.**, **Zhou, Z. and Shen, W.** (2016). An IoT-based online monitoring system for continuous steel casting, *IEEE Internet of Things Journal*, *3*(6), 1355–1363.

[219] **Gopala, P.K.**, **Lai, L. and El Gamal, H.** (2008). On the Secrecy Capacity of Fading Channels, *IEEE Transactions on Information Theory*, *54*(10), 4687–4698.

[220] **Zheng, G.**, **Wong, K.**, **Paulraj, A. and Ottersten, B.** (2009). Collaborative-Relay Beamforming With Perfect CSI: Optimum and Distributed Implementation, *IEEE Signal Processing Letters*, *16*(4), 257–260.

[221] **Wyner, A.D.** (1975). The wire-tap channel, *Bell System Technical Journal*, *54*(8), 1355–1387.

[222] **Maurer, U.M.** (1993). Secret key agreement by public discussion from common information, *IEEE Transactions on Information Theory*, *39*(3), 733–742.

[223] **Ahlswede, R. and Csiszar, I.** (1993). Common randomness in information theory and cryptography. I. Secret sharing, *IEEE Transactions on Information Theory*, *39*(4), 1121–1132.

[224] **Tekin, E.**, **Member, S. and Yener, A.** (2008). The Gaussian multiple access wire-tap channel, *54*(12), 5747–5755.

[225] **Wang, H.M. and Zheng, T.X.** (2016). Wireless physical layer security, *SpringerBriefs in Computer Science*, (9789811015748), 1–19.

[226] **Liu, Y.**, **Chen, H.H. and Wang, L.** (2017). Physical layer security for next generation wireless networks: Theories, technologies and challenges, *IEEE Communications Surveys and Tutorials*, *19*(1), 347–376.

[227] **Ren, K.**, **Su, H. and Wang, Q.** (2011). Secret key generation exploiting channel characteristics in wireless communications, *IEEE Wireless Communications*, *18*(4), 6–12.

[228] **Zeng, K.** (2015). Physical layer key generation in wireless networks: Challenges and opportunities, *IEEE Communications Magazine*, *53*(6), 33–39.

[229] **Khisti, A.**, **Tchamkerten, A. and Wornell, G.W.** (2008). Secure broadcasting over fading channels, *IEEE Transactions on Information Theory*, *54*(6), 2453–2469.

[230] **Liu, H.**, **Yang, J.**, **Wang, Y.**, **Chen, Y. and Koksal, C.E.** (2014). Group secret key generation via received signal strength: Protocols, achievable rates, and implementation, *IEEE Transactions on Mobile Computing*, *13*(12), 2820–2835.

[231] **Czap, L.**, **Member, S.**, **Prabhakaran, V.M.**, **Fragouli, C. and Diggavi, S.N.** (2015). Channels with state-feedback, *61*(9), 4788–4808.

[232] **Safaka, I.**, **Czap, L.**, **Argyraki, K. and Fragouli, C.** (2016). Creating secrets out of packet erasures, *IEEE Transactions on Information Forensics and Security*, *11*(6), 1177–1191.

[233] **Jafari Siavoshani, M.**, **Mishra, S.**, **Fragouli, C. and Diggavi, S.N.** (2017). Multi-Party Secret Key Agreement over State-Dependent Wireless Broadcast Channels, *IEEE Transactions on Information Forensics and Security*, *12*(2), 323–337.

[234] **Tang, T.**, **Jiang, T. and Zou, W.** (2018). Group secret key generation in physical layer, protocols and achievable rates, *2017 17th International Symposium on Communications and Information Technologies, ISCIT 2017*, *2018-Janua*, 1–6.

[235] **Nazer, B. and Gastpar, M.** (2007). Computation over multiple-access channels, *IEEE Transactions on Information Theory*, *53*(10), 3498–3516.

[236] **Zheng, M.**, **Goldenbaum, M.**, **Stańczak, S. and Yu, H.** (2012). Fast average consensus in clustered wireless sensor networks by superposition gossiping, *IEEE Wireless Communications and Networking Conference, WCNC*, 1982–1987.

[237] **Boneh, D. and Silverberg, A.** (2003). Applications of multilinear forms to cryptography, *Contemporary Mathematics*, *324*, 71–90.

[238] **Sabharwal, A.**, **Schniter, P.**, **Guo, D.**, **Bliss, D.W.**, **Rangarajan, S. and Wichman, R.** (2014). In-band full-duplex wireless: Challenges and opportunities., *IEEE Journal on Selected Areas in Communications*, *32*(9), 1637–1652.

[239] **Everett, E.**, **Sahai, A. and Sabharwal, A.** (2014). Passive self-interference suppression for full-duplex infrastructure nodes, *IEEE Transactions on Wireless Communications*, *13*(2), 680–694.

[240] **Zhang, Z.**, **Chai, X.**, **Long, K.**, **Vasilakos, A.V. and Hanzo, L.** (2015). Full duplex techniques for 5G networks: self-interference cancellation, protocol design, and relay selection, *IEEE Communications Magazine*, *53*(5), 128–137.

CURRICULUM VITAE

Personal Information

NAME SURNAME	Ufuk Altun
OCCUPATION	Research Assistant
EMAIL	altunu@itu.edu.tr ufukaltun@trakya.edu.tr
ADDRESS	Department of Electrical and Electronics Engineering Trakya University, Edirne, Turkey
WEB PAGE	https://personel.trakya.edu.tr/ufukaltun
DATE OF BIRTH	31 July 1993

Research Interests

Analog Function Computation	Worked with software-defined radios (USRP modules) to implement a wireless calculator that computes basic calculator functions over the wireless channel
Phy-Layer Security	Considered the security perspective of the analog function computation for the authentication and key generation problems of multi-user networks
Localization	Participated in a funded indoor localization project. The project aimed to take "lognormal mixture shadowing" into account in the path loss model to improve the accuracy of the localization. Specifically, participated in the testbed implementation of the model with WiFi signals.
Jamming Detection OFDM-IM	Participated in an OFDM-IM project. Particularly investigated the jammer detection performance of the OFDM-IM scheme versus OFDM via computer simulations.

Education

2011-2017	**Bachelor of Science** Electronics and Communication Engineering Istanbul Technical University, Istanbul, Turkey Supervisor: Gunes Karabulut Kurt

Publications From This Thesis

JOURNAL	U. Altun, S. Tedik Basaran, G. Karabulut Kurt, and E. Ozdemir, "Scalable Group Secret Key Generation over Wireless Channels," *in progress*
	U. Altun, S. Tedik Basaran, G. Karabulut Kurt, and E. Ozdemir, "Authenticated Data Transmission over Wireless Channels," *IEEE Communication Letters*, doi: 10.1109/LCOMM.2020.3007636
	U. Altun, G. Karabulut Kurt, and E. Ozdemir, "A survey on the simultaneous transmission based communication techniques," *in progress*
PATENT	U. Altun, S. Tedik Basaran, G. Karabulut Kurt, and E. Ozdemir, "A Joint Data Transmission and Authentication Technique over the Wireless Multiple Access Channel," applied to Turkish Patent Institute, 2018/ 11274, August 2018