DYNAMIC CONTROL OF WIRELESS NETWORKS WITH CONFIDENTIAL COMMUNICATIONS

by

YUNUS SARIKAYA

Submitted to the Graduate School of Engineering
and Natural Sciences in partial fulfillment of the requirements
for the degree of Doctor of Philosophy

Sabancı University
July 2014

DYNAMIC CONTROL OF WIRELESS NETWORKS WITH CONFIDENTIAL COMMUNICATIONS

by Yunus Sarıkaya

APPROVED BY

Assoc. Prof. Dr. Özgür Erçetin ....
(Thesis Advisor)

Assoc. Prof. Dr. Özgür Gürbüz ....
(Thesis Co-Advisor)

Assoc. Prof. Dr. Albert Levi ....

Assoc. Prof. Dr. Can Emre Koksal ....

Assoc. Prof. Dr. Onur Kaya ....

DATE OF APPROVAL: 21/07/2014

To my family

DYNAMIC CONTROL OF WIRELESS NETWORKS WITH CONFIDENTIAL COMMUNICATIONS

Yunus Sarıkaya

PhD Thesis, 2014

Thesis Advisor: Assoc. Prof. Dr. Özgür Erçetin
Thesis Co-Advisor: Assoc. Prof. Dr. Özgür Gürbüz

Keywords: ***Physical Layer Security, Wireless Scheduling, Dynamic Control, Cross-layer optimization***

Future wireless communication systems are rapidly transforming to satisfy ever-increasing and varying mobile user demands. Cross-layer networking protocols have the potential to play a crucial role in this transformation by jointly addressing the requirements of user applications together with the time-varying nature of wireless networking. As wireless communications becoming an integral and crucial part of our daily lives with many of our personal data is being shared via wireless transmissions, the issue of keeping personal transactions confidential is at the forefront of any network design. Wireless communications is especially prone to attacks due to its broadcast nature. The conventional cryptographical methods can only guarantee secrecy with the assumption that it is computationally prohibitive for the eavesdroppers to decode the messages. On

the other hand, information-theoretical secrecy as defined by Shannon in his seminal work has the potential to provide perfect secrecy regardless of the computational power of the eavesdropper. Recent studies has shown that information-theoretical secrecy is possible over noisy wireless channels. In this thesis, we aim to design simple yet provably optimal cross-layer algorithms taking into account information-theoretical secrecy as a Quality of Service (QoS) requirement. Our work has the potential to improve our understanding the interplay between the secrecy and networking protocols.

In most of this thesis, we consider a wireless cellular architecture, where all nodes participate in communication with a base station. When a node is transmitting a confidential messages, other legitimate nodes are considered as eavesdroppers, i.e., all eavesdroppers are internal. We characterize the region of achievable open and confidential data rate pairs for a single and then a multi-node scenario. We define the notion of *confidential opportunistic scheduler*, which schedules a node that has the largest instantaneous confidential information rate, with respect to the best eavesdropper node, which has the largest mean cross-channel rate. Having defined the operational limits of the system, we then develop *dynamic* joint scheduling and flow control algorithms when perfect and imperfect channel state information (CSI) is available. The developed algorithms are simple index policies, in which scheduling and flow control decisions are given in each time instant independently.

In real networks, instantaneous CSI is usually unavailable due to computational and communication overheads associated with obtaining this information. Hence, we generalize our model for the case where only the distributions of direct- and cross-channel CSI are available at the transmitter. In order to provide end-to-end reliability, Hybrid Automatic Retransmission reQuest (HARQ) is employed. The challenge of using HARQ is that the dynamic control policies proposed in the preceding chapter are no longer optimal, since the decisions at each time instant are no longer independent. This is mainly due to the potential of re-transmitting a variant of the same message successively until it is decoded at the base station. We solve this critical issue by proposing a novel queuing model, in which the messages transmitted the same number of times previously are stored in the same queue with scheduler selecting a head-of-line

message from these queues. We prove that with this novel queuing model, the dynamic control algorithms can still be optimal.

We then shift our attention to providing confidentiality in multi-hop wireless networks, where there are multiple source-destination pairs communicating confidential messages, to be kept confidential from the intermediate nodes. For this case, we propose a novel end-to-end encoding scheme, where the confidential information is encoded into one very long message. The encoded message is then divided into multiple packets, to be combined at the ultimate destination for recovery, and being sent over different paths so that each intermediate node only has partial view of the whole message. Based on the proposed end-to-end encoding scheme, we develop two different dynamic policies when the encoded message is finite and asymptotically large, respectively. When the encoded message has finite length, our proposed policy chooses the encoding rates for each message, based on the instantaneous channel state information, queue states and secrecy requirements. Also, the nodes keep account of the information leaked to intermediate nodes as well the information reaching the destination in order to provide confidentiality and reliability. We demonstrate via simulations that our policy has a performance asymptotically approaching that of the optimal policy with increasing length of the encoded message.

All preceding work assumes that the nodes are altruistic and/or well-behaved, i.e., they cooperatively participate into the communication of the confidential messages. In the final chapter of the thesis, we investigate the case with non-altruistic nodes, where non-altruistic nodes provide a jamming service to nodes with confidential communication needs and receiving in turn the right to access to the channel. We develop optimal resource allocation and power control algorithms maximizing the aggregate utility of both nodes with confidential communication needs as well as the nodes providing jamming service.

GİZLİ HABERLEŞMELİ KABLOSUZ AĞLARIN DİNAMİK KONTROLÜ

Yunus Sarıkaya

Doktora Tezi, 2014

Tez Danışmanı: Doç. Dr. Özgür Erçetin

Tez Eş Danışmanı: Doç. Dr. Özgür Gürbüz

Anahtar Kelimeler: ***Fiziksel katman güvenliği, Kablosuz çizelgeleme, Dinamik Kontrol, Katmanlar arası optimizasyon***

Geleceğin kablosuz haberleşme sistemleri, devamlı artan ve değişen seyyar kullanıcı taleplerini karşılamak için hızlı bir şekilde dönüşüm geçiriyor. Katmanlar arası ağ oluşturma protokolleri, kullanıcı uygulamalarının gereklerini ve kablosuz ağların zaman ile değisen doğasına birlikte hitap ederek bu dönüşümde kritik bir rol oynama potensiyeline sahiptir. Bir çok kişisel verinin kablosuz haberleşme ile paylaşılmasıyla kablosuz haberleşme hayatımızın tamamlayıcı ve kritik bir parçası oldu ve bu yüzden kişisel işlemlerin gizli tutulması meselesi her türlü ağ tasarımının ön planınında yer alır. Kablosuz haberleşme, özellikle yayımlama doğasından dolayı saldirilara eğilimlidir. Geleneksel kriptografik yöntemler, sadece gizlice dinleyen kimselerin mesajları deşifre etmesini sayisal olarak engelleci olduğu varsayımı ile gizlilik garantisi verebilir. Diğer taraftan Shannon'un seminal çalışmasında tanımlanan bilgi-kuramsal gizlilik, gizlice dinleyen kimsenin hesaplama güçü ne olursa olsun kusursuz gizlilik sağlama potensiyeline sahip. Son zamanlardaki çalışmalar bilgi-kuramsal gizliliğin gürültülü kablosuz kanallar üzerinden mümkün olabileceğini gösterdi. Bu tezde, amaçımız basit ama ispatlanabilir şekilde optimal ve bilgi-kuramsal gizliliği servis kalitelesi gereksinimi olarak alan katmanlar arası algoritmalar tasarlamak. Çalışmamızın gizlilik ile ağ oluşturma protokolleri arasinda etkileşim konusundaki anlayışımızı geliştirme potensiyeli var.

Tezin büyük bölümünde bütün kullanıcıların bas istasyonu ile haberleştiği kablosuz hücresel yapı dikkate aldık. Bir kullanıcı gönderimi sirasinda diğer kullanıcılar gizlice dinleyen kimseler olarak dikkate alınıyor, bir başka deyişle bütün gizlice dinleyenler içeriden. Tek ve çoklu kullanıcı senaryoları için elde edilebilir açık ve gizli veri hız ikilisi bölgesini tanımladık. En iyi gizlice dinleyen kimseye göre en yüksek anlık gizli bilgi hizina sahip kullanıcıyı çizelgeleyen *gizli fırsatçı çizelgeleyici* kavramını tanımladık. Sistemin operasyonel limitlerini tanimladiktan sonra kusursuz ve kusurlu kanal durum bilgisi olduğunda dinamik çizelgeleyici ve akış kontrol algoritmaları geliştirdik. Geliştirelen algoritmalar, çizelgeleme ve akı kontrol kararların her zaman anında bağımsız olarak verildiği basit gösterge politikalarıdır.

Gerçek ağlarda anlık kanal durum bilgisi hesaplama ve haberleşme ek yüklerinden dolayı genellikle bulunmaz. Bu yüzden modelimizi sadece direk ve çapraz kanal durum bilgilerinin sadece dağılımının olduğunu durum olarak genelleştirdik. Uç uca güvenilirliği sağlamak için karma otamatik yeniden iletim işteği kullanılır. Burdaki zorluk bir önceki bölümde sunulan dinamik kontrol yöntemleri artik optimal değil çünkü her zamaninda verilen kararlar artik bağımsız değil. Bunun temel nedeni de ayni mesajın varyantlarının bas istasyonu mesajı deşifre edene kadar gönderimidir. Bu kritik sorunu aynı sayıda gönderiimi yapilan mesajların ayni sirada depolandığı orijinal kuyruklama modeli sunarak çözeriz. Bu orijinal kuyruklama modeli ile dinamik kontrol algoritmalarini hala optimal olabileceğini ıspatlarız.

Daha sonra dikkatimizi ara kullanıcılardan gizli tutulan birden çok kaynak-hedef ikilisinin gizli mesajlarla haberleştiği çoklu hop kablosuz ağlara çeviririz. Bu durum için gizli bilginin çok uzun mesaja kodlandığı orijinal uç uca kodlama yöntemi önerdik. Kodlanan mesaj esas hedefte birleştirilmek uzere bir çok pakete bölünür ve farklı yollar-

dan gönderilir ki her ara kullanıcı sadece butun mesajini kismi görüntüsünü alabilsin. Önerilen uç uca kodlama yöntemine dayanarak, kodlanan mesajın sinirli büyüklükte ve asimptotik olarak büyük olduğu durumlar için iki farkli dinamik algoritma sunduk. Kodlanan mesajın sınırlı büyüklüğe sahip olduğunda, önerilen method her mesaj için kodlama hızını anlık kanal durum bilgisi, sıra durumu ve gizlilik gereğine göre seçer. Ayrıca kullanıcılar ara kullanıcılara sızan bilgiyi ve hedefe ulaşan bilgiyi gizliği ve güvenliği sağlayabilmek için hesaba katarlar. Simulasyonlar üzerinden methodumuz kodlanan mesajını büyüklüğü artıkça asimptotik olarak optimal methoda yaklaştığını gösterdik.

Bütün önceki çalışmalar kullanıcıların fedakar ve/veya iyi davranan olduğunu varsayar. Bir başka değişle işbirliği içinde gizli mesajinin gönderimine katılırlar. Tezin son bölümünde fedakar olmayan kullanıcıların olduğu durumu inceleriz. Bu durumda fedakar olmayan kullanıcılar gizli mesaja sahip kullanıcıya yayın bozma servisi sunar ve karşılığında kanala erişim hakkına sahip olur. Gizli mesajlı kullanıcı ile yayın bozma servisi sunan kullanıcıların faydalarını maksimuma çıkaran optimal kaynak dağıtma ve güç kontrol algoritmaları geliştirdik.

Acknowledgments

I am deeply thankful to many people who have all contributed to this thesis and to making my time as a student a very enriching experience. First, I would like thank my advisor Dr. Özgür Erçetin. Looking into the past, I feel so fortunate to be able work with them. I am grateful for all the occasions when they managed to be there for me even from distant locations and at unusual times to help me when I had a question or problem. I specially appreciate his openness and willingness to guide me to become a better individual in both professional and personal life of mine. I am also very grateful to my co-advisor Dr. Özgür Gürbüz for her valuable guidance, patience and understanding throughout my studies. I greatly appreciated the kindness, honesty and good humour that were part of every interaction we had.

In addition to my advisors, I would like to thank Dr. Can Emre Koksal for providing me valuable research discussions during and after my stay in Ohio State University. I was really grateful to be able to work with a great researcher such as him. I would like to thank Dr. Albert Levi and Dr. Onur Kaya for agreeing to be on my thesis committee and for the many useful comments that they provided.

I would like to thank TÜBİTAK, for providing the necessary motivation and funding.

I was so fortunate to be surrounded by many great friends during my studies in Sabancı University, who made my time at the university very enjoyable and created an inspirational and entertaining atmosphere. Without them, it would be hard to get motivation to continue the hard years of study. I also thank Deniz for her support and presence during the writing process of thesis.

Above all, I would like to thank my family for their endless love, understanding and patience that made me follow my own path. Getting a Ph.D. would not have been possible without their unconditional love and support. It is priceless for me to have a family as caring as them and to know that I can always rely on them.

I would like to thank Sabanci University for supporting this research. This thesis is also supported in part by European Commission under Marie Curie IRSES grant PIRSES-GA-2010-269132 AGILENet.

Contents

List of Figures

Chapter 1

Introduction

During the last two decades, a revolution has taken place in personal and public communication. Many devices like telephones, computers, mouses or keyboards, traditionally connected via cables, are now connected in a wireless manner. Technologies like Wireless LANs, Bluetooth, and Cellular Networks have increased the consumer potential, and users keep requesting for higher data transfer rates. In fact, the wireless revolution is just beginning, especially due to the advance of new technologies like Mesh Networks, and Cognitive Radio Networks. On the other hand, defense and public safety applications are of definite interest for governmental entities, especially in military applications, or data transactions between corporate entities like banks. Thus, this explosive growth, of wireless communications and wireless based services, has lead to an increased focus on the security aspect of these systems. For example, how can we ensure that a wireless transaction is secure and/or personal data is protected and/or military applications are not vulnerable to outside attacks? Indeed, due to the broadcast nature of the wireless communications, the transmissions are susceptible to eavesdropping. In other words, an adversary, eavesdropper, can listen to the transmissions and try to obtain some meaningful information. Therefore, it is imperative to design secure wireless systems, to ensure their continued growth and well being. At this point, security arises as a new quality of service (QoS) constraint that must be accounted for in the network design.

The state of the art technique in combating eavesdropping attacks is to utilize cryptographic approaches, which can be broadly classified into public-key and secret-key protocols. In such cryptographic approaches, the security is guaranteed by designing a protocol such that it is computationally prohibitive for the eavesdropper to decode the message. These protocols are heavily based on unproven assumptions such as hardness of factoring large primes [1]. Thus, it remains unknown whether the protocols will be vulnerable to attacks with novel algorithms and/or increased computational power at the eavesdropper, since there is no rigorous mathematical proofs for the security of such protocols. In addition to these drawbacks, some cryptographic protocols require deploying secret keys at users, which might be highly costly for some applications, such as energy-limited sensor networks.

In 1949, Shannon first proposed information theoretic security in [2]. Shannon avoids the aforementioned limitations of the computational based approach, and introduced a notion of secrecy. According to his secrecy notion, the eavesdropper must get zero information regarding the transmitted message. He showed that this can be guaranteed for Vernam's one time pad scheme only if the source-destination pair shares a common randomness, i.e., secret key, which has higher entropy than that of the message. In fact, the common randomness needed was of the same rate as the source message itself, making the resulting communication schemes, one-time pad, rather impractical.

The result of Shannon was mainly based on the assumption of the noiseless channel between the nodes. Actually, wireless channels are noisy and the quality of the channel varies across time. This property can be exploited to enhance the security of the network. Accordingly, Wyner [3] considered the wiretap channel model, in which the eavesdropper has degraded (more noisy) observations from the channel compared to that of the legitimate receiver, i.e., the eavesdropper is said to be degraded. Under this assumption, Wyner showed that the advantage of the main channel over that of the eavesdropper, in terms of the lower noise level, can be exploited to transmit secret bits using random codes. In other words, it is possible to achieve a non-zero secure rate without sharing a key, where the eavesdropper is limited to learn almost nothing from the transmissions. In particular, Wyner characterized the tradeoff between the message rate and the level of ignorance of the message at the wiretapper, i.e., equivocation rate. This notion, if satisfied, assures that the wiretapper gains only a negligible amount of information regarding the message per channel use. This keyless secrecy result was then extended to a more general (broadcast) model [4] and to the Gaussian setting in [5].

After pioneering work of Wyner [3], information theoretic secrecy was left untouched for almost two decades. Only, in recent years, there has been a number of investigations on wireless information theoretic secrecy. These studies have been largely confined within the boundaries of the physical layer in the wireless scenario and they have significantly enhanced our understanding of the fundamental limits and principles governing the design and analysis of secure wireless communication systems. Despite the significant progress in information theoretic secrecy, most of the work has focused on physical layer techniques and on a single link. The area of wireless information theoretic secrecy remains in its infancy, especially as it relates to the design of wireless networks and its impact on network control and protocol development. Therefore, our understanding of the interplay between the secrecy requirements and the critical functionalities of wireless networks, such as scheduling, routing, and congestion control remains very limited. To that end, in this thesis, we focus on designing novel scheduling and resource allocation algorithms by incorporating information secrecy, *measured by equivocation*, as a QoS metric.

1.1 Contributions and Outline of the Thesis

In this thesis, we investigate the problem of allocating the wireless channel to users such that fairness among users is achieved while ensuring the network is information theoretically secure. For that purpose, we model the entire problem as that of a network utility maximization. Preciously, our aim is to maximize sum of utilities (functions of average rates of users) in a provable secure network, subject to network stability. In particular, we are interested in solutions to this problem that are amenable to online implementation, i.e., in each time instant, decisions are given based on observed channel conditions and system parameters. To provide optimality in such solutions, decisions given in each time instant should be independent, so that time-averages are maximized [6]. Then, the focus is to improve our understanding of how the secrecy requirements affect the network performance by analyzing the solutions. We divide the analysis into following parts, where each part follows the different system assumptions and/or network configurations, and reveals interesting insights based on the interplay between the secrecy and the network protocols.

In Chapter 2, we give several important definitions regarding information theoretical secrecy and stochastic optimization, especially Lyapunov optimization, and provide extensive literature reviews of information theoretical secrecy and stochastic optimization.

In Chapter 3, we consider the single hop uplink setting, in which nodes collect confidential and open information, store them in separate queues and transmit them to the base station. At a given point in time, only one node is scheduled to transmit and it may choose to transmit some combination of open and confidential information. We first we evaluate the region of achievable open and confidential data rate pairs for a single node scenario and the multi-node scenario, and introduce the notion of **confidential opportunistic scheduling**. Confidential opportunistic scheduler schedules the node that has the largest instantaneous confidential information rate, with respect to the best eavesdropper node, which has the largest mean cross-channel rate. Next, we model the problem as that of network utility maximization, and provide a dynamic joint flow control, scheduling and secrecy encoding scheme under perfect and imperfect channel state information (CSI) assumptions.

In Chapter 4, we generalize the system model considered in Chapter 3 to a general case when the instantaneous channel states are not known perfectly, but each node has the knowledge of merely the distribution of its associated uplink channel state as well as the cross channels between itself and every other node. Clearly, without exact instantaneous uplink CSI at the transmitter side, the wireless transmissions are prone to decoding errors, i.e., channel outages, which enforces us to use hybrid ARQ (HARQ) schemes to provide reliability. The main challenge involved in generalizing the network control with hybrid ARQ is encoding confidential and/or open messages over several blocks. This implies that decisions based on observations of current time instant are not necessarily independent due to the potential of re-transmitting a variant of the same message successively until it is decoded at the base station. In the literature, HARQ problems are generally solved by using Markov Decisions Processes (MDPs), which is computationally prohibitive and hard to implement [7], [8], [9]. To resolve this issue and provide provably optimal online algorithm, we develop a novel queuing model. Specifically, in order to handle the messages undergoing a decoding failure event in a simple and effective way, we introduce queues storing the messages retransmitted with the same number of times in previous time-slots. The scheduler can select the head-of-line message from any of these queues to transmit, which makes decisions over each time instant independent. Then, we prove that with this novel queuing model, the dynamic control algorithms is still optimal.

In Chapter 5, we consider the problem of resource allocation and control of multi-hop networks in which multiple source-destination pairs communicate messages, to be kept confidential from the intermediate nodes. In order to achieve confidentiality, our end-to-end dynamic encoding scheme encodes confidential messages across multiple packets, to be combined at the ultimate destination for recovery. The aim here is to exploit multi-path diversity and temporal diversity due to channel variability. We first develop an optimal dynamic policy for the case in which the number of blocks across which secrecy encoding is performed is asymptotically large. Next, we consider encoding across a finite number of packets, which eliminates the possibility of achieving perfect secrecy. For this case, we develop a dynamic policy to choose the encoding rates for each message, based on the instantaneous channel state information, queue states and secrecy outage requirements.

In Chapter 6, we change cooperative node assumptions in previous chapters, and design network control protocols with non-altruistic jamming nodes, from which a source node utilizes jamming service, compensating them with a fraction of its bandwidth for transmission of its data. Particularly, the primary node injects confidential data and secondary nodes inject open data at rates in order to maximize global utility function, while keeping data queues stable and meeting a constraint on the secrecy outage probability. The constraint on the secrecy outage probability is met with the help of jamming service obtained from the secondary nodes.

1.2 Publication Lists

1.2.1 Journal Papers

- Y. Sarikaya, O. Ercetin and O. Gurbuz, “Dynamic Control for Cooperative Jamming with a Non-altruistic Node,” in preparation.

- Y. Sarikaya, O. Ercetin and C.E. Koksal, “Dynamic Network Control for Confidential Multi-hop Communications,” submitted to IEEE/ACM Transactions on Networking, in revision.

- Y. Sarikaya, O. Ercetin and C.E. Koksal, “Confidentiality- Preserving Control of Uplink Cellular Wireless Networks Using Hybrid ARQ, accepted to IEEE/ACM Transactions on Networking.

- C. E. Koksal, O. Ercetin and Y. Sarikaya, “Control of Wireless Networks with Secrecy,” IEEE/ACM Transactions on Networking, vol. 21, no. 1, pp. 324-337, Feb. 2013.

- M. Karaca, Y. Sarikaya, O. Ercetin, T. Alpcan and H. Boche, “Joint Opportunistic Scheduling and Selective Channel Feedback”, IEEE Trans. on Wireless Communication, vol. 12, no. 5, pp. 3024- 3034, June 2013.

- Y. Sarikaya, T. Alpcan and O. Ercetin, “Dynamic Pricing and Queue Stability in Wireless Access Games”, IEEE Special Topics on Signal processing, vol. 6, no. 2, pp. 140-150, April 2012.

1.2.2 Conference Papers

- Y. Sarikaya, O. Ercetin, C. E. Koksal, “Dynamic Network Control for Confidential Multi-hop Communications,” Intl. Symposium on Modeling and Optimization in Mobile, AdHoc, and Wireless Networks (Wiopt) 2013.

- Y. Sarikaya, O. Ercetin, C. E. Koksal, “Wireless Network Control with Privacy Using Hybrid ARQ,” Proceedings of International Symposium on Information

Theory (ISIT) 2012, Cambridge, MA.

- C. E. Koksal, O. Ercetin, Y. Sarikaya, “Control of Wireless Networks with Secrecy,” Proceedings of Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, Sept. 2010.

- M. Karaca, Y. Sarikaya, O. Ercetin, T. Alpcan, H. Boche , “Efficient Wireless Scheduling with Limited Channel Feedback and Performance Guarantees,” Personal Indoor and Mobile Radio Communications (PIMRC) 2012, Sydney, NSW.

- Y. Sarikaya, T. Alpcan, O. Ercetin, “Resource Allocation Game for Wireless Networks with Stability Constraints,” Proceedings of IEEE Conference on Decision and Control (CDC) 2011, Orlando, FA.

- Y. Sarikaya, O. Ercetin, “On Physically Secure and Stable Slotted Aloha System,” 47th Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, Sep 30-Oct 2, 2009.

Chapter 2

Background and Prelimaniries

In this Chapter, we first briefly explain and give some important definitions and theorems regarding the physical layer secrecy. Then, we define queue and network stability, and explain the basic idea behind Lyapunov drift theory which will be used through out this thesis as a framework for designing the network protocols. We end the chapter with a detailed literature review on physical layer secrecy and network control.

2.1 Information-Theoretic Secrecy

Information theoretic secrecy is first proposed by Shannon in [2] called as provable secrecy, and avoids assumptions about computational limitations of eavesdroppers. Shannon considered noiseless links and unlimited computational power and time. He defined perfect secrecy or provable secrecy as:

Definition 1. *Perfect secrecy is only achieved the eavesdropper obtains zero information regarding the transmitted message. Thus, even though eavesdropper has unlimited computational power and time, it is impossible decrypt or break the transmitted message. In particular, he showed that perfect secrecy is achieved when $I(W; Y_e) = 0$. $I(X; Y)$ is the mutual information between vectors X and Y, and W is the confidential message and Y_e is the received symbols of the eavesdropper.*

Then, Shannon showed that this can be guaranteed for the Vernam's one time pad scheme. In this scheme, a confidential message, W, is paired with random secret key, K.

Then, each bit or character of the the confidential message is encrypted by combining it with the corresponding bit from the the key using modular addition. However, to satisfy perfect secrecy, the key which is shared by transmitter-receiver pair, should be truly random and the length of the key (or the entropy of the key) should be higher than the one of the confidential message, i.e., $H(K) \leq H(W)$.

The result of Shannon is pessimistic in the sense that one needs to share a random key that has a length at least that of the message, and the key should be never reused in whole. Furthermore, the result of Shannon was mainly based on the assumption of the noiseless channel between the nodes. Actually, wireless channels are noisy and the quality of the channel varies across time. In fact, this property can be exploited to improve the secrecy of the network. Accordingly, Wyner [3] considered the wiretap channel model, in which the eavesdropper has degraded observations from the channel compared to that of the legitimate receiver, i.e., the legitimate receiver has better channel condition compared to the eavesdropper. Wyner showed that the advantage of having better main channel condition over that of the eavesdropper, in terms of the lower noise level, can be exploited to transmit secret bits using random coding, which is based on binning strategy. Each bin in random coding contains codewords corresponding the same confidential message. A codeword is chosen according to the uniform distribution on the set of codewords in that bin, and sent over the channel. Consequently, Wyner showed that it is possible to achieve a non-zero confidential rate without sharing a key, where the eavesdropper is limited to learn almost nothing from the transmissions. In particular, Wyner defined equivocation rate to measure secrecy level, which characterizes the tradeoff between the message rate and the level of ignorance of the message at the wiretapper. In such a setting, perfect secrecy is said to be achieved if the message rate, $H(W)/N$, can be made arbitrarily close to the equivocation rate, $H(W|Y_e)/N$, which measures the remaining uncertainty in W after observing Y_e, in the limit of large number of channel uses, N. (That is, as $I(W;Y_e) = H(W) - H(W|Y_e)$, $I(W;Y_e)/N$ is made small.) This notion, if satisfied, assures that the wiretapper gains only a negligible amount of information regarding the message per channel use. Next, we will give main assumption and results regarding information-theoretical secrecy based on the work of

Wyner used throughout thesis.

First, we give the main assumption of information-theoretical secrecy as:

Assumption 1. *Each attacker is capable of tapping into all the information transmitted and received by a single intermediate node. Attackers are not capable of changing the content of the information the node forwards, nor do they inject phantom messages into the network. In our model, intermediate nodes are entities, compliant with network operations as they properly execute algorithms, but the messages need to be kept confidential from them.*

Next, we give the results obtained by Wyner in [3] in a multi-user setting. Each node i has a private and an open message, $W_i^{\mathrm{conf}} \in \{1, \ldots, 2^{NR_i^{\mathrm{conf}}}\}$. The aim is to keep all or part of the message W_i^{conf} unconditionally secret from possibly multiple eavesdroppers. The notion of unconditional or information-theoretic secrecy is defined as follows:

Definition 2. *Given the message and randomization sequence, W_i^{conf}, to be transmitted to the base station over N channel uses, the equivocation rate is defined as*

$$\frac{1}{N} H(W_i^{conf}) | Y_j), \tag{2.1}$$

where Y_j is the vector of symbols received by node j.

Perfect secrecy is said to be achieved if the message rate can be made arbitrarily close to the equivocation rate, which measures the remaining uncertainty in confidential message,W_i^{conf} , after observing Y_j. That is to say,

Lemma 1. *To achieve perfect secrecy, following constraint must be satisfied by node i, for all $j \neq i$,*

$$\lim_{N \to \infty} \frac{1}{N} I(W_i^{conf}, Y_j) \leq \epsilon, \tag{2.2}$$

for any given $\epsilon > 0$. In 2.2, the mutual information is used, i.e., $I(X,Y) = H(X) - H(X|Y)$.

2.2 Dynamic Control of Networks

In this section, we begin our treatment of stochastic network optimization, where the goal is to stabilize the network while additionally optimizing some performance metric and/or satisfying some additional constraints. Specifically, the goal is to design a cross-layer strategy for flow control, routing, and resource allocation that provides stability while achieving optimal network fairness. Here, we measure fairness in terms of a general utility function of the long term flow rates.

In particular, for the problem considered in this thesis, the goal is to support a fraction of the traffic demand matrix, λ, to achieve a long term throughput matrix that maximizes the sum of user utilities. The general problem can be thus defined as network utility maximization (NUM) problem as:

$$\max \sum_i U_i(\lambda_i) \tag{2.3}$$

$$\text{subject to Network Stability}$$

$$\text{Additional QoS Constraints,}$$

where as an additional Qos constraint, we consider information-theoretical secrecy, i.e., communications of users in the network should be perfectly secure. In cross-layer designs of wireless networks as a solution to NUM problem, a number of physical and access layer parameters are jointly controlled and in synergy with higher layer functions like transport and routing. Thus, actions at different layers need to be taken by considering the nature of the variability of wireless links, i.e, time-varying nature, in order to control the network in an optimal manner. Lyapunov optimization framework is powerful optimization tool such that it is robust to variability of wireless network, and enables stability and performance optimization to be treated simultaneously. Thus, we use Lyapunov optimization framework to obtain dynamic control algorithms. Next, we give the definition of network stability, and the results of Lyapunov drift analysis, which is backbone of Lyapunov optimization framework.

2.2.1 Queue Stability

A queueing system describes contention among users to share a resource, where resources are called servers, and it exhibits randomness and the time-varying nature of the wireless channel. Furthermore, queueing systems provide an important tool in modeling the performance analysis of telecommunication systems.

Each node i maintains a a queue for storing network layer data. Let Q_i denote the backlog, i.e., unfinished work at time t, stored in a network layer queue at node i. In addition, $A_i(t)$ and $R_i(t)$ are real valued random variables which belong to a certain stochastic process, e.g, for M/M/1 queue stochastic process is poisson process for both. $A_i(t)$ and $R_i(t)$ represent the amount of new task arriving at queue i and the amount of work processed by the server of node i at time t, respectively. It is assumed that both $A_i(t)$ and $R_i(t)$ are independent of each other. Then, the dynamics of a queue can be represented as:

$$Q_i(t+1) = [Q(t) - R_i(t)]^+ + A_i(t), \tag{2.4}$$

where $[x]^+ = \max(0, x)$. We assume that all network layer queues have infinite buffer storage space. Our primary goal for this layer is to ensure that all queues are stable as a QoS requirement, so that time average backlog is finite. This performance criterion tends to yield algorithms that also perform well when network queues have finite buffers that are sufficiently large. In throughout thesis, we use strong stability, i.e.,

Definition 3. *A queue is strongly stable, if*

$$\lim_{T\to\infty} \frac{1}{T} \sum_{t=0}^{T-1} \mathbb{E}\left[Q_i(T)\right] < \infty \tag{2.5}$$

That is, a queue is strongly stable if it has a bounded time average backlog

Definition 4. *A network is strongly stable if all individual queues of the network are strongly stable.*

The network stability condition is as follows:

Lemma 2. *Lemma 3.6. in [6] (Stability Conditions) Consider a queue with an admissible input process $A_i(t)$ with average arrival rate λ, and a server process with time average rate $\bar{\mu}_i$. Then: (a) $\lambda_i \leq \bar{\mu}_i$ is a necessary condition for strong stability. (b) $\lambda_i < \bar{\mu}_i$ is a sufficient condition for strong stability.*

The intuition behind this necessary constraint is that if $\lambda_i > \bar{\mu}_i$, then expected queue backlog necessarily grows to infinity, leading to instability. The sufficient condition is also intuitive, but its proof requires the structure of admissible arrival and service processes as will be done in the next subsection.

2.2.2 Lyapunov Drift Analysis

Before giving the Lyapunov drift analysis, we should give the definition of the achievable rate region. In a multi-user wireless setting, resource is shared among users, and let us consider a scheduler which allocates the channel to an user, and let $\mathcal{I}_i(t)$ represent the scheduler decision. That is to say, when $\mathcal{I}_i(t) = 1$, the channel is allocated to user i at time t, $\mathcal{I}_i(t) = 0$ otherwise. In a wireless channel, the rate is characterized by the channel state, so let $h_i(t)$ be the channel state of user i at time t. Then, the rate of user i (service rate) at time t is:

$$R_i(t) = R_i(h_i(t), \mathcal{I}_i(t)), \tag{2.6}$$

Then the rates of all users in the network can be represented in a vector form as:

$$\mathbf{R}(t) = R(\mathbf{h}(t), \mathcal{I}(t)), \tag{2.7}$$

In [6], the achievable rate region (or the network layer capacity region)is defined as:

Definition 5. *The achievable rate region, Λ, is the closure of the set of all arrival rate matrices (λ_i) that can be stably supported by the network, considering all possible strategies for choosing the control variables to affect routing, scheduling, and resource allocation. That is to say,*

$$\Lambda = \sum_{\mathbf{h} \in \mathcal{H}} \pi(\mathbf{h}) Conv\{R(\mathbf{h}(t), \mathcal{I}(t))\},$$

where $\mathcal{H}$ is the set of all possible channel states, Conv is the convex-hull of the rate set, and $\pi(\mathbf{h})$ is the probability of the realization of the channel state $\mathbf{h}$

Upon characterization of the achievable rate region, the network can be configured to achieve the long term link transmission rates within the achievable rate region Λ. The reason why Lyapunov drift is an important mathematical tool is that that enables us to obtain the solution of a long-term stochastic optimization problem without the need of explicit characterization of the achievable rate region, Λ. The idea of Lyapunov drift is to define a non-negative function of queue backlogs, called a Lyapunov function, as a scalar measure of the aggregate congestion of all queues in the network. Then, network control mechanism gives decisions based on how they affect the change in the Lyapunov function from one slot to the next.

Specifically, we use quadratic function throughout the thesis. Let $\mathbf{Q}(t) = (Q_1(t), Q2(t), \ldots, Q_n(t$ be a collection of queue backlogs in a network with n users at time t. Define the following quadratic Lyapunov function and the one-slot expected Lyapunov drift:

$$L(\mathbf{Q}(t)) = \sum_{i=1}^{n} (Q_i(t))^2, \tag{2.8}$$

$$\Delta(t) = \mathbb{E}\left[L(\mathbf{Q}(t+1)) - L(\mathbf{Q}(t)) | L(\mathbf{Q}(t))\right] \tag{2.9}$$

where the expectation is taken over all possible states of $\mathbf{Q}(t)$. Then,

Lemma 3. *(Lemma 4.1 in [6]) If there exist constants $B > 0$, $\epsilon > 0$, such that for all times t we have:*

$$\Delta(t) \leq B - \epsilon \sum_{i=1}^{n} Q_i(t), \tag{2.10}$$

then, the network is strongly stable, and the bound of the average queue sizes is as follows:

$$\limsup_{T\to\infty} \frac{1}{T} \sum_{t=0}^{T} Q_i(t) \leq \frac{B}{\epsilon} \tag{2.11}$$

The condition of the Lemma 3 ensures that the Lyapunov drift is negative whenever the sum of queue backlogs is sufficiently large. Intuitively, this property ensures network stability because whenever the queue backlog leaves the bounded region, the negative drift eventually drives it back to this region.

Up to this point, we investigated strong stability of the network and how to achieve it. However, in many network control problems, the goal is to stabilize the network while additionally optimizing some performance metric and/or satisfying some additional constraints. Before restating the Lyapunov optimization theorem in [6], we define the following problem: Let our objective be the maximization of time average of a scalar valued function $f(\cdot)$ of another process $\mathbf{R}(t)$ while keeping $\mathbf{Q}(t)$ finite. Note that for NUM problem in (2.3), $f(\cdot)$ is the sum of utilities, i.e., $f(\cdot) = \sum_i U_i(\cdot)$

Theorem 1. *Theorem 5.4 in [6] For the scalar valued function $f(\cdot)$, if the channel states are i.i.d., and if there exists positive constants V, ϵ, B, such that for all times t*

and all unfinished work vector, i.e., queue backlogs, $\mathbf{Q}(t)$ *the Lyapunov drift satisfies:*

$$\Delta(t) - V\mathbb{E}\left[f(\mathbf{R}(t))|\mathbf{Q}(t)\right] \leq B - Vf^* - \epsilon\sum_{i=1}^{n} Q_i(t), \tag{2.12}$$

then the time average utility and queue backlog satisfy:

$$\liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} \mathbb{E}\left[f(\mathbf{R}(t))\right] \geq f^* - \frac{B}{V} \tag{2.13}$$

$$\limsup_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1}\sum_{i=1}^{n} \mathbb{E}\left[Q_i(t)\right] \leq \frac{B + V(\bar{f} - f^*)}{\epsilon}, \tag{2.14}$$

where f^* *is the maximal value of* $\mathbb{E}\left[f(\cdot)\right]$ *and* $\bar{f} = \limsup_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} \mathbb{E}\left[f(\mathbf{R}(k))\right]$.

Theorem 1 is the main result of the Lyapunov optimization. This theorem exhibits the trade-off between achieving optimal rates and queue backlogs. More preciously, the value of V can be chosen so that B/V is arbitrarily small, resulting in achieved utility that is arbitrarily close to optimal. This performance comes at the cost of a linear increase in network congestion with the parameter V. Littles theorem suggests that average queue backlog is proportional to average bit delay, and hence performance can be pushed towards optimality with a corresponding tradeoff in end-to-end network delay.

2.3 Literature Review

In this section, we divide literature review into main part as physical layer security, and network control.

2.3.1 Physical Layer Security

The pioneering work in message secrecy at the physical layer belongs to Wyner [3]. In 1975, Wyner shows that physical layer secrecy is possible without the use of a secret key. The concept of wire-tap channel is introduced by [3] for the first time. The wiretapper is a particular form of eavesdropper, with the specific characteristic that the wire-tappers channel is a degraded version of the legitimate receivers channel. Csiszar and Korner generalized this to the case where the signals at the eavesdropper and the destination are obtained from the transmitted signal through an arbitrary broadcast channel [4].

The main drawback of the wiretap channel introduced by [3] is the assumption that the eavesdropper channel is degraded, i.e., the main channel condition is always better than the eavesdropper channel. Recently, a considerable effort has been made to deal with this issue. For example, [10–12] have unveiled the opportunistic secrecy principle which allows for transforming the multi-path fading variations into a secrecy advantage for the legitimate receiver, even when the eavesdropper is enjoying a higher average signal-to-noise ratio (SNR).

Another way to improve wireless secure communication is to use feedback between legitimate transmitter and receiver. The existence of feedback from the destination to the source is a reasonable assumption for wireless relay networks, since wireless channels are generally bi-directional, and hence, a backward transmission from the destination is easy to implement. This fact, together with the encouraging results by Maurer and others, motivates the study of secrecy protocols with feedback for wireless networks [13]. The fundamental role of feedback in enhancing the secrecy capacity of point-to-point wireless communication links was extended in [14–16]. These works generally assume the perfect feedback channel output, i.e., receiver's noisy channel output is perfectly available to the transmitter in a casual manner. One would expect that feedback which is not public, i.e., which yields different received signals at the source and at the eavesdroppers, can only improve the situation compared to public feedback. On the other hand, the assumption that the public feedback channel is of arbitrarily large capacity is quite strong, and needs to be refined in future work. The assumption that communication over the public channel is authenticated can be motivated through the existence of secure authentication protocols. Extensions to non-authenticated public channels might be possible, similarly to [17–19].

More recent works have explored the use of multiple antennas to induce ambiguity at the eavesdropper under a variety of assumptions on the available transmitter channel state information (CSI) [20–23]. The aim here is to reduce the rate obtained by the eavesdropper. Cooperative communication can also increase the secrecy rate by exploiting the relay channels via cooperative jamming, where a relay creates interference at the eavesdropper by transmitting a jamming signal. In this case, interference between signals from different relay nodes can be used to confuse an eavesdropper. Relay nodes can even generate random signals in order to jam the channel to the eavesdropper (this idea was introduced by Tekin and Yener in [24]). The multi-user aspect of the wireless environment was further-studied in [25–36] revealing the potential gains that can be reaped from appropriately constructed user cooperation policies. However, there is a trade-off, because every jamming signal can potentially hurt the legitimate decoder as well. That is to say, the jamming signal power should be high enough to disturb the received signal at the eavesdropper; however allocating too much power on the jamming signal can also degrade the signal quality at the destination. In a recent work, [37], the cooperative jamming (CJ) power allocation problem is solved with convex optimization and a one-dimensional search algorithm. Particular networks like the relay channel or the multiple-access channel have been studied in [38, 39]. One of the most interesting outcomes of this body of work is the discovery of the positive impacts on secure communications of some wireless phenomena, e.g., interference, which are traditionally viewed as impairments to be overcome.

All of these works generally assume full CSI at the transmitter. However, the assumption that the channel to the eavesdropper is known is not realistic, because it would imply that the eavesdropper is actively participating in the communication, which is not the case in the models of the relevant papers. One possible improvement regarding the first issue (eavesdropper channel uncertainty) is to consider a class of possible eavesdropper channels. If the class, albeit finite, is sufficiently large, it can provide a reasonable approximation for a continuous range of the true eavesdropper channel. The compound wiretap channel studied by Liang, Kramer, Poor and Shamai in [40] shows that the perfect secrecy capacity can be lower bounded for the wiretap channel with a class of eavesdroppers. For degraded compound wiretap channels, the lower bound given in [40] is tight. This work was extended by Liu, Prabhakaran and Vishwanath in [41], where the secrecy capacity was found for a class of non-degraded parallel Gaussian compound channels. Second improvement is to consider that only distributions of the channels are available. In this case, the concern of study is not only secrecy, but reliability too. To accomplish reliability, [42] proposes a secure hybrid ARQ protocol, which is based a block fading wiretap channel. They also introduce two distinct stochastic coding strategies, i.e., incremental reduncacy based coding and repetition based coding. In Chapter 3, we design network control algorithms based on coding proposed by [42]. Another disadvantage of physical layer security is impractical implementation of secure encoding. Wyner proposes stochastic encoder to provide secrecy, which is based on random binning. That is to say, users need to keep multiple codewords spanning a confidential message, and this is impractical according to memory usage. Finally, the design of practical codes that approach the promised capacity limits was investigated in [43, 44].

There are a few number of works on secure multi-hop communications. In [45], a particular wireless relay network called the fan network is studied, where the signal sent by a source node can be heard by all relays via different outputs of a broadcast channel. All the relay nodes are then connected to the destination via a perfect channel by which destination can obtain received signal from all relays without a delay. [46] considers the secret communication between a pair of source and destination nodes in a wireless network with authenticated relays, and derives achievable secure rates for deterministic and Gaussian channels. Furthermore, [47, 48] studies the secrecy capacity scaling problem. Exploitation of path diversity in order to achieve secrecy from external eavesdroppers is studied in [49] and for secrecy via mobility in [50]. In [51] a method is given that modifies any given linear network code into a new code that is secure requiring a large field size. Later, [52] generalized and simplified the method in [51], and showed that the problem of making a linear network code secure is equivalent to the problem of finding a linear code with certain generalized distance properties. Along the same lines, [53] investigates secure communication over wireline networks where a node can observe one of an arbitrarily selected collection of secure link sets.

2.3.2 Network Control

Network control with scheduling in wireless networks is a prominent and challenging problem which attracted significant interest from the networking community. The challenge arises from the fact that the capacity of wireless channel is time varying due to multiple superimposed random effects such as mobility and multipath fading. Optimal scheduling in wireless networks has been extensively studied in the literature under various assumptions [54], [55], [56], [57], [58], [59]. They all studied the throughput-optimal policies which ensure the stability of the queueing network if stability can be indeed achieved under any policy. Starting with the seminal work of Tassiulas and Ephremides [54] where throughput optimality of backpressure algorithm is proven, policies that opportunistically exploit the time varying nature of the wireless channel to schedule users are shown to be at least as good as static policies [55]. Furthermore, three classes of policies that are known to be throughput-optimal include the Max Weight rule [6], the Exponential (EXP) rule [60] and the Log rule [61]. Among the three classes, the throughput-optimal property of the Max Weight type algorithms [62] and the Log rule [61] are both proved by the theory of Lyapunov drift, whereas the EXP rule is proved to be throughput-optimal by the fluid limit technique along with a separation of time scales argument [60]. Specifically, the general Max Weight type algorithms are proved to minimize the Lyapunov drift, and hence, are throughput-optimal. Many dynamic control algorithms belong to this type, which include optimizing the allocation of computer resources [63], and stabilizing packet switch systems [64–67] and satellite and wireless systems [68–70]. In principle, these opportunistic policies schedule the user with the favorable channel condition to increase the overall performance of the system. However, without imposing individual performance guarantees for each user in the system, this type of scheduling results in unfair sharing of resources and may lead to starvation of some users, for example, those far away from the base station in a cellular network. Hence, in order to address fairness issues, scheduling problem was investigated jointly with the network utility maximization problem [71–73], and the stochastic network optimization framework [6] was developed.

The Lyapunov drift theory (which only focuses on controlling a queueing network to achieve stability) is extended to the Lyapunov optimization theory (which enables stability and performance optimization to be treated simultaneously) [74, 75]. For example, utilizing the Lyapunov optimization theory, the Energy-Efficient Control Algorithm (EECA) proposed in [75] stabilizes the system and consumes an average power that is arbitrarily close to the minimum power solution with a corresponding tradeoff in network delay. In [76] and [77], the authors consider the asymptotic single-user and multi-user power-delay tradeoff in the large delay regime and obtain insights into the structure of the optimal control policy in the large delay regime. Although the derived policy (e.g., dynamic backpresssure algorithm) by the Lyapunov drift theory and the Lyapunov optimization theory may not have good delay performance in moderate and light traffic loading regimes, it allows potentially simple solutions with throughput optimality in multi-hop wireless networks. Thus, analyzing delay performance is another issue with Lyapunov optimization theory. There have been some recent papers that analyze delay performance of cross-layer scheduling algorithms [78–82]. In particular, it was shown that the well-known maximum weight scheduling algorithm achieves order-optimal delay in the uplinkdownlink of cellular networks [78] and in most practical large-scale multihop wireless networks [79]. In [83], it was shown that by combining the principle of shortest-path routing and differential backlog routing, end-to-end delay performance can be improved. In [84,85] and [86], the virtual queue technique was used to improve network delay performance.

There are wide range of application areas (which generally have different QoS requirements) of Lyapunov optimization framework due to its relatively simple resulting policies and providing extensive analysis on the solution. For example, in a cognitive radio network, secondary users have transmission opportunity only if primary users are not transmitting. It is desirable to design a scheduling scheme that improves the service received by secondary users while minimizing the collision or interference possibility between primary and secondary users [87, 88]. In [87], a virtual collision queue is introduced that monitors how much a primary user experiences collisions more than a predefined threshold. In [88, 89], authors a cooperative scheduling scheme for cognitive radio networks. In a classic cognitive network, secondary users utilize the slots which are not used by primary users. In contrast, they consider a scenario in which secondary users in good channel state help primary users in bad channel to increase the channel capacity. The secondary users are rewarded immediately or in the long term. Another area is network control design with OFDM channels [90]. For example, in [90–93], authors obtain channel assignment and power allocation solutions that can dynamically adapt to changing channel conditions, and would maximize system throughput under per-user bandwidth (QoS) constraints, in a long-term sense. Since Lyapunov optimization framework is a powerful technique for optimizing wireless network, it is applied to many different problems having different objectives. However, to the best of our knowledge, our work presented in this thesis is the first Lyapunov drift analysis of wireless secure network.

Chapter 3

Control of Wireless Networks with Secrecy

In this chapter, we consider the problem of cross-layer resource allocation in time-varying cellular wireless networks, and incorporate information theoretic secrecy as a Quality of Service constraint. Specifically, each node in the network injects two types of traffic, confidential and open, at rates chosen in order to maximize a global utility function, subject to network stability and secrecy constraints. The secrecy constraint enforces an arbitrarily low mutual information leakage from the source to every node in the network, except for the sink node. We first obtain the achievable rate region for the problem for single and multi-user systems assuming that the nodes have full CSI of their neighbors. Then, we provide a joint flow control, scheduling and secrecy encoding scheme, which does not rely on the knowledge of the prior distribution of the gain of any channel. We prove that our scheme achieves a utility, arbitrarily close to the maximum achievable utility. Numerical experiments are performed to verify the analytical results, and to show the efficacy of the dynamic control algorithm.

3.1 Introduction

In recent years, there have been a number of investigations on wireless information theoretic secrecy. These studies have been largely confined within the boundaries of the *physical layer* in the wireless scenario and they have significantly enhanced our understanding of the fundamental limits and principles governing the design and analysis of secure wireless communication systems. To that end, in this chapter we address the basic wireless network control problem in order to develop a cross-layer resource allocation solution that will incorporate information secrecy, *measured by equivocation*, as a QoS metric. In particular, we consider the single hop uplink setting, in which nodes collect confidential and open information, store them in separate queues and transmit them to the base station. At a given point in time, only one node is scheduled to transmit and it may choose to transmit some combination of open and confidential information. Our objective is to achieve secrecy of information from the other legitimate nodes and we assume that there are no external malicious eavesdroppers in the system. The motivation to study this notion of secrecy is the following. In some scenarios (e.g., tactical, financial, medical), secrecy of communicated information between the nodes is necessary, so that data intended to (or originated from) a node is not shared by any other legitimate node. Such a scenario occurs, for instance, in wireless networks, internal to a local entity (e.g., a company, university, etc.), where users broadcast confidential (e.g., containing credit card numbers, social security numbers, etc.) as well as open information.

First, we evaluate the region of achievable open and confidential data rate pairs for a single node scenario with and without joint encoding of open and confidential information. Then, we consider the multi-node scenario, and introduce **confidential opportunistic scheduling**. We find the achievable confidential information rate regions associated with confidential opportunistic scheduling and show that for both the uplink and the downlink scenarios, it achieves the maximum sum confidential information rate over all joint scheduling and encoding strategies. While confidential opportunistic scheduler is based on the availability of full CSI on the uplink channels, it does not rely on information on the instantaneous cross-channel (i.e., the channel between different nodes) CSI. It requires merely the long-term average rate of the cross-channel rates. To achieve secrecy with this level of CSI, confidential opportunistic scheduler uses an encoding scheme that encodes confidential information over many packets. Note that,

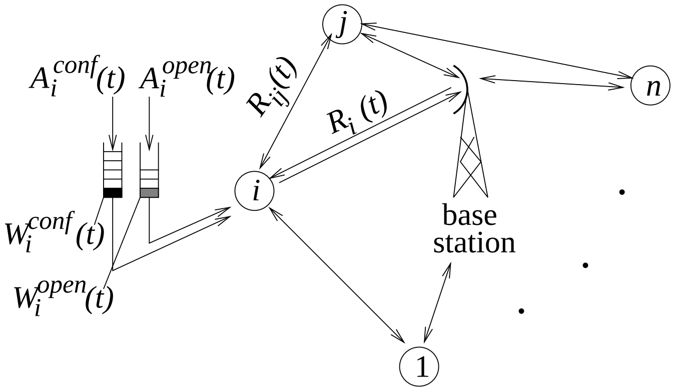


Figure 3.1: Uplink communication with confidential and open information.

in the seminal paper [94], it was shown that opportunistic scheduling (without secrecy) maximizes the sum rate. Our result can be viewed as a generalization of this result to the case with secrecy. Next, we model the problem as that of network utility maximization. We provide a dynamic joint flow control, scheduling and secrecy encoding scheme, which takes into account the *instantaneous* direct- and cross-channel state information but not a priori channel state distribution. In dynamic cross-layer control scheme confidential information is divided into a sequence of messages where each message is encoded into an *individual* packet. We prove that our scheme achieves a utility, arbitrarily close to the maximum utility achievable in this setting. We generalize dynamic cross-layer control scheme to a more general case when instantaneous cross-channel states are not known perfectly. Consequently, we define the notions of *secrecy outage* and *confidential goodput*. Finally, we numerically characterize the performance of the dynamic control algorithm with respect to several network parameters, and show that its performance is fairly close to that of confidential opportunistic scheduler achievable with known channel priors.

3.2 Problem Model

We consider the cellular network illustrated in Fig. 3.1. The network consists of n nodes, each of which has both open and confidential information to be transmitted to a single base station over the associated uplink channel. When a node is transmitting, every other node overhears the transmission over the associated cross channel. We assume every channel to be iid block fading, with a block size of N_1 channel uses. The entire session lasts for N_2 slots, which corresponds to a total of $N = N_1 N_2$ channel uses. We denote the instantaneous achievable rate for the uplink channel of node i by $R_i(t)$, which is the maximum mutual information between output symbols of node i and received symbols at the base station over slot (block) t. Likewise, we denote the rate of the cross channel between nodes i and j with $R_{ij}(t)$, which is the maximum mutual information between output symbols of node i and input symbols of node j over slot t. Note that there is no actual data transmission between any pair of nodes, but parameter $R_{ij}(t)$ will be necessary, when we evaluate the confidential rates between node i and the base station.

Even though our results are general for all channel state distributions, in numerical evaluations, we assume all channels to be *Gaussian* and the transmit power to be constant, identical to P for all slots t, $1 \leq k \leq N_2$. We represent the uplink channel for node i and the cross channel between nodes i and j with a power gain (magnitude square of the channel gains) $h_i(t)$ and $h_{ij}(t)$ respectively over slot t. We normalize the power gains such that the (additive Gaussian) noise has unit variance. Then, as $N_1 \to \infty$,

$$R_i(t) = \log(1 + P h_i(t)) \tag{3.1}$$

$$R_{ij}(t) = \log(1 + P h_{ij}(t)). \tag{3.2}$$

Each node i has a confidential and an open message, $W_i^{\text{conf}} \in \{1, \ldots, 2^{NR_i^{\text{conf}}}\}$ and $W_i^{\text{open}} \in \{1, \ldots, 2^{NR_i^{\text{open}}}\}$ respectively, to be transmitted to the base station over N channel uses, where R_i^{conf} and R_i^{open} denote the (long-term) confidential and open information rates respectively, for node i. Let the vector of symbols received by node i be $\mathbf{Y}_i$. To achieve *perfect secrecy*, following constraint must be satisfied by node i: for all $j \neq i$,

$$\lim_{N \to \infty} \frac{1}{N} I(W_i^{\text{conf}}; \mathbf{Y}_j) \leq \varepsilon \tag{3.3}$$

for any given $\varepsilon > 0$. We define the *instantaneous confidential information rate* of node

i transmitted confidentially from node j over slot t as:

$$R_{ij}^{p}(t) = [R_i(t) - R_{ij}(t)]^+, \tag{3.4}$$

where $[\cdot]^+ = \max(0, \cdot)$. It was shown in [3] that rate (3.4) is achievable as $N_1 \to \infty$ and [10] took it a step further and showed that, as $N_1, N_2 \to \infty$, a long-term confidential information rate of $\mathbb{E}\left[R_{ij}^{p}(t)\right]$ is achievable.

The amount of open traffic, $A_i^{\text{open}}(t)$, and confidential traffic, $A_i^{conf}(t)$, injected in the queues at node i (shown in Fig. 3.1) in slot t are both selected by node i at the beginning of each block. Open and confidential information are stored in separate queues with sizes $Q_i^{\text{open}}(t)$ and $Q_i^{\text{conf}}(k)$ respectively. At any given slot, a scheduler chooses which node will transmit and the amount of open and confidential information to be encoded over the block. We use the indicator variable $\mathcal{I}_i(t)$ to represent the scheduler decision:

$$\mathcal{I}_i(t) = \begin{cases} 1, & \text{confidential information from node } i \\ 0, & \text{otherwise} \end{cases}. \tag{3.5}$$

When we evaluate the region of achievable open and confidential data rate pairs for the single node scenario, in Section 3.3.1, we assume that the transmitting node has perfect causal knowledge of its uplink channel and the cross-channel at every slot t. Thus, the achievable region of confidential and open rates constitutes upper bound on the achievable rates for each node, which we find subsequently for the multiuser setting with partial CSI. For confidential opportunistic scheduler in the multiuser setting, we assume that, each node i has perfect causal knowledge of the uplink channel rate, $R_i(t)$, and its prior distribution. However, we assume that it only has the long-term averages, $\mathbb{E}\left[R_{ij}(t)\right]$, $j \neq i$ of its cross-channel rates. To achieve secrecy with this level of CSI, confidential opportunistic scheduler uses an encoding scheme that encodes confidential information over many packets. When we formulate our problem as that of network utility maximization problem, we only assume knowledge of instantaneous channel gains *without requiring the knowledge of prior distribution of channel gains.*

Hence, confidential encoding is performed over a single block length unlike the case with confidential opportunistic scheduler. Additionally, we analyze a more realistic scenario when the instantaneous channel rates are not known *perfectly*, but estimated with some random additive error. The scheduled transmitter, i, will encode at a rate

$$\hat{R}_i^p(t) = [R_i(t) - R_i^{\text{rand}}(t)]^+,$$

where $R_i^{\text{rand}}(t)$ is the rate margin, chosen such that the estimation error is taken into account. Note that when $R_i^{\text{rand}}(t) < \max_{j \neq i} R_{ij}(t)$, then perfect secrecy constraint (5.2) is violated over slot t. In such a case, we say that *secrecy outage* has occurred. The probability of secrecy outage over slot t when user i is scheduled, is represented as $\rho_i^{\text{secr}}(R_i^{\text{rand}}(t))$. Since perfect secrecy cannot be ensured over every block, we require that expected probability of secrecy outage of each user i is below a given threshold γ_i.

Finally note that, even though, the main focus in this paper is the uplink scenario, in Section 3.3, we generalize the results for the confidential opportunistic scheduler to the downlink scenario as well.

3.3 Achievable Rates and Confidential Opportunistic Scheduling

In this section, we evaluate the region of confidential and open rates achievable by a scheduler for multiuser uplink and downlink setting. We start with a single node transmitting, and thus, the scheduler only chooses whether to encode confidential information at any given point in time or not. We consider the possibility of both the separate and the joint encoding of confidential and open data. For multiuser transmission, we introduce our scheme, *confidential opportunistic scheduling*, evaluate achievable rates and show that it maximizes the sum confidential information rate achievable by any scheduler. Along with confidential opportunistic scheduling, we provide the associated physical-layer secrecy encoding scheme that encodes information over many slots.

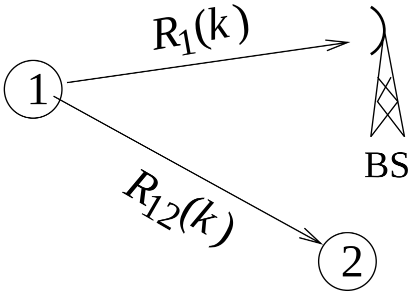


Figure 3.2: Single user confidential communication scenario.

3.3.1 Single User Achievable Rates

Consider the single user scenario in which the primary user (node 1) is transmitting information over the primary channel and a single secondary user (node 2) is overhearing the transmission over the secondary channel as shown in Fig. 3.2. In this scenario, we assume node 2 is passively listening without transmitting information and node 1 has perfect knowledge of instantaneous rates $R_1(t)$ and $R_{12}(t)$ for all t as well as their sample distributions. Over each slot t, the primary user chooses the rate of confidential and open information to be transmitted to the intended receiver. As discussed in [95] it is possible to encode open information at a rate $R_1(t) - R_{12}^p(t)$ over each slot t, jointly with the confidential information at rate $R_{12}^p(t)$. For that, one can simply replace the randomization message of the binning strategy of the achievability scheme with the open message, which is allowed to be decoded by the secondary user. In the rest of the section, we analyze both the case in which open information can and cannot be encoded along with the confidential information. We find the region of achievable confidential and open information rates, $(R_1^{\text{conf}}, R_1^{\text{open}})$, over the primary channel.

Separate encoding of confidential and open messages

First we assume that each block contains either confidential or open information, but joint encoding over the same block is not allowed. Recall that $\mathcal{I}_1(t)$ is the indicator variable, which takes on a value 1, if information is encoded confidentially over slot t and 0 otherwise. Then, one can find R_1^{conf}, associated with the point $R_1^{\text{open}} = \alpha$ by solving the following integer program:

$$\max_{\{\mathcal{I}_1(t)\}\in\{0,1\}} \quad \mathbb{E}\left[\mathcal{I}_1(t)R_{12}^p(t)\right] \tag{3.6}$$

$$\text{subject to} \quad \mathbb{E}\left[(1-\mathcal{I}_1(t))R_1(t)\right] \geq \alpha, \tag{3.7}$$

where the expectations are over the joint distribution of the instantaneous rates $R_1(t)$ and $R_{12}(t)$. Note that, since the channel rates are iid, the solution, $\mathcal{I}_1^*(t) = \mathcal{I}_1^*(R_1(t), R_{12}(t))$ will be a stationary policy. Also, a necessary condition for the existence of a feasible solution is $\mathbb{E}\left[R_1(t)\right] \geq \alpha$. Dropping the block index t for simplicity, the problem leads to the following Lagrangian relaxation:

$$\begin{aligned}\min_{\lambda>0} \max_{\{\mathcal{I}_1\}\in\{0,1\}} & \mathbb{E}\left[\mathcal{I}_1 R_{12}^p\right] + \lambda\left(\mathbb{E}\left[(1-\mathcal{I}_1)R_1\right] - \alpha\right) \\ &= \min_{\lambda>0} \left\{ \max_{\{\mathcal{I}_1\}\in\{0,1\}} \int_0^\infty \int_0^\infty \left[\mathcal{I}_1 R_{12}^p - \lambda(1-\mathcal{I}_1)R_1\right] \right. \\ & \qquad \left. p(R_1, R_{12})\, dR_1 dR_{12} - \lambda\alpha \right\}, \end{aligned} \tag{3.8}$$

where $p(R_1, R_{12})$ is the joint pdf of R_1 and R_{12}. For any given values of the Lagrange multiplier λ and (R_1, R_{12}) pair, the optimal policy will choose $\mathcal{I}_1^*(R_1, R_{12}) = 0$ if the integrant is maximized for $\mathcal{I}_1 = 0$, or it will choose $\mathcal{I}_1^*(R_1, R_{12}) = 1$ otherwise. If both $\mathcal{I}_1 = 0$ and $\mathcal{I}_1 = 1$ lead to an identical value, the policy will choose one of them randomly. The solution can be summarized as follows:

$$\frac{R_{12}^p}{R_1} \underset{\mathcal{I}_1^*=0}{\overset{\mathcal{I}_1^*=1}{\gtrless}} \lambda^*, \tag{3.9}$$

where λ^* is the value of λ for which $\mathbb{E}\left[(1-\mathcal{I}_1^*)R_1\right] = \alpha$, since $\lambda^*(\mathbb{E}\left[(1-\mathcal{I}_1)R_1\right] - \alpha) \leq 0$.

For Gaussian uplink and cross channels described in Section 3.2, the solution can be obtained by plugging (3.1,3.2,3.4) in (3.9):

$$(1 + Ph_1)^{1-\lambda^*} \underset{\mathcal{I}_1^*=0}{\overset{\mathcal{I}_1^*=1}{\gtrless}} 1 + Ph_{12}. \tag{3.10}$$

The associated solution $\mathcal{I}^*$ is graphically illustrated on the (h_1, h_{12}) space in Fig. 3.3

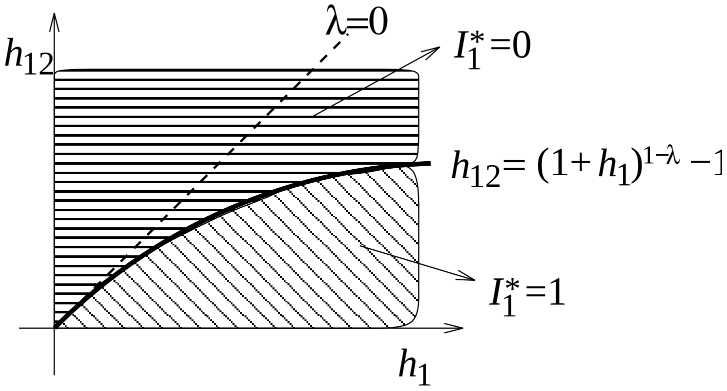


Figure 3.3: Optimal decision regions with separate encoding of confidential and open messages.

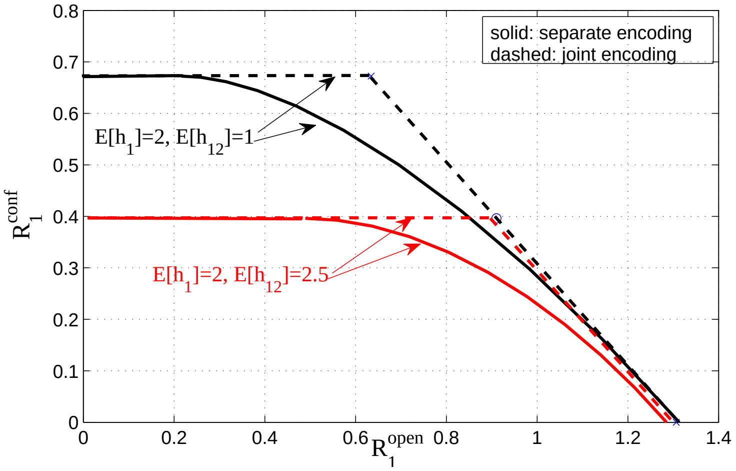


Figure 3.4: Achievable rate regions for the single user scenario with iid Rayleigh block fading channels.

for $P = 1$. As the value of λ varies between 0 and 1, the optimal decision region for $\mathcal{I} = 0$ increases from the upper half of the first quadrant represented by $h_{12} \geq h_1$ to the entire first quadrant, i.e., all $h_1, h_{12} \geq 0$. In Fig. 3.4, the achievable pair of confidential and open information rates, $(R_1^{\text{conf}}, R_1^{\text{open}})$, is illustrated for iid Rayleigh fading Gaussian channels, i.e., the power gains h_1 and h_{12} have an exponential distribution. We considered two different scenarios in which the mean power gains, $(\mathbb{E}\left[h_1\right], \mathbb{E}\left[h_{12}\right])$, are $(2, 1)$ and $(2, 2.5)$, and $P = 1$. The associated boundaries of the rate regions with separate encoding are illustrated with solid curves. To plot these boundaries, we varied λ from 0 to 1 and calculated the achievable rate pair for each point. Note that the flat portion on the top part of the rate regions for separate encoding corresponds to the case in which Constraint (3.7) is inactive. It is also interesting to note that as demonstrated in Fig. 3.4, one can achieve non-zero confidential information rates even when the mean cross channel gain between node 1 and node 2 is higher than the mean uplink channel gain of node 1.

Joint encoding of confidential and open messages

With the possibility of joint encoding of the open and confidential information over the same block, the indicator variable $\mathcal{I}_1(t) = 1$ implies that the confidential and open information rates are $R_{12}^p(t)$ and $R_1(t) - R_{12}^p(t)$ respectively over slot t simultaneously. Otherwise, i.e., if $\mathcal{I}_1(t) = 0$, open encoding is used solely over the block. To find achievable R_1^{conf}, associated with the point $R_1^{\text{open}} = \alpha$, one needs to consider a slightly different optimization problem this time:

$$\max_{\{\mathcal{I}_1(t)\}\in\{0,1\}} \quad \mathbb{E}\left[\mathcal{I}_1(t) R_{12}^p(t)\right] \tag{3.11}$$

$$\text{subject to } \mathbb{E}\left[(1-\mathcal{I}_1(t))R_1(t) + \mathcal{I}_1(t)(R_1(t) - R_{12}^p(t))\right] \geq \alpha, \tag{3.12}$$

This optimization problem can be solved in a similar way by employing Lagrangian relaxation as the problem considered in Section 3.3.1. First, we specify two regions of parameters for which the solution is trivial: 1) if $\mathbb{E}[R_1] < \alpha$, no solution exists for (3.11,3.12), since the uplink channel capacity is not sufficient to meet the desired open rate, α; 2) if $\mathbb{E}[R_1 - R_{12}^p] > \alpha$, then $\mathcal{I}_1^* = 1$ for all slots, i.e., all open information will be encoded jointly with confidential information, since the remaining capacity over that is necessary to support confidential information is sufficient to serve open information at rate α. In this case, Constraint (3.12) is inactive and the achieved confidential information rate is $R_1^{\text{conf}} = \mathbb{E}[R_{12}^p]$.

In all other cases, i.e., $\mathbb{E}[R_1 - R_{12}^p] \leq \alpha \leq \mathbb{E}[R_1]$, it can be shown that the optimal solution can be achieved by the following probabilistic scheme[1]: For any given block,

$$\mathcal{I}_1^* = \begin{cases} 1, & \text{w.p. } p^p \\ 0, & \text{w.p. } 1 - p^p \end{cases}, \tag{3.13}$$

independently of R_1 and R_{12}, where $p^p = \frac{\mathbb{E}[R_1]-\alpha}{\mathbb{E}\left[R_{12}^p\right]}$. The details of the derivation of the described optimal scheme is given in [96]. With this solution, only a fraction p^p of the slots contain jointly encoded confidential and open information, and the remaining $1-p^p$ fraction of the slots contain solely open information. Thus, for a given α, the achieved confidential and open information rates can be found as $R_1^{\text{conf}} = p^p \mathbb{E}\left[R_{12}^p\right] = \mathbb{E}\left[R_1\right] - \alpha$ and $R_1^{\text{open}} = p^p \mathbb{E}\left[R_1 - R_{12}^p\right] + (1-p^p)\mathbb{E}\left[R_1\right] = \alpha$ respectively. Rather surprisingly, it does not matter which slots contain only open information and which ones contain jointly encoded confidential and open information, as long as the desired open information rate α is met. Consequently, a random scheme that chooses $1 - p^p$ fraction of slots for open information only and the rest for jointly encoded open and confidential information suffices to achieve the optimal solution.

By the above analysis, one can conclude that the achievable rate region with joint encoding can be summarized by the intersection of two regions specified by: (i) $(R_1^{\text{conf}} + R_1^{\text{open}}) \leq \mathbb{E}\left[R_1\right]$ and (ii) $R_1^{\text{conf}} \leq \mathbb{E}\left[R_{12}^p\right]$. Any point on the boundary of the region can be achieved by the simple probabilistic scheme described above. One can realize that this region is the maximum achievable rate region, since in our system, the total information rate (confidential and open) is upper bounded by the capacity, $\mathbb{E}\left[R_1\right]$, of uplink channel 1 and the achievable confidential rate is upper bounded by the secrecy capacity, $\mathbb{E}\left[R_{12}^p\right]$, of the associated wiretap channel. Thus, there exists no other scheme that can achieve a larger rate region than the one achieved by the simple probabilistic scheme.

In Fig. 3.4, the achievable pairs of confidential and open information rates, $(R_1^{\text{conf}}, R_1^{\text{open}})$ with joint encoding are illustrated for the iid Rayleigh fading Gaussian channels with the same parameters as the separate encoding scenario. The boundaries of the regions

[1] Note that the solution of Problem (3.11,3.12) is not unique and the described probabilistic solution is just one of them.

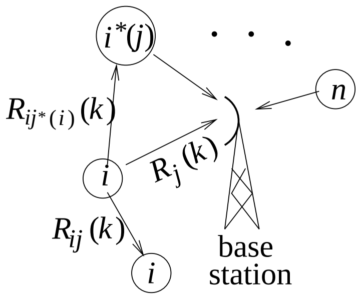


Figure 3.5: Multiuser confidential communication system - uplink

are specified with dashed curves, which are plotted by varying the value of p^p from 0 to 1 and evaluating $(\mathbb{E}[R_1 - R_{12}^p], \mathbb{E}[R_{12}^p])$ pair for each value. Similar to the separate encoding scenario, the flat portion on the top part of the regions corresponds to the case in which Constraint (3.12) is inactive.

3.3.2 Confidential Opportunistic Scheduling and Multiuser Achievable Rates

In this section, we consider the multiuser setting described in Fig. 3.1. We introduce *confidential opportunistic scheduling* (COS) for both the downlink and the uplink scenario and prove that it achieves the maximum achievable sum confidential information rate over the set of all schedulers. COS schedules the node that has the largest instantaneous confidential information rate, with respect to the "best eavesdropper" node, which has the largest mean cross-channel rate. Each node ensures perfect secrecy from its best eavesdropper node by using a binning strategy, which requires only the average cross-channel rates to encode the messages over many slots.

Uplink Scenario

First, we consider the multiuser uplink scenario given in Fig. 3.5. We assume every node i has perfect causal knowledge of its uplink channel rate, $R_i(t)$ for all slots t and the average cross-channel rates, $\mathbb{E}[R_{ij}(t)]$, for all $i \neq j$.

Confidential Opportunistic Scheduling for uplink

We define the best eavesdropper of node i as $j^*(i) \triangleq \text{argmax}_{j \neq i} \mathbb{E}\left[R_{ij}(t)\right]$ and denote its average cross-channel rate with $\bar{R}_i^m \triangleq \mathbb{E}\left[R_{ij^*(i)}(t)\right]$. Note that $j^*(i)$ does not change from one block to another. In COS, only one of the nodes is scheduled for data transmission in any given block. In particular, in slot t, we opportunistically schedule node

$$i^M(t) \triangleq \underset{i \in \{1,\ldots,n\}}{\text{argmax}} \left[R_i(t) - \bar{R}_i^m\right]$$

if $\max_{i \in \{1,\ldots,n\}} \left[R_i(t) - \bar{R}_i^m\right] > 0$ and no node is scheduled for confidential information transmission otherwise, i.e., $i^M(t) = \emptyset$. In case of multiple nodes achieving the same maximum confidential rate, the tie can be broken at random. Indicator variable $\mathcal{I}_i^{\text{COS}}(t)$ takes on a value 1, if node i is scheduled over slot t and 0 otherwise. We denote the probability that node i be scheduled with $p_j^M \triangleq \mathbb{P}\left(i^M(t) = i\right)$ and the associated uplink channel rate when node i is scheduled with $\bar{R}_i^M \triangleq \mathbb{E}\left[R_i(t) | i = i^M(t)\right]$, where the expectations are over the conditional joint distribution of the instantaneous rates of all uplink channels, given $i = i^M(t)$.

As will be shown shortly, confidential opportunistic scheduling achieves a confidential information rate $R_i^{\text{conf}} = p_i^M(\bar{R}_i^M - \bar{R}_i^m)$ for all $i \in \{1, \ldots, n\}$. To achieve this set of rates, we use the following confidential encoding strategy based on binning: To begin, node i generates $2^{Np_i^M(\bar{R}_i^M - \delta)}$ random binary sequences. Then, it assigns each random binary sequence to one of $2^{NR_i^{\text{conf}}}$ bins, so that each bin contains exactly $2^{Np_i^M(\bar{R}_i^m - \delta)}$ binary sequences. We call the sequences associated with a bin, the *randomization sequences* of that bin. Each bin of node i is one-to-one matched with a confidential message $w \in \{1, \ldots, 2^{NR_i^{\text{conf}}}\}$ randomly. This selection (along with the binary sequences contained in each bin) is revealed to the base station and all nodes before the communication starts. Then, whenever the message to be transmitted is selected by node i, the stochastic encoder of that node chooses one of the randomization sequences associated with each bin at random[2], independently and uniformly over

[2] In case of joint encoding of confidential and open information, the randomization sequence is chosen appropriately, corresponding to the desired open message.

all randomization sequences associated with that bin. This particular randomization message is used for the transmission of the message and is not revealed to any of the nodes nor to the base station.

Confidential opportunistic scheduler schedules node $i^M(t)$ in each slot t and the transmitter transmits $N_1 R_{i^M(t)}(t)$ bits of the binary sequence associated with the message of node $i^M(t)$ for all $t \in \{1, \ldots, N_2\}$. Thus, asymptotically, the rate of data transmitted by node i over N_2 slots is identical to:

$$\begin{aligned}\lim_{N_1, N_2 \to \infty} \frac{1}{N} \sum_{t=1}^{N_2} N_1 \mathcal{I}_i^{\mathrm{COS}}(t) R_i(t) &= \lim_{N_1, N_2 \to \infty} \frac{1}{N_2} \sum_{t=1}^{N_2} \mathcal{I}_i^{\mathrm{COS}}(t) R_i(t) \\ &\geq p_i^M (\bar{R}_i^M - \delta) \ \text{ w.p. 1} \qquad (3.14)\end{aligned}$$

for any given $\delta > 0$ from strong law of large numbers. Hence, all of $N(p_i^M(\bar{R}_i^M - \delta))$ bits, generated by each node i is transmitted with probability 1.

Achievable uplink rates with confidential opportunistic scheduling

Theorem 2. *With confidential opportunistic scheduling, a confidential information rate of $R_i^{conf} = p_i^M(\bar{R}_i^M - \bar{R}_i^m)$ is achievable for each node i.*

Proof. The proof of this theorem is based on an equivocation analysis. Let us further introduce the following notation:

W_i^{rand}: randomization sequence associated with message W_i^{conf},

$\mathbf{X}(t)$: transmitted vector of (N_1) symbols over slot t,

$\mathbf{X}_i = \{\mathbf{X}(t) | \mathcal{I}_i^{\mathrm{COS}}(t) = 1\}$: the transmitted signal over slot t, whenever $\mathcal{I}_i^{\mathrm{COS}}(t) = 1$ (i.e., node i is the active transmitter)

$\mathbf{Y}_i(t)$: the received vector of symbols at node i ($\mathbf{Y}_b(t)$ for the base station) over slot t,

$\mathbf{Y}_i^j = \{\mathbf{Y}_i(t) | \mathcal{I}_i^{\mathrm{COS}}(t) = 1\}$: the received signal at node i over slot t, whenever $\mathcal{I}_i^{\mathrm{COS}}(t) = 1$ (i.e., node i is the active transmitter). We use $\mathbf{Y}_i^j$ for the received signal by the base station.

The equivocation analysis follows directly for the described secrecy scheme: For any given node i, we have

$$\begin{align}
H(W_i^{\text{conf}}|\mathbf{Y}_i^j) &\geq H(W_i^{\text{conf}}|\mathbf{Y}_{i^*(j)}^j) \tag{3.15}\\
&= I(W_i^{\text{conf}};\mathbf{Y}_1^j,\ldots,\mathbf{Y}_n^j|\mathbf{Y}_{i^*(j)}^j) + H(W_i^{\text{conf}}|\mathbf{Y}_1^j,\ldots,\mathbf{Y}_n^j) \nonumber\\
&\geq I(W_i^{\text{conf}};\mathbf{Y}_1^j,\ldots,\mathbf{Y}_n^j|\mathbf{Y}_{i^*(j)}^j) \nonumber\\
&= I(W_i^{\text{conf}},W_i^{\text{rand}};\mathbf{Y}_1^j,\ldots,\mathbf{Y}_n^j|\mathbf{Y}_{i^*(j)}^j) \nonumber\\
&\qquad - I(W_i^{\text{rand}};\mathbf{Y}_1^j,\ldots,\mathbf{Y}_n^j|\mathbf{Y}_{i^*(j)}^j,W_i^{\text{conf}}) \tag{3.16}\\
&= I(W_i^{\text{conf}},W_i^{\text{rand}};\mathbf{Y}_1^j,\ldots,\mathbf{Y}_n^j|\mathbf{Y}_{i^*(j)}^j) \nonumber\\
&\qquad - H(W_i^{\text{rand}}|\mathbf{Y}_{i^*(j)}^j,W_i^{\text{conf}}) \nonumber\\
&\qquad + H(W_i^{\text{rand}}|\mathbf{Y}_1^j,\ldots,\mathbf{Y}_n^j,W_i^{\text{conf}}) \nonumber\\
&\geq I(W_i^{\text{conf}},W_i^{\text{rand}};\mathbf{Y}_1^j,\ldots,\mathbf{Y}_n^j|\mathbf{Y}_{i^*(j)}^j) \nonumber\\
&\qquad - H(W_i^{\text{rand}}|\mathbf{Y}_{i^*(j)}^j,W_i^{\text{conf}}) \nonumber\\
&\geq I(W_i^{\text{conf}},W_i^{\text{rand}};\mathbf{Y}_1^j,\ldots,\mathbf{Y}_n^j|\mathbf{Y}_{i^*(j)}^j) - N\varepsilon_1 \tag{3.17}\\
&= I(\mathbf{X}_i;\mathbf{Y}_1^j,\ldots,\mathbf{Y}_n^j|\mathbf{Y}_{i^*(j)}^j) \nonumber\\
&\quad - I(\mathbf{X}_i;\mathbf{Y}_1^j,\ldots,\mathbf{Y}_n^j|\mathbf{Y}_{i^*(j)}^j,W_i^{\text{conf}},W_i^{\text{rand}}) - N\varepsilon_1 \tag{3.18}\\
&\geq I(\mathbf{X}_i;\mathbf{Y}_1^j,\ldots,\mathbf{Y}_n^j|\mathbf{Y}_{i^*(j)}^j) - N(\varepsilon_1+\varepsilon_2) \tag{3.19}\\
&= I(\mathbf{X}_i;\mathbf{Y}_1^j,\ldots,\mathbf{Y}_n^j) - I(\mathbf{X}_i;\mathbf{Y}_{i^*(j)}^j) - N(\varepsilon_1+\varepsilon_2) \tag{3.20}\\
&\geq I(\mathbf{X}_i;\mathbf{Y}_i^j) - I(\mathbf{X}_i;\mathbf{Y}_{i^*(j)}^j) - N(\varepsilon_1+\varepsilon_2) \tag{3.21}\\
&= \sum_{k:\mathcal{I}_i^{\text{COS}}(t)=1} \big[I(\mathbf{X}(t);\mathbf{Y}_i(t)) - I(\mathbf{X}(t);\mathbf{Y}_{i^*(j)}(t))\big] \nonumber\\
&\qquad\qquad\qquad - N(\varepsilon_1+\varepsilon_2) \tag{3.22}\\
&\geq N\left[p_i^M\left((\bar{R}_i^M-\delta)-\bar{R}_i^m\right)-(\varepsilon_1+\varepsilon_2+\varepsilon_3)\right] \tag{3.23}
\end{align}$$

with probability 1, for any positive $(\varepsilon_1,\varepsilon_2,\varepsilon_3)$ triplet and arbitrarily small δ, as N_1, N_2 go to ∞. Here, (3.15) follows since $i^*(j) = \text{argmax}_{i\in\{1,\ldots,n\}} I(W_i^{\text{conf}};\mathbf{Y}_i^j)$ ($W_i^{\text{conf}} \leftrightarrow \mathbf{X}_i \leftrightarrow \mathbf{Y}_{i^*(j)}^j \leftrightarrow \mathbf{Y}_i^j$ forms a Markov chain for all i and data processing inequality), (3.16) is by the chain rule, (3.17) follows from the application of Fano's inequality (as we choose the rate of the randomization sequence to be $N(\bar{R}_i^m-\delta) < I(W_i^{\text{rand}};\mathbf{Y}_{i^*(j)}^j)$, which allows for the randomization message to be decoded at node $i^*(j)$, given the bin index), (3.18) follows from the chain rule and that $(W_i^{\text{conf}}, W_i^{\text{rand}}) \leftrightarrow \mathbf{X}_i \leftrightarrow (\mathbf{Y}_1^j, \ldots, \mathbf{Y}_n^j)$ forms a Markov chain, (3.19) holds since $I(\mathbf{X}_i; \mathbf{Y}_1^j, \ldots, \mathbf{Y}_n^j | \mathbf{Y}_{i^*(j)}^j, W_i^{\text{conf}}, W_i^{\text{rand}}) \leq N\varepsilon_2$ as the transmitted symbol sequence $\mathbf{X}_i$ is determined w.p.1 given $(\mathbf{Y}_{i^*(j)}^j, W_i^{\text{conf}}, W_i^{\text{rand}})$, (3.20) follows from the chain rule, (3.21) holds since $\mathbf{Y}_i^j(t)$ is an entry of vector $[\mathbf{Y}_1^j(t), \ldots, \mathbf{Y}_n^j(t)]$, (3.22) holds because the fading processes are iid, and finally (3.23) follows from strong law of large numbers.

Thus, with the described secrecy scheme, the perfect secrecy constraint is satisfied for all nodes, since for any $j \in \{1, \ldots, n\}$, we have

$$\begin{aligned}
\frac{1}{N} I(W_i^{\text{conf}}; \mathbf{Y}_i^j) &= \frac{1}{N}(H(W_i^{\text{conf}}) - H(W_i^{\text{conf}} | \mathbf{Y}_i^j)) \\
&\leq R_i^{\text{conf}} - \left[p_i^M \left((\bar{R}_i^M - \delta) - \bar{R}_i^m\right) - (\varepsilon_1 + \varepsilon_2 + \varepsilon_3)\right] \\
&\leq \varepsilon, \qquad (3.24)
\end{aligned}$$

for any given $\varepsilon > 0$. We just showed that, with confidential opportunistic scheduling, a confidential information rate of $R_i^{\text{conf}} = p_i^M(\bar{R}_i^M - \bar{R}_i^m)$ is achievable for any given node i.

□

Next we show that confidential opportunistic scheduling maximizes the achievable sum confidential information rate among all schedulers.

Theorem 3. *Among the elements of the set of all schedulers, $\{\mathcal{I}(R_1, \ldots, R_n)\}$, confidential opportunistic scheduler $\mathcal{I}^{COS}(R_1, \ldots, R_n)$ maximizes the sum confidential uplink rate, $R_{sum,up}^{conf} = \sum_{j=1}^n R_i^{conf}$. Furthermore, the maximum achievable sum confidential uplink rate is*

$$R_{sum,up}^{conf} = \sum_{j=1}^{n} \left[p_i^M \left(\bar{R}_i^M - \bar{R}_i^m\right)\right].$$

Proof. The proof uses the notation introduced in the first paragraph of the proof of Theorem 2. To meet the perfect secrecy constraint, it is necessary and sufficient to guarantee $\lim_{N\to\infty} \frac{1}{N} I(W_i^{\text{conf}}; \mathbf{Y}_{i^*(j)}^j) \leq \varepsilon$ for all nodes $j \in \{1, \ldots, n\}$. Since $n < \infty$, one can write an equivalent condition on the sum mutual information over each node:

$$
\begin{aligned}
\varepsilon' &\geq \frac{1}{N}\sum_{j=1}^{n} I(W_i^{\text{conf}}; \mathbf{Y}_{i^*(j)}^j) \\
&= \frac{1}{N}\sum_{j=1}^{n} \Big[H(W_i^{\text{conf}}) - H(W_i^{\text{conf}}|\mathbf{Y}_{i^*(j)}^j)\Big] \\
&= R_{\text{sum}}^{\text{conf}} - \frac{1}{N}\sum_{j=1}^{n} H(W_i^{\text{conf}}|\mathbf{Y}_{i^*(j)}^j) && (3.25) \\
&= R_{\text{sum}}^{\text{conf}} - \frac{1}{N}\sum_{j=1}^{n} \Big[I(W_i^{\text{conf}}; \mathbf{Y}_1^j, \ldots, \mathbf{Y}_n^j|\mathbf{Y}_{i^*(j)}^j) \\
&\qquad\qquad + H(W_i^{\text{conf}}|\mathbf{Y}_1^j, \ldots, \mathbf{Y}_n^j)\Big] \\
&\geq R_{\text{sum}}^{\text{conf}} - \frac{1}{N}\sum_{j=1}^{n} \Big[I(W_i^{\text{conf}}, W_i^{\text{rand}}; \mathbf{Y}_1^j, \ldots, \mathbf{Y}_n^j|\mathbf{Y}_{i^*(j)}^j) \\
&\qquad - I(W_i^{\text{rand}}; \mathbf{Y}_1^j, \ldots, \mathbf{Y}_n^j|\mathbf{Y}_{i^*(j)}^j, W_i^{\text{conf}}) + N\varepsilon_4\Big] && (3.26) \\
&\geq R_{\text{sum}}^{\text{conf}} - \frac{1}{N}\sum_{j=1}^{n} \Big[I(W_i^{\text{conf}}, W_i^{\text{rand}}; \mathbf{Y}_1^j, \ldots, \mathbf{Y}_n^j|\mathbf{Y}_{i^*(j)}^j) + N\varepsilon_4\Big] \\
&\geq R_{\text{sum}}^{\text{conf}} - \frac{1}{N}\sum_{j=1}^{n} \Big[I(\mathbf{X}_i; \mathbf{Y}_1^j, \ldots, \mathbf{Y}_n^j|\mathbf{Y}_{i^*(j)}^j) + N\varepsilon_4\Big] && (3.27) \\
&= R_{\text{sum}}^{\text{conf}} - \frac{1}{N}\sum_{j=1}^{n} \Big[I(\mathbf{X}_i; \mathbf{Y}_1^j, \ldots, \mathbf{Y}_n^j) - I(\mathbf{X}_i; \mathbf{Y}_{i^*(j)}^j) + N\varepsilon_4\Big] && (3.28) \\
&= R_{\text{sum}}^{\text{conf}} - \frac{1}{N}\sum_{j=1}^{n} \big[I(\mathbf{X}_i; \mathbf{Y}_i^j) + I(\mathbf{X}_i; \mathbf{Y}_1^j, \ldots, \mathbf{Y}_n^j|\mathbf{Y}_i^j) \\
&\qquad - I(\mathbf{X}_i; \mathbf{Y}_{i^*(j)}^j) + N\varepsilon_4\Big] && (3.29) \\
\geq R_{\text{sum}}^{\text{conf}} &- \frac{1}{N}\sum_{j=1}^{n} \Big[I(\mathbf{X}_i; \mathbf{Y}_i^j) + H(\mathbf{X}_i|\mathbf{Y}_i^j) - I(\mathbf{X}_i; \mathbf{Y}_{i^*(j)}^j) + N\varepsilon_4\Big] \\
\geq R_{\text{sum}}^{\text{conf}} &- \frac{1}{N}\sum_{j=1}^{n} \Big[I(\mathbf{X}_i; \mathbf{Y}_i^j) + H(W_i^{\text{conf}}|\mathbf{Y}_i^j) - I(\mathbf{X}_i; \mathbf{Y}_{i^*(j)}^j) + N\varepsilon_4\Big] && (3.30) \\
&\geq R_{\text{sum}}^{\text{conf}} - \frac{1}{N}\sum_{j=1}^{n} \Big[I(\mathbf{X}_i; \mathbf{Y}_i^j) - I(\mathbf{X}_i; \mathbf{Y}_{i^*(j)}^j) + N(\varepsilon_4 + \varepsilon_5)\Big] && (3.31) \\
&= R_{\text{sum}}^{\text{conf}} - \frac{1}{N}\sum_{j=1}^{n} \Bigg\{\sum_{k:\mathcal{I}_i(t)=1} [I(\mathbf{X}(t); \mathbf{Y}_b(t)) \\
&\qquad\qquad - I(\mathbf{X}(t); \mathbf{Y}_{i^*(j)}(t))\big] + \varepsilon_4 + \varepsilon_5\big\} && (3.32) \\
&\geq R_{\text{sum}}^{\text{conf}} - \frac{1}{N}\sum_{j=1}^{n} \max_{\mathcal{I}_i(t)} \Bigg\{\sum_{k:\mathcal{I}_i(t)=1} [I(\mathbf{X}(t); \mathbf{Y}_b(t))
\end{aligned}
$$

with probability 1, for any positive ε' and $(\varepsilon_4, \varepsilon_5, \varepsilon_6)$ triplet as N_1, N_2 go to ∞. Here, (3.25) follows from the definition of $R_{\text{sum}}^{\text{conf}}$ and that $\frac{1}{N}H(W_i^{\text{conf}}) = R_i^{\text{conf}}$; (3.26) follows from the chain rule and Fano's inequality (as $H(W_i^{\text{conf}}|\mathbf{Y}_1^j, \ldots, \mathbf{Y}_n^j) \leq H(W_i^{\text{conf}}, W_i^{\text{rand}}|\mathbf{Y}_1^j, \ldots, \mathbf{Y}_n^j) \leq N\varepsilon_4$ since the message pair $(W_i^{\text{conf}}, W_i^{\text{rand}})$ can be decoded with arbitrarily low probability of error given $(\mathbf{Y}_1^j, \ldots, \mathbf{Y}_n^j)$); (3.27) is from the data processing inequality as $(W_i^{\text{conf}}, W_i^{\text{rand}}) \leftrightarrow \mathbf{X}_i \leftrightarrow (\mathbf{Y}_1^j, \ldots, \mathbf{Y}_n^j)$ forms a Markov chain; (3.28) and (3.29) follow from the chain rule; (3.30) follows from the data processing inequality; (3.31) follows since node i decodes message W_i^{conf} with arbitrarily low probability of error ε_5; (3.32) holds since the fading processes are iid; (3.33) holds because confidential opportunistic scheduler chooses $\mathcal{I}_i^{\text{COS}}(t) = \text{argmax}_{\mathcal{I}_i(t)}[R_i(t) - R_{ji^*(j)}(t)] = \text{argmax}_{\mathcal{I}_i(t)}\left[I(\mathbf{X}(t); \mathbf{Y}_b(t)) - I(\mathbf{X}(t); \mathbf{Y}_{i^*(j)}(t))\right]$ for all t; and finally (3.34) follows by an application of the strong law of large numbers. The above derivation leads to the desired result:

$$R_{\text{sum}}^{\text{conf}} \leq \sum_{j=1}^{n} \left[p_i^M \left(\bar{R}_i^M - \bar{R}_i^m\right)\right]. \tag{3.35}$$

We complete the proof noting that the above sum rate is achievable by confidential opportunistic scheduling as shown in (3.23).

Note that, from the above steps, we can also see that the individual confidential information rates given in Theorem 2 are the maximum achievable individual rates with confidential opportunistic scheduling. This is due to the fact that, for any node i, with confidential opportunistic scheduling, the above derivation lead to:

$$\frac{1}{N}H(W_i^{\text{conf}}|\mathbf{Y}_{i^*(j)}^j) \leq p_i^M \left(\bar{R}_i^M - \bar{R}_i^m\right) + \varepsilon \tag{3.36}$$

for any $\varepsilon > 0$ as $N \to \infty$. Consequently, with confidential opportunistic scheduling, no node can achieve any individual confidential rate above that given in (3.36), hence the converse of Theorem 2 also holds.

□

There, we also show that the individual confidential information rates given in Theorem 2 are the maximum achievable individual rates with confidential opportunistic

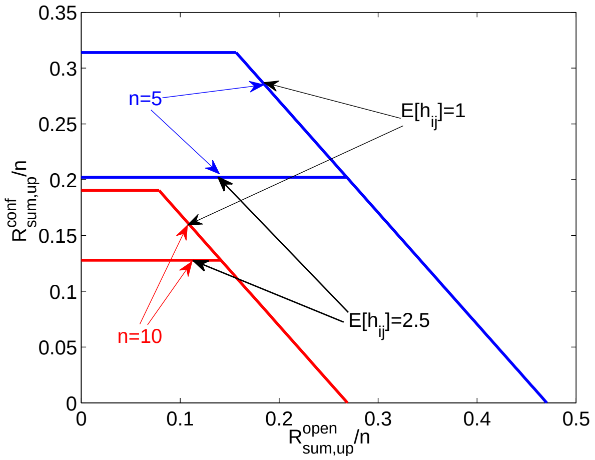


Figure 3.6: Bounds on the achievable sum rate region for the multiuser uplink scenario with iid Rayleigh block fading channels.

scheduling. Hence the converse of Theorem 2 also holds. Combining Theorems 2 and 3, one can realize that confidential opportunistic scheduling achieves the maximum achievable sum confidential information rate. Thus, one cannot increase the individual confidential information rate a single node achieves with COS by an amount $\Delta > 0$, without reducing another node's confidential information rate by more than Δ.

Next, we find the boundary of the region of achievable sum open and sum confidential uplink rate pair with *joint encoding of confidential and open information.* In opportunistic scheduling [55, 94] without any secrecy constraint, the user with the best uplink channel is scheduled for all slots t. Hence, the associated achievable rate can be written as $R^{\text{opp}}_{\text{sum,up}} = \mathbb{E}\left[\max_{j\in\{1,\ldots,n\}} R_i(t)\right]$. Since this constitutes an upper bound for the achievable cumulative information rate [94], the total confidential and open information rate in our system cannot exceed $R^{\text{opp}}_{\text{sum,up}}$. Combining this with Theorem 3, we can characterize an outer bound for the achievable rate region for the sum rates as follows: (i) $R^{\text{conf}}_{\text{sum,up}} + R^{\text{open}}_{\text{sum,up}} \leq R^{\text{opp}}_{\text{sum,up}}$; (ii) $R^{\text{conf}}_{\text{sum,up}} \leq \sum_{j=1}^{n}\left[p_i^M\left(\bar{R}_i^M - \bar{R}_i^m\right)\right]$. Next we illustrate this region and discuss how the entire region can be achieved by COS along with joint encoding of confidential and open messages.

The boundaries of this region is illustrated in Fig. 3.6 for a 5-node and a 10-node system. We assume all channels to be iid Rayleigh fading with mean uplink channel power gain $\mathbb{E}[h_i] = 2$ and mean cross channel power gain $\mathbb{E}[h_{ij}] = 1$ or 2.5 in two separate scenarios for all (i, j). Noise is additive Gaussian with unit variance and transmit power $P = 1$. In these graphs, sum rates are normalized with respect to the number of nodes. One can observe that, the achievable sum rate per node decreases from 0.31 to 0.19 bits/channel use/node for $\mathbb{E}[h_{ij}] = 1$ and from 0.2 to 0.13 bits/channel use/node for $\mathbb{E}[h_{ij}] = 2.5$ as the number of nodes increases from 5 to 10. Also, the open rate per node drops from 0.47 to 0.27 bits/channel use/node with the same increase in the number of nodes.

Note that, any point on the part of the boundary specified by (i) above (flat portion on the top part) is achievable by COS and jointly encoding the confidential information with the appropriate amount of open information used as a randomization message. For instance, the corner point of two boundaries (intersection of (i) and (ii)) is achieved when open information is used completely in place of randomization messages by all nodes. All points on the part of the boundary specified by (ii) can be achieved by time-sharing between the corner point, and point $\left(R^{\text{opp}}_{\text{sum,up}}, 0\right)$, which corresponds to opportunistic scheduling (without secrecy).

Downlink Scenario

Although our main concern in this paper is the opportunistic scheduling subject to perfect secrecy constraint on the uplink channel, we briefly discuss achievable rates on the downlink channel as well. Most of the discussion on downlink channel follows the same line of arguments as given for the uplink channel, so we omit the details. In the multiuser downlink scenario, the base station has a confidential message $W^{\text{conf}}_i \in \{1, \ldots, 2^{NR^{\text{conf}}_i}\}$ to be transmitted to node j, $1 \leq j \leq n$ over the associated downlink channel and all other nodes $i, i \neq j$ overhear the transmission over their downlink channels. The perfect secrecy constraint is required for each message W^{conf}_i and all nodes $i \neq j$. We assume throughout this section that the base station has perfect causal knowledge of the downlink channel rates, i.e., $R_i(t)$ is available at the base station before every block t.

Confidential Opportunistic Scheduling for downlink: Analogous to the uplink scenario, COS schedules one of the nodes for data transmission in a given block. In particular, in slot t, COS schedules the node with the largest instantaneous downlink channel rate:

$$i^M(t) = \operatorname*{argmax}_{i \in \{1,\ldots,n\}} R_i(t)$$

and the indicator variable $\mathcal{I}_i^{\text{COS}}(t)$ takes on a value 1, if node i is scheduled over slot t and 0 otherwise. In case of multiple nodes achieving the maximum downlink channel rate, the tie can be broken at random. Note that in downlink case, scheduling decision only depends on the instantaneous direct downlink rate rather than the instantaneous confidential information rate. This is quite simple, because unlike the uplink case there is a single transmitter. Let $p_i^M \triangleq \mathbb{P}\left(i^M(t) = i\right)$ and $\bar{R}_i^M \triangleq \mathbb{E}\left[R_i(t)|j = j^M(t)\right]$, where the expectation is over the joint conditional distribution of the instantaneous rates of all channels, given $i = i^M(t)$. Let us denote the node with the highest mean downlink rate with:

$$i^m = \operatorname*{argmax}_{i \in \{1,\ldots,n\}} \mathbb{E}\left[R_i(t)\right]$$

and the node with the second best mean achievable rate with:

$$i^{m'} = \operatorname*{argmax}_{i \neq i^m} \mathbb{E}\left[R_i(t)\right].$$

Also, the associated achievable rates are $\bar{R}^m \triangleq \mathbb{E}\left[R_{i^m}(t)\right]$ and $\bar{R}^{m'} \triangleq \mathbb{E}\left[R_{i^{m'}}(t)\right]$.

As will be shown shortly, confidential opportunistic scheduling achieves a confidential information rate $R_i^{\text{conf}} = p_i^M(\bar{R}_i^M - \bar{R}^m)$ for all $j \neq j^m$ and $R_{j^m}^{\text{conf}} = p_{j^m}^M(\bar{R}_{j^m}^M - \bar{R}^{m'})$. Note that by definition $\bar{R}_i^M \geq \bar{R}^m$, since $\bar{R}_i^M$ is the expectation of the maximum rate at every block whereas $\bar{R}^m$ is the mean rate of the user with the highest expected rate over all slots. To achieve this set of rates, we use a similar secrecy encoding strategy based on binning that we have discussed for the uplink scenario.

Achievable downlink rates with confidential opportunistic scheduling: Next, we state the theorems that characterize the achievable confidential information rates in the downlink setting. These theorems are analogous to their counterparts in the uplink scenario. We skip the proofs of these theorems for brevity, as they follow the identical steps as the proofs of Theorems 2 and 3.

Theorem 4. *With confidential opportunistic scheduling, a confidential information rate of* $R_{i^m}^{conf} = p_{i^m}^M(\bar{R}_{i^m}^M - \bar{R}^{m'})$ *is achievable for node* j^m *and a confidential information rate of* $R_i^{conf} = p_i^M(\bar{R}_i^M - \bar{R}^m)$ *is achievable for every other node* $i \neq i^m$.

Here, for node i^m, node $i^{m'}$ plays the role of node $i^*(j^m)$, which had the best cross channel from node i in the corresponding uplink scenario. Similarly, for any other node $i \neq i^m$, node i^m plays the role of $i^*(j)$ in the associated uplink scenario. With $i^*(j^m)$ and $i^*(j)$ replaced with $i^{m'}$ and i^m respectively, the proof of this theorem is identical to the proof of Theorem 2. Also, similar to the uplink scenario, confidential opportunistic scheduling maximizes the achievable sum confidential information rate among all schedulers:

Theorem 5. *Among the elements of the set of all schedulers,* $\{\mathcal{I}(\mathbf{R})\}$, $j \in \{1, \ldots, n\}$, *confidential opportunistic scheduler* $\mathcal{I}^{COS}(\mathbf{R})$ *maximizes the sum confidential downlink rate,* $R_{sum,down}^{conf} = \sum_{i=1}^n R_i^{conf}$. *Furthermore, the maximum achievable sum confidential downlink rate is*

$$\begin{aligned} R_{sum,down}^{conf} &= p_{j^m}^M(\bar{R}_{j^m}^M - \bar{R}^{m'}) + \sum_{j \neq j^m} \left[p_i^M \left(\bar{R}_i^M - \bar{R}^m \right) \right] \\ &= \bar{R}^M - \bar{R}^m + p_{j^m}^M(\bar{R}^m - \bar{R}^{m'}), \end{aligned}$$

where $\bar{R}^M = \mathbb{E}\left[\max_{1 \leq j \leq n} R_i(t)\right]$.

Likewise, the proof of this theorem follows the identical line of argument as the proof of Theorem 3, with $i^*(j^m)$ and $i^*(j)$ replaced with $i^{m'}$ and i^m respectively. Also, the individual confidential information rates given in Theorem 4 are the maximum achievable individual rates with confidential opportunistic scheduling. Hence the converse of Theorem 4 also holds. Theorems 4 and 5 combine to show that confidential opportunistic scheduling achieves the maximum achievable sum confidential information rate.

Note that $\bar{R}^M$ in Theorem 5 is the achievable rate with opportunistic scheduling without any secrecy constraint. Based on the discussions given in Section 3.3.1, with *joint encoding of confidential and open information*, the boundary of the region

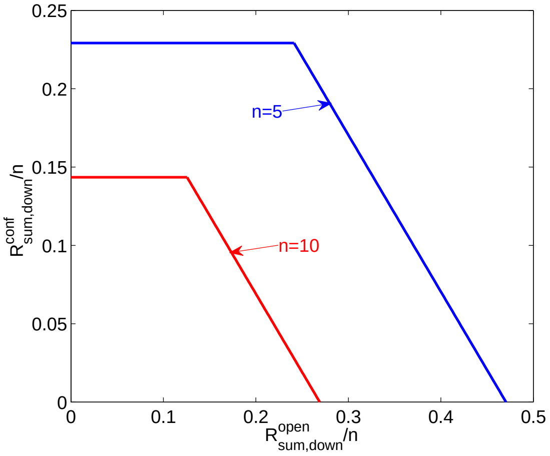


Figure 3.7: Boundaries of the achievable sum rate region for the multiuser downlink scenario with iid Rayleigh block fading channels.

of achievable sum open and sum confidential rate pairs can be characterized by: (i) $R^{\text{conf}}_{\text{sum,down}} + R^{\text{open}}_{\text{sum,down}} \leq \bar{R}^M$; (ii) $R^{\text{conf}}_{\text{sum,down}} \leq \bar{R}^M - \bar{R}^m + p^M_{jm}(\bar{R}^m - \bar{R}^{m'})$. The entire region can be achieved by opportunistic secrecy encoding along with the probabilistic scheme for joint encoding of confidential and open messages for each individual node, as described in Section 3.3.1.

The boundaries of this region is illustrated in Fig. 3.7 for a 5-node and a 10-node system. We assume all channels to be iid Rayleigh fading with mean downlink channel power gain $\mathbb{E}[h_i] = 2$. Noise is additive Gaussian with unit variance and transmit power $P = 1$. In these graphs, sum rates are normalized with respect to the number of nodes.

3.4 Dynamic Control of Confidential Communications

In Section 3.3, we determined the achievable confidential information rate regions associated with confidential opportunistic scheduling which encodes messages over *many slots*. Hence, the delay of decoding confidential information may be extremely long. Also, the confidential opportunistic scheduler was based on the availability of full CSI on the uplinks, and long-term average of cross-channel rates. In this section, we investigate a dynamic control algorithm which does not rely on any a priori knowledge of distributions of direct- or cross-channel rates, and the confidential information is encoded over *a single block*. Hence, a confidential message can be decoded with a maximum delay of only a single block duration. Note that even though by encoding over many slots one may achieve higher confidential information rates, decoding delay may be a more important concern in many practical scenarios.

In particular, each message W_i^{conf} and W_i^{open} are broken into a sequence of messages, $W_i^{\text{conf}}(t)$ and $W_i^{\text{open}}(t)$ respectively and each element of the sequence is encoded into an individual packet, encoded over slot t. The *delay-limited* dynamic cross-layer control algorithm opportunistically schedules the nodes with the objective of maximizing the total expected utility gained from each packet transmission while maintaining the stability of confidential and open traffic queues. The algorithm takes as input the queue lengths and instantaneous direct- and cross-channel rates, and gives as output the scheduled node and its secrecy encoding rate. In the sequel, we only consider joint encoding of confidential and open information as described in Section 3.3.1.

Let $g_i^{\text{conf}}(t)$ and $g_i^{\text{open}}(t)$ be the utilities obtained by node i from confidential and open transmissions over slot t respectively. Let us define the instantaneous confidential information rate of node i as $R_i^p(t) \triangleq \min_{i \neq j} R_{ij}^p(t)$, where $R_{ij}^p(t)$ was defined in (3.4). Also, the instantaneous open rate, $R_i^o(t)$, is the amount of open information node i transmits over slot t. The utility over slot t depends on rates $R_i^p(t)$, and $R_i^o(t)$. In general, this dependence can be described as $g_i^{\text{conf}}(t) = U_i^{\text{conf}}(R_i^p(t))$ and $g_i^{\text{open}}(t) = U_i^{\text{open}}(R_i^o(t))$. Assume that $U_i^{\text{conf}}(0) = 0$, $U_i^{\text{open}}(0) = 0$, and $U_i^{\text{conf}}(\cdot)$, $U_i^0(\cdot)$ are concave non-decreasing functions. We also assume that the utility of a confidential transmission is higher than the utility of open transmission at the same rate. The amount of open traffic $A_i^{\text{open}}(t)$, and confidential traffic $A_i^{\text{conf}}(t)$ injected in the queues at node i have long term arrival rates λ_i^{open} and λ_i^{conf} respectively. Our objective is to support a fraction of the traffic demand to achieve a long term confidential and open throughput that maximizes the sum of utilities of the nodes.

3.4.1 Perfect Knowledge of Instantaneous CSI

We first consider the case when every node i has perfect causal knowledge of its uplink channel rate, $R_i(t)$, and cross-channel rates to all other nodes in the network $R_{ij}(t)$, $\forall j \neq i$, for all slots t. The dynamic control algorithm developed for this case will then provide a basis for the algorithm that we are going to develop for a more realistic case when cross-channel rates are not known perfectly. We aim to find the solution of the following optimization problem:

$$\max \sum_{j=1}^{n} \left(\mathbb{E}\left[g_i^{\text{conf}}(t) \right] + \mathbb{E}\left[g_i^{\text{open}}(t) \right] \right) \tag{3.37}$$

$$\text{subject to } (\lambda_i^{\text{open}}, \lambda_i^{\text{conf}}) \in \Lambda \tag{3.38}$$

The objective function in (3.37) calculates the total expected utility of open and confidential communications where expectation is taken over the random achievable rates (random channel conditions), and possibly over the randomized policy. The constraint (3.38) ensures that confidential and open injection rates are within the achievable rate region supported by the network denoted by Λ. In the aforementioned optimization problem, it is implicitly required that perfect secrecy condition given in (5.2) is satisfied in each block as $N_1 \to \infty$.

The proposed cross-layer dynamic control algorithm is based on the stochastic network optimization framework developed in [97]. This framework allows the solution of a long-term stochastic optimization problem without requiring explicit characterization of the achievable rate region, Λ.

We assume that there is an infinite backlog of data at the transport layer of each node. Our proposed dynamic flow control algorithm determines the amount of open and confidential traffic injected into the queues at the network layer. The dynamics of confidential and open traffic queues is given as follows:

$$Q_i^{\text{conf}}(k+1) = \left[Q_i^{\text{conf}}(t) - R_i^{p}(t) \right]^{+} + A_i^{\text{conf}}(t), \tag{3.39}$$

$$Q_i^{\text{open}}(k+1) = \left[Q_i^{\text{open}}(t) - R_i^{o}(t) \right]^{+} + A_i^{\text{open}}(t), \tag{3.40}$$

where $[x]^+ = \max\{0, x\}$, and the service rates of confidential and open queues are given as,

$$R_i^{\text{conf}}(t) = \mathcal{I}_i^{\text{conf}}(t) \left[R_i(t) - \max_{j \neq i} R_{ij}(t) \right], \text{ and}$$
$$R_i^o(t) = \mathcal{I}_i^{\text{open}}(t) R_i(t) + \mathcal{I}_i^{\text{conf}}(t)(R_i(t) - R_i^p(t)).$$

where $\mathcal{I}_i^{\text{conf}}(t)$ and $\mathcal{I}_i^{\text{open}}(t)$ are indicator functions taking value $\mathcal{I}_i^{\text{conf}}(t) = 1$ when transmitting jointly encoded confidential *and* open traffic, or $\mathcal{I}_i^{\text{open}}(t) = 1$ when transmitting *only* open traffic over slot t respectively. Also note that at any slot t, $\sum_i \mathcal{I}_i^{\text{conf}}(t) + \mathcal{I}_i^{\text{open}}(t) \leq 1$.

Control Algorithm: The algorithm is a simple index policy and it executes the following steps in each slot t:

(1) Flow control: For some $V > 0$, each node i injects $A_i^{\text{conf}}(t)$ confidential and $A_i^{\text{open}}(t)$ open bits, where

$$\left(A_i^{\text{conf}}(t), A_i^{\text{open}}(t)\right) = \underset{A^{\text{conf}}, A^{\text{open}}}{\text{argmax}} \left\{ V \left[U_i^{\text{conf}}(A^{\text{conf}}) + U_i^{\text{open}}(A^{\text{open}}) \right] \right.$$
$$\left. - \left(Q_i^{\text{conf}}(t) A^{\text{conf}} + Q_i^{\text{open}}(t) A^{\text{open}} \right) \right\}$$

(2) Scheduling: Schedule node i and transmit jointly encoded *confidential and open* traffic ($\mathcal{I}_i^{\text{conf}} = 1$), or *only open* ($\mathcal{I}_i^{\text{open}} = 1$) traffic, where

$$(\mathcal{I}_i^{\text{conf}}(t), \mathcal{I}_i^{\text{open}}(t)) = \underset{\mathcal{I}^{\text{conf}}, \mathcal{I}^{\text{open}}}{\text{argmax}} \left\{ Q_i^{\text{conf}}(t) R_i^p(t) + Q_i^{\text{open}}(t) R_i^o(t) \right\},$$

and for each node i, encode confidential data over each slot t at rate

$$R_i^p(t) = \mathcal{I}_i^{\text{conf}}(t) \left[R_i(t) - \max_{i \neq j} R_{ij}(t) \right],$$

and transmit open data at rate

$$R_i^o(t) = \mathcal{I}_i^{\text{open}}(t) R_i(t) + \mathcal{I}_i^{\text{conf}}(t)(R_i(t) - R_i^p(t))$$

Optimality of Control Algorithm

The optimality of the algorithm can be shown using the Lyapunov optimization theorem [6]. For our purposes, we consider confidential and open unfinished work vectors as $\mathbf{Q}^{\text{conf}}(\mathbf{t}) = (Q_1^{\text{conf}}(t), Q_2^{\text{conf}}(t), \ldots, Q_n^{\text{conf}}(t))$, and $\mathbf{Q}^{\text{open}}(\mathbf{t}) = (Q_1^{\text{open}}(t), Q_2^{\text{open}}(t), \ldots, Q_n^{\text{open}}(t))$. Let $L(\mathbf{Q}^{\text{conf}}, \mathbf{Q}^{\text{open}})$ be quadratic Lyapunov function of confidential and open queue backlogs defined as:

$$L(\mathbf{Q}^{\text{conf}}(\mathbf{t}), \mathbf{Q}^{\text{open}}(\mathbf{t})) = \frac{1}{2} \sum_i \left[(Q_i^{\text{conf}}(t))^2 + (Q_i^{\text{open}}(t))^2 \right]. \tag{3.41}$$

Also consider the one-step expected Lyapunov drift, $\Delta(t)$ for the Lyapunov function (6.22) as:

$$\begin{aligned} \Delta(t) = \mathbb{E}\big[& L(\mathbf{Q}^{\text{conf}}(\mathbf{k+1}), \mathbf{Q}^{\text{open}}(\mathbf{k+1})) \\ & - L(\mathbf{Q}^{\text{conf}}(\mathbf{t}), \mathbf{Q}^{\text{open}}(\mathbf{t})) \bigm| \mathbf{Q}^{\text{conf}}(\mathbf{t}), \mathbf{Q}^{\text{open}}(\mathbf{t}) \big]. \end{aligned} \tag{3.42}$$

The following lemma provides an upper bound on $\Delta(t)$.

Lemma 4.

$$\begin{aligned} \Delta(t) \leq B - & \sum_i \mathbb{E}\left[Q_i^{conf}(t)(R_i^p(t) - A_i^{conf}(t)) \bigm| Q_i^{conf}(t) \right] \\ & - \sum_i \mathbb{E}\left[Q_i^{open}(t)(R_i^{open}(t) - A_i^{open}(t)) \bigm| Q_i^{open}(t) \right], \end{aligned} \tag{3.43}$$

where $B > 0$ is a constant.

Proof. ince the maximum transmission power is finite, in any interference-limited system transmission rates are bounded. Let $R_i^{p,max}$ and $R_i^{o,max}$ be the maximum confidential and open rates for user i, which depends on the channel states. Also assume that the arrival rates are bounded, i.e., $A_i^{p,max}$ and $A_i^{o,max}$ be the maximum number of confidential and open bits that may arrive in a block for each user. Hence, the following inequalities can be obtained for each confidential queue:

$$\begin{aligned}
&(Q_i^{\text{conf}}(k+1))^2 - (Q_i^{\text{conf}}(t))^2 \\
&\quad = \left(\left[Q_i^{\text{conf}}(t) - R_i^p(t)\right]^+ + A_i^{\text{conf}}(t)\right)^2 - (Q_i^{\text{conf}}(t))^2 \\
&\quad \le (Q_i^{\text{conf}}(t))^2 + (A_i^{\text{conf}}(t))^2 + (R_i^p(t))^2 \\
&\quad\quad - 2Q_i^{\text{conf}}(t)\left[R_i^p(t) - A_i^{\text{conf}}(t)\right] - (Q_i^{\text{conf}}(t))^2 \\
&\quad \le (R_i^p(t))^2 + (A_i^{\text{conf}}(t))^2 - 2Q_i^{\text{conf}}(t)[R_i^p(t) - A_i^{\text{conf}}(t)] \\
&\quad \le B_1 - 2Q_i^{\text{conf}}(t)[R_i^p(t) - A_i^{\text{conf}}(t)] \qquad (3.44)
\end{aligned}$$

where $B_1 = (R_i^{p,max})^2 + (A_i^{p,max})^2$. The same line of derivation can be performed for open queues to obtain:

$$\begin{aligned}
&(Q_i^{\text{open}}(k+1))^2 - (Q_i^{\text{open}}(t))^2 \\
&\quad = \left([Q_i^{\text{open}}(t) - R_i^o(t)]^+ + A_i^{\text{open}}(t)\right)^2 - (Q_i^{\text{open}}(t))^2 \\
&\quad \le B_2 - 2Q_i^{\text{open}}(t)[R_i^o(t) - A_i^{\text{open}}(t)] \qquad (3.45)
\end{aligned}$$

where $B_2 = (R_i^{o,max})^2 + (A_i^{o,max})^2$.

Hence, by taking expectation, multiplying by $\frac{1}{2}$, and summing (3.44)-(3.45) over all $j = 1, \ldots, n$, we obtain the upper bound on $\Delta(t)$ as given in the Lemma, where $B = n(B_1 + B_2)/2$. □

Now, we present our main result showing that our proposed dynamic control algorithm can achieve a performance arbitrarily close to the optimal solution while keeping the queue backlogs bounded.

Theorem 6. *If $R_i(t) < \infty$ for all j, k, then dynamic control algorithm satisfies:*

$$\liminf_{N_2 \to \infty} \frac{1}{N_2} \sum_{k=0}^{N_2-1} \sum_{j=1}^{n} \mathbb{E}\left[g_i^{conf}(t) + g_i^{open}(t)\right] \geqslant g^* - \frac{B}{V}$$

$$\limsup_{N_2 \to \infty} \frac{1}{N_2} \sum_{k=0}^{N_2-1} \sum_{j=1}^{n} \mathbb{E}\left[Q_i^{conf}(t)\right] \leqslant \frac{B + V(\bar{g} - g^*)}{\epsilon_1}$$

$$\limsup_{N_2 \to \infty} \frac{1}{N_2} \sum_{k=0}^{N_2-1} \sum_{j=1}^{n} \mathbb{E}\left[Q_i^{open}(t)\right] \leqslant \frac{B + V(\bar{g} - g^*)}{\epsilon_2},$$

where $B, \epsilon_1, \epsilon_2 > 0$ are constants, g^* is the optimal solution of (3.37)-(3.38) *and $\bar{g}$ is the maximum possible aggregate utility.*

Proof. Lyapunov Optimization Theorem [6] suggests that a good control strategy is the one that minimizes the following:

$$\Delta^U(t) = \Delta(t) - V\mathbb{E}\left[\sum_i \left(g_i^{\text{conf}}(t) + g_i^{\text{open}}(t)\right) \,\middle|\, \mathbf{Q}^{\text{conf}}(\mathbf{t}), \mathbf{Q}^{\text{open}}(\mathbf{t})\right] \tag{3.46}$$

By using (6.24), we may obtain an upper bound for (6.25), as follows:

$$\begin{aligned}\Delta^U(t) < B &- \sum_i \mathbb{E}\left[Q_i^{\text{conf}}(t)[R_i^p(t) - A_i^{\text{conf}}(t)] \,\middle|\, Q_i^{\text{conf}}(t)\right] \\ &- \sum_i \mathbb{E}\left[Q_i^{\text{open}}(t)[R_i^o(t) - A_i^{\text{open}}(t)] \,\middle|\, Q_i^{\text{open}}(t)\right] \\ &- V\mathbb{E}\left[\sum_i U_i^{\text{conf}}(A_i^{\text{conf}}(t)) + \sum_i U_i^{\text{open}}(A_i^{\text{open}}(t))\right]\end{aligned} \tag{3.47}$$

By rearranging the terms in (6.26) it is easy to observe that our proposed dynamic network control algorithm minimizes the right hand side of (6.26).

If the confidential and open arrival rates are in the feasible region, it has been shown in [98] that there must exist a stationary scheduling and rate control policy that chooses the users and their transmission rates independent of queue backlogs and only with respect to the channel statistics. In particular, the optimal stationary policy can be found as the solution of a deterministic policy if a priori channel statistics are known.

Let U^* be the optimal value of the objective function of the problem (3.37)-(3.38) obtained by the aforementioned stationary policy. Also let $\lambda_i^{\text{conf}*}$ and $\lambda_i^{\text{open}*}$ be optimal confidential and open traffic arrival rates found as the solution of the same problem. In particular, the optimal input rates $\lambda_i^{\text{conf}*}$ and $\lambda_i^{\text{open}*}$ could in principle be achieved by the simple backlog-independent admission control algorithm of including all new arrivals $(A_i^{\text{conf}}(t), A_i^{\text{open}}(t))$ for a given node i in slot t independently with probability $(\zeta_i^{\text{conf}}, \zeta_i^{\text{open}}) = (\lambda_i^{\text{conf}*}/\lambda_i^{\text{conf}}, \lambda_i^{\text{open}*}/\lambda_i^{\text{open}})$. Then, the right hand side (RHS) of (6.26) can be rewritten as

$$\begin{aligned} B - \sum_i \mathbb{E}\left[Q_i^{\text{conf}}(t)\right] \mathbb{E}\left[R_i^p(t) - A_i^{\text{conf}}(t)\right] \\ - \sum_i \mathbb{E}\left[Q_i^{\text{open}}(t)\right] \mathbb{E}\left[R_i^o(t) - A_i^{\text{open}}(t)\right] - VU^*. \end{aligned} \tag{3.48}$$

Also, since $(\lambda_i^{\text{conf}*}, \lambda_i^{\text{open}*}) \in \Lambda$, i.e., arrival rates are strictly interior of the rate region, there must exist a stationary scheduling and rate allocation policy that is independent of queue backlogs and satisfies the following:

$$\mathbb{E}\left[R_i^{\text{conf}} \mid \mathbf{Q}^{\text{conf}}\right] \geq \lambda_i^{\text{conf}*} + \epsilon_1 \tag{3.49}$$

$$\mathbb{E}\left[R_i^{\text{open}} \mid \mathbf{Q}^{\text{open}}\right] \geq \lambda_i^{\text{open}*} + \epsilon_2 \tag{3.50}$$

Clearly, any stationary policy should satisfy (6.26). Recall that our proposed policy minimizes RHS of (6.26), and hence, any other stationary policy (including the optimal policy) has a higher RHS value than the one attained by our policy. In particular, the stationary policy that satisfies (6.27)-(6.28), and implements aforementioned probabilistic admission control can be used to obtain an upper bound for the RHS of our proposed policy. Inserting (6.27)-(6.28) into (3.48), we obtain the following upper bound for our policy:

$$RHS < B - \sum_i \epsilon_1 \mathbb{E}[Q_i^{\text{conf}}(t)] - \sum_i \epsilon_2 \mathbb{E}[Q_i^{\text{open}}(t)] - VU^*. \tag{3.51}$$

This is exactly in the form of Lyapunov Optimization Theorem given in Theorem 1, and hence, we can obtain bounds on the performance of the proposed policy and the sizes of queue backlogs as given in Theorem 1.

□

3.4.2 Imperfect Knowledge of Instantaneous CSI

In the previous section, we performed our analysis assuming that at every block *exact* instantaneous cross-channel rates are available. However, unlike the uplink direct channel rate which can be determined by the base station prior to the data transmission (e.g., via pilot signal transmission), cross-channel rates are harder to be estimated. Indeed, in a non-cooperative network in which nodes do not exchange their CSI, the cross-channel rates $\{R_{ij}, j \neq i\}$ can only be inferred by node i from the received signals over the reverse channel as nodes $j \neq i$ are transmitting to the base station. Hence, at a given block, nodes only have *a posteriori* channel distribution. Based on this *a posteriori* channel distribution, nodes may estimate CSI of their cross-channels.

Let us denote the *estimated* rate of the cross-channel (j, i) with $\hat{R}_{ij}(t)$. We also define *cross-channel rate margin* $R_i^{\mathrm{rand}}(t)$ as the cross-channel rate a node uses when it encodes confidential information. More specifically, node i encodes its confidential information at rate:

$$R_i^p(t) = R_i(t) - R_i^{\mathrm{rand}}(t), \tag{3.52}$$

i.e., $R_i^{\mathrm{rand}}(t)$ is the rate of the randomization message node i uses in the random binning scheme for confidentiality. Note that, if $R_i^{\mathrm{rand}}(t) < \max_{i \neq j} R_{ij}(t)$, then node i will not meet the perfect secrecy constraint at slot t, leading to a *secrecy outage*. In the event of a secrecy outage, the confidentially encoded message is considered as an *open* message. The probability of secrecy outage over slot t for the scheduled node i, given the estimates of the cross channel rates is:

$$\rho_i^{\mathrm{secr}}(R_i^{\mathrm{rand}}(t)) = \mathbb{P}\left(\max_{i \neq j} R_{ij}(t) > R_i^{\mathrm{rand}}(t) \;\middle|\; \{\hat{R}_{ij}(t), i \neq j\} \right). \tag{3.53}$$

Compare the aforementioned definition of *secrecy outage* with the *channel outage* [99] experienced in fast varying wireless channels. In time-varying wireless channels, channel outage occurs when received signal and interference/noise ratio drops below a threshold necessary for correct decoding of the transmitted signal. Hence, the largest rate of reliable communications at a given outage probability is an important measure of channel quality. In the following, we aim to determine utility maximizing achievable confidential and open transmission rates for given *secrecy outage* probabilities. In particular, we consider the solution of the following optimization problem:

$$\max \sum_{j=1}^{n} \left(\mathbb{E}\left[g_i^{\text{conf}}(t) \right] + \mathbb{E}\left[g_i^{\text{open}}(t) \right] \right) \tag{3.54}$$

$$\text{subject to } (\lambda_i^{\text{open}}, \lambda_i^{\text{conf}}) \in \Lambda, \tag{3.55}$$

$$\text{and } \rho_i^{\text{secr}}(R_i^{\text{rand}}(t)) = \gamma_i, \tag{3.56}$$

where γ_i is the tolerable secrecy outage probability. Aforementioned optimization problem is the same as the one given for perfect CSI except for the last constraint. The additional constraint (3.56) requires that only a certain prescribed proportion of confidential transmissions are allowed to violate the perfect secrecy constraint. Due to secrecy outages we define *confidential goodput* of user i as $\mathbb{E}\left[R_i^p(t) \left(1 - \rho_i^{\text{secr}}(R_i^{\text{rand}}(t)) \right) \right]$. Note that confidential goodput only includes confidential messages for which perfect secrecy constraint is satisfied. All confidential messages for which (5.2) is violated are counted as successful open transmissions.

Similar to the perfect CSI case, we argue that a dynamic policy can be used to achieve asymptotically optimal solution. Unlike the algorithm given in the perfect CSI case, the algorithm for imperfect CSI first determines the confidential data encoding rate so that the secrecy outage constraint (3.56) is satisfied in current block. Hence, the confidential encoding rate at a particular block is determined by the estimated channel rates and the secrecy outage constraint.

Control Algorithm: Similar to the perfect CSI case, our algorithm involves two steps in each slot t:

(1) Flow Control: For some $V > 0$, each node injects $A_i^{\text{conf}}(t)$ confidential and

$A_i^{\text{open}}(t)$ open bits, where

$$\begin{aligned}\left(A_i^{\text{conf}}(t), A_i^{\text{open}}(t)\right) = \underset{A_i^{\text{conf}}, A_i^{\text{open}}}{\operatorname{argmax}} \ & V\left[U_i^{\text{conf}}(A_i^{\text{conf}})(1-\gamma_i)\right.\\ & \left.+U_i^{\text{open}}(A_i^{\text{open}})(1-\gamma_i) + U_i^{\text{open}}(A_i^{\text{open}} + A_i^{\text{conf}})\gamma_i\right]\\ & - Q_i^{\text{conf}}(t)A_i^{\text{conf}} - Q_i^{\text{open}}(t)A_i^{\text{open}}. \qquad (3.57)\end{aligned}$$

(2) Scheduling: Schedule node i and transmit jointly encoded *confidential and open* traffic ($\mathcal{I}_i^{\text{conf}} = 1$) or *only* open ($\mathcal{I}_i^{\text{open}} = 1$) traffic, where

$$\left(\mathcal{I}_i^{\text{conf}}(t), \mathcal{I}_i^{\text{open}}(t)\right) = \underset{\mathcal{I}^{\text{conf}}, \mathcal{I}^{\text{open}}}{\operatorname{argmax}} \left\{Q_i^{\text{conf}}(t)R_i^{\text{conf}}(t) + Q_i^{\text{open}}(t)R_i^{o}(t)\right\}.$$

For each node i, encode confidential data over each slot t at rate

$$\begin{aligned}R_i^p(t) &= \mathcal{I}_i^{\text{conf}}(t)\left[R_i(t) - R_i^{\text{rand}}(t)\right],\\ R_i^{\text{rand}}(t) &= p_i^{\text{out}^{-1}}(\gamma_i),\end{aligned}$$

and transmit open data at rate

$$R_i^o(t) = \mathcal{I}_i^{\text{open}}(t)R_i(t) + \mathcal{I}_i^{\text{conf}}(t)(R_i(t) - R_i^p(t)).$$

Optimality of Control Algorithm

The optimality of the control algorithm with imperfect CSI can be shown in a similar fashion as for the control algorithm with perfect CSI. We use the same Lyapunov function defined in (6.22) which results in the same one-step Lyapunov drift function (6.23). Hence, Lemma 9 also holds for the case of imperfect CSI, but with a different constant B' due to the fact that higher maximum confidential information rates can be achieved by allowing secrecy outages.

Lyapunov Optimization Theorem suggests that a good control strategy is the one that minimizes the following:

$$\Delta^U(t) = \Delta(t) - V\mathbb{E}\left[\sum_i (g_i^{\text{conf}}(t) + g_i^{\text{open}}(t)) \;\middle|\; \mathbf{Q}^{\text{conf}}(t), \mathbf{Q}^{\text{open}}(t)\right] \tag{3.58}$$

In (3.58), expectation is over all possible channel states. The expected utility for confidential and open transmissions are respectively given as:

$$\begin{aligned}
\mathbb{E}\left[g_i^{\text{conf}}(t)\right] &= \mathbb{E}\left[g_i^{\text{conf}}(t)|\mathcal{I}_i^{\text{conf}}(t), R_i^{\text{rand}}(t)\right] \\
&= (1-\gamma_i)\mathbb{E}\left[U_i^{\text{conf}}\left(A_i^{\text{conf}}(t)\right)\right], \qquad (3.59) \\
\mathbb{E}\left[g_i^{\text{open}}(t)\right] &= \mathbb{E}\left[g_i^{\text{open}}(t)|\mathcal{I}_i^{\text{conf}}(t), \mathcal{I}_i^{\text{open}}(t), R_i^{\text{rand}}(t)\right] \\
&= \gamma_i\mathbb{E}\left[U_i^{\text{open}}(A_i^{\text{conf}}(t) + A_i^{\text{open}}(t))\right] \\
&\qquad + (1-\gamma_i)\mathbb{E}\left[U_i^{\text{open}}(A_i^{\text{open}}(t))\right]. \qquad (3.60)
\end{aligned}$$

Note that (3.59)-(3.60) are obtained due to Constraint (3.56). By combining Lemma 9 with (3.59)-(3.60) we may obtain an upper bound for (3.58), as follows:

$$\begin{aligned}
\Delta^U(t) <& B' - \sum_i \mathbb{E}\left[Q_i^{\text{conf}}(t)[R_i^p(t) - A_i^{\text{conf}}(t)]\right] \\
&- \sum_i \mathbb{E}\left[Q_i^{\text{open}}(t)[R_i^o(t) - A_i^{\text{open}}(t)]\right] - V\mathbb{E}\left[\sum_i (1-\gamma_i)U_i^{\text{conf}}\left(A_i^{\text{conf}}(t)\right)\right. \\
&\left. + \sum_i \gamma_i U_i^{\text{open}}(A_i^{\text{conf}}(t) + A_i^{\text{open}}(t)) + (1-\gamma_i)U_i^{\text{open}}(A_i^{\text{open}}(t))\right]. \qquad (3.61)
\end{aligned}$$

Now, it is clear that the proposed dynamic control algorithm minimizes the right hand side of (3.61). The steps of proving the optimality of the dynamic control algorithm are exactly the same as those given in Theorem 10, and hence, we skip the details.

Theorem 7. *If $R_i(t) < \infty$, for all j, k then dynamic control algorithm satisfies:*

$$\liminf_{N_2\to\infty} \frac{1}{N_2} \sum_{k=0}^{N_2-1} \sum_{j=1}^{n} \mathbb{E}[g_i^{conf}(t) + g_i^{open}(t)] \geq g'^{*} - \frac{B'}{V} \tag{3.62}$$

$$\limsup_{N_2\to\infty} \frac{1}{N_2} \sum_{k=0}^{N_2-1} \sum_{j=1}^{n} \mathbb{E}[Q_i^{conf}(t)] \leq \frac{B' + V(\bar{g}' - g'^{*})}{\epsilon_2'}$$

$$\limsup_{N_2\to\infty} \frac{1}{N_2} \sum_{k=0}^{N_2-1} \sum_{j=1}^{n} \mathbb{E}[Q_i^{open}(t)] \leq \frac{B' + V(\bar{g}' - g'^{*})}{\epsilon_1'},$$

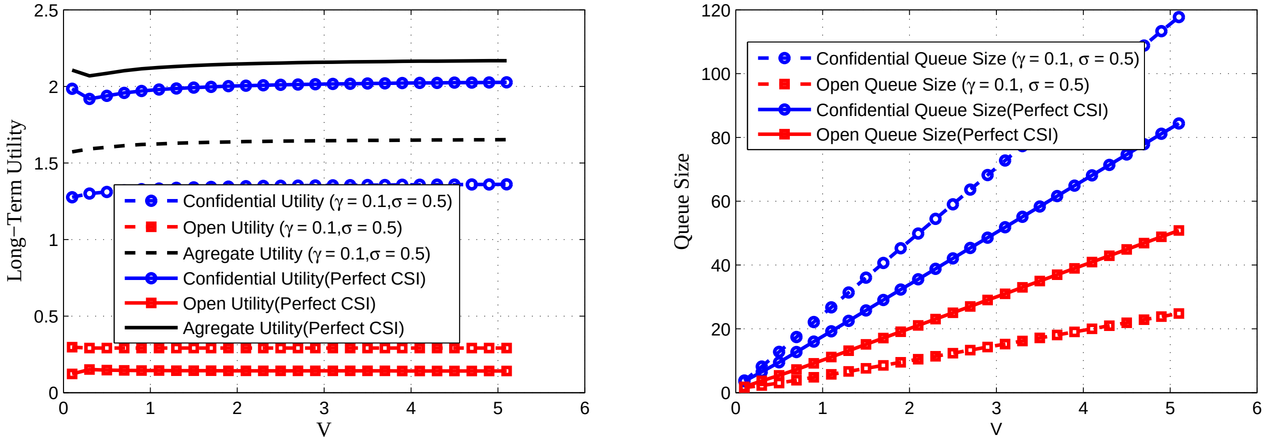
where $B', \epsilon_1', \epsilon_2' > 0$ are constants, g'^{*} is the optimal solution of (3.54)-(3.56) *and $\bar{g}'$ is the maximum possible aggregate utility.*

3.5 Numerical Results

In our numerical experiments, we considered a network consisting of ten nodes and a single base station. The direct channel between a node and the base station, and the cross-channels between pairs of nodes are modeled as iid Rayleigh fading Gaussian channels. Thus, direct-channel and cross-channel power gains are exponentially distributed with means chosen uniformly randomly in the intervals $[2, 8]$, and $[0, 1]$, respectively. The noise normalized power is $P = 1$. In our simulations, we consider both of the cases when perfect instantaneous CSI is available, and when instantaneous CSI can only be estimated with some error. Unless otherwise indicated, in the case of imperfect CSI, we take the tolerable secrecy outage probability as 0.1. We assumed the use of an unbiased estimator for the cross-channel power gains and modeled the associated estimation error with a Gaussian random variable:

$$\hat{h}_{ij}(t) = h_{ij}(t) + e_{ij}(t),$$

where $e_{ij}(t) \sim \mathcal{N}(0, \sigma^2)$ for all t. Gaussian estimation error can be justified as discussed in [100] or by the use of a recursive ML estimator as in [101]. Unless otherwise stated, we take $\sigma = 0.5$, i.e., the estimation error is rather significant relative to the mean



(a) Long-term Utility

(b) Average queue length

Figure 3.8: Numerical results with respect to optimization parameter V.

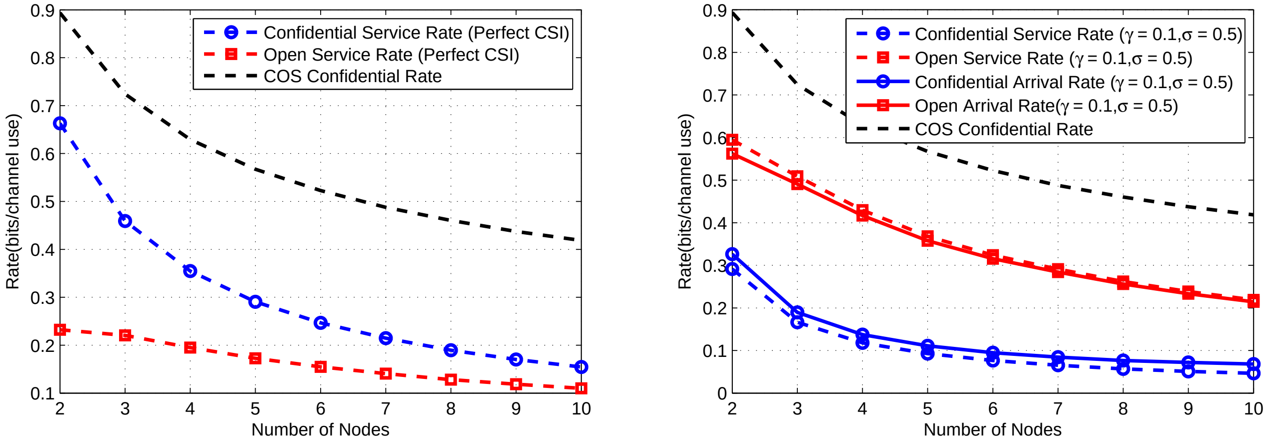
cross-channel gain. Note that, in this section, we choose the margin $R_i^{\text{rand}}(t)$ such that

$$\mathbb{P}\left(R_i^{\text{rand}}(t) < \max_{i \neq j} \left[\log(1 + P h_{ij}) \right] \middle| \{\hat{h}_{ij}, i \neq j\} \right) \leq \gamma_i.$$

We consider logarithmic confidential and open utility functions where the confidential utility is κ times more than open utility at the same rate. More specifically, we take for a scheduled node i, $U_i^{\text{conf}}(t) = \kappa \cdot \log(1 + R_i^p(t))$, and $U_i^{\text{open}}(t) = \log(1 + R_i^o(t))$. We take $\kappa = 5$ in all the experiments except for the one inspecting the effect of κ. The rates depicted in the graphs are per node arrival or service rates calculated as the total arrival or service rates achieved by the network divided by the number of nodes, i.e., the unit of the plotted rates is bits/channel use/node. Finally, for perfect CSI, we only plot the service rates since arrival and service rates are identical.

In Fig. 6.4a-3.8b, we investigate the effect of system parameter V in our dynamic control algorithm. Fig. 6.4a shows that for $V > 4$, long-term utilities converge to their optimal values fairly closely. It is also observed that CSI estimation error results in a reduction of approximately 25% in aggregate utility. Fig. 3.8b depicts the well-known relationship between V and queue backlogs, where queue backlogs increase when V is increased.

In Fig. 3.9a-3.9b, the effect of increasing number of nodes on the achievable confi-



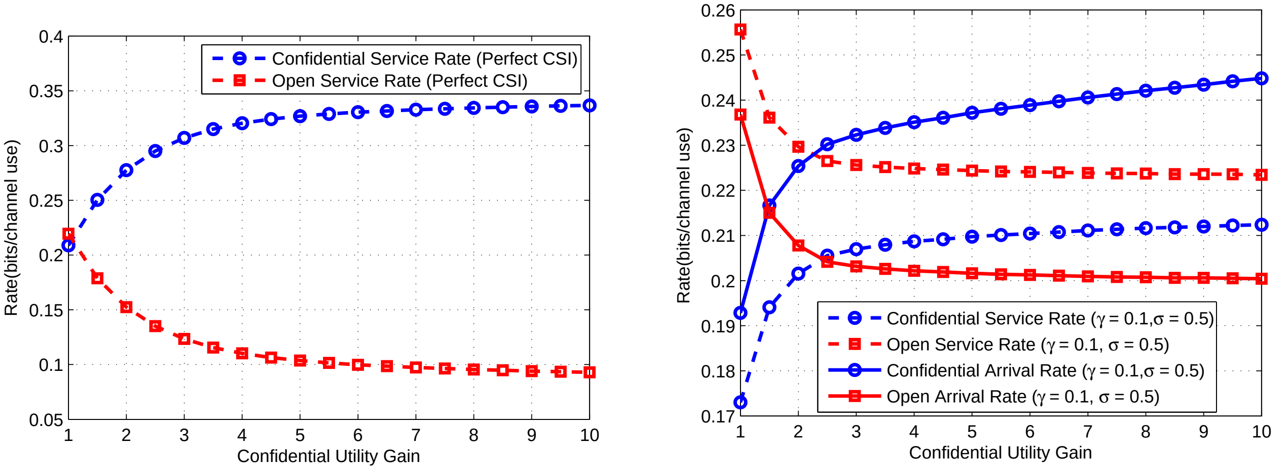
(a) Perfect CSI

(b) Imperfect CSI

Figure 3.9: Confidential and open rates with respect to number of nodes

dential and open rates obtained with the proposed dynamic control algorithm is shown. In both figures, the confidential information rate achieved by COS algorithm given in Section 3.3 is also depicted. From Fig. 3.9a, we first notice that by using the dynamic control algorithm which is based only on the instantaneous CSI, the confidential service rate is reduced by more than 25% as compared to the maximum confidential information rate achieved by COS which uses a priori CSI to encode over many slots. This difference increases with increasing number of nodes. However, for both COS and dynamic control algorithms, the achievable rates decrease with increasing number of nodes since more nodes overhear ongoing transmissions. Meanwhile, open service rate also decreases due to the fact that there is a smaller number of transmission opportunities per node with increasing number of nodes. Fig. 3.9b depicts that confidential service rate has decreased by approximately 50% due to CSI estimation errors. It is also interesting to note that confidential arrival rate is higher than the confidential service rate, since all confidential messages for which perfect secrecy constraint cannot be satisfied are considered as successful open messages. Hence, open service rate is observed to be higher than the open arrival rate.

We next analyze the effect of κ, which can also be interpreted as the ratio of utility of confidential and open transmissions taking place at the same rate. We call this ratio *confidential utility gain*. Fig. 3.10a shows that when confidential utility gain is greater



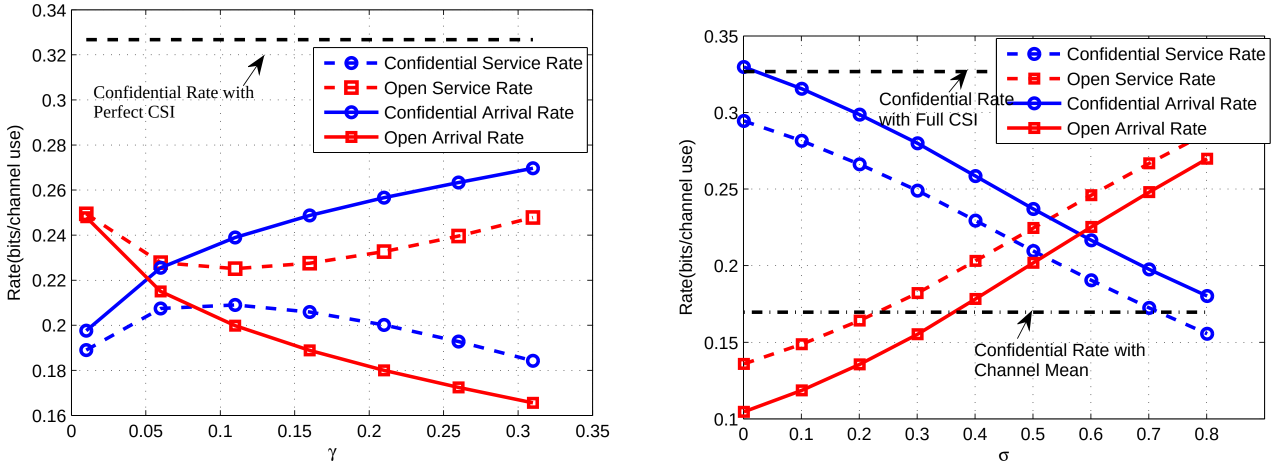
(a) Perfect CSI

(b) Imperfect CSI

Figure 3.10: Confidential and open rates with respect to increasing amount of confidential utility gain.

than 5, then the confidential and open service rates converge to their respective limits. These limits depend on the channel characteristics, and their sum is approximately equal to the maximum achievable rate of the channel. However, when there is CSI estimation error, Fig. 3.10b shows that although an identical qualitative relationship between arrival rates and confidential utility gain is still observed, confidential service rate is lower than the confidential arrival rate by a fraction of γ almost uniformly in the range of κ.

In Fig. 3.11a, we investigate the effect of the tolerable secrecy outage probability. It is interesting to note that confidential service rate increases initially with increasing tolerable outage probability. This is because for low γ values, in order to satisfy the tight secrecy outage constraint, a low instantaneous confidential information rate is chosen. However, when γ is high more secrecy outages are experienced at the expense of higher instantaneous confidential information rates. This is also the reason why we observe that the difference between the confidential service and arrival rates is increasing. We note that when CSI estimation error is present, the highest confidential service rate is obtained when γ is approximately equal to 0.1. The highest confidential service rate with CSI estimation error is approximately 30% lower than the confidential service rate with the perfect CSI.



(a) Effect of γ.

(b) Effect of σ.

Figure 3.11: Confidential and open rates with respect to tolerable secrecy outage probability.

We finally investigate the effect of the quality of CSI estimator in Fig. 3.11b. For this purpose, we vary the standard deviation of the Gaussian random variable modeling the estimation error. As expected the highest confidential service rate is obtained when $\sigma = 0$. However, it is important to note that this value is still lower than the confidential service rate with perfect CSI, since secrecy outages are still permitted in 10% of confidential transmissions. We have also investigated the performance of the dynamic control algorithm when a posteriori CSI distribution is not available. In this case, scheduling and flow control decisions are based only on the mean cross channel gains. When only mean cross channel gains are available, the achieved confidential service rate per node is approximately equal to 0.16 bits per channel use, which is significantly lower than the confidential service rate with perfect CSI. In particular, it is only when the standard deviation of the estimation error is 0.7 that the confidential service rate with noisy channel estimator has the same confidential service rate achievable utilizing only mean channel gains.

3.6 Chapter Summary

In this paper, we studied the achievable confidential and open information rate regions of single- and multi-user wireless networks with node scheduling. We introduce confidential opportunistic scheduling along with a confidential encoding strategy, and show that it maximizes the sum confidential information rate for both multiuser uplink communication when perfect CSI is available for only the main uplink channels. Then, we described a cross-layer dynamic algorithm that works without prior distribution of channel states. We prove that our algorithm, which is based on simple index policies, achieves utility arbitrarily close to achievable optimal utility. The simulation results also verify the efficacy of the algorithm.

Chapter 4

Confidentiality-Preserving Control of Uplink Cellular Wireless Networks Using Hybrid ARQ

In the previous chapter, we investigated the cross-layer resource allocation problem with confidentiality in a cellular wireless network, where users transmit information to the base station, secretly from the other users. One of the main drawbacks of the cross-layer resource allocation algorithms such as the one proposed in chapter 3 is that, instantaneous channel states between users and/or the base station are assumed to be available or they can be estimated fairly accurately. However, in general, neither the base station nor any other legitimate node in the network is aware of CSI of other nodes. CSI must be acquired (e.g., via pilot signal transmission) by consuming part of resources, which is otherwise used for data transmission. The overhead due to acquiring CSI increases with increasing number of users in the network. To that end, in this chapter, we investigate the cross-layer resource allocation problem with confidentiality under a more realistic and practical network model, where both the users and the base station are oblivious to the instantaneous channel state information, and we obtain an optimal dynamic control algorithm.

4.1 Introduction

As in chapter 3, we consider an uplink cellular wireless network in which each node generates both open and confidential information to be transmitted to the base station. When a node is transmitting a confidential packet, other legitimate nodes are considered as “internal eavesdroppers.” In this setting, we assume that each node has the knowledge of merely the distribution of its associated uplink channel state as well as the cross channels between itself and every other node. Also a node does not receive any CSI from the base station apart from the 1-bit ACK/NAK signal indicating whether the transmission of the node is successful or not. We pose the problem as that of a network utility maximization in which information theoretic secrecy, *measured by equivocation*, is incorporated as a Quality of Service constraint. We develop a joint flow control and scheduling scheme, which is based on index policies, requiring very simple optimization problems to be solved in each slot. To accomplish reliability, we utilize an incremental redundancy HARQ scheme based on code puncturing. Our scheme relies on mutual information accumulation at each re-transmission. For confidential transmissions, we employ secure incremental redundancy HARQ developed in [42], which considers a block fading wire-tap channel with a single source-destination pair, and a single (external) eavesdropper. We engineer our scheme carefully to utilize resources efficiently and avoid secrecy outages to meet the secrecy outage constraint. Ultimately, we prove that our dynamic control scheme is optimal, i.e., it achieves the maximum utility, achievable by any flow control and scheduling scheme.

There are a few works regarding to optimization of the network without knowing channel state information. The issue here is that since the channel states are not available at the transmitter, it should use retransmission to provide reliability. However, this leads to correlation among consecutive transmissions of the message, and to the need of using complex algorithm to obtain optimal solution. For example, [102] develops a cross-layer solution for downlink cellular systems with imperfect CSI at the transmitter by employing rateless codes. The problem in [102] is a constrained partial observed Markov decision problem (CPOMDP), which is known to be hard to solve.

The same hard problems are also encountered in [103] and [104]. However, in Chapter 4, we obtain the optimal solution with a simplex method by using Lyapunov optimization theory described in the previous section. Without confidential information, there has been a number of studies that develop cross-layer resource allocation solutions on HARQ-based transmissions. In [7] and [8], wireless routing with mutual information accumulation based coding is investigated with the aim of energy minimization. They conclude that obtaining optimal solution requires complex and combinatorial networking decisions concerning which nodes participate in transmission, and which decode ordering to use. Thus, they propose greedy and heuristic algorithms resulting in suboptimal solutions. In [105], wireless scheduling with HARQ was investigated with the aim of minimizing the average of a cost function which was defined as an increasing function of the queue lengths. The solution to this problem was obtained for only specific types of cost functions by applying dynamic programming techniques. In [9] transmit power and modulation order adaptation strategies, based on semi-Markov decision process are investigated for the HARQ schemes over correlated Rayleigh fading channels. Here, the authors do not consider multi-user setting and their goal is to minimize transmission power, buffer delay and packet overflow. [103] aims to optimize the mapping between signal-to-interference-and-noise ratio (SINR) and modulation and coding scheme (MCS) to maximize the throughput by taking into account the type of HARQ scheme employed. [104] analyzes the interaction between TCP, Hybrid Automatic Repeat Request (HARQ) and scheduling techniques. [102] develops a cross-layer solution for downlink cellular systems with imperfect CSI at the transmitter by employing rateless codes. The problem in [102] is a constrained partial observed Markov decision problem (CPOMDP), which is known to be hard to solve. However, by using a modified Lyapunov drift method, they develop a dynamic network control scheme. The focus in all these works has solely been on the transmission of open messages and confidentiality of messages has not been a constraint.

Clearly, without exact instantaneous uplink CSI at the transmitter side, the wireless transmissions are prone to decoding errors, i.e., channel outages. Traditionally, reliability is accomplished via a standard automatic-repeat-request (ARQ) protocol, where, if a packet cannot be decoded, it is discarded and retransmitted again. However, hybrid ARQ (HARQ) schemes make use of forward error correction (FEC) coding so that the information collected from previous failed transmissions are combined to improve the likelihood of decoding success [106]. The main challenge involved in generalizing the network control with hybrid ARQ is encoding confidential and/or open messages over several blocks. This implies that the time-scales involved in the physical layer and the network layer cannot be decoupled, *eliminating the time-scale separation assumption*.

In recent studies, this challenge is overcome by introducing virtual queues for the messages, which are partially decoded or by giving scheduling decisions over many slots, i.e., T-slot scheduling [107]. However, this approach requires a feedback on instantaneous CSI from the receiver, informing the transmitting node about the accumulated information. The problem of dynamic network control without CSI is notoriously difficult even with only open packet arrivals. In order to design a cross-layer dynamic control algorithm for confidential communications, the rate of information leakage to other nodes in the network is required to be quantified over each slot independently. This leads to some unique technical issues that were not addressed in the existing studies on dynamic network resource allocation. To our best knowledge, our scheme is the first provably-optimal scheme that handles a hybrid traffic involving both open and confidential packets, without an instantaneous CSI. To achieve this, our approach overcomes a number of technical challenges. In particular:

(a) Re-transmissions of the same confidential or open message are correlated with each other. We develop a novel queue model that eliminates the correlation between subsequent re-tranmissions of the same message.

(b) The objective function of the associated NUM problem is coupled among the nodes in the network. In order to decompose the problem into that of a centralized scheduling sub-problem and independent flow control sub-problems solved by each node, we transformed our optimization formulation by introducing a new auxiliary variable and a corresponding constraint.

The rest of the chapter is organized as follows. Section 5.2 describes the system model, where we give the channel model and a brief summary of incremental redundancy based HARQ for both confidential and open messages. In Section 4.2.3, we characterize the achievable rate region and formulate the problem. In Section 4.3, we formulate the problem as a network utility maximization (NUM) problem, and give solution by using dual decomposition. Section 4.4 gives our novel queue model and our joint flow and scheduling algorithm. In Section 4.5, we investigate the effects of the system parameters on the performance of the algorithm via numerical experiments. Section 4.6 concludes this work by summarizing our contributions.

4.2 System Model and Preliminaries

4.2.1 System Model

We consider a the same network model presented in chapter 3 as illustrated in Fig. 3.1. More preciously, the system consists of n nodes and a base station. The traffic injected by each of these nodes consists of both open and confidential packets. These packets are to be transmitted to the base station via an *unreliable* uplink channel. When a node is transmitting, every other node overhears the transmission over the associated cross channels. Hence, nodes treat each other as "internal eavesdroppers" when transmitting confidential information.

Time is slotted, and each slot has a length of N channel uses (physical layer symbols), where N is sufficiently large to allow for invoking random coding arguments. Both the main and the cross channels experience independent identically distributed (iid) block fading, in which the channel gain is constant over a slot and it is varying independently from slot to slot. Let $h_i(t)$ and $h_{ij}(t)$ be *instantaneous* complex channel gains of the uplink channel of node i and the cross channel between node i and node j in slot t, respectively. Let $\mathbf{z}_i(t)$ denote block of transmitted complex symbols of user i in slot t. Then, the corresponding blocks of received symbols at the base station $\mathbf{y}_i(t)$, and node j in slot t $\mathbf{y}_{ij}(t)$, are respectively defined as:

$$\mathbf{y}_i(t) = h_i(t)\mathbf{z}_i(t) + \mathbf{u}_i(t), \tag{4.1}$$

$$\mathbf{y}_{ij}(t) = h_{ij}(t)\mathbf{z}_i(t) + \mathbf{u}_{ij}(t), \tag{4.2}$$

where $\mathbf{u}_i(t)$ and $\mathbf{u}_{ij}(t)$ are circularly symmetric complex Gaussian noise sequences of the main and the cross channels, respectively. Even though our results are general for all distributions for the channel gains, in numerical evaluations we assume all channel gains to be *Gaussian* and the transmit power to be constant, identical to P over all slots t. We normalize the power gains such that the (additive Gaussian) noise has unit variance. Then, as $N \to \infty$, $R_i(t)$ and $R_{ij}(t)$ can be obtained as:

$$R_i(t) = \log(1 + P\,|g_i(t)|^2),$$
$$R_{ij}(t) = \log(1 + P\,|g_{ij}(t)|^2)$$

bits/channel use.

Finally, we assume that transmitters do not have the knowledge of the instantaneous values of $h_i(t)$ and $h_{ij}(t)$, but their distributions are available[1].

4.2.2 Transmission Scheme and Secrecy

Due to the lack of the knowledge of the instantaneous values of $g_i(t)$ and $g_{ij}(t)$, to provide reliability and secrecy, we employ HARQ scheme based on mutual information. In this chapter, we adopt the so called *incremental redundancy (INR)* HARQ which achieves high throughput efficiency by adapting its error correcting code redundancy to the varying channel conditions [106], [42][2]. Briefly, in INR HARQ scheme, only a selected number of coded symbols are transmitted at every slot. The selected number of coded symbols form a codeword of a punctured code. If a retransmission is requested,

[1] The distribution of main and cross channel gains can be inferred by node i from the received signals over the reverse channels, exploiting channel reciprocity, when the base station or nodes $j \neq i$ are transmitting.

[2] The dynamic control algorithm proposed in the subsequent sections can be easily modified for other HARQ schemes such as repetition-coding-based HARQ.

additional redundancy symbols are sent under possibly different channel conditions. An analysis of the throughput performance of different HARQ protocols is found in [106].

One should realize that, since instantaneous CSI is not available, one cannot choose the code rates based on a particular fading channel state. Instead, a particular HARQ scheme is chosen and the same code is used for each user at all times. Specifically, each node i has a confidential message $W_i^{\text{conf}} \in \{1, 2, \ldots, 2^{NC_i^{\text{conf}}}\}$ and open message $W_i^{\text{open}} \in \{1, 2, \ldots, 2^{NC_i^{\text{open}}}\}$, where C_i^{conf} and C_i^{open} denote the rates (to remain unchanged at all times) of confidential and open information respectively for node i. Every incoming open or confidential transport layer message into node i, $i = 1, \ldots, n$, is encoded by using a mother code of length MN channel uses. The obtained codeword x_i is divided into M blocks each of length N channel uses and represented as $[x_i^1, x_i^2, \ldots, x_i^M]$. Let first transmission occur at time slot t_1, where node i sends the block x_i^1 under channel gain $g_i(t_1)$, which is then attempted to be decoded by the base station. If it can be decoded, the base station sends back an acknowledgement (ACK); otherwise, a negative acknowledgement (NAK) is sent. Depending on the scheduling policy which decides on the order of transmissions among the nodes in the network, a second transmission opportunity is given to node i at time slot t_2 under a possibly different channel gain realization $g_i(t_2)$. The transmitter sends the block x_i^2, and the base station attempts to decode by combining the previous block x_i^1 with x_i^2. Similarly, at each subsequent retransmission the base station attempts to decode the code by combining all received previous blocks of the same message. The procedure is repeated until the base station successfully decodes the message, the message is dropped by the transmitter, or all blocks of the mother code is transmitted. We assume that the number of blocks, M, is chosen sufficiently large to keep the probability of decoding failure due to exceeding the maximum number of retransmissions approximately identical to zero.

The main difference between the transmission of confidential and open messages with INR HARQ is that for confidential messages the mother code is designed to be a *Wyner code* of length MN [42]. Wyner code is constructed by a random binning strategy, which basically inserts a randomization message to the actual message to increase the level of secrecy [3]. Let $\mathcal{C}\left(\frac{C_i^{\text{code}}}{M}, \frac{C_i^{\text{conf}}}{M}, MN\right)$ be a Wyner code of size $2^{NC_i^{\text{code}}}$ codewords, generated to convey a confidential message set $\mathcal{W}_i^{\text{conf}} = \{1, 2, \ldots, 2^{NC_i^{\text{conf}}}\}$. Thus, every codeword has a length of NC_i^{code} bits to convey NC_i^{conf} bits of confidential information. In the first transmission, the transmitted codeword, x_i^1, form a codeword of a punctured code of length N, $\mathcal{C}(C_i^{\text{code}}, C_i^{\text{conf}}, N)$. Similarly, after rth transmission of the confidential message, the combined codeword set, $[x_i^1, \ldots, x_i^r]$ form a codeword of a punctured Wyner code of length rN, $\mathcal{C}\left(\frac{C_i^{\text{code}}}{r}, \frac{C_i^{\text{conf}}}{r}, rN\right)$.

After each re-transmission, both the base station and internal eavesdroppers accumulate information equal to the instantaneous main and cross channel rates at the slot the re-transmission takes place. For example, let kth transmission of message W_i^{conf} from node i occur at slot t_k. Then, the mutual information gained by the base station during this re-transmission is $R_i(t_k)$. With INR HARQ, the accumulated mutual information at the base station after r re-transmissions is $\sum_{k=1}^{r} R_i(t_k)$. The message is correctly decoded by the base station after r transmissions, if the rate of information accumulation exceeds the code rate, i.e., $\sum_{k=1}^{r} R_i(t_k) > C_i^{\text{code}}$. Let $\rho_{(i,r)}^{\text{conf}}$ denote the probability of decoding failure of confidential message which is transmitted r times, i.e.,

$$\rho_{(i,r)}^{\text{conf}} = \mathbb{P}\left(\sum_{k=1}^{r} R_i(t_k) < C_i^{\text{code}}\right). \tag{4.3}$$

Similarly, the mutual information gained by node $j \neq i$ at the kth transmission of message W_i^{conf} at time t is $R_{ij}(t_k)$, and the total accumulated mutual information at node j after r transmissions is $\sum_{k=1}^{r} R_{ij}(t_k)$. Due to the lack of the knowledge of instantaneous cross channel gains, perfect secrecy cannot be ensured with probability 1 for confidential information. Note that $C_i^{\text{code}} - C_i^{\text{conf}}$ can be interpreted as the rate of the randomization message node i uses in the random binning scheme. A *secrecy outage* takes place after rth transmission of a message, if the total accumulated mutual information at one of the internal eavesdroppers exceeds the rate of the randomization message:

$$\sum_{k=1}^{r} R_{ij}(t_k) > C_i^{\text{code}} - C_i^{\text{conf}},$$

for some $j \neq i$. Let $\rho_{(i,r)}^{\text{secr}}$ denote the probability of secrecy outage of a message that is transmitted r times, i.e.,

$$\rho_{(i,r)}^{\text{secr}} = \mathbb{P}\left(\max_{j \neq i} \left\{ \sum_{k=1}^{r} R_{ij}(t_k) \right\} > C_i^{\text{code}} - C_i^{\text{conf}} \right). \tag{4.4}$$

Note that the secrecy outage probability, $\rho_{(i,r)}^{\text{secr}}$, is an increasing function of the number of transmission attempts, r, since overhearing nodes obtain more information at each retransmission. In our problem, we will require that the probability of secrecy outage of each user i is below a given threshold, $\gamma_i,\ i = 1, \ldots, n$.

For the case of transmission of open messages, the transmitter encodes the information and cyclic redundancy check (CRC) bits by a mother code [106] with a fixed rate C_i^{open}. In each transmission, only the systematic part of the codeword and a selected number of parity bits are transmitted. Decoding is attempted at the receiver side by combining all previously transmitted codes. Let the kth transmission of open message from node i occur at slot t_k^o. If the accumulated information is larger than the fixed rate, $\sum_{k=1}^{r} R_i(t_k^o) > C_i^{\text{open}}$, the decoding of the open message is successful. Then, the decoding failure probability of the open message, which is transmitted r times is calculated as:

$$\rho_{(i,r)}^{\text{open}} = \mathbb{P}\left(\sum_{k=1}^{r} R_i(t_k^o) < C_i^{\text{open}} \right). \tag{4.5}$$

Given the encoding rates, $C_i^{\text{code}}, C_i^{\text{conf}}$ and C_i^{open}, the probabilities in (4.3)-(4.5) can be easily calculated according to the known iid distributions of $R_i(t_k)$, $R_{ij}(t_k)$ and $R_i(t_k^o)$, $k = 1, \ldots, r.$ and they are time-invariant[3].

[3] This assumption is reasonable for both slow fading and fast fading channel models in which the sequence of channel states over time slots for each node is iid, and so the probabilities are obtained by averaging over the channel distributions.

As discussed in [95], it is possible to encode open information at a rate $C_i^{\text{code}} - C_i^{\text{conf}}$, jointly with the private information at rate C_i^{conf}. For that, during generation of mother code, one can simply replace the randomization message of the binning strategy of the achievability scheme with the open message, which is allowed to be decoded by other users.

4.2.3 Characterization of Achievable Rate Region

We call an arrival rate vector an *achievable rate* vector with respect to a set of given outage constraints $\gamma_1, \ldots, \gamma_n$, if there exists a scheduling strategy and associated HARQ codes for each node such that all queues in the system remain stable and the long-term average rate of the occurrence of an outage (decoding or secrecy) event for each user i remains below γ_i. Here, we characterize the rates achievable in a multi-user communication system employing HARQ transmission scheme with incremental redundancy as described in the previous section. We characterize achievable rate regions of two different policies and then show the equivalence of both.

(1) Conventional policy: In this policy, the scheduler chooses a node to transmit, and the scheduled node transmits a message until it is successfully decoded by the base station. This policy is employed by the majority of works in the scope of the cross-layer control with HARQ [9, 107].

(2) Proposed policy: In this policy, each node groups its messages according to their transmission attempts, and scheduler selects a message from any of these groups.

To characterize the achievable rate region under the conventional scheduling policy, let us define a randomized policy, which schedules a confidential or open message of node i with probabilities π_i^{conf} and π_i^{open}, respectively and the transmission is repeated r times until a maximum retransmission limit is reached, or when a message transmitted r times previously is dropped with probability $d_{(i,r)}$. Let $\pi_{(i,r)}^{\text{conf}}$ and $\pi_{(i,r)}^{\text{open}}$ be the portion of all transmissions that node i is active in sending the confidential and open messages transmitted r times previously, respectively.

We present the achievable rate regions under the knowledge of the probabilities of secrecy outage and decoding failure of confidential messages transmitted $r-1$ times previously, $\rho^{\text{secr}}_{(i,r)}$, $\rho^{\text{conf}}_{(i,r)}$ and the probability of decoding failure of open messages transmitted $r-1$ times previously, $\rho^{\text{open}}_{(i,r)}$.

Proposition 1. *The achievable rate region under the conventional policy, Γ, consists of all rates, λ_i^{conf} and λ_i^{open}, for which there exists probabilities, π_i^{conf} and π_i^{open}, and $d_{(i,r)}$ such that for all i*

$$\pi^{conf}_{(i,r)} = \pi^{conf}_{(i,r-1)}\rho^{conf}_{(i,r-1)}(1-d_{(i,r-1)}),\ \forall r = 2,\dots,M, \tag{4.6}$$

$$\pi^{open}_{(i,r)} = \pi^{open}_{(i,r-1)}\rho^{open}_{(i,r-1)},\ \forall r = 2,\dots,M, \tag{4.7}$$

$$\pi^{conf}_{i} = \sum_{r=1}^{M}\pi^{conf}_{(i,r)}, \tag{4.8}$$

$$\pi^{open}_{i} = \sum_{r=1}^{M}\pi^{open}_{(i,r)}, \tag{4.9}$$

$$1 \geq \sum_{i=1}^{n}\left(\pi^{conf}_{i} + \pi^{open}_{i}\right) \tag{4.10}$$

$$C^{conf}_{i}\gamma_i \geq C^{conf}_{i}\sum_{r=1}^{M}\pi^{conf}_{(i,r)}\rho^{secr}_{(i,r)}\left((1-\rho^{conf}_{(i,r)}) + \rho^{conf}_{(i,r)}d_{(i,r)}\right), \tag{4.11}$$

$$\lambda^{conf}_{i} \leq C^{conf}_{i}\pi^{conf}_{(i,1)}, \tag{4.12}$$

$$\lambda^{open}_{i} \leq C^{open}_{i}\pi^{open}_{(i,1)}. \tag{4.13}$$

The necessity of the above conditions can be proven following the same approach in Theorem 3.8 in [6].

Conditions (4.6) and (4.7) represent that the messages should be transmitted until it is successfully decoded by the base station. (4.10) follows that only one node is allowed to transmit either confidential or open information at a given slot. A confidential message transmitted r times previously undergoes secrecy outage regardless of the final decodability of the confidential message at the destination, when one of the eavesdropper accumulates information at a rate exceeding the rate of randomized information. Hence, the probability that a confidential message transmitted r times, undergoes a secrecy outage, is $\rho^{\text{secr}}_{(i,r)}\Big((1-\rho^{\text{conf}}_{(i,r)})+\rho^{\text{conf}}_{(i,r)}d_{(i,r)}\Big)$. Condition (4.11) defines a secrecy outage constraint which can be interpreted as the portion of average confidential information intercepted by other nodes, γ_i. Conditions (4.12) and (4.13) represent the flow conservation constraints, i.e., the departure rates of the confidential and open messages should be larger than or equal to the corresponding arrival rates. Since the message is successively transmitted until encountering a successful decoding event of that message, it is convenient to use $\pi^{\text{conf}}_{(i,1)}$ and $\pi^{\text{open}}_{(i,1)}$ as the departure rates.

In the conventional policy, given that a node is scheduled to transmit, whether or not a successful transmission will occur in that slot is not an iid random variable but rather it depends on the number of times that the message is transmitted previously, which is characterized by the conditions (4.6) and (4.7). For that reason, nodes need to keep track of the number of times that the message is transmitted previously. Hence, the transmissions in subsequent time-slots under the conventional scheduling policy is temporally coupled. This coupling between successive transmission decisions eliminates the possibility of using standard dynamic control algorithms. Hence, we propose a novel scheduling approach where the messages are grouped according to the number of times they are transmitted, and the scheduler selects a message from any of these groups to transmit. Let us define a stationary policy that selects the confidential and open messages among all messages transmitted r times previously with probabilities $\hat{\pi}^{\text{conf}}_{(i,r)}$ and $\hat{\pi}^{\text{open}}_{(i,r)}$, respectively. In contrast to conventional policy where $\pi^{\text{conf}}_{(i,r)}$ and $\pi^{\text{open}}_{(i,r)}$ are dictated completely by the number of retransmissions of the transmitted message once node i is scheduled, now with the proposed policy at each slot we may serve a different message from a different user which was transmitted r times previously.

Proposition 2. *The achievable rate region under the proposed policy, $\hat{\Gamma}$, consists of all rates, λ^{conf}_i and λ^{open}_i, for which there exists $\hat{\pi}^{conf}_{(i,r)}$ and $\hat{\pi}^{open}_{(i,r)}$, and $d_{(i,r)}$ such that for all i*

$$C_i^{conf}\hat{\pi}_{(i,r)}^{conf} \geq C_i^{conf}\hat{\pi}_{(i,r-1)}^{conf}(1-d_{(i,r-1)})\rho_{(i,r-1)}^{conf},\ \forall r = 2,\ldots,M, \tag{4.14}$$

$$C_i^{open}\hat{\pi}_{(i,r)}^{open} \geq C_i^{open}\hat{\pi}_{(i,r-1)}^{open}\rho_{(i,r-1)}^{open},\ \forall r = 2,\ldots,M, \tag{4.15}$$

$$1 \geq \sum_{i=1}^{n}\sum_{r=1}^{M}\left(\hat{\pi}_{(i,r)}^{conf} + \hat{\pi}_{(i,r)}^{open}\right), \tag{4.16}$$

$$C_i^{conf}\gamma_i \geq C_i^{conf}\sum_{r=1}^{M}\hat{\pi}_{(i,r)}^{conf}\rho_{(i,r)}^{secr}\left((1-\rho_{(i,r)}^{conf}) + \rho_{(i,r)}^{conf}d_{(i,r)}\right), \tag{4.17}$$

$$\lambda_i^{conf} \leq \hat{\pi}_{(i,1)}^{conf}C_i^{conf}, \tag{4.18}$$

$$\lambda_i^{open} \leq \hat{\pi}_{(i,1)}^{open}C_i^{open}. \tag{4.19}$$

Our subsequent algorithm development depends strictly on the achievable rate region as specified by Proposition 2. The sufficiency part for the network stability is proven in Section 4.4 by constructing a dynamic stabilizing policy for any rate vector that is in the achievable rate region.

Conditions (4.14) and (4.15) represent retransmission constraints which implies that the messages for which the base station fails to decode, should be transmitted in later time instants. (4.18) and (4.19) represent again the flow conservation constraints.

The importance of the Proposition 2 is that the message that is scheduled to transmit previously, corresponding to a particular user does not necessarily have priority over the users other messages, and the scheduler selects a message from any of these groups to transmit. More specifically, in the region specified by Proposition 2, we can construct a network that contains *virtual nodes* as shown in Section 4.4, which handle the messages the base station fails to decode. Specifically, in order to handle the messages undergoing a decoding failure event in a simple and effective way, we introduce queues that store the messages transmitted the same number of times previously. The intuition behind the introduction of these queues is to transform coupling introduced by the successive transmissions of the message into virtual nodes, and thus removing the need of the number of times a message is transmitted in making scheduling decisions. As we show in Section 4.4, the optimal solution can be obtained by using standard dynamic network control algorithms [6].

Proposition 3. *The achievable rate region $\hat{\Gamma}$ defined in Proposition 2 is the same as Γ defined in Proposition 1.*

Proof. Here, we provide the proof for the confidential messages by identifying the achievable rate regions for confidential messages, but it can be shown in a similar way for the open messages. Let $\boldsymbol{\lambda}^{\text{conf}}$ be the rate vector defined as $\left[\lambda_1^{\text{conf}}, \ldots, \lambda_n^{\text{conf}}\right]$. First, we show that if $\boldsymbol{\lambda}^{\text{conf}} \in \Gamma$, then it should lie in $\hat{\Gamma}$ as well. This can be shown directly by determining $\hat{\pi}_{(i,1)}^{\text{conf}}$ which is equal to (or larger than) $\pi_{(i,1)}^{\text{conf}}$, since the departure rates are completely characterized by $\hat{\pi}_{(i,1)}^{\text{conf}}$ and $\pi_{(i,1)}^{\text{conf}}$. Note that, with conventional policy given the control decisions, π_i^{conf} and $d_{(i,r)}$, we uniquely obtain $\pi_{(i,r)}$ using (4.6) and (4.8) as:

$$\pi_{(i,r)}^{\text{conf}} = \pi_i^{\text{conf}} \frac{\prod_{n=1}^{r-1} \rho_{(i,n)}^{\text{conf}} (1 - d_{(i,n)})}{1 + \sum_{m=1}^{M-1} \prod_{n=1}^{m} \rho_{(i,n)}^{\text{conf}} (1 - d_{(i,n)})} \tag{4.20}$$

Suppose that (4.14) is realized with equality. Then, if the stationary random scheduling decision of the proposed policy, $\hat{\pi}_{(i,r)}^{\text{conf}}$, is selected such that $\hat{\pi}_{(i,r)}^{\text{conf}} = \pi_{(i,r)}^{\text{conf}}$, where $\pi_{(i,r)}^{\text{conf}}$ is obtained in (4.20), $\boldsymbol{\lambda}^{\text{conf}} \in \hat{\Gamma}$ as well.

The other direction can be shown by proving that for any $\boldsymbol{\lambda}^{\text{conf}} + \epsilon_1 \in \hat{\Gamma}$, $\boldsymbol{\lambda}^{\text{conf}} + \epsilon_2 \in \Gamma$, and $\epsilon_2 \leq \epsilon_1$.

Since $\boldsymbol{\lambda}^{\text{conf}} + \epsilon_1 \in \hat{\Gamma}$, we have

$$\lambda_i^{\text{conf}} + \epsilon_1 \leq C_i^{\text{conf}} \hat{\pi}_{(i,1)}^{\text{conf}}$$

Let $\epsilon \geq 0$ be a variable reflecting the slack in inequality (4.14):

$$\hat{\pi}_{(i,r)}^{\text{conf}} = \hat{\pi}_{(i,r-1)}^{\text{conf}} \rho_{(i,r-1)}^{\text{conf}} (1 - d_{(i,r-1)}) + \epsilon, \tag{4.21}$$

Now, we need to determine whether there exists $\pi_{(i,1)}^{\text{conf}}$ referring to the departure rate such that λ_i^{conf} is in the region specified by Γ. By letting $\sum_{r=1}^{M} \hat{\pi}_{(i,r)}^{\text{conf}} = \sum_{r=1}^{M} \pi_{(i,r)}^{\text{conf}}$, we have that (4.10) and (4.8) satisfied, and by using (4.6) for $\pi_{(i,r)}^{\text{conf}}$ and (4.21) for $\hat{\pi}_{(i,r)}^{\text{conf}}$, we obtain $\pi_{(i,1)}^{\text{conf}}$ as:

$$\pi^{\text{conf}}_{(i,1)} = \hat{\pi}^{\text{conf}}_{(i,1)} + \frac{(M-1)\epsilon}{1+\sum_{m=1}^{M-1}\prod_{n=1}^{m}\rho^{\text{conf}}_{(i,n)}(1-d_{(i,n)})},$$

where M is the maximum number of times that a message can be retransmitted. By letting $\epsilon_2 = \epsilon_1 - \frac{C_i^{\text{conf}}(M-1)\epsilon}{1+\sum_{m=1}^{M-1}\prod_{n=1}^{m}\rho^{\text{conf}}_{(i,n)}(1-d_{(i,n)})}$, we have

$$\lambda_i^{\text{conf}} + \epsilon_2 \leq C_i^{\text{conf}}\pi^{\text{conf}}_{(i,1)}.$$

Thus, we have $\boldsymbol{\lambda}^{\text{conf}} + \epsilon_2 \in \Gamma$. Notice that, the second term of ϵ_2 is non-negative implying that ϵ_2 is always equal to or smaller than ϵ_1. Furthermore, in the first part, we prove that for $\boldsymbol{\lambda}^{\text{conf}} \in \Gamma$, $\boldsymbol{\lambda}^{\text{conf}} \in \hat{\Gamma}$ as well, so ϵ_2 cannot have a negative value. As $\epsilon_1 \to 0$, ϵ_2 and ϵ approach zero as well, which proves that in the boundary of the region $\hat{\Gamma}$, (4.14) is realized with equality, and $\Gamma = \hat{\Gamma}$.

□

We acknowledge that even though the region specified by Proposition 2 is the same as the one specified with Proposition 1, the base station now needs to store the transmitted parts of the messages until they are successfully decoded. Thus, each packet is assumed to have an appropriate header field with source and packet number identifiers so that the base station buffers the packets according to these identifiers. This creates a system with delayed successful transmission of the messages, which does not affect the rate region but may increase the average network delay.

4.3 Optimal Scheduling and Flow Control

Next, we formulate the problem as a static optimization problem. Using dual decomposition, we then obtain a dynamic solution to this problem and prove its optimality using stochastic Lyapunov techniques.

4.3.1 Network Utility Maximization

Our objective is to design a joint flow control and scheduling algorithm that maximizes the aggregate network utility, while keeping the probability of secrecy outage below a certain level. We assume that a node obtains a utility, only from messages successfully decoded by the base station. Recall that the base station may decide to drop a confidential message if its further retransmission of the message may violate the secrecy outage constraint of the node. Let μ_i^{drop} be the average rate of confidential information being dropped, i.e., $\mu_i^{\text{drop}} = C_i^{\text{conf}} \sum_{r=1}^{M} \pi_{(i,r)}^{\text{conf}} \rho_{(i,r)}^{\text{conf}} d_{(i,r)}$. Hence, the goodput of node i is $\lambda_i^{\text{conf}} - \mu_i^{\text{drop}}$ from which it obtains a utility of $U_i^{\text{conf}}(\lambda_i^{\text{conf}} - \mu_i^{\text{drop}})$. Also, node i obtains a utility of $U_i^{\text{open}}(\lambda_i^{\text{open}})$ from the transmission of open messages. In this chapter, we consider the following problem:

$$\begin{aligned} (P): \quad & \max \sum_{i=1}^{n} U_i^{\text{conf}}(\lambda_i^{\text{conf}} - \mu_i^{\text{drop}}) + U_i^{\text{open}}(\lambda_i^{\text{open}}) \qquad (4.22) \\ & \text{subject to } \ (4.14) - (4.19), \end{aligned}$$

where the maximization is over the parameters $\pi_{(i,r)}^{\text{conf}}, \pi_{(i,r)}^{\text{open}}, d_{(i,r)}, \lambda_i^{\text{conf}}, \lambda_i^{\text{open}}$.

The optimization problem (P) is referred to as a Network Utility Maximization (NUM) problem, which is usually solved by decomposing it into a centralized scheduling sub-problem, and n independent flow control sub-problems solved by each node i. However, the objective function (4.22) is coupled among the nodes in the network, which in turn prohibits such a decomposition. The coupling is due to the parameter μ_i^{drop} depending on the scheduling decisions, which inevitably affects all the nodes in the system. The coupling in the objective function is usually harder to deal with than the coupling in the constraints, since the latter can be decomposed by using primal or dual decompositions (see [108] and the references therein). In order to address the coupling in the objective function, we introduce an auxiliary variable λ_i^{drop} corresponding to each μ_i^{drop}, and add an additional inequality constraint with respect to the auxiliary variable. Hence, we convert the coupling in the objective function to a coupling in the constraint, which can then be decoupled by dual decomposition and solved by introducing additional dual variable. The modified version of the optimization problem (4.22) is given as follows:

$$(Q): \quad \max \sum_{i=1}^{n} U_i^{\text{conf}}(\lambda_i^{\text{conf}} - \lambda_i^{\text{drop}}) + U_i^{\text{open}}(\lambda_i^{\text{open}}) \tag{4.23}$$

$$\text{subject to} \quad (4.14) - (4.19),$$

$$\mu_i^{\text{drop}} \leq \lambda_i^{\text{drop}}, \tag{4.24}$$

for all i, where the maximization is over the parameters $\pi_{(i,r)}^{\text{conf}}, \pi_{(i,r)}^{\text{open}}, d_{(i,r)}, \lambda_i^{\text{conf}}, \lambda_i^{\text{open}}, \lambda_i^{\text{drop}}$. Note that the new decision variable λ_i^{drop} can be interpreted as the average rate of confidential information that is going to be dropped later by the node. Since the objective function (4.23) is a decreasing function of λ_i^{drop}, (4.24) is always active at the optimal point. Hence, the optimal solution of (P) is the same as that of (Q).

4.3.2 Dual Decomposition

Note that the objective function (4.23) is separable into individual user utility maximization problems, and due to the definition of the constraints in (4.14)-(4.19) and (4.24), there is no correlation among successive transmissions. Here, we solve the problem using dual decomposition method that is particularly appealing to our problem structure.

Let us first introduce dual variables $\{\mathbf{q}^{\text{conf}}, \mathbf{q}^{\text{open}}, \mathbf{q}^{\text{drop}}, \mathbf{k}\}$ to relax constraints in (4.14)-(4.19) and (4.24), respectively. Then we have the dual function as:

$$D(\mathbf{q}^{\text{conf}}, \mathbf{q}^{\text{open}}, \mathbf{q}^{\text{drop}}, \mathbf{k}) = \max_{\boldsymbol{\pi}, \mathbf{d}} L(\boldsymbol{\pi}^{\text{conf}}, \boldsymbol{\pi}^{\text{open}}, \mathbf{d}; \mathbf{q}^{\text{conf}}, \mathbf{q}^{\text{open}}, \mathbf{q}^{\text{drop}}, \mathbf{k}), \tag{4.25}$$

where

$$\begin{aligned}
&L(\boldsymbol{\pi}^{\text{conf}}, \boldsymbol{\pi}^{\text{open}}, \mathbf{d}; \mathbf{q}^{\text{conf}}, \mathbf{q}^{\text{open}}, \mathbf{q}^{\text{drop}}, \mathbf{k}) \\
&= \sum_i \left(U_i^{\text{conf}}(\lambda_i^{\text{conf}} - \lambda_i^{\text{drop}}) + U_i^{\text{open}}(\lambda_i^{\text{open}}) \right) \\
&+ q_{(i,1)}^{\text{conf}} \left(\pi_{(i,r)}^{\text{conf}} C_i^{\text{conf}} - \lambda_i^{\text{conf}} \right) + q_{(i,1)}^{\text{open}} \left(\pi_{(i,r)}^{\text{open}} C_i^{\text{open}} - \lambda_i^{\text{open}} \right) \\
&+ C_i^{\text{conf}} \sum_{r=2}^{M} q_{(i,r)}^{\text{conf}} \left(\pi_{(i,r)}^{\text{conf}} - \pi_{(i,r-1)}^{\text{conf}} (1 - d_{(i,r-1)}) \rho_{(i,r-1)}^{\text{conf}} \right) \\
&+ C_i^{\text{open}} \sum_{r=2}^{M} q_{(i,r)}^{\text{open}} \left(\pi_{(i,r)}^{\text{open}} - \pi_{(i,r-1)}^{\text{open}} \rho_{(i,r-1)}^{\text{open}} \right) - q_i^{\text{drop}} \left(\mu_i^{\text{drop}} - \lambda_i^{\text{drop}} \right) \\
&- k_i C_i^{\text{conf}} \sum_{r=1}^{M} \left(\pi_{(i,r)}^{\text{conf}} \rho_{(i,r)}^{\text{secr}} ((1 - \rho_{(i,r)}^{\text{conf}}) + \rho_{(i,r)}^{\text{conf}} d_{(i,r)}) \right). \qquad (4.26)
\end{aligned}$$

Let $\boldsymbol{\lambda}^{\text{conf}}$,$\boldsymbol{\lambda}^{\text{open}}$, $\boldsymbol{\pi}$ and $\mathbf{d}$ represent the vectors of primal variables of the rates of flows of confidential and open traffic, the probabilities of scheduling and dropping, respectively; $\mathbf{q}^{\text{conf}}$, $\mathbf{q}^{\text{open}}$, $\mathbf{q}^{\text{drop}}$ and $\mathbf{k}$ represent the vectors of corresponding dual variables.

Let $\lambda_i^{\text{conf}^*}$, $\lambda_i^{\text{drop}^*}$ and $\lambda_i^{\text{open}^*}$ be the optimal rates of confidential, dropped and open information, respectively. Slater's condition in [109] states that, since the objective function is concave and the constraints are affine functions, the duality gap is zero and therefore $D(\mathbf{q}^{\text{conf}^*}, \mathbf{q}^{\text{open}^*}, \mathbf{q}^{\text{drop}^*}, \mathbf{k}^*) = \sum_i \left(U_i^{\text{conf}}(\lambda_i^{\text{conf}^*} - \lambda_i^{\text{drop}^*}) + U_i^{\text{open}}(\lambda_i^{\text{open}^*}) \right)$ where

$$\mathbf{q}^{\text{conf}^*}, \mathbf{q}^{\text{open}^*}, \mathbf{q}^{\text{drop}^*}, \mathbf{k}^* \in \underset{q_{(i,r)}^{\text{conf}} \geq 0, q_{(i,r)}^{\text{open}} \geq 0, q_i^{\text{drop}} \geq 0, k_i \geq 0}{\operatorname{argmin}} D(\mathbf{q}^{\text{conf}}, \mathbf{q}^{\text{open}}, \mathbf{q}^{\text{drop}}, \mathbf{k}).$$

We are interested to obtain the optimal primal variables, i.e., $(\lambda_i^{\text{conf}^*}, \lambda_i^{\text{drop}^*}, \lambda_i^{\text{open}^*})$ as flow rates and $(\boldsymbol{\pi}^{\text{conf}^*}, \boldsymbol{\pi}^{\text{open}^*}, \mathbf{d}^*)$ as scheduling and dropping decisions. We notice that the dual function in (4.25) can be decomposed into the following subproblems:

$$\begin{aligned}D(\mathbf{q}^{\text{conf}}, \mathbf{q}^{\text{open}}, \mathbf{q}^{\text{drop}}, \mathbf{k}) =& D_1(\mathbf{q}^{\text{conf}}, \mathbf{q}^{\text{open}}, \mathbf{q}^{\text{drop}}) \\ &+ D_2(\mathbf{q}^{\text{conf}}, \mathbf{q}^{\text{open}}, \mathbf{q}^{\text{drop}}, \mathbf{k})\end{aligned}$$

where

$$\begin{aligned}D_1(\mathbf{q}^{\text{conf}}, \mathbf{q}^{\text{open}}, \mathbf{q}^{\text{drop}}) = &\max_{\lambda_i^{\text{conf}}, \lambda_i^{\text{open}}, \lambda_i^{\text{drop}}} \sum_i \Big(U_i^{\text{conf}}(\lambda_i^{\text{conf}} - \lambda_i^{\text{drop}}) \\ +U_i^{\text{open}}(\lambda_i^{\text{open}})) - q_{(i,1)}^{\text{conf}} \lambda_i^{\text{conf}} - q_{(i,1)}^{\text{open}} \lambda_i^{\text{open}} + q_i^{\text{drop}} \lambda_i^{\text{drop}},\end{aligned} \tag{4.27}$$

$$\begin{aligned}D_2(\mathbf{q}^{\text{conf}}, \mathbf{q}^{\text{open}}, \mathbf{q}^{\text{drop}}, \mathbf{k}) = &\max_{\pi_{(i,r)}^{\text{conf}}, \pi_{(i,r)}^{\text{open}}, d_{(i,r)}} \sum_{r=1}^{M} q_{(i,r)}^{\text{conf}} \pi_{(i,r)}^{\text{conf}} C_i^{\text{conf}} \\ - \sum_{r=2}^{M} \pi_{(i,r-1)}^{\text{conf}} (1 - d_{(i,r-1)}) \rho_{(i,r-1)}^{\text{conf}} C_i^{\text{conf}} + \sum_{r=1}^{M} q_{(i,r)}^{\text{open}} \pi_{(i,r)}^{\text{open}} C_i^{\text{open}} \\ - \sum_{r=2}^{M} q_{(i,r)}^{\text{open}} \pi_{(i,r-1)}^{\text{open}} C_i^{\text{open}} \rho_{(i,r-1)}^{\text{open}} - q_i^{\text{drop}} \mu_i^{\text{drop}} \\ - k_i C_i^{\text{conf}} \sum_{r=1}^{M} \Big(\pi_{(i,r)}^{\text{conf}} \rho_{(i,r)}^{\text{secr}} ((1 - \rho_{(i,r)}^{\text{conf}}) + \rho_{(i,r)}^{\text{conf}} d_{(i,r)}) \Big) .\end{aligned} \tag{4.28}$$

Subproblems (4.27) and (4.28) can be solved separately resulting in a cross-layer optimization algorithm for joint scheduling and flow control, to be showed in the next section.

The dual problem can be solved using the subgradient projection method [110]. Let $\mathbf{Gq}^{\text{conf}}$, $\mathbf{Gq}^{\text{open}}$, $\mathbf{Gq}^{\text{drop}}$ and $\mathbf{Gk}$ be the subgradients of respective dual variables. Since primal variables $\boldsymbol{\pi}^{\text{conf}}$, $\boldsymbol{\pi}^{\text{open}}$ and $\mathbf{d}$ are obtained as a solution of maximization in dual objective function (4.25) at point $(q^{\text{conf}}, q^{\text{open}}, q^{\text{drop}}, k)$, the subgradients of function (4.25) can be expressed as follows:

$$Gq^{\text{conf}}_{(i,r)} = \begin{cases} \lambda^{\text{conf}}_i - \pi^{\text{conf}}_{(i,r)} C^{\text{conf}}_i, & \text{if } r = 1 \\ \pi^{\text{conf}}_{(i,r-1)}(1 - d_{(i,r-1)})\rho^{\text{conf}}_{(i,r-1)} C^{\text{conf}}_i - \pi^{\text{conf}}_{(i,r)} C^{\text{conf}}_i, & \text{otherwise} \end{cases}, \tag{4.29}$$

$$Gq^{\text{open}}_{(i,r)} = \begin{cases} \lambda^{\text{open}}_i - \pi^{\text{open}}_{(i,r)} C^{\text{open}}_i, & \text{if } r = 1 \\ \pi^{\text{open}}_{(i,r-1)}\rho^{\text{open}}_{(i,r-1)} C^{\text{open}}_i - \pi^{\text{conf}}_{(i,r)} C^{\text{open}}_i, & \text{otherwise} \end{cases}, \tag{4.30}$$

$$Gq^{\text{drop}}_i = \mu^{\text{drop}}_i - \lambda^{\text{drop}}_i, \tag{4.31}$$

$$Gk_i = \sum_{r=1}^{M} \pi^{\text{conf}}_{(i,r)} \rho^{\text{secr}}_{(i,r)} \left((1 - \rho^{\text{conf}}_{(i,r)}) + \rho^{\text{conf}}_{(i,r)} d_{(i,r)} \right) C^{\text{conf}}_i - \gamma_i C^{\text{conf}}_i. \tag{4.32}$$

The subgradient projection method finds the optimal solution by updating the dual variables in each iteration step t in the opposite direction of the subgradients:

$$q^{\text{conf}}_{(i,r)}(t+1) = [q^{\text{conf}}_{(i,r)}(t) + \alpha G q^{\text{conf}}_{(i,r)}]^+, \tag{4.33}$$

$$q^{\text{open}}_{(i,r)}(t+1) = [q^{\text{open}}_{(i,r)}(t) + \alpha G q^{\text{open}}_{(i,r)}]^+, \tag{4.34}$$

$$q^{\text{drop}}_i(t+1) = [q^{\text{drop}}_i(t) + \alpha G q^{\text{drop}}_i]^+, \tag{4.35}$$

$$k_i(t+1) = [k_i(t) + \alpha G k_i]^+, \tag{4.36}$$

where α is positive constant step size.

The dual decomposition approach only provides an intuition behind the solution, but the real network has dynamic arrivals. In the next section, we present a complete solution which takes into account these dynamics, and establish its convergence and optimality.

4.3.3 Joint Encoding of Confidential and Open Information

In the case of joint encoding, a node can transmit $C^{\text{code}}_i - C^{\text{conf}}_i$ rate of open information upon successful transmission of a confidential message. Since open bits are used on the behalf of randomization bits, they should not be transmitted in the previous slots so that overhearing nodes do not have any information about the jointly encoded open bits. Thus, jointly encoded open bits are selected from newly arrived bits. In addition, we assume that by dropping confidential message, we drop jointly encoded open bits as well. To take into account joint encoding, we first need to modify condition (4.19) as:

$$\sum_{r=1}^{M} \pi^{\text{conf}}_{(i,r)} \left(C^{\text{code}}_i - C^{\text{conf}}_i\right) \Big((1-\rho^{\text{conf}}_{(i,r)}) + \rho^{\text{conf}}_{(i,r)} d_{(i,r)}\Big) + \pi^{\text{open}}_{(i,1)} C^{\text{open}}_i \geq \lambda^{\text{open}}_i, \ \forall i, \tag{4.37}$$

Let $\mu^{\text{o,drop}}_i$ be the average rate of open information being dropped, i.e., $\mu^{\text{o,drop}}_i = \left(C^{\text{code}}_i - C^{\text{conf}}_i\right) \sum_{r=1}^{M} \pi^{\text{conf}}_{(i,r)} \rho^{\text{conf}}_{(i,r)} d_{(i,r)}$. Hence, node i obtains a utility of $U^{\text{open}}_i(\lambda^{\text{open}}_i - \mu^{\text{o,drop}}_i)$ from the transmission of open messages and the transmission of jointly encoded confidential messages. By following the same steps in Section 4.3.1, we obtain the optimization problem with joint encoding as follows:

$$(J): \quad \max \sum_{i=1}^{n} U^{\text{conf}}_i(\lambda^{\text{conf}}_i - \lambda^{\text{drop}}_i) + U^{\text{open}}_i(\lambda^{\text{open}}_i - \lambda^{\text{o,drop}}_i) \tag{4.38}$$

$$\text{subject to } \ (4.14)-(4.18), (4.24), (4.37),$$

$$\mu^{\text{o,drop}}_i \leq \lambda^{\text{o,drop}}_i, \tag{4.39}$$

for all i, where the maximization is over the parameters $\pi^{\text{conf}}_{(i,r)}, \pi^{\text{open}}_{(i,r)}, d_{(i,r)}, \lambda^{\text{conf}}_i, \lambda^{\text{open}}_i, \lambda^{\text{drop}}_i, \lambda^{\text{o,drop}}_i$. Note that the newly added decision variable $\lambda^{\text{o,drop}}_i$ can be interpreted as the average rate of open information that is going to be jointly dropped with confidential information later by the node.

Based on the given optimization problem (J), the Lagrangian function of (Q) defined in (4.26) should be modified as:

$$\begin{aligned}
&L(\boldsymbol{\pi}^{\text{conf}}, \boldsymbol{\pi}^{\text{open}}, \mathbf{d}; \mathbf{q}^{\text{conf}}, \mathbf{q}^{\text{open}}, \mathbf{q}^{\text{drop}}, \mathbf{k}) \\
&= \sum_i \left(U_i^{\text{conf}}(\lambda_i^{\text{conf}} - \lambda_i^{\text{drop}}) + U_i^{\text{open}}(\lambda_i^{\text{open}} - \lambda_i^{\text{o,drop}}) \right) \\
&- q_i^{\text{o,drop}} \left(\mu_i^{\text{o,drop}} - \lambda_i^{\text{o,drop}} \right) + q_{(i,1)}^{\text{conf}} \left(\pi_{(i,r)}^{\text{conf}} C_i^{\text{conf}} \right) \\
&+ q_{(i,1)}^{\text{open}} \left(\pi_{(i,r)}^{\text{open}} C_i^{\text{open}} + \sum_{r=1}^{M} \pi_{(i,r)}^{\text{conf}} \pi_{(i,r)}^{\text{conf}} \left(C_i^{\text{code}} - C_i^{\text{conf}} \right) - \lambda_i^{\text{open}} \right) \\
&+ C_i^{\text{conf}} \sum_{r=2}^{M} q_{(i,r)}^{\text{conf}} \left(\pi_{(i,r)}^{\text{conf}} - \pi_{(i,r-1)}^{\text{conf}} (1 - d_{(i,r-1)}) \rho_{(i,r-1)}^{\text{conf}} \right) \\
&+ C_i^{\text{open}} \sum_{r=2}^{M} q_{(i,r)}^{\text{open}} \left(\pi_{(i,r)}^{\text{open}} - \pi_{(i,r-1)}^{\text{open}} \rho_{(i,r-1)}^{\text{open}} \right) - q_i^{\text{drop}} \left(\mu_i^{\text{drop}} - \lambda_i^{\text{drop}} \right) \\
&- k_i C_i^{\text{conf}} \sum_{r=1}^{M} \left(\pi_{(i,r)}^{\text{conf}} \rho_{(i,r)}^{\text{secr}} ((1 - \rho_{(i,r)}^{\text{conf}}) + \rho_{(i,r)}^{\text{conf}} d_{(i,r)}) \right).
\end{aligned} \tag{4.40}$$

where $q_i^{\text{o,drop}}$ is a dual variable to relax constraint in (4.39). Based on modified Lagrangian function in (4.40), it is straightforward to modify subproblems in (4.27) and (4.28) and subgradient in (4.30). In addition, the dual variable $q_i^{\text{o,drop}}$ is updated in each iteration step t as:

$$q_i^{\text{o,drop}}(t+1) = [q_i^{\text{o,drop}}(t) + \alpha \left(\mu_i^{\text{o,drop}} - \lambda_i^{\text{o,drop}} \right)]^{+} \tag{4.41}$$

With the above modifications, it is straightforward to generalize all subsequent development to handle the scenario with joint encoding of open and confidential messages.

4.4 Queue Model and Dynamic Control

In this section, we relate each subproblem derived from the dual decomposition with a functionality of wireless networks such as scheduling and flow control. The solution given by (4.28) gives the steady state probabilities of transmissions from each node.

However, the cross-layer algorithm presented here is a simple index policy, which observes the current state and makes a decision dynamically.

4.4.1 Queuing Model

We can associate each of the dual variables $(\mathbf{q}^{\text{conf}}, \mathbf{q}^{\text{open}})$ with a queue. These queues are obtained by simply making the change of variable at the update of dual variables as $\alpha Q_{(i,r)}^{\text{conf}}(t) = q_{(i,r)}^{\text{conf}}(t)$ and $\alpha Q_{(i,r)}^{\text{open}}(t) = q_{(i,r)}^{\text{open}}(t)$. Note that these queues store codewords of messages having been transmitted the same number of times, i.e., $Q_{(i,r)}^{\text{conf}}(t)$ and $Q_{(i,r)}^{\text{open}}(t)$ denote the sizes of the queues storing codewords for confidential and open messages respectively, of node i that are already transmitted $r-1$ times by time slot t as illustrated in Fig. 4.1. Since the maximum number of transmission attempts is M, there are a total of $2M$ queues at each node. By definition, $Q_{(i,1)}^{\text{conf}}(t)$ and $Q_{(i,1)}^{\text{open}}(t)$ refer to the sizes of queues storing packets not transmitted yet by slot t. In addition, at each time slot, nodes decide how much confidential and open information they admit to their respective queues. Hence, the arrivals to these queues are exogenous with rates $A_i^{\text{conf}}(t)$ and $A_i^{\text{open}}(t)$ bits per channel use, respectively. We assume that arrival processes are stationary and ergodic, and the arrival rates, $A_i^{\text{conf}}(t)$ and $A_i^{\text{open}}(t)$ have long-term average rates λ_i^{conf} and λ_i^{open} respectively, i.e., $\lambda_i^{\text{conf}} \triangleq \mathbb{E}\left[A_i^{\text{conf}}(t)\right]$ and $\lambda_i^{\text{open}} \triangleq \mathbb{E}\left[A_i^{\text{open}}(t)\right]$ and the maximum number of arrivals are bounded by finite numbers, $A_i^{\text{conf,max}}$ and $A_i^{\text{open,max}}$. Arrivals to all other queues are triggered by a NAK feedback received from the base station due to a decoding failure of a previous transmission attempt. For example, after the transmission of the codeword x_i^r, if the base station fails to decode the message, the codeword x_i^{r+1} is inserted into the next queue $r+1$. Note that all codewords x_i^r , $r = 1, \ldots, M$ are generated from the same mother code. For ease of exposition, we call these codewords as packets of the same message.

At each time slot, the length of each of the $2M$ queues, and the secrecy outage and decoding failure probabilities are observed. Based on this information, a node and one of its $2M$ queues is scheduled and the head of line packet from this queue is transmitted. Let $\mathcal{S}_{(i,r)}^{\text{conf}}(t)$ and $\mathcal{S}_{(i,r)}^{\text{open}}(t)$, be indicator variables representing the scheduler decision. Specifically, $\mathcal{S}_{(i,r)}^{\text{conf}}(t) = 1$ if a packet at the head of line of the rth queue

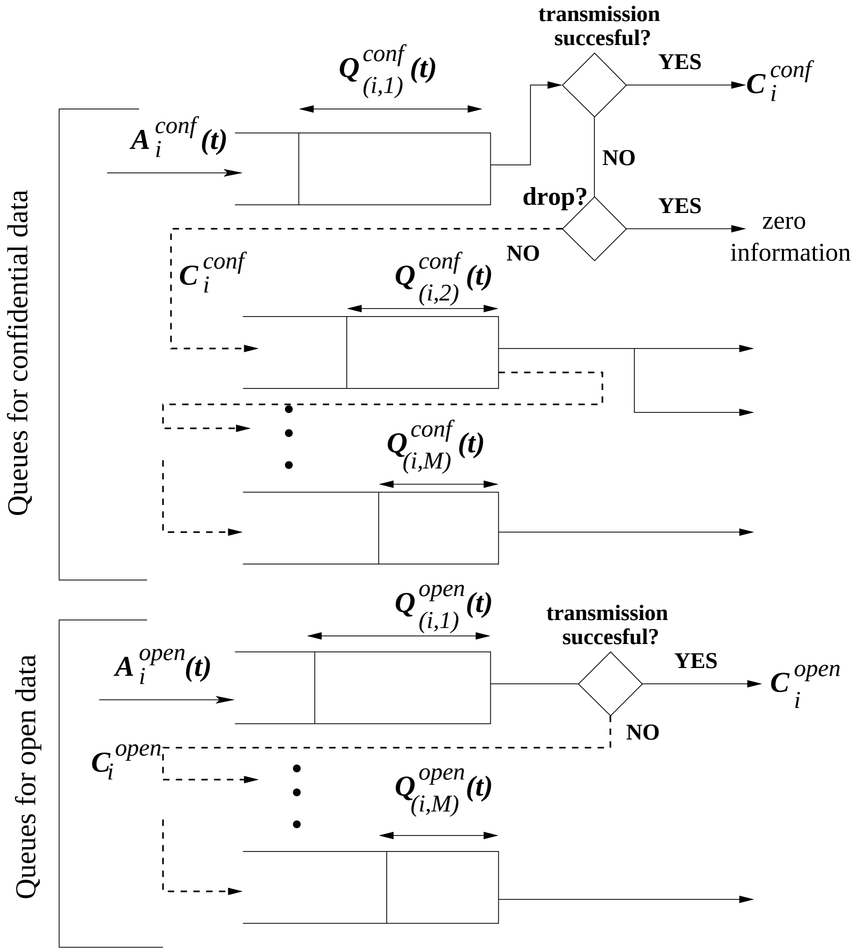


Figure 4.1: Queue model

storing confidential codewords of node i is scheduled to be served, and $\mathcal{S}^{\text{conf}}_{(i,r)}(t) = 0$ otherwise. Likewise, $\mathcal{S}^{\text{open}}_{(i,r)}(t) = 1$ if a packet at the head of line of the rth queue storing open messages of node i is scheduled to be served, and $\mathcal{S}^{\text{open}}_{(i,r)}(t) = 0$ otherwise. By definition, $\sum_{i=1}^{n}\sum_{r=1}^{M}\mathcal{S}^{\text{conf}}_{(i,r)}(t) + \mathcal{S}^{\text{open}}_{(i,r)}(t) \leq 1$ for all $t > 0$. Recall that, $\pi^{\text{conf}}_{(i,r)}$ and $\pi^{\text{open}}_{(i,r)}$ are the steady-state scheduling probability of the confidential and open messages that are transmitted $r-1$ times. These probabilities are the long-term averages of the aforementioned scheduling decisions, i.e., $\pi^{\text{conf}}_{(i,r)} = \lim_{t\to\infty}\frac{1}{t}\sum_{\tau=0}^{t}\mathcal{S}^{\text{conf}}_{(i,r)}(\tau)$ and $\pi^{\text{open}}_{(i,r)} = \lim_{t\to\infty}\frac{1}{t}\sum_{\tau=0}^{\tau}\mathcal{S}^{\text{open}}_{(i,r)}(\tau)$. Similarly, let $\mathcal{D}_{(i,r)}(t)$ be an indicator variable taking value of 1 if node i decides to drop the head of line packet in its rth confidential queue at slot t, and 0 otherwise. Then, $d_{(i,r)} = \lim_{t\to\infty}\frac{1}{t}\sum_{\tau=0}^{t}\mathcal{D}_{(i,r)}(\tau)$.

Also, let $\mathcal{F}^{\text{conf}}_{(i,r)}(t)$ and $\mathcal{F}^{\text{open}}_{(i,r)}(t)$ denote indicator variables for the decoding success/failure of a packet from the rth confidential and open queues respectively, transmitted in slot t. Precisely, $\mathcal{F}^{\text{conf}}_{(i,r)}(t) = 1$ if a confidential message in its rth transmission attempt cannot be decoded by the base station, i.e., a NAK feedback is received. Similarly, $\mathcal{F}^{\text{open}}_{(i,r)}(t) = 1$ if an open message in its rth transmission attempt cannot be decoded by the base station in slot t. We note that the long-term averages of $\mathcal{F}^{\text{conf}}_{(i,r)}(t)$ and $\mathcal{F}^{\text{open}}_{(i,r)}(t)$ give the probabilities of decoding failure at the rth transmission attempt of a confidential and open message, respectively, i.e., $\rho^{\text{conf}}_{(i,r)} = \lim_{t\to\infty} \frac{1}{t}\sum_{\tau=0}^{t} \mathcal{F}^{\text{conf}}_{(i,r)}(\tau)$ and $\rho^{\text{open}}_{(i,r)} = \lim_{t\to\infty} \frac{1}{t}\sum_{\tau=0}^{t} \mathcal{F}^{\text{open}}_{(i,r)}(\tau)$.

The dynamics of confidential and open traffic queues, $Q^{\text{conf}}_{(i,1)}(t)$ and $Q^{\text{open}}_{(i,1)}(t)$ are given as follows:

$$Q^{\text{conf}}_{(i,1)}(t+1) = \left[Q^{\text{conf}}_{(i,1)}(t) - \mathcal{S}^{\text{conf}}_{(i,1)}(t)C^{\text{conf}}_i\right]^+ + A^{\text{conf}}_i(t), \tag{4.42}$$

$$Q^{\text{open}}_{(i,1)}(t+1) = \left[Q^{\text{open}}_{(i,1)}(t) - \mathcal{S}^{\text{open}}_{(i,1)}(t)C^{\text{open}}_i\right]^+ + A^{\text{open}}_i(t), \tag{4.43}$$

where $[x]^+ = \max(0, x)$.

The dynamics of other confidential and open traffic queues, for $r \neq 1$, are as follows:

$$\begin{aligned} Q^{\text{conf}}_{(i,r)}(t+1) = &\left[Q^{\text{conf}}_{(i,r)}(t) - \mathcal{S}^{\text{conf}}_{(i,r)}(t)C^{\text{conf}}_i\right]^+ \\ &+ \mathcal{S}^{\text{conf}}_{(i,r-1)}(t)\mathcal{F}^{\text{conf}}_{(i,r-1)}(t)(1-\mathcal{D}_{(i,r-1)}(t))C^{\text{conf}}_i, \end{aligned} \tag{4.44}$$

$$\begin{aligned} Q^{\text{open}}_{(i,r)}(t+1) = &\left[Q^{\text{open}}_{(i,r)}(t) - \mathcal{S}^{\text{open}}_{(i,r)}(t)C^{\text{open}}_i\right]^+ \\ &+ \mathcal{S}^{\text{open}}_{(i,r-1)}(t)\mathcal{F}^{\text{open}}_{(i,r-1)}(t)C^{\text{open}}_i. \end{aligned} \tag{4.45}$$

Comparing (4.33)-(4.34) with (4.42)-(4.45), we can deduce the relationships of queue lengths with the corresponding dual variables as $Q^{\text{conf}}_{(i,r)}(t) = q^{\text{conf}}_{(i,r)}(t)/\alpha$ and $Q^{\text{open}}_{(i,r)}(t) = q^{\text{open}}_{(i,r)}(t)/\alpha$. In addition, we can relate the dual variables $q^{\text{drop}}_i(t)$ and $k_i(t)$ with virtual queues representing the secrecy outage and dropping constraints in (4.17) and (4.24) as:

$$K_i(t+1) = \Bigg[K_i(t) + C_i^{\text{conf}} \Bigg(\sum_{r=1}^{M} \mathcal{S}_{(i,r)}^{\text{conf}}(t)\rho_{(i,r)}^{\text{secr}} \Big((1-\mathcal{I}_{(i,r)}^{\text{conf}}(t)) + \mathcal{I}_{(i,r)}^{\text{conf}}(t)\mathcal{D}_{(i,r)}(t)\Big) - \gamma_i\Bigg)\Bigg]^+, \tag{4.46}$$

$$Q_i^{\text{drop}}(t+1) = \Bigg[Q_i^{\text{drop}}(t) - A_i^{\text{drop}}(t) + C_i^{\text{conf}} \sum_{r=1}^{M} \mathcal{S}_{(i,r)}^{\text{conf}}(t)\mathcal{F}_{(i,r)}^{\text{conf}}(t)\mathcal{D}_{(i,r)}(t)\Bigg]^+. \tag{4.47}$$

The arrivals and departures to the queue defined by (4.46) are the number of the confidential bits undergoing secrecy outage and the number of confidential bits allowed to undergo outage as given by the outage constraint, respectively. Similarly, the arrivals to the queue in (4.47) are confidential bits that are going to be dropped in subsequent slots, and departures are confidential bits actually dropped in the current slot. The state of the virtual queue at any given point is an indicator on the amount by which we have exceeded the allowable outage constraint. Thus, the larger the state of these queues, the more conservative our dynamic algorithm has to get toward meeting these constraints. In the long run, we should guarantee strong stability of the virtual queues, which in turn guarantees the constraints to be satisfied [6].

4.4.2 Cross-layer optimization algorithm

With the queueing model described in the previous section, we can use the queue length information instead of dual variables to solve the optimization problem presented in (4.23). Furthermore, our proposed scheme is based on simple index policies, involving the solution of simple optimization problems that depend only on the instantaneous state of the system. Note that, even though the secrecy outage and decoding failure probabilities are static, the information in real confidential and open queues, and virtual queues are dynamically changing over each time slot.

Control Algorithm: The algorithm executes the following steps in each slot t:

(1) Flow control: For some $\alpha > 0$, each node i injects $A_i^{\text{conf}}(t)$, and $A_i^{\text{open}}(t)$ bits of confidential and open information to real queues $Q_{(i,1)}^{\text{conf}}(t)$ and $Q_{(i,1)}^{\text{open}}(t)$ respectively. Also, node i adds $A_i^{\text{drop}}(t)$ virtual bits into virtual queue $Q_i^{\text{drop}}(t)$. We choose these parameters as the solution of:

$$\begin{aligned}
&\left(A_i^{\text{conf}}(t), A_i^{\text{drop}}(t), A_i^{\text{open}}(t)\right) \\
&= \underset{A^{\text{conf}}\geq 0, A^{\text{drop}}\geq 0, A^{\text{open}}\geq 0}{\text{argmax}} \left\{ \frac{1}{\alpha}\left[U_i^{\text{conf}}(A^{\text{conf}} - A^{\text{drop}}) + U_i^{\text{open}}(A^{\text{open}})\right] \right. \\
&\quad \left. - Q_i^{\text{conf}}(t)A^{\text{conf}} - Q_i^{\text{open}}(t)A^{\text{open}} + Q_i^{\text{drop}}(t)A^{\text{drop}} \right\}
\end{aligned}$$

(2) Scheduling: Select a node i, and one of its confidential ($\mathcal{S}_{(i,r)}^{\text{conf}}(t) = 1$) or open ($\mathcal{S}_{(i,r)}^{\text{open}}(t) = 1$) queues for transmission. If the transmission is from a confidential data queue but NAK feedback is received from the base station, determine whether to drop the confidential message ($\mathcal{D}_{(i,r)}(t) = 1$) or not. We choose these parameters as the solution of:

$$\begin{aligned}
&\left(\mathcal{S}_{(i,r)}^{\text{conf}}(t), \mathcal{S}_{(i,r)}^{\text{open}}(t), \mathcal{D}_{(i,r)}(t)\right) \\
&= \underset{\mathcal{S}^{\text{conf}}, \mathcal{S}^{\text{open}}, \mathcal{D}}{\text{argmax}} \left\{ \sum_{k=1}^{M} \left(Q_{(i,k)}^{\text{conf}}(t)\mathcal{S}_{(i,k)}^{\text{conf}}(t)C_i^{\text{conf}} + Q_{(i,k)}^{\text{open}}(t)\mathcal{S}_{(i,k)}^{\text{open}}(t)C_i^{\text{open}}\right) \right. \\
&\quad - \sum_{k=1}^{M-1} \left(Q_{(i,k+1)}^{\text{conf}}(t)\mathcal{S}_{(i,k)}^{\text{conf}}(t)\mathcal{I}_{(i,k)}^{\text{conf}}(t)(1 - \mathcal{D}_{(i,k)}(t))C_i^{\text{conf}}\right. \\
&\quad \left. +Q_{(i,k+1)}^{\text{open}}(t)\mathcal{S}_{(i,k)}^{\text{open}}(t)\mathcal{I}_{(i,k)}^{\text{open}}(t)C_i^{\text{open}}\right) \\
&\quad -Q_i^{\text{drop}}(t)\sum_{k=1}^{M}\mathcal{S}_{(i,k)}^{\text{conf}}(t)\mathcal{I}_{(i,k)}^{\text{conf}}(t)\mathcal{D}_{(i,k)}(t)C_i^{\text{conf}} - K_i(t)C_i^{\text{conf}} \\
&\quad \left. \left(\sum_{k=1}^{M}\mathcal{S}_{(i,k)}^{\text{conf}}(t)\rho_{(i,k)}^{\text{secr}}\left((1 - \mathcal{I}_{(i,k)}^{\text{conf}}(t)) + \mathcal{I}_{(i,k)}^{\text{conf}}(t)\mathcal{D}_{(i,k)}(t)\right) - \gamma_i\right)\right\},
\end{aligned}$$

where $\sum_{i=1}^{n}\sum_{k=1}^{M}\mathcal{S}_{(i,k)}^{\text{conf}}(t) + \mathcal{S}_{(i,k)}^{\text{open}}(t) = 1$. The queues in each node are updated with respect to the ACK/NAK feedback received from the base station. If $\mathcal{S}_{(i,r)}^{\text{conf}}(t) = 1$ and NAK feedback is received from the base station, $\mathcal{D}_{(i,r)}(t+1)$ is determined as follows:

$$\mathcal{D}_{(i,r)}(t+1) = \begin{cases} 1, & \text{if } Q^{\text{conf}}_{(i,r+1)}(t+1) > Q^{\text{drop}}_i(t+1) \\ & \qquad\qquad +K_i(t+1)\rho^{\text{secr}}_{(i,r)} \\ 0, & \text{otherwise.} \end{cases}$$

For all other cases, $\mathcal{D}_{(i,r)}(t+1) = 0$.

Theorem 8. *If $C_i^{conf} < \infty$ and $C_i^{open} < \infty$ for all i, and $A_i^{conf}(t) < A_i^{conf,max} < \infty$ and $A_i^{open}(t) < A_i^{open,max} < \infty$ for all i, t then for some given $\alpha > 0$ the proposed dynamic control algorithm satisfies:*

$$\sum_{i=1}^{n} U_i^{conf}(\lambda_i^{conf} - \lambda_i^{drop}) + U_i^{open}(\lambda_i^{open}) \geqslant U^* - B\alpha$$

$$\limsup_{T\to\infty} \frac{1}{T}\sum_{\tau=0}^{T-1}\sum_{i=1}^{n} \mathbb{E}\left[Q^{conf}_{(i,1)}(\tau)\right] \leqslant \frac{B + (\bar{U} - U^*)/\alpha}{\epsilon_1}$$

$$\limsup_{T\to\infty} \frac{1}{T}\sum_{\tau=0}^{T-1}\sum_{i=1}^{n} \mathbb{E}\left[Q^{open}_{(i,1)}(\tau)\right] \leqslant \frac{B + (\bar{U} - U^*)/\alpha}{\epsilon_2},$$

where

$$\lambda_i^{conf} = \liminf_{T\to\infty} \frac{1}{T}\sum_{\tau=0}^{T-1} A_i^{conf}(\tau),$$

$$\lambda_i^{drop} = \liminf_{T\to\infty} \frac{1}{T}\sum_{\tau=0}^{T-1} A_i^{drop}(\tau),$$

$$\lambda_i^{open} = \liminf_{T\to\infty} \frac{1}{T}\sum_{\tau=0}^{T-1} A_i^{open}(\tau),$$

$B, \epsilon_1, \epsilon_2 > 0$ are constants, and U^* is the optimal aggregate utility, i.e., the solution of the problem in (4.23)-(4.24) *and $\bar{U}$ is the maximum possible aggregate utility.*

Proof. Let $\mathbf{Q}(t) = (Q^{\text{conf}}_{(1,1)}(t), \ldots, Q^{\text{conf}}_{(1,M)}(t), \ldots, Q^{\text{conf}}_{(n,M)}(t),$
$Q^{\text{open}}_{(1,1)}(t), \ldots, Q^{\text{open}}_{(1,M)}(t), \ldots, Q^{\text{open}}_{(n,M)}(t),$
$Q^{\text{drop}}_1(t), \ldots, Q^{\text{drop}}_n(t), K_1(t), \ldots, K_n(t))$ be a vector of all real and virtual queues in the system. We consider a quadratic Lyapunov function of the form:

$$L(\mathbf{Q}(t)) = \frac{1}{2}\sum_{i=1}^{n}\left[\sum_{r=0}^{M}\left((Q^{\text{conf}}_{(i,r)}(t))^2 + (Q^{\text{open}}_{(i,r)}(t))^2\right) + (Q^{\text{drop}}_{i}(t))^2 + (K_i(t))^2\right].$$

Also we define the one-step expected Lyapunov drift, $\Delta(\mathbf{Q}(t))$ as: $\Delta(\mathbf{Q}(t)) = \mathbb{E}\left[L(t+1) - L(t)|\mathbf{Q}(t)\right]$.

The following lemma provides an upper bound on $\Delta(\mathbf{Q}(t))$.

Lemma 5.

$$\begin{aligned}
&\Delta(\mathbf{Q}(t)) \leq B - \sum_{i=1}^{n}\mathbb{E}\left[Q^{\mathit{conf}}_{(i,1)}(t)(\mathcal{S}^{\mathit{conf}}_{(i,1)}(t)C^{\mathit{conf}}_{i} - A^{\mathit{conf}}_{i}(t))\right]\\
&-\sum_{i=1}^{n}\sum_{r=2}^{M}\mathbb{E}\left[Q^{\mathit{conf}}_{(i,r)}(t)C^{\mathit{conf}}_{i}(\mathcal{S}^{\mathit{conf}}_{(i,r)}(t) - \mathcal{S}^{\mathit{conf}}_{(i,r-1)}\mathcal{F}^{\mathit{conf}}_{(i,r-1)}(t)(1-\mathcal{D}_{(i,r-1)}(t))\right]\\
&-\sum_{i=1}^{n}\mathbb{E}\left[Q^{\mathit{open}}_{(i,1)}(t)(\mathcal{S}^{\mathit{open}}_{(i,1)}(t)C^{\mathit{open}}_{i} - A^{\mathit{open}}_{i}(t))\right]\\
&-\sum_{i=1}^{n}\sum_{r=2}^{M}\mathbb{E}\left[Q^{\mathit{open}}_{(i,r)}(t)C^{\mathit{open}}_{i}(\mathcal{S}^{\mathit{open}}_{(i,r)}(t) - \mathcal{S}^{\mathit{open}}_{(i,r-1)}\mathcal{F}^{\mathit{open}}_{(i,r-1)})\right]\\
&-\sum_{i=1}^{n}\mathbb{E}\left[Q^{\mathit{drop}}_{i}(t)\left(\sum_{r=1}^{M}\mathcal{S}^{\mathit{conf}}_{(i,r)}(t)\mathcal{F}_{(i,r)}(t)\mathcal{D}_{(i,r)}(t)C^{\mathit{conf}}_{i} - A^{\mathit{drop}}_{i}(t)\right)\right]\\
&-\sum_{i=1}^{n}\mathbb{E}\left[K_i(t)C^{\mathit{conf}}_{i}\left(\sum_{r=1}^{M}\mathcal{S}^{\mathit{conf}}_{(i,r)}(t)\rho^{\mathit{secr}}_{(i,r)}\left((1-\mathcal{F}^{\mathit{conf}}_{(i,r)}(t)) + \mathcal{F}^{\mathit{conf}}_{(i,r)}(t)\mathcal{D}_{(i,r)}\right) - \gamma_i\right)\right]
\end{aligned}\tag{4.48}$$

where $B > 0$ is a constant. Note that all expectations are conditioned on $\mathbf{Q}(t)$.

In an interference-limited practical wireless system both the transmission power and the transmission rate is bounded. We assume that the confidential and open arrival rates are also bounded by $A^{\text{conf,max}}_{i}$, $A^{\text{open,max}}_{i}$. By following simple algebraic manipulations one can obtain a bound for the difference $(Q^{\text{conf}}_{(i,1)}(t+1))^2 - (Q^{\text{conf}}_{(i,1)}(t))^2$.

$$\begin{aligned}
&\frac{(Q^{\text{conf}}_{(i,1)}(t+1))^2 - (Q^{\text{conf}}_{(i,1)}(t))^2}{2}\\
&= \left(\left[Q^{\text{conf}}_{(i,1)}(t) - \mathcal{S}^{\text{conf}}_{(i,1)}(t)C^{\text{conf}}_{i}\right]^{+} + A^{\text{conf}}_{i}(t)\right)^2/2 - (Q^{\text{conf}}_{(i,1)}(t))^2/2\\
&\leq (C^{\text{conf}}_{i})^2/2 + (A^{\text{conf}}_{i}(t))^2/2 - Q^{\text{conf}}_{(i,1)}(t)[\mathcal{S}^{\text{conf}}_{(i,1)}(t)C^{\text{conf}}_{i} - A^{\text{conf}}_{(i,1)}(t)]\\
&\leq B_1 - Q^{\text{conf}}_{(i,1)}(t)[\mathcal{S}^{\text{conf}}_{(i,1)}(t)C^{\text{conf}}_{i} - A^{\text{conf}}_{(i,1)}(t)]\\
&\text{where } B_1 = \frac{(C^{\text{conf}}_{i})^2 + (A^{\text{conf,max}}_{i})^2}{2}
\end{aligned}$$

The bounds for other types of queues in the system can be derived in a similar fashion. The derivations of these bounds are omitted for brevity. Summing up all bounds, we obtain the result given in (6.24).

Theorem 1 suggests that a good control strategy is the one that minimizes the following:

$$\Delta^U(t) =\Delta(t) - \frac{1}{\alpha}\mathbb{E}\left[\sum_i U_i^{\text{conf}}\left(A_i^{\text{conf}}(t) - A_i^{\text{drop}}(t)\right) + U_i^{\text{open}}(A_i^{\text{open}}(t))|\mathbf{Q}(t)\right] \tag{4.49}$$

where $U_i^{\text{conf}}(t)$ and $U_i^{\text{open}}(t)$ are confidential and open utility obtained in slot t. By using (6.24), we may obtain an upper bound for (6.25).

$$\begin{aligned} &\Delta^U(t) < \text{RHS of (6.24)} \\ &-\frac{1}{\alpha}\mathbb{E}\left[\sum_i U_i^{\text{conf}}\left(A_i^{\text{conf}}(t) - A_i^{\text{drop}}(t)\right) + \sum_i U_i^{\text{open}}(A_i^{\text{open}}(t))|\mathbf{Q}(t)\right] \end{aligned} \tag{4.50}$$

Our proposed dynamic network control algorithm is designed such that it minimizes the right hand side of (6.26). If the arrival rates and the secrecy outage parameter, γ_i, are in the feasible region, it has been shown in [6] that there must exist a stationary scheduling and rate control policy that chooses the users independent of queue backlogs. Let U^* be the optimal value of the objective function of the problem (4.23)-(4.24) obtained by the aforementioned stationary policy. Also let $\lambda_i^{\text{conf}^*}$, $\lambda_i^{\text{open}*}$, $\lambda_i^{\text{drop}^*}$, be optimal traffic arrival rates, and the confidential goodput and packet dropping rates found as the solution of the same problem. Note that the expectations on the right hand side of (6.26) can be written separately due to independence of backlogs with scheduling and rate control policy. Also, since the rates are in the achievable rate region, i.e., arrival rates are strictly interior of the rate region, there must exist a stationary scheduling and rate allocation policy that is independent of queue backlogs which satisfies the following:

$$
\begin{aligned}
&C_i^{\text{conf}}\pi_{(i,1)}^{\text{conf}} \geq \lambda_i^{\text{conf}^*} + \epsilon_1 \ , \ C_i^{\text{open}}\pi_{(i,1)}^{\text{open}} \geq \lambda_i^{\text{open}^*} + \epsilon_2 \ , \\
&\mu_i^{\text{drop}} + \epsilon_3 \geq \lambda_i^{\text{drop}^*} \ , \text{ and} \\
&\quad C_i^{\text{conf}}\gamma_i \geq C_i^{\text{conf}} \sum_{r=1}^{M} \pi_{(i,r)}^{\text{conf}} \rho_{(i,r)}^{\text{secr}} \left((1-\rho_{(i,r)}^{\text{conf}}) + \rho_{(i,r)}^{\text{conf}} d_{(i,r)} \right) + \epsilon_4
\end{aligned}
\tag{4.51}
$$

Recall that our proposed policy minimizes RHS of (6.26), and thus, any other stationary policy has a higher RHS value. By using optimal stationary policy, we can obtain an upper bound for the RHS of our proposed policy. Inserting (4.51) into (6.26) and using the independence of queue backlogs with scheduling and rate policy, we obtain the following bound:

$$
\begin{aligned}
RHS <& B - \sum_i \epsilon_1 \mathbb{E}\left[Q_{(i,1)}^{\text{conf}}(t)\right] - \sum_i \epsilon_2 \mathbb{E}\left[Q_{(i,1)}^{\text{open}}(t)\right] - \sum_i \epsilon_3 \mathbb{E}\left[Q_i^{\text{drop}}(t)\right] \\
&- \sum_i \epsilon_4 \mathbb{E}\left[K_i(t)\right] - V\mathbb{E}\left[\sum_i U_i^{\text{conf}}(A_i^{\text{conf}}(t) - A_i^{\text{drop}}(t)) + U_i^{\text{open}}(A_i^{\text{open}}(t))\right] \\
<& B - \sum_i \epsilon_1 \mathbb{E}\left[Q_{(i,1)}^{\text{conf}}(t)\right] - \sum_i \epsilon_2 \mathbb{E}\left[Q_{(i,1)}^{\text{open}}(t)\right] - \sum_i \epsilon_3 \mathbb{E}\left[Q_i^{\text{drop}}(t)\right] \\
&- \sum_i \epsilon_4 \mathbb{E}\left[K_i(t)\right] - \frac{U^*}{\alpha}.
\end{aligned}
\tag{4.52}
$$

where (4.52) follows from Jensen's inequality together with concavity of $U_i^{\text{conf}}(.)$ and $U_i^{\text{open}}(.)$, and $U^* = \sum_i U_i^{\text{conf}}(\lambda_i^{\text{conf}^*} - \lambda_i^{\text{drop}^*}) + U_i^{\text{open}}(\lambda_i^{\text{open}^*})$. This is exactly in the form of Lyapunov Optimization Theorem given in Theorem 1, and hence, we can obtain bounds on the performance of the proposed policy and the sizes of queue backlogs as given in Theorem 8.

□

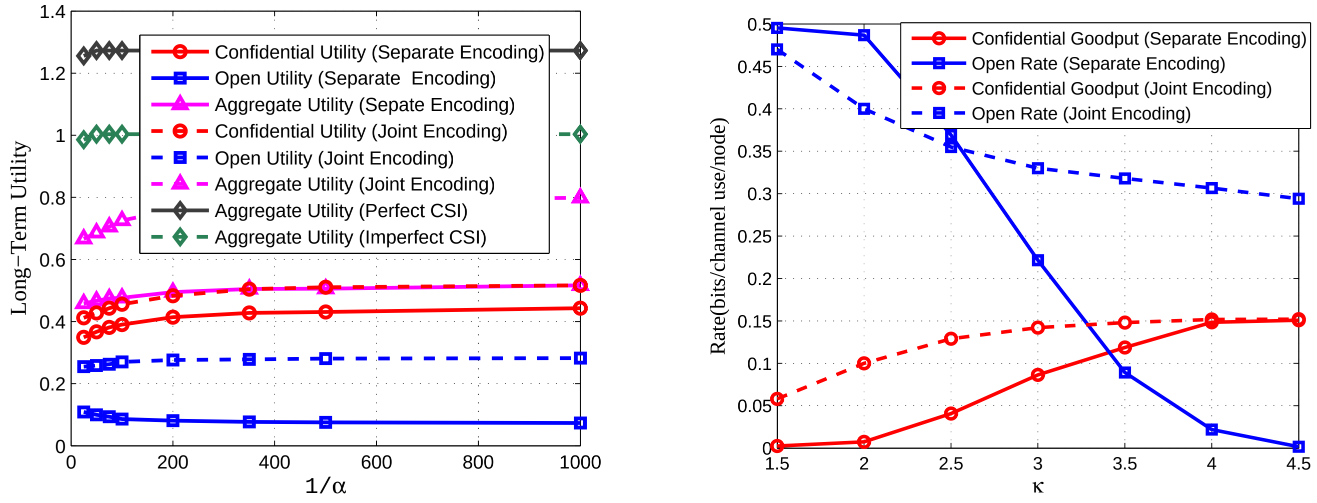
According to Theorem 8, there is a trade-off in choosing the parameter α, i. e., smaller values achieve a solution closer to the optimal, but at the same time increases the aggregate queue length. Note that, Theorem 1 gives performance bounds for the separate encoding. However, the performance bounds with joint encoding can be obtained by following similar approach done in Theorem 1.

Discussion: Our cross-layer algorithm relies on the assumption that only one user is scheduled to transmit to the base station while other users behave as passive eavesdroppers. However, the same model can be extended to a multi-user scheduling setting where a number of users can transmit at the same time slot. Multiple users accessing to the same channel can be modeled as medium access control (MAC) channel. For the MAC channel, the achievable confidential rates can be found as in [111]. The results in [111] show that the achievable rates of each transmitting node depend on the set of active nodes, i.e., the nodes which are actively transmitting in slot t. More precisely, if we allow simultaneous scheduling of multiple nodes, the possible number of schedules grow exponentially with the number of active users. Furthermore, for any given set of scheduled users, the number of rate allocations depend on the order of decoding for the associated MAC channel. Consequently, the set of possible rate allocations for each active user grows super-exponentially with the number of active users. Thus, the number of queues defined for each schedule and the complexity of the scheduling algorithm increase fairly significantly. Even if multi-user scheduling have potential to improve the network performance, one needs to take into account the increased complexity as well as the performance improvement when designing the system.

4.5 Numerical Results

In our numerical evaluations, we consider an uplink wireless cellular network consisting of four nodes and a single base station. The uplink channel between a node and the base station, and the cross-channels between pairs of nodes are modeled as iid Rayleigh fading Gaussian channels. The power gains of the channels are exponentially distributed with the probability density function (PDF) $f(h_i) = (1/\overline{h_i})e^{-h_i/\overline{h_i}}$, and the cross-channel between node i and node j has the PDF $f(h_{ij}) = (1/\overline{h_{ij}})e^{-h_{ij}/\overline{h_{ij}}}$, where $\overline{h_i}$ and $\overline{h_{ij}}$ are the average channel gains of the uplink channel and the cross-channel between node i and node j, respectively. Let $\overline{h_i}$ and $\overline{h_{ij}}$ be chosen at random, uniformly distributed in the intervals $[6, 10]$, and $[0.5, 2]$, respectively. The normalized transmit power is taken as $P = 1$ in every slot and for all nodes.

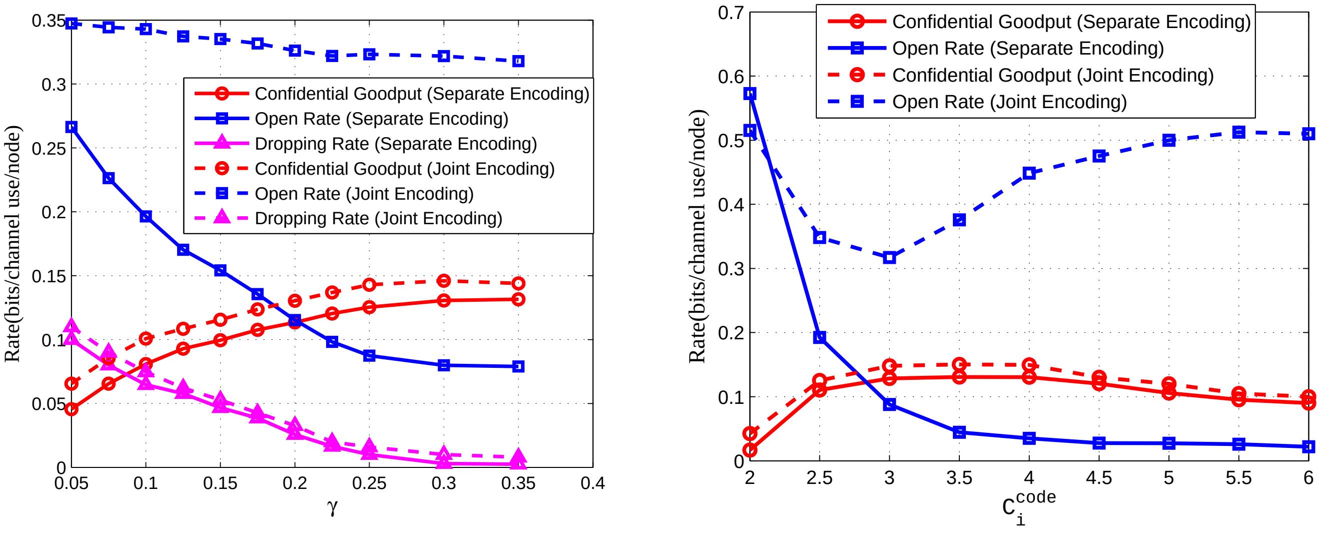
We consider logarithmic confidential and open utility functions where the con-



(a) Long-term Utility vs. $1/\alpha$

(b) confidential and open rates vs. κ

Figure 4.2: Numerical results with respect to parameters V and κ



(a) confidential and open rates vs. γ

(b) confidential and open rates vs. C_i^{code}

Figure 4.3: Numerical results with respect to parameters γ and C_i^{code}.

fidential utility is chosen to be κ times the open utility for a given rate[4]. More precisely, $U_i^{\text{open}}(x) = \frac{1}{\kappa}U_i^{\text{conf}}(x) = \log(1+x)$. We take $\kappa = 3.5$ in all experiments except for the one investigating the effect of κ. In addition, we select encoding rates as $C_i^{\text{code}} = 3$, $C_i^{\text{conf}} = 1$, and $C_i^{\text{open}} = 3$ for all i in all experiments except for the one inspecting the effect of C_i^{code}. The rates depicted in the graphs are average per node rates calculated as the total rates achieved by the network divided by the number of nodes. The unit of the plotted rates is bits/channel-use/node. We simulate both control algorithm presented in Section 4.4.2 (we refer to this policy as Algorithm with Separate Encoding) and its joint encoding version where the randomization message is selected from open bits (we refer to this policy as Algorithm with Joint Encoding).

In Fig. 6.4a, we investigate the effect of system parameter $\frac{1}{\alpha}$ in our dynamic control algorithms and illustrate the effect of different assumptions on CSI. To solve perfect and imperfect CSI cases, we use the control algorithms presented in chapter 3. In addition, we use joint encoding for both perfect and imperfect CSI cases. We take $\gamma = 0.25$ for all nodes. The first thing we noticed that, without CSI (i.e, only the distributions of channel gains are available at the transmitter), we have %40 and %20 utility loss compared to perfect and imperfect CSI cases, respectively. In addition, as expected, the total utility increases with increasing $\frac{1}{\alpha}$ and Fig. 6.4a shows that the long-term utilities for $\frac{1}{\alpha} > 200$ converges to their optimal values fairly closely verifying the results in Theorem 8 for both algorithms with separate and joint encoding. We obtain higher utility with joint encoding since one can utilize additional resources by using open bits instead of randomization bits.

For the rest of the experiments, we take $\frac{1}{\alpha} = 200$. Fig. 4.2b analyzes the effect of κ, which can also be interpreted as the ratio of utility of confidential and open transmissions taking place at the same rate. We call this ratio *confidential utility gain*. As expected, the confidential goodput increases while the open rate decreases as the confidential utility gain increases. Interestingly, for small values of confidential utility gain, the confidential rate is approximately zero for the algorithm with separate encoding. This is due to fact that confidential transmissions consume more resources,

[4] We utilize logarithmic utility function to provide proportional fairness.

and thus, open transmission is more preferable with comparable utility gains. On the other hand, for the algorithm with joint encoding, the confidential rate is non-zero even with small κ values since resources is utilizes more efficiently by encoding open bits jointly with confidential bits. On the other hand, when confidential utility gain is high, system favors confidential transmissions to maximize the total network utility for both algorithms.

Fig. 4.3a illustrates the effect of the secrecy outage probability constraint, γ. As seen from Fig. 4.3a, algorithms with separate and joint encoding exhibits similar behaviors with increasing γ except that the algorithm with joint encoding achieves higher open rate as expected. Confidential goodput increases with increasing γ. This is because for low γ values, in order to satisfy a tight secrecy outage constraint, a larger fraction of confidential messages are dropped. Meanwhile, open rate decreases with increasing γ, since there is a smaller number of transmission opportunities left for open messages with more confidential information being transmitted by the node. Starting around $\gamma = 0.25$, the secrecy outage constraint becomes inactive, since the constraint is realized with strict inequality.

We finally investigate the effect of encoding rate C_i^{code} for $\gamma = 0.25$ in Fig. 4.3b. Initially, confidential goodput increases with increasing encoding rate C_i^{code} for both control algorithms. Note that for small randomization rates, i.e., $C_i^{\text{code}} - C_i^{\text{conf}}$, other nodes can accumulate information on the confidential messages over the cross-channels. Hence, the probability of secrecy outages is high, and the transmitter drops confidential messages more frequently in order to satisfy the given secrecy outage constraint γ. As randomization rate increases, the confidential goodput increases until $C_i^{\text{code}} = 3$. Note that, any further increase in C_i^{code} results in a decrease in confidential goodput, since the base station needs to collect more information to successfully decode the message, which in turn increases the probability of decoding failures. This result clearly exhibits a *tradeoff between secrecy and reliability.* Transmitter needs to add sufficient randomization to ensure perfect secrecy, but beyond a certain point, too much randomization harms the reliability of the communication. Meanwhile, open rate decreases with increasing C_i^{code} for the algorithm with separate encoding, since, as C_i^{code} increases, nodes use more resources to transmit confidential messages, and a smaller number of transmission opportunities remain for open transmissions. Differently, for the algorithm with joint encoding, with increasing C_i^{code}, a node can jointly encode increasing number of open bits with confidential bits. After $C_i^{\text{code}} = 3$, this increase of jointly encoded open bits dominates the decrease in transmission opportunities for open transmissions, which results in increasing open rate with increasing C_i^{code} .

4.6 Chapter Summary

We considered the problem of resource allocation in wireless cellular networks where nodes have both open and confidential information to be transmitted to the base station over time-varying uplink channels. All nodes in the network are considered as internal eavesdroppers from which the confidential information needs to be protected. Unlike other works in the literature, we develop a provably-optimal scheme that handles a hybrid traffic involving both open and confidential packets, without an instantaneous CSI. Given only the statistical distribution of main and cross-channels, we have developed a reliable cross-layer dynamic control algorithm based on HARQ transmission with incremental redundancy. We believe our new technique also contributes to the field of network control [6, 112], even without confidential information transmissions, since it enables the use of Lyapunov techniques in the analysis of the schemes such as HARQ, which is based on encoding information over many blocks.

Chapter 5

Dynamic Network Control for Confidential Multi-hop Communications

In Chapter 5, we consider the problem of resource allocation and control of multihop networks in which multiple source-destination pairs communicate confidential messages, to be kept confidential from the intermediate nodes. We pose the problem as that of network utility maximization, into which confidentiality is incorporated as an additional quality of service constraint. We develop a simple, and yet provably optimal dynamic control algorithm that combines flow control, routing and end-to-end secrecy-encoding. In order to achieve confidentiality, our scheme exploits multipath diversity and temporal diversity due to channel variability. Our end-to-end dynamic encoding scheme encodes confidential messages across multiple packets, to be combined at the ultimate destination for recovery. We first develop an optimal dynamic policy for the case in which the number of blocks across which secrecy encoding is performed is asymptotically large. Next, we consider encoding across a finite number of packets, which eliminates the possibility of achieving perfect secrecy. For this case, we develop a dynamic policy to choose the encoding rates for each message, based on the instantaneous channel state information, queue states and secrecy outage requirements. By numerical analysis, we observe that the proposed scheme approaches the optimal rates asymptotically with increasing block size. Finally, we address the consequences of practical implementation issues such as infrequent queue updates and de-centralized scheduling. We demonstrate the efficacy of our policies by numerical studies under various network conditions.

5.1 Introduction

In some scenarios (e.g., tactical, financial, medical), confidentiality of communicated information between the nodes is necessary, so that data intended to (or originated from) a node is not shared by any other node. Even in scenarios in which confidentiality is not necessary, it may be dangerous to assume that nodes will always remain uncompromised. Keeping different nodes' information confidential can be viewed as a precaution to avoid a captured node from gaining access to information from other uncaptured nodes.

In this chapter, we consider wireless networks in which messages are carried between the source destination pairs cooperatively in a multi-hop fashion via intermediate nodes. In a multihop network, as data packets are transferred, intermediate nodes obtain all or part of the information through directly forwarding data packets or overhearing the transmission of nearby nodes. This poses a clear problem when transferring confidential messages. Thus, we build efficient algorithms for confidential multiuser communication over multihop wireless networks without the source-destination pairs having to share any secret key a priori. The metric we use to measure the confidentiality is the mutual information leakage rate to the relay nodes, i.e., the *equivocation rate*. We require this rate to be arbitrarily small with high probability and impose this in the resource allocation problem via an additional constraint.

To provide the basic intuition behind our approaches and how the source nodes can achieve confidentiality from the relay nodes, consider the following simple example of a diamond network given in Fig. 5.1. Let the source node have a single bit of information to be transmitted to the destination node, with *perfect secrecy* (with 0 mutual information leaked) from the relay nodes r_1 and r_2. The issue is that, the source cannot transmit this bit directly over one of the possible paths (through r_1

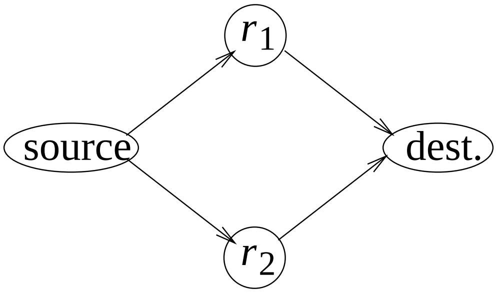


Figure 5.1: Diamond network

or r_2), since either r_1 or r_2 would obtain it, violating the confidentiality constraint. This problem can be solved by adding random noise (i.e., randomization bit) on the information bit, and sending the noise and the noise corrupted message over different paths, which can then be combined at the destination. The details of the process is as follows:

(1) Let b denote the information bit. The source generates a noise bit N at random, with $\mathbb{P}(N=0) = \mathbb{P}(N=1) = \frac{1}{2}$.

(2) Source node transmits N to relay r_1 and $b \oplus N$ to relay r_2. Then, the relay nodes forward these bits to the destination.

(3) Destination node reconstructs the original bit by a simple xor operation: $b = N \oplus (b \oplus N)$.

Note that with the information available to the relay nodes, there is no way that they can make an educated guess about the information bit, since they have *zero* mutual information: $I(b; N) = I(b; N \oplus b) = 0$. Full confidentiality is achieved here at the expense of halving of the data rate, i.e., for each information bit the source has, the network has to carry two bits to the destination. Furthermore, one can see that the existence of multiple paths from the source to the destination is crucial to achieve perfect secrecy. However, a source cannot route confidential information arbitrarily over the relay nodes. Hiding information from the other nodes can be made possible by a careful design of end-to-end coding, data routing on top of other network mechanisms, flow control and scheduling in order for an efficient resource utilization. Clearly, the example is highly simplistic and ignores many important issues, which we explicitly consider in this chapter. In particular:

(a) To achieve confidentiality, one needs to encode blocks of information across multiple packets. We develop a novel adaptive end-to-end encoding scheme, that takes certain observations from the network and chooses the appropriate code rate to maintain confidentiality for each block of data.

(b) In a multihop network, each node possibly overhears the transmission of a packet multiple times as it is transmitted over multiple hops. We take into account such accumulation of information over multiple transmissions. Thus, we need to go beyond the scenario given in Fig. 5.1, in which the paths are disjoint and each intermediate node has only one path crossing.

(c) We combine a variety of strategies developed in the context of information theoretic secrecy with basic networking mechanisms such as flow control and routing. Such a unifying framework is non-existent in the literature as it pertains to multihop information transmission. For that purpose, we model the entire problem as that of a network utility maximization, in which confidentiality is incorporated as an additional constraint and develop the associated dynamic flow control, routing, and scheduling mechanisms.

(d) We take into account wireless channel variations in our scheduling and routing policies as well as end-to-end encoding scheme for confidentiality. For that purpose, we assume that transmitters have perfect *instantaneous* channel state information (CSI) of their own channels.

Attacker model: Each attacker is capable of tapping into all the information transmitted and received by a single intermediate node. Attackers are not capable of changing the content of the information the node forwards, nor do they inject phantom messages into the network. In our model, intermediate nodes are entities, compliant with network operations as they properly execute algorithms, but the messages need to be kept confidential from them.

We address the problem in two parts. In the first part, we ignore the delay issue and consider the possibility of encoding across multiple blocks of information in order to maximize the confidential data throughput. For any given encoding rate (not necessarily optimized for the network conditions), we provide a dynamic network control scheme that achieves a utility, close to the maximum achievable utility (for that particular encoding rate), subject to *perfect* secrecy constraint, i.e., guaranteeing with probability 1 that an arbitrarily low mutual information is leaked to the intermediate nodes on the confidential message.

The problem of network control with confidential messages has been studied (as shall be discussed in the next section), in the past for the single-hop setting. The main additional challenges involved in generalizing this problem to multihop networks are dynamic end-to-end encoding and multipath routing. Standard dynamic control algorithms give control decisions in each time slot independently by assuming time-scale separation, i.e., independent transmissions of subsequent slots [6]. The confidential message is encoded across many blocks, which implies that the time-scale involved in physical-layer resource allocation cannot be decomposed from the time scales involved in network-layer resource allocation, eliminating the time-scale separation assumption of standard dynamic control algorithms. This leads to some unique technical issues that were not addressed in the existing studies on network resource allocation. In addition, the existing schemes for wireless multihop networks are not concerned with how information ought to be spatially distributed in the network [112,113]. Additional "virtual" queues need to be maintained to keep track of the leaked information to other nodes in the network to make sure that information from the source node is sufficiently spatially distributed in the network. Hence, unlike the standard multihop dynamic algorithm where the objective is to only increase end-to-end flow rates, in our problem, increasing the flow rate and keeping confidentiality of the messages appear as two conflicting objectives.

In the second part, we consider practical delay requirements for each user, which eliminates the possibility of encoding over an arbitrarily long block. Due to finite codewords, subsequent blocks associated with a given secrecy-encoded message cannot be decoupled Also, the network mechanism cannot react to an undesirably large rate of accumulation at a given node at a time scale faster than the number of blocks across which the message is encoded. For the same reason, achieving perfect secrecy for all confidential messages is not possible. Consequently, we define the notion of *secrecy outage*, and impose a probabilistic constraint on the probability that a message experiences a secrecy outage. We develop a dynamic policy to choose the encoding rates for each message, based on the instantaneous channel state information, queue states and secrecy outage requirements. We demonstrate that our proposed scheme approaches the maximum achievable rates asymptotically, with increasing block size.

Finally, we investigate some practical implementation issues. In particular, we consider the case where queue length information is exchanged among the nodes not at every block but every $K > 1$ blocks in order to reduce the control overhead. We show that our proposed algorithm still achieves asymptotic optimality but with longer average queue lengths. Another important practical limitation is the unavailability of a centralized scheduler. Hence, we propose a distributed scheduling algorithm, and investigate its performance via simulations, since the optimality can no longer be guaranteed.

5.2 System Model

We consider a multi-hop wireless network with K source-destination node pairs communicating with each other via intermediate relay nodes. Let S and D be the sets of information ingress and egress nodes in the network, respectively. There is no direct connection between the nodes in S and D, and messages from a source node to the intended destination node are relayed by intermediate nodes in the network. Let E be the set of intermediate nodes which are untrusted and/or prone to be compromised by an external attacker, i.e., E denotes the set of eavesdroppers among intermediate nodes. Note that we may have some trusted intermediate nodes in the network. Thus, the set of all intermediate nodes may not be equal to the set of eavesdroppers, E. For ease of exposition, we consider a set of logical links, L, connecting the nodes in the network, i.e., nodes i and j can communicate only if link $(i, j) \in L$.

Each source node in S aims to keep its information confidential from all other nodes in the network except the intended destination node in D. To that end, a source node precodes its message, divides it into multiple pieces, and sends separate pieces over different paths to the destination. Henceforth, none of the intermediate relay nodes in

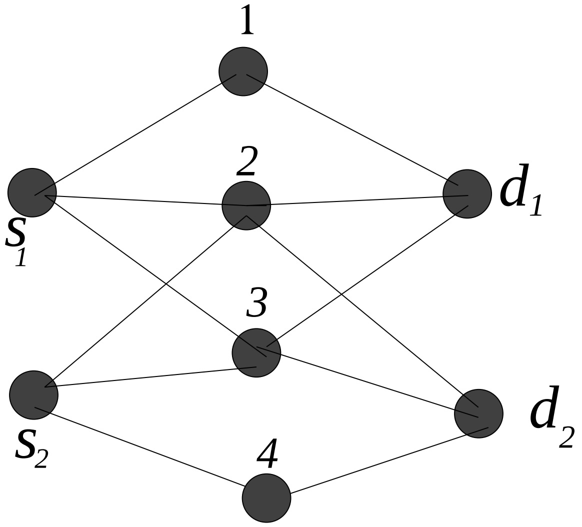


Figure 5.2: A multi-hop network.

the set of A will accumulate sufficient amount of information to decode the confidential message, even in part.

We assume every channel to be i.i.d. block fading, with a block size of N_1 channel uses (physical-layer symbols) where N_1 is sufficiently large to allow for invoking random coding arguments with arbitrarily low error probability. We denote the instantaneous achievable rate of the channel between nodes i and j in block t by $R_{ij}(t)$, where $R_{ij}(t)$ is the maximum mutual information between the output symbols of node i and input symbols of node j. We assume that the nodes are capable of obtaining perfect instantaneous CSI, i.e., node i has reach to the rates of the channels to its neighbors, $R_{ij}(t)$. Even though our results are general for all channel state distributions, in numerical evaluations, we use Gaussian channels, as will be described in Section 5.7.

We assume the wireless transceivers to operate in a half duplex fashion, i.e., a node cannot transmit and receive simultaneously. Hence, two links sharing a common ingress or egress node cannot be active simultaneously. We define a set of links that can transmit simultaneously as a *set of concurrently active links* indexed by e. Also, let E be the collection of all sets of concurrently active links. Set E depends on the assumed interference model. For example, consider a sample multi-hop network as shown in Fig. 5.2 with node-exclusive interference model. Examples of sets of concurrently active links include $\{(s_1, 1), (s_2, 4), (2, d_1)\}$, $\{(s_1, 1), (s_2, 4), (2, d_2)\}$, $\{(s_1, 2), (1, d_1), (4, d_2)\}$, and $\{(s_2, 3), (1, d_1), (4, d_2)\}$. At the beginning of every block, the scheduler chooses a particular set of concurrently active links. We use indicator variable $\mathcal{I}_e(t)$ to represent the scheduler decision, where $\mathcal{I}_e(t)$ is one if set e is scheduled for transmission in block t, and it is zero otherwise. By definition, $\sum_{e \in E} \mathcal{I}_e(t) \leq 1$ for all $t > 0$.

There are K different flows in the network, one for each source-destination node pair. Each flow in the network is identified by the index of its ingress node, and thus, the network flow problem considered in this work can be modeled as a multi-commodity flow problem. Let $\mathcal{I}_{ij}^s(t)$ be an indicator function taking a value of 1, if link (i, j) carries commodity s in block t. Hence, the total flow rate of commodity s over link (i, j) in block t is:

$$\mu_{ij}^s(t) = \begin{cases} R_{ij}(t), & \text{if } (i,j) \in e, \mathcal{I}_e(t) = 1, \mathcal{I}_{ij}^s(t) = 1 \\ 0, & \text{otherwise} \end{cases}. \tag{5.1}$$

Due to broadcast nature of wireless communications, transmissions are overheard by unintended receivers. At every transmission, overhearing neighboring nodes and the node which receives information from the active link accumulate information for each commodity s. Let k be a node overhearing a transmission of commodity s over link (i, j), i.e., there is a link $(i, k) \in L$. Then, whenever node k is not active transmitting or receiving, i.e., no link originating or terminating at node k is scheduled, it accumulates no larger than $f_k^{s,i}(t) = \min(R_{ik}(t), \max_{j \neq i} \mu_{ij}^s(t))$ bits of information over block t over link (i, j), since overhearing information cannot exceed the actual transmitted information. In Sections 5.4 and 5.5, we assume that the centralized scheduler has the reach to instantaneous channel state information, i.e., $R_{ij}(t)$ is available causally. In the subsequent section, we relax this assumption, and propose a distributed algorithm, i.e., nodes determine the scheduling decision by only using their local information.

5.3 End-to-End Confidential Encoding Rates

In this section, we describe our secrecy encoding strategy and provide an achievable confidential data rate, i.e., *secrecy rate* for a given source-destination pair, when the sequence of scheduling and routing decisions are given. We consider the system operation over N_s blocks, which corresponds to a total of $N = N_1 N_s$ channel uses. We will focus on the rate of secure data transmitted by the source node and the amount of mutual information leaked to each intermediate node by N_s blocks to analyze the secrecy rate.

Our secrecy encoding strategy is motivated by Wyner encoding [3] to provide confidentiality, which basically inserts a randomization message to the actual message to achieve equivocation. Let $C(R_s^{\mathrm{code}}, R_s^{conf}, N)$ be a Wyner code of size $2^{NR_s^{\mathrm{code}}}$ codewords, generated to convey a confidential message set $W_s \in \{1, \ldots, 2^{NR_s^{conf}}\}$. In Wyner coding, a (stochastic) encoder at source node s maps each confidential message $w_s \in W_s$ of size NR_s^{conf} bits to a codeword that has a length of NR_s^{code} bits. Thus, we refer to R_s^{conf} as the confidential information injection rate. Here, N represents the number of channel uses for the entire session, rather than the number of channel uses, source s is actively transmitting[1].

Let the vector of symbols received by node k be $\mathbf{Y}_k^s$. We define *perfect secrecy* of message W_s as the following constraint to be satisfied:

$$\frac{1}{N} I(W_s, \mathbf{Y}_k^s) \leq \varepsilon, \tag{5.2}$$

for all k for any given $\varepsilon > 0$.

In this chapter, we focus on ergodic strategies, i.e., for all $(i,j) \in L$ and $s \in S$,

$$\lim_{N_s \to \infty} \frac{1}{N_s} \sum_{t=1}^{N_s} \mu_{ij}^s(t) = \bar{\mu}_{ij}^s$$

for some $\bar{\mu}_{ij}^s \geq 0$, with probability 1. Hence, we also have for all nodes k and $s \in S$

[1] Thus, one should view the number of channel uses N in Wyner encoder notation $C(R_s^{\mathrm{code}}, R_s^{conf}, N)$ as a parameter that specifies the number of bits, NR_s^{conf}, at the input and the number of bits, NR_s^{code}, at the output of the encoder as opposed to the number of channel uses that the source transmits the message.

$$\lim_{N_s \to \infty} \frac{1}{N_s} \sum_{t=1}^{N_s} \sum_{i \neq k} f_k^{s,i}(t) = \bar{f}_k^s$$

since $R_{ij}(t)$ is i.i.d. and $\mu_{ij}^s(t)$ is ergodic. In the following theorem, we provide the rate at which the Wyner encoder ought to choose the encoding parameters for a given scheduling and routing strategy.

Theorem 9. *Given an ergodic joint scheduling and routing policy confidential information injection rate achieving perfect secrecy can be lower bounded as:*

$$R_s^{conf} \geq \sum_{(s,i) \in L} \bar{\mu}_{si}^s - \max_{\forall j \neq s,d} \bar{f}_j^s, \tag{5.3}$$

for each source-destination pair (s,d), as $N_s \to \infty$.

Next, we give the proof the theorem. Note that, the special case of Theorem 9 that holds for deterministic channels was given in [45].

Proof. The variant of Wyner encoding strategy we use is based on random coding and binning [114]. First, let us describe this strategy. To begin, node s generates $2^{N(R_s - \delta)}$ random binary sequences. Then, it assigns each random binary sequence to one of $2^{NR_s^{conf}}$ bins, so that each bin contains exactly $2^{N(R_s^{\text{code}} - R_s^{conf} - \delta)}$ binary sequences. We call the sequences associated with a bin, the *randomization sequences* of that bin. Each bin of source s is one-to-one matched with a confidential message $W_s \in \{1, \ldots, 2^{NR_s^{conf}}\}$ randomly and this selection is revealed to the destination and all nodes before the communication starts. Then, the stochastic encoder of node s selects one of the randomization sequences associated with each bin at random, independently and uniformly over all randomization sequences associated with that bin. Whenever a message is selected by node s, this particular randomization message is used. This selection is not revealed to any of the nodes nor to the destination.

Without loss of generality, we assume that the routes between source and destination have p multi-paths and each path may consist of a different number of hops. Let us denote H_k as the number of hops along kth path. Let us denote the randomization sequence of message W_s as W_s^r for source s, and denote the transmitted vector of channel symbols from node located at hop i along path k as $\mathbf{X^s_{i,k}} = [X^s_{i,k}(1), \ldots, X^s_{i,k}(N_s)]$, where $X^s_{i,k}(t)$ represents the transmitted vector of N_1 symbols in block t at hop i along path k. Note that transmitted vectors in the first hop only consists of transmission of the source s. The received signal at intermediate *relay* node located at hop i along path k is $\mathbf{Y^s_{i,k}} = [Y^s_{i,k}(1), \ldots, Y^s_{i,k}(N_s)]$, where $Y^s_{i,k}(t)$ represents the received vector of symbols at nodes of hop i along path k in block t. Also, the received signal at overhearing neighbor node j when a node at hop i along path k is transmitting, is $\mathbf{Z^{j,s}_{i,k}} = [Z^{j,s}_{i,k}(1), \ldots, Z^{j,s}_{i,k}(N_s)]$. For notational convenience, let us define $\mathbf{X^s} = [\mathbf{X^s_{1,1}}, \ldots, \mathbf{X^s_{H_1,1}}, \ldots, \mathbf{X^s_{1,p}}, \ldots, \mathbf{X^s_{H_p,p}}]$ and $\mathbf{Z^{j,s}} = [\mathbf{Z^{j,s}_{1,1}}, \ldots, \mathbf{Z^{j,s}_{H_1,1}}, \ldots, \mathbf{Z^{j,s}_{1,p}}, \ldots, \mathbf{Z^{j,s}_{H_p,p}}]$ as transmitted vector of symbols by all nodes and the total received signal by the overhearing neighbor node j, respectively.

Next, we provide the equivocation analysis for a given joint scheduling and routing decision. Note that, our objective is to find a value for R_s^{conf} for which perfect secrecy is achievable. To achieve perfect secrecy, we require $R_s^{\text{code}} - R_s^{conf}$ to be lower bounded by the conditional entropy $H(W_s|\mathbf{Z^{j,s}})$. For any given intermediate node j, the following can be written for the conditional entropy:

$$
\begin{aligned}
& H(W_s|\mathbf{Z}^{\mathbf{j,s}}) = I(W_s;\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,1}},\ldots,\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,p}}|\mathbf{Z}^{\mathbf{j,s}}) + H(W_s|\mathbf{Z}^{\mathbf{j,s}},\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,1}},\ldots,\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,p}}) \\
& \geq I(W_s;\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,1}},\ldots,\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,p}}|\mathbf{Z}^{\mathbf{j,s}}) && (5.4) \\
& = I(W_s,W_s^r;\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,1}},\ldots,\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,p}}|\mathbf{Z}^{\mathbf{j,s}}) - I(W_s^r;\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,1}},\ldots,\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,p}}|\mathbf{Z}^{\mathbf{j,s}},W_s) && (5.5) \\
& = I(W_s,W_s^r;\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,1}},\ldots,\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,p}}|\mathbf{Z}^{\mathbf{j,s}}) - H(W_s^r|\mathbf{Z}^{\mathbf{j,s}},W_s) \\
& + H(W_s^r|\mathbf{Z}^{\mathbf{j,s}},\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,1}},\ldots,\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,p}},W_s) \\
& \geq I(W_s,W_s^r;\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,1}},\ldots,\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,p}}|\mathbf{Z}^{\mathbf{j,s}}) - H(W_s^r|\mathbf{Z}^{\mathbf{j,s}},W_s) && (5.6) \\
& \geq I(W_s,W_s^r;\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,1}},\ldots,\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,p}}|\mathbf{Z}^{\mathbf{j,s}}) - N\epsilon_1 && (5.7) \\
& = I(\mathbf{X}^{\mathbf{s}};\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,1}},\ldots,\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,p}}|\mathbf{Z}^{\mathbf{j,s}}) - I(\mathbf{X}^{\mathbf{s}};\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,1}},\ldots,\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,p}}|\mathbf{Z}^{\mathbf{j,s}},W_s,W_s^r) - N\epsilon_1 && (5.8) \\
& \geq I(\mathbf{X}^{\mathbf{s}};\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,1}},\ldots,\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,p}}|\mathbf{Z}^{\mathbf{j,s}}) - N(\epsilon_1+\epsilon_2) && (5.9) \\
& = I(\mathbf{X}^{\mathbf{s}};\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,1}},\ldots,\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,p}},\mathbf{Z}^{\mathbf{j,s}}) - I(\mathbf{X}^{\mathbf{s}};\mathbf{Z}^{\mathbf{j,s}}) - N(\epsilon_1+\epsilon_2) && (5.10) \\
& \geq I(\mathbf{X}^{\mathbf{s}};\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,1}},\ldots,\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,p}}) - I(\mathbf{X}^{\mathbf{s}};\mathbf{Z}^{\mathbf{j,s}}) - N(\epsilon_1+\epsilon_2) && (5.11) \\
& \geq I(\mathbf{X}^{\mathbf{s}};\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,1}},\ldots,\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,p}}) - \sum_{k=1}^{p}\sum_{i=1}^{H_k} I(\mathbf{X}^{\mathbf{s}}_{\mathbf{i,k}};\mathbf{Z}^{\mathbf{j,s}}_{\mathbf{i,k}}) - N(\epsilon_1+\epsilon_2) && (5.12) \\
& \geq \sum_{t=1}^{N_2}\left[I(\mathbf{X}^{\mathbf{s}}(t);Y^s_{1,k}(t),\ldots,Y^s_{1,p}(t)) - \sum_{k=1}^{p}\sum_{i=1}^{H_k} I(X^s_{i,k}(t);Z^{j,s}_{i,k}(t))\right] \\
& - N(\epsilon_1+\epsilon_2) && (5.13) \\
& \geq N\left[\sum_{(s,i)\in L}\bar{\mu}^s_{si} - \bar{f}^s_j - (\epsilon_1+\epsilon_2)\right] && (5.14)
\end{aligned}
$$

with probability 1, for any positive (ϵ_1,ϵ_2) doublet, as $N_1, N_s \to \infty$. (5.5) is by the chain rule, (5.7) follows from the application of Fano's equality, (5.8) follows from the chain rule and that $(W_s, W_s^r) \leftrightarrow (\mathbf{X}^{\mathbf{s}}) \leftrightarrow (\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,1}},\ldots,\mathbf{Y}^{\mathbf{s}}_{\mathbf{H_1,1}},\ldots,\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,p}},\ldots,\mathbf{Y}^{\mathbf{s}}_{\mathbf{H_p,p}},\mathbf{Z}^{\mathbf{j,s}})$ forms a Markov chain, (5.9) holds since $I(\mathbf{X}^{\mathbf{s}};\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,1}},\ldots,\mathbf{Y}^{\mathbf{s}}_{\mathbf{1,p}}|\mathbf{Z}^{\mathbf{j,s}},W_s,W_s^r) \leq N\epsilon_2$ as the transmitted symbols sequences $\mathbf{X}^{\mathbf{s}}$ is determined w.p.1 given $(\mathbf{Z}^{\mathbf{j,s}},W_s,W_s^r)$ (with the routing history), and (5.10) follows from the chain rule. (5.12) follows from the definition of transmission across p path and multiple hops, $I(\mathbf{X}^{\mathbf{s}}_{\mathbf{i,k}};\mathbf{Y}^{\mathbf{s}}_{\mathbf{l,m}}) = 0$ when $i \neq l$ or $k \neq m$. Hence, $I(\mathbf{X}^{\mathbf{s}};\mathbf{Z}^{\mathbf{j,s}}) \leq \sum_{k=1}^{p}\sum_{i=1}^{H_k} I(\mathbf{X}^{\mathbf{s}}_{\mathbf{i,k}};\mathbf{Z}^{\mathbf{j,s}}_{\mathbf{i,k}})$. (5.13) holds since the fading processes are iid for a strategy [2] that chooses the transmitted packets injected by the source to be independent in different blocks, and finally (5.14) follows from ergodicity. Noting that (5.14) holds for any j and combining it with (5.15), completes the proof.

□

Two immediate observations one can make based on Theorem 9 are the following: First, Wyner encoder encapsulates secret information of NR_s^{conf} bits into a block of NR_s^{code}, which are injected by the source into the network. Thus, we have:

$$R_s^{\text{code}} \leq \lim_{N_s \to \infty} \frac{1}{N_s} \sum_{t=1}^{N_s} \sum_{(s,i)\in L} \mu_{si}^s(t) = \sum_{(s,i)\in L} \bar{\mu}_{si}^s. \tag{5.15}$$

Consequently, Theorem 9 implies that, for a given joint routing and scheduling strategy, rate

$$R_s^{\text{conf}} \geq \min_{j \neq s} \left\{ R_s^{\text{code}} - \bar{f}_j^s \right\}$$

can be achieved. Second, if there exists a node j through which all possible paths between a given source s and its destination are passing, then $R_s^{conf} = 0$ for that source s, since $\bar{f}_j^s$ is identical to $\sum_{(s,i)\in L} \bar{\mu}_{si}^s$ for node j. This underlines the necessity of the existence of multiple paths between a source-destination pair in order to achieve a non-zero confidential data rate.

Before finalizing this section, there are two important notes we would like to make. Firstly, the theorem provides a rate of encoding for which perfect secrecy can be achieved by an appropriate choice of secrecy encoding for a given routing and scheduling policy. It does *not* imply that an end-to-end confidential information rate of R_s^{conf} is achievable. For that, it is important to design routing and scheduling mechanisms that keeps all the queues in the network stable and at the same time deliver all the packets to the destination reliably. We will show how to achieve this in the next section. Secondly, the rate provided in Theorem 9 is achieved as the number of blocks $N_s \to \infty$. This implies that, encoding for confidentiality is done across an infinitely-long sequence of

[2] Since we are interested in an achievability scheme, it is sufficient to show that the provided rate is achievable by any particular strategy.

blocks[3]. The network mechanisms we provide in the next section achieve maximum achievable rate of confidential information, also over infinitely many blocks. Following that, we incorporate a more practical constraint of encoding over a finite number of blocks, imposing a hard limit on the decoding delay.

5.4 Multihop Network Control with Confidentiality

In the previous section, we provided the set of secrecy encoding rates that enables confidentiality of information transmitted by the source. However, we were not concerned with whether the packets reach the destination or not and the mechanisms that make it happen. In this section, our objective is to develop a stationary control policy giving joint scheduling and routing decisions that achieves end-to-end confidential transmission of information. To that end, we state a network utility maximization problem and provide a scheme that maximizes aggregate network utility while achieving perfect secrecy over infinitely many blocks. We develop our solution based on the following assumptions:

A1. We consider the large block size asymptotics, i.e., secrecy encoding is across $N_s \to \infty$ blocks.

A2. There is a centralized scheduler with the perfect knowledge of instantaneous CSI of all channels.

A3. The secrecy encoding rate is fixed: source node s uses the $C(2^{NR_s^{\text{code}}}, 2^{N\alpha_s R_s^{\text{code}}}, N)$ encoder. Thus, the confidential information injection rate is $R_s^{conf} = \alpha_s R_s^{\text{code}}$. These rates $\{R_s^{conf},\ s \in S\}$, lie in the region of rates for which perfect secrecy is achievable, as specified in Theorem 9.

Assumption A1. allows our developed mechanisms to react to an undesirably large rate of accumulation at a given node at a time scale faster than the number of blocks across which the message is encoded. Assumption A2. can be achieved by

[3] The number of blocks need to be large enough for sufficient averaging of the variations in the channels.

nodes sending their CSI to the centralized scheduler at the expense of increased control overhead. Assumption A3. states that the a priori encoding rate of the message may not maximize the confidential throughput of the source node.

Next, we develop a dynamic algorithm taking as input the queue lengths and the accumulated information at the intermediate nodes, and gives as output the scheduled node and the admitted confidential flows in to the queues of the sources.

Let $U_s(x)$ be utility obtained by source s when the confidential transmission rate is x bits/channel use. We assume that $U_s(\cdot)$ is a continuously differentiable, increasing and strictly concave function. There is an infinite backlog at the transport layer, which contains the secrecy-encoded messages. In each block, source node s determines the amount of encoded information admitted to its queue at the network level. Let $A_s(t)$ be the amount of traffic injected into the queue of source s at block t, and $x_s = \lim_{N_s \to \infty} \frac{1}{N_s} \sum_t A_s(t)$ be the long term arrival rate. Our objective is to support the traffic demand to achieve a long term confidential rate that maximizes the sum of utilities of the sources.

The arrival rate, x_s includes both the confidential and randomization bits. Hence, for the arrival rate of x_s, the confidential information rate is $\alpha_s x_s$, and source s attains a long term expected utility of $U_s(\alpha_s x_s)$. Recall that the rate of information obtained by any intermediate node should not exceed the randomization rate, $(1 - \alpha_s)x_s$, to ensure perfect secrecy. Hence, the optimization problem can be defined as follows:

$$\max_{A_s(t), \mathcal{I}_e(t), \mathcal{I}_{ij}^s(t)} \sum_{s \in S} U_s(\alpha_s x_s) \tag{5.16}$$

$$\text{s.t. } x_s \leq \sum_{\{i | (s,i) \in L\}} \bar{\mu}_{si}^s, \, \forall s \in S \tag{5.17}$$

$$\sum_{\{j | (i,j) \in L\}} \bar{\mu}_{ij}^s - \sum_{\{i | (j,i) \in L\}} \bar{\mu}_{ji}^s \geq 0, \, \forall \; i \notin S, D \tag{5.18}$$

$$\bar{f}_j^s \leq (1 - \alpha_s) x_s, \, \forall s \in S, \forall j \notin S, D, \tag{5.19}$$

Constraint (5.17) ensures the stability of the queues at the source nodes; Constraint (5.18) is the flow conservation constraint at the intermediate nodes; and Constraint (5.19) is the confidentiality constraint, which ensures that the information obtained by any of the intermediate nodes does not exceed the rate of the randomization message $(1-\alpha_s)x_s$, implying that the requirement in (5.2) is met.

To solve the optimization problem (5.16)-(5.19), we employ a cross-layer dynamic control algorithm based on the stochastic network optimization framework developed in [6]. This framework allows the solution of a long-term stochastic optimization problem without requiring the explicit characterization of the achievable rate regions[4].

Let $Q_s(t)$ denote the queue size at ingress node s. Each intermediate node keeps a separate queue $Q_i^s(t)$ for each commodity s. The queue evolution equation for each queue can be stated as follows:

$$Q_s(t+1) = \left[Q_s(t) - \sum_{\{i|(s,i)\in L\}} \mu_{si}^s(t) \right]^+ + A_s(t),$$

$$Q_i^s(t+1) = \left[Q_i^s(t) - \sum_{\{j|(i,j)\in L\}} \mu_{ij}^s(t) \right]^+ + \sum_{\{j|(j,i)\in L\}} \mu_{ji}^s(t), \ \forall i \neq S, D,$$

where $[.]^+$ denotes the projection of the term to $[0, +\infty)$. To meet Constraint (5.19), we maintain a virtual queue:

$$Z_j^s(t+1) = \left[Z_j^s(t) + \sum_{i\neq j} f_j^{s,i}(t) - (1-\alpha_s)A_s(t) \right]^+ \tag{5.20}$$

Strong stability of this queue ensures that the constraint is satisfied [6], i.e., perfect secrecy is achieved in our case. Note that to perform the update in (5.20), nodes need to have access to instantaneous CSI of all neighboring nodes.

Control Algorithm 1 (with Perfect CSI): The algorithm executes the following steps in each block t:

(1) Flow control: For some $H > 0$, each source s injects $A_s(t)$ bits into its queues, where

[4] Note that, while we know that the arrival rates lie in the region of rates for perfect secrecy (Theorem 9), we do not know the achievable end-to-end rates with confidentiality.

$$A_s(t) = \operatorname*{argmax}_{A} \left\{ HU_s(\alpha_s A) - Q_s(t)A + \sum_{j \notin S} Z_j^s(t)(1-\alpha_s)A \right\}.$$

(2) Scheduling: In each block, t, the scheduler chooses the set of links e if $\mathcal{I}_e(t) = 1$ and flow s on the link $(i,j) \in e$ if $\mathcal{I}_{ij}^s(t) = 1$, where

$$(s,e) = \operatorname*{argmax}_{s \in S, e \in E} \left\{ \sum_{(i,j) \in e} (Q_i^s(t) - Q_j^s(t))\mu_{ij}^s(t) - \sum_{j \notin S,D} \sum_{i \neq j} Z_j^s(t) f_j^{s,i}(t) \right\}$$

Optimality of Control Algorithm: Now, we show that our proposed dynamic control algorithm can achieve a performance arbitrarily close to the optimal solution while keeping the queue backlogs bounded.

Theorem 10. *If $R_{ij}(t) < \infty$ for all (i,j) links and for all t blocks, then control algorithm satisfies:*

$$\begin{aligned}
\liminf_{t \to \infty} \frac{1}{t} \sum_{\tau=0}^{t-1} \sum_{s \in S} \mathbb{E}\left[U_s(\tau)\right] &\geqslant U^* - \frac{B}{H} \\
\limsup_{t \to \infty} \frac{1}{t} \sum_{\tau=0}^{t-1} \sum_{s \in S} \mathbb{E}\left[Q_s(\tau)\right] &\leqslant \frac{B + H(\bar{U} - U^*)}{\epsilon_1} \\
\limsup_{t \to \infty} \frac{1}{t} \sum_{\tau=0}^{t-1} \sum_{s \in S} \sum_{i \notin S,D} \mathbb{E}\left[Q_i^s(\tau)\right] &\leqslant \frac{B + H(\bar{U} - U^*)}{\epsilon_2}
\end{aligned}$$

where $B, \epsilon_1, \epsilon_2$ are positive constants, U^* is the optimal aggregate utility, i.e., the solution of (5.16-5.19), and $\bar{U}$ is the maximum possible instantaneous aggregate utility.

Proof. The optimality of the algorithm can be shown by applying the Lyapunov optimization theorem [6]. We consider queue backlog vectors for commodity s as $\mathbf{Q}(t) = (Q_1(t), \ldots, Q_K(t))$, $\mathbf{Q}^s(t) = (Q_1^s(t), \ldots, Q_n^s(t))$, and $\mathbf{Z}^s(t) = (Z_1^s(t), \ldots, Z_n^s(t))$, where n is the number of intermediate relay nodes in the network. Let $L(\mathbf{Q}(t), \mathbf{Q}^s(t), \mathbf{Z}^s(t))$ be a quadratic Lyapunov function of real and virtual queue backlogs for commodity s defined as:

$$L(\mathbf{Q(t)}, \mathbf{Q^s(t)}, \mathbf{Z^s(t)}) = \frac{1}{2}\sum_{s\in S} Q_s(t) + \sum_{i=1}^{n} \left[(Q_i^s(t))^2 + (Z_i^s(t))^2\right]. \tag{5.21}$$

Also consider the one-step expected Lyapunov drift, $\Delta(t)$ for the Lyapunov function as:

$$\begin{split}\Delta(t) = \mathbb{E}\,[L(\mathbf{Q(t+1)}, \mathbf{Q^s(t+1)}, \mathbf{Z^s(t+1)}) \\ - L(\mathbf{Q(t)}, \mathbf{Q^s(t)}, \mathbf{Z^s(t)})|\mathbf{Q(t)}, \mathbf{Q^s(t)}, \mathbf{Z^s(t)}].\end{split} \tag{5.22}$$

The following lemma provides an upper bound on $\Delta(t)$.

Lemma 6.

$$\begin{aligned}\Delta(t) \le B - \sum_{s\in S}\mathbb{E}&\left[Q_s(t)\left(A_s(t) - \sum_{\{i|(s,i)\in L\}}\mu_{si}^s(t)\right)\;\middle|\; Q_s(t)\right]\\ -\sum_{s\in S}\sum_{i\notin S,D}\mathbb{E}&\left[Q_i^s(t)\left(\sum_{j|(i,j)\in L}\mu_{ij}^s(t) - \sum_{i|(i,j)\in L}\mu_{ji}^s(t)\right)\;\middle|\; Q_i^s(t)\right]\\ -\sum_{s\in S}\sum_{i\notin S,D}\mathbb{E}&\left[Z_i^s(t)\left((1-\alpha_s)A_s(t) + \sum_{j\neq i} f_i^{s,j}(t)\right)\;\middle|\; Z_i^s(t)\right],\end{aligned} \tag{5.23}$$

where $B > 0$ is a constant.

Proof. Since the maximum transmission power is finite, in any interference-limited system transmission rates are bounded. Let $\mu_{ij}^{s,\max}$ be the maximum rate over link (i,j) for commodity s, which depends on the channel states. Also assume that the arrival rate is bounded, i.e., $A_s^{\max}$ is the maximum number of bits that may arrive in a block for each source. By simple algebraic manipulations one can obtain a bound for the difference $(Q_s(t+1))^2 - (Q_s(t))^2$ and also for other queues to obtain the result in (6.24).

Applying the above lemma, we can complete our proof. In particular, Lyapunov Optimization Theorem [6] suggests that a good control strategy is the one that minimizes the following:

$$\Delta^U(t) = \Delta(t) - H\mathbb{E}\left[\sum_s (U_s(t))\,|\,(\mathbf{Q(t)}, \mathbf{Q^s(t)}, \mathbf{Z^s(t)})\right]. \tag{5.24}$$

By using (6.24) in the lemma, we obtain an upper bound for (6.25), as follows:

$$\begin{aligned}
\Delta^U(k) < B - &\sum_{s\in S} \mathbb{E}\left[Q_s(t) \left(A_s(t) - \sum_{\{i|(s,i)\in L\}} \mu^s_{si}(t) \right) \middle| \; Q^s_i(t) \right] \\
- &\sum_{s\in S} \sum_{i\notin S,D} \mathbb{E}\left[Q^s_i(t) \left(\sum_{j|(i,j)\in L} \mu^s_{ij}(t) - \sum_{i|(i,j)\in L} \mu^s_{ji}(t) \right) \middle| \; Q^s_i(t) \right] \\
- &\sum_{s\in S} \sum_{i\notin S,D} \mathbb{E}\left[Z^s_i(t) \; ((1-\alpha_s)A_s(t) + \sum_{j\neq i} f^{s,j}_i(t)) \;\middle|\; Z^s_i(t) \right] \\
- &H\mathbb{E}\left[\sum_s U_s((1-\alpha_s)A_s(t)) \right] \qquad (5.25)
\end{aligned}$$

It is easy to observe that our proposed dynamic network control algorithm minimizes the right hand side of (6.26) by rearranging the terms in (6.26).

If the arrival rates and the given encoding rate, α_s, are in the feasible region, it has been shown in [6] that there must exist a stationary scheduling and rate control policy that chooses the users and their transmission rates independent of queue backlogs and only with respect to the channel statistics. In particular, the optimal stationary policy can be found as the solution of a deterministic policy if the channel statistics are known a priori.

Let U^* be the optimal value of the objective function of the problem (5.16-5.19) obtained by the aforementioned stationary policy. Also let ${\lambda_s}^*$ be optimal traffic arrival rates found as the solution of the same problem. In particular, the optimal input rate ${\lambda_s}^*$ could in principle be achieved by the simple backlog-independent admission control algorithm of new arrival $A_s(t)$ for a given commodity s in block t independently with probability $\zeta_s = {\lambda_s}^*/\lambda_s$.

Also, since ${\lambda_s}^*$ is in the achievable rate region, i.e., arrival rates are strictly interior of the rate region, there must exist a stationary scheduling and rate allocation policy that is independent of queue backlogs and satisfies the following:

$$\sum_{\{i|(s,i)\in L\}} \bar{\mu}_{si}^{s} \geq \lambda_s{}^{*} + \epsilon_1 \tag{5.26}$$

$$\sum_{j|(i,j)\in L} \bar{\mu}_{ij}^{s} \geq \sum_{i|(i,j)\in L} \bar{\mu}_{ji}^{s} + \epsilon_2 \tag{5.27}$$

$$\bar{f}_i^{s} \leq (1-\alpha_s)\lambda_s{}^{*} + \epsilon_3. \tag{5.28}$$

Note that as we consider stationary and ergodic policies, long-term averages in (6.27)-(6.29) correspond to expectations of the same variables as in (6.26). Clearly, any stationary policy should satisfy (6.26). Recall that our proposed policy minimizes the right hand side (RHS) of (6.26), and hence, any other stationary policy (including the optimal policy) has a higher RHS value than the one attained by our policy. In particular, the stationary policy that satisfies (6.27)-(6.29), and implements aforementioned probabilistic admission control can be used to obtain an upper bound for the RHS of our proposed policy. Inserting (6.27)-(6.29) into (6.26), we obtain the following upper bound for our policy:

$$\begin{aligned} RHS < B - \sum_{s\in S} \epsilon_1 \mathbb{E}[Q_s(t)] - \sum_{s\in S}\sum_{i\notin S,D} \epsilon_2 \mathbb{E}[Q_i^s(t)] \\ - \sum_{s\in S}\sum_{i\notin S,D} \epsilon_3 \mathbb{E}[Z_i^s(t)] - HU^{*}. \end{aligned}$$

This is exactly in the form of Lyapunov Optimization Theorem given in [6], and hence, we can obtain bounds on the performance of the proposed policy and the sizes of queue backlogs as given in Theorem 1.

□

This theorem shows that it is possible to get arbitrarily close to the optimal utility by choosing H sufficiently large at the expense of proportionally increased average queue sizes. However, since all queues remain bounded, the destination is receiving packets at the rate as they are injected at the source as $N_s \to \infty$.

To finalize this section, we note that, while we count on the secrecy encoding rates to lie in the region specified in Theorem 9, we do not claim any rate in that region is satisfied by our scheme. In fact, we do not specify the set of achievable rates for our problem. However, we show that, our scheme achieves the maximum achievable region of end-to-end rates. The main significance of the algorithm presented in this section is that, it can be considered as a benchmark against which all other algorithms developed with one or more of the assumptions A1.-A3. relaxed can be compared.

5.5 Confidential Multihop Network Control with a Finite Decoding Delay Constraint

In Section 5.4, we propose a dynamic control algorithm associated with end-to-end secrecy encoding, where messages are encoded over infinitely many blocks. Hence, the decoding delay of confidential message may be infinitely long. In this section, we consider a more practical case by removing Assumption A1., i.e., there is a hard constraint on the number of blocks a given confidential message is encoded, $N_s < \infty$. The entire data including actual confidential bits and the randomization bits sent by source s is $N_s R_s^{\text{code}}$, where R_s^{code} is defined as before. We assume that the length of the message $N_s R_s^{\text{code}}$ is determined a priori based on the required end-to-end delay between the source and destination nodes. We also remove Assumption A3., where end-to-end confidential data rate may not be in general equal to R_s^{conf}.

Unlike the infinite-block case, since a message is encoded across a finite number of blocks, subsequent packets associated with a given secrecy-encoded message cannot be decoupled. Therefore, achieving perfect secrecy for all messages is not possible. Hence, we define the notion of *secrecy outage*. We say that a secrecy outage event occurs, when the confidential message is intercepted by any intermediate node, i.e., the perfect secrecy constraint (5.2) is violated. Secrecy outages can be completely avoided in the infinite-block scenario, since the network mechanisms can react to an undesirably large rate of accumulation at a given node at a time scale faster than the number of blocks across which the message is encoded. However, here, the reaction time may be too slow and the accumulated information at a node may already exceed the threshold for perfect secrecy. Consequently, rather than perfect secrecy, we impose a constraint on the event that a message experiences a *secrecy outage.* In particular, we assume that, each source has the knowledge[5] of the amount of accumulated information at the intermediate nodes for its messages, so it can identify (but not necessarily avoid) the occurrence of the event of secrecy outage. On the other hand, unlike the infinite-block case, each of the messages encoded across finite number of blocks, k, can be encoded with a different confidential rate $R_s^{k,priv}$, determined based on the history of prior messages experiencing secrecy outages. Thus, a scheme can adaptively vary its confidential data rate to improve the performance.

As in Section 5.4, our objective is to maximize the aggregate long-term confidential utility of K source-destination pairs. Let x_s^{conf} be the average rate of confidential messages injected into the queue of the source node s, $p_s^{out}(R_s^{k,priv})$ be the long-term average of secrecy outages of the message k of source node s when encoded with confidentiality rate $R_s^{k,priv}$, and γ_s be the maximum allowable portion of actual confidential bits experiencing secrecy outage. We consider the solution of the following optimization problem:

$$\max_{R_s^{k,priv},\mathcal{I}_e(t),\mathcal{I}_{ji}^s(t)} \sum_{s\in S} U(x_s^{\text{conf}}) \tag{5.29}$$

$$\text{s. t. } x_s^{\text{conf}} \leq \bar{R}_s^{priv} \tag{5.30}$$

$$\bar{R}_s^{out} \leq \gamma_s \bar{R}_s^{priv} \tag{5.31}$$

$$\sum_{\{j|(i,j)\in L\}} \bar{\mu}_{ij}^s - \sum_{\{i|(i,j)\in L\}} \bar{\mu}_{ij}^s \geq 0, \tag{5.32}$$

where $\bar{R}_s^{priv} = \lim_{K\to\infty} \frac{1}{K}\sum_{k=1}^{K} R_s^{k,priv}$ and $\bar{R}_s^{out} = \lim_{K\to\infty} \frac{1}{K}\sum_{k=1}^{K} R_s^{k,priv} p_s^{out}(R_s^{k,priv})$.

Constraint (5.30) ensures that the long-term service rate is larger than the long-term arrival rate; Constraint (5.31) ensures that the portion of the actual confidential bits experiencing secrecy outage is lower than γ_s; and Constraint (5.32) is for the flow conservation at intermediate nodes.

[5] In the next section, we address this assumption and investigate the possibility of infrequent update of the amount of accummulated information in the intermediate nodes.

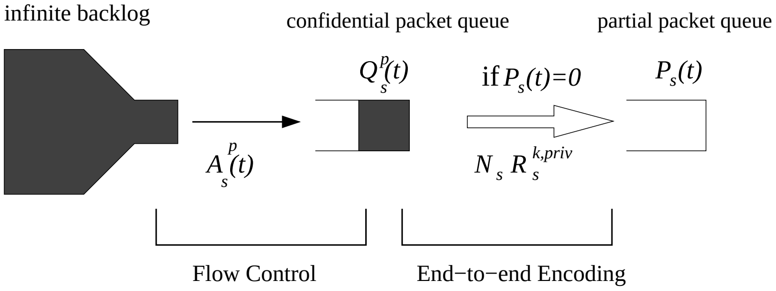


Figure 5.3: Queues in a source node used for Control Algorithm 3.

Once again, we employ a cross-layer dynamic control algorithm based on the stochastic network optimization framework to solve the optimization problem (5.29-5.32). Clearly, in this problem, since the message is encoded across a finite number of blocks, a control decision given in a time slot depends on the decisions of the same message given in the subsequent time slots. Thus, the optimality of dynamic control algorithms cannot be claimed. In the following, we develop a sub-optimal solution which performs scheduling by treating the messages as if they are infinite length messages, but at the same time chooses confidential encoding rates of individual messages by keeping account of information experiencing secrecy outages.

The source node s has two separate queues operating at two different time scales as illustrated in Fig. 5.3. The first queue stores the confidential information that has been neither secrecy-encoded nor transmitted in previous blocks. Let $Q_s^{\text{conf}}(t)$ denote the length of the confidential information queue at block t. In every block t, $A_s^{\text{conf}}(t)$ confidential bits are admitted into the queue, where x_s^{conf} is the long term average rate of admitted confidential bits. Departures from this queue occur only when a new secrecy-encoded message is created. Let $k_s(t)$ be the number of secrecy-encoded messages created by block t. The $k_s(t)$th confidential message is encoded with rate $R_s^{k_s(t),priv}$, so the actual confidential bits in the message is $N_s R_s^{k_s(t),priv}$ whereas the complete length of the encoded message including the randomization bits is always $N_s R_s^{\text{code}}$ for every secrecy-encoded message. Once a new confidential message is created, it is admitted to the second queue, which stores the bits of partially transmitted confidential message $k_s(t)$. Let $P_s(t)$ denote the size of this partial message queue at block t. The departures from this queue may occur at any block t depending on the outcome of the scheduling and routing decisions. A new secrecy-encoded message is admitted to the queue only when the partial message queue has emptied, i.e., $P_s(t) = 0$. Hence, $k_s(t+1) = k_s(t)+1$, if $P_s(t) = 0$. The evolution of the states of the queues at each source s can be stated as:

$$Q_s^{\text{conf}}(t+1) = \begin{cases} \left[Q_s^{\text{conf}}(t) - N_s R_s^{k_s(t+1),priv}\right]^+ + A_s^{\text{conf}}(t) & \text{if } P_s(t) = 0, \\ Q_s^{\text{conf}}(t) + A_s^{\text{conf}}(t), & \text{otherwise} \end{cases},$$

$$P_s(t+1) = \begin{cases} N_s R_s^{\text{code}} & \text{if } P_s(t) = 0 \\ \left[P_s(t) - \sum_{i|(s,i)\in L} \mu_{si}^s(t)\right]^+ & \text{otherwise} \end{cases}.$$

At every intermediate node, there is a queue for each source s. Let $Q_i^s(t)$ denote the size of the queue at intermediate node j for source s. Then, we have

$$Q_i^s(t+1) = \left[Q_i^s(t) - \sum_{j|(i,j)\in L} \mu_{ij}^s(t)\right]^+ + \sum_{j|(j,i)\in L} \mu_{ji}^s(t).$$

In order to determine the occurrence of secrecy outages, each source keeps track of the accumulated information at each intermediate node (we address this issue in the next section). Let $Z_i^s(t)$ be the number of bits that must be accumulated by intermediate node i to decode the $k_s(t)$th confidential message of source s at block t. Note that a secrecy outage occurs in $k_s(t)$th message, if $Z_i^s(t) = 0$ for any intermediate node i.

$$Z_i^s(t+1) = \begin{cases} (R_s^{\text{code}} - R_s^{k_s(t+1),priv})N_s & \text{if } P_s(t) = 0 \\ \left[Z_i^s(t) - \sum_{j\neq i} f_i^{s,j}(t)\right]^+ & \text{otherwise} \end{cases}.$$

The constraint in (5.31) can be represented by a virtual queue, which keeps account of confidential information experiencing secrecy outages. Hence, there is only an arrival of $R_s^{k,priv}$ if kth message has undergone secrecy outage.

$$V_s^{k+1} = \begin{cases} \left[V_s^k + R_s^{k,priv} - \gamma_s R_s^{k,priv}\right]^+ & \text{if outage in } k\text{th message} \\ \left[V_s^k - \gamma_s R_s^{k,priv}\right]^+ & \text{if no outage in } k\text{th message} \end{cases}.$$

Control Algorithm 2 (with Finite Encoding Block):

For each source s:

(1) End-to-end Encoding: At every generation of new confidential message, i.e., $P_s(t) = 0$, let $k_s(t+1) = k_s(t)+1$, and determine end-to-end confidential encoding rate:

$$R_s^{k_s(t+1),priv} = \underset{r}{\operatorname{argmax}} \left\{Q_s^{\text{conf}}(t) - V_s^{k_s(t)} \left(rp_s^{out}(r) - r\gamma_s\right)\right\}$$

(2) Flow control: At each block t, for some $H > 0$, each source s injects $A_s^{\text{conf}}(t)$ confidential bits into its queues

$$A_s^{\text{conf}}(t) = \underset{a}{\operatorname{argmax}} \left\{HU_s(a) - Q_s^{\text{conf}}(t)a\right\}.$$

(3) Scheduling: At each block, t , the scheduler chooses the set of links e if $\mathcal{I}_e(t) = 1$ and flow s on the link $(i,j) \in e$ if $\mathcal{I}_{ij}^s(t) = 1$, where

$$(s,e) = \underset{s\in S, e\in E}{\operatorname{argmax}} \left\{ \sum_{(s,i)\in e} \left(\frac{R_s^{\text{code}}}{R_s^{k_s(t),priv}} Q_s^{\text{conf}}(t) + P_s(t) - Q_i^s(t) \right) \mu_{si}^s(t) \right.$$
$$\left. + \sum_{(i,j)\in e} \left(Q_i^s(t) - Q_j^s(t)\right) \mu_{ij}^s(t) - \sum_{j\notin S,D} \sum_{i\neq j} Z_j^s(t) f_j^{s,i}(t) \right\}$$

and $Q_s^{\text{conf}}(t)$ is multiplied by $R_s^{\text{code}}/R_s^{k_s(t),priv}$ in order to normalize it to the size of other queues in the network.

Note that the long-term average of secrecy outages $p_s^{out}(R)$ can only be calculated if the scheduling decisions are known a priori. Since this is not the case, we use an estimate of secrecy outage probability as discussed in Section 5.7.

Finally, we would like to re-iterate that, Control Algorithm 2 does not guarantee obtaining the optimal solution of (5.29) - (5.32) due to the dependance of decisions between subsequent blocks. We verify by extensive numerical analysis that its performance is still close to the optimal in a variety of scenarios.

5.6 Reducing the Overhead and Distributed Implementation

The algorithms presented in the Section 5.4 and 5.5 solve constrained optimization problems in a centralized fashion. The centralized algorithms provide an upper bound on the network performance, which can be used a benchmark to evaluate the performance of distributed algorithms. In this section, we design algorithms relaxing the assumptions necessary for Control Algorithm 1, where the instantaneous queue length information is not available and/or a centralized scheduler is absent in the network. Note that the flow control portions of the algorithms provided in the previous sections were already distributed, i.e, each node decides its admitted flow by only local information. Thus, they remain the same as given in Section 5.4, in the rest of the sequel.

5.6.1 Infrequent Queue Length Updates

In this section, we consider the setup described in Section 5.4, and relax the assumption of the availability of the queue state information of each node at every point in time. Indeed, scheduling requires a significant overhead due to control traffic carrying the queue length information across the entire network. To reduce this overhead, we consider transmission of queue length information not in every slot, but once every K slots. Let $\hat{Q}_s(t)$ and $\hat{Q}_i^s(t)$ denote the estimates of the queue lengths at source s and at node i for commodity s, respectively, at time t. Furthermore, let $\hat{Z}_i^s(t)$ denote the estimate of the virtual queue at node i used for the accumulated information about commodity s. In particular, these estimates are the last updates of the queue lengths, prior to time t, received by the scheduler. Further, suppose that at each time slot, the scheduler gives the routing decision according to the solution of the following equation:

$$(s,e) = \operatorname*{argmax}_{s\in S, e\in E} \left\{ \sum_{(i,j)\in e} (\hat{Q}_i^s(t) - \hat{Q}_j^s(t))\mu_{ij}^s(t) - \sum_{j\notin S,D} \sum_{i\neq j} \hat{Z}_j^s(t) f_j^{s,i}(t) \right\}.$$

Next, we show that the performance attained by a system where queue lengths are updated infrequently is again arbitrarily close to the optimal solution.

Theorem 11. *If $R_{ij}(t) < \infty$ for all (i,j) links and for all t blocks, then control algorithm satisfies:*

$$\begin{aligned}
\liminf_{t\to\infty} \frac{1}{t} \sum_{\tau=0}^{t-1} \sum_{s\in S} \mathbb{E}\left[U_s(\tau)\right] &\geqslant U^* - \frac{B + B'(K-1)}{H} \\
\limsup_{t\to\infty} \frac{1}{t} \sum_{\tau=0}^{t-1} \sum_{s\in S} \mathbb{E}\left[Q_s(\tau)\right] &\leqslant \frac{B + B'(K-1) + H(\bar{U} - U^*)}{\epsilon_1'} \\
\limsup_{t\to\infty} \frac{1}{t} \sum_{\tau=0}^{t-1} \sum_{s\in S} \sum_{i\notin S,D} \mathbb{E}\left[Q_i^s(\tau)\right] &\leqslant \frac{B + B'(K-1) + H(\bar{U} - U^*)}{\epsilon_2'}
\end{aligned}$$

where $B, B', \epsilon_1', \epsilon_2'$ are positive constants, U^* is the optimal aggregate utility, i.e., the solution of (5.16-5.19), and $\bar{U}$ is the maximum possible instantaneous aggregate utility.

Proof. For the proof, we follow the similar approach used in the proof of theorem 10, i.e., applying the Lyapunov optimization theorem. However, here, we use K-slot Lyapunov drift instead of the one-step expected Lyapunov drift. We again use quadratic Lyapunov function as in (6.22). Assume that nodes transmit its exact queue values in every K slots, i.e., in $\ldots, t-K, t, t+K, \ldots$. Thus, $\hat{Q}(t) = \hat{Q}(t+\tau)$ for $0 \leq \tau \leq K$. Consider the K-step expected Lyapunov drift, $\hat{\Delta}_K(t)$ as:

$$\begin{aligned}
\hat{\Delta}_K(t) = \mathbb{E}\Big[& L(\mathbf{\hat{Q}(t+K)}, \mathbf{\hat{Q}^s(t+K)}, \mathbf{\hat{Z}^s(t+K)}) \\
& - L(\mathbf{\hat{Q}(t)}, \mathbf{\hat{Q}^s(t)}, \mathbf{\hat{Z}^s(t)}) | \mathbf{\hat{Q}(t)}, \mathbf{\hat{Q}^s(t)}, \mathbf{\hat{Z}^s(t)}\Big]. \quad (5.33)
\end{aligned}$$

By using the result in Lemma 9. We bound K-step Lyapunov drift as:

$$\hat{\Delta}_K(t) \leq -\sum_{\tau=1}^{K}\sum_{s\in S}\mathbb{E}\left[\hat{Q}_s(t)\left(A_s(t+\tau) - \sum_{\{i|(s,i)\in L\}}\mu_{si}^s(t+\tau)\right)\middle|\ \hat{Q}_s(t)\right]$$
$$-\sum_{\tau=1}^{K}\sum_{s\in S}\sum_{i\notin S,D}\mathbb{E}\left[\hat{Q}_i^s(t)\left(\sum_{j|(i,j)\in L}\mu_{ij}^s(t+\tau) - \sum_{j|(j,i)\in L}\mu_{ji+\tau}^s(t)\right)\middle|\ Q_i^s(t)\right]$$
$$-\sum_{\tau=1}^{K}\sum_{s\in S}\sum_{i\notin S,D}\mathbb{E}\left[\hat{Z}_i^s(t)\left((1-\alpha_s)A_s(t+\tau) + \sum_{j\neq i}f_i^{s,j}(t+\tau)\right)\middle|\ \hat{Z}_i^s(t)\right] + BK, \qquad (5.34)$$

Note that the difference of queue sizes in slot t and queue sizes in slot $t+\tau$ is bounded by $\tau\left(\max(A_s^{\max}, \mu_{ij}^{s,\max})\right)$, i.e., $\hat{Q}_s(t) - Q_s(t+\tau) \leq \tau\left(\max(A_s^{\max}, \mu_{ij}^{s,\max})\right)$. Then we can rewrite (5.34) as:

$$\hat{\Delta}_K(t) \leq -\sum_{\tau=1}^{K}\sum_{s\in S}\mathbb{E}\left[Q_s(t+\tau)\left(A_s(t+\tau) - \sum_{\{i|(s,i)\in L\}}\mu_{si}^s(t+\tau)\right)\middle|\ \hat{Q}_s(t)\right]$$
$$-\sum_{\tau=1}^{K}\sum_{s\in S}\sum_{i\notin S,D}\mathbb{E}\left[Q_i^s(t+\tau)\left(\sum_{j|(i,j)\in L}\mu_{ij}^s(t+\tau) - \sum_{j|(j,i)\in L}\mu_{ji+\tau}^s(t)\right)\middle|\ Q_i^s(t)\right]$$
$$-\sum_{\tau=1}^{K}\sum_{s\in S}\sum_{i\notin S,D}\mathbb{E}\left[Z_i^s(t+\tau)\left((1-\alpha_s)A_s(t+\tau) + \sum_{j\neq i}f_i^{s,j}(t+\tau)\right)\middle|\ Z_i^s(t)\right]$$
$$+ BK + B'K(K-1), \qquad (5.35)$$

where $B' = \frac{\max((A_s^{max})^2, (\mu_{ij}^{s,max})^2)}{2}$. In (5.35), we obtain a bound for the K-step Lyapunov drift. We define one-step expected Lyapunov drift as:

$$\hat{\Delta}(t) = \mathbb{E}\Big[L(\mathbf{\hat{Q}(t+1)}, \mathbf{\hat{Q}^s(t+1)}, \mathbf{\hat{Z}^s(t+1)})$$
$$- L(\mathbf{\hat{Q}(t)}, \mathbf{\hat{Q}^s(t)}, \mathbf{\hat{Z}^s(t)})|\mathbf{\hat{Q}(t)}, \mathbf{\hat{Q}^s(t)}, \mathbf{\hat{Z}^s(t)}\Big]. \qquad (5.36)$$

Then, we obtain one-step Lyapunov drift, $\hat{\Delta}(t)$ from (5.35) as:

$$
\begin{aligned}
\hat{\Delta}(t) \leq B + B'(K-1) - \sum_{s\in S} \mathbb{E}\left[Q_s(t) \left(A_s(t) - \sum_{\{i|(s,i)\in L\}} \mu_{si}^s(t) \right) \middle| \hat{Q}_s(t) \right] \\
- \sum_{s\in S} \sum_{i\notin S,D} \mathbb{E}\left[Q_i^s(t) \left(\sum_{j|(i,j)\in L} \mu_{ij}^s(t) - \sum_{j|(j,i)\in L} \mu_{ji}^s(t) \right) \middle| Q_i^s(t) \right] \\
- \sum_{s\in S} \sum_{i\notin S,D} \mathbb{E}\left[Z_i^s(t) \left((1-\alpha_s)A_s(t) + \sum_{j\neq i} f_i^{s,j}(t) \right) \middle| Z_i^s(t) \right] \\
= B'(K-1) + \text{RHS of } (26) \qquad (5.37)
\end{aligned}
$$

After obtaining bound on the $\hat{\Delta}(t)$, we can obtain bounds on the performance of the proposed policy and the sizes of queue backlogs as given in Theorem 11 by following the same lines in the proof of theorem 10. □

This theorem shows that it is still possible to get arbitrarily close to the optimal utility by choosing H sufficiently large. However, the lack of availability of timely queue state information negatively affects the performance bounds. In particular, for a given value of H, the bound on the achieved utility decreases by a factor, proportional to K. Likewise, the upper bounds on the queue sizes increase by a factor, proportional to K. There may be alternative ways to update the queue length information instead of a periodic update. For example, the queue length information for each queue can be updated whenever the absolute value of the difference between the current length and the last update exceeds some threshold. Along the lines of the proof of Theorem 11, one can again show that this algorithm is arbitrarily close to optimality. In addition, it was shown in [115] that this update mechanism reduces the average queue sizes as compared to the periodic sampling.

5.6.2 Distributed Implementation

In the previous section, we dealt with the issue of reducing the overhead of the centralized scheduling. Here, we seek a distributed algorithm where each node participates in scheduling using only local information: We assume that the nodes have information of the instantaneous CSI only between themselves and their neighbors, and only of the queue lengths of their neighbors.

Algorithm 1: Distributed Scheduling Algorithm

```
Each node $i$ carries out the following steps over each block $t$:
    1) Calculate weight $W_{ij}^s(t) = (Q_i^s(t) - Q_j^s(t))R_{ij}(t) - \sum_{k \neq S,D} Z_k^s(t) R_{ik}(t)$ for each link pair $(i, j)$. Ties are broken randomly.
    2) Find node $j^*$ such that $W_{ij^*}^s(t)$ is maximized over all links $(i, j)$ with free neighbors $j$. If having received a matching request from $j^*$, then link $(i, j)$ is a matched link. Node $i$ sends a matched reply to $j^*$ and a drop message to all other free neighbors. Otherwise, node $i$ sends a matching request to node $j^*$.
    3) Upon receiving a matching request from neighbor $j$, if $j = j^*$, then link $(i, j)$ is a matched link. Node $i$ sends a matched reply to node $j$ and a drop message to all other free neighbors. If $j \neq j^*$, node $i$ just stores the received message.
    4) Upon receiving a matched reply from neighbor $j$, node $i$ knows link $(i, j)$ is a matched link, and sends a drop message to all other free neighbors.
    5) Upon receiving a drop message from neighbor $j$, node $i$ knows that $j$ is in a matched link, and excludes $j$ from its set of free neighbors.
    6) If node $i$ is in a matched link or has no free neighbors, no further action is taken. Otherwise, it repeats steps 2) through 5).
    7) Matched links are allowed to transmit, i.e., if link $(i, j)$ is a matched link, node $i$ transmits data to node $j$.
```

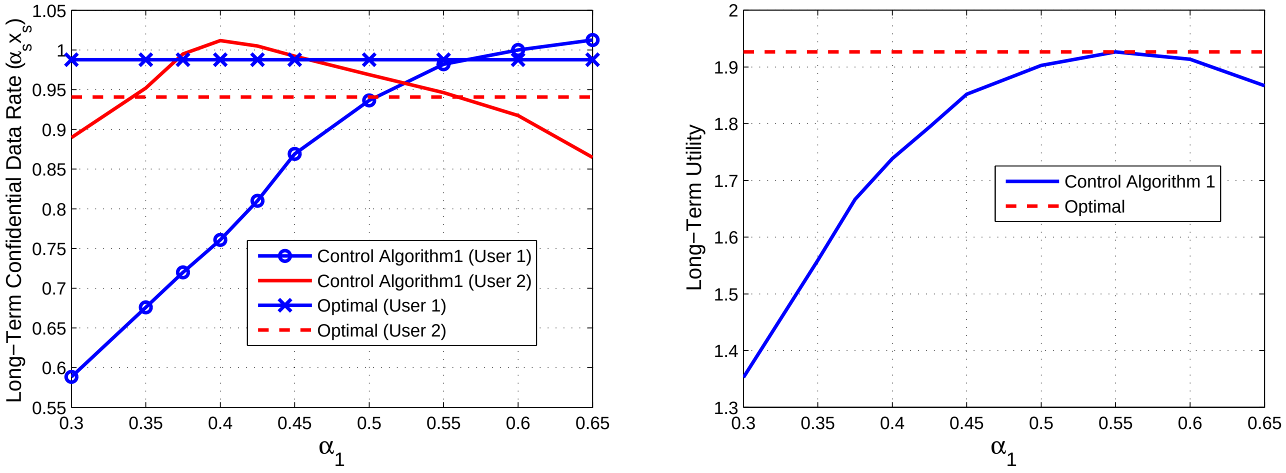
The scheduling problem of the control algorithms designed in the previous sections can be reduced to a maximum weighted matching problem[6], which is polynomial time solvable, but requires a centralized implementation. Each node needs to notify the central node of its weight and local connectivity information such that the central node can reconstruct the network topology. A few distributed approximation algorithms exist for the maximum weighted matching problem, e.g., [116] and [117]. Here, we make use of the distributed scheduling algorithm presented in [117], where the maximum weighted matching is obtained sequentially. Let a link that has been chosen to be in the matching be called a matched link. Nodes that are not related to any matched link are called free. A matching request is transmitted to enquire the possibility to choose the link with a neighbor as a matched link. A matched reply is sent to confirm that the link with a

[6] A matching in a graph is a subset of links, no two of which share a common node. The weight of a matching is the total weight of all its links. A maximum weighted matching in a graph is a matching whose weight is maximized over all matchings of the graph.

neighbor is matched. A node sends a drop message to inform its neighbors that it is not free anymore. Algorithm 1 gives the details of the distributed scheduling algorithm.

At the beginning of each slot, node i does not have information about which of its neighbors will transmit in that slot. Thus, it considers as leaked information to all its free neighbors while computing weights of its links, even if some of those neighbors may transmit in the following iteration[7]. However, when all matched links are set, node i overhears the surrounding transmissions, and updates the virtual queues related to the overheard information of its neighbors, i.e., $Z_j^s(t)$. In Section 5.7, we demonstrate that the proposed distributed scheduling algorithm results in a small degradation in the overall performance.

5.7 Numerical Results



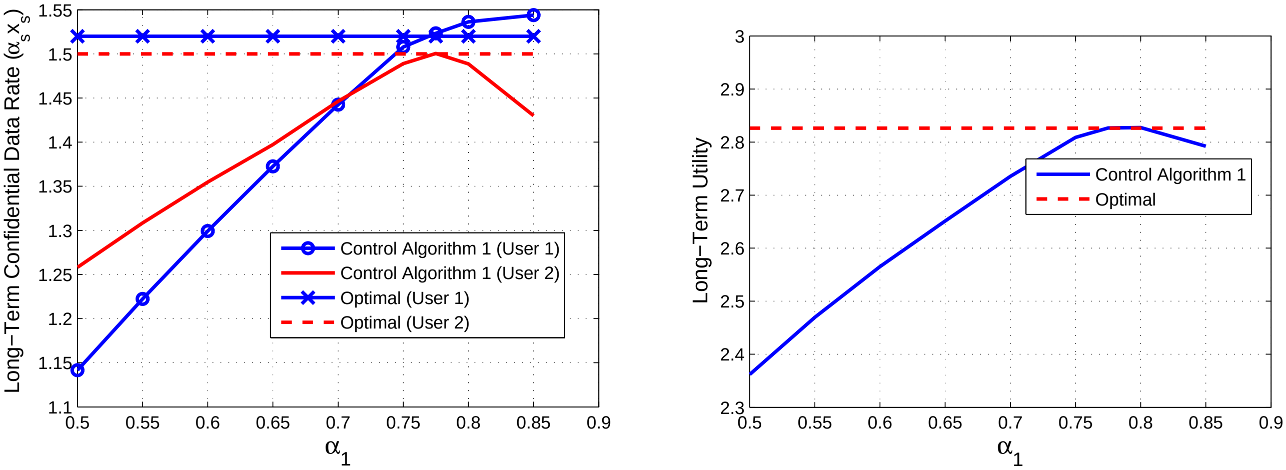
(a) α_1 vs Long-Term Confidential Data Rate ($\alpha_s x_s$)

(b) α_1 vs Long-term Total Utility

Figure 5.4: Performance evaluation of Control Algorithm 1 presented in Section 5.4, when all intermediate nodes are eavesdroppers.

The channels between nodes are modeled as iid Rayleigh fading Gaussian channels. The noise normalized transmit power is taken as constant and identical to $P = 1$ in every block and for all nodes. Let the power gain of the channel between nodes i and

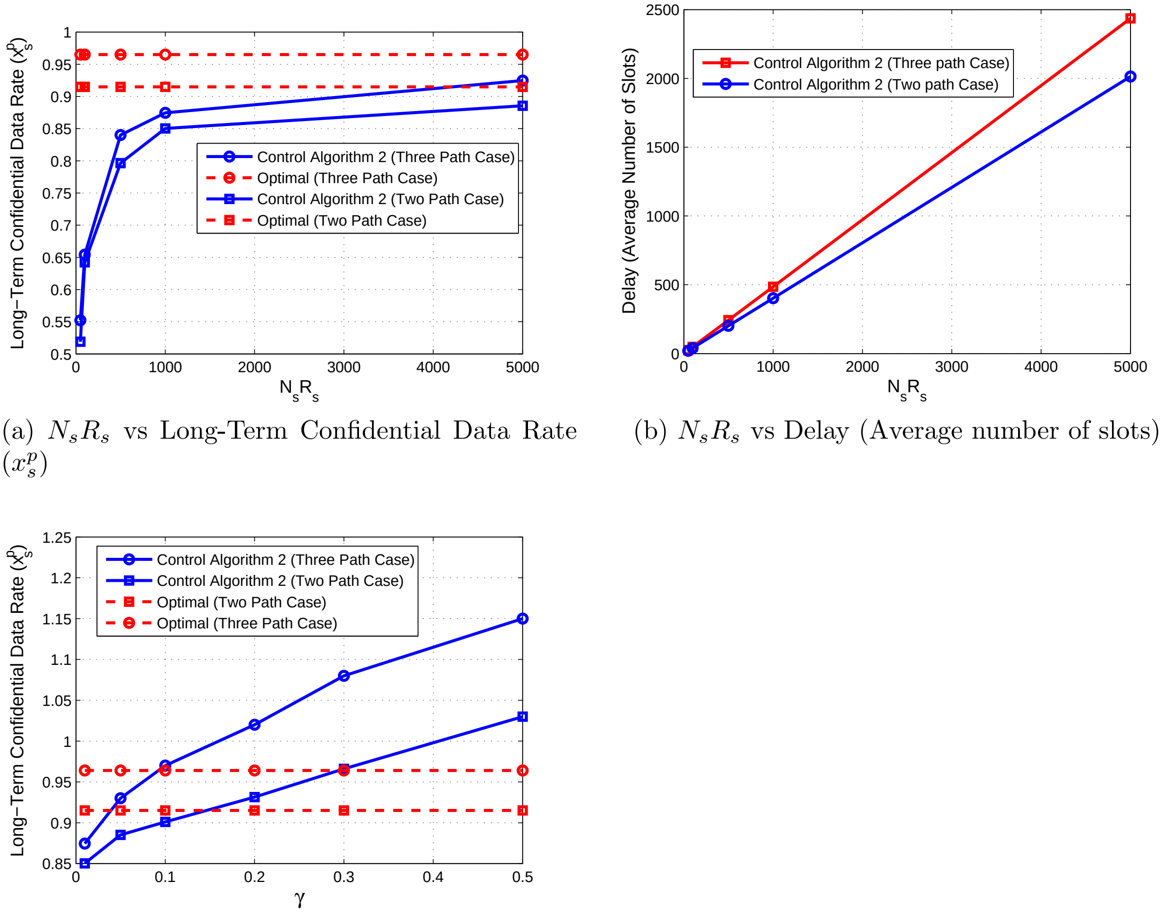
[7] As we consider a node-exclusive interference model, nodes cannot transmit and receive information at the same time.



(a) α_1 vs Long-Term Confidential Data Rate ($\alpha_s x_s$)

(b) α_1 vs Long-term Total Utility

Figure 5.5: Performance evaluation of Control Algorithm 1 presented in Section 5.4, when the number of eavesdroppers among all intermediate nodes are two.



(a) N_sR_s vs Long-Term Confidential Data Rate (x_s^p)

(b) N_sR_s vs Delay (Average number of slots)

(c) γ vs Long-Term Confidential Data Rate (x_s^p)

Figure 5.6: Performance evaluation of Control Algorithm 2 presented in Section 5.5.

j be $h_{ij}(t)$ at block t. Then, as $N_1 \to \infty$, $R_{ij}(t) = \log(1 + Ph_{ij}(t))$. The power gains of the channels are exponentially distributed, where the means of the link are as given in Table I. We consider a logarithmic utility function[8], $U_s(t) = \kappa + \log(A_s^p(t))$, where $A_s^p(t)$ is the confidential information admitted in block t. Note that, $A_s^p(t) = \alpha_s A_s(t)$ for the control algorithm presented in Section 5.4. We take $\kappa = 3$ and $H = 100$ in all experiments.

Table 5.1: Mean channel gains

(s_1, 1)	(s_1, 2)	(s_1, 3)	(s_2, 2)	(s_2, 3)	(s_2, 4)
6	8	10	4	8	6
(1, d_1)	(2, d_1)	(3, d_1)	(2, d_2)	(3, d_2)	(4, d_2)
6	8	10	4	8	6

In Fig. 5.4a-6.5a, we investigate the performance of Control Algorithm 1, when all intermediate nodes are considered as eavesdroppers, i.e., $\{1, 2, 3, 4\} \in E$. For the network depicted in Fig. 5.2, we numerically obtain the encoding rate, α_s^*, resulting in the maximum long-term total utility for source s. For the above set of values, we obtain $\alpha_1^* = 0.55$ and $\alpha_2^* = 0.509$, which corresponds to optimal long-term average arrival rates $x_1^* = 1.8$ and $x_2^* = 1.85$, respectively. In the experiments, we fix $\alpha_2 = \alpha_2^*$ and vary the value of α_1 to analyze the effect of α_s on the confidential data rates and total utility. From Fig. 5.4a, we first notice that, long-term confidential data rate of source s_1 increases with increasing α_1, since source s_1 sends a larger amount of confidential information for each encoded message. It is interesting to note that long-term confidential data rate of source s_2 increases initially with increasing α_1. This is because, for low α_1 values, in order to provide fairness between the sources, source s_1 admits more packets to its queue (e.g., $x_1 = 1.96$, when $\alpha_1 = 0.3$), increasing its queue size. As a result, scheduling decisions are dictated by the stability constraint of source s_1's queue, and thus, the long-term arrival rate of source s_2 is lower when α_1 is smaller (e.g., $x_2 = 1.78$ when $\alpha_1 = 0.3$). However, when α_1 is high, satisfying the perfect secrecy dominates the scheduling decisions, and source s_1 divides its transmission over the paths more equally at the expense of lower long-term arrival rates, x_1 and x_2. Fig. 6.5a depicts the relationship between α_1 and the long-term total utility. As expected,

[8] We utilize logarithmic utility function to provide proportional fairness.

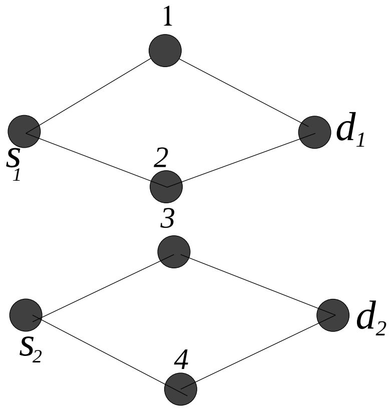
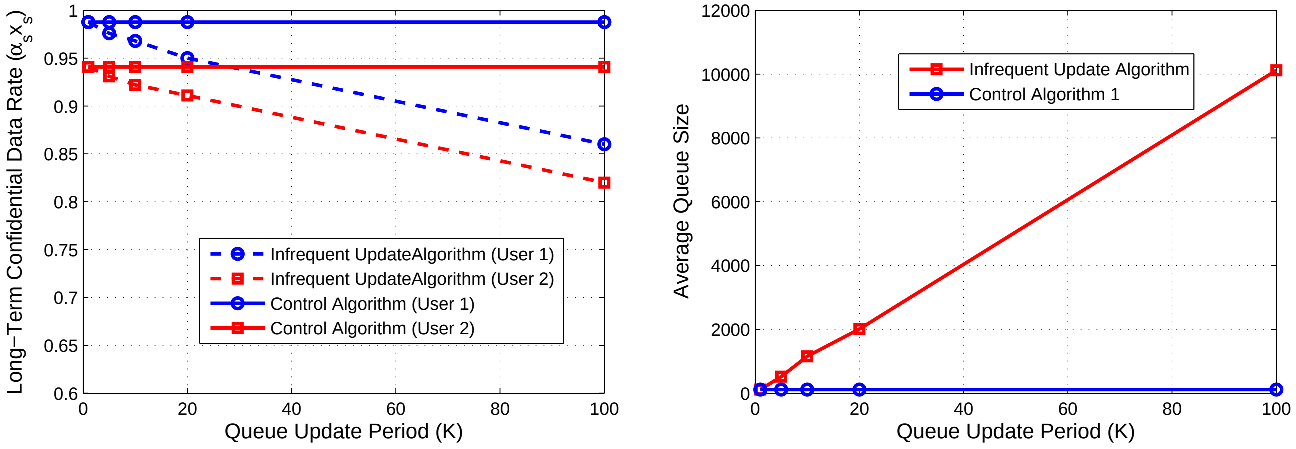


Figure 5.7: A multi-hop network with two available paths.

the total utility increases with increasing α_1 until $\alpha_1 = \alpha_1^*$. As α_1 increases, there is a gain due to incorporating more confidential information into each encoded message of source s_1. However, when α_1 is high, long-term arrival rates of both sources decrease as discussed previously. Thus, when $\alpha_1 > \alpha_1^*$, the loss due to decrease in x_1 and x_2 dominates the gain due to increasing α_1.

Next, in Fig. 5.5a-5.5b, we conducted the same analysis, when the number of eavesdroppers among all intermediate nodes is 2, i.e., the size of the set E is 2. We run simulations for all such possible sets of E, e.g., $\{1,4\} \in E$ or $\{2,3\} \in E$, and the results in Fig. 5.5a-5.5b are the average of the rates obtained for each set of E. We obtain the average encoding rates as $\alpha_1^* = 0.775$ and $\alpha_2^* = 0.77$, which corresponds to long-term average arrival rates $x_1^* = 1.96$ and $x_2^* = 1.95$, respectively. Again, we fix $\alpha_2 = \alpha_2^*$ and vary the value of α_1 to analyze the effect of α_s on the confidential data rates and total utility. If we compare the results in Fig. 5.5a-5.5b and Fig. 5.4a-6.5a, with the decreasing number of attackers among the intermediate nodes, the long-term confidential data rate increases. The reason is that since we have some trusted paths, i.e, paths that do not have attackers, we can encapsulate more confidential information over each encoded message. Lastly, we investigate the same scenario with no attackers in the network. In this scenario, Control Algorithm 1 simply corresponds to backpressure algorithm, since we can send the confidential information without encoding, i.e., with $\alpha_1^* = 1$ and $\alpha_2^* = 1$, and with the arrival rates $x_1 = 1.98$ and $x_1 = 1.92$.

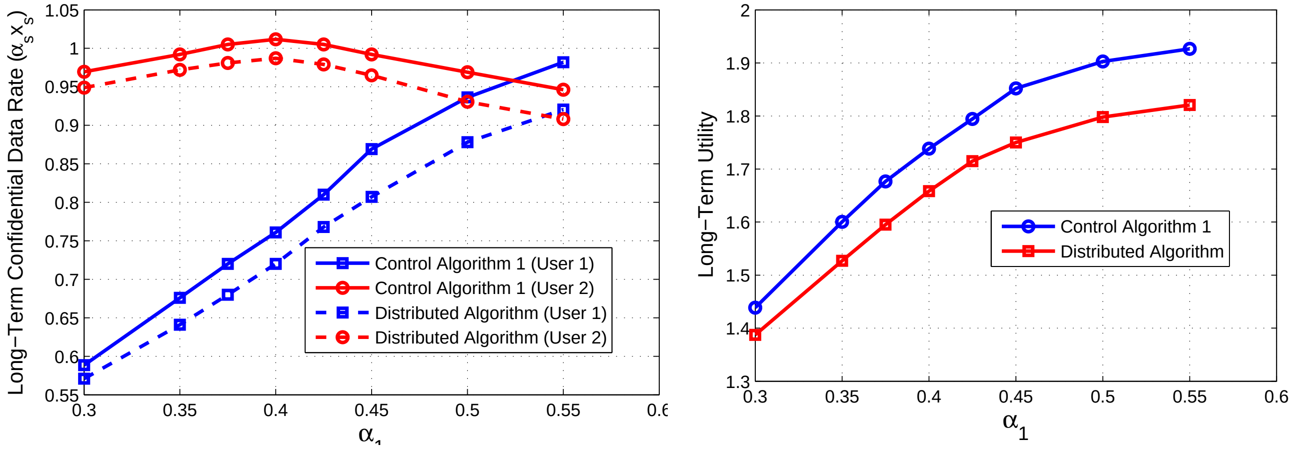
We next analyze the performance of Control Algorithm 2 with the different num-



(a) K vs Long-Term Confidential Data Rate ($\alpha_s x_s$)

(b) K vs Average Queue Size

Figure 5.8: Performance evaluation of infrequent queue update algorithm presented in Section 5.6.1.



(a) α_1 vs Long-Term Confidential Data Rate ($\alpha_s x_s$)

(b) α_1 vs Long-term Total Utility

Figure 5.9: Performance evaluation of distributed scheduling algorithm presented in Section 5.6.2.

ber of available paths. We used the network in Fig. 5.2 for a network with three paths and the network in Fig. 5.7 with two paths. Notice that in the network in Fig. 5.7, s_1 and s_2 do not have a communication link to node 3 and 2, respectively. For the network in Fig. 5.7, we use the main channel gains given in Table 5.7 except $(s_1, 3), (s_2, 2)$ and $(3, d_1), (2, d_2)$ which have zero mean channel gains. In numerical experiments, we use $\frac{R^2}{(R_s)^2}$ as the estimate of $p_s^{out}(R)$ for $0 < R < R_s$. In Fig. 5.6a, the effect of increasing $N_s R_s$ on the long-term confidential data rate, x_s^p, is shown. We first take the secrecy outage parameter, $\gamma_s = 0.01$, for all users. Fig. 5.6a depicts that when $N_s R_s = 50$ [9], the long-term confidential data rate has reduced by approximately 50%, compared to the optimal rates obtained for $N_s \to \infty$. However, the confidential data rate increases with increasing $N_s R_s$, and it gets close to the optimal confidential data rates, $\alpha_s^* x_s^*$, when $N_s R_s$ is large enough, i.e., $N_s R_s = 5000$. This is due to fact that when the transmission of a message takes smaller number of blocks, the portion of confidential bits inserted into the codeword, $R_s^{k,conf}/R_s$, gets smaller to satisfy the secrecy constraint. In addition, as the $N_s R_s$ increases, the dependance of the scheduling decisions between subsequent packets associated with a given secrecy-encoded message decreases, so i.i.d. approximation of control algorithm presented in Section 5.5 becomes more accurate. In Fig. 5.6b, we investigate delay with increasing $N_s R_s$. Here, we define delay as the average number of slots used to transmit an encoded confidential message from the source to its destination. It is interesting to note that even though long-term confidential data rate increases with an increasing number of available paths, it may also result in higher delay as depicted in Fig. 5.6b. The reason is that with more paths we can encode the message with more confidential information, but with an increasing congestion among the shared links. Finally, we investigate the effect of secrecy outage parameter, $\gamma_s = \gamma$ for all sources, on x_s^p. Fig. 5.6c shows that when the secrecy outage constraint is relaxed, i.e., γ is increased, the long-term confidential data rate increases for both networks. This result is expected, since sources can insert more confidential information into the encoded message, $R_s^{k,conf}$, with a higher secrecy outage parameter.

[9] If the average rate in a block t is 0.5 bits/channel use, the message is approximately transmitted in 100 blocks.

Note that, the optimal rate is obtained when there is no secrecy outages. Thus, after $\gamma = 0.1$ and $\gamma = 0.15$, the long-term confidential data rates exceed the optimal rates for the network in Fig. 5.2 and 5.7, respectively.

Next, we analyze the performance of the algorithm presented in Section 5.6.1 for the network depicted in Fig. 5.2, where the queue length information is periodically updated (we refer to this policy as the Infrequent Update Algorithm). We first analyze the effect of the periodic update parameter, K, on the long-term confidential data rate when H is the same for all experiments, i.e., $H = 100$. In addition, α_1 and α_2 are selected as 0.55 and 0.509, respectively. In Fig. 5.8a, we observe that as expected, the confidential data rate decreases with increasing K. This is due to fact that with a large K, the algorithm cannot closely track the queue length values which in turn deteriorates the performance of the scheduler. We evaluate the effect of K on the average queue size, when both infrequent update algorithm and Control Algorithm 1 converge to the optimal point fairly closely. To achieve near-optimal performance, we set the value of H for different values of K leading to optimal confidential data rates. In Fig. 5.8b, we plot average queue sizes with respect to K. Confirming theoretical results, with increasing K, we obtain larger average queue sizes, i.e., larger delays.

Finally, we analyze the performance of control algorithm presented in Section 5.6.2, where distributed scheduling is performed (We refer to this policy as Distributed Algorithm). The results are shown in Fig. 5.9a and Fig. 5.9b. Here, we select $\alpha_2 = 0.509$ and varies α_2. As expected, the long-term confidential data rates are smaller than those achieved with centralized scheduling, since topology and queue length information is not known globally, and the routing pattern is changed due to distributed scheduling. Our simulation results show that the degradation of performance of Control Algorithm 1 with distributed scheduling is relatively small: distributed scheduling results in a approximately 10% reduction in aggregate utility.

5.8 Chapter Summary

In this chapter, we considered the problem of resource allocation in wireless multi-hop networks where sources have confidential information to be transmitted to their corresponding destinations with the help of intermediate nodes over time-varying uplink channels. All intermediate nodes are considered as internal eavesdroppers from which the confidential information needs to be protected. To provide confidentiality in such setting, we propose encoding the message over long blocks of information which are transmitted over different paths. Then, we designed a dynamic control algorithm for a given encoding rate and we prove that our algorithm achieves utility arbitrarily close to the maximum achievable utility. In this problem, we find out that increasing the flow rate and keeping confidentiality is two conflicting objective unlike standard dynamic algorithms, and the proposed algorithm also considers spatial distribution of the flows over each path. Next, we consider the system, where the messages are encoded over finite number of blocks. For this system, transmissions of each block of the same message are dependant with each other. Thus, we propose a sub-optimal algorithm, and show that the proposed algorithm approaches the optimal solution as the number of blocks which the message are encoded, increases.

Finally, we deal with implementational issues of the proposed algorithms. First, we decrease overhead imposed by the updates transmitted to the scheduler. For that purpose, we design infrequent queue update algorithm, where users updates their queue length information periodically. We show that this algorithm again approaches the optimal solution in the expense of increasing average queue lengths. Then, we investigate distributed version of our dynamic control algorithms, where the scheduler decision is given according to local information available to each node. The simulation results illustrated that the reduction in confidentiality rate due to usage of distributed algorithm is relatively small.

Chapter 6

Dynamic Control for Cooperative Jamming with Non-altruistic Nodes

In the previous chapters, we assume that the nodes are altruistic, i.e., they invest their resources for the good of the whole system, and cooperate in the communication of confidential messages. In this chapter, we consider a cognitive radio network with non-altruistic jamming nodes, from which a source node utilizes jamming service to improve its confidential transmission, compensating them with a fraction of its bandwidth for transmission of its data. We develop optimal resource allocation and power control algorithms maximizing the aggregate utility of primary and secondary nodes with confidential communication needs as well as the nodes providing jamming service. Our scheme achieves a utility, arbitrarily close to the maximum achievable utility.

6.1 Introduction

Recently, information theoretic security has gained significant attention, provisioning an ultimate goal of guaranteing security against adversaries with unlimited computational resources. Particularly, deploying cooperative jammers that transmit Gaussian noise [24] or jamming codewords [37] can help to improve secure communication rates between legitimate nodes by impairing the reception of the eavesdropper.

The jamming signal power should be high enough to disturb the received signal at the eavesdropper; however, allocating too much power on the jamming signal can also degrade the signal quality at the destination. Thus, recent studies about the secrecy gains acquired with the cooperative jamming involves the optimization of jamming powers with the objective of maximizing the secrecy rate [38, 39]. However, they generally assume dedicated jamming nodes to the benefit of the system performance. This assumption is not valid, especially for the nodes with limited power. To that end, [118] has investigated a class of secrecy problem in cognitive radio networks with non-altruistic nodes. They propose a distributed solution using a game-theoretic framework where a source node, towards the maximization of its secrecy rate, utilizes the jamming services from non-altruistic nodes, and in return these nodes obtain utilization of some fraction of the bandwidth of the source node for their own data. One of the main drawbacks of the cross-layer resource allocation algorithms such as the one proposed in [118, 119] is that, instantaneous channel states between users and/or the eavesdropper are assumed to be available or they can be estimated fairly accurately. However, in general, neither the base station nor any other legitimate node in the network is aware of the CSI of the eavesdropper. Since CSI of nodes must be acquired (e.g., via pilot signal transmission) at the expense of some of the resources, which can otherwise be used for data transmission. Furthermore, the CSI of the eavesdropper, which is assumed to be passive, is impossible to obtain. To address this issue, here, we analyze a realistic scenario where only the distribution of the channel gains to the eavesdropper is available. Due to the lack of the knowledge of instantaneous channel gains, perfect secrecy cannot be ensured with probability 1 for confidential information. Thus, to meet a constraint on the secrecy outage probability, secondary nodes transmit jamming signals to disturb the signal received by the eavesdropper, and in return, they gain access to the channel to send their own data which is proportional to the power of their jamming signals. Secondly, with the goal of maximizing the aggregate utility, i.e., sum of the utilities of a source (primary) node and separate non-altruistic jamming (secondary) nodes, we model the problem in form of network utility maximization. We provide a dynamic solution, in which a joint flow control, power and bandwidth allocation scheme is obtained by using the stochastic optimization framework [6]. We prove

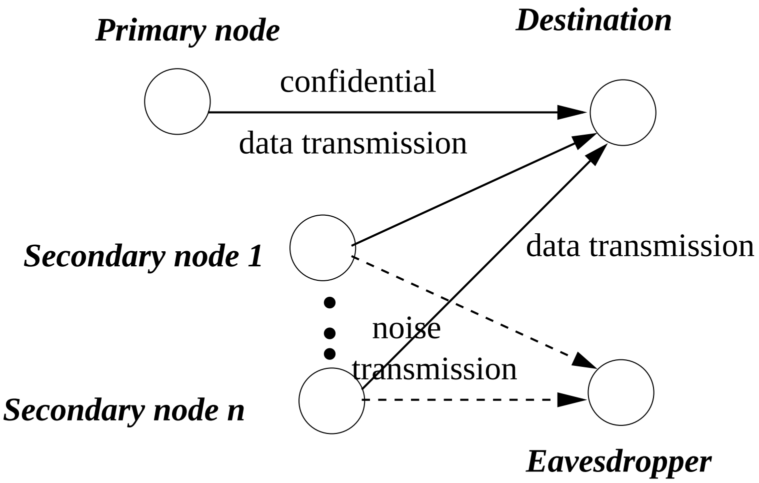


Figure 6.1: Network Model

that our scheme achieves a utility, arbitrarily close to the maximum achievable utility.

6.2 System Model and Preliminaries

6.2.1 System Model

We consider a cognitive radio network of one primary user and n secondary users, all wishing to communicate with a common destination as shown in Figure 6.1, and there is an eavesdropper whose goal is to interpret the information transmitted by the primary user without trying to modify it. Since secondary users do not own the spectrum band, the transmission has to be approved by the primary node.

Traffic is assumed to be a mixture of confidential data stored by the primary node and open data stored by the secondary nodes. Let $A_p(t)$ and $A_i(t)$ represent input rates in bits per channel use with which data is injected in the primary node and the secondary node i in slot t, respectively. The rates $A_p(t)$ and $A_i(t)$ have long-term averages λ_p and λ_i, respectively. $U_p(\lambda)$ represents the utility obtained by the primary node from the transmission of confidential data, and $U_i(\lambda)$ is the utility obtained by the secondary node i from the transmission of open data, both at a rate of λ bits per channel use. We assume that $U_p(0) = 0$, $U_i(0) = 0$, and $U_p(.)$ and $U_i(.)$ are continuously differentiable, monotonically increasing and concave functions.

Time is slotted where the time-slot is the resource to be shared among the primary and secondary users, and each slot has a length of N channel uses (physical layer symbols), where N is sufficiently large to allow for invoking random coding arguments. All channels undergo quasi-static flat Rayleigh fading, i.e., all channel gains have exponential distribution, in which the channel gain remains constant within a time slot and varies independently from slot to slot. For a time slot t, $h_{SD}(t)$ denotes the gain of the channel between the source and the destination nodes; $h_{SE}(t)$ is the gain of the source-eavesdropper channel; $h_{J_iE}(t)$ and $h_{J_iD}(t)$ denote the gains of the channels from the secondary node i to the eavesdropper and destination node respectively. We normalize the power gains such that the (additive Gaussian) noise has unit variance.

We denote the instantaneous achievable rate for the main channel by $R_p(t)$, which is the mutual information between the channel between the primary node and destination in time slot t. Likewise, $R_e(t)$ corresponds to the mutual information between the channel input at the primary node and the channel output at the eavesdropper.

In our work, we consider cooperative jamming where the secondary user creates interference at the eavesdropper by transmitting a jamming signal [38]. We assume that each secondary node independently transmits noise signal, which lies in the null space of the secondary node-destination channel, thus creating zero interference to the destination [120]. Defining P_s and $P_i^J(t)$ as the transmission powers of the primary node and secondary node i respectively in a cooperative jamming setting in time slot t, the transmission rates, $R_p(t)$ and $R_e(t)$, can be obtained as:

$$\begin{aligned} R_p(t) =& \log\left(1 + P_s h_{SD}(t)\right) \\ R_e(t) =& \log\left(1 + \frac{P_s h_{SE}(t)}{1 + \sum_i h_{J_iE}(t) P_i^J(t)}\right) \end{aligned} \tag{6.1}$$

Let $\beta_i(t)$ be the fraction of time slot granted to the secondary user i in slot t for cooperating with the primary user to enhance its secrecy rate. Defining $P_i^T(t)$ as the transmission power of the secondary node i reserved for its own transmission, the instantaneous achievable rate of the secondary node is:

$$R_i^T(t) = \beta_i(t) \log \left(1 + P_i^T(t) h_{J_iD}(t)\right)$$

6.2.2 Confidential Transmission Scheme and Secrecy

We assume the availability of perfect channel-state information (CSI) of the channels to the destination, $h_{SD}(t)$ and $h_{J_iD}(t)$, at the transmitters. We assume that transmitters do not have the knowledge of the instantaneous values of the gains of eavesdropper channels, $h_{SE}(t)$ and $h_{J_iE}(t)$, but their distributions are available [1]. One should realize that, since instantaneous CSI is not available, one cannot choose the code rates based on a particular fading channel state. Instead, a particular coding rate is chosen for the confidential message and the same code is used for the primary node at all times. Specifically, the primary node uses Wyner coding to provide confidentiality, which basically inserts a randomization message to the actual message to increase the level of secrecy [3]. Let $C(R_p^{\text{code}}; R_p^{\text{conf}}; N)$ be a Wyner code of size $2NR_p^{\text{code}}$ codewords, generated to convey a confidential message set $W_p \in 1, \ldots 2NR_p^{\text{conf}}$. Thus, every codeword has a length of NR_p^{code} bits to convey NR_p^{conf} bits of confidential information.

Let the vector of symbols received by the eavesdropper be Y_e. To achieve perfect secrecy, the following constraint must be satisfied by the primary node, for all t,

$$\lim_{N \to \infty} \frac{1}{N} I(W_p; Y_e) \leq \epsilon. \tag{6.2}$$

Next, we define the notion of *secrecy outage* employed in our analysis. We say that the secrecy outage event occurs, when the confidential message is intercepted by an eavesdropper node. This is when the perfect secrecy constraint in (6.2) is violated, such that $R_p^{\text{code}} - R_p^{\text{conf}} < R_e(t)$. Specifically, when $R_p^{\text{code}} - R_p^{\text{conf}}$, the rate of the randomization message the source uses in the random binning scheme for secrecy in

[1] Since the eavesdropper does not participate in communication but passively listens to the channel, the primary and secondary nodes can guess the location of the eavesdropper and estimate the statistics of their channel to this node.

time slot t, is lower than the actual rate of the eavesdropper, $R_e(t)$, in time slot t, a secrecy outage has occurred. The probability of secrecy outage in time slot t is given by,

$$\rho_p^{\text{secr}}(t) = P(R_p^{\text{code}} - R_p^{\text{conf}} < R_e(t)). \tag{6.3}$$

As a quality of service (QoS) requirement, the expected probability of secrecy outage of the primary node can be required to be below a given threshold γ. Note that the primary node may not have channel quality to satisfy this QoS requirement. With the help of secondary users, the primary user may have a higher secrecy rate and meet this constraint, which provides the incentive to share the spectrum with the secondary user. The secondary users, on the other hand, are willing to join the cooperation because they need such a spectrum opportunity to transmit their own data streams. This lays the incentive foundation of cooperation.

The potential cooperation can be established in the following procedure. The primary user first announces the jamming power levels of the secondary users such that the secrecy outage requirement is satisfied. Then, the maximum spectrum shared with the secondary users is determined by these jamming power levels, i.e., the expected value of $\beta_i(t)$ is below a prescribed level, which is assumed to be proportional to the jamming power level of node i. Thus, the primary user first aims to minimize total jamming power purchased from the secondary nodes while satisfying secrecy outage requirement. Secondly, based on the predetermined jamming power, we seek a solution to the spectrum sharing problem, where we want to maximize the sum utilities of the primary node and secondary nodes.

6.3 Jamming Power Optimization and Cross-layer Algorithm

In this section, our objective is to design a cross-layer algorithm considering joint flow control, time and power optimization problems while satisfying a secrecy outage constraint of the primary node. We investigate two problems for this objective. In the first problem, we aim to minimize the total jamming power subject to the secrecy outage constraint of the primary node. In the second problem, we aim to maximize the aggregate utility of the primary and secondary nodes by the optimized jamming powers obtained in the first problem.

In time-varying wireless channels, a channel outage occurs when the received signal to interference/noise ratio drops below a threshold necessary for decoding the transmitted signal. Likewise, a secrecy outage event occurs, when the randomized information rate drops below the information rate obtained by the eavesdropper. In this case, the amount of randomized bits is not sufficient to confuse the eavesdropper, and the eavesdropper interferes with the secret packet. In the following, we analyze the secrecy outage probability, ρ_p^{secr}.

Lemma 7. *Given the statistics of the channels to the eavesdropper and the chosen secret encoding rates as R_p^{code} and R_p^{conf}, respectively, the secrecy outage probability, is calculated as:*

$$\rho_p^{secr} = \sum_{i=1}^{n} \left(\prod_{j=1, j\neq i}^{n} \frac{\lambda_j}{\lambda_j - \lambda_i} \right) e^{-\lambda_{SE} D} \left[1 - \frac{\lambda_{SE}}{\lambda_{SE} + \frac{\lambda_i}{D}} \right] \tag{6.4}$$

where $D = 2^{R_p^{code} - R_p^{conf}} - 1$, and $\lambda_i = \frac{1}{P_i^J \mathbb{E}\left[h_{J_i E}\right]}$ for the secondary node i and $\lambda_{SE} = \frac{1}{P_s \mathbb{E}[h_{SE}]}$ for the source node.

Proof. In order to derive the secrecy outage probability, we first need to statistically characterize $R_e(t)$ in (6.1), since transmitters do not have the knowledge of the instantaneous values of the gains of eavesdropper channels, $h_{SE}(t)$ and $h_{J_iE}(t)$, but their distributions are available. Note that the channel gains are exponentially distributed with parameters $\lambda_{SE} = \frac{1}{P_s \mathbb{E}[h_{SE}]}$ and $\lambda_i = \frac{1}{P_i^J \mathbb{E}\left[h_{J_i E}\right]}$. We define Z and $(X_i)_{i=1,\ldots,n}$ as independent exponential random variables with distinct respective parameters λ_{SE} and $\lambda_i,\ i = 1, \ldots, n$. We start with the distribution of the sum of independent exponential random variables for the summation in the denominator of the rational term in the log function, i.e., interference terms created by the secondary nodes, in (6.1). The sum of independent exponential distributions is hypoexponentially distributed [121]. Defining $Y = X_1 + \ldots + X_n$, the probability density function (PDF) of Y is :

$$f_Y(y) = \sum_{i=1}^{n} \lambda_i e^{-y\lambda_i} \left(\prod_{j=1, j\neq i}^{n} \frac{\lambda_j}{\lambda_j - \lambda_i} \right) \tag{6.5}$$

We know that Z is also exponential with pdf $f_Z(z) = \lambda_{SE} e^{-\lambda_{SE} z}$. Now, re-writing the definition in (6.3), we are ready to extrect the secrecy outage probability,

$$\begin{aligned} P_s^{\text{out}} &= \mathbb{P}\left(R_p^{\text{code}} - R_p^{\text{conf}} < \log\left(1 + \frac{Z}{1+Y}\right)\right) \\ &= \mathbb{P}\left(D < \frac{Z}{1+Y}\right) = \mathbb{P}\left(D(1+Y) < Z\right) \end{aligned} \tag{6.6}$$

where $D = 2^{R_p^{\text{code}} - R_p^{\text{conf}}} - 1$. Since the random variables Z and Y are independent, we can calculate the secrecy outage probability as:

$$\begin{aligned} P_s^{\text{out}} &= \int_{z=D}^{\infty} \int_{y=0}^{z/D-1} f_Z(z) f_Y(y) dydz \\ &= \sum_{i=1}^{n} \int_{z=D}^{\infty} \int_{y=0}^{z/D-1} \lambda_{SE} e^{-\lambda_{SE} z} \lambda_i e^{-y\lambda_i} \left(\prod_{j=1, j\neq i}^{n} \frac{\lambda_j}{\lambda_j - \lambda_i} \right) dydz \\ &= \sum_{i=1}^{n} \left(\prod_{j=1, j\neq i}^{n} \frac{\lambda_j}{\lambda_j - \lambda_i} \right) \int_{z=D}^{\infty} \lambda_{SE} e^{-\lambda_{SE} z} \left[1 - e^{-(z/D-1)\lambda_i} \right] \\ &= \sum_{i=1}^{n} \left(\prod_{j=1, j\neq i}^{n} \frac{\lambda_j}{\lambda_j - \lambda_i} \right) e^{-\lambda_{SE} D} \left[1 - \frac{\lambda_{SE}}{\lambda_{SE} + \frac{\lambda_i}{D}} \right] \end{aligned} \tag{6.7}$$

Now, we obtain the result in Lemma 1. This has concluded the proof.

□

6.3.1 Jamming Power Allocation

Here, we focus on designing the transmission scheme such that the probability of secrecy outage ρ_p^{secr} can satisfy the maximum allowable portion of secret bits experiencing secrecy outage, γ, while minimizing the total jamming power of the secondary nodes. Specifically, we analyze the following problem:

$$\min_{P_i^J} \sum_{i=1}^{n} P_i^J \tag{6.8}$$

$$\text{subject to } \rho_p^{\text{secr}} \leq \gamma \tag{6.9}$$

Note that the above problem is a static optimization problem, since only the statistics of the channels to the eavesdropper are known, and the secrecy outage probability calculated in Lemma 7 is a function of the mean of channel gains. Since the secrecy outage probability is a decreasing function of the jamming powers, the constraint in 6.9 is realized with equality. Let $\mathbf{P}^{J*} = [P_1^{*J}, P_2^{*J}, \ldots, P_n^{*J}]$ be optimal values of jamming power levels which are the solution of the optimization problem in (6.8) and (6.9). The optimal jamming powers, $\mathbf{P}^{J*}$, are obtained by the primary node in an offline fashion before the start of spectrum sharing session. One way to solve the problem in (6.8) and (6.9) is to use one of the search methods such as the bisection method. Note that to have an unique solution, the secrecy outage needs to be a convex function with respect to jamming power levels.

Lemma 8. *The secrecy outage probability, P_s^{out} is convex function with respect to jamming power of the secondary nodes, P_i^J.*

Proof. To prove the convexity of multivariate function P_s^{out}, we need to examine the Hessian matrix, and show that the Hessian matrix is positive definite. The Hessian matrix is defined as:

$$G = \begin{bmatrix} b_1 & a_{12} & \ldots & a_{1n} \\ a_{21} & b_2 & \ldots & a_{2n} \\ \vdots & & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & b_n \end{bmatrix}, \tag{6.10}$$

where $b_i = \partial^2 P_s^{out}/\partial(P_i^J)^2$ and $a_{ij} = \partial^2 P_s^{out}/\partial P_i^J \partial P_j^J$. To obtain the Hessian matrix, we first obtain the derivative of P_s^out with respect to P_i^J. We obtain the derivative of the secrecy outage probability with respect to P_i^J as follows:

$$\frac{\partial P_s^{out}}{P_1^J} = \frac{\mathbb{E}\left[h_{J_iE}\right](P_s\mathbb{E}\left[h_{SE}\right])^n D}{A_i^2 \prod_{j\neq i} A_j} \tag{6.11}$$

where n is the number of the secondary nodes. By using the result in (6.11), we obtain the elements of the Hessian matrix as follows:

$$\begin{aligned} b_i &= 2\frac{\mathbb{E}\left[h_{J_iE}\right]^2 (P_s\mathbb{E}\left[h_{SE}\right])^n D^2}{A_i^3 \prod_{j\neq i} A_j} \\ a_{ij} &= \frac{\mathbb{E}\left[h_{J_iE}\right]\mathbb{E}\left[h_{J_jE}\right](P_s\mathbb{E}\left[h_{SE}\right])^n D^2}{A_i^2 A_j^2 \prod_{k\neq i,j} A_k} \end{aligned} \tag{6.12}$$

As we obtain the Hessian matrix, we use Sylvester's criterion to prove positive definiteness of the Hessian matrix [122]. This criterion suggests that a matrix is positive definite if and only if the determinants of all upper-left k by k sub-matrices and the matrix itself are positive. It is straightforward to show that all these determinants are positive. This has concluded the proof.

□

6.3.2 Cross-layer Algorithm

Our objective is to design a joint flow control, time allocation algorithm that maximizes the aggregate network utility given the optimal jamming power allocation of the secondary nodes, $\mathbf{P}^{J*}$. We aim to find the solution of the following problem:

$$\max_{P_i^T(t),\beta_i(t)} \mathbb{E}\left[U_p(\lambda_p)\right] + \sum_{i=1}^{n} \mathbb{E}\left[U_i(\lambda_i)\right] \tag{6.13}$$

$$\text{subject to } \lambda_p \leq \mathbb{E}\left[(1-\sum_{i=1}^{n}\beta_i(t))R_p^{\text{conf}}\right] \tag{6.14}$$

$$\lambda_i \leq \mathbb{E}\left[R_i^T(t)\right] \tag{6.15}$$

$$\mathbb{E}\left[P_i^T(t)\right] \leq \alpha_i \tag{6.16}$$

$$\mathbb{E}\left[\beta_i(t)\right] \leq \theta_i P_i^{J*} \tag{6.17}$$

The objective function in (6.13) calculates the total expected utility of the primary and secondary nodes over random stationary channel conditions, and the time and power allocation decisions. Condition (6.16) requires that the average power used for its own transmission by the secondary node should be smaller than a given constant power budget α. Condition (6.17) is the spectrum allocation constraint of the secondary nodes, where we assume that the average allocated spectrum to the secondary node i is smaller than some portion of its jamming power, i.e, $\theta_i P_i^{J*}$, used to help the confidential transmission of the primary node.

Next, we propose a dynamic control solution based on the stochastic network optimization framework developed in [6]. This framework allows the solution of a long-term stochastic optimization problem without requiring the explicit characterization of the achievable rate regions. The dynamics of the primary and secondary node i queues $Q_p(t)$ and $Q_i(t)$ are given as follows:

$$Q_p(t+1) = \left[Q_p(t) - (1 - \sum_{i=1}^{n} \beta_i(t))R_p^{\text{conf}}\right]^+ + A_p(t), \tag{6.18}$$

$$Q_i(t) = \left[Q_i(t) - R_i^T(t)\right]^+ + A_i(t), \tag{6.19}$$

where $[\cdot]^+ = \max\{0, \cdot\}$, and we can relate the constraints in (6.16) and (6.17) with a virtual queue as:

$$Z_i(t+1) = \left[Z_i(t) + P_i^T(t) - \alpha\right]^+, \tag{6.20}$$

$$K_i(t+1) = \left[K_i(t) + \beta_i(t) - \theta_i P_i^{J*}\right]^+, \tag{6.21}$$

Strong stability of (6.20) and (6.21) ensure that the constraints are also satisfied [6].

Control Algorithm: The algorithm executes the following steps in each slot t:

Flow Control: For some $V > 0$, the primary node and secondary node i injects $A_p(t)$ and $A_i(t)$ bits, respectively, where

$$(A_p(t), A_i(t)) = \underset{A_p, A_i}{\operatorname{argmax}} V \left[U_p(A_p) + \sum_{i=1}^{n} U_i(A_i) \right] - Q_p(t) A_p - \sum_{i=1}^{n} Q_i(t) A_i$$

Time and Power Allocation: For some $P_i^{J*} > 0$ and $P_s > 0$, the primary node shares $\beta_i(t)$ portion of the slot with the secondary node i, and the secondary node allocates the power $P_i^T(t)$ for its own transmissions. We choose these parameters as the solution of:

$$\begin{aligned} \{\beta_i(t), P_i^T(t)\} = \underset{\beta_i, P_i^T}{\operatorname{argmax}} & \, Q_p(t)(1 - \sum_{i=1}^{n} \beta_i(t)) R_p^{\text{conf}} \\ & + \sum_{i=1}^{n} \left(Q_i(t) R_i^T(t) - Z_i(t) P_i^T(t) - K_i(t) \beta_i(t) \right). \end{aligned}$$

Theorem 12. *If $R_T(t) < \infty$ for all t, then dynamic control algorithm satisfies:*

$$\begin{aligned} \liminf_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} U_p(\lambda_p) + \sum_{i=1}^{n} U_i(\lambda_i) &\geqslant U^* - \frac{B}{V}, \\ \liminf_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} \mathbb{E}\left[Q_p(t)\right] &\leq \frac{B + V(\bar{U} - U^*)}{\epsilon_1} \\ \liminf_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} \sum_{i=1}^{n} \mathbb{E}\left[Q_i(t)\right] &\leq \frac{B + V(\bar{U} - U^*)}{\epsilon_2} \end{aligned}$$

where $B, \epsilon_1, \epsilon_2 > 0$ are constant, U^* is the optimal aggregate utility, and and $\bar{U}$ is the maximum possible aggregate utility.

Theorem 12 can be proven following the same approach in Theorem 4.5 in [6].

Proof. The optimality of the algorithm can be shown by applying the Lyapunov optimization theorem [6]. We consider queue backlog vectors as $\mathbf{Q}(t) = (Q_p(t), Q_1(t), \ldots, Q_n(t))$, $\mathbf{K}(t) = (K_1(t), \ldots, K_n(t))$, and $\mathbf{Z}(t) = (Z_1(t), \ldots, Z_n(t))$, where n is the number of secondary nodes in the network. Let $L(\mathbf{Q}, \mathbf{K}, \mathbf{Z})$ be a quadratic Lyapunov function of real and virtual queue backlogs defined as:

$$L(\mathbf{Q(t)},\mathbf{K(t)},\mathbf{Z(t)}) = \frac{1}{2}\left(Q_p(t)^2 + \sum_{i=1}^{n}\left[(Q_i(t))^2 + (Z_i(t))^2 + (K_i(t))^2\right]\right). \quad (6.22)$$

Also consider the one-step expected Lyapunov drift, $\Delta(t)$ for the Lyapunov function as:

$$\Delta(t) = \mathbb{E}\left[L(\mathbf{Q(t+1)},\mathbf{K(t+1)},\mathbf{Z(t+1)})\right.$$
$$\left. - \; L(\mathbf{Q(t)},\mathbf{K(t)},\mathbf{Z(t)}) | \mathbf{Q(t)},\mathbf{K(t)},\mathbf{Z(t)}\right]. \quad (6.23)$$

The following lemma provides an upper bound on $\Delta(t)$.

Lemma 9.

$$\begin{aligned}\Delta(t) \leq B - \mathbb{E}&\left[Q_p(t)\left(A_p(t) - (1-\sum_{i=1}^{n}\beta_i(t))R_p^{conf}\right) \;\middle|\; Q_p(t)\right]\\ &- \sum_{i=1}^{n}\mathbb{E}\left[Q_i(t)\left(A_i(t) - R_i^T(t)\right) \;\middle|\; Q_i(t)\right]\\ &- \sum_{i=1}^{n}\mathbb{E}\left[Z_i(t)\left(P_i^T(t) - \alpha\right) \;\middle|\; Z_i(t)\right]\\ &- \sum_{i=1}^{n}\mathbb{E}\left[K_i(t)\left(\beta_i(t) - \theta_i P_i^{J*}\right) \;\middle|\; K_i(t)\right] \quad (6.24)\end{aligned}$$

where $B > 0$ is a constant.

Proof. Since the maximum transmission power is finite, in any interference-limited system transmission rates are bounded. Also assume that the arrival rates are bounded, i.e., $A_p^{\max}$ and $A_i^{\max}$ are the maximum number of bits that may arrive in a slot for the primary node and secondary node i, respectively. By simple algebraic manipulation one can obtain a bound for the difference $\left(Q_i(t+1)\right)^2 - \left(Q_i(t)\right)^2$ and also for other queues to obtain the result in (6.24)

Applying the above lemma, we can complete our proof. In particular, Lyapunov Optimization Theorem [6] suggests that a good control strategy is the one that minimizes the following:

$$\Delta^U(t) = \Delta(t) - V\mathbb{E}\left[U_p(t) + \sum_{i=1}^{n}(U_i(t)) \,|\, (\mathbf{Q(t)},\mathbf{K(t)},\mathbf{Z(t)})\right]. \quad (6.25)$$

By using (6.24) in the lemma, we obtain an upper bound for (6.25), as follows:

$$\begin{aligned}\Delta^U(k) \leq B - \mathbb{E}&\left[Q_p(t)\left(A_p(t) - (1 - \sum_{i=1}^{n}\beta_i(t))R_p^{\text{conf}}\right) \Bigg| \; Q_p(t)\right] \\ &- \sum_{i=1}^{n}\mathbb{E}\left[Q_i(t)\left(A_i(t) - R_i^T(t)\right) \mid Q_i(t)\right] \\ &- \sum_{i=1}^{n}\mathbb{E}\left[Z_i(t)\left(P_i^T(t) - \alpha\right) \mid Z_i(t)\right] \\ &- \sum_{i=1}^{n}\mathbb{E}\left[K_i(t)\left(\beta_i(t) - \theta_i P_i^{J*}\right) \mid K_i(t)\right] \\ &- V\mathbb{E}\left[U_p(A_p(t)) + \sum_{i=1}^{n}U_i(A_i(t))\right] \qquad (6.26)\end{aligned}$$

Our proposed dynamic network control algorithm is designed such that it minimizes the right hand side of (6.26). If the arrival rates, and the time allocation parameter, θ_i, are in the feasible region, it has been shown in [6] that there must exist a stationary time and power allocations and rate control policy that chooses the allocations and their arrival rates independent of queue backlogs and only with respect to the channel statistics. In particular, the optimal stationary policy can be found as the solution of a deterministic policy if the channel statistics are known a priori.

Let U^* be the optimal value of the objective function of the problem (6.13-6.17) obtained by the aforementioned stationary policy. Also let ${\lambda_p}^*$ and ${\lambda_i}^*$ be optimal traffic arrival rates of the primary node and secondary node i, respectively, found as the solution of the same problem. Note that the expectations on the right hand side of (6.26) can be written separately due to independence of backlogs with allocation and rate control policy. In particular, the optimal input rate ${\lambda_p}^*$ and ${\lambda_i}^*$ could in principle be achieved by the simple backlog-independent admission control algorithm of new arrival $A_i(p)$ and $A_i(t)$ for the primary node and the secondary node i in block t independently with probability $\zeta_p = {\lambda_p}^*/\lambda_p$ and $\zeta_i = {\lambda_i}^*/\lambda_i$, respectively.

Also, since ${\lambda_p}^*$ and ${\lambda_i}^*$ are in the achievable rate region, i.e., arrival rates are strictly interior of the rate region, there must exist a stationary scheduling and rate allocation policy that is independent of queue backlogs and satisfies the followings:

$$\mathbb{E}\left[\sum_{\{i|(s,i)\in L\}} \mu_{si}(t)|\mathbf{Q}\right] \geq \lambda_p{}^* + \epsilon_1 \tag{6.27}$$

$$\mathbb{E}\left[\sum_{i=1}^{n} R_i^T(t)|\mathbf{Q}\right] \geq \lambda_i^* + \epsilon_2 \tag{6.28}$$

$$\mathbb{E}\left[P_i^T(t)|\mathbf{Z}\right] + \epsilon_3 \leq \alpha_i \tag{6.29}$$

$$\mathbb{E}\left[\beta_i(t)|\mathbf{K}\right] + \epsilon_4 \leq \theta_i P_i^{J*} \tag{6.30}$$

Clearly, any stationary policy should satisfy (6.26). Recall that our proposed policy minimizes the right hand side (RHS) of (6.26), and hence, any other stationary policy (including the optimal policy) has a higher RHS value than the one attained by our policy. In particular, the stationary policy that satisfies (6.27)-(6.30), and implements aforementioned probabilistic admission control can be used to obtain an upper bound for the RHS of our proposed policy. Inserting (6.27)-(6.30) into (6.26), we obtain the following upper bound for our policy:

$$\begin{aligned} RHS < B - \epsilon_1 \mathbb{E}[Q_p(t)] - \epsilon_2 \sum_{i=1}^{n} \mathbb{E}[Q_i(t)] \\ - \epsilon_3 \sum_{i=1}^{n} \mathbb{E}[Z_i(t)] - \epsilon_4 \sum_{i=1}^{n} \mathbb{E}[K_i(t)] - VU^*. \end{aligned}$$

where (55) follows from Jensen's inequality together with concavity of $U_p(.)$ and $U_i(.)$. This is exactly in the form of Lyapunov Optimization Theorem given in [6], and hence, we can obtain bounds on the performance of the proposed policy and the sizes of queue backlogs as given in Theorem 12. □

6.4 Numerical Results

In our simulation results, we consider logarithmic utility functions of the primary and secondary nodes, where the utility obtained by the primary node is $\kappa > 1$ times more than the utility obtained by the secondary node at the same rate. More specifically, we

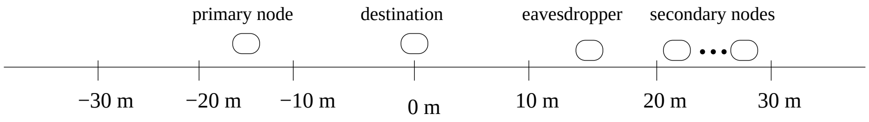


Figure 6.2: Linear Network Topology

take $U_p(x) = \kappa \log(1+x)$ and $U_i(x) = \log(1+x)$. The utility function $U(x) = \log(1+x)$ captures resource allocation according to the criterion of proportional fairness, which is based on maximizing total throughput while allowing users at least a minimal level of service. The source power is set as, $P_s = 1$ watt, which is also the same as the average power constraint at the relays, i.e., $\alpha_i = 1$ watt, $\forall i$ as otherwise stated. The noise variance is $\sigma^2 = 10^{-6}$ and the bandwidth is $W = 1$ Hz, for simplicity. We consider Rayleigh fading channels, so the channel gains are exponentially distributed with their means calculated in general as $E[h^2] = d^(- c/2)$, where d is the distance between considered nodes, and c is the path loss exponent, chosen as 3.5. We consider a linear topology as depicted in Fig. 6.2, where all the nodes are placed along a horizontal line. The destination node is located at the origin (0 m) and the primary node is placed at (-15) m. We use 5 secondary nodes and they are randomly location at the range of [20-30]. The location eavesdropper node is changed in the next experiment. In addition, θ_i, α_i and α_i are taken as 0.1, 1 and 0.1, respectively for all i unless otherwise stated. In addition, $\hat{R}_p$ and $\hat{R}_p^{\text{priv}}$ are taken as 2 and 1, respectively.

In the first experiment, we evaluate the optimal jamming power purchased by the primary node to meet its secrecy outage constraint. We evaluate the result for three different secrecy outage constraints, i.e., for $\gamma = 0.01, 0.1, 0.2$. With the destination node at 0 m., the primary node is placed at -10 m., and five secondary nodes are randomly placed within (20-30) m. from the destination node, we let the location of the eavesdropper node vary from -40 m. to 40 m. from the source node. We obtain the optimal jamming power curve as shown in Fig. 6.3. As the eavesdropper gets closer to the destination node, i.e., the location of 0 m, the jamming power transmitted by the secondary nodes increases to meet secrecy outage constraint. On the other hand, from 30 m to 40 m and -30 m to -40 m, the optimal jamming power is zero, since the secrecy outage constraint can be met without help of the secondary nodes.

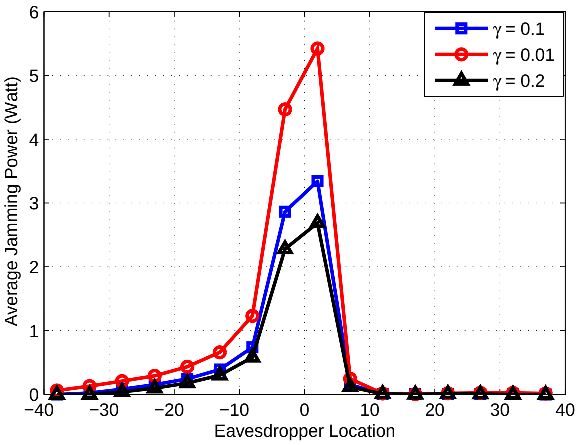
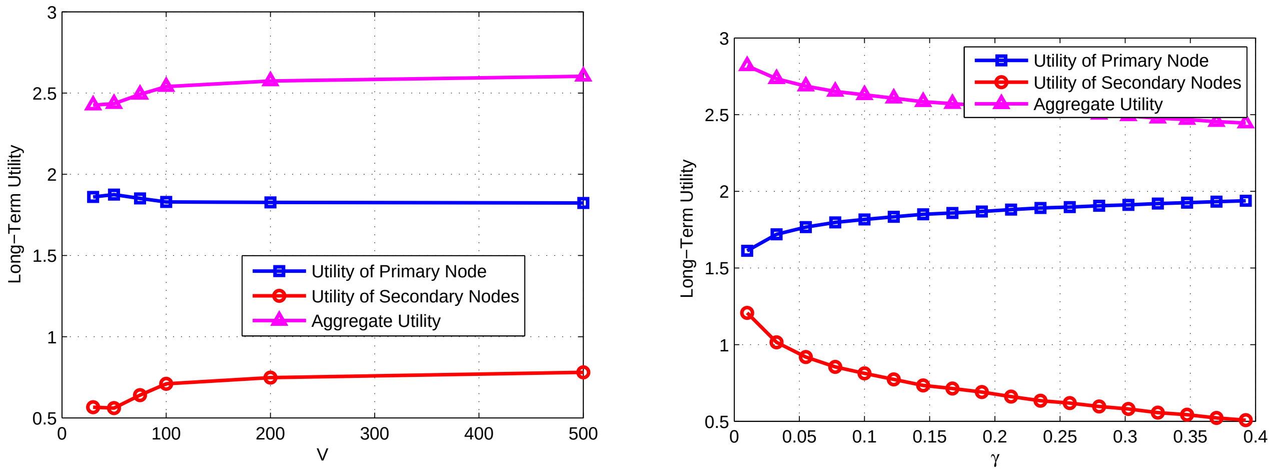


Figure 6.3: Optimal jamming powers with respect to the location of the eavesdropper

In the next simulations, we fixed the location of the eavesdropper at 15 m and analyze the performance of the proposed algorithm with different parameters. First, we investigate the effect of system parameter V in our dynamic control algorithm. Fig. 6.4a shows that for $V > 200$, long-term utilities converge to their optimal values fairly closely at the expense of increasing queue sizes verifying the theoretical result given in Theorem 12. In Fig. 6.4b, we analyzed the effect of secrecy outage constraint, γ, on the long-term utility obtained by the primary and secondary nodes. As depicted in Fig. 6.4b, the utility obtained by the secondary nodes decreases with increasing γ, since less jamming power is needed to meet the secrecy outage constraint of the primary node, and time allocated to the secondary nodes decreases. Meanwhile, the utility obtained by the primary node increases, since there is a higher number of transmission opportunities left for the primary node.

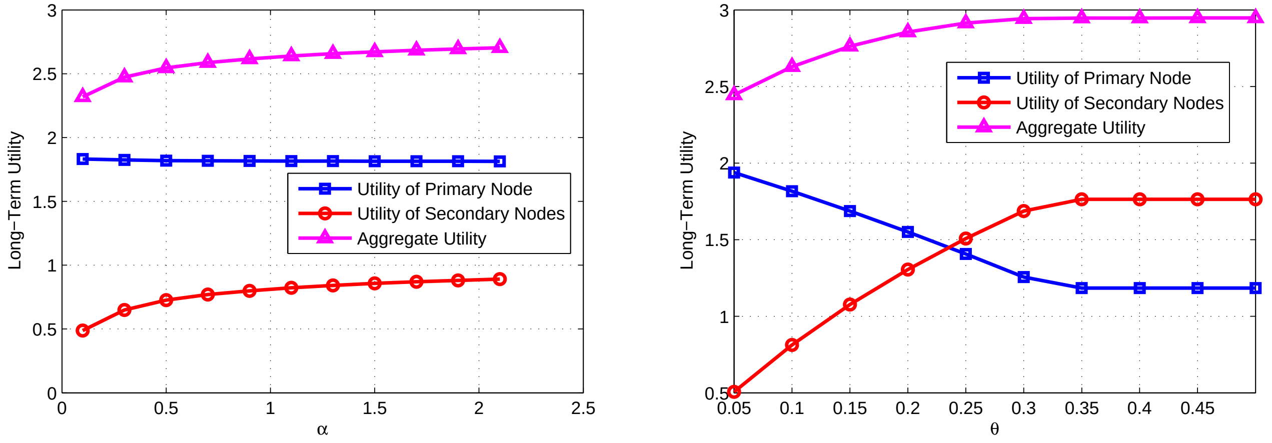
In Fig. 6.5a, we investigate the effect of the power constraint of the secondary nodes, α_i. As expected, the utility of the secondary nodes increasing with α_i, since they can use more power on each of their transmissions. After $\alpha_i = 1$, the power constraint becomes inactive, since the constraint is realized with strict inequality. Fig. 6.5b, we analyzed the effect of θ_i, which can be interpreted as scale parameter of time allocation constraint with jamming power transmitted by the secondary nodes. In Fig. 6.5b, we observed that after $\theta_i = 0.35$, the utilities converges since the time allocation constraint of the secondary nodes becomes inactive, and realized with strict inequality. Meanwhile, the utility obtained by the the primary node decreases, since less time slots



(a) V vs Long-Term Utility

(b) γ vs Long-Term Utility

Figure 6.4: Performance evaluation with respect to V and γ_i

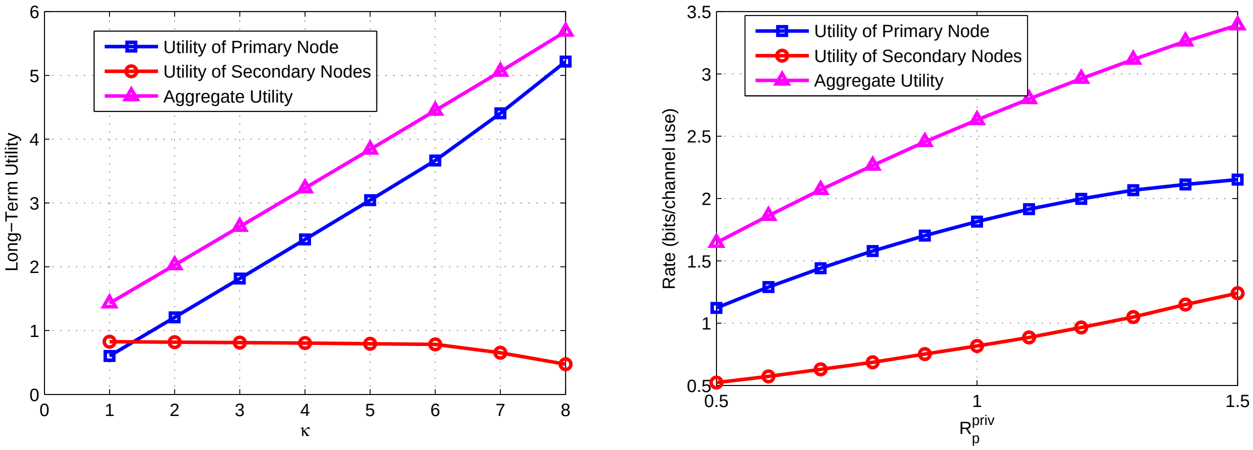


(a) α vs Long-Term Utility

(b) θ vs Long-Term Utility

Figure 6.5: Performance evaluation with respect to α_i and θ_i

is left for the transmission of the primary node.



(a) κ vs Long-Term Utility

(b) $\hat{R}_p^{\text{priv}}$ vs Long-Term Utility

Figure 6.6: Performance evaluation with respect to κ and $\hat{R}_p^{\text{priv}}$

We next analyze the effect of κ, which can also be interpreted as the ratio of utilities of primary and secondary nodes' transmissions taking place at the same rate. Fig. 6.6a shows that utility obtained by the primary node increases with the increasing κ. Meanwhile, the utility of the secondary nodes decreases. The reason is that with increasing κ, the algorithm gives priority to the transmission of the primary node, and the transmissions of the secondary nodes takes place in a small number of time slots. Fig. 6.6b depicts the effect of $\hat{R}_p^{\text{priv}}$. We first notice that, long-term utility of the primary node increases with increasing $\hat{R}_p^{\text{priv}}$, since the primary node sends a larger amount of private information for each encoded message. It is interesting to note that long-term utilities increases with increasing $\hat{R}_p^{\text{priv}}$. The reason is that with higher $\hat{R}_p^{\text{priv}}$, the private information is encoded with less randomization rate, and the eavesdropper needs to obtain less information to interfere the private information. Thus, the secondary nodes transmit more jamming power to confuse the eavesdropper, and in return, they gain higher number of opportunities for their own transmissions.

6.5 Chapter Summary

In this chapter, we have proposed a dynamic solution for enhancing secret communications in wireless channel with a non-altruistic jammer where secondary users help a primary user to enhance secrecy against an intelligent and passive eavesdropper. Assuming that the transmitters only know their channel to the legitimate receiver and has statistical CSI on their channel to eavesdropper, we have formulated and solved a network utility maximization problem. Simulation results are presented to verify the performance.

Chapter 7

Conclusions and Future Work

In this thesis, we have studied resource allocation problem for various network topologies in which information-theoretic secrecy is incorporated as QoS requirement. Specifically, the joint scheduling and flow control algorithms developed in the first part of the thesis including chapter 3 and chapter 4 are for wireless cellular networks in which all nodes in the network are considered as internal eavesdroppers from which the confidential information needs to be protected. In chapter 5 and chapter 6, we have designed dynamic control algorithms for wireless multi-hop and cognitive radio networks, respectively.

In chapter 3, we have obtained the achievable confidential and open information rate regions of single- and multi-user wireless networks with node scheduling. We have proved that confidential opportunistic scheduling along with a secrecy encoding strategy maximizes the sum confidential information rate for both multiuser uplink and downlink communication when perfect CSI is available for only the main uplink channels. Then, through Lyapunov optimization technique, we developed optimal joint scheduling and flow control policies that achieve maximum aggregate utility and provide fairness among users. The proposed algorithm is based on simple index policies, and thus it is easily implementable without imposing high overhead in the network. Then, we have considered imperfect CSI case, in which the cross-channel gains are estimated with some error. Here, we have slightly revised the problem by imposing a secrecy outage constraint, and developed provably optimal algorithm. In chapter 4, we have developed dynamic control algorithm without an instantaneous CSI. To provide reliable communication, we used HARQ transmission with incremental redundancy. Here, we have proposed a new achievable rate region with HARQ and showed that it is equal to its conventional counterpart in which a message is transmitted until it is successfully decoded by the base station. Based on the proposed achievable rate region, we have designed a NUM problem and obtained a cross-layer algorithm. Through Lyapunov optimization framework, our cross-layer algorithm is provably optimal, i.e., maximizes the aggregate utility.

In chapter 4, we have considered the problem of resource allocation in wireless multihop networks where sources have confidential information to be transmitted to their corresponding destinations with the help of intermediate nodes. We have proposed a end-to-end encoding scheme to provide confidentiality from intermediate nodes, which makes use of time-varying nature of wireless links. First, we have obtained the achievable rate region based on the end-to-end scheme given scheduling and routing decisions. Then, we have designed a dynamic control algorithm, which gives scheduling decision to maximize the aggregate utility for a given encoding rate. The interesting result here is that increasing the flow rate and keeping confidentiality is two conflicting objective unlike standard dynamic algorithms, and the proposed algorithm also considers spatial distribution of the flows over each path. The reason is that to increase the flow rate, nodes should transmit the messages over the best available channel, but by using the same path over long durations, intermediate nodes along this path obtain more information, and decreases the confidentiality. Next, we consider the system with delay constraint, i.e., the messages are encoded over finite number of blocks. For this system, transmissions of each block of the same message are dependant with each other. Thus, we propose a sub-optimal algorithm, and show that the proposed algorithm approaches the optimal solution as the number of blocks which the message are encoded, increases. Finally, in chapter 5, we have designed a dynamic network control in cognitive radio network, in which primary node transmits its confidential message in the presence of a passive eavesdropper, and secondary users help a primary user to enhance secrecy of transmitted message. Here, we have designed two problems: In the first problem, we aim to minimize jamming powers of the secondary nodes with a secrecy outage constraint of the primary node. In the second problem, based on the optimal jamming power allocation, we have introduced a NUM problem, and solved it by using Lyapunov optimization framework.

We now present some ideas which will motivate future studies on this topic. We generally assume a centralized scheduler, but the complexity of the scheduling algorithms increases as the number of nodes in the network increases. Hence, designing distributed algorithms will be an interesting research direction along this topic. Note that, we have designed a distributed scheduling algorithm in chapter 5 for multi-hop communication. However, we could not provide performance bounds of the proposed distributed scheduling algorithm. Thus, we will provide theoretical analysis of the scheduling algorithms in wireless secure network. In addition, eavesdroppers are assumed to be passive (they only listen the transmissions). An advanced attack might include active eavesdroppers, which can jam the wireless channel. Securing information and designing dynamic algorithms in such scenarios is an interesting avenue for further research.

In chapter 5, we have designed provably optimal algorithm when the message are encoded across arbitrarily large blocks, i.e., the delay of the message is infinite. As the future work, we will provide an optimal dynamic algorithm when the delay of the message is finite, and theoretically analyze the trade-off between the optimal rate and delay. For the cognitive radio networks, we will analyze the general problem where multiple primary nodes and eavesdroppers are present in the network. In this case, primary nodes will compete each other to buy jamming power from secondary nodes, and need a game-theoretic formulation to obtain optimal jamming power of the secondary nodes. Also, it will be an interesting direction to extend our works for the multichannel wireless system, i.e., OFDM networks.

Bibliography

[1] C. Boyd, *Cryptography and Coding*, H. Beker and F. Piper, Eds. Oxford, UK: Clarendon Press, 1989.

[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Tech. J.*, vol. 28, pp. 656–715, Oct. 1949.

[3] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1380, Oct. 1975.

[4] I. Csiszar and J. Körner, "Broadcast channels with confidential messages," vol. 24, no. 3, pp. 339–348, May 1978.

[5] S. L. Y. Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[6] L. Georgiadis, M. J. Neely, and L. Tassiulas, "Resouce allocation and cross-layer control in wireless networks," *Foundations and Trends in Networking*, vol. 1, no. 1, pp. 1–144, 2006.

[7] M. J. Neely and R. Urgaonkar, "Optimal backpressure routing for wireless networks with multi-user diversity," *Proc. Conf. Info. Sci. Sys.*, pp. 18–25, Jan. 2006.

[8] T. Girici and A. C. Kazez, "Energy efficient routing with mutual information accumulation," *Proc. Intl. Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks*, pp. 425–430, May 2012.

[9] A. K. Karmokar, D. V. Djonin, and V. K. Bhargava, "Cross-Layer Rate and Power Adaptation Strategies for IR-HARQ Systems over Fading Channels with Memory: A SMDP-Based Approach," *IEEE Trans. on Communications*, vol. 56, no. 8, pp. 1352–1365, Aug. 2008.

[10] P. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[11] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Intl. Symposium on Information Theory*, Seattle, WA, July 2006, pp. 356–360.

[12] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[13] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[14] L. Lai, H. El Gamal, and H. V. Poor, "The wiretap channel with feedback: Encryption over the channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 11, pp. 5059 – 5067, Nov. 2008.

[15] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y. Kim, "The secrecy capacity of the wiretap channel with rate-limited feedback," *IEEE Trans. Inf. Theory*, 2009, to appear.

[16] D. Gunduz, R. Brown, and H. V. Poor, "Secret communication with feedback," in *Proc. IEEE Intl. Symposium on Information Theory and its Applications*, Auckland, New Zealand, Dec. 2008.

[17] U. M. Maurer and S. Wolf, "Secret key agreement over a non-authenticated channel - Part I: Definitions and bounds," *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 822–831, Apr. 2003.

[18] ——, "Secret key agreement over a non-authenticated channel - Part II: The simulatability condition," *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 832–838, Apr. 2003.

[19] ——, "Secret key agreement over a non-authenticated channel - Part III: Privacy amplification," *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 839–851, Apr. 2003.

[20] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, 2009, to appear.

[21] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, Oct. 2007, submitted.

[22] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033 – 4039, Sept. 2009.

[23] R. Liu and H. V. Poor, "Secrecy capacity region of a multi-antenna Gaussian broadcast channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 1235–1249, Mar. 2009.

[24] E. Tekin and A. Yener, "The general gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, June 2008.

[25] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sept. 2008.

[26] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747 – 5755, Dec. 2008.

[27] Y. Liang and H. V. Poor, "Multiple access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[28] A. Khisti, A. Tchamkerten, and G. W. Wornell, “Secure broadcasting over fading channels,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, June 2008.

[29] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[30] Z. Li, R. Yates, and W. Trappe, “Secure communication over wireless channels,” in *Proc. Information Theory and Application Workshop*, La Jolla, CA., Jan. 2007.

[31] O. Simeone and A. Yener, “The cognitive multiple access wire-tap channel,” in *Proc. Conf. on Information Science and Systems*, Baltimore, MD, Mar. 2009.

[32] P. Parada and R. Blahut, “Secrecy capacity of SIMO and slow fading channels,” in *Proc. IEEE Intl. Symposium on Information Theory*, Adelaide, Australia, Sep. 2005, pp. 2152–2155.

[33] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic, “The discrete memoryless multiple access channel with confidential messages,” in *Proc. IEEE Intl. Symposium on Information Theory*, Seattle, WA, July 2006, pp. 957–961.

[34] Y. Oohama, “Relay channels with confidential messages,” *IEEE Trans. Inf. Theory*, Nov. 2006, submitted.

[35] E. Ekrem and S. Ulukus, “The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.

[36] M. Yuksel, X. Liu, and E. Erkip, “A secure communication game with a relay helping the eavesdropper,” in *Proc. IEEE Information Theory Workshop*, Taormina, Italy, Oct. 2009.

[37] E. Tekin and A. Yener, “The relay-eavesdropper channel: Cooperation for secrecy,” *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[38] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. on Signal Processing*, vol. 58, no. 3, pp. 4033–4039, March 2010.

[39] G. Zheng, L. Choo, and K. Wong, "Optimal Cooperative Jamming to Enhance Physical Layer Security Using Relay," *IEEE Trans. on Signal Processing*, vol. 59, no. 3, March 2011.

[40] Y. Liang, G. Kramer, H. Poor, and S. Shamai, "Compound wire-tap channels," *in Proc. of the Allerton Conf. on Commun., Control and Computing, Allerton*, 2007.

[41] T. Liu, V. Prabhakaran, and S. Vishwanath, "The secrecy capacity of a class of parallel gaussian compound wiretap channels," *in Proc. of the IEEE Int. Symposium on Inform. Theory*, Jul. 2008.

[42] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "On the Throughput of Secure Hybrid-ARQ Protocols for Gaussian Block-Fading Channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1575–1591, March 2009.

[43] R. Liu, Y. Liang, H. V. Poor, and P. Spasojevic, "Secure nested codes for type II wiretap channels," in *Proc. IEEE Information Theory Workshop*, Lake Tahoe, CA, Sep. 2-6 2007.

[44] M. Bloch, A. Thangaraj, S. W. McLaughlin, and J.-M. Merolla, "LDPC based secret key agreement over the gaussian wiretap channel," in *Proc. IEEE Intl. Symposium on Information Theory*, Seattle, WA, July 2006, pp. 1179 – 1183.

[45] E. Peron, "Information-theoretic secrecy for wireless networks," Ph.D. dissertation, Ecole polytechnique fdrale de Lausanne(EPFL), 2009.

[46] E. Perron, S. Diggavi, and E. Telatar, "On cooperative wireless network secrecy," in *Proc. IEEE Conf. Computer Communications (Infocom)*, vol. 4, Rio de Janeiro, Brazil, Sep. 2009, pp. 1935–1943.

[47] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, “On secrecy capacity scaling in wireless networks,” *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3000–3015, May 2012.

[48] C. Capar, D. Goeckel, B. Liu, and D. Towsley, “Secret communication in large wireless networks without eavesdropper location information,” in *Proc. IEEE Conf. Computer Communications (Infocom)*, Orlando, FL, March 2012, pp. 1152–1160.

[49] A. Shamir, “How to share a secret,” *Commun. ACM*, vol. 22, pp. 612–613, Nov. 1979.

[50] W. Lou, W. Liu, and Y. Fang, “Spread: enhancing data confidentiality in mobile ad hoc networks,” in *Proc. IEEE Conf. Computer Communications (Infocom)*, March 2004, pp. 2404–2413.

[51] N. Cai and R. Yeung, “Secure network coding,” in *Proc. IEEE Intl. Symposium on Information Theory*, Lausanne, Switzerland, June 2002, p. 323.

[52] J. Feldman, T. Malkin, R. Servedio, and C. Stein, “On the capacity of secure network coding,” in *Proc. Allerton Conf. on Communication, Control, and Computing*, Monticello, IL, Sep. 2004.

[53] T. Cui, T. Ho, and J. Kliewer, “On secure network coding with nonuniform or restricted wiretap sets,” *IEEE Trans. Inf. Theory*, vol. 59, no. 1, pp. 166–176, Jan. 2013.

[54] L. Tassiulas and A. Ephremides, “Jointly optimal routing and scheduling in packet ratio networks,” *IEEE Transactions on Information Theory*, vol. 38, no. 1, pp. 165 –168, Jan. 1992.

[55] X. Liu, E. K. P. Chong, and N. B. Shroff, “A framework for opportunistic scheduling in wireless networks,” *Computer Networks*, vol. 41, no. 4, pp. 451–474, 2003.

[56] J. Huang, V. Subramanian, R. Agrawal, and R. Berry, "Downlink scheduling and resource allocation for ofdm systems," *IEEE Transactions on Wireless Communications*, vol. 8, no. 1, pp. 288 –296, 2009.

[57] R. Urgaonkar and M. J. Neely, "Opportunistic scheduling with reliability guarantees in cognitive radio networks," *IEEE Trans. Mob. Comput.*, vol. 8, no. 6, pp. 766–777, 2009.

[58] J. Jaramillo and R. Srikant, "Optimal scheduling for fair resource allocation in ad hoc networks with elastic and inelastic traffic," *IEEE/ACM Trans. on Networking*, vol. 19, no. 4, pp. 1125–1136, Aug. 2011.

[59] A. Stolyar, "Greedy primal-dual algorithm for dynamic resource allocation in complex networks," *Queueing Systems*, vol. 54, pp. 203–220, 2006, 10.1007/s11134-006-0067-2. [Online]. Available: http://dx.doi.org/10.1007/s11134-006-0067-2

[60] S. Shakkottai and A. Stolyar, "Scheduling for multiple flows sharing a time varying channel: the exponential rule," *in Analytic Methods in Applied Probability*, vol. 207, pp. 185–202, 2003.

[61] B. Sadiq, S. Baek, and G. de Veciana, "Delay-optimal opportunistic scheduling and approximations: the log rule," Apr. 2009.

[62] M. Andrews, K. Kumaran, K. Ramanan, A. Stolyar, R. Vijayakumar, and P. Whiting, "Scheduling in a queueing system with asynchronously varying service rates," *in Probability in the Engineering and Informational Sciences*, vol. 18, no. 2, p. 245, 2004.

[63] P. P. Bhattacharya, L. Georgiadis, P. Tsoucas, and I. Viniotis, "Adaptive lexicographic optimization in multi-class m/gi/1 queues," *Mathematics of Operations Research*, vol. 18, no. 3, pp. 705–740, 1993.

[64] I. Keslassy and N. McKeown, “Analysis of scheduling algorithms that provide 100 percent throughput in input-queued switches,” *in Proceedings of the 39th Annual Allerton Conf. on Communication, Control, and Computing*, Oct. 2001.

[65] E. Leonardi, M. Mellia, F. Neri, and M. A. Marsan, “Bounds on average delays and queue size averages and variances input-queued cell-based switches,” pp. 1095–1103, 2001.

[66] V. A. N. McKeown, A. Mekkittikul and J. Walrand, “Achieving 100 percent throughput in an input-queued switch,” vol. 47, no. 8, pp. 1260–1267, Aug. 1999.

[67] P. R. Kumar and S. P. Meyn, “Stability of queueing networks and scheduling policies,” *IEEE Transactions on Automatic Control*, vol. 40, no. 251–260, 1995.

[68] L. Tassiulas and A. Ephremides, “Dynamic server allocation to parallel queues with randomly varying connectivity,” *IEEE Trans. Inf. Theory*, vol. 39, no. 2, pp. 466–478, Mar. 1993.

[69] M. Andrews, K. Kumaran, K. Ramanan, A. Stolyar, and P. Whiting, “Providing quality of service over a shared wireless link,” *IEEE Communications Magazine*, vol. 39, no. 2, pp. 150–154, 2001.

[70] , “Power allocation and routing in multibeam satellites with time-varying channels,” *IEEE/ACM Trans. on Networking*, vol. 11, pp. 138–152, Feb. 2001.

[71] F. P. Kelly, A. K. Maulloo, and D. K. H. Tan, “Rate Control for Communication Networks: Shadow Prices, Proportional Fairness and Stability,” *The Journal of the Operational Research Society*, vol. 49, no. 3, pp. 237–252, 1998. [Online]. Available: http://dx.doi.org/10.2307/3010473

[72] S. H. Low and D. E. Lapsley, “Optimization flow control-i: basic algorithm and convergence,” *IEEE/ACM Trans. Netw.*, vol. 7, no. 6, pp. 861–874, 1999.

[73] X. Wang and K. Kar, “Cross-layer rate control for end-to-end proportional fairness in wireless networks with random access,” in *MobiHoc*, 2005, pp. 157–168.

[74] M. J. Neely, E. modiano, and C. E. Rohrs, "Dynamic power allocation and routing for time varing wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 1, pp. 89–103, Jan. 2005.

[75] M. J. Neely, "Energy optimal control for time-varying wireless networks," *IEEE Trans. Inf. Theory*, vol. 52, no. 7, pp. 2915–2934, July 2006.

[76] R. A. Berry and R. Gallager, "Communication over fading channels with delay constraints," *IEEE Trans. Inf. Theory*, vol. 48, pp. 1135–1148, May 2002.

[77] M. J. Neely, "Optimal energy and delay tradoffs for multi-user wireless downlinks," *IEEE Trans. Inf. Theory*, vol. 53, no. 9, pp. 3095–3113, Sept. 2007.

[78] ——, "Order optimal delay for opportunistic scheduling in multiuser wireless uplinks and downlinks," *IEEE/ACM Trans. on Networking*, vol. 16, no. 5, pp. 1188–1199, Oct. 2008.

[79] L. B. Le, K. Jagannathan, and E. Modiano, "Delay analysis of maximum weight scheduling in wireless ad hoc networks," *in Proc. CISS*, pp. 389–394, Mar. 2009.

[80] W. Khan, L. B. Le, and E. Modiano, "Autonomous routing algorithms for networks with wide-spread failures," *in Proc. IEEE MILCOM*, pp. 1–6, Oct. 2009.

[81] M. Neely, "Delay analysis for maximal scheduling inwireless networks with bursty traffic," pp. 385–393, 2008.

[82] G. R. Gupta and N. B. Shroff, "Delay analysis for multi-hop wireless networks," pp. 2356–2364, 2009.

[83] L. Ying, S. Shakkottai, and A. Reddy, "On combining shortest-path and back-pressure routing over multihop wireless networks," pp. 1674–1684, 2009.

[84] L. Bui, R. Srikant, and A. Stolyar, "Novel architecture and algorithms for delay reduction in back-pressure scheduling and routing," pp. 2936–2940, 2009.

[85] R. Li, L. Ying, A. Eryilmaz, and N. B. Shroff, "A unified approach to optimizing performance in networks serving heterogeneous flows," pp. 253–261, 2009.

[86] M. Neely, "Delay-based network utility maximization," pp. 1–9, 2010.

[87] C. Luo, F. R. Yu, H. Ji, and V. C. Leungr, "Optimal channel access for tcp performance improvement in cognitive radio networks," *Wireless Networks*, vol. 17, pp. 479–492, Feb. 2011.

[88] R. Urgaonkar and M. J. Neely, "Opportunistic scheduling with realibility guarantees in cognitive radio networks," pp. 253–261, 2009.

[89] M. Karaca, K. Khalil, E. Ekici, and O. Ercetin, "Optimal scheduling and power allocation in cooperate-to-join cognitive radio networks," *IEEE/ACM Trans. on Networking*, vol. 21, no. 6, pp. 1708–1721, Feb. 2011.

[90] L. Xiang and K. Kar, "Dynamic channel assignment and power allocation in multichannel wireless networks with per-user bandwidth guarantees." *Proc. Intl. Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks*, pp. 377–382, 2011.

[91] Y. Yang, B. Yang, and X. Guan, "Pricing-based cross-layer scheduling and energy management over ofdm downlink networks," pp. 1538–1543, Jun. 2013.

[92] M. V. Nguyen, C. S. Hong, and S. Lee, "Cross-layer optimization for congestion and power control in ofdm-based multi-hop cognitive radio networks," *IEEE/ACM Trans. on Networking*, vol. 60, no. 8, pp. 2101–2112, Aug. 2012.

[93] ——, "Joint rate adaption, power control, and spectrum allocation in ofdma-based multi-hop crns," vol. 96, no. 1, pp. 242–253, Jan. 2013.

[94] R. Knopp and P. A. Humblet, "Information capacity and power control in single-cell multiusercommunications," in *Proc. IEEE Intl. Conf. on Communication*, vol. 1, Seattle, WA, Jun. 18-22, 1995, pp. 331–335.

[95] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[96] C. E. Koksal and O. Ercetin, "Control of wireless networks with secrecy," Technical Report, 2010, http://arxiv.org/abs/cs/1101.3444.

[97] L. Georgiadis, M. J. Neely, and L. Tassiulas, "Resource allocation and cross-layer control in wireless networks," *Foundations and Trends in Networking*, vol. 1, no. 1, 2006.

[98] M. J. Neely, "Energy optimal control for time-varying wireless networks," *IEEE Transactions on Information Theory*, vol. 52, no. 7, pp. 2915–2934, 2006.

[99] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication.* New York: Cambridge University Press, 2005.

[100] P. Frenger, "Turbo decoding for wireless systems with imperfect channel estimates," vol. 48, no. 0, pp. 1437–1440, 2000.

[101] C. E. Koksal and P. Schniter, "Robust rate-adaptive wireless communication using ack/nak-feedback," *IEEE Trans. on Signal Processing*, 2012, to appear.

[102] Y. Sun, C. E. Koksal, S. J. Lee, and N. B. Shroff, "Network control without csi using rateless codes for downlink cellular systems." in *Proc. IEEE Conf. Computer Communications (Infocom)*, Turin, Italy, 2013.

[103] H. T. Zheng and H. Viswanathan, "Optimizing the ARQ performance in downlink packet data systems with scheduling," *IEEE Trans. on Wireless Communications*, vol. 4, pp. 495–506, Mar. 2005.

[104] M. Assaad and D. Zeghlache, "Cross-Layer design in HSDPA system to reduce the TCP effect," *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 614–625, Mar. 2006.

[105] J. Huang, R. A. Berry, and M. L. Honig, "Wireless scheduling with hybrid arq," *IEEE Trans. on Wireless Communications*, vol. 4, no. 6, pp. 2801–2810, Nov. 2005.

[106] S. Lin, J. D. J. Costello, and M. J. Miller, "Automatic-repeat-request error control schemes," *IEEE Communications Magazine*, vol. 22, pp. 5–16, Dec. 1984.

[107] J. Yang, Y. Liu, and S. C. Draper, "Optimal scheduling policies with mutual information accumulation in wireless networks." in *Proc. IEEE Conf. Computer Communications (Infocom)*, 2012, pp. 1062–1070.

[108] D. P. Palomar and M. Chiang, "A Tutorial on Decomposition Methods for Network Utility Maximization," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 8, pp. 1439–1451, June 2007.

[109] S. Boyd and L. Vandenberghe, *Convex Optimization.* New York, NY: Cambridge University Press, 2004.

[110] D. P. Bertsekas and J. N. Tsitsiklis, *Parallel and Distributed Computation: Numerical Methods.* Upper Saddle Rive, NJ: Prentice-Hall, 1989.

[111] Y. Liang and H. V. Poor, "Generalized multiple access channels with confidential messages," in *Proc. IEEE Intl. Symposium on Information Theory*, Seattle, WA, July 2006, pp. 952–956.

[112] X. Lin and N. B. Shroff, "Utility maximization for communication networks with multipath routing," *IEEE Trans. on Automatic Control*, vol. 51, no. 5, pp. 766–781, May 2006.

[113] Y. Chen, R. Hwang, and Y. Lin, "Multipath qos routing with bandwidth guarantee," in *Proc. IEEE Global Telecommunications Conf.*, vol. 4, Sep. 2001.

[114] A. E. Gamal and K. Young-han, *Network Information Theory.* Cambridge University Press, 2011.

[115] A. Eryilmaz, R. Srikant, and J. R. Perkins, "Stable scheduling policies for fading wireless channels," *IEEE Trans. Inf. Theory*, vol. 13, no. 2, pp. 411–424, Apr. 2005.

[116] S. Sanghavi, D. Shah, and A. Willsky, "Message-passing for maximum weight independent set," *IEEE Trans. Inf. Theory*, vol. 55, no. 11, pp. 4822–4834, Nov. 2009.

[117] J. Hoepman, "Simple distribute weighted matchings," Oct. 2004, available at http://arxiv.org /abs/cs/0410047.

[118] I. Stanojev and A. Yener, "Cooperative jamming via spectrum leasing," in *Proc. Intl. Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks*, Princeton, NJ, May 2011, pp. 265–272.

[119] Y. Sarikaya, O. Ercetin, and O. Gurbuz, "Dynamic control for cooperative jamming with a non-altruistic node." in *Communications and Network Security (CNS)*, National Harbor, MD, 2013, pp. 381–382.

[120] S. Luo, J. Li, and A. Petropulu, "Outage constrained secrecy rate maximization using cooperative jamming," *IEEE Statistical Signal Processing Workshop (SSP)*, pp. 389–392, Aug. 2012.

[121] K. Smaili, T. Kadri, and S. Kadry, "Hypoexponential Distribution with Different Parameters," *Applied Mathematics*, vol. 4, no. 4, pp. 624–631, Apr. 2013.

[122] A. R. Horn and R. C. Johnson, *Matrix Analysis.* Cambridge University Press, 1990.