University of Saskatchewan

Game-Theoretic Relay Selection and Power Control in Fading Wireless Body Area Networks

by

Hussein Moosavi

A thesis submitted in partial fulfillment for the
degree of Master of Science

in the

College of Graduate Studies and Research
Department of Electrical and Computer Engineering

Permission to Use

In presenting this thesis in partial fulfillment of the requirements for a Postgraduate degree from the University of Saskatchewan, it is agreed that the Libraries of this University may make it freely available for inspection. Permission for copying of this thesis in any manner, in whole or in part, for scholarly purposes may be granted by the professors who supervised this thesis work or, in their absence, by the Head of the Department of Electrical and Computer Engineering or the Dean of the College of Graduate Studies and Research at the University of Saskatchewan. Any copying, publication, or use of this thesis, or parts thereof, for financial gain without the written permission of the author is strictly prohibited. Proper recognition shall be given to the author and to the University of Saskatchewan in any scholarly use which may be made of any material in this thesis.

Request for permission to copy or to make any other use of material in this thesis in whole or in part should be addressed to:

Head of the Department of Electrical and Computer Engineering
57 Campus Drive
University of Saskatchewan
Saskatoon, Saskatchewan, Canada
S7N 5A9

University of Saskatchewan

Abstract

College of Graduate Studies and Research
Department of Electrical and Computer Engineering

Master of Science

by Hussein Moosavi

The trend towards personalized ubiquitous computing has led to the advent of a new generation of wireless technologies, namely wireless body area networks (WBANs), which connect the wearable devices into the Internet-of-Things.

This thesis considers the problems of relay selection and power control in fading WBANs with energy-efficiency and security considerations.

The main body of the thesis is formed by two papers. Ideas from probability theory are used, in the first paper, to construct a performance measure signifying the energy efficiency of transmission, while in the second paper, information-theoretic principles are leveraged to characterize the transmission secrecy at the wireless physical layer (PHY).

The hypothesis is that exploiting spatial diversity through multi-hop relaying is an effective strategy in a WBAN to combat fading and enhance communication throughput.

In order to analytically explore the problems of optimal relay selection and power control, proper tools from game theory are employed. In particular, non-cooperative game-theoretic frameworks are developed to model and analyze the strategic interactions among sensor nodes in a WBAN when seeking to optimize their transmissions in the uplink.

Quality-of-service (QoS) requirements are also incorporated into the game frameworks, in terms of upper bounds on the end-to-end delay and jitter incurred by multi-hop transmission, by borrowing relevant tools from queuing theory.

The proposed game frameworks are proved to admit Nash equilibria, and distributed algorithms are devised that converge to stable Nash solutions.

The frameworks are then evaluated using numerical simulations in conditions approximating actual deployment of WBANs. Performance behavior trade-offs are investigated in an IEEE 802.15.6-based ultra wideband WBAN considering various scenarios. The frameworks show remarkable promise in improving the energy efficiency and PHY secrecy of transmission, at the expense of an admissible increase in the end-to-end latency.

Acknowledgments

I would like to express my gratitude to my supervisor, Prof. Francis Bui, whose fastidious approach, expertise, and understanding added immensely to my graduate experience. I appreciate his support throughout my Master's degree program without which this thesis would never have been possible.

I must acknowledge the other members of my thesis committee, Prof. Eric Salt and Prof. Ha Nguyen from the Dept. of Electrical and Computer Engineering, and Prof. Michael Horsch from the Dept. of Computer Science, for examining this thesis and for their insightful comments.

I would also like to thank my family for their constant support and encouragement. I doubt that I will ever be able to convey my appreciation fully.

Contents

List of Figures

Abbreviations

2TE	**2**-hop **T**opology **E**xtension
ASR	**A**chievable **S**ecrecy **R**ate
BAN	**B**ody **A**rea **N**etwork
CP	**C**ontention **P**robability
CSI	**C**hannel **S**tate **I**nformation
CSMA/CA	**C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **A**voidance
DBPSK	**D**ifferentially encoded **B**inary **P**hase **S**hift **K**eying
DT	**D**irect **T**ransmission
DTPC	**D**irect **T**ransmission with **P**ower **C**ontrol
IR-UWB	**I**mpulse **R**adio **U**ltra **W**ide **B**and
MANET	**M**obile **A**d-hoc **N**etwork
MAC	**M**edium **A**ccess **C**ontrol
MTFG	**M**ulti-hop **T**opology **F**ormation **G**ame
PHY	**PHY**sical layer
POP	**P**acket **O**utage **P**robability
QoS	**Q**uality **o**f **S**ervice
RSPCG	**R**elay **S**election and **P**ower **C**ontrol **G**ame
SNR	**S**ignal to **N**oise **R**atio
SOP	**S**ecrecy **O**utage **P**robability
ST	**S**tar **T**opology
WBAN	**W**ireless **B**ody **A**rea **N**etwork
WSN	**W**ireless **S**ensor **N**etwork

To Mom and Dad,
"who took me to the library."

Chapter 1

Introduction

The rapid growth in micro- and nano-technology physiological sensors, intelligent integrated circuits, and low-power wireless communication have enabled a new generation of wireless sensor networks that measure the physiological and contextual data profiling the human body activities. A wireless body area network (WBAN), also referred to as a body area network (BAN), is a network of computing devices which enables wireless data communication around the human body.

A WBAN typically consists of several sensor/actuator nodes that collect various physiological changes of the human body, together with a central network coordinator called a hub, to which the sensors wirelessly communicate the collected vital signs for monitoring purposes. The sensor nodes may be located in the proximity of the body, placed on the body surface, implanted inside the human body, or even in the blood stream [1, 2].

WBAN technology is an interdisciplinary area which facilitates inexpensive and continuous health monitoring, computer-assisted rehabilitation, and early detection of medical conditions, with real-time updates of medical records through the Internet.

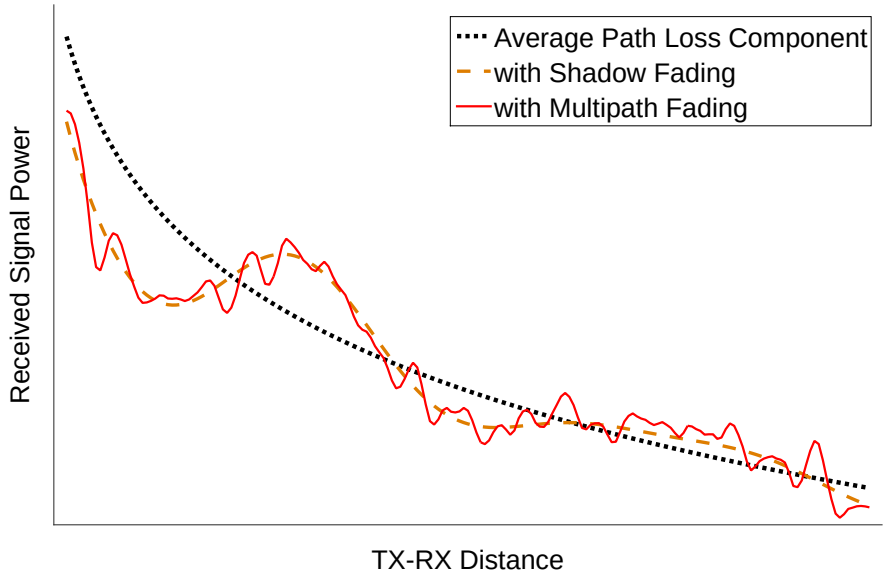

FIGURE 1.1: Changes in the received signal power in a WBAN due to body motion

1.1 Challenges

Demanding operating conditions and fundamental resource constraints in WBANs render many traditional wireless sensor network (WSN) solutions inappropriate, if not obsolete, for these networks [2, 3].

Although WBANs are similar to mobile ad hoc networks (MANETs) in the sense that their topology changes with group-based movement rather than node-based movement, a WBAN has more frequent topology changes and a higher moving speed. Moreover, small lightweight sensor devices in a WBAN have more strict energy constraints compared to conventional WSNs, especially in terms of transmit power. Node replacements, particularly for implant nodes, can be quite uncomfortable. But more importantly, the radio transmission in the vicinity of the human body is highly lossy and inefficient [4]. Fig. 1.1 illustrates the effects of the body motion on the signal power measured by a receiver node in a WBAN.

A radio signal experiences three major phenomena through the propagation channel before being received by the intended node [5, 6], as shown in Fig. 1.1:

- average path loss, caused by geometric signal spreading, which is proportional to the inverse-square distance between the TX-RX pair,
- large-scale fading due to shadowing, arising from the variation in the environment surrounding the body including the signal blockage caused by the movement of the body parts, and
- small-scale fading due to multipath, describing signal fluctuations within a small local area caused by motion-induced changes in the multiple propagation paths between the TX-RX pair.

While the path loss and shadow fading lead to only slow variations in signal power at the typical body motion speeds, multipath can cause rapid fluctuations in the amplitude and phase of the received signal as signal propagation paths change due to motion.

Other unique challenges posed by the WBAN application scenarios include complex and unpredictable variation in channel conditions, low radio transmission range, temperature rise and interference, and heterogeneous data collection from different sensors with different sampling rates [3].

1.2 Problem Statement

Energy efficiency and security are among the most vexing issues in WBANs. Small lightweight sensor devices in a WBAN have scarce energy resources, and shadowing effects of the human body make the radio transmission in the vicinity of the body highly lossy and inefficient. Preserving energy at sensor nodes by adjusting transmit power is, therefore, increasingly crucial to prolong the lifetime of the WBAN.

Also the broadcast nature of the wireless medium leaves WBANs highly prone to eavesdropping and raises the probability of security lapses. For many networking applications, notably those in medical settings, a WBAN needs to handle data with stringent confidentiality and liability requirements, which makes the security of the communication links critical.

One effective strategy to combat fading and enhance the energy-efficiency and secrecy of wireless communications is to exploit spatial diversity through multi-hop relaying [7–12]. While the complexity involved in a star topology is relatively low, the quality of direct links between nodes and the hub generally deteriorates under severe fading conditions, and the nodes in a star architecture cannot react to such changes except by increasing their transmit power. In a multi-hop architecture, on the other hand, nodes can communicate with the hub through relay nodes which allows them to adapt to changes in the environment, thereby better performance.

Although the coordination of nodes in multi-hop communications increases complexity, this is not as significant an issue in WBANs as in other WSNs due to the small number of nodes in a WBAN. Also, most sensor nodes in WBANs are low rate sensors and the physiological signals usually can be sampled periodically, which imply that nodes can take turns sending the data with lower chances of colliding with one another. Therefore multi-hop architecture is even more feasible in WBANs [2, 13–16].

Furthermore, a comprehensive WBAN solution must take into account different conditions of operation and quality-of-service (QoS) constraints in WBANs. In particular, managing latency is of primary importance in WBANs, since the collected physiological and contextual data are generally required to be delivered to the hub in a timely manner. Especially when multi-hop transmission is considered, it introduces additional latency to the system, which makes latency management even more relevant.

Motivated by these developments, this thesis is dedicated to the design and development of analytical frameworks for latency-aware relay selection and power control in fading WBANs with energy-efficiency and security considerations.

1.3 Application Areas

Initial applications of WBANs are in the healthcare domain, especially for continuous monitoring and logging vital parameters of patients suffering from chronic diseases. WBAN

technologies, once widely adopted, are expected to be a breakthrough invention in healthcare, leading to concepts like telemedicine and mobile health becoming a practical reality.

For instance, a WBAN in place on a heart disease patient can alert the hospital, even before they have a heart attack, through measuring changes in their vital signs. Similarly, a WBAN on a diabetic patient could auto inject insulin through a pump, as soon as their insulin level declines.

In addition to enabling inexpensive and continuous health monitoring, body-centric wireless communications accommodate a wide variety of applications, such as fitness and sports, entertainment, and military.

Extending the technology to new areas could also assist communication by seamless exchanges of information between individuals, or between individual and machines.

1.4 Methodology

Instead of relying mainly on heuristic and ad hoc solutions, networking issues have recently been investigated analytically, especially to unravel the theoretical performance behaviors and expected requirements to design practical systems. Game theory—a field of applied mathematics dealing with multi-player strategic decision making—provides a bag of promising tools for such methodical analyses [17]. Game theory can be employed to model and analyze the interactions of agents in wireless communications and design frameworks based on the obtained analytical results. Decisions derived from such game-theoretic analyses help understand the underlying incentive mechanisms among the interacting agents, find the optimal network architectures, allocate limited resources, and balance perceived security risks. The emerging interest in studying wireless networking problems from a game-theoretic perspective is evident from the increasing number of publications in this field (see for example the survey papers [18–23] and the references therein).

This thesis applies a set of tools from non-cooperative game theory to explore the problem of optimal relay selection and power control in WBANs. Appropriate game models are formulated to describe the interaction among interested agents in a WBAN. Game players and strategy sets are identified, utility functions are characterized, and equilibrium behaviors are investigated.

Ideas and principles from probability theory and information theory are used to construct performance measures that characterize energy-efficiency and secrecy of transmission at the wireless physical layer (PHY) in fading WBANs.

Also, proper tools from queuing theory are employed to derive analytical expressions for end-to-end latency incurred by multi-hop transmission in a WBAN.

1.5 Background on Strategic Non-Cooperative Game Theory

The brief background provided here on strategic non-cooperative game theory is primarily taken from [17].

A strategic game is a model of interactive decision-making in which each player chooses his plan of action once and for all, and these decision are made simultaneously. Referring to the actions of the players as "simultaneous" does not necessarily mean that the actions are taken at the same point in time, but that no player is informed of the choice of others when choosing a plan of action.

A non-cooperative game is one in which players make decisions independently. Note that players may cooperate in a non-cooperative game, but cooperation must be self-enforcing rather than enforced through third parties.

A strategic non-cooperative game, denoted by $\langle \mathcal{N}, \{\mathcal{A}_n\}_{n\in\mathcal{N}}, \{\succsim_n\}_{n\in\mathcal{N}}\rangle$ or, if the qualifier $n \in \mathcal{N}$ is clear, simply by $\langle \mathcal{N}, \{\mathcal{A}_n\}, \{\succsim_n\}\rangle$, consists of a finite set $\mathcal{N}$ of players and, for each player n, a non-empty set $\mathcal{A}_n$ of actions and a preference relation $\succsim_n$.

A collection of all players' actions $\boldsymbol{a} = \{a_i\}_{i\in\mathcal{N}}$ is referred to as an action profile or an outcome. Note that for each player $n \in \mathcal{N}$, the preference relation $\succsim_n$ is defined on the set of outcomes $\mathcal{A} = \times_{i\in\mathcal{N}}\mathcal{A}_i$. The requirement that the preferences of each player n be defined over $\mathcal{A}$, rather than $\mathcal{A}_n$, means that each player may care not only about his own action but also about the actions taken by the others.

The preference relation of a player may simply reflect the player's feelings about the possible outcomes. Under a wide range of circumstances, the preference relation $\succsim_n$ of player n can be specified by a utility function $u_n : \mathcal{A} \to \mathbb{R}$ (also called a payoff function), in the sense that $u_n(\boldsymbol{a}) \geq u_n(\boldsymbol{a'})$ whenever $\boldsymbol{a} \succsim_n \boldsymbol{a'}$. The values of such a function are referred to as utilities (or payoffs). In the case that players' preference relations are represented by their corresponding utility functions, the game is denotes by $\langle \mathcal{N}, \{\mathcal{A}_n\}, \{u_n\}\rangle$.

The basic assumption that underlies game theory is that decision makers are rational, in the sense that they have clear preferences and chooses their actions deliberately after some process of optimization.

A solution is a systematic description of the outcomes that may emerge in a game. The most commonly used solution concept in non-cooperative game theory is that of Nash equilibrium.

Definition 1.1 (Nash Equilibrium)**.** For an outcome $\boldsymbol{a} = \{a_i\}_{i\in\mathcal{N}}$ and any $n \in \mathcal{N}$, let $\boldsymbol{a}_{-n}$ be the list $\{a_i\}_{i\in\mathcal{N}\setminus\{n\}}$ of actions of the outcome $\boldsymbol{a}$ for all players except n. A Nash equilibrium of a strategic game $\langle \mathcal{N}, \{\mathcal{A}_n\}, \{u_n\}\rangle$ is an outcome $\boldsymbol{a}^* \in \mathcal{A}$ with the property that for every player $n \in \mathcal{N}$ we have

$$u_n(\boldsymbol{a}^*_{-n}, a^*_n) \geq u_n(\boldsymbol{a}^*_{-n}, a_n) \qquad \forall a_n \in \mathcal{A}_n\textbf{.} \tag{1.1}$$

■

Therefore for $\boldsymbol{a}^*$ to be a Nash equilibrium it must be that no player n has an action yielding a utility that is greater than that generated when he chooses a^*_n, given that every

other player i chooses his equilibrium action a_i^*. In brief, no unilateral deviation is profitable for players, given the actions of the others.

1.6 Assumptions

The assumptions made in this study are as follows:

- The studied WBAN is based on IEEE 802.15.6, with the PHY, MAC layer, and security functions as defined in the standard. The network consists of a single hub and a number of sensor nodes.
- Game players (*i.e.*, legitimate sensor nodes) are rational (*i.e.*, they pursue well-defined exogenous objectives) and reason strategically (*i.e.*, they take into account their knowledge or expectations of other players' behavior).
- To be consistent with typical application scenarios, it is assumed that the players lack the complete information of the game. In particular, players only have statistical knowledge of the channels to their neighbors.
- In the uplink of a WBAN, each node has a single path that connects it to the hub. Therefore, the multi-hop network graph is in the form of a tree structure. Note that in many emerging wireless systems which involve communications over hierarchical architectures, tree-based communication is expected to be a central theme [24–28].

1.7 Scope and Limitations

While the developed frameworks are simulated and assessed under realistic WBAN conditions, empirical measurements are not conducted and is considered beyond the scope of this work. Instead, the focus of the research is on establishing the analytical frameworks

and assessing the performance behaviors for various generalized, albeit somewhat contrived, scenarios.

Due to the resource constraints of sensor nodes, complex game models may not be applicable to the considered problems. Also in development of algorithms to compute the equilibria, these resource constraints must be taken into account.

It also should be noted that WBANs span a wide spectrum of applications with different constraints and requirements. Therefore there is no single solution that is optimal for all applications.

1.8 Literature Review

The brief literature review provided here is twofold. First, recent applications of game theory for energy efficiency and security in general WSNs are reviewed. Then, the latest works concerning transmission energy efficiency and PHY security in WBANs are reported.

1.8.1 Game-Theoretic Approaches to Energy Efficient and Security in WSNs

Game theory has been used to address different issues of energy efficiency in WSNs.

In the context of energy harvesting WSNs, a game-theoretic approach has been taken to investigate the issue of efficient allocation of energy resources in the network (for example, from dedicated power nodes) among energy-harvesting sensor nodes [29, 30].

For mobile WSNs, the issue is to regulate mobility such that the nodes residual energy resources are used efficiently and the lifetime of the network is extended. This has been studied using game theory in [31].

Game theory also has been applied to study the distributed transmit power control in device-to-device wireless communication, for example in [32].

Similarly, game theory has been used for analytical investigation of different security issues in WSNs.

In security-sensitive WSN applications, optimal allocation of radio resources for security services is a pertinent issue. In [33] for example, allocation of network intrusion detection resources is studied through a game-theoretic approach. Another example is [34] where overhead management of the trust evaluation process is investigated using game theory.

Game theory has also been used for optimal exploitation of random characteristics of the wireless medium to achieve security at the physical layer in multiuser wireless settings, for example in [35].

1.8.2 Transmission Energy Efficiency and PHY security in WBANs

Among different energy efficiency issues of WSNs, transmit power control at sensor nodes is particularly relevant in WBANs, given the high radio transmission loss in the vicinity of human body and energy-constraints of small physiological sensor devices.

One approach to the problem is to form a capacitive body-coupled communication network among sensor nodes and use it in combination with radio frequency transmissions. This has been studied in [36] to combat body shadowing affects and reduce transmit power at the sensor nodes.

Also, channel state information (CSI) at the transmitter has been used to design power control mechanisms, for example in [37–39]. Such mechanisms aim at minimizing packet retransmissions at sensor nodes, and thereby reducing the unnecessary transmit energy expenditure. Furthermore, it has been shown in [38] that relay transmissions can improve the energy-efficiency and extend the lifetime of sensor nodes.

The problem of joint transmit power and QoS control has also been recently considered in the literature, for example in [40].

The overhead associated with complex cryptographic techniques makes them less feasible for implementation in WBANs. It is, therefore, necessary to explore the applicability of alternative approaches to security in WBANs, particularly PHY security.

In this regard, secret key generation from the wireless channel measurements in periods of significant WBAN channel fluctuation is studied in [41, 42].

Multi-hop relaying also has been shown in [43] to improve the link capacity in WBANs, which can be leveraged to secure communications at the wireless physical layer.

1.9 Research Objectives and Thesis Organization

The main objectives of the research are as follows:

- to develop quantitative performance measures for energy efficiency and PHY security of radio transmissions under statistical CSI knowledge in a fading WBAN,
- to characterize the average end-to-end packet latency incurred by multi-hop transmissions in a WBAN as a QoS measure,
- to formulate proper game frameworks using the hitherto developed performance and QoS measures,
- to identify and prove the existence of the Nash equilibria for the formulated games,
- to devise distributed, fast-converging, cross-layer algorithms among sensor nodes to compute the stable equilibrium solutions,
- to evaluate the frameworks using numerical simulations in conditions approximating actual deployment of WBANs under various scenarios, and
- to examine the impact of system parameters on the performance behaviors.

The rest of the thesis is organized as follows. Energy-efficient intra-WBAN communication with QoS provisioning is studied in Chap. 2. Secure intra-WBAN communication with QoS provisioning is investigated in Chap. 3. Finally, concluding remarks and possible future directions are provided Chap. 4.

Chapter 2

Optimal Relay Selection and Power Control with Quality-of-Service Provisioning in Wireless Body Area Networks

This chapter includes a manuscript entitled "Optimal Relay Selection and Power Control with Quality-of-Service Provisioning in Wireless Body Area Networks" by Hussein Moosavi and Francis Minhthang Bui, submitted to the *IEEE Transactions on Wireless Communications*, on October 2015. This work was supported in part by funding from the Natural Sciences and Engineering Research Council of Canada (NSERC).

A game-theoretic approach is proposed to investigate the problem of relay selection and power control with quality of service constraints in multiple-access wireless body area networks (WBANs). Each sensor node seeks a strategy that ensures the optimal energy efficiency and, at the same time, provides a guaranteed upper bound on the end-to-end packet delay and jitter. The existence of Nash equilibrium for the proposed non-cooperative game is proved, the Nash power control solution is analytically calculated, and a distributed algorithm is provided that converges to a Nash relay selection solution. The game theoretic

analysis is then employed in an IEEE 802.15.6-based WBAN to gauge the validity and effectiveness of the proposed framework. Performance behaviors in terms of energy efficiency and end-to-end delay and jitter are examined for various scenarios. Results demonstrate the merits of the proposed framework, particularly for moving WBANs under severe fading conditions.

2.1 Introduction

The trend towards personalized ubiquitous computing has led to the advent of a new class of wireless technologies, namely wireless body area networks (WBANs). A typical WBAN is a heterogeneous network of body-worn or implanted sensor nodes collecting vital signs and motion readings, along with a network coordinator called a hub.

Body-centric wireless communications accommodate a wide variety of applications, from health monitoring, to entertainment, military, and many other areas, with diverse quality of service (QoS) requirements [2, 3].

The unique challenges posed by WBAN technologies, such as fundamental resource constraints, and the demanding deployment environment of these systems, for example the high variation in network conditions, difficulty to predict mobility patterns, and limits of wireless radio range, together render many traditional wireless sensor network (WSN) solutions inappropriate, if not obsolete, for WBANs.

One of the most vexing issues raised from the adoption of WBAN technologies is energy efficiency. Small lightweight sensor devices in a WBAN have scarce energy resources. Besides, the transceiver is known to be the most energy-consuming part in a sensor node and the radio transmission in the vicinity of the human body is highly lossy and inefficient [2, 4]. Preserving energy by adjusting transmit power is, therefore, crucial to prolong the lifetime of the WBAN and is a major design concern.

The game-theoretic power control in wireless networks has been studied extensively in the literature. The number of successfully received bits per unit of energy is used to measure the energy efficiency in [7, 8, 44, 45]. The performance utility, however, is characterized by packet error rate, the estimation of which may not be feasible in a practical WBAN. Underlying channel conditions change frequently in a WBAN due to the body movements and other interferences in the surrounding environment, and therefore the instantaneous channel state information is likely to be unknown to the transmitter.

Energy efficiency, as stated earlier, may severely suffer in a WBAN due to the high path loss and attenuation of the wireless signals near the human body. Relay transmission is shown to be a promising strategy to overcome this hurdle in wireless settings, as it enhances the effective received signal-to-noise ratio (SNR) and, in turn, improves the energy efficiency [7–9, 46, 47]. Multi-hop relaying is particularly germane to WBANs also, since the distance between sensor nodes in a WBAN is relatively short and the quality of direct links between nodes and hub generally deteriorates under severe fading conditions [38, 48, 49].

Exploiting spatial diversity through multi-hop transmission, however, imposes additional latency to the system. Managing packet latency is of primary relevance in WBAN, as the collected physiological and contextual data may have a critical nature (*e.g.*, heart rate information) and need to be delivered to the hub in a timely manner.

Motivated by these developments, we employ a set of tools from game theory to study the problem of joint relay selection and power control in WBANs. The objective is to use the radio resources as efficiently as possible while ensuring the QoS requirements.

2.1.1 Summary of Contributions

We examine the problem of relay selection and power control with latency provisioning in the uniquely constrained context of WBANs. The main contributions of the work are as follows.

- The packet outage probability is adapted to construct the energy-efficiency performance metric, as it is more meaningful in realistic WBAN fading channels.
- Analytical expressions for the average end-to-end delay and jitter incurred by multi-hop transmission in a slotted Aloha medium access WBAN are developed.
- A game-theoretic approach is proposed wherein each node seeks to select its next hop in the uplink and choose its transmit power in a distributed manner in order to maximize its energy efficiency and at the same time meet the QoS requirements in terms of upper bounds on end-to-end delay and jitter. We prove the proposed game admits Nash equilibrium and characterize the power control and relay selection equilibria.
- The game theoretic framework is then employed to investigate the performance behavior trade-offs among energy efficiency and QoS in an IEEE 802.15.6-based ultra wideband (UWB) WBAN, considering various scenarios. The framework proves promising in significantly improving the energy efficiency of transmissions at the expense of an admissible increase in the end-to-end delay and jitter.

2.1.2 Paper Organization

The remainder of this paper is organized as follows. Sec. 2.2 provides the system model of the WBAN. Sec. 2.3 characterizes the end-to-end packet outage probability in WBAN. The end-to-end packet delay and jitter in WBAN are formulated in Sec. 2.4. Sec. 2.5 describes the relay selection and power control game framework. The effectiveness and applicability of the framework are validated in Sec. 2.6 and the numerical results are analyzed. Finally, concluding remarks and possible future directions are offered in Sec. 2.7.

2.2 System Model

In this section, architecture of the WBAN, propagation model of the wireless channel, and method of accessing the shared wireless medium are described.

2.2.1 WBAN Architecture

We consider a WBAN composed of N on-body sensor nodes transmitting their sensed data to a common hub H in the uplink. Let $\mathcal{N}$ denote the set of all sensor nodes with a typical element of n.

Each sensor node may either directly transmit its packets to the hub or it may exploit spatial diversity by choosing a multi-hop transmission path to enhance the performance in fading conditions. This results in a network topology graph $G(\mathcal{V},\mathcal{E})$, where $\mathcal{V} = \mathcal{N} \cup \{\mathsf{H}\}$ denotes the set of all vertices with a typical element of i and $\mathcal{E}$ denotes the set of all the edges. We formally define a transmission path as follows.

Definition 2.1 (Path)**.** A K-hop uplink path l in the graph G from a node $n \in \mathcal{N}$ to another node $i \in \mathcal{V}$ is defined as a sequence of nodes $l = \langle m_1, \cdots, m_{K+1} \rangle$ such that $m_1 = n$, $m_{K+1} = i$, and the link $\langle m_k, m_{k+1} \rangle \in \mathcal{E}$ $\forall k \in \{1, \cdots, K\}$.

■

The overall network architecture in the uplink therefore is a tree topology whereby each sensor node n is connected to the hub through a unique path denoted by $l_n = \langle n, \cdots, \mathsf{H} \rangle$. The assumption is that intermediate nodes are willing to relay the packets of their peers. The limitations on how many relays each node can reliably support is discussed later in Sec. 2.5.1.

2.2.2 Channel Model

Besides the signal attenuation due to geometric signal spreading, wireless channels also experience small-scale fading, that is, fluctuations caused by arrival of signal by multiple propagation paths. An on-body WBAN channel is typically modeled to undergo log-normal fading [6, 43]. Therefore, the received SNR from a sensor node $n \in \mathcal{N}$ as measured at another node $i \in \mathcal{V} \backslash \{n\}$ follows a log-normal distribution, with the following PDF

$$f(\gamma_{\langle n,i \rangle}) = \frac{1}{\gamma_{\langle n,i \rangle} \sigma_{\langle n,i \rangle} \sqrt{2\pi}} \exp\left(-\frac{(\gamma^{\mathrm{dB}}_{\langle n,i \rangle} - \mu_{\langle n,i \rangle})^2}{2\sigma^2_{\langle n,i \rangle}} \right), \tag{2.1}$$

where $\mu_{\langle n,i \rangle}$ and $\sigma_{\langle n,i \rangle}$ denote the mean and standard deviation of the received SNR $\gamma_{\langle n,i \rangle}$ in dB, respectively.

2.2.3 Slotted Aloha medium access in IEEE 802.15.6

There are two random access methods outlined in the IEEE 802.15.4 for obtaining the contended allocations in a WBAN, namely carrier sense multiple access with collision avoidance (CSMA/CA) and slotted Aloha access. For this work, we focus on the latter scenario, *i.e.*, sensor nodes seek access to the shared wireless medium using slotted Aloha. We briefly summarize the protocol, as described in more detail in [50].

The protocol restricts the sensor nodes to transmit only at the beginning of discrete time slots. Each node maintains a contention probability α to determine if it obtains a new contended allocation in an Aloha slot. A node that has a packet to transmit starts the slotted Aloha access by setting its α to $\alpha_{\max}$ which equals $\frac{3}{8}$. (We consider a user priority of 5 for all the sensor nodes, designated to medical data or network control traffic.) The node then draws a value r from the interval [0, 1] at random and obtain the contended slot for transmission if $r \leq \alpha$. Otherwise, the node backs off until the next time slot before contending for another allocation.

When a node transmits a packet but the destination fails to receive it, the node shall halve its α for even number of consecutive failures or keep α unchanged otherwise. Note that the node shall set its α to $\alpha_{\min}$ if halving the α makes it smaller than $\alpha_{\min}$ which equals $\frac{3}{16}$.

2.3 End-to-End Packet Outage Probability

The packet error rate is a widely used reliability measure especially in wireless communications. A received packet is declared corrupted if at least one bit is erroneous. Assuming pairwise independent bit errors, the packet error rate $\lambda_{\langle n,i \rangle}$ over a single-hop link between a

transmitter $n \in \mathcal{N}$ and a receiver $i \in \mathcal{V}\backslash\{n\}$ is given by

$$\lambda_{\langle n,i\rangle} = 1 - \left(1 - \lambda^b_{\langle n,i\rangle}\right)^{M_b}, \tag{2.2}$$

where $\lambda^b_{\langle n,i\rangle}$ and M_b are the bit error rate over the $\langle n,i\rangle$ link and the packet size in bits, respectively. For the non-coherent differentially encoded binary phase-shift keying (DBPSK) modulation scheme, $\lambda^b_{\langle n,i\rangle}$ is given by [51]

$$\lambda^b_{\langle n,i\rangle} = \frac{1}{2}\exp(-\gamma^b_{\langle n,i\rangle}), \tag{2.3}$$

where $\gamma^b_{\langle n,i\rangle}$ stands for the received SNR per bit from n as measured at i. $\gamma^b_{\langle n,i\rangle}$ itself can be expressed as

$$\gamma^b_{\langle n,i\rangle} = \frac{W\gamma_{\langle n,i\rangle}}{R_b} \tag{2.4}$$

where W and R_b are the bandwidth in Hertz and transmission rate in bits per second, respectively.

It is, however, difficult to obtain packet error rate in a practical WBAN, as the instantaneous SNR is likely to be unknown to the communicating parties due to the severe fading of radio signals near the human body. Rather, it is more meaningful to adopt the packet outage probability (POP) to assess the reliability of transmissions in realistic fading channels, which signifies the fraction of fading realizations where a prescribed packet error rate is guaranteed.

For a target packet error rate $\underline{\lambda}$, the POP over the single-hop link between n and i is

$$\begin{aligned} P^{\text{out}}_{\langle n,i\rangle} = \Pr\left\{\lambda_{\langle n,i\rangle} > \underline{\lambda}\right\} &= \Pr\left\{\frac{R_b}{W}\ln\left(2 - 2\sqrt[M_b]{1-\underline{\lambda}}\right)^{-1} > \gamma_{\langle n,i\rangle} > 0\right\} \\ &= \int_{\gamma_{\langle n,i\rangle}=0}^{\frac{R_b}{W}\ln\left(2-2\sqrt[M_b]{1-\underline{\lambda}}\right)^{-1}} f\left(\gamma_{\langle n,i\rangle}\right) d\gamma_{\langle n,i\rangle} \\ &= \Phi\left(\frac{\left[\frac{R_b}{W}\ln\left(2 - 2\sqrt[M_b]{1-\underline{\lambda}}\right)^{-1}\right]^{\text{dB}} - \mu_{\langle n,i\rangle}}{\sigma_{\langle n,i\rangle}}\right), \end{aligned} \tag{2.5}$$

where Φ is the cumulative distribution function of the standard normal distribution and is defined as

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} \exp(-\frac{t^2}{2})\, dt.$$

We assume all the channel fading gains are mutually independent, which is realistic in most practical WBAN scenarios (Correlated shadowing for geographically proximate links is shown to be negligible compared to the other components of the path loss [43]). Therefore, the packet outage over a multi-hop path occurs regardless of which hop suffers from the outage. The POP of a K-hop transmission path $l = \langle m_1, \cdots, m_{K+1} \rangle$, in turn, is obtained as follows

$$P_l^{\text{out}} = 1 - \prod_{k=1}^{K} \left(1 - P_{\langle m_k, m_{k+1} \rangle}^{\text{out}}\right). \tag{2.6}$$

As the received SNR over short single hops in multi-hop transmission improves compared to the received SNR over the direct link to the hub, the POP over a multi-hop path is expected to be significantly smaller than the POP for direct transmission.

2.4 End-to-End Delay and Jitter

While multi-hop relaying can improve the reliability of transmissions, it also introduces additional queuing and medium access delay at the intermediate relay nodes and increases the average jitter.

The traffic flow of each node is composed of the node's own generated traffic as well as the traffic forwarded to the node by its descendants to be relayed. That is, the traffic load arriving at each sensor node follows a general distribution. Likewise, the packet service time at each node does not have a specific distribution as it depends on the characteristics of the medium access protocol and the physical constraints imposed by the network topology. It is, therefore, realistic to describe each sensor node as a GI/G/1 queue [52], with the assumption of each node handling one packet at a time with a first-come, first-served service discipline.

In the following, we first obtain the expected value and variance of the inter-arrival time and service time distributions for each node which later are used to derive the average end-to-end delay and jitter over a multi-hop WBAN path.

2.4.1 Inter-Arrival Time Distribution

We choose a Poisson packet arrival at the MAC layer of the sensor nodes as we want to obtain conservative performance bounds. Let us assume for each sensor node $n \in \mathcal{N}$ the data packets collected by the sensor itself arrive at the sensor node according to a Poisson distribution with the expected arrival rate of κ_n packet(s) per second. We denote the probability distribution of packet inter-arrival times at a node n by A_n. Accordingly, for a leaf sensor node (*i.e.*, a node with no descendant) A_n is exponentially distributed with expected value and variance of κ_n^{-1} and κ_n^{-2}, respectively.

For a relaying sensor node with descendants, A_n comprises the inter-arrival time of packets generated by node n itself as well as the inter-arrival time of packets received successfully from the children (*i.e.*, immediate descendants) of n to be relayed in the uplink. Note that the latter itself is the aggregated inter-departure times of packets from the children of n.

Let $\mathcal{C}_n$ be the set of children of the node n in the tree structure. As the distributions of the traffic generated by n and its children are pairwise independent, we have

$$\mathbb{A}_n(t) = \mathbb{A}_{\langle n,n\rangle}(t) \prod_{c \in \mathcal{C}_n} \mathbb{D}_{\langle c,n\rangle}(t), \tag{2.7}$$

where $\mathbb{A}_n$, $\mathbb{A}_{\langle n,n\rangle}$, and $\mathbb{D}_{\langle c,n\rangle}$ are the moment generating functions of the inter-arrival distribution of packets at the node n, the inter-arrival distribution of self-generating packets at n, and the inter-departure distribution of packets transmitted by c to be received by n.

Now let us denote the service time distribution of packets transmitting from a node c to node n by $S_{\langle c,n\rangle}$, with the moment generating function $\mathbb{S}_{\langle c,n\rangle}$. The moment generating

function of the inter-departure distribution of packets from c (with non-Poisson arrival) to n can be approximated by [53]

$$\mathbb{D}_{\langle c,n\rangle}(t) = \rho_{\langle c,n\rangle}\mathbb{S}_{\langle c,n\rangle}(t) + (1-\rho_{\langle c,n\rangle})\mathbb{S}_{\langle c,n\rangle}(t)\mathbb{A}_c(t), \tag{2.8}$$

where $\rho_{\langle c,n\rangle}$ is the utilization factor of the node c when transmitting to n and is given by $\frac{\mathbf{E}[S_{\langle c,n\rangle}]}{\mathbf{E}[A_c]}$. Note that the expected value (*i.e.*, the first moment) of $D_{\langle c,n\rangle}$ is equal to the expected value of A_c regardless of the service time distribution, *i.e.*,

$$\begin{aligned}\mathbf{E}[D_{\langle c,n\rangle}] &= \frac{d}{dt}\mathbb{D}_{\langle c,n\rangle}(t)\big|_{t=0} \\ &= \rho_{\langle c,n\rangle}\mathbf{E}[S_{\langle c,n\rangle}] + (1-\rho_{\langle c,n\rangle})(\mathbf{E}[S_{\langle c,n\rangle}] + \mathbf{E}[A_c]) \\ &= \mathbf{E}[A_c].\end{aligned} \tag{2.9}$$

Using Eqs. (2.7), (2.8), and (2.9), and given that the moment generating function of a random variable at $t = 0$ always exists and is equal to 1, the expected value of the inter-arrival distribution of packets at a sensor node n is obtained by

$$\mathbf{E}[A_n] = \frac{d}{dt}\mathbb{A}_n(t)\big|_{t=0} = \mathbf{E}[A_{\langle n,n\rangle}] + \sum_{c\in\mathcal{C}_n}\mathbf{E}[A_c]. \tag{2.10}$$

Similarly, the variance (*i.e.*, the second moment about the mean) of the inter-arrival distribution of packets at n is retrieved by[1]

$$\begin{aligned}\mathbf{V}[A_n] &= \frac{d^2}{dt^2}\mathbb{A}_n(t)\big|_{t=0} - \mathbf{E}[A_n]^2 \\ &= \mathbf{V}[A_{\langle n,n\rangle}] + (1-\mathbf{E}[A_{\langle n,n\rangle}])\sum_{c\in\mathcal{C}_n}\mathbf{E}[A_c] - \left[\sum_{c\in\mathcal{C}_n}\mathbf{E}[A_c]\right]^2 + \\ &\quad \sum_{c\in\mathcal{C}_n}\sum_{c\prime\in\mathcal{C}_n\setminus\{c\}}\mathbf{E}[A_c]\mathbf{E}[A_{c\prime}] + \sum_{c\in\mathcal{C}_n}\Bigg[\mathbf{V}[S_{\langle c,n\rangle}] - \mathbf{E}[S_{\langle c,n\rangle}]^2 + 2\mathbf{E}[S_{\langle c,n\rangle}]\mathbf{E}[A_c] + \\ &\quad (1-\frac{\mathbf{E}[S_{\langle c,n\rangle}]}{\mathbf{E}[A_c]})(\mathbf{V}[A_c] + \mathbf{E}[A_c]^2)\Bigg].\end{aligned} \tag{2.11}$$

[1]See Appendix A.

We assume the queues are stable, *i.e.*, $\rho_n \leq 1 \; \forall n \in \mathcal{N}$. To prevent an over-saturated condition in the network, we also assume the transmission rate of each node is greater than the accumulated traffic rate forwarded by the node.

2.4.2 Service Time Distribution

In order to find the distribution of service time at a sensor node (*i.e.*, the time a node spends to transmit a packet without any error), we need to derive the packet transmission time distribution first. We consider a WBAN wherein the sensor nodes seek access to the shared wireless medium using slotted Aloha. Similar lines of reasoning can be followed for a CSMA/CA-based WBAN.

Each Aloha slot shall be greater than or equal to the time required to transmit a packet, that is

$$\tau = \frac{M_b}{R_b} + \varepsilon \approx \frac{M_b}{R_b}, \tag{2.12}$$

where M_b and R_b are the packet size (in bits) and data transmission rate, respectively. In Eq. (2.12), ε represents the time taken for a node to receive an ACK/NACK from its destination and is assumed to be negligible compared to $\frac{M_b}{R_b}$.

Let T_n denote the probability distribution for the time required to transmit a packet from the instance a node n starts the slotted Aloha access process until it finishes transmission. It is evident that T_n follows a geometric distribution with the probability mass function given by

$$\Pr\{T_n = k\tau\} = \alpha_n(1-\alpha_n)^{k-1} \qquad k = 1, 2, \cdots, \tag{2.13}$$

where α_n is the contention probability maintained by node n.

Then the moment generating function of the transmission time distribution from node n is

$$\mathbb{T}_n(t) = \mathbf{E}[e^{tT_n}] = \sum_{k=1}^{\infty} \alpha_n (1-\alpha_n)^{k-1} e^{tk\tau}$$
$$= \frac{\alpha_n \, e^{t\tau}}{1-(1-\alpha_n)e^{t\tau}}. \tag{2.14}$$

Now we obtain the probability of a successful packet transmission for a sensor node. The probability that a packet sent over a one-hop link is successfully received by its destination depends on whether a collision occurs or not as well as on the received SNR.

A packet transmitted by a sensor node will be lost due to collision if at least one of the nodes within the carrier sensing range of the receiver, other than transmitter itself, tries to transmit during the same time slot. We assume that all the nodes are within the carrier sensing range of each other due to the small scale of WBANs and, furthermore, that no node can receive a packet while transmitting. Given the fact that a node transmits with a probability equal to its utilization factor (*i.e.*, if it has a packet for transmission), the collision rate of a packet transmitted by a sensor node $n \in \mathcal{N}$ denoted by χ_n is given by

$$\chi_n = 1 - \prod_{x \in \mathcal{N} \setminus \{n\}} (1-\rho_x). \tag{2.15}$$

If no collision occurs, the average packet error rate $\bar{\lambda}_{\langle n,i \rangle}$ over a link between the transmitter n and a receiver i is a function of the average received SNR per bit as suggested by Eqs. (2.2) and (2.3).

The average probability of successful packet transmission from n to i denoted by $\pi_{\langle n,i \rangle}$ is therefore given by

$$\pi_{\langle n,i \rangle} = 1 - \left[\chi_n + (1-\chi_n)\bar{\lambda}_{\langle n,i \rangle}\right]. \tag{2.16}$$

An automatic-repeat-request mechanism is considered whereby a sensor node keeps retransmitting a packet until the packet is successfully received at the destination. We assume the retransmissions are independent. The service time at the sensor node n when

transmitting to another node i is therefore a compound probability distribution in which the compounded distribution is geometric with success probability of $\pi_{\langle n,i\rangle}$ and the distribution of transmission time T_n is the compounding distribution [54]. The moment generating function of the service time distribution of packets transmitting from n to i is given by

$$\begin{aligned}\mathbb{S}_{\langle n,i\rangle}(t) &= \sum_{k=1}^{\infty} \pi_{\langle n,i\rangle}(1-\pi_{\langle n,i\rangle})^{k-1}\mathbb{T}_n^k(t) \\ &= \pi_{\langle n,i\rangle}\mathbb{T}_n(t)\big|_{\alpha=\alpha_{\max}} + \\ &\quad \pi_{\langle n,i\rangle}(1-\pi_{\langle n,i\rangle})\mathbb{T}_n^2(t)\big|_{\alpha=\alpha_{\max}} + \\ &\quad \frac{\pi_{\langle n,i\rangle}(1-\pi_{\langle n,i\rangle})^2\mathbb{T}_n^3(t)|_{\alpha=\alpha_{\min}}}{1-(1-\pi_{\langle n,i\rangle})\mathbb{T}_n(t)|_{\alpha=\alpha_{\min}}}. \end{aligned} \tag{2.17}$$

Note that in Eq. (2.17) node n sets its contention probability α_n to $\alpha_{\max}$ for the first two transmissions and fixes it to $\alpha_{\min}$ for the rest of transmission attempts.

Using Eqs. (2.14) and (2.17) and the properties of the moment generating function, the expected value and variance of the service time at n when transmitting to i are derived respectively as

$$\begin{aligned}\mathbf{E}[S_{\langle n,i\rangle}] &= \frac{d}{dt}\mathbb{S}_{\langle n,i\rangle}(t)\big|_{t=0} \\ &= \frac{8}{3}\tau\left(\frac{2}{\pi_{\langle n,i\rangle}} - 3\pi_{\langle n,i\rangle} + 2\pi_{\langle n,i\rangle}^2\right), \end{aligned} \tag{2.18}$$

and

$$\begin{aligned}\mathbf{V}[S_{\langle n,i\rangle}] &= \frac{d^2}{dt^2}\mathbb{S}_{\langle n,i\rangle}(t)\big|_{t=0} - \mathbf{E}[S_{\langle n,i\rangle}]^2 \\ &= \frac{\tau^2}{9}\left(\frac{256}{\pi_{\langle n,i\rangle}^2} - \frac{48}{\pi_{\langle n,i\rangle}} + 768 - 1976\pi_{\langle n,i\rangle} + 528\pi_{\langle n,i\rangle}^2 + 768\pi_{\langle n,i\rangle}^3 - 256\pi_{\langle n,i\rangle}^4\right). \end{aligned} \tag{2.19}$$

2.4.3 Average Delay and Jitter

Let us denote the distribution of the total packet latency experienced at a sensor node n when transmitting to another node i by $L_{\langle n,i\rangle}$. This latency includes both the queuing delay

as well as the service delay. Given the moment generating functions of packet inter-arrival time and service time at n, the moment generating function of $L_{\langle n,i\rangle}$ denoted by $\mathbb{L}_{\langle n,i\rangle}$ can be approximated as [55]

$$\mathbb{L}_{\langle n,i\rangle}(t) = \frac{\left(1-\mathbf{E}[A_n]\mathbf{E}[S_{\langle n,i\rangle}]\right)(t-1)\mathbb{S}_{\langle n,i\rangle}(t)\left(1-\mathbb{A}_n(\mathbb{S}_{\langle n,i\rangle}(t))\right)}{\mathbf{E}[A_n]\left(1-\mathbb{S}_{\langle n,i\rangle}(t)\right)\left(t-\mathbb{A}_n(\mathbb{S}_{\langle n,i\rangle}(t))\right)}. \tag{2.20}$$

The expected value and variance of the total delay at n when transmitting to i then are obtained from Eq. (2.20) respectively as

$$\mathbf{E}[L_{\langle n,i\rangle}] = \mathbf{E}[S_{\langle n,i\rangle}] + \frac{\mathbf{E}[A_n]\mathbf{V}[S_{\langle n,i\rangle}] + \mathbf{E}[S_{\langle n,i\rangle}]\mathbf{V}[A_n]}{2\left(1-\mathbf{E}[A_n]\mathbf{E}[S_{\langle n,i\rangle}]\right)}, \tag{2.21}$$

and

$$\mathbf{V}[L_{\langle n,i\rangle}] = \frac{\mathbf{E}[A_n]^2\mathbf{V}[S_{\langle n,i\rangle}] + \mathbf{E}[S_{\langle n,i\rangle}]^2\mathbf{V}[A_n]}{4\mathbf{E}[A_n]\mathbf{E}[S_{\langle n,i\rangle}]} + \frac{\mathbf{V}[A_n]^2\mathbf{V}[S_{\langle n,i\rangle}] + \mathbf{V}[S_{\langle n,i\rangle}]^2\mathbf{V}[A_n]}{\left(\mathbf{V}[A_n]+\mathbf{V}[S_{\langle n,i\rangle}]\right)^2}. \tag{2.22}$$

The average end-to-end delay experienced by a packet over a K-hop transmission path $l = \langle m_1, \cdots, m_{K+1}\rangle$ is the aggregate of the delays at the nodes en route, and is given by

$$\mathbf{E}[L_l] = \sum_{k=1}^{K} \mathbf{E}[L_{\langle m_k, m_{k+1}\rangle}]. \tag{2.23}$$

Likewise, the average variation in the end-to-end packet delay (also known as jitter) experienced over a path l is the sum of the standard deviations of the total delays at the individual nodes, and is given by

$$\mathbf{V}[L_l]^{\frac{1}{2}} = \sum_{k=1}^{K} \mathbf{V}[L_{\langle m_k, m_{k+1}\rangle}]^{\frac{1}{2}}. \tag{2.24}$$

2.5 The Joint Relay Selection and Power Control Game

We formulate a non-cooperative game wherein each sensor node seeks to selfishly maximize the energy efficiency of its transmissions in the uplink of the WBAN while adhering to the applicable QoS constraints. We model the utility function of a node as the ratio of the goodput to the transmit power over the path it takes to connect to the hub, and specify the QoS requirements in terms of the upper bounds on the packet outage probability as well as the average end-to-end delay. Energy consumption in the sensor nodes is approximated by energy utilized for data transmission, as the computation energy is negligible by comparison. Depending on the nature of data and the required end-to-end transmission reliability, sensor nodes may have different QoS requirements.

Formally, the joint relay selection and power control game (RSPCG) is specified by $\mathcal{G} = \langle \mathcal{N}, \{\mathcal{A}_n\}, \{u_n\} \rangle$ where $\mathcal{N} = \{1, \ldots, N\}$ is the set of players with a typical element of n, $\mathcal{A}_n = \mathcal{R}_n \times \left[0, \bar{P}_n\right]$ is the action set of player n with an action $a_n = (r_n, p_{\langle n, r_n \rangle})$ corresponding to a choice of relaying node and transmit power, and u_n is the utility function associated with player n. Here, $\mathcal{R}_n$ and $\bar{P}_n$ are the set of potential relays to which n can connect in the uplink, and the maximum transmit power available to n. Without loss of generality and for brevity of exposition, we assume $\bar{P}_n$ is large and identical for all the sensor nodes.

We assume sensor nodes have no incentive to disconnect from the WBAN, *i.e.*, the network graph is always connected.

2.5.1 Utility and Quality of Service

Given the strategies of the other nodes, each node makes its relay selection and power control decisions independently, seeking the maximum possible utility while satisfying the applicable QoS demands.

It is assumed that a sensor node $n \in \mathcal{N}$ chooses to connect to a relay node $r_n \in \mathcal{R}_n$ in the uplink and, in turn, form a unique K-hop transmission path $l_n = \langle m_1, \cdots, m_{K+1} \rangle$ to the hub, where $m_1 = n$, $m_2 = r_n$, and $m_{K+1} = \mathsf{H}$.

For wireless networks with fundamental energy constraints, the ratio of a node's goodput to the consumed transmit power is a commonly used measure for energy efficiency [45, 56]. Let us specify the transmit power of a path l as the sum of the transmit powers of the nodes along the path, and denote it by p_l. We model the utility function of n as

$$\begin{aligned} u_n &= R_b \frac{(1 - P^{\text{out}}_{l_n})}{p_{l_n}} \\ &= R_b \frac{\prod_{k=1}^{K} \left(1 - P^{\text{out}}_{\langle m_k, m_{k+1} \rangle}\right)}{\sum_{k=1}^{K} p_{\langle m_k, m_{k+1} \rangle}} \\ &= R_b \frac{(1 - P^{\text{out}}_{\langle n, r_n \rangle}) \prod_{k=2}^{K} \left(1 - P^{\text{out}}_{\langle m_k, m_{k+1} \rangle}\right)}{p_{\langle n, r_n \rangle} + \sum_{k=2}^{K} p_{\langle m_k, m_{k+1} \rangle}} \\ &= R_b \frac{(1 - P^{\text{out}}_{\langle n, r_n \rangle})(1 - P^{\text{out}}_{l_{r_n}})}{p_{\langle n, r_n \rangle} + p_{l_{r_n}}}. \end{aligned} \tag{2.25}$$

This utility function represents the least number of bits that are successfully received by the hub per unit of energy consumed for a transmitting node given a target packet error rate, and has units of bits per joule.

We also consider the QoS measures of sensor node n to be the average packet latency δ_n and jitter θ_n experienced over the transmission path l_n taken by n to the hub, *i.e.*,

$$\begin{aligned} \delta_n = \mathbf{E}[L_{l_n}] &= \sum_{k=1}^{K} \mathbf{E}[L_{\langle m_k, m_{k+1} \rangle}] \\ &= \mathbf{E}[L_{\langle n, r_n \rangle}] + \sum_{k=2}^{K} \mathbf{E}[L_{\langle m_k, m_{k+1} \rangle}] = \mathbf{E}[L_{\langle n, r_n \rangle}] + \delta_{r_n}, \end{aligned} \tag{2.26}$$

and

$$\theta_n = \mathbf{V}[L_{l_n}]^{\frac{1}{2}} = \sum_{k=1}^{K} \mathbf{V}[L_{\langle m_k, m_{k+1}\rangle}]^{\frac{1}{2}}$$
$$= \mathbf{V}[L_{\langle n, r_n\rangle}]^{\frac{1}{2}} + \sum_{k=2}^{K} \mathbf{V}[L_{\langle m_k, m_{k+1}\rangle}]^{\frac{1}{2}} = \mathbf{V}[L_{\langle n, r_n\rangle}]^{\frac{1}{2}} + \theta_{r_n}. \tag{2.27}$$

Eqs. (2.25), (2.26), and (2.27) signify that the utility or QoS measures of a sensor node n depend on its transmit power and qualities of the first hop in its path to the hub $\langle n,r_n\rangle$, as well as the utility or QoS measures of the immediate relay node n chooses to connect to in the uplink, r_n.

We specify the QoS constraints of sensor node n by (Δ_n, Θ_n) where Δ_n and Θ_n are the upper bounds on the average delay and jitter, respectively. These requirements allows for determining the maximum tolerable end-to-end latency and jitter in the WBAN for scheduling uplink/downlink allocation intervals or real-time monitoring requirements.

Note also that these QoS constraints, in effect, limit the number of relays each node can reliably support in the uplink. That is because as the number of descendants of a node increases, the queuing delay and its variation at the node rise which, in turn, result in a higher latency and jitter over the entire path. Therefore once the delay or jitter over a path reaches the corresponding QoS constraint, nodes within that path can no longer admit new connections.

2.5.2 Power Control

In a given network topology, a best response power control strategy for a node $n \in \mathcal{N}$ is a utility maximizing choice of transmit power while fixing the transmit powers of all the other nodes, and is given by the solution of the following constrained optimization

$$\max_{p_{\langle n,r_n\rangle}} u_n \qquad \text{s.t.} \qquad \delta_n \leq \Delta_n,\, \theta_n \leq \Theta_n. \tag{2.28}$$

Note that for a matched filter receiver, the average received SNR from n as measured at r_n is given by

$$\bar{\gamma}_{\langle n,r_n\rangle} = \frac{p_{\langle n,r_n\rangle}|h_{\langle n,r_n\rangle}|^2}{N_0 W} \tag{2.29}$$

where $h_{\langle n,r_n\rangle}$ is the channel gain and N_0 is the thermal noise spectral density.

Moreover, the developments in Sec. 2.4.2 suggest that, in a fixed network topology, the delay and jitter constraints can be translated to corresponding lower bounds on the average received SNR.

The maximization in (2.28) is, therefore, equivalent to

$$\max_{\bar{\gamma}_{\langle n,r_n\rangle}} u_n \qquad \text{s.t.} \qquad \bar{\gamma}_{\langle n,r_n\rangle} \geq \hat{\gamma}^{\Delta}_{\langle n,r_n\rangle},\ \bar{\gamma}_{\langle n,r_n\rangle} \geq \hat{\gamma}^{\Theta}_{\langle n,r_n\rangle}. \tag{2.30}$$

Let us first consider the maximization problem (2.30) without any constraints. We can write

$$\max_{\bar{\gamma}_{\langle n,r_n\rangle}} R_b \left[1 - \prod_{k=2}^{K} \Phi\left(g\left(\bar{\gamma}_{\langle m_k,m_{k+1}\rangle}\right)\right)\right] \frac{1 - \Phi\left(g\left(\bar{\gamma}_{\langle n,r_n\rangle}\right)\right)}{N_0 W \left(\frac{\bar{\gamma}_{\langle n,r_n\rangle}}{|h_{\langle n,r_n\rangle}|^2} + \sum_{k=2}^{K} \frac{\bar{\gamma}_{\langle m_k,m_{k+1}\rangle}}{|h_{\langle m_k,m_{k+1}\rangle}|^2}\right)}, \tag{2.31}$$

where

$$g\left(\bar{\gamma}_{\langle m_k,m_{k+1}\rangle}\right) = \frac{10\log_{10}\left[\frac{R_b \ln\left(2-2\sqrt[M_b]{1-\underline{\lambda}}\right)^{-1}}{W\bar{\gamma}_{\langle m_k,m_{k+1}\rangle}}\right]}{\sigma_{\langle m_k,m_{k+1}\rangle}}. \tag{2.32}$$

Note that when the transmit powers of all other nodes are fixed, the utility of node n is only a function of the average received SNR $\bar{\gamma}_{\langle n,r_n\rangle}$. By taking the derivative of the utility with respect to $\bar{\gamma}_{\langle n,r_n\rangle}$ and equating it to zero, it is readily shown that u_n is maximized when $\bar{\gamma}_{\langle n,r_n\rangle} = \tilde{\gamma}_{\langle n,r_n\rangle}$, the solution of the following scalar equation

$$\Phi\left(-g\left(\bar{\gamma}_{\langle n,r_n\rangle}\right)\right) = \frac{10}{\sqrt{2\pi}\ln(10)\sigma_{\langle n,r_n\rangle}} \exp\left(-\frac{g\left(\bar{\gamma}_{\langle n,r_n\rangle}\right)^2}{2}\right) \left(1 + \frac{|h_{\langle n,r_n\rangle}|^2 \sum_{k=2}^{K} \frac{\bar{\gamma}_{\langle m_k,m_{k+1}\rangle}}{|h_{\langle m_k,m_{k+1}\rangle}|^2}}{\bar{\gamma}_{\langle n,r_n\rangle}}\right). \tag{2.33}$$

For the constrained maximization problem (2.30), the optimal SNR $\tilde{\gamma}$ may not be feasible in which case the sensor node has to adjust its transmit power to guarantee the lowest SNR required to meet its QoS constraints. This, of course, leads to a reduction in the node's energy efficiency. In particular, node n would choose its transmit power such that the average received SNR $\gamma^*_{\langle n,r_n\rangle} = \max\left\{\tilde{\gamma}_{\langle n,r_n\rangle}, \hat{\gamma}^{\Delta}_{\langle n,r_n\rangle}, \hat{\gamma}^{\Theta}_{\langle n,r_n\rangle}\right\}$ is maintained.

It is straightforward to show that u_n is a decreasing function of $\bar{\gamma}_{\langle n,r_n\rangle}$ for all $\bar{\gamma}_{\langle n,r_n\rangle} \geq \tilde{\gamma}$. Therefore, $u_n(\bar{\gamma}'_{\langle n,r_n\rangle}) < u_n(\bar{\gamma}_{\langle n,r_n\rangle})$ for all $\bar{\gamma}'_{\langle n,r_n\rangle} > \bar{\gamma}_{\langle n,r_n\rangle} \geq \tilde{\gamma}_{\langle n,r_n\rangle}$, *i.e.*, node n has no incentive to transmit at a power higher than $\gamma^*_{\langle n,r_n\rangle}$.

In the context of the non-cooperative RSPCG, an N-tuple $\boldsymbol{p} = \left\{p_{\langle n,r_n\rangle}\right\}_{n\in\mathcal{N}}$ is said to constitute a Nash equilibrium power control solution iff no unilateral deviation in transmit power strategy by any single node is profitable for that node.

The following proposition proves the existence of a power control Nash equilibrium and characterizes the equilibrium solution for the RSPCG.

Proposition 2.1 (Nash Power Control Solution). *If $\underline{\lambda} < 1 - 2^{-M}$, then the RSPCG admits a unique power control Nash equilibrium given by $\boldsymbol{p}^* = \left\{p^*_{\langle n,r_n\rangle}\right\}_{n\in\mathcal{N}}$ where $p^*_{\langle n,r_n\rangle} = \frac{N_0 W}{|h_{\langle n,r_n\rangle}|^2}\gamma^*_{\langle n,r_n\rangle}\ \forall n \in \mathcal{N}$.*

Proof: The condition $\underline{\lambda} < 1 - 2^{-M}$ ensures the function $g(.)$ can be defined for $\bar{\gamma} > 0$. Now, let $p_{\langle n,r_n\rangle} = p^*_{\langle n,r_n\rangle}\ \forall n \in \mathcal{N}$. Then the output SNR for each node n will be equal to $\gamma^*_{\langle n,r_n\rangle}$, *i.e.*, every node is playing its best response transmit power strategy. Therefore, $\boldsymbol{p}*$ is a power control Nash equilibrium.

Note that the two sides of the Eq. (2.33) are strictly monotonic with respect to $\bar{\gamma}$, with opposite monotonicity. This guarantees the equation exhibits a unique root $\tilde{\gamma}_{\langle n,r_n\rangle}$ for each node $n \in \mathcal{N}$. It readily follows that each node has a unique best response strategy and, therefore, the equilibrium with $\boldsymbol{p} = \boldsymbol{p}^*$ is a unique Nash solution. ■

From (2.25) and (2.33), the utility of node n at the equilibrium is given by

$$u_n^* = \frac{10R_b|h_{\langle n,r_n\rangle}|^2 \prod_{k=2}^{K} \Phi\left(-g\left(\bar{\gamma}^*_{\langle m_k,m_{k+1}\rangle}\right)\right)}{\sqrt{2\pi}\ln(10)N_0 W\sigma_{\langle n,r_n\rangle}} \frac{\exp\left(-\frac{g\left(\gamma^*_{\langle n,r_n\rangle}\right)^2}{2}\right)}{\gamma^*_{\langle n,r_n\rangle}}. \tag{2.34}$$

2.5.3 Relay Selection

Consider sensor nodes choose their equilibrium power control strategies in every network topology configuration. A best response relay selection strategy for a node $n \in \mathcal{N}$ is a utility maximizing choice of relaying node given the relay choices of all the other nodes, and is given by the solution of the following constrained optimization

$$\max_{r_n} u_n \qquad \text{s.t.} \qquad \delta_n \leq \Delta_n,\, \theta_n \leq \Theta_n. \tag{2.35}$$

A joint relay selection strategy by all sensor nodes $\boldsymbol{r} = \{r_n\}_{n\in\mathcal{N}}$ results in a network graph $G_{\boldsymbol{p}}$. In the following, we present a graph formation algorithm based on the concept of the best response relay selection.

The bootstrapping phase includes network discovery where each sensor node detects its neighboring nodes as potential partners for multi-hop transmission and learns the current state of the WBAN. Having discovered the network, sensor nodes iteratively and in an arbitrary sequence interact with their neighbors and choose their best response relaying nodes given their current knowledge of the network topology.

An N-tuple $\boldsymbol{r}$ is said to constitute a Nash equilibrium topology iff no unilateral deviation in relay selection strategy by any single node is profitable for that node.

The above described iterative approach among sensor nodes to selecting the best response relays is guaranteed to converge to a Nash topology as proved by the following proposition.

Proposition 2.2 (Nash Relay Selection Solution). *The presented relay selection algorithm is guaranteed to converge to a final Nash topology after a finite number of iterations regardless of the initial network topology and the sequence of best response selections.*

Proof: Let $G_{\boldsymbol{r}}$ be the resultant topology graph from the joint relay selection strategy $\boldsymbol{r}$. Topology graph evolution from $G_{\boldsymbol{r}}$ to another graph $G_{\boldsymbol{r}'}$ entails a best response relay selection by an arbitrary sensor node $n \in \mathcal{N}$. This best response choice by n may impact the utility of three different types of nodes in the network: the utility of n itself does not decrease as per the definition of a best response strategy; utilities of the descendants of n also do not decrease as a raise in the utility of a node can only lead to increase in the utility of its descendants as suggested by (2.25); finally, utilities of the nodes that are not connected to or are parents of n are not affected by a best response relay choice of node n. Therefore, every move from a graph $G_{\boldsymbol{r}}$ to a graph $G_{\boldsymbol{r}'}$ does not lead to any decrease in the utility of any node in the network. Based on this fact, and given that the number of tree topologies interconnecting a finite number of nodes is finite, it yields that the algorithm eventually converges to a stable Nash topology after a finite number of iterations. ■

2.5.4 RSPCG Algorithm Implementation

The RSPCG algorithm can be implemented in a distributed fashion which, compared to a centralized implementation, is less complex and more readily scalable in practice.

Each sensor node goes through a discovery phase on startup, where it detects the potential relay nodes in its vicinity for uplink transmission. Well-known discovery techniques [57] can be used in this phase to learn about the presence of neighbors.

Here, for each sensor node $n \in \mathcal{N}$ we define the potential relay set $\mathcal{R}_n$ as the set of nodes to which n can connect in the uplink, *i.e.*, the relay set of n is disjoint from its set of

descendants $\mathcal{D}_n$ in the tree structure. Also, potential relays need to be able to decode the signal transmitted by n at its maximum transmit power with negligibly small error. Hence, $\mathcal{R}_n = \left\{ i \in \mathcal{V} \backslash \left(\{n\} \cup \mathcal{D}_n \right) | \hat{\gamma}^b_{\langle n,i \rangle} > 0\,\mathrm{dB} \right\} \forall n \in \mathcal{N}$, where $\hat{\gamma}^b_{\langle n,i \rangle}$ is the average received SNR per bit from n with transmit power $\bar{P}_n$ as measured at i.

Subsequent to discovery phase, sensor nodes play an iterative relay selection and power control game in an arbitrary but sequential order. In every iteration each sensor node n interacts, using pairwise negotiations over a control channel, with its discovered potential relays, acquires the current network topology information as well as the POP, transmit power, and QoS measures of its prospective parents, calculates its best response power control strategies corresponding to each of its potential relays, then identifies its best response relay selection strategy and executes it by replacing its current link with the newly identified one. The game goes on until convergence to a Nash topology.

As suggested by (2.25), (2.26), and (2.27), each sensor node needs to only assess the utility and QoS measures of its prospective immediate hops in the uplink to make its best response decision. Note that when a prospective next-hop node is asked to report its QoS measures to its neighbors, it must first update its end-to-end delay and jitter, as accepting new descendants increases the queuing time and, in turn, end-to-end delay and jitter at the node.

Steps of the RSPCG algorithm is summarized in Algorithm 1.

Much of the computational complexity of the algorithm lies in the process of best response selection. In particular, the computational complexity of identifying the best response strategy for each sensor node n has a time complexity of $\mathcal{O}(|\mathcal{R}_n|)$.

Another source of complexity is the number of algorithm iterations till convergence. While this is upper bounded in theory by the number of spanning trees definable on the set of network graph vertices $\mathcal{V}$, the algorithm converges much faster in a practical implementation as a sensor node does not need attempting to connect to every other node in the network before identifying its best response.

INITIALIZATION
forall $n \in \mathcal{N}$ **do**
  $r_n \leftarrow \mathsf{Hub}$; //star network topology
  $p_{\langle n,r_n \rangle} \leftarrow p_0$; //pre-defined TX power
end

NETWORK DISCOVERY
forall $n \in \mathcal{N}$ **do**
  n finds its potential relay set $\mathcal{R}_n$;
end

DISTRIBUTED RELAY SELECTION AND POWER CONTROL
repeat in an arbitrary but sequential order
  forall $n \in \mathcal{N}$ **do**
    forall $r_n \in \mathcal{R}_n$ **do**
      n interacts with r_n over a control channel;
      n computes its utility maximizer $p^*_{\langle n,r_n \rangle}$;
      n computes its utility $u_n(r_n, p^*_{\langle n,r_n \rangle})$;
    end
    n selects it utility maximizer r^*_n;
  end
until *convergence to a stable Nash topology*;

ENERGY-EFFICIENT MULTI-HOP TRANSMISSION
Sensor nodes transmit their packets, where applicable;

Algorithm 1: RSPCG algorithm for relay selection and power control

Last but not least, the algorithm is adaptable to a dynamically changing WBAN setting as it can be repeated periodically within different time intervals depending on the frequency and magnitude of changes in the network. In this case, the best response interactions between sensor nodes can be piggybacked over regular data transmissions instead of requiring dedicated control channels, which can significantly reduce radio usage in small sensor devices.

2.6 Model Validation

In this section, the game theoretic analysis is employed in an IEEE 802.15.6-based UWB WBAN to gauge the validity and effectiveness of the proposed framework. To this end, we

examine the performance behaviors for various scenarios. In particular, we consider moving versus stationary WBAN scenarios with respect to the motion of the human body. Also three schemes are considered with respect to the transmission approach, namely multi-hop transmission using the proposed relay selection and power control game (RSPCG), direct transmission with power control using Proposition 2.1 (DTPC), and direct transmission with prearranged transmit power (DT).

2.6.1 Simulation Setup

A WBAN consisting of ten on-body sensor nodes is considered. As shown in Fig. 2.1, the nodes are placed on the head, left arm, left hand, chest, right arm, right hand, left leg, left foot, right leg, and right foot of the subject. The node H located on the center waist is the hub and the other ten sensor nodes try to communicate with it.

For the wireless propagation model in a moving WBAN, the results of the measurement campaign conducted in [43] are used, where average path loss and fading statistics are characterized on a per-link basis. The measurements are of a subject walking freely around a room, for an UWB center frequency of 4.2 GHz. The total path loss of the wireless channel is given by

$$PL^{\mathrm{dB}} = \overline{PL}^{\mathrm{dB}} + \mathcal{N}(\mu,\sigma) + \epsilon, \tag{2.36}$$

where $\overline{PL}$ is the average path loss of the channel, $\mathcal{N}(\mu,\sigma)$ a Gaussian distribution with mean μ and standard deviation σ which models the fading amplitude of the channel in dB, and ϵ is the correlation of the channel with itself and other links in the network which is negligible compared to the other two components of the path loss. Parameters of the channel propagation model are provided in [43] for different links in the WBAN.

Also a receiver noise figure of 10 dB and implementation loss of 5 dB are considered as per the optional UWB PHY specifications provided in IEEE 802.15.6.

To validate the model in an stationary scenario, the following path loss model is adopted based on the measurements taken in a hospital room for UWB frequencies of $3.1 - 10.6$ GHz

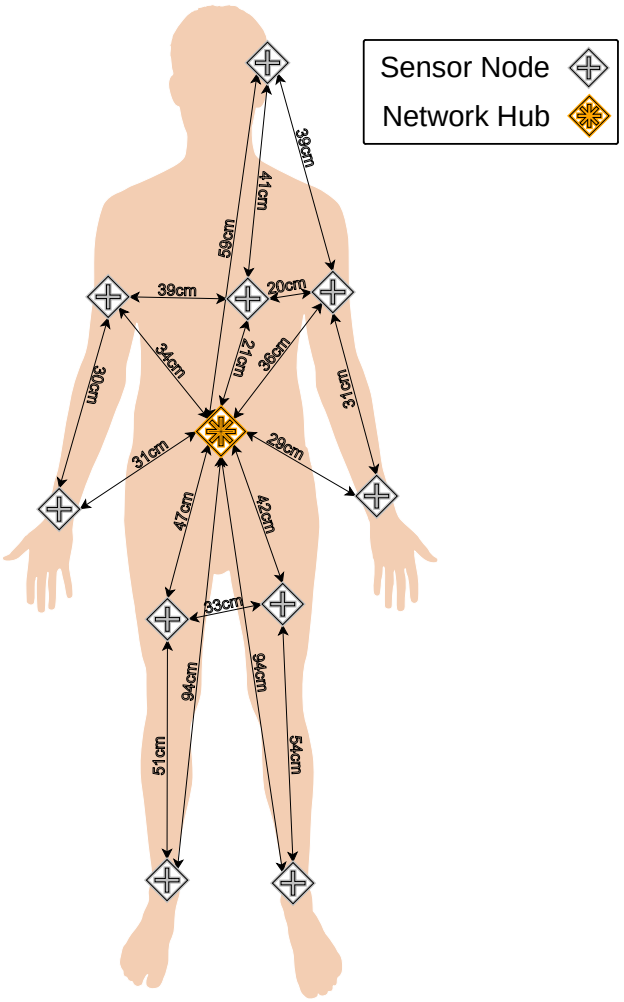

FIGURE 2.1: Architecture of the WBAN (The network is composed of ten sensor nodes and a hub. Graphical dimensions are not to scale, and numerical values correspond to those in [43].)

[6]

$$PL(d)^{\mathrm{dB}} = \beta \log_{10}(d) + \mathcal{N}(\mu,\sigma), \tag{2.37}$$

where d is Tx-Rx distance in millimeters and parameters β, μ, and σ are chosen to be 19.2, 3.38, and 2.8, respectively.

We assume the wireless links are symmetric and that the transceivers of all the sensor nodes are identical with the same transmission range.

2.6.2 Parameter Setting

The maximum signal transmit power for a transceiver is chosen to be 55 nW (-42.6 dBm) and 12 nW (-49.2 dBm) for moving and stationary WBAN scenarios, respectively. These are the transmission powers for which the POP of a target packet error rate of 10^{-3} stays less than or equal to 10^{-3} over the reference Chest-Hub link for both scenarios. Choosing identical $\bar{P}_n$ for all $n \in \mathcal{N}$ is suitable for homogeneous sensors, with comparable data rates, and helps to achieve uniform energy consumption across the WBAN, thereby extending the network lifetime.

The target packet error rate $\underline{\lambda}$ and the packet size are set to 10^{-12} and 100 octets (800 bits), respectively, for utility optimization.

We consider an expected arrival packet rate of $\kappa_n = 1 \ \forall n \in \mathcal{N}$, *i.e.*, each sensor node generates 1 packet per second at its application layer which is typical for health monitoring devices sending patient physiological information. Note that even though continuous patient monitoring devices may collect medical readings several times per second, these readings are usually aggregated in the node and then transmitted to the hub, thereby reducing the radio usage.

Other parameters of the physical layer required for simulation include working frequency, modulation scheme, channel bandwidth, and uncoded source bit rate, which are set to 4492.8 MHz, differentially encoded binary phase-shift keying (DBPSK), 499.2 MHz, and 0.4875 Mbps, respectively, as specified for the IEEE 802.15.6 impulse radio UWB (IR-UWB) PHY.

Lastly, the ambient air temperature is assumed to be 21 in computing the thermal noise spectral density N_0.

2.6.3 Numerical Results and Analysis

In the following, the obtained equilibrium results are presented to investigate how the expected performance behaviors differ for multi-hop relay transmission using RSPCG versus direct transmission, and for moving versus stationary WBAN scenarios. In particular, we examine equilibrium topology and power control scheme, node path power consumption, energy efficiency, end-to-end QoS in terms of delay and jitter, number of transmission hops, and number of algorithm iterations till convergence to a Nash solution.

2.6.3.1 Topology and Power Control Scheme

Fig. 2.2 presents the relaying node and transmit power selection strategies each node adopts at the equilibrium when $\Delta_n \geq 32.5$ ms and $\Theta_n \geq 168.6$ ms $\forall n \in \mathcal{N}$ in the moving WBAN scenario, and $\Delta_n \geq 16.1$ ms and $\Theta_n \geq 96.2$ ms $\forall n \in \mathcal{N}$ in the stationary case. This signifies the optimal cooperation scheme between nodes in the WBAN using the RSPCG.

Note that more nodes tend to adopt a multi-hop transmission strategy in the moving scenario compared to the stationary case (five nodes in the moving WBAN versus two nodes in the stationary case). The number of transmission hops in the moving scenario is more than that of the stationary case also. For instance in Fig. 2.2, the optimal strategies for Head and LHand nodes in the moving WBAN are to connect to the hub via three-hop links, while in the stationary WBAN both nodes choose to directly communicate with the hub. This is an expected result, as the body movements most likely degrade the channel quality especially between nearby nodes. The exception is LFoot node that, while choosing two-hop transmission in the stationary scenario, plays a direct transmission strategy in the moving case, as the body movement in this case actually improves the quality of direct channel between LFoot node and the hub.

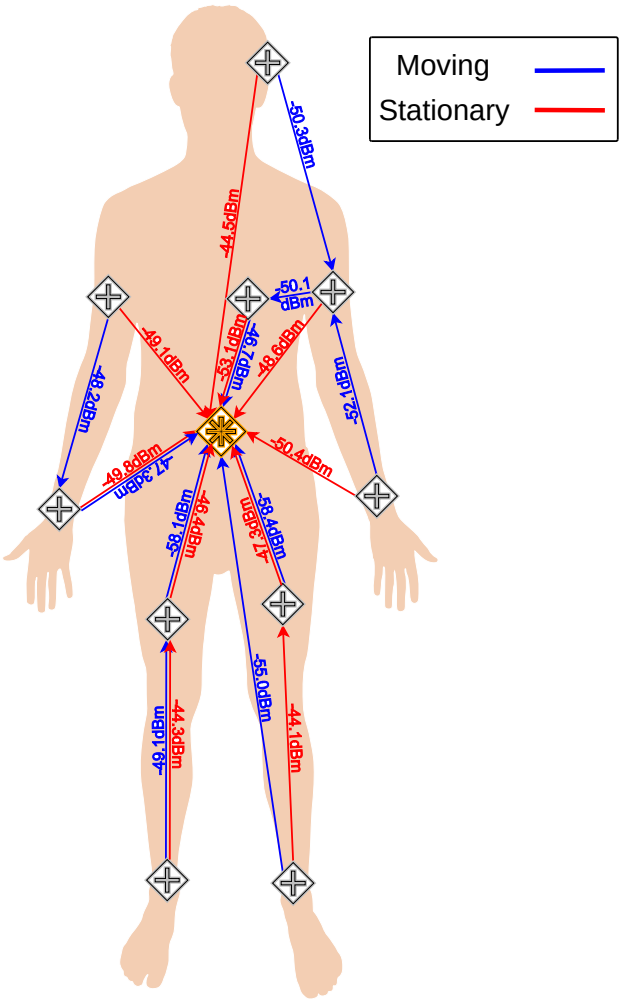

FIGURE 2.2: Optimal topology and power control scheme at the equilibrium formed by the proposed RSPCG for moving and stationary WBANs ($\underline{\lambda} = 10^{-12}$, $M = 800$ bits, $\Delta \geq 32.5$ ms and $\Theta \geq 168.6$ ms for moving WBAN, $\Delta \geq 16.1$ ms and $\Theta \geq 96.2$ ms for stationary WBAN)

2.6.3.2 Node Path Power Consumption

Cumulative power consumption over nodes' path to the hub is depicted in Figs. 2.3 and 2.4 for moving and stationary WBAN scenarios, respectively.

As evident in Figs. 2.3 and 2.4, mean and standard deviation of path power consumption for multi-hop transmission using RSPCG are noticeably less than those of the direct transmission using DTPC, especially in the moving scenario. This signifies how much RSPCG decreases power consumption and improves uniformity of power dissipation in the network in both moving and stationary cases.

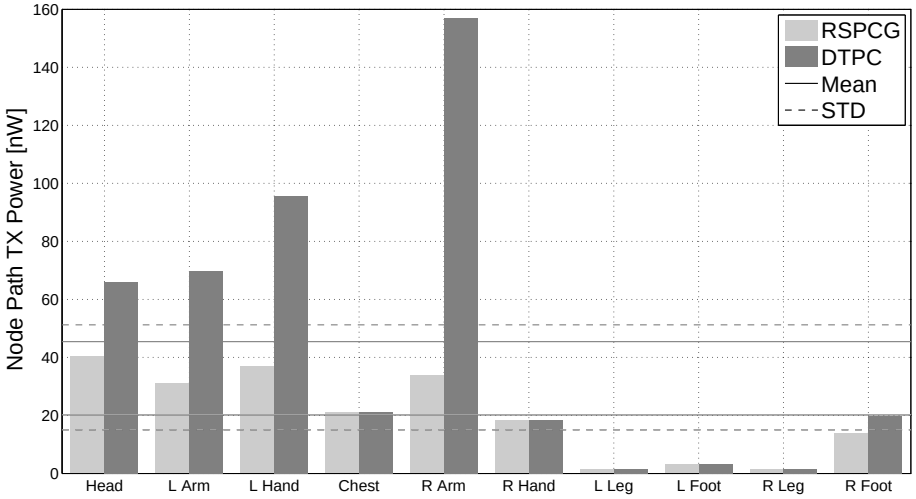

FIGURE 2.3: Node path transmit power consumption of RSPCG compared to DTPC for moving WBAN ($\underline{\lambda} = 10^{-12}$, $M = 800$ bits, $\Delta \geq 32.5$ ms and $\Theta \geq 168.6$ ms)

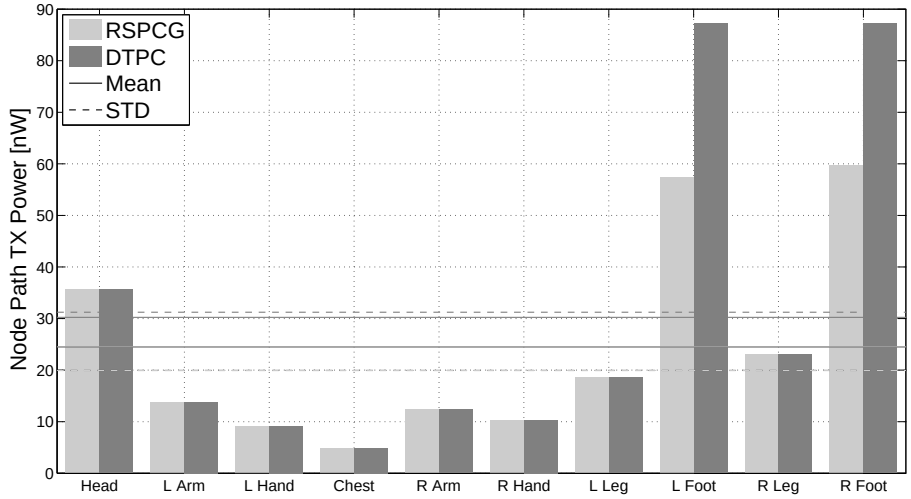

FIGURE 2.4: Node path transmit power consumption of RSPCG compared to DTPC for stationary WBAN ($\underline{\lambda} = 10^{-12}$, $M = 800$ bits, $\Delta \geq 16.1$ ms and $\Theta \geq 96.2$ ms)

Note that, since the architecture of the considered WBAN is almost symmetric with the hub located on the center waist of subject, the path power consumption of the mirror nodes is roughly the same in the stationary WBAN. However this does not hold in the moving scenario due to the motion variations, and therefore the LHand path, for instance, consumes significantly more power in comparison to the RHand path.

2.6.3.3 Energy Efficiency

Fig. 2.5 depicts the average utility per node of RSPCG compared to for DTPC and DT as the prescribed packet error rate increases in moving and stationary WBAN scenarios. Node utility as formulated in Sec. 2.5.1 signifies the energy efficiency of transmission.

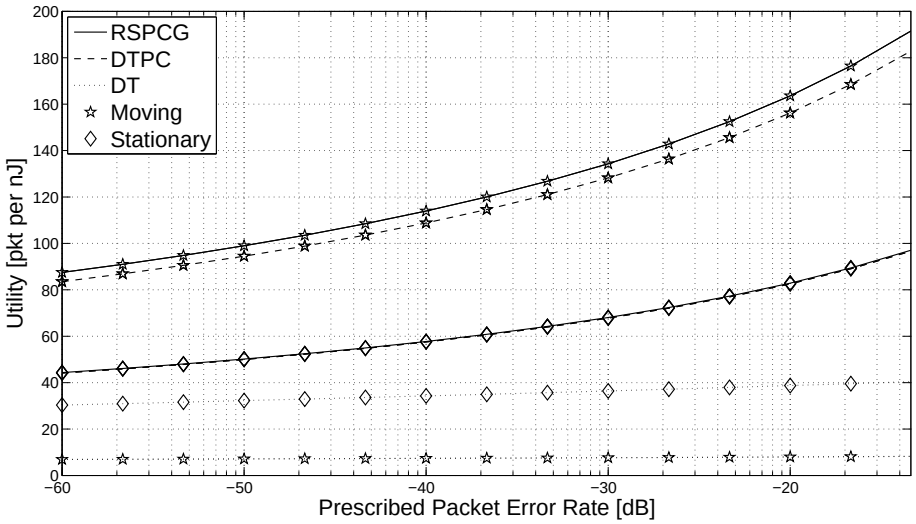

FIGURE 2.5: Average utility per node versus prescribed PER for moving and stationary WBANs ($M = 800$ bits, $\Delta \geq 32.5$ ms and $\Theta \geq 168.6$ ms for moving WBAN, $\Delta \geq 16.1$ ms and $\Theta \geq 96.2$ ms for stationary WBAN)

Raising the target packet error rate accordingly increases the utility. Note that RSPCG surpasses DT in terms of energy efficiency for both moving and stationary scenarios. However, the utility enhancement of the RSPCG is greater in the moving WBAN compared to the stationary case. RSPCG has a better energy efficiency performance compared to DTPC in the moving WBAN, while the two approaches yield comparable utilities in the stationary scenario. It is also noted from Fig. 2.5 that DT is a more profitable transmission approach in

the stationary WBAN compared to in the moving case, while the opposite holds for DTPC and particularly RSPCG.

Figs. 2.6 and 2.7 illustrate the node utility versus the prescribed packet error rate for nodes Head, LArm, and RFoot in moving and stationary WBAN scenarios, respectively. We opt not to show the results for the other nodes due to space limitations, but the performance behaviors follow similar trends as those presented.

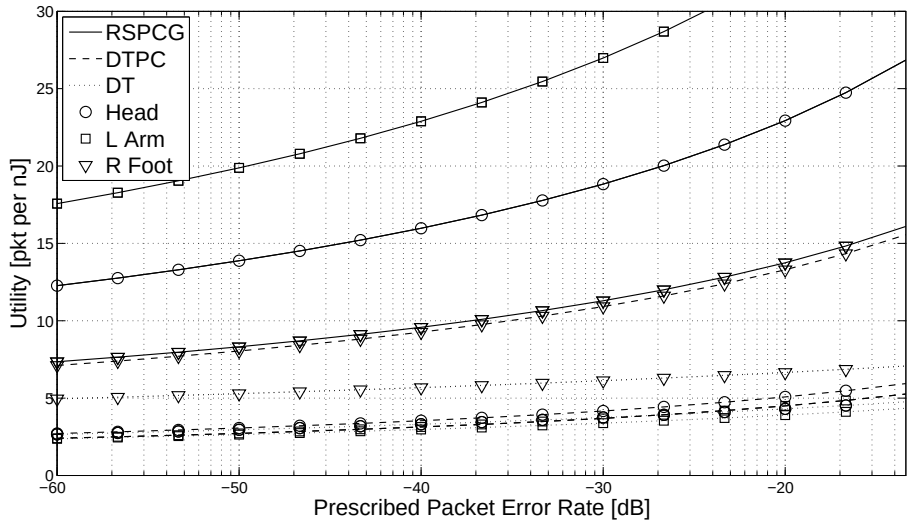

FIGURE 2.6: Utility of nodes Head, LArm, and RFoot versus prescribed PER for moving WBAN ($M = 800$ bits, $\Delta \geq 32.5$ ms and $\Theta \geq 168.6$ ms)

The utility of all the tree nodes resulting from RSPCG are higher than for the other transmission approaches in both moving and stationary scenarios. RSPCG in particular ameliorates the node energy efficiency in the moving WBAN where the quality of direct links to the hub are degraded due to body movements. For instance in Fig. 2.6, while the utilities resulting from DTPC and DT remain quite the same for nodes Head, LArm, RSPCG outperforms both approaches especially in higher target packet error rate values.

Note in the moving scenario in Fig. 2.6 that as the prescribed packet error rate increases, among the considered nodes LArm is the most beneficiary of RSPCG approach, while RFoot compared to Head gains less utility enhancement from RSPCG. That is because in the moving WBAN, the quality of the path RFoot takes in the lower half of the body is subject to a

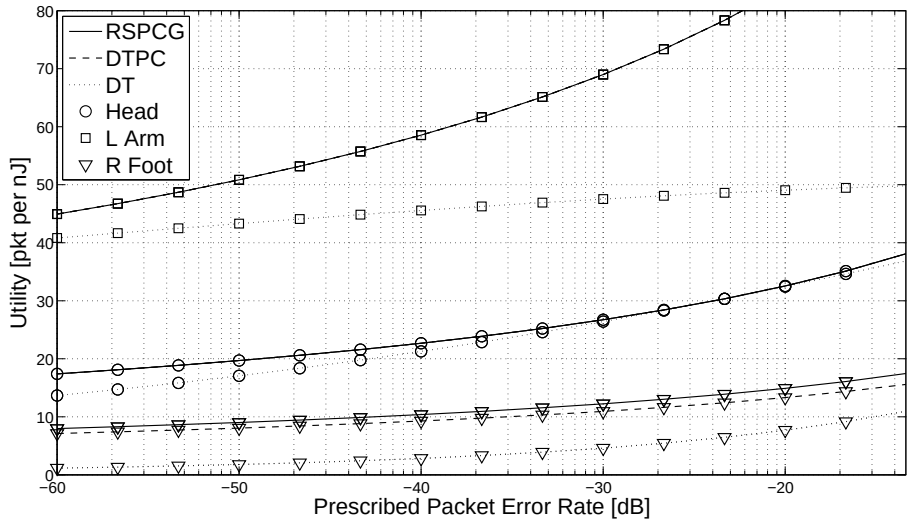

FIGURE 2.7: Utility of nodes Head, LArm, and RFoot versus prescribed PER for stationary WBAN ($M = 800$ bits, $\Delta \geq 16.1$ ms and $\Theta \geq 96.2$ ms)

higher degradation compared to the quality of Head's transmission path in the upper body half.

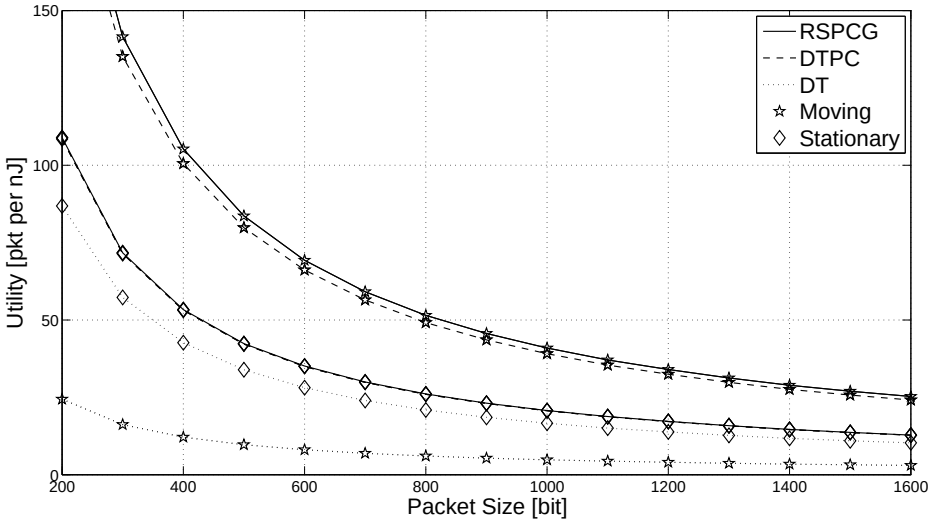

FIGURE 2.8: Average utility per node versus packet size for moving and stationary WBANs ($\underline{\lambda} = 10^{-12}$, $\Delta \geq 32.5$ ms and $\Theta \geq 168.6$ ms for moving WBAN, $\Delta \geq 16.1$ ms and $\Theta \geq 96.2$ ms for stationary WBAN)

Fig. 2.8 depicts the average utility per node of RSPCG compared to for the other two transmission approaches as the packet size increases in moving and stationary WBAN

scenarios.

Energy efficiency gradually declines as packets get larger for all cases. Note that RSPCG again outperforms the other two transmission approaches in both moving and stationary WBANs. The performance gain resulting from the RSPCG in the moving WBAN is again well above that for the stationary scenario.

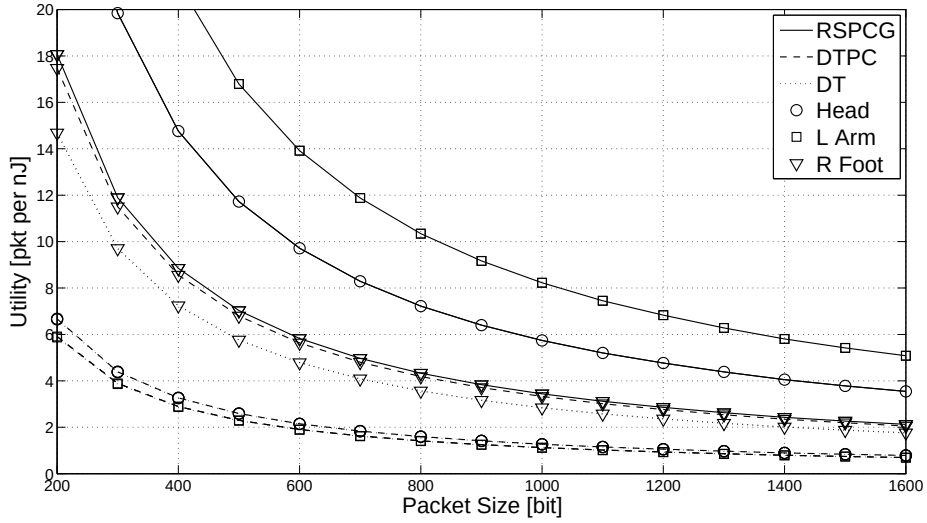

FIGURE 2.9: Utility of nodes Head, LArm, and RFoot versus packet size for moving WBAN ($\underline{\lambda} = 10^{-12}$, $\Delta \geq 32.5$ ms and $\Theta \geq 168.6$ ms)

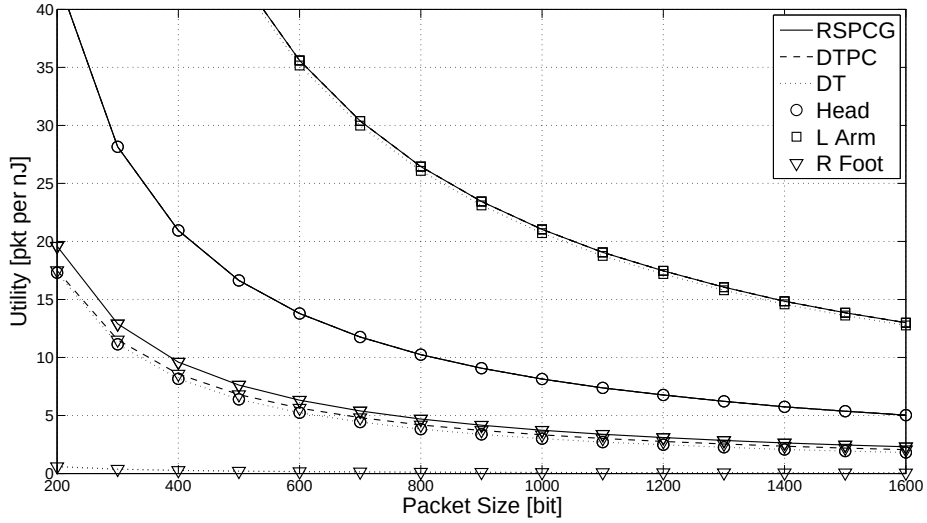

FIGURE 2.10: Utility of nodes Head, LArm, and RFoot versus packet size for stationary WBAN ($\underline{\lambda} = 10^{-12}$, $\Delta \geq 16.1$ ms and $\Theta \geq 96.2$ ms)

The node utility versus packet size for nodes Head, LArm, and RFoot is illustrated in Figs. 2.9 and 2.10 in moving and stationary WBANs, respectively.

Again RSPCG yields a higher energy efficiency for all the tree nodes compared to the other transmission approaches, especially in the moving WBAN.

Figs. 2.11 and 2.12 depict the node utility resulting from RSPCG versus the QoS constraints for nodes Head, LArm, and RFoot in moving and stationary WBAN scenarios, respectively.

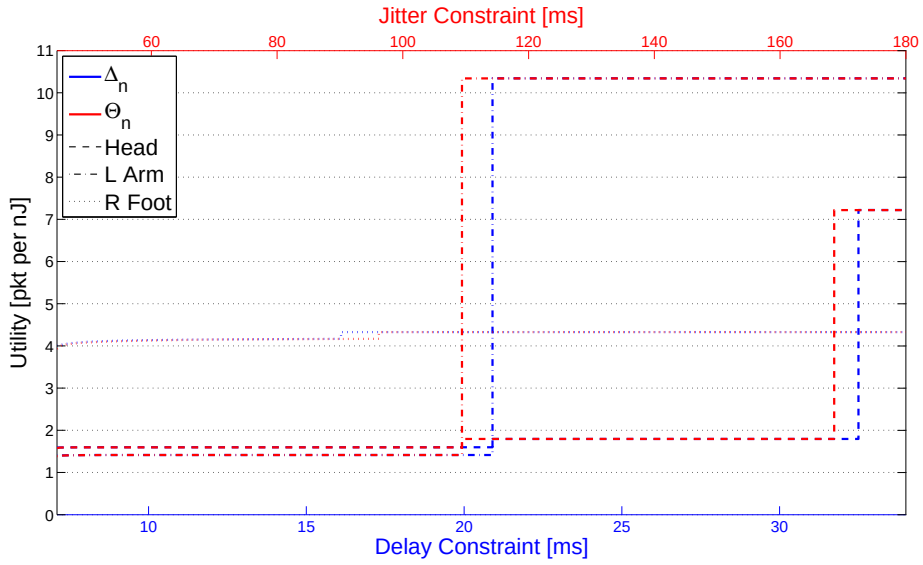

FIGURE 2.11: Utility of nodes Head, LArm, and RFoot resulting from RSPCG versus delay and jitter constraints for moving WBAN ($\underline{\lambda} = 10^{-12}$, $M = 800$ bits)

As the permissible end-to-end delay and jitter increase, nodes are likely to increase their number of transmission hops in order to guarantee their maximum achievable utility.

In Fig. 2.11 for instance, in order to adhere to the lowest possible upper bounds on delay and jitter (*i.e.*, $\Delta_{10} = 6.9$ ms and $\Theta_{10} = 44$ ms), node RFoot has to take a direct transmission strategy to the hub with a power choice higher than its optimal direct transmit power. As the delay and jitter constraints relax, RFoot is allowed to adjust its transmit power and steadily improve its utility, until the node reaches its optimal direct transmit power after which point it no longer improve its energy efficiency while directly transmitting. The utility of RFoot therefore remains constant until the QoS constraints are relaxed enough so that the

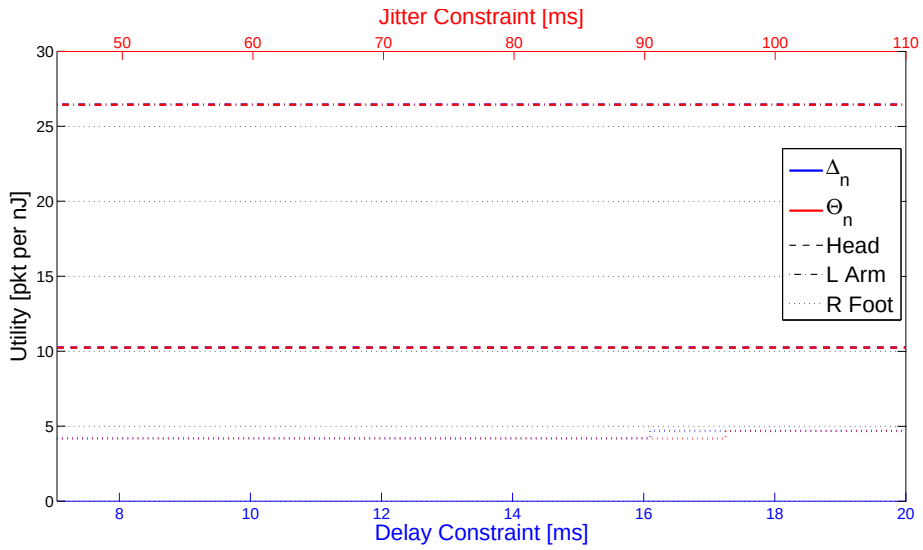

FIGURE 2.12: Utility of nodes Head, LArm, and RFoot resulting from RSPCG versus delay and jitter constraints for stationary WBAN ($\underline{\lambda} = 10^{-12}$, $M = 800$ bits)

node can choose a two-hop transmission path to the hub (at $\Delta_{10} = 16.1$ ms and $\Theta_{10} = 96.2$ ms). Note that there are leaps on corresponding diagrams at this point in Fig. 2.11. The node utility remains unchanged for higher QoS constraints.

In Fig. 2.11, note that the diagrams associated with LArm and RFoot has only one leap each, while there are two leaps on the diagrams for Head. That is because when QoS constraints allow, Head increases its transmission hops to three in order to maximize its energy efficiency.

Also in Fig. 2.12, there is a leap in the utility of RFoot when it changes its direct transmission approach to two-hop transmission (at $\Delta_{10} = 16.1$ ms and $\Theta_{10} = 96.2$ ms), but the utilities of the other two nodes remain unchanged for different QoS constraints.

2.6.3.4 End-to-End QoS

Fig. 2.13 depicts the average end-to-end delay per node resulting from RSPCG compared to DTPC and DT as the packet size increases in moving and stationary WBAN scenarios. Larger packet size entails a higher service time as it increases both the transmission time as well as the packet error rate, which in turn result in a higher end-to-end latency. Note that

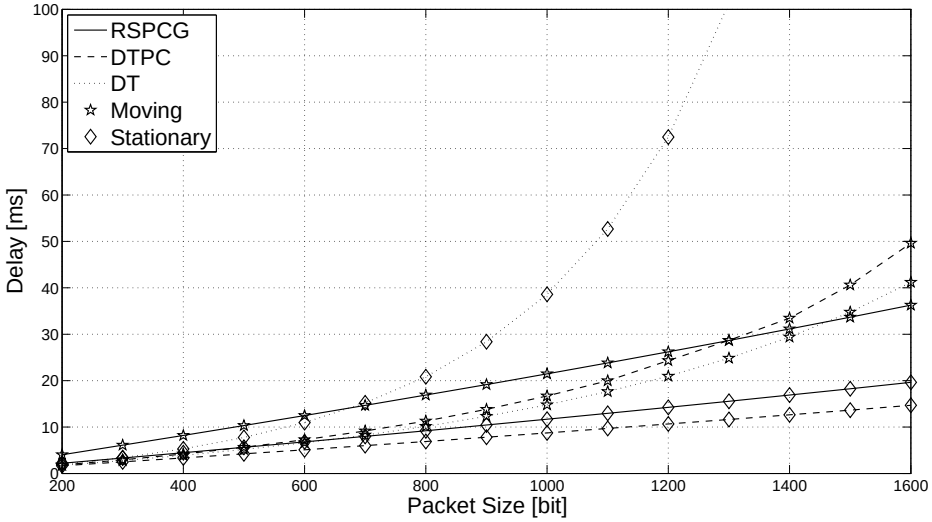

FIGURE 2.13: Average end-to-end delay per node versus packet size for moving and stationary WBAN scenarios ($\underline{\lambda} = 10^{-12}$)

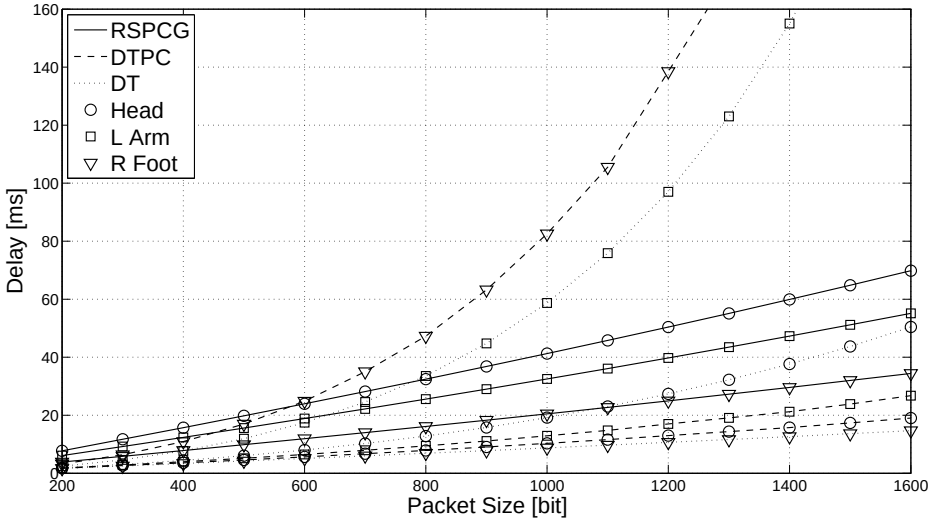

FIGURE 2.14: End-to-end delay of nodes Head, LArm, and RFoot versus packet size for moving WBAN ($\underline{\lambda} = 10^{-12}$)

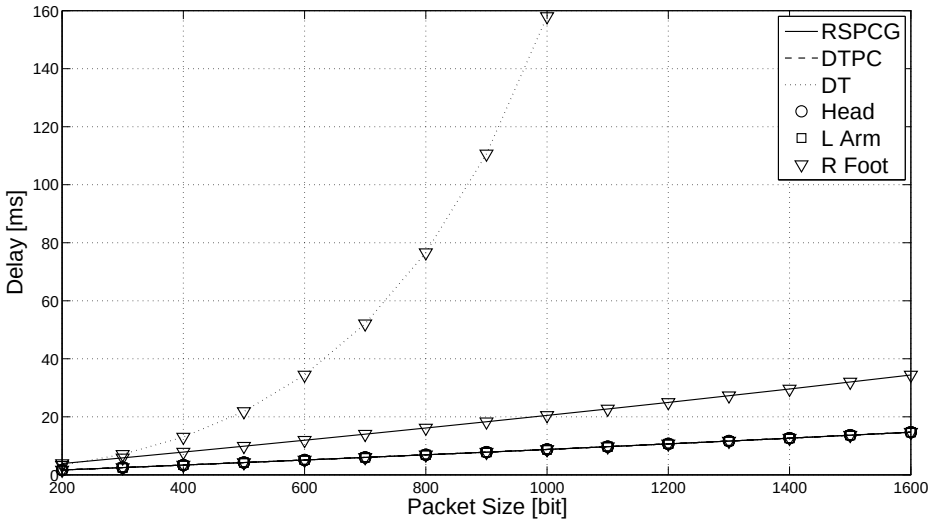

FIGURE 2.15: End-to-end delay of nodes Head, LArm, and RFoot versus packet size for stationary WBAN ($\underline{\lambda} = 10^{-12}$)

RSPCG introduces some extra delay to the system as expected. Yet as the packets get larger, the packet error rate for direct transmission rises at a higher pace compared to for RSPCG which results in considerably higher delays of DT and DTPC for longer packets compared to RSPCG. Also for the RSPCG, the average end-to-end delay in the moving WBAN is higher compared to the stationary WBAN which stems from the higher number of hops in the moving scenario.

The end-to-end delay versus packet size for nodes Head, LArm, and RFoot is presented in Figs. 2.14 and 2.15 in moving and stationary WBANs, respectively.

Fig. 2.16 illustrates the average end-to-end jitter per node for different transmission approaches versus the packet size in moving and stationary WBAN scenarios. Note that packet jitter is substantially higher than delay in all cases. The same trends can be observed here as were noted in Fig. 2.13, *e.g.*, the end-to-end jitter for direct transmission increases at a higher pace compared to that of RSPCG as the packets get larger.

Also the end-to-end jitter versus packet size for nodes Head, LArm, and RFoot is presented in Figs. 2.17 and 2.18 in moving and stationary WBANs, respectively.

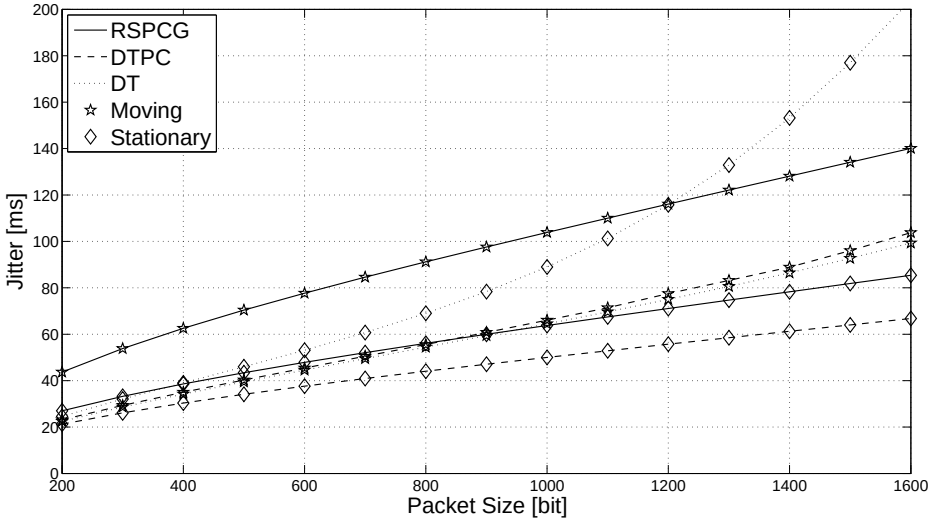

FIGURE 2.16: Average end-to-end jitter per node versus packet size for moving and stationary WBAN scenarios ($\underline{\lambda} = 10^{-12}$)

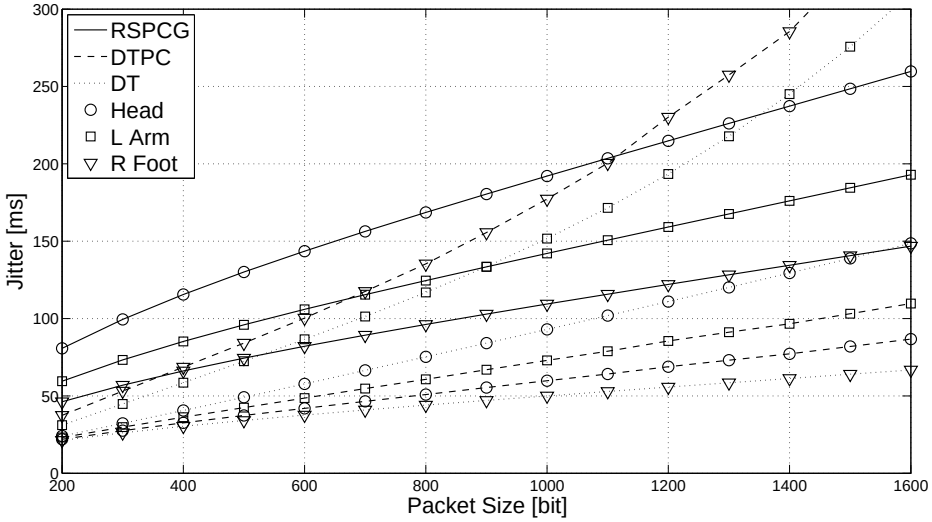

FIGURE 2.17: End-to-end jitter of nodes Head, LArm, and RFoot versus packet size for moving WBAN ($\underline{\lambda} = 10^{-12}$)

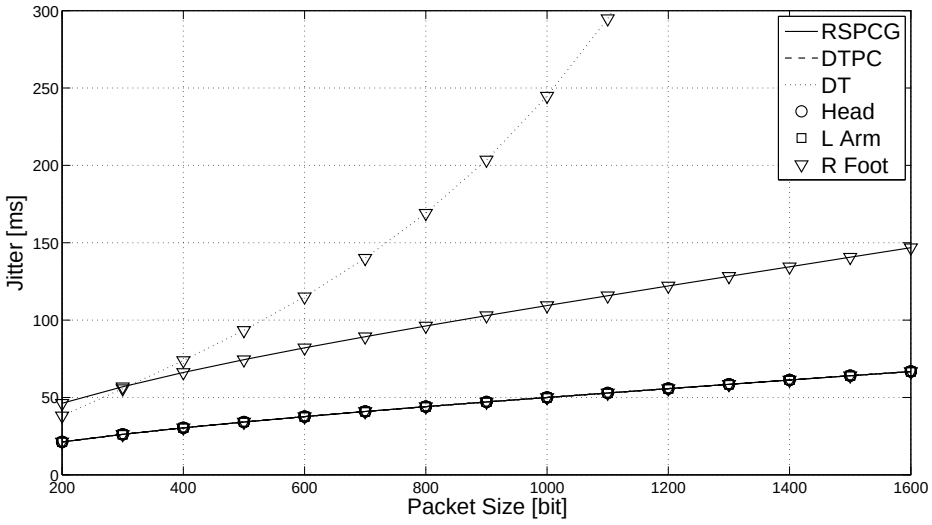

FIGURE 2.18: End-to-end jitter of nodes Head, LArm, and RFoot versus packet size for stationary WBAN ($\underline{\lambda} = 10^{-12}$)

2.6.3.5 Number of Transmission Hops

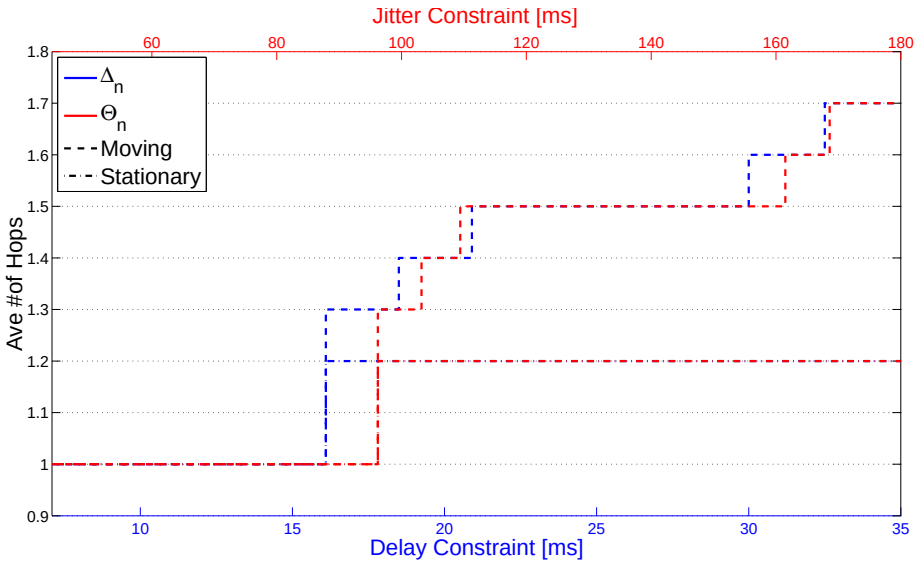

FIGURE 2.19: Average number of transmission hops per node resulting from RSPCG versus delay and jitter constraints for moving and stationary WBANs ($\underline{\lambda} = 10^{-12}$, $M = 800$ bits)

Fig. 2.19 illustrates the effect of QoS constraints on the Nash topology of the WBAN. As the QoS constraints increase, more nodes consider multi-hop transmission to enhance their energy efficiency. Note that the QoS constraints, in effect, bound the maximum number of connections a node can accept in the uplink. That is because as the number of descendants

of a node increases, both the expected value and variance of the packet inter-arrival time for the node rise (see Eqs. (2.10) and (2.11)), leading to a higher delay at the node (Eq. (2.21)) and, in turn, over the entire path to the hub.

Note that the minimum delay and jitter constraints for the given parameter values are 6.9 ms and 44 ms, respectively, which corresponds to the case of direct transmission to the hub with zero packet error rate.

2.6.3.6 Number of Algorithm Iterations

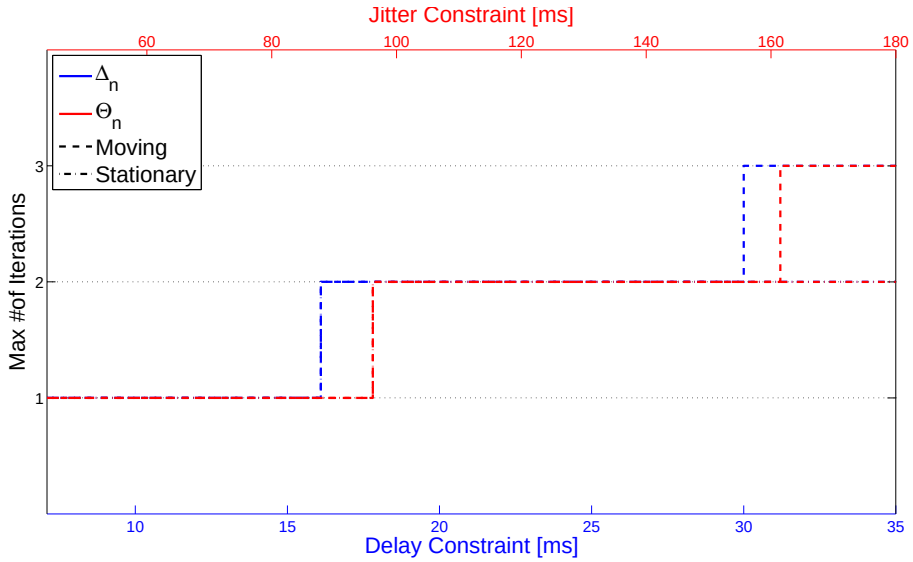

FIGURE 2.20: Maximum number of iterations till convergence to a Nash solution resulting from RSPCG versus delay and jitter constraints for moving and stationary WBAN ($\underline{\lambda} = 10^{-12}$, $M = 800$ bits)

Fig. 2.20 shows the effect of QoS constraints on the number of algorithm iterations till convergence to a Nash solution, starting with the star topology.

For higher QoS constraints, nodes are more likely to consider relay transmission which, in turn, induces more iterations for the algorithm to converge. The number of iterations till convergence to a Nash topology differs depending on the sequence of nodes taking action. The maximum number of iterations is therefore considered, which remains lower than or equal to 3 in all cases as evident in Fig. 2.20.

2.7 Conclusion and Future Work

A non-cooperative game framework is developed to analyze the problem of QoS-constrained relay selection and power control in multi-hop WBANs, wherein each sensor node, under fading conditions, seeks to maximize its transmission energy efficiency while satisfying its end-to-end delay and jitter requirements. We prove the existence of Nash equilibrium for the proposed game, analytically characterize the Nash power control solution, and provide a distributed algorithm that converges to a Nash topology.

The game theoretic analysis is then employed to examine the performance behaviors in an IEEE 802.15.6-based UWB WBAN, considering various scenarios with respect to transmission approach as well as the body motion. Equilibrium results suggest RSPCG is particularly germane to moving WBANs where channel conditions change frequently. It is observed that nodes are more inclined towards taking a multi-hop transmission strategy in the moving scenario compared to the stationary case. RSPCG decreases power consumption and enhances uniformity of power dissipation in the network. Furthermore, it improves energy efficiency performance of the WBAN at the expense of an admissible increase in the end-to-end delay and jitter.

A future direction is to incorporate physical layer security considerations into the game framework in the presence of eavesdroppers. In terms of implementation plausibility, it should also behoove us to assess and quantify the propriety of the model parameters and assumptions in the context of various practical application scenarios.

Chapter 3

Delay-Aware Optimization of Spatial Diversity with Respect to Physical Layer Security in Wireless Body Area Networks

Once the problem of energy efficiency with QoS provisioning is properly addressed, the next logical step is to secure the communication links in the WBAN, which is studied in this chapter. Note that the combination of energy efficiency and security into a unified WBAN solution is discussed later in Chap. 4.

This chapter includes a manuscript entitled "Delay-Aware Optimization of Spatial Diversity with Respect to Physical Layer Security in Wireless Body Area Networks" by Hussein Moosavi and Francis Minhthang Bui, submitted to the *IEEE Transactions on Information Forensics and Security*, on August 2015. This work was supported in part by funding from the Natural Sciences and Engineering Research Council of Canada (NSERC).

Joint optimization of the physical layer security with end-to-end latency provisioning is studied in the uniquely constrained context of wireless body area networks. A game-theoretic

framework is proposed wherein body-worn health-care devices interact in the presence of wiretappers and under fading channel conditions to find the most secure multi-hop path to the hub while adhering to the end-to-end delay requirement imposed by the application. We model the problem as the search for a Nash network topology where no unilateral deviation in strategy by any single sensor node improves the secrecy of it transmissions, and provide a distributed algorithm guaranteed to converge to a stable Nash solution. The framework is evaluated using numerical simulations in conditions approximating actual deployment of wireless body area networks for moving and stationary scenarios. Results validate the merits of the proposed framework to improve the security of transmissions compared to the star topology and IEEE 802.15.6 two-hop topology extension schemes at the cost of an admissible increase in the end-to-end delay.

3.1 Introduction

Wireless body area networks (WBANs) are at the forefront of emerging technologies in the trend towards personalized mobile health-care. A WBAN typically consists of several sensor nodes that measure the physiological and contextual data profiling the human body activities, and a central hub to which the sensors wirelessly communicate the collected vital signs for monitoring purposes.

For many networking applications, notably those in medical settings, it is critical that the communication links in a WBAN system are secure and reliable. This is because a WBAN system in these applications typically needs to handle medical data with stringent confidentiality and liability requirements. That said, enabling secure transmission among such body-worn wireless devices is a significant challenge given the operating conditions and constraints in WBANs. Sensor nodes with low power and computational capabilities are in close proximity of one another and channel variations are complex and unpredictable due to motion, shadowing effects of the human body and multipath propagation. Furthermore, the broadcast nature of the wireless medium leaves WBANs highly prone to eavesdropping and raises the probability of security lapses.

3.1.1 Related Works

Secure communications are conventionally realized through cryptographic techniques at the upper layers of the wireless network protocol stack, which relies on the computational difficulty of certain mathematical tasks. However, the overhead associated with complex encryption algorithms make them less feasible for implementation in wireless body-worn solutions with resource constraints.

An alternative approach is to secure transmissions at the wireless physical layer (PHY) by leveraging information theoretic principles [35]. PHY security exploits the random characteristics of wireless channels, such as fading or noise, to enhance transmission secrecy without requiring encryption keys.

Wyner suggested in his seminal work [58] that perfect secrecy is achievable using only the characteristics of the wireless channel subject to the condition that the wiretap channel is more noisy than that of the legitimate nodes. The key concept that characterizes this approach to PHY security is the secrecy capacity, *i.e.*, the maximum rate of secret information achievable between a legitimate transmitter-receiver pair without being tapped by an unauthorized receiver [59, 60].

The ergodic secrecy rate is ill-defined under finite delay constraints in a practical WBAN. It is likely that the instantaneous channel state information (CSI) of the legitimate channel is unknown to the transmitter due to the severe fading of radio signals near the human body. Besides, it is realistic to assume the transmitter only has the statistics on the wiretap channel at its disposal, as the wiretapper has no incentive to let the transmitter know its channel state information. It is therefore appropriate to adopt the secrecy outage probability (SOP) to evaluate the secrecy performance of transmissions, which signifies the fraction of fading realizations where a prescribed secrecy rate is guaranteed.

The other obstacle arising from the fading conditions in WBANs is that the secrecy capacity may be severely limited when sensor nodes directly communicate to the hub, due to the degradation of effective received signal-to-noise ratio (SNR). Multi-hop relaying is

a potential strategy to cope with the problem, as it has been recognized as an effective technique in WBANs to combat wireless fading and improve link throughput by exploiting the spatial diversity [61–63]. In this respect, PHY security of multi-hop communications in general wireless settings has recently been studied and shown to be promising to enhance the secrecy capacity of wireless channels [10–12, 64–66].

Note that exploiting spatial diversity through multi-hop transmission comes with the cost of introducing extra delay to the system. It is therefore prudent to capture the impact of multi-hop relaying on the end-to-end latency in the analysis, which is particularly critical for scheduling allocation intervals and real-time monitoring requirements of the WBAN.

3.1.2 Summary of Contributions

This work investigates the problem of delay-aware optimization of PHY security in the context of WBANs. The main contributions of the work are as follows.

- A system model is provided for intra-WBAN multi-hop communications of body-worn devices in the uplink in the presence of off-body wiretappers.
- The secrecy outage probability is adapted in this context as the performance metric as it is more meaningful in realistic fading channels compared with the ergodic secrecy rate.
- The average end-to-end delay for multi-hop transmission in a slotted Aloha medium access WBAN is characterized.
- A multi-hop topology formation game (MTFG) is proposed that formally formulates the problem of jointly optimizing the PHY secrecy outage probability with end-to-end delay provisioning in the uplink of a multi-hop WBAN. The convergence of the algorithm to a stable Nash topology is proved.
- The proposed game framework is evaluated using numerical simulations in conditions approximating actual deployment of WBANs for moving and stationary scenarios. The

impact of various PHY parameters on the performance behaviors of the system is examined. The framework shows remarkable promise in significantly improving the PHY secrecy of transmissions, compared to that in the star topology and IEEE 802.15.6 two-hop topology extension schemes, at the cost of an admissible increase in the end-to-end delay.

3.1.3 Paper Organization

The rest of the paper proceeds as follows. Sec. 3.2 presents the system model. PHY security and end-to-end latency are characterized in Secs. 3.3 and 3.4, respectively. The multi-hop topology formation game is formulated in Sec. 3.5. Numerical simulation results are provided and the proposed framework is validated in Sec. 3.6. Finally, Sec. 3.7 concludes the paper.

3.2 System Model

We consider a WBAN composed of N on-body sensor nodes transmitting their sensed data to a common hub H in the uplink, while W passive wiretappers are present in the vicinity who can individually tap into the sensor nodes' communications.

Let $\mathcal{N}$ and $\mathcal{W}$ denote the sets of all sensor nodes and wiretappers, respectively. Fig. 3.1 illustrates the system model.

Besides the signal attenuation due to geometric signal spreading, all legitimate and wiretap channels also experience small-scale fading, that is, fluctuations caused by arrival of signal by multiple propagation paths.

The legitimate channel is typically modeled to undergo log-normal fading [6, 43]. Therefore, the received SNR from an on-body sensor node $n \in \mathcal{N}$ as measured at another on-body node follows a log-normal distribution, with the following PDF

$$f(\gamma_n) = \frac{1}{\gamma_n \sigma_n \sqrt{2\pi}} \exp\left[-\frac{(\gamma_n^{\mathrm{dB}} - \mu_n)^2}{2\sigma_n^2}\right], \tag{3.1}$$

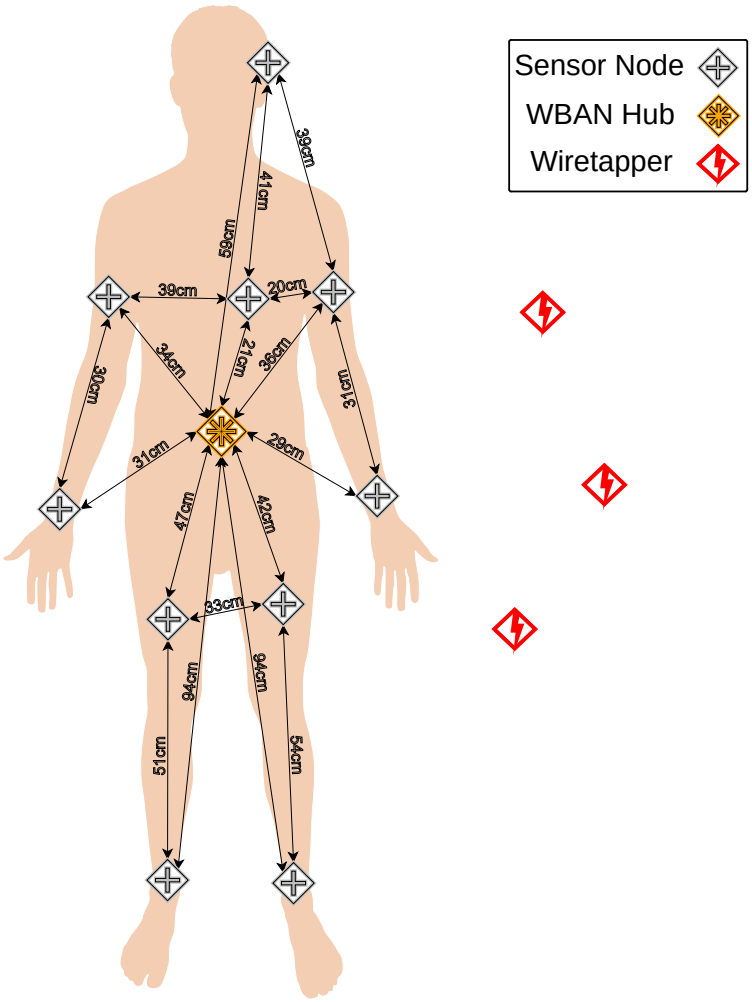

FIGURE 3.1: A typical WBAN with off-body wiretappers in the vicinity

where μ_n and σ_n denote the mean and standard deviation of the received SNR γ_n in dB, respectively. (The receiver's index is not specifically indicated in Eq. (3.1) for notational convenience, but note that the SNR measurements at different receiver nodes are varied due to their different communication channels.)

The off-body wiretap channel is modeled as small-scale Rayleigh fading [6]. Therefore, the received SNR γ_w from a sensor node as measured at a wiretapper $w \in \mathcal{W}$ follows an exponential distribution with parameter λ_w

$$f(\gamma_w) = \lambda_w \exp(-\lambda_w \gamma_w). \tag{3.2}$$

As the wiretappers are relatively far away from the WBAN, without loss of generality and for brevity of exposition all signals received by a wiretapper are assumed to experience identical fading conditions and path loss attenuation.

Within the WBAN, each sensor node may either directly transmit its packets to the hub or it may exploit spatial diversity by choosing a multi-hop transmission path. This results in a network topology graph $G(\mathcal{V},\mathcal{E})$ with $\mathcal{V} = \mathcal{N} \cup \{\mathsf{H}\}$ denoting the set of all vertices and $\mathcal{E}$ denoting the set of all the edges. We formally define a transmission path as follows.

Definition 3.1 (Path)**.** A K-hop uplink path in the graph G from a node $n \in \mathcal{N}$ to another node $i \in \mathcal{V}$ is defined as a sequence of nodes $\langle m_1, \cdots, m_{K+1} \rangle$ such that $m_1 = n$, $m_{K+1} = i$, and the link $\langle m_k, m_{k+1} \rangle \in \mathcal{E}$ $\forall k \in \{1, \cdots, K\}$. ■

The final network architecture in the uplink therefore is a tree topology whereby each sensor node $n \in \mathcal{N}$ is connected to the hub through a single path denoted by $l_n = \langle n, \cdots, \mathsf{H} \rangle$. The assumption is that intermediate nodes are willing to relay the packets of their peers. The limitations on how many relays each node can reliably support is discussed later in Sec. 3.5.1.

There are two random access methods outlined in the IEEE 802.15.4 for obtaining the contended allocations in a WBAN, namely carrier sense multiple access with collision avoidance (CSMA/CA) and slotted Aloha access [50]. Here, we consider the slotted Aloha as the medium access protocol for demonstration purposes.

3.2.1 Slotted Aloha medium access in IEEE 802.15.6

Here, we briefly summarize the slotted Aloha protocol, as described in more detail in [50]. The protocol restricts the sensor nodes to transmit only at the beginning of discrete time slots. Each node maintains a contention probability (CP) to determine if it obtains a new contended allocation in an Aloha slot. A node that has a packet to transmit starts the slotted Aloha access by setting its CP to $CP_{\max}$ which equals $\frac{3}{8}$. (We consider a user priority of 5 for all the sensor nodes designated to medical data or network control traffic.) The

node then draws a value z from the interval [0, 1] at random and obtain the contended slot for transmission if $z \leq CP$. Otherwise, the node backs off until the next time slot before contending for another allocation.

When a node transmits a packet but the destination fails to receive it, the node shall halve its CP for even number of consecutive failures or keep CP unchanged otherwise. Note that the node shall set its CP to $CP_{\min}$ if halving the CP makes it smaller than $CP_{\min}$ which equals $\frac{3}{16}$.

3.3 Characterization of PHY Security

We do not address the issue of authentication, which is a distinct problem beyond the scope of this paper. Instead, we assume the initial trust is already established between legitimate nodes in the WBAN during the bootstrapping phase, and the identity of nodes (*i.e.*, whether they are malicious or honest) is common knowledge in the network.

Our threat model considers one or more wiretappers in the vicinity of WBAN. Each wiretapper samples the channel at the same time as the legitimate sensor nodes, but measures a different multipath channel, as it is separated from the communicating parties by a distance greater than one radio wavelength (approximately 67 mm for the 4492.8 MHz working frequency) [67].

We adopt Wyner's wiretap channel model [58] to characterize the secrecy of transmission from an information-theoretic perspective. The transmitter's objective is to find an encoding scheme that simultaneously achieves arbitrarily small probability of decoding error at the legitimate receiver and zero mutual information between the transmitted message and the received signal at the wiretapper. Using Wyner's encoding scheme, each transmitting sensor node chooses two rate parameters, namely, the rate of the actual messages R and the rate of transmitted codewords R'. When the rate redundancy $R' - R$ is larger than the channel capacity of the best wiretapper link, perfect secrecy is guaranteed. Moreover, the

codeword rate R' must be less than the channel capacity of the legitimate receiver so it can decode the transmitted message with negligibly small error.

Therefore, the achievable secrecy rate (ASR) for a single-hop link with Gaussian signaling between a sensor node $n \in \mathcal{N}$ and another node $i \in \mathcal{V}$ is given by

$$\begin{aligned} R_{\langle n,i \rangle} &= \left[C_{\langle n,i \rangle} - \max_{1 \leq w \leq W} C_{\langle n,w \rangle} \right]^+ \\ &= \left[\log_2(1+\gamma_n) - \max_{1 \leq w \leq W} \log_2(1+\gamma_w) \right]^+, \end{aligned} \tag{3.3}$$

where $C_{\langle n,i \rangle}$ is the Shannon capacity of the legitimate channel, $C_{\langle n,w \rangle}$ is the Shannon capacity of the w^{th} wiretap channel, and $x^+ \triangleq \max\{x,0\}$.

For a target secrecy rate $\underline{R}$, the SOP of the single-hop link between n and i is

$$\begin{aligned} P^{\text{out}}_{\langle n,i \rangle} &= \Pr\left\{ R_{\langle n,i \rangle} < \underline{R} \right\} = \Pr\left\{ \log_2 \frac{1+\gamma_n}{1+\gamma_{\bar{w}}} < \underline{R} \right\} \\ &= \Pr\left\{ \gamma_{\bar{w}} > 0,\, 2^{\underline{R}}(\gamma_{\bar{w}}+1) - 1 > \gamma_n > 0 \right\}, \end{aligned} \tag{3.4}$$

where $\bar{w} \in \mathcal{W}$ is the wiretapper with the best channel. Therefore,

$$\begin{aligned} P^{\text{out}}_{\langle n,i \rangle} &= \int_{\gamma_{\bar{w}}=0}^{\infty} \int_{\gamma_n=0}^{2^{\underline{R}}(\gamma_{\bar{w}}+1)-1} f(\gamma_n) f(\gamma_{\bar{w}})\, d\gamma_n\, d\gamma_{\bar{w}} \\ &= \int_0^{\infty} \Phi\left(\frac{\left[2^{\underline{R}}(\gamma_{\bar{w}}+1) - 1 \right]^{\text{dB}} - \mu_n}{\sigma_n} \right) \lambda_{\bar{w}} \exp(-\lambda_{\bar{w}} \gamma_{\bar{w}})\, d\gamma_{\bar{w}}, \end{aligned} \tag{3.5}$$

where Φ is the cumulative distribution function of the standard normal distribution and is defined as

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} \exp(-\frac{t^2}{2})\, dt.$$

For multi-hop transmissions, we assume independent randomization is used in the codebooks at each hop to avoid the diversity combining at the wiretapper. Therefore, the secrecy outage occurs regardless of which hop suffers from the outage. The SOP of a K-hop

transmission path $l = \langle m_1, \cdots, m_{K+1} \rangle$, in turn, is obtained as follows

$$P_l^{\text{out}} = 1 - \prod_{k=1}^{K} \left(1 - P_{\langle m_k, m_{k+1} \rangle}^{\text{out}}\right). \tag{3.6}$$

As the received SNR over short single hops in multi-hop transmission improves compared to the received SNR over the direct link, the SOP of multi-hop link is expected to be significantly smaller than the SOP for direct transmission.

3.4 Characterization of End-to-End Latency

Multi-hop transmission, although allowing for exploiting spatial diversity, introduces additional queuing and medium access delay at each relay node.

The traffic load of each node comprises the node's own generated traffic as well as the traffic forwarded to the node by its descendants to be relayed. That is, each sensor node has its unique traffic load. The packet service time at each node also differs from one node to another as it depends on the characteristics of the medium access protocol and the physical constraints imposed by the tree structure of the network graph. It is, therefore, realistic to assume that both inter-arrival and service times at each node follow general distributions. Furthermore, we assume each sensor node acts as one server which is able to handle one packet at a time with a first-come, first-served service discipline. Therefore, we can describe each sensor node as a GI/G/1 queue [52].

We first obtain the moment generating functions of the probability distributions of the packet inter-arrival time and service time at each sensor node, which later are used to derive the average end-to-end delay over a multi-hop WBAN path.

3.4.1 Traffic Distribution

The traffic load of sensor nodes can be quantified using the underlying topology of the network and the inter-arrival distributions of the packets. Let $\mathcal{C}_n$ be the set of children (immediate descendants) of a node $n \in \mathcal{N}$ in the tree structure. Also let us denote the inter-arrival distribution of packets at the MAC layer of n by A_n, with the moment generating function M_{A_n}. This distribution comprises the inter-arrival time of packets generated by node n itself with moment generating function of $M^n_{A_n}$, and the inter-arrival time of packets received successfully from the children of node n to be relayed in the uplink with moment generating function of $M^{\mathcal{C}_n}_{A_n}$. These two inter-arrival times are statistically independent and, therefore, the moment generating function of their sum is given by

$$M_{A_n}(t) = M^n_{A_n}(t) M^{\mathcal{C}_n}_{A_n}(t). \tag{3.7}$$

Note that the inter-arrival distribution of packets successfully received by node n is the aggregated inter-departure times of packets from the children of n. As these inter-departure times are also pairwise independent random variables, $M^{\mathcal{C}_n}_{A_n}$ can be given by

$$M^{\mathcal{C}_n}_{A_n}(t) = \prod\nolimits_{c \in \mathcal{C}_n} M_{D_c}(t), \tag{3.8}$$

where M_{D_c} denotes the moment generating function of the inter-departure distribution of packets from node c.

Now let us denote the service time distribution of packets at n by S_n, with the moment generating function M_{S_n}. Given the moment generating functions of the inter-arrival time and the service time of packets at node n, the moment generating function of the inter-departure distribution of packets form node n can be approximated by [68]

$$M_{D_n}(t) = \rho_n M_{S_n}(t) + (1 - \rho_n) M_{S_n}(t) M_{A_n}(t), \tag{3.9}$$

where ρ_n is the utilization factor of node n and is given by $\frac{\mathbf{E}[S_n]}{\mathbf{E}[A_n]}$.

We assume the queues are stable, *i.e.*, $\rho_n \leq 1 \; \forall n \in \mathcal{N}$. To prevent an over-saturated condition in the network, we also assume the transmission rate of each node is greater than the accumulated traffic rate forwarded by the node.

Given Eqs. (3.7), (3.8), and (3.9), and using the first and second moments of A_n, the expected value and variance of the packet inter-arrival time at each sensor node can be obtained.

3.4.2 Transmission Time Distribution

We consider a WBAN wherein the sensor nodes seek access to the shared wireless medium using slotted Aloha. Similar lines of reasoning can be followed to derive the distribution of transmission time in a CSMA/CA-based multi-hop WBAN [55].

Each Aloha slot shall be greater than or equal to the time required to transmit a packet, that is

$$\tau = \frac{L_b}{R} + \varepsilon \approx \frac{L_b}{R}, \tag{3.10}$$

where L_b and R are the packet length (in bits) and date transmission rate, respectively. In Eq. (3.10), ε represents the time taken for a node to receive an ACK/NACK from its destination and is assumed to be negligible compared to $\frac{L_b}{R}$.

Let T_n denote the probability distribution for the time required to transmit a packet from the instance a node n starts the slotted Aloha access process until it finishes transmission. It is evident that T_n follows a geometric distribution with the probability mass function given by

$$\Pr\{T_n = k\tau\} = CP_n(1 - CP_n)^{k-1} \qquad k = 1, 2, \cdots, \tag{3.11}$$

where CP_n is the contention probability maintained by node n.

Then the moment generating function of the transmission time distribution from node n is

$$M_{T_n}(t) = \mathbf{E}[e^{tT_n}] = \sum_{k=1}^{\infty} CP_n(1 - CP_n)^{k-1} e^{tk\tau} = \frac{CP_n\, e^{t\tau}}{1 - (1 - CP_n)e^{t\tau}}. \tag{3.12}$$

3.4.3 Service Time Distribution

In order to find the distribution of service time at a sensor node (*i.e.*, the time a node spends to transmit a packet without any error), it is required to derive the probability of a successful packet transmission first.

The probability that a packet sent over a one-hop link is successfully received by its destination depends on whether a collision occurs or not as well as on the received SNR.

A packet transmitted by a sensor node will be lost due to collision if at least one of the nodes within the carrier sensing range of the receiver, other than transmitter itself, tries to transmit during the same time slot. We assume that all the nodes are within the carrier sensing range of each other due to the small scale of WBANs and, furthermore, that no node can receive a packet while transmitting. Given the fact that a node transmits with a probability equal to its utilization factor (*i.e.*, if it has a packet for transmission), the collision rate of a packet transmitted by a sensor node $n \in \mathcal{N}$ denoted by χ_n is given by

$$\chi_n = 1 - \prod_{x \in \mathcal{N} \setminus \{n\}} (1 - \rho_x). \tag{3.13}$$

If no collision occurs, the packet error rate for node n denoted by ζ_n is a function of the received SNR from transmitter n and, for the differentially encoded binary phase-shift keying (DBPSK) modulation scheme, is given by

$$\zeta_n = 1 - \left[1 - \frac{1}{2} \exp(-\bar{\gamma}_n^b)\right]^{L_b}. \tag{3.14}$$

$\bar{\gamma}_n^b$ in Eq. (3.14) stands for the average received SNR per bit from n and is given by

$$\bar{\gamma}_n^b = \frac{B\,\bar{\gamma}_n}{R}, \tag{3.15}$$

where $\bar{\gamma}_n$, B, and R are the average received SNR from n, bandwidth in Hertz, and transmission rate in bit per second, respectively.

From Eqs. (3.13) and (3.14), the average probability of successful packet transmission for node n denoted by π_n is therefore given by

$$\pi_n = 1 - [\chi_n + (1 - \chi_n)\zeta_n]\,. \tag{3.16}$$

An automatic-repeat-request mechanism is considered whereby a sensor node keeps retransmitting a packet until the packet is successfully received at the destination. We assume the retransmissions are independent. The service time at a sensor node n is therefore a compound probability distribution in which the compounded distribution is geometric with success probability of π_n and the distribution of transmission time T_n is the compounding distribution [54]. The moment generating function of S_n (probability distribution of service time at node n) is given by

$$\begin{aligned} M_{S_n}(t) &= \sum_{k=1}^{\infty} \pi_n (1-\pi_n)^{k-1} M_{T_n}^k(t) \\ &= \pi_n M_{T_n}(t)\big|_{CP=CP_{\max}} + \\ &\quad \pi_n(1-\pi_n) M_{T_n}^2(t)\big|_{CP=CP_{\max}} + \\ &\quad \frac{\pi_n(1-\pi_n)^2 M_{T_n}^3(t)|_{CP=CP_{\min}}}{1-(1-\pi_n)M_{T_n}(t)|_{CP=CP_{\min}}}. \end{aligned} \tag{3.17}$$

Note that in Eq. (3.17) node n sets its contention probability CP_n to $CP_{\max}$ for the first two transmissions and fixes it to $CP_{\min}$ for the rest of transmission attempts.

Using Eqs. (3.12) and (3.17) and the properties of the moment generating function, the average and variance of the service time at node n are derived respectively as

$$\mathbf{E}[S_n] = M'_{S_n}(t)\big|_{t=0} = \frac{8}{3}\tau\left(\frac{2}{\pi_n} - 3\pi_n + 2\pi_n^2\right), \tag{3.18}$$

and

$$\begin{aligned}\mathbf{V}[S_n] &= M''_{S_n}(t)\big|_{t=0} - \mathbf{E}[S_n]^2 \\ &= \frac{\tau^2}{9}\left(\frac{256}{\pi_n^2} - \frac{48}{\pi_n} + 768 - 1976\pi_n + 528\pi_n^2 + 768\pi_n^3 - 256\pi_n^4\right). \end{aligned} \tag{3.19}$$

3.4.4 End-to-End Delay

Given the moment generating functions of inter-arrival time and service time of packets at a node n, we can approximate the moment generating function of total packet delay experienced at the node n (*i.e.*, queuing delay plus service delay) as [55]

$$M_{\Delta_n}(t) = \frac{(1 - \mathbf{E}[A_n]\mathbf{E}[S_n])\,(t-1)M_{S_n}(t)\,(1 - M_{A_n}(M_{S_n}(t)))}{\mathbf{E}[A_n]\,(1 - M_{S_n}(t))\,(t - M_{A_n}(M_{S_n}(t)))}. \tag{3.20}$$

The average packet delay at node n then is derived from Eq. (3.20) as

$$\mathbf{E}[\Delta_n] = \mathbf{E}[S_n] + \frac{\mathbf{E}[S_n]\mathbf{V}[A_n] + \mathbf{E}[A_n]\mathbf{V}[S_n]}{2\,(1 - \mathbf{E}[S_n]\mathbf{E}[A_n])}. \tag{3.21}$$

The average end-to-end delay experienced by a packet over a K-hop transmission path $l = \langle m_1, \cdots, m_{K+1}\rangle$ is the aggregate of the delays at the nodes en route, and is given as

$$\mathbf{E}[\Delta^l] = \sum_{k=1}^{K} \mathbf{E}[\Delta_{m_k}]. \tag{3.22}$$

3.5 Multi-hop Topology Formation Game

We formulate a multi-hop topology formation game (MTFG) wherein each sensor node seeks to choose a path to the network hub such that it minimizes its own security cost in the presence of wiretapper while meeting its QoS requirements. We model the cost function for a node in terms of the secrecy outage probability of the path it takes to connect to the

hub, and the QoS requirement of a node in terms of the average end-to-end delay of its transmission path to the hub.

The framework of network formation games is used where sensor nodes interact with one other to form a multi-hop topology. We formulate a non-cooperative game in which sensor nodes are selfish in the sense that each node seeks to optimize its own cost function.

The interactions between the sensor nodes will result in a network graph $G(\mathcal{V},\mathcal{E})$. The objective is to find some desired $\mathcal{E}$ among all the possible configurations.

For a sensor node $n \in \mathcal{N}$, the strategy space $\mathcal{S}_n$ is the set of nodes to which it can connect in the uplink. Note that the strategy space of n is disjoint from its set of descendants $\mathcal{D}_n$ in the tree structure, *i.e*, $\mathcal{S}_n = \{i | i \in \mathcal{V} \backslash (\{n\} \cup \mathcal{D}_n)\}\ \forall n \in \mathcal{N}$.

We assume sensor nodes have no incentive to disconnect from the WBAN, *i.e.*, the network topology graph is always connected. In practice, when a sensor node adopts a strategy, it terminates its previous connection in the uplink (if any) and connects to a new node, which uniquely determines its path to the hub.

3.5.1 Formulation of Security Cost and QoS Measure

Assume that, in a network graph G, a sensor node $n \in \mathcal{N}$ chooses to connect to a node s_n from its strategy space in the uplink and, in turn, form a K-hop transmission path $l_n = \langle m_1, \cdots, m_{K+1} \rangle$ to the hub.

We model the security cost function of node n as the SOP of its transmission path to hub, *i.e.*,

$$
\begin{aligned}
c_n(G) &= P_{l_n}^{\text{out}} \\
&= 1 - \prod_{k=1}^{K} \left(1 - P_{\langle m_k, m_{k+1}\rangle}^{\text{out}}\right) \\
&= P_{\langle n,s_n\rangle}^{\text{out}} - \left(P_{\langle n,s_n\rangle}^{\text{out}} - 1\right) \left[1 - \prod_{k=2}^{K} \left(1 - P_{\langle m_k, m_{k+1}\rangle}^{\text{out}}\right)\right] \\
&= P_{\langle n,s_n\rangle}^{\text{out}} - \left(P_{\langle n,s_n\rangle}^{\text{out}} - 1\right) c_{s_n}(G). \qquad (3.23)
\end{aligned}
$$

This cost function reflects the performance of transmission in terms of PHY security.

We also model the QoS measure of node n as the average end-to-end packet delay experienced over its transmission path to the hub, *i.e.*,

$$
\begin{aligned}
q_n(G) &= \mathbf{E}[\Delta^{l_n}] \\
&= \sum_{k=1}^{K} \mathbf{E}[\Delta_{m_k}] \\
&= \mathbf{E}[\Delta_n] + \sum_{k=2}^{K} \mathbf{E}[\Delta_{m_k}] \\
&= \mathbf{E}[\Delta_n] + q_{s_n}(G). \qquad (3.24)
\end{aligned}
$$

Eqs. (3.23) and (3.24) reveal that the cost or QoS measure of a sensor node n depend on the qualities of the first hop in its path to the hub $\langle n,s_n\rangle$ as well as the cost or QoS measure of the immediate node that n chooses to connect to in the uplink, s_n.

For each sensor node n, the average end-to-end packet delay is required to be less than or equal to an upper bound denoted by δ_n. This delay constraint allows the hub or sensor nodes to specify the maximum tolerable end-to-end latency in the WBAN for scheduling uplink/downlink allocation intervals or real-time monitoring requirements. Note also that the delay constraint, in effect, bounds the maximum number of connections that can be accepted by a relaying node. That is because as the number of descendants of a node

increases, the queuing delay at the node rises which, in turn, leads to a higher latency over the entire path. Therefore once the delay over a path reaches the delay constraint, nodes within that path can no longer admit new connections.

3.5.2 MTFG Algorithm

Sensor nodes interact with one other to form a tree topology that governs their multi-hop transmissions. For each sensor node $n \in \mathcal{N}$, a strategy choice $s_n \in \mathcal{S}_n$ leads to a network graph $G_{s_n,\boldsymbol{s}_{-n}}$ given the joint strategy choice of all the other nodes $\boldsymbol{s}_{-n} = \{s_m\}_{m\in\mathcal{N}\setminus\{n\}}$. Given the strategies of all the other nodes, each node seeks to choose a cost minimizer strategy while satisfying its QoS constraint. Such a strategy is known as a best response and is formally defined as follows.

Definition 3.2 (Best Response)**.** A best response for a node $n \in \mathcal{N}$ is a strategy $s_n^* \in \mathcal{S}_n$ such that, $c_n\left(G_{s_n^*,\boldsymbol{s}_{-n}}\right) \leq c_n\left(G_{s_n,\boldsymbol{s}_{-n}}\right)\ \forall s_n \in \mathcal{S}_n$ s.t. $q_n\left(G_{s_n^*,\boldsymbol{s}_{-n}}\right) \leq \delta_n$, given the joint strategy choice of all the other nodes $\boldsymbol{s}_{-n}$. ■

We present a topology formation algorithm based on this concept of the best response. The bootstrapping phase includes network discovery where each sensor node detects its neighboring nodes as potential partners for multi-hop transmission and learns the current state of the WBAN.

Having discovered the network, sensor nodes iteratively and in an arbitrary sequence interact with their neighbors and choose their best responses given their current knowledge of the network topology. This iterative approach among sensor nodes to selecting the best response is guaranteed to converge as proved by the following proposition.

Proposition 3.1 (Algorithm Convergence). *The presented MTFG algorithm is guaranteed to converge to a final topology after a finite number of iterations regardless of the initial network topology and the sequence of best response selections.*

Proof: Let G_t be the resultant topology graph at the end of t iterations. Topology graph evolution from a graph G_t to a graph G_{t+1} entails a best response selection by an arbitrary

sensor node $n \in \mathcal{N}$. This best response choice by n may impact the security cost of three different types of nodes in the network: the cost of n itself does not increase as per the definition of a best response strategy; costs of the descendants of n also do not increase as a reduction in the cost of a node can only lead to decrease in the security costs of its descendants as suggested by Eq. (3.23); finally, costs of the nodes that are not connected to or are parents of n are not affected by a best response choice of node n. Therefore, every move from a graph G_t to a graph G_{t+1} does not lead to any increase in the cost of any node in the network. Based on this fact, and given that the number of tree topologies interconnecting a finite number of nodes is finite, it yields that the algorithm eventually converges after a finite number of iterations. ■

We introduce the following concept of a Nash Topology as an extension of the renowned Nash equilibrium which is appropriate for investigating the stability of the network topology.

Definition 3.3 (Nash Topology)**.** A network topology interconnecting a set of nodes is a Nash topology iff no unilateral deviation in strategy by any single sensor node results in a security cost reduction for that. ■

A direct consequence of Proposition 3.1 is that any topology resulting from the proposed algorithm is a stable Nash topology.

3.5.3 Algorithm Implementation

The proposed MTFG algorithm can be implemented in a distributed fashion which, compared to a centralized implementation, is less complex and more readily scalable in practice.

Each sensor node commences a discovery phase first in order to detect its neighboring nodes for uplink transmission. Well-known discovery techniques [57] can be used in this phase to learn about the presence of neighbors. Here, for each sensor node $n \in \mathcal{N}$ we define the neighbor set $\mathcal{TR}_n$ as the set of nodes that can decode the signal transmitted by n with negligibly small error, *i.e.*, $\mathcal{TR}_n = \{i \in \mathcal{V} | \bar{\gamma}_n^b > 0\,\text{dB}\}$.

Subsequent to discovery phase, sensor nodes play an iterative multi-hop topology formation game in an arbitrary but sequential order. In every iteration each sensor node $n \in \mathcal{N}$ interacts, using pairwise negotiations over a control channel, with its discovered neighbors, acquires the current network topology information as well as the security cost and QoS measure of its prospective next hops, identifies its best response strategy $s_n^* \in \mathcal{S}_n$, and executes it by replacing its current link with the new link s_n^*. The game goes on until convergence to a Nash topology.

As suggested by Eqs. (3.23) and (3.24), each sensor node needs to only assess the security cost and QoS measure of its prospective immediate hops in the uplink to make its best response decision. Note that when a prospective next-hop node is asked to report its QoS measure to its neighbors, it must first update its end-to-end delay, as accepting new descendants increases the queuing time and, in turn, end-to-end delay at the node.

Algorithm 2 summarizes the steps of the MTFG algorithm.

Much of the computational complexity of the algorithm lies in the process of best response selection. In particular, the computational complexity of identifying the best response strategy for each sensor node n has a time complexity of $\mathcal{O}(|\mathcal{TR}_n \backslash \mathcal{D}_n|)$, where $\mathcal{D}_n$ is the set of descendants of node n.

Another source of complexity is the number of algorithm iterations till convergence. While this is upper bounded in theory by the number of spanning trees definable on the set of network graph vertices $\mathcal{V}$, the algorithm converges much faster in a practical implementation as a sensor node does not need to try connecting to every other node in the network before identifying its best response.

Last but not least, the algorithm is adaptable to a dynamically changing WBAN setting as it can be repeated periodically within different time intervals depending on the frequency and magnitude of changes in the network. In this case, the best response interactions between sensor nodes can be piggybacked over regular data transmissions instead of requiring dedicated control channels, which can significantly reduce radio usage in small sensor devices.

INITIALIZATION
forall $n \in \mathcal{N}$ **do**
| $s_n \leftarrow \mathsf{Hub}$; //star network topology
end

NETWORK DISCOVERY
forall $n \in \mathcal{N}$ **do**
| n finds its transmission range set $\mathcal{TR}_n$;
end

DISTRIBUTED MULTI-HOP TOPOLOGY FORMATION
repeat in an arbitrary but sequential order
| **forall** $n \in \mathcal{N}$ **do**
| | **forall** $s_n \in \mathcal{TR}_n$ **do**
| | | n interacts with s_n over a control channel;
| | | n computes its security cost $c_n\left(G_{s_n,\boldsymbol{s}_{-n}}\right)$;
| | **end**
| | n selects it security cost minimizer s_n^*;
| **end**
until *convergence to a stable Nash topology*;

SECURE MULTI-HOP TRANSMISSION
Sensor nodes transmit their packets, where applicable;

Algorithm 2: MTFG algorithm for multi-hop topology formation

3.6 Model Validation

In this section, the proposed MTFG is employed in an IEEE 802.15.6-based ultra wideband (UWB) WBAN to gauge the validity and effectiveness of the proposed framework. To this end, we examine the system performance behaviors for various scenarios. In particular, we consider moving versus stationary WBAN scenarios with respect to the motion of the human body. Also three scenarios are considered with respect to the transmission approach, namely the proposed multi-hop topology formation game (MTFG), two-hop topology extension (2TE) with prearranged relaying nodes as described by IEEE 802.15.6 standard, and single-hop star topology (ST).

3.6.1 Simulation Setup

We consider a WBAN consisting of ten on-body sensor nodes as illustrated in Fig. 3.1. The nodes are placed on the head, left arm, left hand, chest, right arm, right hand, left leg, left foot, right leg, and right foot of the subject. The WBAN has one hub located on the center waist. The network is initially organized according to a star topology.

For the wireless propagation model in a moving WBAN, the results of the measurement campaign conducted in [43] is used, where average path loss and fading statistics are characterized on a per-link basis. The measurements are of a subject walking freely around a room, for an UWB center frequency of 4.2 GHz. The total path loss of the wireless channel is given by

$$PL^{\mathrm{dB}} = \overline{PL}^{\mathrm{dB}} + \mathcal{N}(\mu,\sigma) + \varepsilon, \tag{3.25}$$

where $\overline{PL}$ is the average path loss of the channel, $\mathcal{N}(\mu,\sigma)$ a Gaussian distribution with mean μ and standard deviation σ which models the fading amplitude of the channel in dB, and ϵ represents the correlation effect of the channel with itself and other links which is negligible compared to the other two components. Parameter values of the channel propagation model are provided in [43] for different links in the WBAN.

Also a receiver noise figure of 10 dB and implementation loss of 5 dB are considered as per the optional UWB PHY specifications provided in IEEE 802.15.6.

To validate the model in an stationary scenario, the following path loss model is adopted based on the measurements taken in a hospital room for UWB frequencies of $3.1 - 10.6$ GHz [6]

$$PL(d)^{\mathrm{dB}} = \alpha \log_{10}(d) + \mathcal{N}(\mu,\sigma), \tag{3.26}$$

where d is TX-RX distance in millimeters and parameters α, μ, and σ are chosen to be 19.2, 3.38, and 2.8, respectively.

We assume the wireless links are symmetric and that the transceivers of all the sensor nodes are identical with the same transmission range.

For IEEE 802.15.6 two-hop topology extension scenario, we consider nodes Head, LFoot, and RFoot to relay their communications through relaying nodes Chest, LLeg, and RLeg respectively, while other sensor nodes directly connect to the hub. Note that the three relayed nodes are the farthest from the hub and the relaying nodes are chosen for the best link qualities over the two-hop transmission path.

3.6.2 Parameter Setting

We assume for each sensor node $n \in \mathcal{N}$, data packets collected by the sensor itself arrive to the sensor node according to the Poisson distribution with the expected arrival rate of κ_n packet(s) per second. Although the arrival of medical traffic of the sensor nodes may be periodic or Poisson distributed, we choose the Poisson distributed arrival as we want to obtain conservative performance bounds. Therefore the probability distribution of inter-arrival time of packets generated by node n is exponentially distributed with mean κ^{-1} and with the moment generating function

$$M^n_{A_n}(t) = \frac{\kappa}{\kappa - t}. \tag{3.27}$$

As the number of descendants of a sensor node increases, both the expected value and variance of inter-arrival time of traffic at the node rise as suggested by Eq. (3.7).

We consider $\kappa_n = 1 \ \forall n \in \mathcal{N}$, *i.e.*, each sensor node generates 1 packet per second at its application layer which is typical for health monitoring devices sending patient physiological information. Note that even though continuous patient monitoring devices may collect medical readings several times per second, these readings are usually aggregated in the node and then transmitted to the hub, thereby reducing the radio usage.

Each transceiver transmits with a power of 85 μW and 18 μW for moving and stationary WBAN scenarios, respectively. These are the transmission powers for which the outage probability for a target packet error rate of 10^{-3} stays less than or equal to 10^{-4} (*i.e.*, $\Pr\{\zeta > 10^{-3}\} < 10^{-4}$) over the reference Chest-Hub link for both scenarios.

The target secrecy rate $\underline{R}$, inverse of the average received SNR at the best wiretapper $\lambda_{\bar{w}}$, and packet length L are set to 0.5 bit/s/Hz, 0.2, and 100 octets (800 bits), respectively.

Other required parameters of the physical layer include working frequency, modulation scheme, channel bandwidth, and coded data bit rate which are chosen to be 4492.8 MHz, differentially encoded binary phase-shift keying (DBPSK), 499.2 MHz, and 0.243 Mbps, respectively as specified for the IEEE 802.15.6 impulse radio UWB (IR-UWB) PHY.

Lastly, the ambient air temperature is assumed to be 21 in computing the thermal noise spectral density.

3.6.3 Numerical Results and Analysis

Starting with the star topology, the MTFG algorithm in all cases converged after no more than three iterations. In the following, the obtained results are presented to investigate how the performance behaviors differ for MTFG compared to 2TE and ST in moving and stationary WBAN scenarios. In particular, we examine Nash topology of the network, SOP performance, end-to-end latency, and the effects of delay constraint on the equilibrium.

3.6.3.1 Nash Topology

Fig. 3.2 illustrates the Nash topology at the equilibrium for moving and stationary WBANs. Sensor nodes with poor direct link quality to the hub exploit spatial diversity by adopting two- or three-hop transmission strategies in order to enhance the PHY secrecy of their communications. Note that the number of transmission hops in the moving scenario is higher than that for the stationary case. In particular, the optimal strategy for node LHand in the

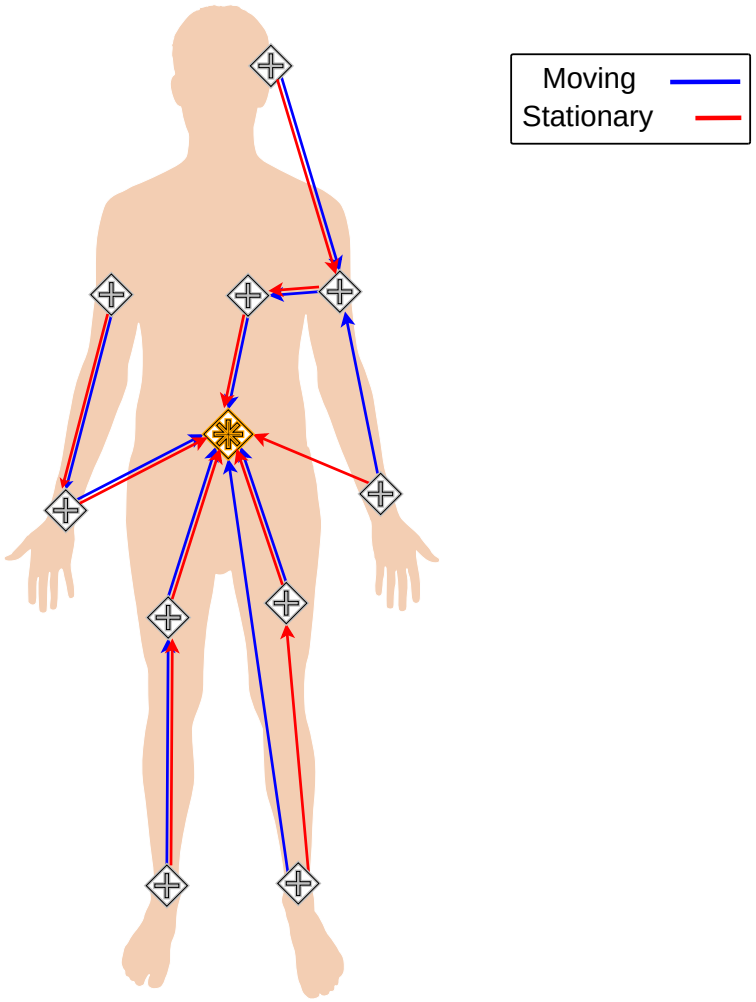

FIGURE 3.2: Nash topology formed by the proposed MTFG for moving and stationary WBAN scenarios ($P_{\mathrm{t}} = 85\,\mu$W for moving WBAN and $P_{\mathrm{t}} = 18\,\mu$W for stationary WBAN, $\lambda_{\bar{w}} = 0.2$, $\underline{R} = 0.5\,$bit/s/Hz, $L = 800\,$bits, $\kappa = 1\,$pkt/s, $\delta \geq 70\,$ms for moving WBAN and $\delta \geq 59.5\,$ms for stationary WBAN)

moving WBAN is to connect to the hub via a three-hop link, while it chooses to directly communicates with the hub in the stationary WBAN. This is an expected result, as the body movement is likely to degrade the channel quality, especially between nearby nodes. Somewhat interestingly, node LFoot chooses two-hop transmission in the stationary WBAN, despite its direct transmission strategy in the moving scenario, as the body movement actually ameliorates the quality of direct link in this case.

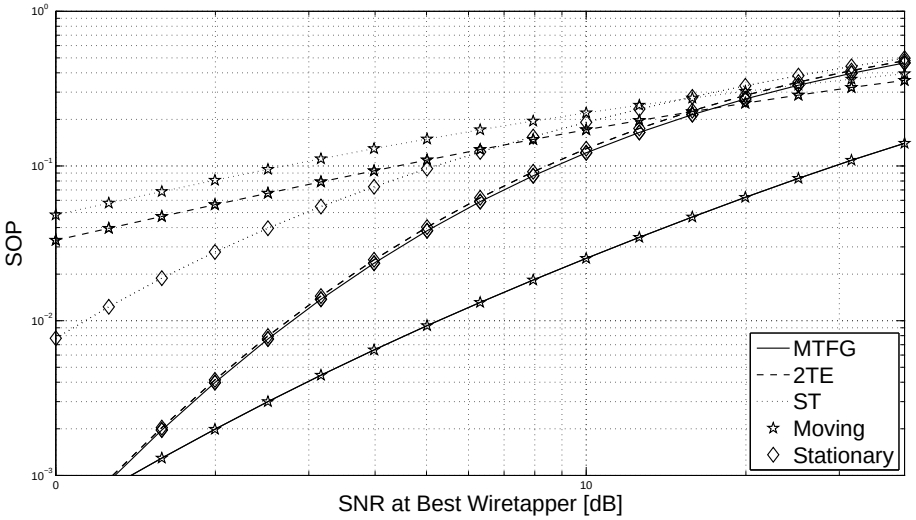

FIGURE 3.3: Average secrecy outage probability per node as expected received SNR at best wiretapper $\frac{1}{\lambda_{\bar{w}}}$ increases for moving and stationary WBAN scenarios ($P_{\mathrm{t}} = 85\,\mu\mathrm{W}$ for moving WBAN and $P_{\mathrm{t}} = 18\,\mu\mathrm{W}$ for stationary WBAN, $\underline{R} = 0.5\,\mathrm{bit/s/Hz}$)

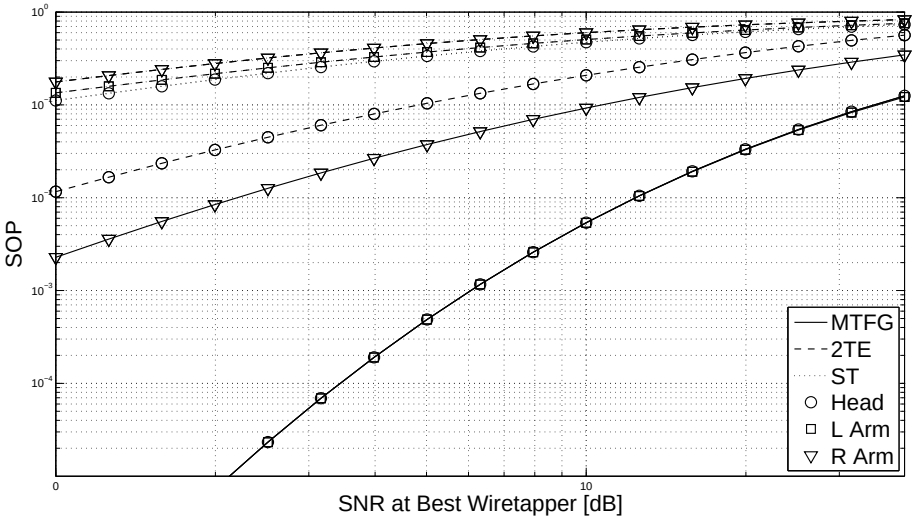

FIGURE 3.4: Secrecy outage probability of nodes Head, LArm, and RArm as expected received SNR at best wiretapper $\frac{1}{\lambda_{\bar{w}}}$ increases for moving WBAN scenario ($P_{\mathrm{t}} = 85\,\mu\mathrm{W}$, $\underline{R} = 0.5\,\mathrm{bit/s/Hz}$)

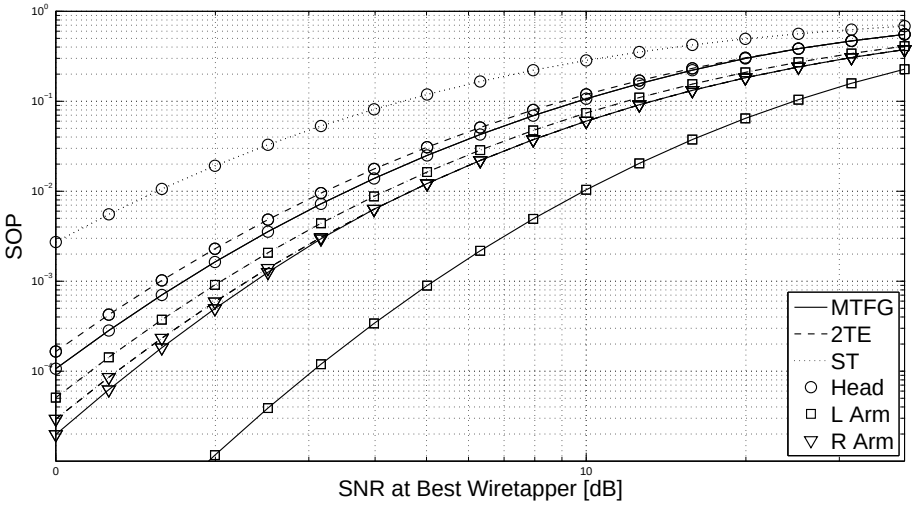

FIGURE 3.5: Secrecy outage probability of nodes Head, LArm, and RArm as expected received SNR at best wiretapper $\frac{1}{\lambda_{\tilde{w}}}$ increases for stationary WBAN scenario ($P_{\mathrm{t}} = 18\,\mu\mathrm{W}$, $\underline{R} = 0.5\,\mathrm{bit/s/Hz}$)

3.6.3.2 SOP Performance

Fig. 3.3 depicts the average SOP performance per node of MTFG compared to 2TE and ST as the quality of the best wiretap channel improves in moving and stationary WBAN scenarios. Physical secrecy gradually declines as the expected received SNR at the wiretapper increases for all cases. It is observed that MTFG surpasses the other two approaches in terms of SOP performance in the moving WBAN, while it performs slightly better than 2TE in the stationary scenario. The SOP resulting from ST remains higher than for the others. Note that as the wiretap channel improves, the SOP performance difference between MTFG, 2TE, and ST decreases in both moving and stationary WBANs, *i.e.*, the sensor nodes are likely to decrease their number of transmission hops in order to guarantee their lowest achievable SOP in the presence of better wiretappers.

Figs. 3.4 and 3.5 illustrate the SOP performance versus expected received SNR at the best wiretapper for nodes Head, LArm, and RArm in moving and stationary WBANs, respectively. The SOP of all the tree nodes resulting from MTFG is lower than for the other transmission approaches in both moving and stationary scenarios. However, the performance gain resulting from the MTFG in the moving WBAN is well above that for the stationary

scenario. This is as expected, since in the moving WBAN with higher channel fluctuations, the capacity of legitimate and wiretap channels are likely to differ more significantly, thus in turn leading to a better PHY security performance.

Again the SOP performance of MTFG approaches those of 2TE and ST for better wiretap channels. In Fig. 3.5 for instance as the expected received SNR at the wiretapper increases, it is optimal for nodes Head and RArm to change their next-hop strategies to Chest (two-hop TX) and hub (direct TX), respectively. Also note that in Fig. 3.4 node Head exhibits roughly the same SOP performance as node LArm does, *i.e.*, the link Head-LArm does not essentially deteriorate the SOP of the whole path to the hub.

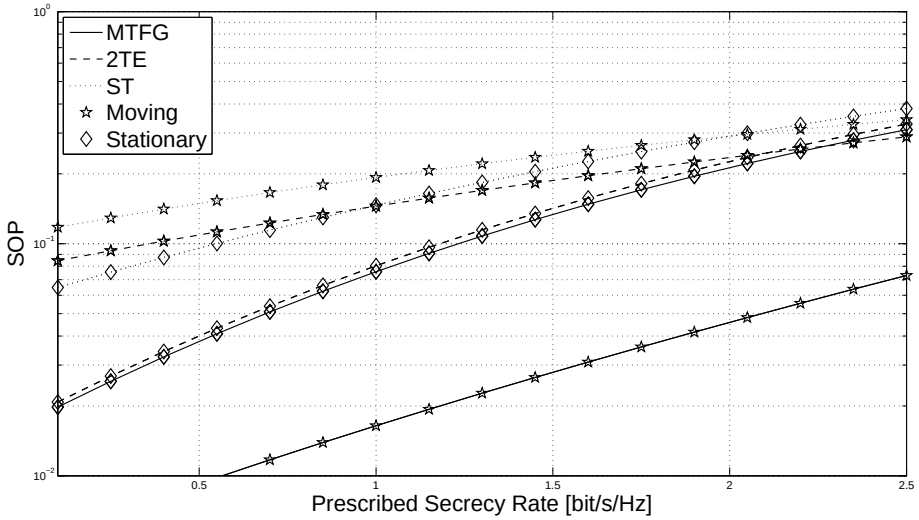

FIGURE 3.6: Average secrecy outage probability per node as prescribed secrecy rate $\underline{R}$ increases for moving and stationary WBAN scenarios ($P_{\mathrm{t}} = 85\,\mu$W for moving WBAN and $P_{\mathrm{t}} = 18\,\mu$W for stationary WBAN, $\lambda_{\bar{w}} = 0.2$)

Fig. 3.6 depicts the average SOP performance per node of MTFG compared to the other two transmission approaches as the prescribed secrecy rate increases in moving and stationary WBAN scenarios. Raising the target secrecy rate accordingly increases the SOP. Note that MTFG again outperforms the other two transmission approaches especially in the moving WBAN. The same trends can be observed here as were noted in Fig. 3.3, *e.g.*, an increase in the prescribed secrecy rate results in a decline in the performance difference between MTFG, 2TE, and ST in both moving and stationary scenarios.

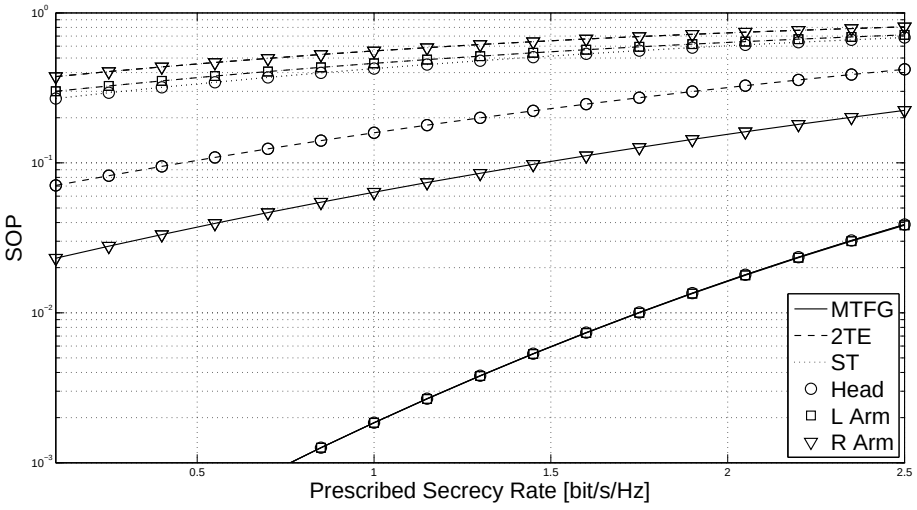

FIGURE 3.7: Secrecy outage probability of nodes Head, LArm, and RArm as prescribed secrecy rate $\underline{R}$ increases for moving WBAN scenario ($P_{\mathrm{t}} = 85\,\mu\mathrm{W}$, $\lambda_{\bar{w}} = 0.2$)

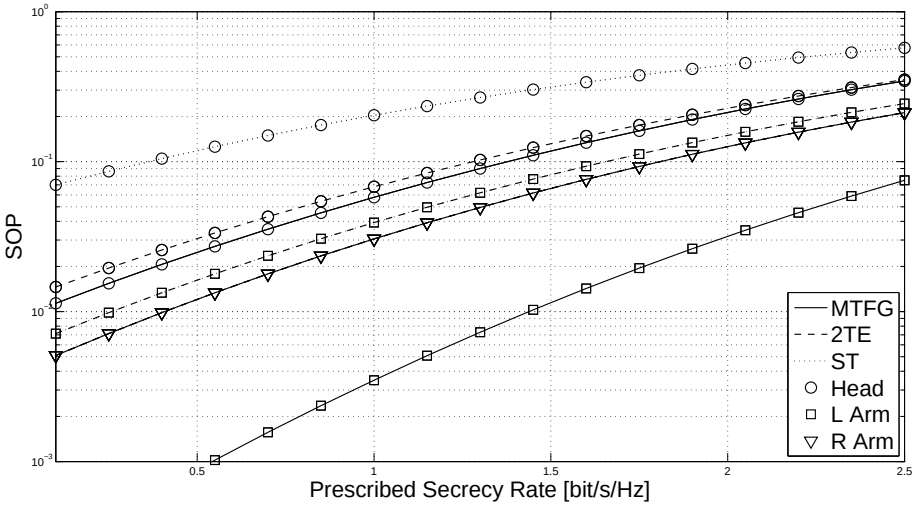

FIGURE 3.8: Secrecy outage probability of nodes Head, LArm, and RArm as prescribed secrecy rate $\underline{R}$ increases for stationary WBAN scenario ($P_{\mathrm{t}} = 18\,\mu\mathrm{W}$, $\lambda_{\bar{w}} = 0.2$)

The SOP performance versus prescribed secrecy rate for nodes Head, LArm, and RArm is illustrated in Figs. 3.7 and 3.8 in moving and stationary WBANs, respectively. Again MTFG yields a higher SOP performance gain in the moving WBAN compared to the stationary scenario. In Fig. 3.8, note that the SOP performance of the node RArm for different transmission approaches is roughly the same in the stationary scenario.

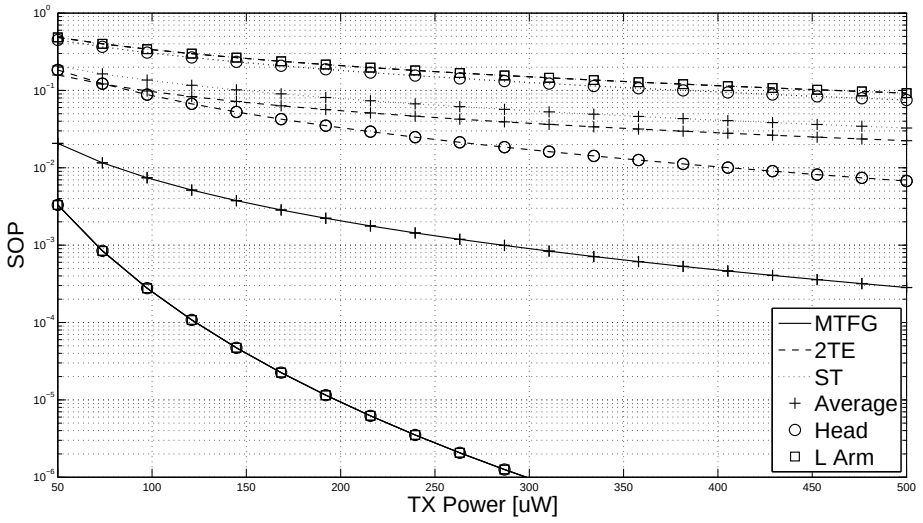

FIGURE 3.9: Secrecy outage probability of average per node, node Head, and node LArm as transmission power P_{t} increases for moving WBAN scenario ($\lambda_{\bar{w}} = 0.2$, $\underline{R} = 0.5\,\mathrm{bit/s/Hz}$)

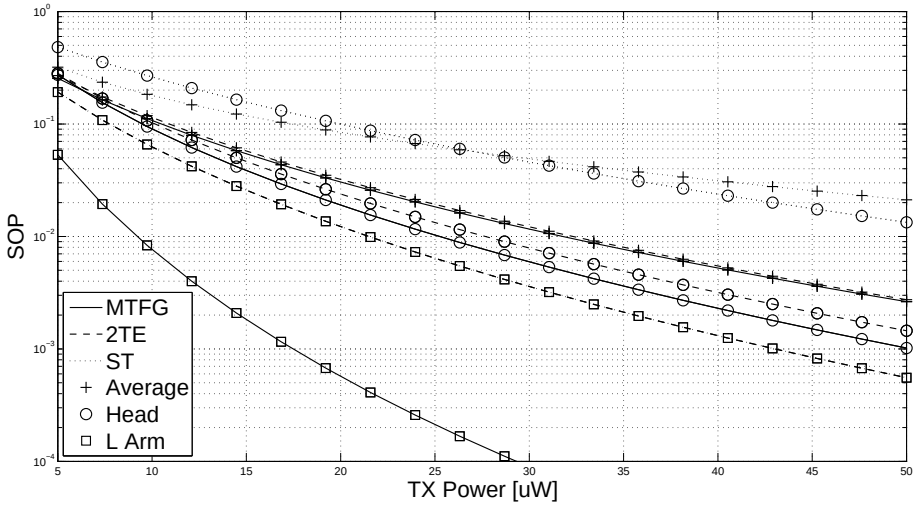

FIGURE 3.10: Secrecy outage probability of average per node, node Head, and node LArm as transmission power P_{t} increases for stationary WBAN scenario ($\lambda_{\bar{w}} = 0.2$, $\underline{R} = 0.5\,\mathrm{bit/s/Hz}$)

Figs. 3.9 and 3.10 depict the SOP performance of MTFG compared to 2TE and ST approaches as the transmission power increases in moving and stationary WBAN scenarios, respectively. The SOP performance improves steadily as the transmission power rises, and MTFG exhibits a better performance behavior compared to the other two approaches. Note that the SOP performance enhancement resulting from the MTFG is again greater in the moving WBAN compared to the stationary scenario. Once the transmission power reaches a threshold, the SOP is saturated as higher transmission powers results in higher SNR at both legitimate receiver and the wiretapper. For lower transmission powers, nodes may consider to change their strategy and adopt a transmission path with lower number of hops in order to minimize their PHY security cost.

3.6.3.3 End-to-End Latency

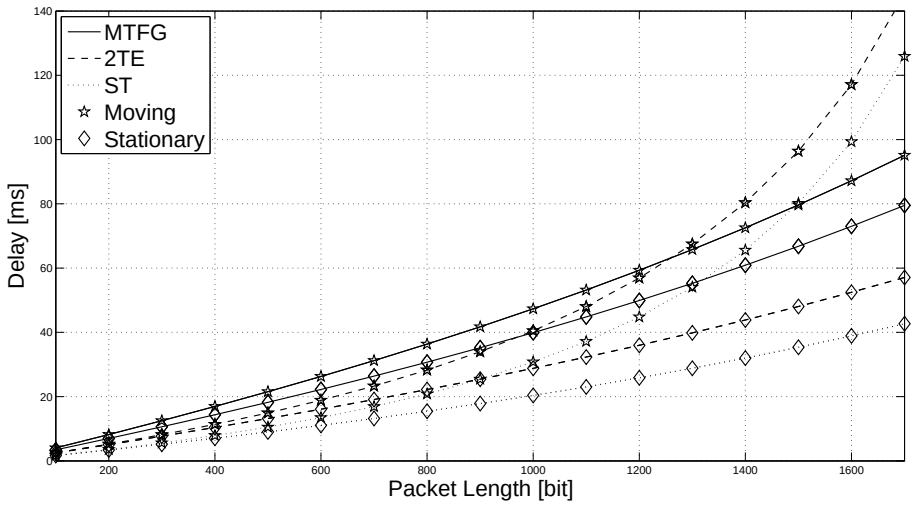

FIGURE 3.11: Average end-to-end delay per node as packet length L increases for moving and stationary WBAN scenarios ($P_\mathrm{t} = 85\,\mu\mathrm{W}$ for moving WBAN and $P_\mathrm{t} = 18\,\mu\mathrm{W}$ for stationary WBAN, $\kappa = 1\,\mathrm{pkt/s}$)

Fig. 3.11 depicts the average end-to-end delay per node resulting from MTFG compared to 2TE and ST as the packet length increases in moving and stationary WBAN scenarios. Larger packet length entails a higher service time as it increases both the transmission time as well as the packet error rate, which in turn result in a higher end-to-end latency. Note that

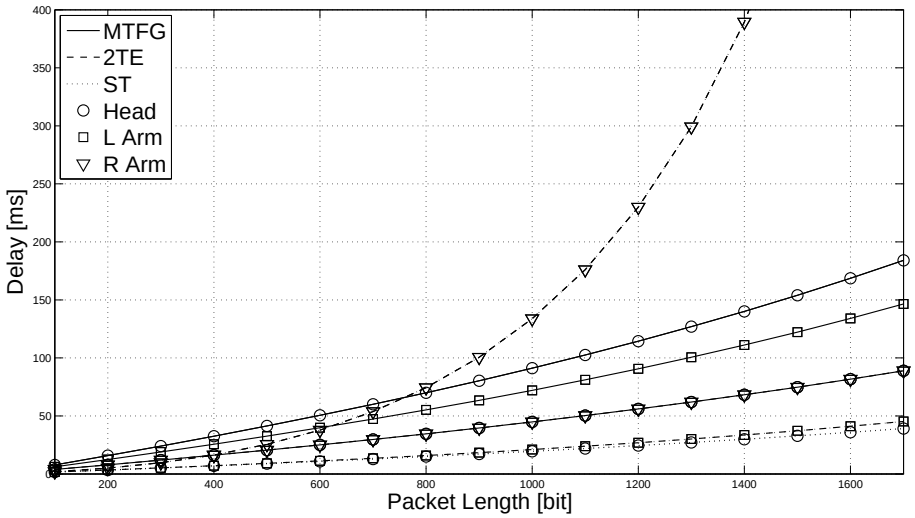

FIGURE 3.12: End-to-end delay of nodes Head, LArm, and RArm as packet length L increases for moving WBAN scenario ($P_\mathrm{t} = 85\,\mu\mathrm{W}$, $\kappa = 1\,\mathrm{pkt/s}$)

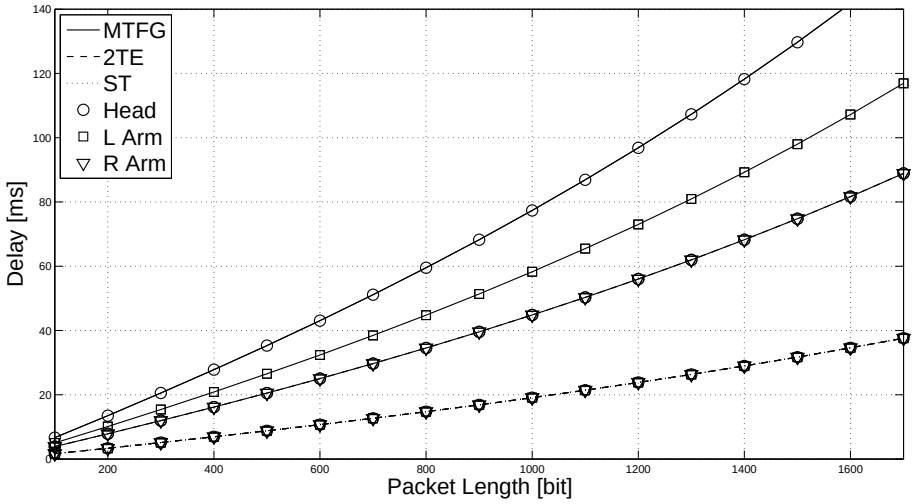

FIGURE 3.13: End-to-end delay of nodes Head, LArm, and RArm as packet length L increases for stationary WBAN scenario ($P_\mathrm{t} = 18\,\mu\mathrm{W}$, $\kappa = 1\,\mathrm{pkt/s}$)

MTFG introduces some extra delay to the system as expected. Yet as the packets get longer, the packet error rates of 2TE and ST rise at a higher pace compared to MTFG which results in considerably higher delays of 2TE and ST for longer packets compared to MTFG. Also the average end-to-end latency in the moving WBAN is higher compared to the stationary WBAN which stems from the higher number of hops in the moving scenario.

The end-to-end delay versus packet length for nodes Head, LArm, and RArm is presented in Figs. 3.12 and 3.13 in moving and stationary WBANs, respectively. In Fig. 3.12, note that for node RArm longer packets are more prone to the transmission error when being directly transmitted to the hub than being relayed by node RHand, which accounts for the noticeably higher delay of 2TE and ST approaches compared to MTFG in larger packet lengths.

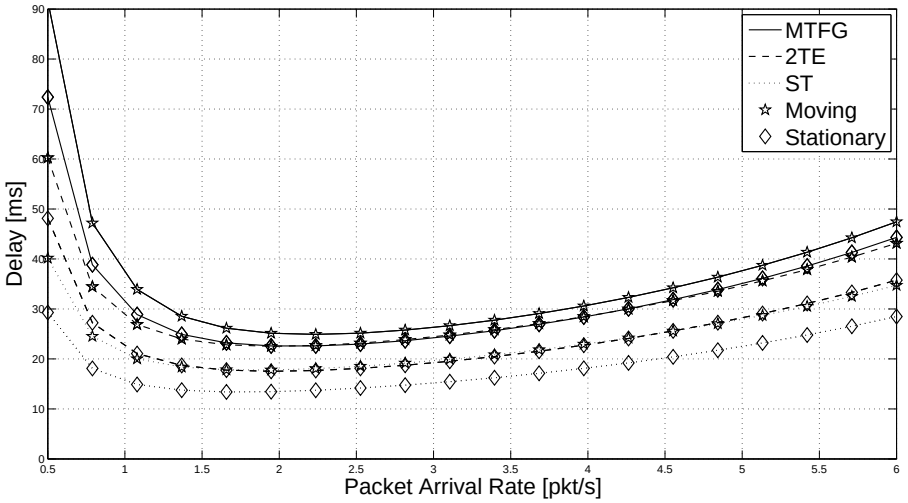

FIGURE 3.14: Average end-to-end delay per node as packet arrival rate κ increases for moving and stationary WBAN scenarios ($P_{\mathrm{t}} = 85\,\mu$W for moving WBAN and $P_{\mathrm{t}} = 18\,\mu$W for stationary WBAN, $L = 800\,$bits)

Fig. 3.14 illustrates the average end-to-end delay per node resulting from MTFG compared to 2TE and ST as the packet arrival rate rises in moving and stationary WBAN scenarios. A higher packet arrival rate on the one hand brings about a lower packet inter-arrival time, but on the other hand increases the service time through heightening the utilization factor of sensor nodes and in turn the probability of collision. Note that the former has a debilitating effect on the delay while the latter amplifies that. For very small packet arrival rates, the packet inter-arrival time has the dominant effect on the delay. Therefore when the

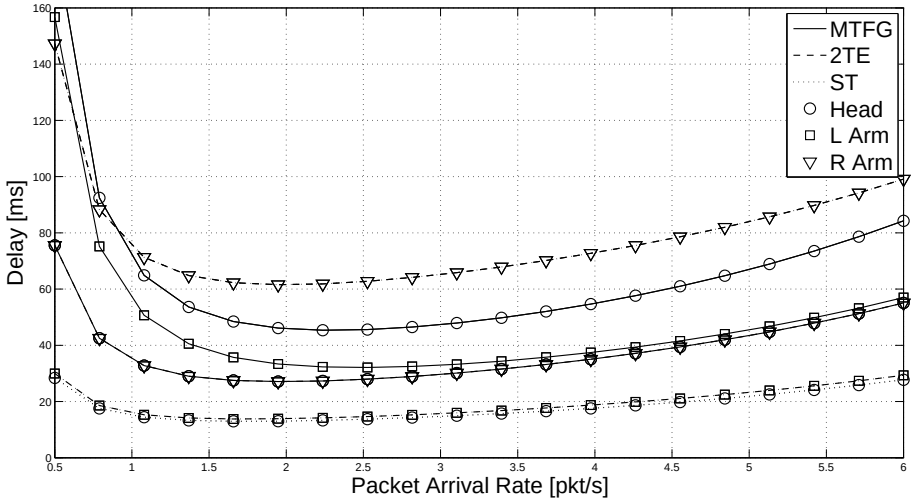

FIGURE 3.15: End-to-end delay of nodes Head, LArm, and RArm as packet arrival rate κ increases for moving WBAN scenario ($P_{\mathrm{t}} = 85\,\mu\mathrm{W}$, and $L = 800\,\mathrm{bits}$)

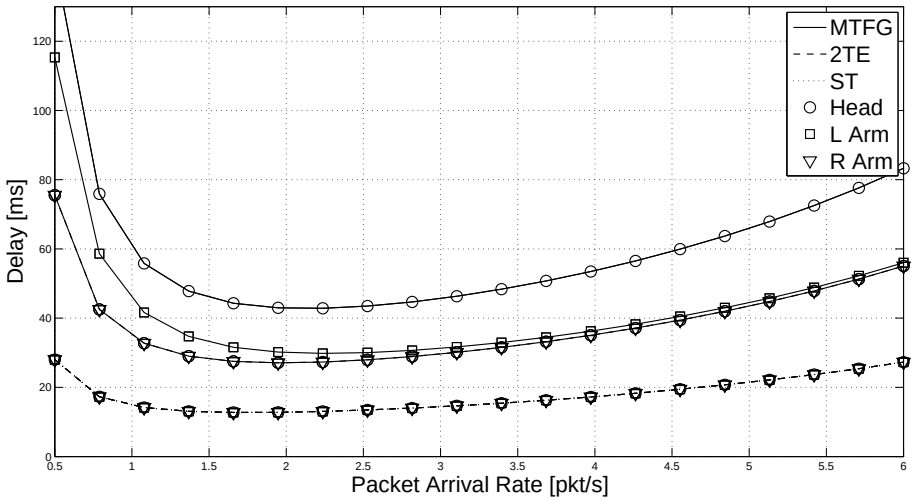

FIGURE 3.16: End-to-end delay of nodes Head, LArm, and RArm as packet arrival rate κ increases for stationary WBAN scenario ($P_{\mathrm{t}} = 18\,\mu\mathrm{W}$, and $L = 800\,\mathrm{bits}$)

packet arrival rate increases, the end-to-end delay declines up to some point after which the delay starts to steadily increase. Again the MTFG exhibits more end-to-end latency than the other two approaches and the average end-to-end delay for the moving WBAN with more number of hops is higher compared to the stationary case.

Figs. 3.15 and 3.16 present the end-to-end delay versus packet arrival rate for nodes Head, LArm, and RArm in moving and stationary WBANs, respectively. In Fig. 3.15, note that the end-to-end delay for node RArm resulting from 2TE and ST approaches stands higher than for MTFG regardless of the packet arrival rate. This is because packets transmitted from RArm experience a higher packet error rate, and in turn a higher end-to-end latency, over a single-hop path compared to a two-hop path to the hub.

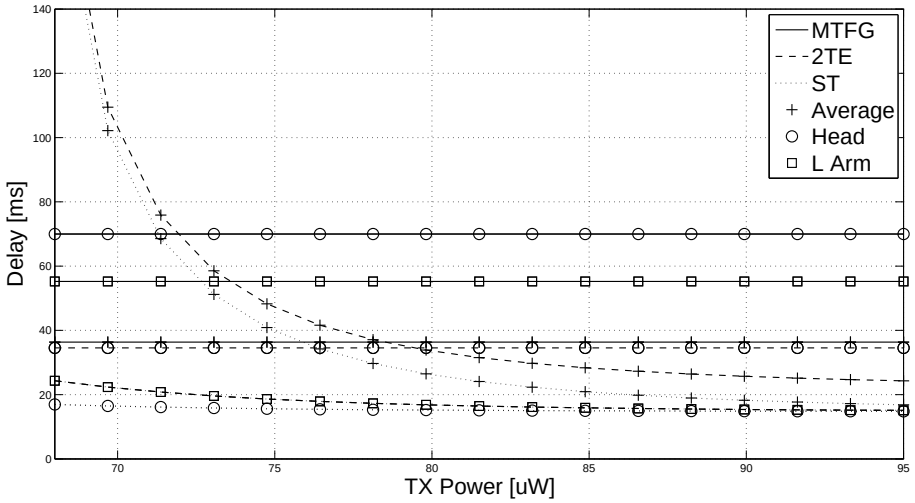

FIGURE 3.17: End-to-end delay of average per node, node Head, and node LArm as transmission power P_t increases for moving WBAN scenario ($L = 800$ bits, $\kappa = 1$ pkt/s)

The end-to-end delay versus transmission power for MTFG, 2TE and ST approaches is illustrated in 3.17 and 3.18 in moving and stationary scenarios, respectively. As the transmission power decreases, the packet error rate for ST and 2TE rises more rapidly compared to MTFG which in turn leads to higher end-to-end delays for ST and 2TE approaches. Note also that once the transmission power exceeds a threshold for which the packet error rate is close to zero, the end-to-end latency is saturated and no longer is affected by increasing the transmission power.

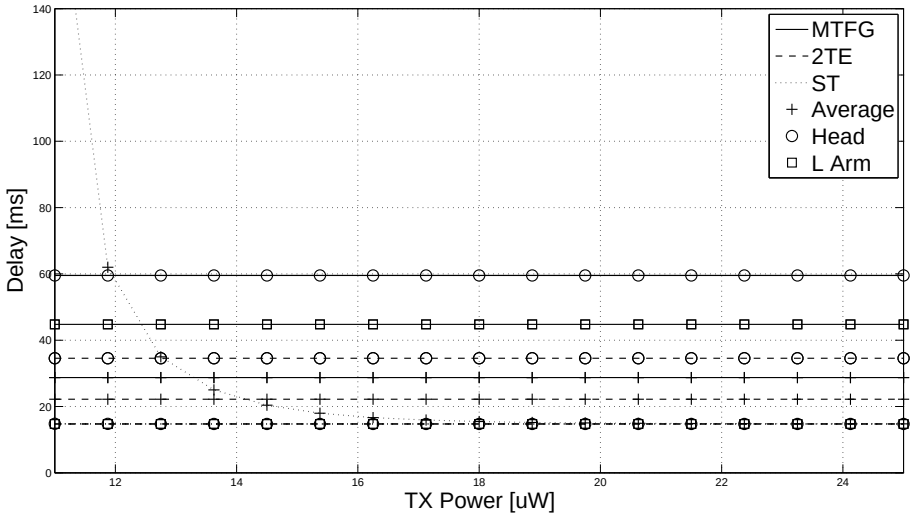

FIGURE 3.18: End-to-end delay of average per node, node Head, and node LArm as transmission power P_{t} increases for stationary WBAN scenario ($L = 800\,\mathrm{bits}$, and $\kappa = 1\,\mathrm{pkt/s}$)

3.6.3.4 Effects of Delay Constraint

Fig. 3.19 illustrates the effects of delay constraint on the Nash topology of the WBAN as well as the number of algorithm iterations till convergence (starting with the star topology).

As the delay constraint increases, more nodes consider multi-hop transmission to enhance their SOP performance. Note that the delay constraint, in effect, bounds the maximum number of connections a node can accept in the uplink. That is because as the number of descendants of a node increases, both the expected value and variance of the packet inter-arrival time for the node rise (see Eq. (3.7)), leading to a higher delay at the node (Eq. (3.21)) and, in turn, over the entire path to the hub.

It also takes more iterations for the algorithm to converge for higher delay constraints. The number of iterations till convergence to a Nash topology differs depending on the sequence of nodes taking action. The maximum number of iterations is therefore considered which remains lower than or equal to 3 in all cases.

Note that the minimum delay constraint for the given parameter values is 14.7 ms which is the end-to-end delay for direct transmission to the hub with zero packet error rate.

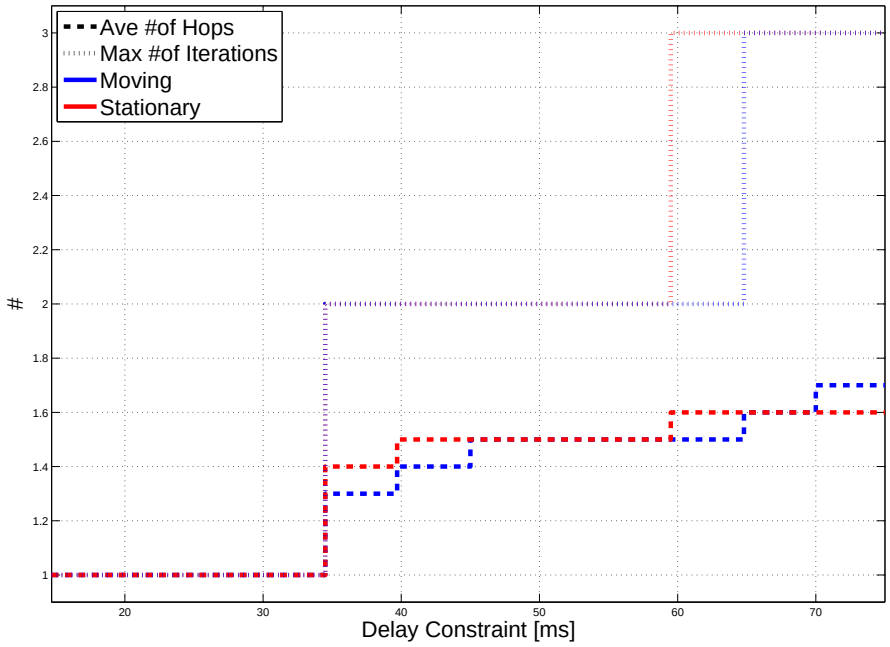

FIGURE 3.19: Average number of hops per node and maximum number of iterations till convergence to Nash topology resulting from multi-hop topology formation game as delay constraint δ increases for moving and stationary WBAN scenarios ($L = 800$ bits, $\kappa = 1$ pkt/s)

3.7 Conclusion and Future Work

A multi-hop topology formation game (MTFG) is proposed that formally formulates the problem of optimizing multi-hop transmission in the uplink of a WBAN in terms of PHY security and with end-to-end delay provisioning. In this game, the body-worn sensor nodes interact in the presence of wiretappers and under fading channel conditions to choose the best path to the hub that guarantees the minimum secrecy outage probability achievable while maintaining the end-to-end delay required by the constraints. We provide a distributed algorithm to search for a Nash network topology where no sensor node has an incentive to unilaterally deviate from its strategy, and prove it converges to a stable Nash solution. The validity and effectiveness of the proposed framework is gauged by numerical simulations in realistic WBAN conditions. To this end, the performance behaviors of the system are examined for various scenarios with respect to connection type (*i.e.*, direct versus two-hop

versus multi-hop transmission) and the motion of the human body (*i.e.*, stationary versus moving WBAN). Results demonstrate the merits of the proposed framework compared to star topology and IEEE 802.15.6 two-hop topology extension schemes. In particular, MTFG outperforms the other two approaches in terms of SOP performance at the cost of an admissible increase in the end-to-end delay, with better performance gains in the moving WBAN compared to the stationary scenario. The performance of the framework can be adjusted to balance the conflicting requirements of security and latency for different application scenarios.

A natural extension of this work is to incorporate wholly on-body wireless communications among body-worn sensors, medical implant devices, and portable hubs, into the framework. Another future direction is to investigate the exploitation of the multi-hop transmission delay to obfuscate the communications for temporal privacy.

Chapter 4

Conclusion

In this final chapter, the major contributions of the thesis are summarised first. Then, the possible future extensions to this thesis and areas of future developments in WBAN technologies are briefly discussed.

4.1 Summary of Contributions

The contributions of the two papers forming the body of this thesis are provided in Secs. 2.1.1 and 3.1.2, respectively. We briefly review the main highlights here once again for the sake of completeness:

- Appropriate energy-efficiency and PHY security performance measures are developed for intra-WBAN communication under realistic channel fading conditions.
- Analytical expressions for the average end-to-end delay and jitter incurred by multi-hop transmission in a slotted Aloha medium access WBAN are derived.
- Two game-theoretic frameworks are proposed to model and analyze the strategic interactions among sensor nodes in a WBAN when seeking to optimize their transmissions in the uplink and at the same time adhere to the QoS requirements in terms of upper

bounds on the end-to-end delay and jitter. The proposed games are proved to admit Nash equilibria and distributed algorithms are provided that converge to stable Nash solutions.

- The game frameworks are evaluated using numerical simulations in conditions approximating actual deployment of WBANs for various scenarios. Performance behavior trade-offs are analyzed and impacts of system parameters on the equilibrium results are examined. The frameworks show remarkable promise in improving the throughput of intra-WBAN communications.

4.2 Future Works

Throughout this thesis two different frameworks have been proposed, respectively in Chaps. 2 and 3, for latency-aware intra-WBAN communications with energy-efficiecy and PHY security considerations. A natural next extension to the thesis is to combine these two frameworks into a unified WBAN solution, which is the subject of a future work.

One of the crucial challenges in wide deployment of WBAN technologies is interference [3, 69]. Density and topology changes induced by the body movements within a WBAN may result in nodes moving into each other's coverage and cause unexpected interference. Furthermore, with the increasing number of WBAN devices and use of wireless technologies with higher coverage area, the coexistence issues between WBANs, as well as with other wireless networks become more important. In this respect, the problems of inter- and intra-WBAN interference should be given more research attention. In particular, cross-layer power control solutions should be designed that address the interference challenges at physical and MAC layers. Such solutions should be robust enough to support interference-agile scenarios (*e.g.*, multiple WBANs with varying traffic in parallel applications), without compromising QoS requirements. It is also worthwhile to investigate the effectiveness of multi-hop cooperative transmission for intra-WBAN interference mitigation.

Last but not least, it is important that a WBAN can interconnect with other networks, as the collected physiological data, in many WBAN applications, needs to be forwarded to a personal server or an access point for further processing [1, 2]. Therefore, interoperability of WBANs and other wireless technologies is another area of future exploration, for effective integration of WBANs within existing network infrastructure.

Appendix A

Derivation of Eq. (2.11)

$$
\begin{aligned}
\mathbf{V}[A_n] &= \frac{d^2}{dt^2}\mathbb{A}_n(t)\big|_{t=0} - \mathbf{E}[A_n]^2 \\
&= \frac{d^2}{dt^2}\left\{\mathbb{A}_{\langle n,n\rangle}(t)\prod_{c\in\mathcal{C}_n}\left[\rho_{\langle c,n\rangle}\mathbb{S}_{\langle c,n\rangle}(t) + (1-\rho_{\langle c,n\rangle})\mathbb{S}_{\langle c,n\rangle}(t)\mathbb{A}_c(t)\right]\right\}_{t=0} - \\
&\quad \left[\mathbf{E}[A_{\langle n,n\rangle}] + \sum_{c\in\mathcal{C}_n}\mathbf{E}[A_c]\right]^2 \\
&= \frac{d^2}{dt^2}\mathbb{A}_{\langle n,n\rangle}(t)\big|_{t=0} + \sum_{c\in\mathcal{C}_n}\frac{d}{dt}\left[\rho_{\langle c,n\rangle}\mathbb{S}_{\langle c,n\rangle}(t) + (1-\rho_{\langle c,n\rangle})\mathbb{S}_{\langle c,n\rangle}(t)\mathbb{A}_c(t)\right]_{t=0} + \\
&\quad \frac{d}{dt}\mathbb{A}_{\langle n,n\rangle}(t)\big|_{t=0}\sum_{c\in\mathcal{C}_n}\frac{d}{dt}\left[\rho_{\langle c,n\rangle}\mathbb{S}_{\langle c,n\rangle}(t) + (1-\rho_{\langle c,n\rangle})\mathbb{S}_{\langle c,n\rangle}(t)\mathbb{A}_c(t)\right]_{t=0} + \\
&\quad \sum_{c\in\mathcal{C}_n}\frac{d^2}{dt^2}\left[\rho_{\langle c,n\rangle}\mathbb{S}_{\langle c,n\rangle}(t) + (1-\rho_{\langle c,n\rangle})\mathbb{S}_{\langle c,n\rangle}(t)\mathbb{A}_c(t)\right]_{t=0} + \\
&\quad \sum_{c\in\mathcal{C}_n}\sum_{c\prime\in\mathcal{C}_n\setminus\{c\}}\left\{\frac{d}{dt}\left[\rho_{\langle c,n\rangle}\mathbb{S}_{\langle c,n\rangle}(t) + (1-\rho_{\langle c,n\rangle})\mathbb{S}_{\langle c,n\rangle}(t)\mathbb{A}_c(t)\right]_{t=0}\right. \\
&\quad \left.\frac{d}{dt}\left[\rho_{\langle c\prime,n\rangle}\mathbb{S}_{\langle c\prime,n\rangle}(t) + (1-\rho_{\langle c\prime,n\rangle})\mathbb{S}_{\langle c\prime,n\rangle}(t)\mathbb{A}_{c\prime}(t)\right]_{t=0}\right\} - \\
&\quad \left[\mathbf{E}[A_{\langle n,n\rangle}] + \sum_{c\in\mathcal{C}_n}\mathbf{E}[A_c]\right]^2 \\
&= \mathbf{V}[A_{\langle n,n\rangle}] + \mathbf{E}[A_{\langle n,n\rangle}]^2 + (1+\mathbf{E}[A_{\langle n,n\rangle}])\sum_{c\in\mathcal{C}_n}\mathbf{E}[A_c] +
\end{aligned}
$$

$$\sum_{c\in\mathcal{C}_n}[\mathbf{V}[S_{\langle c,n\rangle}]+\mathbf{E}[S_{\langle c,n\rangle}]^2+(1-\rho_{\langle c\prime,n\rangle})(2\mathbf{E}[S_{\langle c,n\rangle}]\mathbf{E}[A_c]+$$

$$\mathbf{V}[A_c]+\mathbf{E}[A_c]^2)]+\sum_{c\in\mathcal{C}_n}\sum_{c\prime\in\mathcal{C}_n\setminus\{c\}}\mathbf{E}[A_c]\mathbf{E}[A_{c\prime}]-\left[\mathbf{E}[A_{\langle n,n\rangle}]+\sum_{c\in\mathcal{C}_n}\mathbf{E}[A_c]\right]^2$$

$$=\mathbf{V}[A_{\langle n,n\rangle}]+(1-\mathbf{E}[A_{\langle n,n\rangle}])\sum_{c\in\mathcal{C}_n}\mathbf{E}[A_c]-\left[\sum_{c\in\mathcal{C}_n}\mathbf{E}[A_c]\right]^2+$$

$$\sum_{c\in\mathcal{C}_n}\sum_{c\prime\in\mathcal{C}_n\setminus\{c\}}\mathbf{E}[A_c]\mathbf{E}[A_{c\prime}]+\sum_{c\in\mathcal{C}_n}\Bigg[\mathbf{V}[S_{\langle c,n\rangle}]-\mathbf{E}[S_{\langle c,n\rangle}]^2+2\mathbf{E}[S_{\langle c,n\rangle}]\mathbf{E}[A_c]+$$

$$(1-\frac{\mathbf{E}[S_{\langle c,n\rangle}]}{\mathbf{E}[A_c]})(\mathbf{V}[A_c]+\mathbf{E}[A_c]^2)\Bigg].$$

Bibliography

[1] Min Chen, Sergio Gonzalez, Athanasios Vasilakos, Huasong Cao, and Victor C Leung. Body area networks: A survey. *Mobile Networks and Applications*, 16(2):171–193, 2011.

[2] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour. Wireless body area networks: A survey. *Communications Surveys Tutorials, IEEE*, 16(3):1658–1686, Third 2014. ISSN 1553-877X. doi: 10.1109/SURV.2013.121313.00064.

[3] R. Cavallari, F. Martelli, R. Rosini, C. Buratti, and R. Verdone. A survey on wireless body area networks: Technologies and design challenges. *Communications Surveys Tutorials, IEEE*, 16(3):1635–1657, Third 2014. ISSN 1553-877X. doi: 10.1109/SURV.2014.012214.00007.

[4] M.S. Mohammadi, E. Dutkiewicz, Qi Zhang, and Xiaojing Huang. Optimal energy efficiency link adaptation in IEEE 802.15.6 IR-UWB body area networks. *Communications Letters, IEEE*, 18(12):2193–2196, Dec 2014. ISSN 1089-7798. doi: 10.1109/LCOMM.2014.2364226.

[5] D.B. Smith, D. Miniutti, T.A. Lamahewa, and L.W. Hanlen. Propagation models for body-area networks: A survey and new outlook. *Antennas and Propagation Magazine, IEEE*, 55(5):97–117, Oct 2013. ISSN 1045-9243. doi: 10.1109/MAP.2013.6735479.

[6] Kamya Yekeh Yazdandoost, Kamran Sayrafian-Pour, et al. Channel model for body area network (BAN). *IEEE P802.15-08-0780-09-0006*, page 25, April 2009.

[7] F. Shams, G. Bacci, and M. Luise. Energy-efficient power control for multiple-relay cooperative networks using Q-learning. *Wireless Communications, IEEE Transactions on*, 14(3):1567–1580, March 2015. ISSN 1536-1276. doi: 10.1109/TWC.2014.2370046.

[8] Bingyi Guo, Quansheng Guan, F.R. Yu, Shengming Jiang, and V.C.M. Leung. Energy-efficient topology control with selective diversity in cooperative wireless ad hoc networks: A game-theoretic approach. *Wireless Communications, IEEE Transactions on*, 13(11): 6484–6495, Nov 2014. ISSN 1536-1276. doi: 10.1109/TWC.2014.2325864.

[9] Wei Zhong, Gang Chen, Shi Jin, and Kai-Kit Wong. Relay selection and discrete power control for cognitive relay networks via potential game. *Signal Processing, IEEE Transactions on*, 62(20):5411–5424, Oct 2014. ISSN 1053-587X. doi: 10.1109/TSP.2014.2347261.

[10] S. Tomasin. Routing over multi-hop fading wiretap networks with secrecy outage probability constraint. *Communications Letters, IEEE*, 18(10):1811–1814, Oct 2014. ISSN 1089-7798. doi: 10.1109/LCOMM.2014.2352298.

[11] Jianhua Mo, Meixia Tao, and Yuan Liu. Relay placement for physical layer security: A secure connection perspective. *Communications Letters, IEEE*, 16(6):878–881, June 2012. ISSN 1089-7798. doi: 10.1109/LCOMM.2012.042312.120582.

[12] Lun Dong, Zhu Han, A.P. Petropulu, and H.V. Poor. Improving wireless physical layer security via cooperating relays. *Signal Processing, IEEE Transactions on*, 58(3):1875–1888, March 2010. ISSN 1053-587X. doi: 10.1109/TSP.2009.2038412.

[13] N. Torabi and V.C.M. Leung. Cross-layer design for prompt and reliable transmissions over body area networks. *Biomedical and Health Informatics, IEEE Journal of*, 18(4): 1303–1316, July 2014. ISSN 2168-2194. doi: 10.1109/JBHI.2013.2283232.

[14] S. Ivanov, D. Botvich, and S. Balasubramaniam. Cooperative wireless sensor environments supporting body area networks. *Consumer Electronics, IEEE Transactions on*, 58(2):284–292, May 2012. ISSN 0098-3063. doi: 10.1109/TCE.2012.6227425.

[15] E. Reusens, W. Joseph, B. Latre, B. Braem, G. Vermeeren, E. Tanghe, L. Martens, I. Moerman, and C. Blondia. Characterization of on-body communication channel and energy efficient topology design for wireless body area networks. *Information Technology in Biomedicine, IEEE Transactions on*, 13(6):933–945, Nov 2009. ISSN 1089-7771. doi: 10.1109/TITB.2009.2033054.

[16] S. Singh, F. Ziliotto, U. Madhow, E. Belding, and M. Rodwell. Blockage and directivity in 60 ghz wireless personal area networks: from cross-layer model to multihop mac design. *Selected Areas in Communications, IEEE Journal on*, 27(8):1400–1413, October 2009. ISSN 0733-8716. doi: 10.1109/JSAC.2009.091010.

[17] Martin J Osborne and Ariel Rubinstein. *A course in game theory*. MIT press, 1994.

[18] D.T. Hoang, X. Lu, D. Niyato, P. Wang, D.I. Kim, and Z. Han. Applications of repeated games in wireless networks: A survey. *Communications Surveys Tutorials, IEEE*, PP (99):1–1, 2015. ISSN 1553-877X. doi: 10.1109/COMST.2015.2445789.

[19] Chungang Yang, Jiandong Li, and A. Anpalagan. Strategic bargaining in wireless networks: basics, opportunities and challenges. *Communications, IET*, 8(18):3435–3450, 2014. ISSN 1751-8628. doi: 10.1049/iet-com.2014.0399.

[20] Mohammad Hossein Manshaei, Quanyan Zhu, Tansu Alpcan, Tamer Bacşar, and Jean-Pierre Hubaux. Game theory meets network security and privacy. *ACM Computing Surveys (CSUR)*, 45(3):25, 2013.

[21] Zhu Han. *Game theory in wireless and communication networks: theory, models, and applications*. Cambridge University Press, 2012.

[22] Luiz A DaSilva, Hanna Bogucka, and Allen B MacKenzie. Game theory in wireless networks. *Communications Magazine, IEEE*, 49(8):110–111, 2011.

[23] Dimitris E Charilas and Athanasios D Panagopoulos. A survey on game theory applications in wireless networks. *Computer Networks*, 54(18):3421–3430, 2010.

[24] Peters Steven W, Panah Ali Y, Truong Kien T, et al. Relay architectures for 3gpp lte-advanced. *EURASIP Journal on Wireless Communications and Networking*, 2009, 2009.

[25] Hyunkee Min, Woohyun Seo, Jemin Lee, Sungsoo Park, and Daesik Hong. Reliability improvement using receive mode selection in the device-to-device uplink period underlaying cellular networks. *Wireless Communications, IEEE Transactions on*, 10(2): 413–418, 2011.

[26] Chia-Hao Yu, Klaus Doppler, Cassio B Ribeiro, and Olav Tirkkonen. Resource sharing optimization for device-to-device communication underlaying cellular networks. *Wireless Communications, IEEE Transactions on*, 10(8):2752–2763, 2011.

[27] Arunabha Ghosh, Jun Zhang, Jeffrey G Andrews, and Rias Muhamed. *Fundamentals of LTE*. Pearson Education, 2010.

[28] Jeffrey G Andrews, Arunabha Ghosh, and Rias Muhamed. Fundamentals of wimax, 2007.

[29] N. Michelusi and M. Zorzi. Optimal adaptive random multiaccess in energy harvesting wireless sensor networks. *Communications, IEEE Transactions on*, 63(4):1355–1372, April 2015. ISSN 0090-6778. doi: 10.1109/TCOMM.2015.2402662.

[30] Yuanye Ma, He Chen, Zihuai Lin, Yonghui Li, and B. Vucetic. Distributed and optimal resource allocation for power beacon-assisted wireless-powered communications. *Communications, IEEE Transactions on*, 63(10):3569–3583, Oct 2015. ISSN 0090-6778. doi: 10.1109/TCOMM.2015.2468215.

[31] A. Vazintari and P.G. Cottis. Mobility management in energy constrained self-organizing delay tolerant networks: An autonomic scheme based on game theory. *Mobile Computing, IEEE Transactions on*, PP(99):1–1, 2015. ISSN 1536-1233. doi: 10.1109/TMC.2015.2462951.

[32] Lingyang Song, D. Niyato, Zhu Han, and E. Hossain. Game-theoretic resource allocation methods for device-to-device communication. *Wireless Communications, IEEE*, 21(3): 136–144, June 2014. ISSN 1536-1284. doi: 10.1109/MWC.2014.6845058.

[33] Hussein Moosavi and Francis M. Bui. A game-theoretic framework for robust optimal intrusion detection in wireless sensor networks. *Information Forensics and Security, IEEE Transactions on*, 9(9):1367–1379, Sept 2014. ISSN 1556-6013. doi: 10.1109/TIFS.2014.2332816.

[34] Junqi Duan, Deyun Gao, Dong Yang, Chuan Heng Foh, and Hsiao-Hwa Chen. An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for iot applications. *Internet of Things Journal, IEEE*, 1(1):58–69, Feb 2014. ISSN 2327-4662. doi: 10.1109/JIOT.2014.2314132.

[35] A. Mukherjee, S.A.A. Fakoorian, Jing Huang, and A.L. Swindlehurst. Principles of physical layer security in multiuser wireless networks: A survey. *Communications Surveys Tutorials, IEEE*, 16(3):1550–1573, Third 2014. ISSN 1553-877X. doi: 10.1109/SURV.2014.012314.00178.

[36] A. Argyriou, A. Caballero Breva, and M. Aoun. Optimizing data forwarding from body area networks in the presence of body shadowing with dual wireless technology nodes. *Mobile Computing, IEEE Transactions on*, 14(3):632–645, March 2015. ISSN 1536-1233. doi: 10.1109/TMC.2014.2321768.

[37] F. Di Franco, C. Tachtatzis, R.C. Atkinson, I. Tinnirello, and I.A. Glover. Channel estimation and transmit power control in wireless body area networks. *Wireless Sensor Systems, IET*, 5(1):11–19, 2015. ISSN 2043-6386. doi: 10.1049/iet-wss.2013.0070.

[38] A. Maskooki, Cheong Boon Soh, E. Gunawan, and K.S. Low. Adaptive routing for dynamic on-body wireless sensor networks. *Biomedical and Health Informatics, IEEE Journal of*, 19(2):549–558, March 2015. ISSN 2168-2194. doi: 10.1109/JBHI.2014.2313343.

[39] Seungku Kim and Doo-Seop Eom. Link-state-estimation-based transmission power control in wireless body area networks. *Biomedical and Health Informatics, IEEE Journal of*, 18(4):1294–1302, July 2014. ISSN 2168-2194. doi: 10.1109/JBHI.2013.2282864.

[40] E. Ibarra, A. Antonopoulos, E. Kartsakli, J. Rodrigues, and C. Verikoukis. QoS-aware energy management in body sensor nodes powered by human energy harvesting. *Sensors Journal, IEEE*, PP(99):1–1, 2015. ISSN 1530-437X. doi: 10.1109/JSEN.2015.2483064.

[41] S.T. Ali, V. Sivaraman, and D. Ostry. Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices. *Mobile Computing, IEEE Transactions on*, 13(12):2763–2776, Dec 2014. ISSN 1536-1233. doi: 10.1109/TMC.2013.71.

[42] Lu Shi, Jiawei Yuan, Shucheng Yu, and Ming Li. Mask-ban: Movement-aided authenticated secret key extraction utilizing channel characteristics in body area networks. *Internet of Things Journal, IEEE*, 2(1):52–62, Feb 2015. ISSN 2327-4662. doi: 10.1109/JIOT.2015.2391113.

[43] S. Van Roy, F. Quitin, Lingfeng Liu, C. Oestges, F. Horlin, J. Dricot, and P. De Doncker. Dynamic channel modeling for multi-sensor body area networks. *Antennas and Propagation, IEEE Transactions on*, 61(4):2200–2208, April 2013. ISSN 0018-926X. doi: 10.1109/TAP.2012.2231917.

[44] A. Zappone, Zhijiat Chong, E.A. Jorswieck, and S. Buzzi. Energy-aware competitive power control in relay-assisted interference wireless networks. *Wireless Communications, IEEE Transactions on*, 12(4):1860–1871, April 2013. ISSN 1536-1276. doi: 10.1109/TWC.2013.031313.121103.

[45] F. Meshkati, H.V. Poor, S.C. Schwartz, and R.V. Balan. Energy-efficient resource allocation in wireless networks with quality-of-service constraints. *Communications, IEEE Transactions on*, 57(11):3406–3414, Nov 2009. ISSN 0090-6778. doi: 10.1109/TCOMM.2009.11.050638.

[46] H. Khayatian, R. Saadat, and J. Abouei. Coalition-based approaches for joint power control and relay selection in cooperative networks. *Vehicular Technology, IEEE Transactions on*, 62(2):835–842, Feb 2013. ISSN 0018-9545. doi: 10.1109/TVT.2012.2222681.

[47] H. Xiao and S. Ouyang. Power control game in multisource multirelay cooperative communication systems with a quality-of-service constraint. *Intelligent Transportation Systems, IEEE Transactions on*, PP(99):1–10, 2014. ISSN 1524-9050. doi: 10.1109/TITS.2014.2322932.

[48] Hussein Moosavi and Francis M. Bui. Delay-aware optimization of spatial diversity with respect to physical layer security in wireless body area networks. *submitted to IEEE Transactions on Information Forensics and Security*, September 2015.

[49] Yifan Chen, Jianqi Teo, J.C.Y. Lai, E. Gunawan, Kay Soon Low, Cheong Boon Soh, and P.B. Rapajic. Cooperative communications in ultra-wideband wireless body area networks: Channel modeling and system diversity analysis. *Selected Areas in Communications, IEEE Journal on*, 27(1):5–16, January 2009. ISSN 0733-8716. doi: 10.1109/JSAC.2009.090102.

[50] IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks. *IEEE Std 802.15.6-2012*, pages 1–271, Feb 2012. doi: 10.1109/IEEESTD.2012.6161600.

[51] John Proakis and Masoud Salehi. *Digital Communications*. McGraw-Hill, 5th edition, November 2007. ISBN 978-0072957167.

[52] Donald Gross. *Fundamentals of queueing theory*. John Wiley & Sons, 2008.

[53] Tadeusz Czachórski and Ferhan Pekergin. Diffusion approximation as a modelling tool. In Demetres D. Kouvatsos, editor, *Network Performance Engineering*, volume 5233 of *Lecture Notes in Computer Science*, pages 447–476. Springer Berlin Heidelberg, 2011. ISBN 978-3-642-02741-3. doi: 10.1007/978-3-642-02742-0_20. URL http://dx.doi.org/10.1007/978-3-642-02742-0_20.

[54] Charalambos A. Charalambides. *Compound and Mixture Distributions*, pages 281–342. John Wiley & Sons, Inc., 2005. ISBN 9780471733188. doi: 10.1002/0471733180.ch7. URL http://dx.doi.org/10.1002/0471733180.ch7.

[55] M. Baz, P.D. Mitchell, and D.A.J. Pearce. Analysis of queuing delay and medium access distribution over wireless multihop pans. *Vehicular Technology, IEEE Transactions on*, 64(7):2972–2990, July 2015. ISSN 0018-9545. doi: 10.1109/TVT.2014.2354475.

[56] D. Goodman and N. Mandayam. Power control for wireless data. *Personal Communications, IEEE*, 7(2):48–54, Apr 2000. ISSN 1070-9916. doi: 10.1109/98.839331.

[57] S. Vasudevan, M. Adler, D. Goeckel, and D. Towsley. Efficient algorithms for neighbor discovery in wireless networks. *Networking, IEEE/ACM Transactions on*, 21(1):69–83, Feb 2013. ISSN 1063-6692. doi: 10.1109/TNET.2012.2189892.

[58] A.D. Wyner. The wire-tap channel. *Bell System Technical Journal, The*, 54(8):1355–1387, Oct 1975. ISSN 0005-8580. doi: 10.1002/j.1538-7305.1975.tb02040.x.

[59] A. Khisti and Gregory W. Wornell. Secure transmission with multiple antennas I: The MISOME wiretap channel. *Information Theory, IEEE Transactions on*, 56(7):3088–3104, July 2010. ISSN 0018-9448. doi: 10.1109/TIT.2010.2048445.

[60] F. Oggier and B. Hassibi. The secrecy capacity of the MIMO wiretap channel. *Information Theory, IEEE Transactions on*, 57(8):4961–4972, Aug 2011. ISSN 0018-9448. doi: 10.1109/TIT.2011.2158487.

[61] Hussein Moosavi and Francis M. Bui. Optimal relay selection and power control with quality-of-service provisioning in wireless body area networks. *submitted to IEEE Transactions on Wireless Communications*, October 2015.

[62] A. Michalopoulou, A.A. Alexandridis, K. Peppas, T. Zervos, F. Lazarakis, K. Dangakis, and D.I. Kaklamani. Statistical analysis for on-body spatial diversity communications at 2.45 GHz. *Antennas and Propagation, IEEE Transactions on*, 60(8):4014–4019, Aug 2012. ISSN 0018-926X. doi: 10.1109/TAP.2012.2201073.

[63] D.B. Smith and D. Miniutti. Cooperative selection combining in body area networks: Switching rates in gamma fading. *Wireless Communications Letters, IEEE*, 1(4):284–287, August 2012. ISSN 2162-2337. doi: 10.1109/WCL.2012.041612.120047.

[64] Jinbei Zhang, Luoyi Fu, and Xinbing Wang. Asymptotic analysis on secrecy capacity in large-scale wireless networks. *Networking, IEEE/ACM Transactions on*, 22(1):66–79, Feb 2014. ISSN 1063-6692. doi: 10.1109/TNET.2013.2244230.

[65] W. Saad, Xiangyun Zhou, B. Maham, T. Basar, and H.V. Poor. Tree formation with physical layer security considerations in wireless multi-hop networks. *Wireless Communications, IEEE Transactions on*, 11(11):3980–3991, November 2012. ISSN 1536-1276. doi: 10.1109/TWC.2012.091812.111923.

[66] O.O. Koyluoglu, C.E. Koksal, and H.E. Gamal. On secrecy capacity scaling in wireless networks. *Information Theory, IEEE Transactions on*, 58(5):3000–3015, May 2012. ISSN 0018-9448. doi: 10.1109/TIT.2012.2184692.

[67] William C Jakes and Donald C Cox. *Microwave mobile communications*. Wiley-IEEE Press, 1994.

[68] Demetres D Kouvatsos. *Network Performance Engineering: A Handbook on Convergent Multi-service Networks and Next Generation Internet*, volume 5233. Springer Science & Business Media, 2011.

[69] A. Boulis, D. Smith, D. Miniutti, L. Libman, and Y. Tselishchev. Challenges in body area networks for healthcare: the mac. *Communications Magazine, IEEE*, 50(5):100–106, May 2012. ISSN 0163-6804. doi: 10.1109/MCOM.2012.6194389.