Delay-Aware Optimization of Physical Layer Security in Multi-Hop Wireless Body Area Networks

Hussein Moosavi*, *Student Member, IEEE*, and Francis Minhthang Bui, *Member, IEEE*

***Abstract*—Joint optimization of the physical layer security with end-to-end delay management is studied in the uniquely constrained context of wireless body area networks. A game-theoretic framework is proposed wherein body-worn sensor 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 requirements 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 its transmissions, and provide a distributed algorithm guaranteed to converge to a Pareto-dominant Nash solution. The framework is evaluated through 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 with a best-channel algorithm, at the expense of an admissible increase in the end-to-end delay.**

***Index Terms*—Wireless body area network (WBAN), physical layer security, fading, spatial diversity, multi-hop relaying, delay, game theory.**

I. Introduction

Wireless body area networks (WBANs) are at the forefront of emerging technologies towards personalized mobile healthcare. 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 for the communication links in a WBAN to be secure and reliable. This is because a WBAN in these applications typically needs to handle medical data with stringent confidentiality and liability requirements. That said, enabling secure transmissions among such body-worn wireless devices is a significant challenge, given the operating conditions and constraints in WBANs. In particular, 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.

Secure communications are conventionally realized through cryptographic techniques at the upper layers of the wireless network protocol stack, which rely on the computational difficulty of certain mathematical tasks. However, the overhead associated with complex encryption algorithms makes 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 [1]. 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 [2] 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 those 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 [3], [4]. 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 evaluate the secrecy performance of transmissions using the secrecy outage probability (SOP), 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 the effective received signal-to-noise ratio (SNR). Multi-hop relaying is a potential strategy to cope with this 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 [5]–[8]. In this respect, PHY secrecy of cooperative relay communications has been extensively studied in general wireless settings [9]–[14]. Furthermore, recent works have shown the potential of multi-hop relaying to enhance the PHY security in wireless

 This work was supported in part by funding from the Natural Sciences and Engineering Research Council of Canada (NSERC). The authors are with the Department of Electrical and Computer Engineering, University of Saskatchewan, SK, S7N 5A9, Canada (e-mail: hussein.moosavi@usask.ca; francis.bui@usask.ca).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2016.2566446, IEEE Transactions on Information Forensics and Security

sensor networks and, more particularly, in WBANs [15], [16]. 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.

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. First, 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 to the ergodic secrecy rate. The average end-to-end delay for multi-hop transmission in a slotted Aloha medium access WBAN is then characterized. Subsequently, a multi-hop topology formation game is proposed that formally formulates the problem of jointly optimizing the PHY secrecy outage probability with end-to-end delay management in the uplink of a multi-hop WBAN. A distributed algorithm based on the proposed game is provided and proved to converge to a Pareto-dominant Nash topology. 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. The rest of the paper proceeds as follows. Section II presents the system model. PHY security and end-to-end latency are characterized in Sections III and IV, respectively. The multi-hop topology formation game is formulated in Section V. Numerical simulation results are provided and the proposed framework is validated in Section VI. Finally, Section VII concludes the paper.

II. 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, and 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. 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 signal arrivals via multiple propagation paths. We assume that statistical CSI knowledge for both legitimate and wiretap channels is available at the transmitters, *i.e.*, each transmitter node has estimates of the mean and standard deviation of the received SNR as measured at its neighbors.

The legitimate channel is typically modeled to undergo log-normal fading [17], [18]. 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

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

where μ_n and σ_n denote the mean and standard deviation of the received SNR γ_n in dB, respectively, and $u(.)$ is the unit step function.[1]

The off-body wiretap channel is modeled as small-scale Rayleigh fading [18]. 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

$$f(\gamma_w) = \lambda_w \exp(-\lambda_w \gamma_w) u(\gamma_w). \quad (2)$$

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.

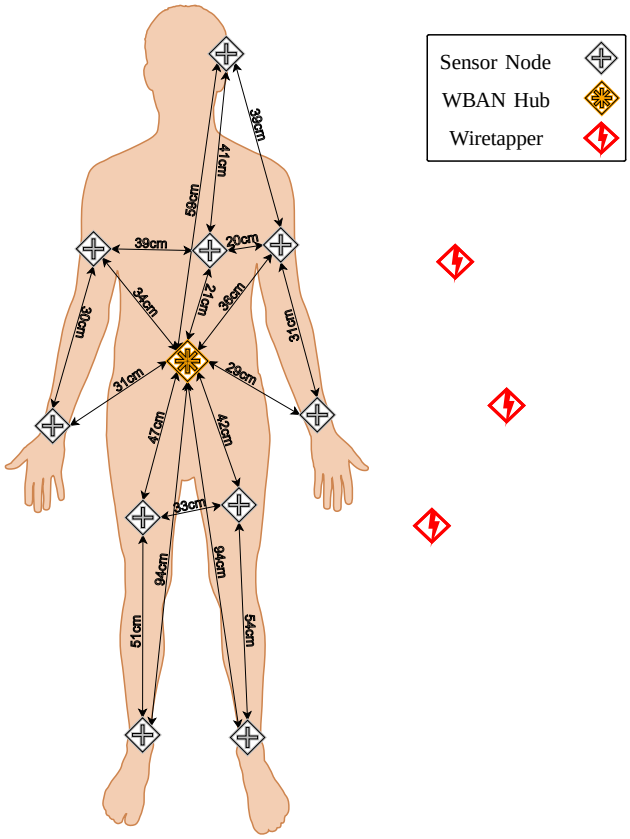


Fig. 1. A typical WBAN with off-body wiretappers in the vicinity

[1]The receiver's index is not specifically indicated in Eq. (1) for notational convenience, but note that the SNR measurements at different receiver nodes are varied due to their different communication channels.

Definition 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 rooted 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 are discussed later in Section V-A.

There are two random access methods outlined in the IEEE 802.15.6 standard for obtaining the contended allocations in a WBAN, namely carrier sense multiple access with collision avoidance (CSMA/CA) and slotted Aloha access. Here, we consider the slotted Aloha as the medium access protocol for demonstration purposes. The protocol, as described in more detail in the standard [19], 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 obtains 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 $\frac{3}{16}$.

III. 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) [20]. We adopt Wyner's wiretap channel model [2] to characterize the secrecy of transmission from an information-theoretic perspective. Wyner showed that when the wiretap channel is degraded relative to the channel of the legitimate receiver, prefect transmission secrecy is achievable, with an arbitrarily small probability of decoding error at the intended receiver and zero mutual information between the transmitted message and the received signal at the wiretapper.

The achievable secrecy rate (*i.e.*, maximum rate of secret transmissions) 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

$$\begin{aligned} R_{\langle n,i\rangle} &= \left[C_{\langle n,i\rangle} - \max_{1\leq w\leq W} C_{\langle n,w\rangle}\right]^+ \\ &= \left[\log_2(1+\gamma_n) - \max_{1\leq w\leq W} \log_2(1+\gamma_w)\right]^+, \end{aligned} \quad (3)$$

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

$$\begin{aligned} P^{\text{out}}_{\langle n,i\rangle} &= \Pr\left\{R_{\langle n,i\rangle} < \underline{R}\right\} \\ &= \Pr\left\{\log_2 \frac{1+\gamma_n}{1+\gamma_{\bar{w}}} < \underline{R}\right\} \\ &= \Pr\left\{\gamma_{\bar{w}} > 0,\ 2^{\underline{R}}(\gamma_{\bar{w}}+1) - 1 > \gamma_n > 0\right\}, \end{aligned} \quad (4)$$

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

$$\begin{aligned} P^{\text{out}}_{\langle n,i\rangle} &= \int_{\gamma_{\bar{w}}=0}^{\infty} \int_{\gamma_n=0}^{2^{\underline{R}}(\gamma_{\bar{w}}+1)-1} f(\gamma_n) f(\gamma_{\bar{w}})\, d\gamma_n\, d\gamma_{\bar{w}} \\ &= \int_0^{\infty} \Phi\left(\frac{\left[2^{\underline{R}}(\gamma_{\bar{w}}+1)-1\right]^{\text{dB}} - \mu_n}{\sigma_n}\right) \lambda_{\bar{w}} \exp(-\lambda_{\bar{w}}\gamma_{\bar{w}}) d\gamma_{\bar{w}}, \end{aligned} \quad (5)$$

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 that 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

$$P^{\text{out}}_l = 1 - \prod_{k=1}^{K} \left(1 - P^{\text{out}}_{\langle m_k,m_{k+1}\rangle}\right). \quad (6)$$

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 the multi-hop link is expected to be significantly smaller than the SOP of the direct transmission.

IV. 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 [21].

In this section, we first obtain the moment generating functions of the probability distributions of the packet inter-arrival time and service time at each sensor node. These functions are then used to derive the average end-to-end delay over a multi-hop WBAN path.

A. 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

$$M_{A_n}(t) = M^n_{A_n}(t) M^{\mathcal{C}_n}_{A_n}(t). \tag{7}$$

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

$$M^{\mathcal{C}_n}_{A_n}(t) = \prod\nolimits_{c \in \mathcal{C}_n} M_{D_c}(t), \tag{8}$$

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 from node n can be approximated by [22]

$$M_{D_n}(t) = \rho_n M_{S_n}(t) + (1-\rho_n) M_{S_n}(t) M_{A_n}(t), \tag{9}$$

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. (7), (8), and (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.

B. Transmission Time Distribution

We consider a WBAN wherein the sensor nodes seek access to the shared wireless medium using slotted Aloha.[2]

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

$$\tau = \frac{L_b}{R} + \varepsilon \approx \frac{L_b}{R}, \tag{10}$$

where L_b and R are the packet length (in bits) and date transmission rate, respectively. In Eq. (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

$$\Pr\{T_n = k\tau\} = CP_n(1-CP_n)^{k-1} \qquad k = 1,\ 2,\ \cdots, \tag{11}$$

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

$$\begin{aligned} M_{T_n}(t) = \mathbf{E}[e^{tT_n}] &= \sum_{k=1}^{\infty} CP_n(1-CP_n)^{k-1} e^{tk\tau} \\ &= \frac{CP_n\, e^{t\tau}}{1-(1-CP_n)e^{t\tau}}. \end{aligned} \tag{12}$$

C. Service Time Distribution

In order to find the distribution of the service time at a sensor node (*i.e.*, the time a node spends to transmit a packet without any error), the probability of a successful packet transmission needs to be derived 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 the transmitter itself, tries to transmit during the same time slot. We assume that all the nodes are within the carrier sensing range of one another 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

$$\chi_n = 1 - \prod_{x \in \mathcal{N} \setminus \{n\}} (1-\rho_x). \tag{13}$$

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

$$\zeta_n = 1 - \left[1 - \frac{1}{2}\exp(-\bar{\gamma}_n)\right]^{L_b}. \tag{14}$$

[2]Similar lines of reasoning can be followed to derive the distribution of transmission time in a CSMA/CA-based multi-hop WBAN [23].

From Eqs. (13) and (14), the average probability of successful packet transmission for node n, denoted by π_n, is therefore given by

$$\pi_n = 1 - [\chi_n + (1-\chi_n)\zeta_n]. \tag{15}$$

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 [24]. The moment generating function of S_n (probability distribution of service time at node n) is given by

$$\begin{aligned} M_{S_n}(t) &= \sum_{k=1}^{\infty} \pi_n (1-\pi_n)^{k-1} M_{T_n}^k(t) \\ &= \pi_n M_{T_n}(t)\big|_{CP=CP_{\max}} + \\ &\quad \pi_n(1-\pi_n) M_{T_n}^2(t)\big|_{CP=CP_{\max}} + \\ &\quad \frac{\pi_n(1-\pi_n)^2 M_{T_n}^3(t)|_{CP=CP_{\min}}}{1-(1-\pi_n)M_{T_n}(t)|_{CP=CP_{\min}}}. \end{aligned} \tag{16}$$

Note that in Eq. (16) 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. (12) and (16) and the properties of the moment generating function, the average and variance of the service time at node n are obtained respectively as

$$\mathbf{E}[S_n] = M'_{S_n}(t)\big|_{t=0} = \frac{8}{3}\tau\left(\frac{2}{\pi_n} - 3\pi_n + 2\pi_n^2\right), \tag{17}$$

and

$$\begin{aligned} \mathbf{V}[S_n] &= M''_{S_n}(t)\big|_{t=0} - \mathbf{E}[S_n]^2 \\ &= \frac{\tau^2}{9}\left(\frac{256}{\pi_n^2} - \frac{48}{\pi_n} + 768 - 1976\pi_n + 528\pi_n^2 + \right. \\ &\quad \left. 768\pi_n^3 - 256\pi_n^4\right). \end{aligned} \tag{18}$$

D. 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 the total packet delay experienced at the node n (*i.e.*, queuing delay plus service delay) as [23]

$$M_{\Delta_n}(t) = \frac{(1-\mathbf{E}[A_n]\mathbf{E}[S_n])\,(t-1)M_{S_n}(t)\,(1-M_{A_n}(M_{S_n}(t)))}{\mathbf{E}[A_n]\,(1-M_{S_n}(t))\,(t-M_{A_n}(M_{S_n}(t)))}. \tag{19}$$

The average packet delay at node n then is derived from Eq. (19) as

$$\mathbf{E}[\Delta_n] = \mathbf{E}[S_n] + \frac{\mathbf{E}[S_n]\mathbf{V}[A_n] + \mathbf{E}[A_n]\mathbf{V}[S_n]}{2\,(1-\mathbf{E}[S_n]\mathbf{E}[A_n])}. \tag{20}$$

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

$$\mathbf{E}[\Delta^l] = \sum_{k=1}^{K} \mathbf{E}[\Delta_{m_k}]. \tag{21}$$

V. 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 wiretappers, 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 another to form a multi-hop topology. Formally speaking, MTFG is specified by $\mathcal{G} = \langle \mathcal{N}, \{\mathcal{S}_n\}, \{c_n\}\rangle$ where $\mathcal{N} = \{1, \ldots, N\}$ is the set of players with a typical element of n, $\mathcal{S}_n$ is the set of strategies of player n with a strategy s_n corresponding to a choice of a next-hop node in the uplink, and c_n is the cost function associated with player n. 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. 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.

A. 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, forms 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.*,

$$\begin{aligned} c_n(G) &= P_{l_n}^{\text{out}} \\ &= 1 - \prod_{k=1}^{K}\left(1 - P_{\langle m_k, m_{k+1}\rangle}^{\text{out}}\right) \\ &= P_{\langle n, s_n\rangle}^{\text{out}} - \left(P_{\langle n, s_n\rangle}^{\text{out}} - 1\right)\left[1 - \prod_{k=2}^{K}\left(1 - P_{\langle m_k, m_{k+1}\rangle}^{\text{out}}\right)\right] \\ &= P_{\langle n, s_n\rangle}^{\text{out}} - \left(P_{\langle n, s_n\rangle}^{\text{out}} - 1\right) c_{s_n}(G). \end{aligned} \tag{22}$$

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.*,

$$\begin{aligned} q_n(G) &= \mathbf{E}[\Delta^{l_n}] \\ &= \sum_{k=1}^{K} \mathbf{E}[\Delta_{m_k}] \\ &= \mathbf{E}[\Delta_n] + \sum_{k=2}^{K} \mathbf{E}[\Delta_{m_k}] \\ &= \mathbf{E}[\Delta_n] + q_{s_n}(G). \end{aligned} \tag{23}$$

Eqs. (22) and (23) reveal that the cost and 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 and 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, 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.

B. MTFG Algorithm

Sensor nodes interact with one another to form a rooted 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 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 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 sequence of best response selections. For each sensor node $n \in \mathcal{N}$, this best response choice 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 a decrease in the security costs of its descendants as suggested by Eq. (22). 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, for every move from a graph G^t to a graph G^{t+1}, $\exists n \in \mathcal{N}$ such that $c_n\left(G^{t+1}\right) < c_n\left(G^t\right)$. Based on this fact, and given that the number of rooted tree topologies spanning a finite number of vertices is finite, it follows that the algorithm eventually converges to a final topology G^* after a finite number of iterations, such that $c_n(G^*) \leq c_n(G)$ for all $n \in \mathcal{N}$ and all the possible rooted tree topologies G. ■

We introduce the following concept of a Pareto-dominant Nash equilibrium Topology which is appropriate for investigating the stability of the network topology.

Definition 3 (Pareto-Dominant Nash Topology) A strategy profile $\boldsymbol{s}^* = \{s_n^*\}_{n\in\mathcal{N}}$ is said to constitute a Nash equilibrium topology iff no unilateral deviation in strategy by any single sensor node results in a security cost reduction for that. A Nash equilibrium topology is, furthermore, called Pareto-dominant iff the topology does not increase the security cost of any node and reduces the cost incurred by at least one node, compared to the other Nash topologies. ■

A direct consequence of Proposition 1 is that any topology resulting from the proposed algorithm is a Pareto-dominant Nash topology. Note that a deviation from such topology by any sensor node not only increases the security cost of the deviant node itself, but also brings about higher costs for the node's descendants.

C. 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 set of strategies for uplink transmission. Well-known discovery techniques [25] 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 set of strategies $\mathcal{S}_n$ as the set of nodes to which n can connect in the uplink and that can decode the signal transmitted by n with negligibly small error. Note that $\mathcal{S}_n$ is disjoint from the set $\mathcal{D}_n$ of descendants of n in the tree structure. Therefore, each sensor node n forms its set of strategies as $\mathcal{S}_n = \{i \in \mathcal{V} \,|\, i \notin (\{n\}\cup\mathcal{D}_n),\ \bar{\gamma}_n > 0\,\text{dB}\}$.

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 the members of its discovered set of strategies, 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. (22) and (23), 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.

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

NETWORK DISCOVERY
forall $n \in \mathcal{N}$ **do**
  n finds its set of strategies $\mathcal{S}_n$;
end

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

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

Algorithm 1: MTFG algorithm

Algorithm 1 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 $\mathcal{O}(|\mathcal{S}_n|)$. Another source of complexity is the number of algorithm iterations till convergence. While this is upper bounded in theory by the number of rooted 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. More specifically, it can be shown that the maximum number of iterations till convergence is equal to the height of the equilibrium tree.

Before closing this section, it is worth pointing out that 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.

VI. MODEL VALIDATION

In this section, the proposed MTFG is employed in an IEEE 802.15.6-based ultra wideband (UWB) WBAN to assess 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 as described by IEEE 802.15.6 standard with a best channel algorithm (2TBC), and single-hop star topology (ST).

A. Simulation Setup

We consider a WBAN consisting of ten on-body sensor nodes as illustrated in Fig. 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. We assume the wireless links are symmetric and that the transceivers of all the sensor nodes are identical with the same transmission range.

For the wireless propagation model in a moving WBAN, the results of the measurement campaign conducted in [17] 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

$$PL^{\text{dB}} = \overline{PL}^{\text{dB}} + \mathcal{N}(\mu,\sigma) + AC^{\text{dB}} + \sum CC^{\text{dB}}, \qquad (24)$$

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 that models the fading amplitude of the channel in dB, and AC and CC represent the effects of the temporal auto-correlation of the channel with itself and its cross-correlation with the other links, respectively.

Auto-correlation, itself, is a function of time and is given by

$$AC^{\text{dB}}(t) = \alpha \exp(-\beta t) + (1-\alpha)\exp(-\eta t)\cos(2\pi\nu t), \quad (25)$$

where the first and the second terms represent the main decaying component and the periodical component, respectively, α is the ratio between the main decaying component and the periodical component, β is the decay constant of the main decaying component, η is the decay constant of the periodical component, and ν is the frequency of the periodical component. We consider the average twenty-second effect of the auto-correlation in simulations.

Parameter values of the channel propagation model are provided in [17] for different links in the WBAN. 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.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2016.2566446, IEEE Transactions on Information Forensics and Security

To validate the model in a 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 [18]

$$PL(d)^{\text{dB}} = \xi \log_{10}(d) + \mathcal{N}(\mu,\sigma), \tag{26}$$

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

For IEEE 802.15.6 two-hop topology extension with a best channel algorithm, nodes may consider a two-hop relayed path to the hub instead of direct transmission, choosing a relaying node in the uplink with the best channel quality to achieve the highest received SNR.

B. 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

$$M^n_{A_n}(t) = \frac{\kappa}{\kappa - t}. \tag{27}$$

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. (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 42 nW (-43.8 dBm) and 9 nW (-50.5 dBm) 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 $21°C$ in computing the thermal noise spectral density.

C. 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 2TBC and ST in moving and stationary WBAN scenarios. In particular, we examine Nash topology of the network, SOP performance with prefect and imperfect statistical CSI knowledge, end-to-end latency, and the effects of delay constraint on the equilibrium.

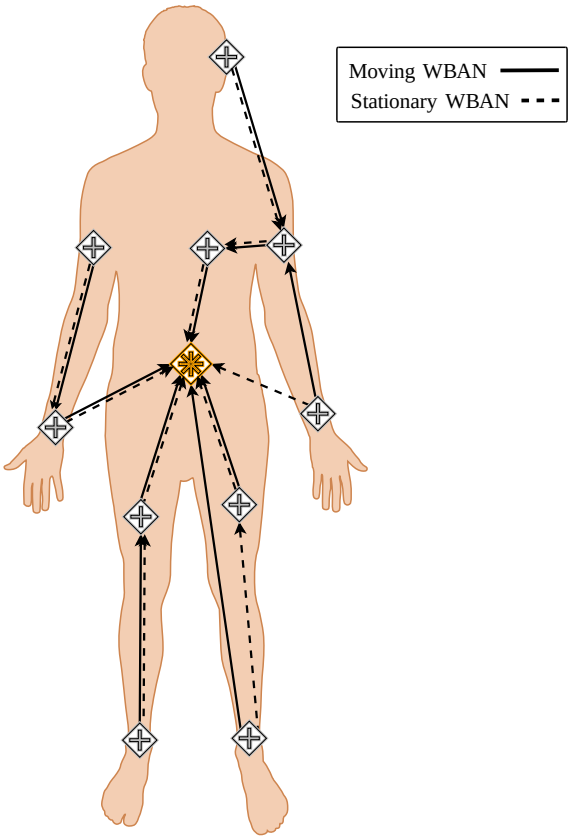


Fig. 2. Nash topology formed by the proposed MTFG for moving and stationary WBAN scenarios ($P_{\text{t}} = 42$ nW for moving WBAN and $P_{\text{t}} = 9$ nW for stationary WBAN, $\lambda_{\bar{w}} = 0.2$, $\underline{R} = 0.5$ bit/s/Hz, $L = 800$ bits, $\kappa = 1$ pkt/s, $\delta \geq 70$ ms for moving WBAN and $\delta \geq 59.5$ ms for stationary WBAN)

1) Nash Topology: Fig. 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 moving WBAN is to connect to the hub via a three-hop link, while it chooses to directly communicate 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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2016.2566446, IEEE Transactions on Information Forensics and Security

body movement actually ameliorates the quality of direct link in this case.

2) SOP Performance with Perfect Statistical CSI: First, we assume that noiseless statistical CSI knowledge of both legitimate and wiretap channels is available at the transmitters. Figs. 3 and 4 illustrate the SOP performance versus expected received SNR at the best wiretapper for nodes Head, LArm, and RArm in moving and stationary WBANs, respectively. 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 2TBC in the stationary scenario particularly for Head and RArm. In other words, the performance gain resulting from the MTFG in the moving WBAN is well above that of 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.

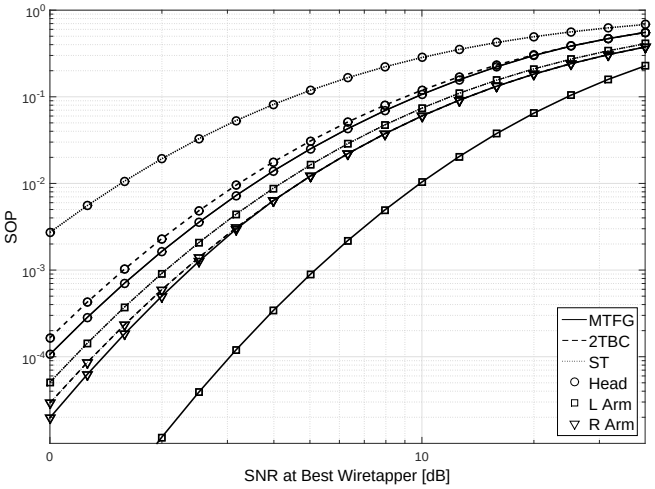


Fig. 4. Secrecy outage probability of nodes Head, LArm, and RArm as expected received SNR at best wiretapper $\frac{1}{\lambda_{\bar{w}}}$ increases for stationary WBAN scenario ($P_{\mathrm{t}} = 9$ nW, $\underline{R} = 0.5$ bit/s/Hz)

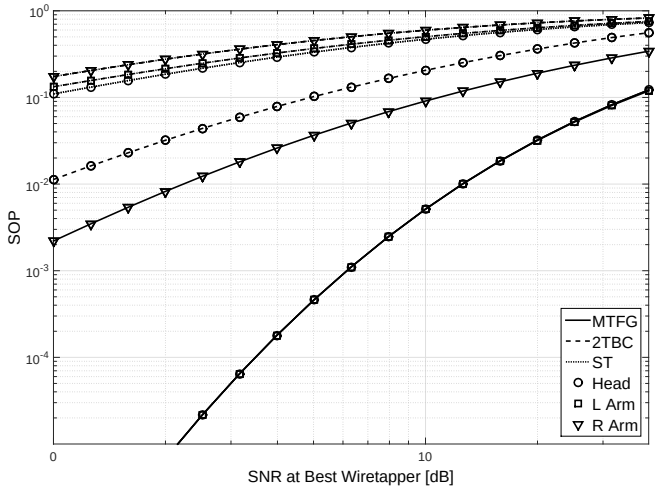


Fig. 3. Secrecy outage probability of nodes Head, LArm, and RArm as expected received SNR at best wiretapper $\frac{1}{\lambda_{\bar{w}}}$ increases for moving WBAN scenario ($P_{\mathrm{t}} = 42$ nW, $\underline{R} = 0.5$ bit/s/Hz)

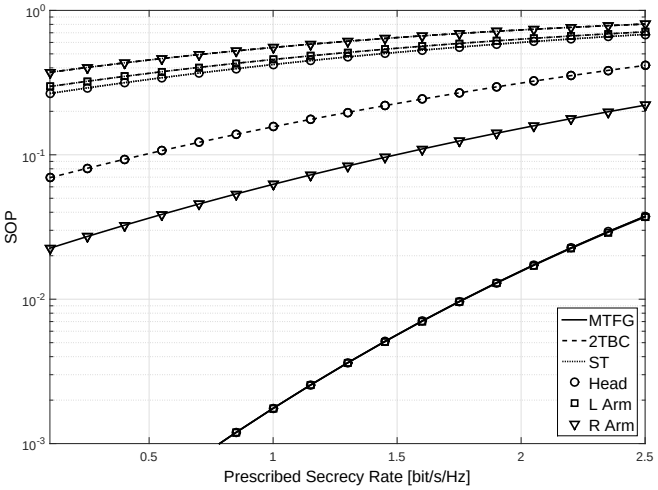


Fig. 5. Secrecy outage probability of nodes Head, LArm, and RArm as prescribed secrecy rate $\underline{R}$ increases for moving WBAN scenario ($P_{\mathrm{t}} = 42$ nW, $\lambda_{\bar{w}} = 0.2$)

Note that as the quality of the wiretap channel improves, the SOP performance difference between MTFG, 2TBC, 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. In Fig. 4, for instance, as the expected received SNR at the wiretapper increases, it is optimal for Head and RArm nodes to change their next-hop strategies to Chest node (*i.e.*, two-hop TX) and hub (*i.e.*, direct TX), respectively. Also note that in Fig. 3 node Head exhibits roughly the same SOP performance as LArm does, *i.e.*, the link Head-LArm does not essentially deteriorate the SOP of the whole path to the hub.

The SOP performance versus prescribed secrecy rate for nodes Head, LArm, and RArm is illustrated in Figs. 5 and 6 in moving and stationary WBANs, respectively. 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 Figs. 3 and 4, *e.g.*, an increase in the prescribed secrecy rate results in a decline in the performance difference between MTFG, 2TBC, and ST in both moving and stationary scenarios. Also note that in Fig. 6, the SOP performance of the node RArm for different transmission approaches is roughly the same in the stationary scenario.

3) SOP Performance with Imperfect Statistical CSI: In a noisy environment, the CSI estimates at the transmitters may be erroneous. Apart from the utilized estimation technique, the CSI estimation error is dependent on the noise level present in the channel. We model the channel estimation error as additive

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2016.2566446, IEEE Transactions on Information Forensics and Security

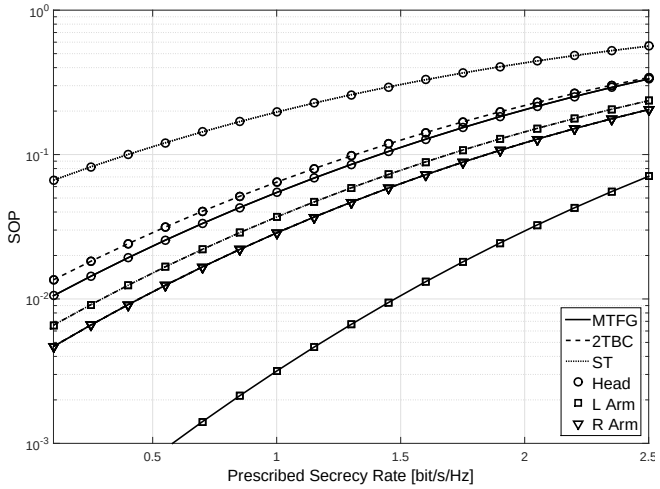


Fig. 6. Secrecy outage probability of nodes Head, LArm, and RArm as prescribed secrecy rate $\underline{R}$ increases for stationary WBAN scenario ($P_{\mathrm{t}} = 9$ nW, $\lambda_{\bar{w}} = 0.2$)

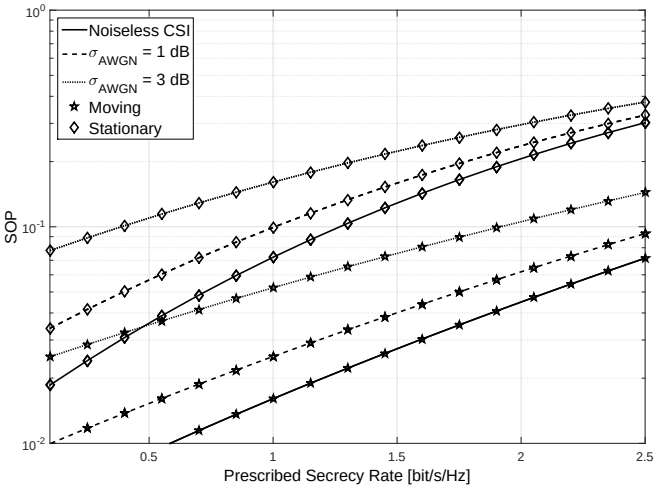


Fig. 8. Average secrecy outage probability per node of MTFG algorithm with imperfect CSI as prescribed secrecy rate $\underline{R}$ increases for moving and stationary WBAN scenarios ($P_{\mathrm{t}} = 42$ nW for moving WBAN and $P_{\mathrm{t}} = 9$ nW for stationary WBAN, $\lambda_{\bar{w}} = 0.2$)

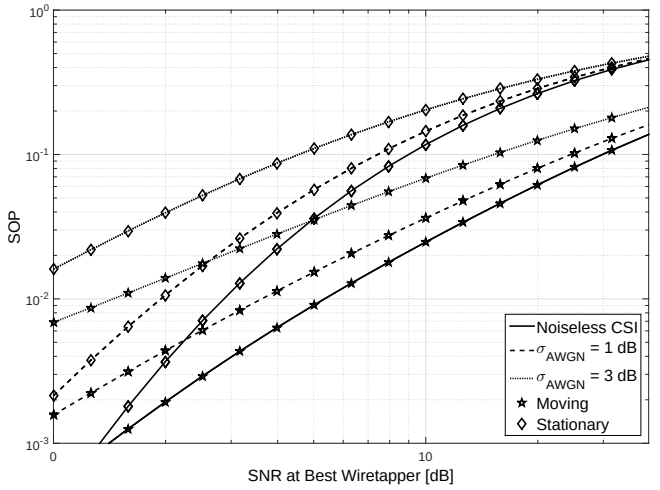


Fig. 7. Average secrecy outage probability per node of MTFG algorithm with imperfect CSI as expected received SNR at best wiretapper $\frac{1}{\lambda_{\bar{w}}}$ increases for moving and stationary WBAN scenarios ($P_{\mathrm{t}} = 42$ nW for moving WBAN and $P_{\mathrm{t}} = 9$ nW for stationary WBAN, $\underline{R} = 0.5$ bit/s/Hz)

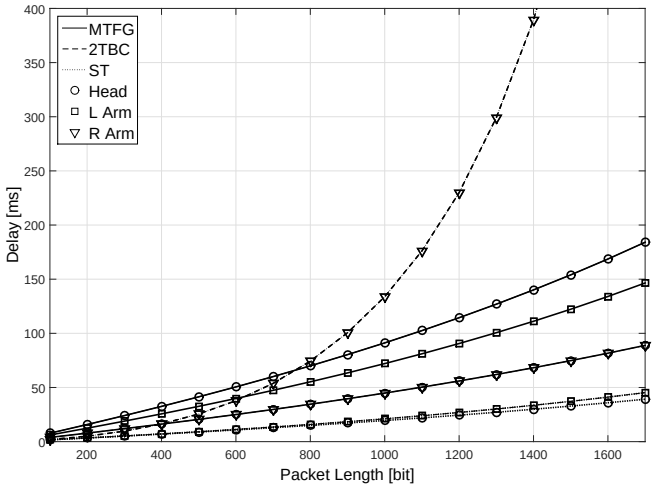


Fig. 9. End-to-end delay of nodes Head, LArm, and RArm as packet length L increases for moving WBAN scenario ($P_{\mathrm{t}} = 42$ nW, $\kappa = 1$ pkt/s)

white Gaussian noise (AWGN) with zero mean and variance of σ_{AWGN}, added to the statistical CSI measurements.

Figs. 7 and 8 depict the impact of the CSI uncertainty on the average SOP performance per node resulting from MTFG in moving and stationary WBAN scenarios. The results are obtained when the variance of the Gaussian noise is either 0 dB, 1 dB, or 3 dB. Compared to the case of noiseless CSI, it is observed that the SOP performance declines as the noise variance increases in both moving and stationary WBANs.

4) End-to-End Latency: The end-to-end delay versus packet length for nodes Head, LArm, and RArm is presented in Figs. 9 and 10 in moving and stationary WBANs, respectively. 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 results in a higher end-to-end latency. Note that MTFG introduces some extra delay to the system as expected. Yet as the packets get longer, the packet error rate over direct links increases at a higher pace compared to over multi-hop paths. In Fig. 9, for instance, longer packets of RArm are more prone to the transmission error when being directly transmitted to the hub than being relayed by RHand, which accounts for the noticeably higher delay of 2TBC and ST approaches compared to MTFG in larger packet lengths. 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.

Figs. 11 and 12 present the end-to-end delay versus packet arrival rate for nodes Head, LArm, and RArm in moving and stationary WBANs, respectively. A higher packet arrival rate

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2016.2566446, IEEE Transactions on Information Forensics and Security

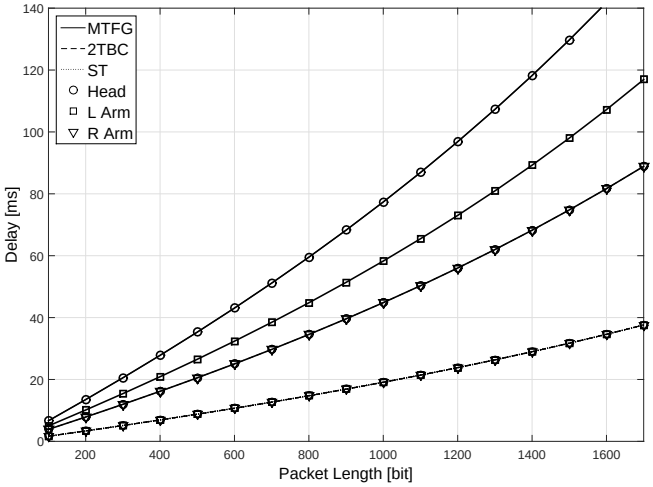


Fig. 10. End-to-end delay of nodes Head, LArm, and RArm as packet length L increases for stationary WBAN scenario ($P_{\mathrm{t}} = 9$ nW, $\kappa = 1$ pkt/s)

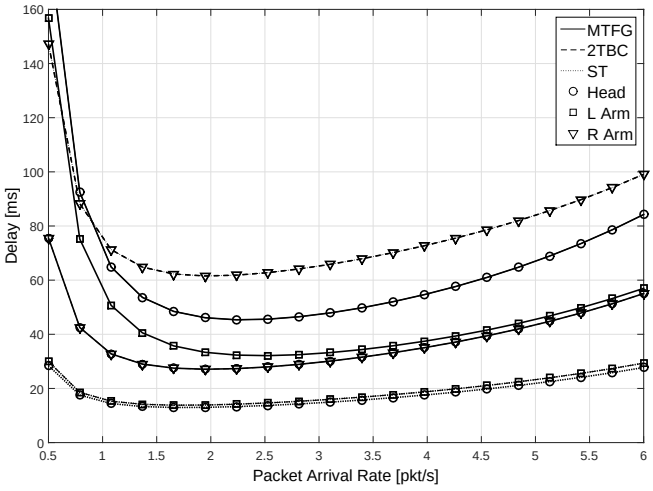


Fig. 11. End-to-end delay of nodes Head, LArm, and RArm as packet arrival rate κ increases for moving WBAN scenario ($P_{\mathrm{t}} = 42$ nW, and $L = 800$ bits)

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 it. For very small packet arrival rates, the packet inter-arrival time has the dominant effect on the delay. Therefore when the 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 that for the stationary case. In Fig. 11, note that the end-to-end delay for node RArm resulting from 2TBC and ST approaches is higher than for MTFG regardless of the packet arrival rate. This is because packets transmitted from RArm experience

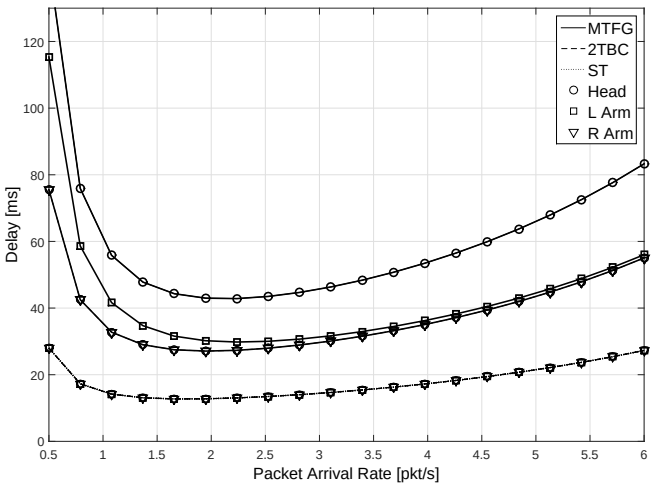


Fig. 12. End-to-end delay of nodes Head, LArm, and RArm as packet arrival rate κ increases for stationary WBAN scenario ($P_{\mathrm{t}} = 9$ nW, and $L = 800$ bits)

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.

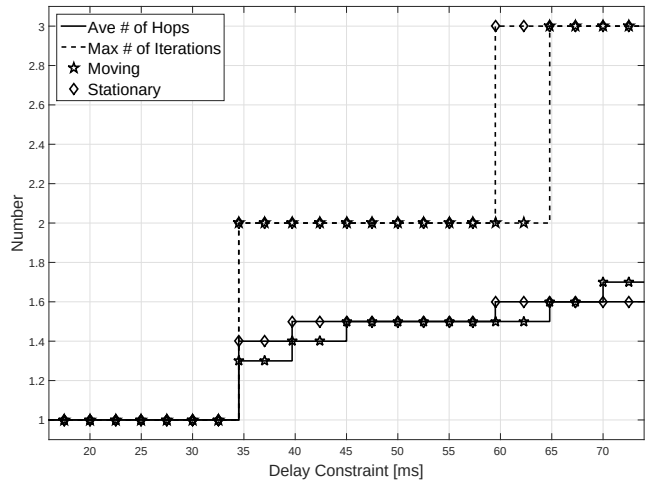


Fig. 13. Average number of hops per node and maximum number of iterations till convergence to Nash topology resulting from MTFG algorithm as delay constraint δ increases for moving and stationary WBAN scenarios ($L = 800$ bits, $\kappa = 1$ pkt/s)

5) Effects of Delay Constraint: Fig. 13 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. (7)), leading to a higher delay at the node (Eq. (20)) 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.

VII. 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 management. 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 Pareto-dominant Nash solution. The validity and effectiveness of the proposed framework are assessed 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 the star topology and IEEE 802.15.6 two-hop topology extension with a best channel algorithm. 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 as compared to in the stationary scenario. The performance of the framework can be adjusted to balance the conflicting requirements of security and latency for different applications.

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.

References

[1] 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*, vol. 16, no. 3, pp. 1550–1573, 2014.

[2] A.D. Wyner, "The wire-tap channel," *Bell System Technical Journal, The*, vol. 54, no. 8, pp. 1355–1387, October 1975.

[3] A. Khisti and Gregory W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *Information Theory, IEEE Transactions on*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[4] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *Information Theory, IEEE Transactions on*, vol. 57, no. 8, pp. 4961–4972, August 2011.

[5] Hussein Moosavi and Francis M. Bui, "Optimal relay selection and power control with quality-of-service provisioning in wireless body area networks," *accepted for publication in Wireless Communications, IEEE Transactions on*, April 2016.

[6] 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*, vol. 60, no. 8, pp. 4014–4019, August 2012.

[7] D.B. Smith and D. Miniutti, "Cooperative selection combining in body area networks: Switching rates in gamma fading," *Wireless Communications Letters, IEEE*, vol. 1, no. 4, pp. 284–287, August 2012.

[8] Hussein Moosavi and Francis M. Bui, "Routing over multi-hop fading wireless body area networks with reliability considerations," *submitted to Engineering in Medicine and Biology Society (EMBC), 2016 38th Annual International Conference of the IEEE*, February 2016.

[9] Jinbei Zhang, Luoyi Fu, and Xinbing Wang, "Asymptotic analysis on secrecy capacity in large-scale wireless networks," *Networking, IEEE/ACM Transactions on*, vol. 22, no. 1, pp. 66–79, February 2014.

[10] S. Tomasin, "Routing over multi-hop fading wiretap networks with secrecy outage probability constraint," *Communications Letters, IEEE*, vol. 18, no. 10, pp. 1811–1814, October 2014.

[11] 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*, vol. 11, no. 11, pp. 3980–3991, November 2012.

[12] Jianhua Mo, Meixia Tao, and Yuan Liu, "Relay placement for physical layer security: A secure connection perspective," *Communications Letters, IEEE*, vol. 16, no. 6, pp. 878–881, June 2012.

[13] O.O. Koyluoglu, C.E. Koksal, and H.E. Gamal, "On secrecy capacity scaling in wireless networks," *Information Theory, IEEE Transactions on*, vol. 58, no. 5, pp. 3000–3015, May 2012.

[14] Lun Dong, Zhu Han, A.P. Petropulu, and H.V. Poor, "Improving wireless physical layer security via cooperating relays," *Signal Processing, IEEE Transactions on*, vol. 58, no. 3, pp. 1875–1888, March 2010.

[15] Jinho Choi, Jeongseok Ha, and Hyoungsuk Jeon, "Physical layer security for wireless sensor networks," in *Personal Indoor and Mobile Radio Communications (PIMRC), 2013 IEEE 24th International Symposium on*, September 2013, pp. 1–6.

[16] Hao Niu, Li Sun, M. Ito, and K. Sezaki, "Secure transmission through multihop relaying in wireless body area networks," in *Consumer Electronics (GCCE), 2014 IEEE 3rd Global Conference on*, October 2014, pp. 395–396.

[17] 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*, vol. 61, no. 4, pp. 2200–2208, April 2013.

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

[19] "IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks," *IEEE Std 802.15.6-2012*, pp. 1–271, February 2012.

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

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

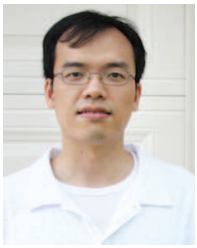
[22] Demetres D Kouvatsos, *Network Performance Engineering: A Handbook on Convergent Multi-service Networks and Next Generation Internet*, vol. 5233, Springer Science & Business Media, 2011.

[23] 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*, vol. 64, no. 7, pp. 2972–2990, July 2015.

[24] Charalambos A. Charalambides, *Compound and Mixture Distributions*, pp. 281–342, John Wiley & Sons, Inc., 2005.

[25] S. Vasudevan, M. Adler, D. Goeckel, and D. Towsley, "Efficient algorithms for neighbor discovery in wireless networks," *Networking, IEEE/ACM Transactions on*, vol. 21, no. 1, pp. 69–83, February 2013.

Hussein Moosavi (S'13) received the B.Sc. degree in electrical engineering from the Isfahan University of Technology (IUT), Iran, in 2011. During 2011-2012 he was with the APA-IUT CERT—affiliated with the Iran Telecommunication Research Center—as an R&D Engineer, where he was involved in the development and implementation of statistical machine learning solutions for analyzing the Internet traffic. He joined the University of Saskatchewan (UofS), Canada, in 2013, and completed the M.Sc. degree in electrical engineering, in 2015. His M.Sc. research was focused on game- and information-theoretic signal processing for wireless communications, and was funded by grants from the Natural Sciences and Engineering Research Council of Canada (NSERC). He also was the recipient of the Innovation and Opportunity Scholarship—awarded by the Ministry of Advanced Education, Government of Saskatchewan—for "innovative research", in 2014, and two UofS Graduate Scholarships, in 2013 and 2014, respectively. Presently he is a Research Assistant with the Department of Electrical and Computer Engineering, University of Saskatchewan. His current research interests lie in the areas of statistical pattern recognition and deep machine learning, big data analytics, and applied game theory.



Francis Minhthang Bui (S'99-M'08) received the B.A. degree (with distinction) in French language and the B.Sc. degree (with distinction) in electrical engineering from the University of Calgary, Calgary, AB, Canada, in 2001. He then received the M.A.Sc. and Ph.D. degrees from the University of Toronto, Toronto, ON, Canada, in 2003 and 2009, respectively, all in electrical engineering. He was the recipient of various scholarships and awards, including the NSERC Undergraduate Research Award, NSERC Postgraduate Scholarship for Master's Studies, and NSERC CGS for Doctoral Studies. He is currently an Assistant Professor of Electrical and Computer Engineering with the University of Saskatchewan, Saskatoon, SK, Canada. Dr. Bui's research interests include information processing and optimization, with applications in communications and biomedical engineering.