Tree Formation with Physical Layer Security Considerations in Wireless Multi-Hop Networks

Walid Saad, Xiangyun Zhou, Behrouz Maham, Tamer Başar, and H. Vincent Poor

***Abstract*—Physical layer security has emerged as a promising technique that complements existing cryptographic approaches and enables the securing of wireless transmissions against eavesdropping. In this paper, the impact of optimizing physical layer security metrics on the architecture and interactions of the nodes in multi-hop wireless networks is studied. In particular, a game-theoretic framework is proposed using which a number of nodes interact and choose their optimal and secure communication paths in the uplink of a wireless multi-hop network, in the presence of eavesdroppers. To this end, a tree formation game is formulated in which the players are the wireless nodes that seek to form a network graph among themselves while optimizing their multi-hop secrecy rates or the path qualification probabilities, depending on their knowledge of the eavesdroppers' channels. To solve this game, a distributed tree formation algorithm is proposed and is shown to converge to a stable Nash network. Simulation results show that the proposed approach yields significant performance gains in terms of both the average bottleneck secrecy rate per node and the average path qualification probability per node, relative to classical best-channel algorithms and the single-hop star network. The results also assess the properties and characteristics of the resulting Nash networks.**

***Index Terms*—Physical layer security, network formation, game theory, multi-hop networks.**

I. Introduction

THE ongoing advances in wireless technologies (e.g., cognitive radio, device-to-device communications, etc.) have introduced new security challenges in next-generation networks. Despite the proven efficiency of classical cryptographic techniques, the associated overhead and complexity may make it hard to implement encryption algorithms in future large-scale, heterogeneous, and distributed wireless networks. To overcome this problem, recently, significant research has been devoted to studying the ability of the wireless physical layer (PHY) for providing secure communications [1–14]. The main idea is to develop an information-theoretic construct that exploits the wireless channel's PHY characteristics, such as fading or noise, traditionally seen as impediments, for improving the security of wireless transmission with little computational overhead. The pioneering work of Wyner showed that *perfect secrecy* is achievable from an information-theoretic viewpoint using only the properties of the communication channel [1]. This has motivated many recent studies on physical layer security in fading channels [2–14]. The main design criterion for PHY security is the concept of a secrecy rate [3], defined as the rate of secret information that can be transmitted between two nodes, without being tapped by an eavesdropper.

Toward deploying PHY security solutions in next-generation networks, one important design challenge is to better understand how the incorporation of PHY security notions, such as secrecy rate, affects and impacts the network's operation and architecture. In particular, many emerging wireless systems, such as the IEEE WiMAX 802.16 [15], next-generation LTE-Advanced systems [16–18], or cognitive ad hoc networks [19–21], involve communications over hierarchical architectures, such as a multi-hop tree for uplink transmission [16–18], [22–28]. The interplay between the need for ensuring secrecy and the formation of such a tree architecture is an important problem that has been relatively unexplored in the literature. In fact, most existing studies have focused on the secrecy of either single-hop or two-hop (cooperative) transmissions [2–6], [10]. Although a few exceptions can be found in the study of asymptotic behavior such as capacity scaling laws [11], [12] and percolation [13], [14] in ad hoc networks, little has been done to understand how the formation of a multi-hop wireless network is impacted by the need for jointly optimizing physical layer security.

The main contribution of this paper is to study the impact of optimizing physical layer security measures on the multi-hop communication tree architecture governing the uplink of next-generation wireless networks. For this purpose, we formulate a tree formation game among a number of legitimate wireless nodes that seek to transmit data to a common base station, in the presence of eavesdroppers. In this game, each node must decide on its preferred path to the base station by optimizing a utility that reflects the security of the chosen path. We consider two scenarios with different assumptions about the knowledge of the eavesdroppers' channels available to the legitimate nodes and derive a utility for path optimization in each scenario: the utility is given as the bottleneck secrecy rate of the chosen path when the full channel knowledge of the

Manuscript received October 27, 2011; revised March 5 and July 16, 2012; accepted July 17, 2012. The associate editor coordinating the review of this paper and approving it for publication was D. Tarchi.

W. Saad is with the Electrical and Computer Engineering Department, University of Miami, Coral Gables, FL, USA (e-mail: walid@miami.edu).

X. Zhou is with the Research School of Engineering, Australian National University, Australia (e-mail: xiangyun.zhou@anu.edu.au).

B. Maham is with the School of Electrical and Computer Engineering, University of Tehran, Tehran, Iran (e-mail: bmaham@ut.ac.ir).

T. Başar is with the Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, USA (e-mail: basar1@illinois.edu).

H. V. Poor is with the Electrical Engineering Department, Princeton University, Princeton, NJ, USA (e-mail: poor@princeton.edu).

A preliminary version of this work was presented as an invited paper at the Third International Workshop on Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP) [47]. This work was supported in part by the Australian Research Council's Discovery Projects funding scheme (project no. DP110102548), and in part by an AFOSR MURI Grant (FA9550-10-1-0573).

Digital Object Identifier 10.1109/TWC.2012.091812.111923

eavesdroppers is available, while it is given as the path qualification probability, i.e., the probability of achieving a certain target rate over the entire multi-hop path, when only statistical channel knowledge is known. To solve the tree formation game, we propose a distributed algorithm that allows the nodes to interact and decide on their multi-hop communication paths. We show that the proposed algorithm converges to a stable Nash network. Using simulations, we show that the proposed tree formation game yields significant performance gains, in terms of both the average bottleneck secrecy rate per node and the average path qualification probability per node, relative to classical best-channel algorithms and the single-hop star network.

The rest of this paper is organized as follows: Section II presents the system model and Section III presents the game formulation. Section IV discusses the proposed utility metrics while Section V presents the proposed tree formation algorithm. Simulation results are analyzed in Section VI. Finally conclusions are drawn in Section VII.

II. System Model

A. Network Model

Consider a wireless network composed of N nodes that need to transmit data to a common base station (BS) in the uplink. Let $\mathcal{N}$ denote the set of all such nodes. In this network, K eavesdroppers are present and able to tap into the transmission of the nodes, individually (i.e., no cooperation is allowed). We let $\mathcal{K}$ denote the set of all eavesdroppers. The channel between any two nodes experiences both path loss attenuation and small-scale fading. We assume quasi-static Rayleigh fading channels. For a transmission from node $i \in \mathcal{N}$ to (a different) node $j \in \mathcal{N} \cup \mathcal{K}$, the received signal-to-noise ratio (SNR) is given by

$$\gamma_{i,j} = \frac{P_i \cdot d_{i,j}^{-\mu} \cdot |h_{i,j}|^2}{\sigma^2}, \tag{1}$$

where P_i is the transmit power of node i, σ^2 is the variance of the Gaussian receiver noise, $d_{i,j}$ is the distance between node i and node j, μ denotes the path loss exponent, and $|h_{i,j}|^2$ is the fading gain which follows an exponential distribution with unit mean. The average SNR is hence given by

$$\bar{\gamma}_{i,j} = \frac{P_i \cdot d_{i,j}^{-\mu}}{\sigma^2}. \tag{2}$$

For simplicity and without loss of generality, we assume that all the channel fading gains are independent of one another and the nodes have the same transmit power given as $P_i = \tilde{P},\ \forall i \in \mathcal{N}$. To transmit their packets, the nodes can either use a direct link to the BS or adopt multi-hop transmission. In this respect, we assume that the nodes are willing to relay each other's packets and that they can use orthogonal transmissions during multi-hop, similar to those in [16-18], [22], [29] and [30]. Consequently, the final topology governing the network is a hierarchical uplink *tree structure*[1] whereby each node $i \in \mathcal{N}$ is connected to the BS either directly or through one or more nodes in $\mathcal{N}$. Such a multi-hop communication network is envisioned to be a strong candidate for deployment in emerging wireless systems such as LTE-Advanced [16–18], [31], WiMAX 802.16j [15], [32], [33], or IEEE 802.11s [34].

[1]While the scope of this paper is limited to tree networks, the proposed approach can be extended to other network architectures as well, with some modification in the game-theoretic formulation.

B. Secure Transmission Scheme

Hereinafter, we assume that the identity of the nodes (i.e., whether they are malicious or honest) is common knowledge in the network. This assumption is similar to ones in most of the existing physical layer security literature [2–14] and could model a variety of practical scenarios. On the one hand, this model can capture a scenario in which the nodes suspect the presence of malicious eavesdroppers at specific pre-determined network locations (e.g., in a battlefield or military scenario). On the other hand, the studied model is also applicable to a network in which the eavesdroppers are not malicious nodes, but rather are legitimate participants in the network. In such a case, the proposed model applies to situations in which some messages are not intended for all nodes of the network such as when some content is "premium" content and should be received only by those who have paid for it (legitimate receivers) while others (eavesdroppers) should be denied access (e.g., as in [9]). This is also applicable to cognitive networks in which the primary users might have some messages that they wish to secure against known secondary users [23].

In the presence of the eavesdroppers, the legitimate nodes will attempt to choose a secure multi-hop path to the base station. Wyner's celebrated wire-tap channel model [1] is adopted to characterize the secrecy of message transmissions from an information-theoretic viewpoint. In the wire-tap channel model, the message signal is received by a legitimate receiver and an eavesdropper via two separate channels. The objective of the transmitter is to find an encoding scheme that simultaneously achieves reliability at the legitimate receiver and secrecy against the eavesdropper. Reliability requires the received signal at the legitimate receiver to be decoded with arbitrarily small probability of error. Moreover, secrecy is measured by the mutual information between the transmitted message and the received signal at the eavesdropper. Perfect secrecy is achieved if this mutual information goes to zero rate-wise and it implies that the transmitted message is independent of the received signal at the eavesdropper. With perfect secrecy, the eavesdropper cannot do any better than a guessing-based exhaustive search for data detection and its bit error rate (BER) stays at 1/2.

We assume that Wyner's encoding scheme is used at each node [1], i.e., the transmitting node chooses two rate parameters, namely, the rate of transmitted codewords R' and the rate of the actual messages R. A positive rate redundancy $R'-R > 0$ is needed to provide secrecy against the eavesdropper. A Wyner code of length M is constructed by generating $2^{MR'}$ codewords $x^M(w,v)$ of length N, where $w = 1, 2, ..., 2^{MR}$ and $v = 1, 2, ..., 2^{M(R'-R)}$. For each message index w, we randomly select v from $\{1, 2, ..., 2^{M(R'-R)}\}$ with uniform probability and transmit the codeword $x^M(w,v)$. Clearly, the rate redundancy $R' - R$ determines the number of codewords

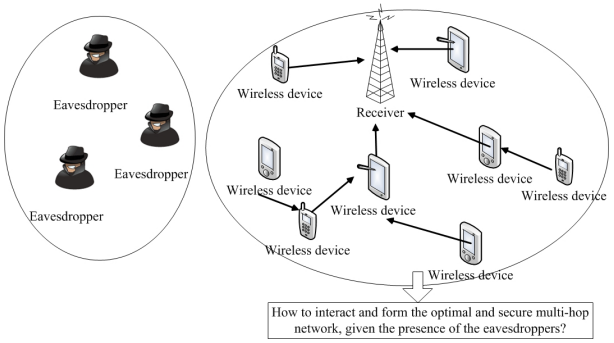


Fig. 1. An illustration of the studied model for multi-hop transmission with physical layer security considerations.

associated with each message. When the rate redundancy is larger than the channel capacities of all the non-cooperating eavesdroppers, perfect secrecy can be achieved. Additionally, the legitimate receiving node can decode the transmitted message with negligibly small error if the codeword rate R' is below the channel capacity of the legitimate link. Hence, a secure and reliable transmission over each single-hop link requires a careful design of the two rate parameters. A detailed description of the wire-tap channel model and Wyner's encoding scheme can be found in [1], [35], and [36]. In Section IV, we will describe the specific choices of the rate parameters in two different scenarios.

Given these physical layer security considerations, the main objective of the nodes is to interact in order to select their next hops, i.e., form a graph G that interconnects them while taking into account the presence of the eavesdroppers. An illustration of the proposed model is shown in Fig. 1.

We note that the proposed scenario is relevant for studying how physical layer security can be deployed in many scenarios in the *uplink* of practical wireless systems such as LTE and 802.16j in which tree-based communication is expected to be a central theme [16–18], [22–28], [34] (e.g., via relay stations or via the use of device-to-device (D2D) communications). Other networks in which tree multi-hop communication is also relevant include ad hoc and cognitive radio networks [23]. Certainly, this work presents only a first step toward a better understanding of how physical layer security can be incorporated into realistic networks.

III. Tree Formation Game: Formulation

To form a multi-hop network, the nodes need to interact with one another. Moreover, each node is selfish, in the sense that it needs to optimize its own utility. Hence, there is a need to model these interactions in order to get insight into the multi-hop network architectures that will emerge from them. To do so, we will use the framework of network formation games. Network formation games are game-theoretic techniques that are rooted in social networks and used to study friendship relationships between individuals which are often modeled as graphs [37]. In these games, several independent decision makers (players) interact for the purpose of forming a network graph $G = (\mathcal{V}, \mathcal{E})$ among themselves, with $\mathcal{V}$ the set of nodes or vertices in the graph and $\mathcal{E}$ the set of directed edges or arrows. The objective of network formation is to find some desired set of directed edges $\mathcal{E}$ among all the possible configurations given the objectives of the involved entities. Due to the similarity between forming friendship relationships and forming the proposed multi-hop network structure, network formation games provide a suitable framework for analyzing our model.

To this end, the proposed multi-hop tree formation in the presence of the eavesdroppers is formulated as a tree formation game in which the players are the nodes. The interactions between the nodes will result in a *directed* graph $G(\mathcal{V}, \mathcal{E})$ with $\mathcal{V} = \{1, \ldots, N+1\}$ denoting the set of all vertices (all N nodes in $\mathcal{N}$ and the BS) and $\mathcal{E}$ denoting the set of all edges (links) between pairs of nodes. Each node seeks to connect to the BS through a certain chosen path defined as follows.

Definition 1: A *path* between any two nodes i and j in the graph G is defined as a sequence of nodes $l_1, \ldots, l_M$ such that $l_1 = i$, $l_M = j$ and each directed link $(l_k, l_{k+1}) \in G$ for each $k \in \{1, \ldots, M-1\}$. We denote the set T_i as the set of all paths from node i to the BS, and thus $|T_i|$ represents the number of paths from node i to the BS.

In the uplink of a wireless network, each node will have a single path that connects it to the base station. Therefore, we will deal only with multi-hop *tree structures*, and hence for any node i we have $|T_i| = 1, \ \forall\, i \in \mathcal{V}$. Hereinafter, we denote by $t_i \in T_i$ the path between any node i and the BS.

The second component of the game is the set of *strategies*. In the proposed game, the strategy space of any node $i \in \mathcal{N}$ is the set of nodes in $\mathcal{V}$ to which i can connect in the uplink. We note that, due to factors such as computational capabilities, each node $j \in \mathcal{N}$ can only accept a limited number ϱ_j of connections from other nodes. Hence, the strategy space of a node i will exclude any node j that has more than ϱ_j links already connected to it.

The strategy of any node i is to choose the link that it wants to form from its strategy space. A node i cannot choose to connect to another node j which is already connected to it either directly or indirectly, i.e., a node cannot choose to connect to its descendants in the tree structure. Normally, for a current network graph G, let $\mathcal{A}_i = \{j \in \mathcal{V} \setminus \{i\} |\ \exists$ links $(i_0 = j, i_1), (i_1, i_2), \ldots, (i_p, i_{p+1} = i),$ s.t. $(i_l, i_{l+1}) \in G, \ \forall l\}$ be the set of nodes that are descendants of node i, and $\mathcal{S}_i = \{(i,j) | j \in \mathcal{V} \setminus (\{i\} \bigcup \mathcal{A}_i)\}$ be the set of links corresponding to the nodes (including the BS) with whom i can form a link. In consequence, the strategy of a node i is to select the link $s_i \in \mathcal{S}_i$ that it wants to form, i.e., choose the node to which it will connect. As we restrict our analysis to tree networks, any link formation, i.e., choice of a strategy $s_i \in \mathcal{S}_i$ is, in practice, a replace operation in which the node disconnects its previous link (if any) and chooses the new link s_i. Every choice of s_i uniquely determines the path t_i used by node i to connect to the BS. To complete the formulation of the game, next, we define the utilities, i.e., the metrics for each node.

IV. Tree Formation Game: Utility

As discussed in the previous section, the strategy of an arbitrary node i in the network formation game is to select a link from $\mathcal{S}_i$. Given a network graph G, for every strategy

choice $s_i \in \mathcal{S}_i$, a given node i will experience a different performance measure or utility (with physical layer security considerations). In the following, for our game, we provide a definition for a node's utility function in two different scenarios: in the first scenario, the nodes have full knowledge of the channels to the eavesdroppers, i.e., full channel state information (CSI); while in the second scenario, only the statistics of the channels to the eavesdroppers are known by the nodes. In both scenarios, the full knowledge of the channel to the intended receiver is assumed to be known at the corresponding transmitter.

A. Full Eavesdroppers' CSI

Under full knowledge of the eavesdroppers' CSI, the rate choices of the Wyner's encoding scheme can be made to achieve perfect secrecy for every message transmission. Specifically, the codeword rate R' is chosen arbitrarily close to the capacity of the legitimate link, whilst the rate difference $R' - R$ is set arbitrarily close to the capacity of the best eavesdropper link, i.e., the eavesdropper whose link from the transmitter has the highest capacity. As a result, the message transmission is both decodable at the legitimate receiver and secure against the eavesdroppers. The achievable secrecy rate with Gaussian signaling from node i to node j is hence given by [10, Eq. (15)]:

$$C_{i,j} = \left(C^d_{i,j} - \max_{1\le k\le K} C^e_{i,k}\right)^+ \quad (3)$$

$$= \left(\log_2(1+\gamma_{i,j}) - \max_{1\le k\le K} \log_2(1+\gamma_{i,k})\right)^+, \quad (4)$$

where $C^d_{i,j}$ is the Shannon capacity for the link from node i to node j, $C^e_{i,k}$ is the Shannon capacity of the link from node i to the eavesdropper $k \in \mathcal{K}$, and $a^+ \triangleq \max(a, 0)$.

When multi-hop transmission is considered, the secrecy over a single hop is generally a necessary condition for the secrecy over the entire path. This is due to the fact that the eavesdroppers may be able to take advantage of the signal receptions from multiple transmissions of the same message along the path. Nevertheless, the authors in [12] showed that the secrecy over each hop also guarantees the secrecy over the entire path if independent randomization is used in the code at each hop. In this work, we focus only on the scenarios in which the secrecy of each hop guarantees the secrecy of the entire path. Hence, the secrecy rate performance of a chosen path (or strategy) is limited by the minimum rate of all the intermediate links, which we refer to as the *bottleneck secrecy rate*. In other words, the bottleneck secrecy rate resulting from a chosen strategy can be used as a performance indicator during tree formation. Formally, given the network graph G, for any node $i \in \mathcal{N}$, the bottleneck secrecy rate experienced by this node is

$$u_i(G) = \min_{(j,l)\in t_i} C_{j,l} \quad (5)$$

$$= \min\left(C_{i,n}, u_n(G)\right), \quad (6)$$

where t_i is the path selected by node i, determined by its chosen strategy $s_i = (i, n)$ and $C_{j,l}$ is the achievable secrecy rate over the link (j, l) and is given by (4). We can see that the utility of a node i depends on the utility, i.e., the bottleneck secrecy rate, of the directly connected node n it selects, as well as the quality of the first-hop link (i, n).

B. Statistical Eavesdropper's CSI

When the eavesdropper's instantaneous CSI is unknown to the legitimate nodes, perfect secrecy cannot always be guaranteed[2]. In this scenario, we adopt the concept of *secrecy graph* so as to characterize whether a secure link exists for a given set of realizations of the eavesdroppers' channel fading states [13], [39]: a directed link between two nodes exists in the secrecy graph when a successful transmission with a prescribed message rate R can be made with perfect secrecy given the realizations of the eavesdroppers' channel fading states. Hence, the existence of a link in the secrecy graph depends on the instantaneous qualities of the eavesdroppers' channels. In addition, we say that a path is *qualified* if all the intermediate links exist in the secrecy graph, i.e., all the intermediate links support the prescribed rate R. Since the knowledge of the legitimate receiver's instantaneous CSI is available at the transmitter, the rate of the transmitted codewords R' can still be chosen arbitrarily close to the capacity of the receiver's channel for each link. The secrecy of transmission over each link depends on whether the rate redundancy $R' - R$ is larger than the channel capacities of all the eavesdroppers.

Since the eavesdroppers' channel fading states are random and unknown to the nodes, we use a probabilistic measure on the level of security. In particular, we define a utility function, named the *path qualification probability*, as the probability that the path from node i to the BS is qualified, i.e., the probability that the path exists in the secrecy graph, when selecting the strategy s_i. Note that the random variables that determine this probability are the eavesdropper's channel fading gains in all hops which are independent of each other. Therefore, the existence of a secure transmission is independent among different hops (or links).

The probability of having a secure single-hop transmission from node i to node j with a prescribed rate R is given by

$$p_{i,j} = \mathbb{P}\left(C^d_{i,j} - R > \max_{1\le k\le K} C^e_{i,k}\right) \quad (7)$$

$$= \mathbb{P}\left((1+\gamma_{i,j})2^{-R} > 1+\gamma_{em}\right) \quad (8)$$

$$= F_{em}\left((1+\gamma_{i,j})2^{-R} - 1\right), \quad (9)$$

where $\gamma_{em} = \max_{1\le k\le K} \gamma_{i,k}$ and $F_{em}(\cdot)$ denotes the cumulative distribution function (CDF) of γ_{em} given by

$$F_{em}(x) = \mathbb{P}(\gamma_{em} < x) \quad (10)$$

$$= \mathbb{P}(\gamma_{i,1} < x, \gamma_{i,2} < x, ..., \gamma_{i,K} < x) \quad (11)$$

$$= \prod_{k=1}^{K} \mathbb{P}(\gamma_{i,k} < x) \quad (12)$$

$$= \begin{cases} \prod_{k=1}^{K}\left(1 - \exp\left(-\frac{x}{\bar{\gamma}_{i,k}}\right)\right), & \text{if } x \ge 0, \\ 0, & \text{if } x < 0, \end{cases} \quad (13)$$

[2]An exception can be found in [38] which requires the number of antennas at the legitimate nodes to be larger than that at any eavesdropper, and hence, is not applicable to the scenarios considered in this work.

which is obtained using the fact that $\gamma_{i,k}, \forall k \in \mathcal{K}$ are independent and exponentially distributed with means $\bar{\gamma}_{i,k}$. When the capacity of the legitimate receiver's channel $C^d_{i,j}$ is less than the prescribed message rate R, the second condition in (13) happens (i.e., $x < 0$), which makes $p_{i,j} = 0$. Since $C^d_{i,j}$ is known to node i, transmission is never allowed when $C^d_{i,j} < R$.

Having found $p_{i,j}$, the path qualification probability for any node $i \in \mathcal{N}$ can be computed as

$$v_i(G) = \prod_{(j,l)\in t_i} p_{j,l} \quad (14)$$

$$= p_{i,n} \cdot v_n(G), \quad (15)$$

where t_i is the path selected by node i, determined by its chosen strategy $s_i = (i, n)$, when graph G is in place. Similar to the case of full eavesdropper's CSI, the utility of the node i depends only on the utility of the directly connected node n it selects, as well as the quality of the link (i, n).

Having defined the possible utilities, the next step is to devise an algorithm that enables the nodes to form the desired tree structure, given their individual objectives.

V. Tree Formation Game: Algorithm

A. Proposed Algorithm

In the proposed tree formation game, the nodes need to interact so as to agree on a graph that will govern their multi-hop transmission network. To this end, each node has an incentive to select a path in order to optimize its own utility either in (6) or (15), depending on the CSI knowledge. First, we remark that no node has an incentive to disconnect from the network, i.e., each node needs to transmit its data using either a multi-hop path or a direct transmission. As a result, hereinafter, we deal solely with *connected* graphs.

Each strategy choice s_i by a node i can lead to a new graph structure. Hence, we let $G_{s_i,\boldsymbol{s}_{-i}}$, denote the graph formed when a given node i chooses a strategy $s_i \in \mathcal{S}_i$ while all other nodes choose a vector of strategies $\boldsymbol{s}_{-i} = [s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_N]$. To find a desired strategy, a node aims to maximize its utility, given any observation it has on the current graph and eavesdroppers' states. In this respect, it will prove useful to define the concept of a *best response*, as follows:

Definition 2: For any node $i \in \mathcal{N}$, a *best response* is a strategy $s^*_i \in \mathcal{S}_i$ such that $u_i(G_{s^*_i,\boldsymbol{s}_{-i}}) \geq u_i(G_{s_i,\boldsymbol{s}_{-i}}),\ \forall s_i \in S_i$ (under statistical CSI knowledge, this inequality should be verified for $v(\cdot)$).

Therefore, the best response for any node $i \in \mathcal{N}$ is a selected path that maximizes the node's desired utility, given *fixed strategies* from all other nodes. It is well known that deriving optimal network formation algorithms is a very challenging task, and there are no generic rules for this formation in the literature [40]. However, some notable algorithms have been studied in social and economic networks for various game models with directed and undirected graphs [37], [40–43]. Nevertheless, these algorithms are restricted to specific utilities which are mainly related to social networks and are inapplicable to a wireless network such as in this work. To this end, we propose a novel tree formation algorithm, based on best response and composed of three main stages: discovery, tree formation, and multi-hop transmission.

In the first stage, each node observes its environment so as to discover neighboring nodes and learn the current network state. At this stage, the nodes can use well-known learning and discovery techniques such as in [44] and [45] so as to discover their neighbors. For example, during the initial operation of the network, in which all nodes are directly connected to the BS, each node can detect the strength of other nodes' uplink signals (through techniques similar to those used in ad hoc routing discovery [44]) and, thus, find partners for multi-hop communications. For each node $i \in \mathcal{N}$, the outcome of the neighbor discovery phase is a listing of potential neighboring partners as well as the current observed state of the network.

Following network discovery, the nodes will engage in the second stage of the proposed algorithm, i.e., the tree formation phase. In this phase, having discovered the network, each node chooses its best response, given its current knowledge about the network graph. The proposed approach is myopic, in the sense that each node aims at optimizing its current utility, without accounting for a far sighted future evolution of the network[3]. Here, we assume that the nodes make their best response decisions, sequentially, in an arbitrary order. This order is generally determined by the actual operation of the network (e.g., which node makes the first decision, etc.). To find its best response, a node i will interact, using pairwise negotiations over a control channel, with its neighboring nodes. As seen in (6) and (15), a node needs only to obtain the utility of a prospective parent node, so as to assess its own performance and, hence, make a decision on its best response. During these negotiations, the nodes can also acquire the CSI from one another, hence helping them in evaluating their utilities. Alternatively, the CSI can also be conveyed from the base station as in [23], [27] and [28]. This pairwise interaction process can occur with low complexity as the involved nodes do not need to exchange a lot of control information. Hence, the tree formation phase will consist of a number of iterations in which, sequentially, each node chooses its best response. The convergence of this phase of the algorithm is guaranteed as follows:

Theorem 1: Given any initial network graph G_0 and any sequence of best response interactions, the proposed tree formation algorithm is guaranteed to converge to a final network graph G_M, after M iterations.

Proof: Any iteration m of the proposed tree formation process consists of a sequence of best response links chosen by the nodes. Let G_m be the graph reached at the end of any arbitrary iteration m. Hence, the process can be represented by the following sequence:

$$G_0 \rightarrow G_1 \rightarrow G_2 \rightarrow \cdots \rightarrow G_m \rightarrow \cdots \quad (16)$$

A move from a graph G_m to a graph G_{m+1} in (16) represents the choice of a best response by an arbitrary node i. To this end, clearly, when a node i chooses its best response, as per Definition 2, the utility of node i does not decrease. This best response choice by a node i may impact three types of

[3]Although the proposed approach can be extended to accommodate far sighted approaches, in general, these approaches are more complex to implement, notably in a wireless context [37].

TABLE I
PROPOSED ALGORITHM FOR TREE FORMATION.

Initial Network State

Initially, the network is organized according to a certain graph G_0 (e.g., a star network or others).

Proposed tree formation process based on three phases

Phase I - Network Discovery:

a) Each node detects neighboring uplink transmissions.

b) Each node uses the detected signals to discover and learn about the presence of neighboring nodes using well-known discovery and learning techniques such as in [44–46].

Phase II - Distributed Tree Formation:

repeat

In an arbitrary but sequential order, the nodes play an iterative tree formation game.

a) In every iteration m, each node $i \in \mathcal{N}$ interacts with the discovered nodes, over a control channel.

b) Each node $i \in \mathcal{N}$ identifies its best response $s_i^* \in \mathcal{S}_i$.

c) Each node $i \in \mathcal{N}$ executes its best response by replacing its current link with a new link s_i^* so as to maximize its utility.

until convergence to a Nash network G_M after M iterations.

Phase III - Multi-hop Transmission with Physical Layer Security Considerations:

The nodes transmit their packets over the Nash network G_M.

nodes: (I)- nodes that are connected to node i either directly or indirectly, (II)- nodes that are not connected to i, (III)- nodes that are parents of node i. Following a best response by node i, the utilities of any node $j \neq i$ that is connected to i are also guaranteed not to decrease, since, as is clear through (6) and (15), an improvement in the utility of a node on a given path can only lead to an improvement in the utilities of its children. Further, it is clear that nodes in categories (II) and (III) are not affected by the best response choice of node i. Therefore, every move from a graph G_m to a graph G_{m+1} in (16) leads to an *increase* or does not lead to any decrease in the total utility of the network, i.e., the sum of all utilities.

Based on this fact, and given that the number of tree structures that interconnect a finite number of nodes is *finite*, then, the sequence in (16) will eventually end after a finite number of iterations M. Hence, the proposed tree formation algorithm is guaranteed to converge to a final network G_M, irrespective of the starting network or the order of the sequence of best responses. ■

Following the convergence to the final network, the nodes can actually engage in the final stage of the algorithm which is the actual transmission phase. In this phase, the nodes will transmit their packets, using multi-hop transmission where applicable, and, subsequently achieve the desired utility measures, with regard to physical layer security. The proposed algorithm is summarized in Table I.

Moreover, it is of interest to investigate the stability of the network resulting from our proposed algorithm in Table I. Here, it is useful to introduce the following concept [41]:

Definition 3: Any network graph G interconnecting a set of nodes $\mathcal{N}$ is said to be a *Nash network* iff no node $i \in \mathcal{N}$ is able to improve its utility by changing its current strategy $s_i \in \mathcal{S}_i$.

Inherently, a Nash network is basically an extension of the renowned concept of a Nash equilibrium, when applied to network formation games. A Nash network is, in fact, a network graph in which the links chosen by each node constitute a best response, and, hence, no node has an incentive to unilaterally change its link choice. A direct consequence of Theorem 1 is that any network resulting from our proposed approach is a stable network, that is:

Corollary 1: Any graph structure G_M resulting from the algorithm in Table I is a stable Nash network.

Note that the proposed tree formation algorithm can be used for the two different CSI scenarios. The only difference between them is the utility function used by the nodes when selecting their paths. In the case of full eavesdropper CSI knowledge, the utility is defined as the bottleneck secrecy rate, which is the achievable secrecy rate over all the intermediate links over the selected path. In the case of statistical eavesdropper CSI knowledge, the utility is defined as the path qualification probability, which is the probability that all the intermediate links can support a prescribed secrecy rate.

B. Distributed Implementation

In practice, the proposed algorithm can be implemented in a distributed manner. Following neighbor discovery, the nodes enter into a *negotiations phase* during which, the nodes can communicate, in a pairwise manner, over a control channel such as the temporary ad hoc channel or using device-to-device links [16–18]. This can be done via the following steps:

1) A node sends a "request for information" packet to each node in its list of neighbors (e.g., sequentially).
2) A node that receives a "request for information", responds with an estimate of its current utility.
3) All nodes store the received information.

In order to identify a best response operation, the nodes will use these pairwise interactions to acquire information on their prospective utilities. In the case of full CSI knowledge about the eavesdroppers, a node can easily estimate its utility using (6) given its available CSI information. Alternatively, if the nodes are aware only of statistical CSI about the eavesdroppers, then the utility in (15) is used and it can be evaluated by knowing only the average SNR values, i.e., the prospective locations of malicious nodes. Having evaluated its prospective utility, each node can identify its best response and signal, over the control channel, its willingness to connect to its chosen node. This is repeated until convergence to the Nash network.

With regard to complexity, the main complexity of the proposed algorithm lies in identifying a best response link. To do so, the nodes need to interact with one another. For instance, given a present network graph G, for every node, the computational complexity of finding its preferred partner, i.e., choosing a best response, is easily seen to be $O(|\mathcal{N} \setminus \mathcal{A}_i|)$, where $\mathcal{A}_i$ is the set of nodes connected to i. The worst case scenario is for the star topology in which case $|\mathcal{N} \setminus \mathcal{A}_i| = |\mathcal{N}| = N$. Another overhead of the tree formation algorithm lies in the utility update process after a new strategy is chosen by each node. Whenever a node i changes its parent node, its utility changes and so do the utilities of its descendants (i.e., all the nodes that are either directly or indirectly connected to node i). Hence, node i needs to inform its child nodes to update their utilities, and

then the child nodes inform the grandchildren, etc. In this way, the finally converged network is a Nash network with respect to the actual utilities of all the nodes. However, the network may choose not to include the utility update process in order to reduce the overhead and complexity. In this case, the proposed algorithm can still run as described in Table I and its convergence would still be guaranteed as per Theorem 1; however, the nodes would then use the currently perceived utility of their parent node to make their decisions. In this case, the converged network without the utility update process is still a Nash network with respect to the (possibly outdated) utilities known at all the nodes.

A further point to note is that the number of iterations till convergence is upper bounded by the total number of spanning trees over the set $\mathcal{N}$. However, in practice this total number of required iterations is reduced by various factors. On the one hand, in a practical implementation, a wireless node does not need to investigate every single node in the network so as to choose its strategy. In fact, a node needs to rely only on local information (e.g., on the nodes within its vicinity) so as to make its next-hop decision. The nodes can explore such information, for example, by monitoring neighboring transmissions or through the control or pilot channels broadcast by the base station. This implies that, in practice, the nodes will not have to visit every single network graph, before convergence. On the other hand, for large networks, the complexity can be further reduced by splitting the large network into multiple areas and applying the proposed algorithm only within each area. By doing so, one can reduce the overall complexity.

The proposed algorithm can also adapt the network to environmental changes such as slow mobility or the arrival/departure of nodes. To do so, the nodes can periodically repeat the process described in Table I. In this respect, periodically, the nodes re-evaluate the existing network by performing the discovery phase and by evaluating their utility. The interval between two consecutive attempts to detect an environmental change is chosen depending on the experienced dynamics of the environment. Once an environmental change is detected, e.g., due to a change in the perceived utility or the discovery of a new node, a node can decide to re-engage in the discovery and tree formation phase of the proposed algorithm. This will eventually lead to a new round of tree formation which, as proven in Theorem 1, will also converge to a new Nash network (convergence is guaranteed irrespective of the starting network and/or the node sequence). Hence, the proposed approach allows for adaptation of the network structure to periodic and slow environmental changes.

VI. Simulation Results and Analysis

For our simulations, we consider a square area of 2.5 km $\times$ 2.5 km with the BS at the center. In this area, the nodes and eavesdroppers are randomly deployed. The transmit power of each node is set to 20 mW, the noise variance is set to -100 dBm, and the path loss exponent is set to $\mu = 3$. Unless stated otherwise, for the case with statistical eavesdropper CSI, we set the prescribed rate to $R = 0.2$. We set the maximum number of connections that can be accepted by a node i to $\varrho_i = 4, \forall i \in \mathcal{N}$.

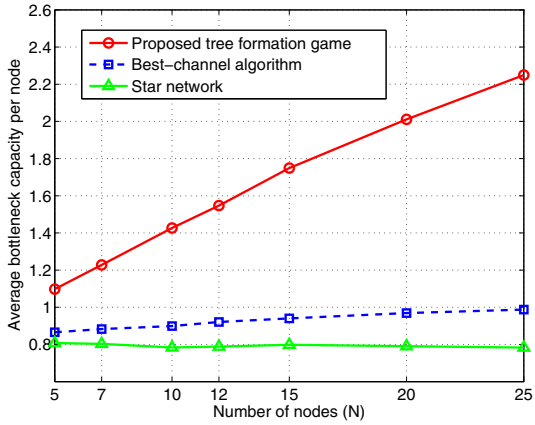


Fig. 2. Average bottleneck secrecy per node as the number of nodes N increases for a network with $K = 3$ eavesdroppers (case of full CSI knowledge).

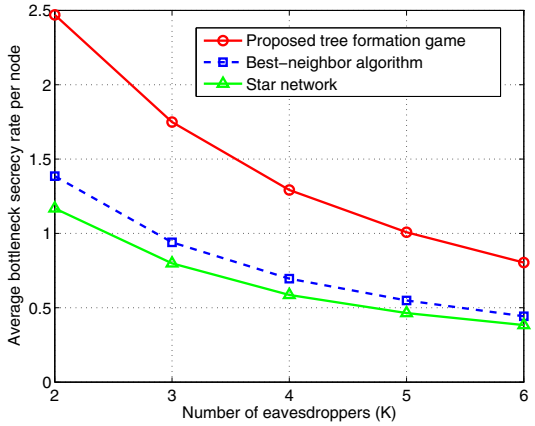


Fig. 3. Average bottleneck secrecy per node as the number of eavesdroppers K increases for a network with $N = 15$ nodes (case of full CSI knowledge).

In Figure 2, we evaluate the performance of the proposed approach for a network with $K = 3$ eavesdroppers as the number of nodes N varies in the case of full CSI knowledge. Figure 2 compares the average bottleneck secrecy rate per node resulting from the proposed game, the star network, and a best-channel algorithm in which each nodes chooses the next hop having the best channel. In Figure 2, we see that, as N increases, the average bottleneck secrecy rate per node increases for the proposed game and the best-channel algorithm. This increase is due to the fact that, as more nodes are deployed, the likelihood of finding a multi-hop route with improved secrecy increases. Figure 2 demonstrates that the proposed game yields significant gains, increasing with the network size N and reaching up to 127.8% and 187.1% at $N = 25$ nodes, relative to the best channel algorithm and the star network, respectively.

Figure 3 shows the average bottleneck secrecy rate achieved per node for a network with $N = 15$ nodes as the number of eavesdroppers, K, varies in the case of full eavesdropper CSI knowledge. In Figure 3, we can see that as the number of eavesdroppers, K, increases the average bottleneck secrecy rate decreases for all three schemes. This decrease is due to the fact that the deployment of additional eavesdroppers leads

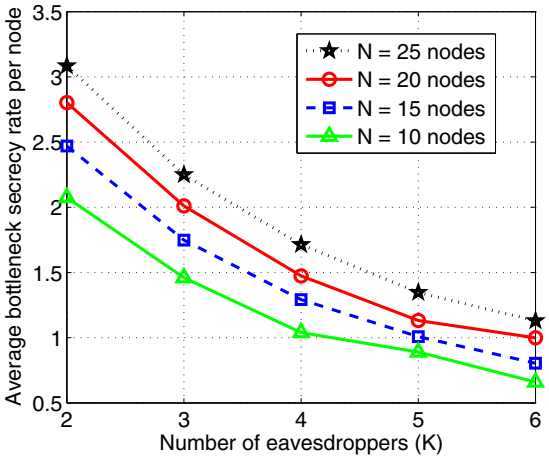


Fig. 4. Average bottleneck secrecy per node as the number of eavesdroppers K and network size N vary (case of full CSI knowledge).

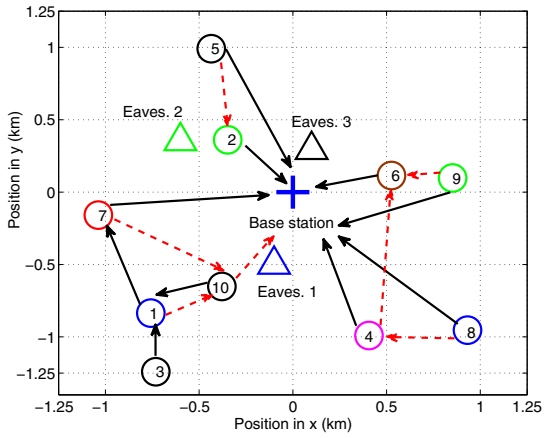


Fig. 5. A snapshot of the network structure resulting from the proposed tree formation game for a network having $N = 10$ nodes for the scenario with $K = 3$ eavesdroppers (solid lines) and the scenario in which no eavesdroppers are present (dashed lines).

to an increased security threat for all hops at the physical layer. Figure 3 shows that, for all K, the proposed network formation game achieves a significant performance gain, in terms of the average bottleneck secrecy rate, reaching up to 85.9% and 120% (at $K = 3$ eavesdroppers) relative to the best channel algorithm and the star network, respectively.

Figure 4 shows the average bottleneck secrecy rate achieved per node as both the numbers of nodes N and eavesdroppers K vary. This figure shows that as the number of nodes increases, the average bottleneck secrecy rate per node increases at all K. This is a byproduct of the fact that for larger networks, the nodes are more likely to find more secure routes to send their data. Moreover, Figure 4 shows that, as the number of eavesdroppers increases, the average bottleneck secrecy decreases for all network sizes, due to the increasing threat. Hence, although having larger networks yields better cooperation possibilities, an increase in the number of eavesdroppers would limit the prospective gains.

In Figure 5, we show a snapshot of the Nash networks resulting from running the proposed game in two scenarios: (a)- a scenario in which no eavesdroppers are present and the nodes maximize their bottleneck throughput (dashed lines), and (b)- a scenario in which $K = 3$ eavesdroppers are deployed in the network of (a) and the nodes update their transmission choices while taking into account their physical layer security measures (solid lines). This figure is generated for $N = 10$ randomly deployed nodes with random realizations for the Rayleigh fading channels. Figure 5 clearly illustrates the impact of physical layer security considerations on multi-hop wireless transmission. First, prior to the deployment of eavesdroppers, typically, each node chooses the path with the best channels. However, once the eavesdroppers enter the network, the nodes would replace their links with new ones so as to optimize their bottleneck secrecy rate. For example, in the presence of Eavesdropper 1 and because of its proximity to node 10, both Nodes 1 and 7 update their selected communication path. For instance, Node 7 decides to connect directly to the base station while Node 1 decides to connect to Node 7 instead of Node 10 (although the channel between Nodes 1 and 10 is better than the channel between Nodes 1

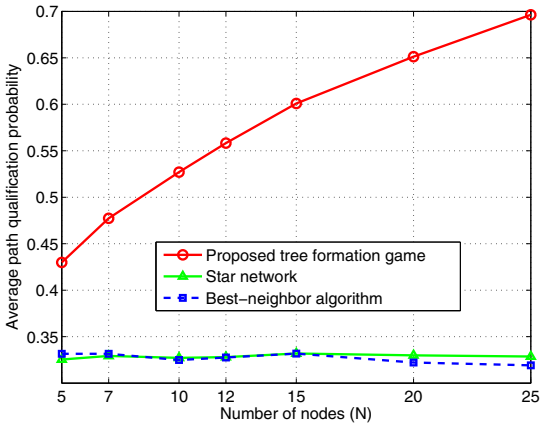


Fig. 6. Average path qualification probability per node as the number of nodes increases (case of statistical CSI knowledge).

and 7). Node 10 avoids connecting directly to the base station and chooses to connect to Node 1 instead. This is due to the fact that the channel between Node 10 and Node 1 is better than its direct channel to the base station which implies that, in the presence of Eavesdropper 1, Node 10 prefers to use the multi-hop transmission through Node 1 despite the longer transmission path. Due to the presence of Eavesdropper 2 and its proximity to Node 2, Node 5 decides to break its link with Node 2 and replaces it with a direct connection to the base station. Nonetheless, some nodes such as Nodes $2, 3$, and 6 do not modify their transmission choices before and after the deployment of the eavesdroppers.

In Figure 6, we evaluate the performance of the proposed algorithm for the case in which only statistical CSI on the eavesdroppers' channels is available. Figure 6 shows the average path qualification probability per node resulting from the proposed approach, the best-channel scheme, and the star network, for a network with $K = 3$ eavesdroppers as the number of nodes N varies. In this figure, we can see that as the number of nodes increases, the average path qualification probability per node resulting from the proposed game increases. This increase is due to the fact that, as more

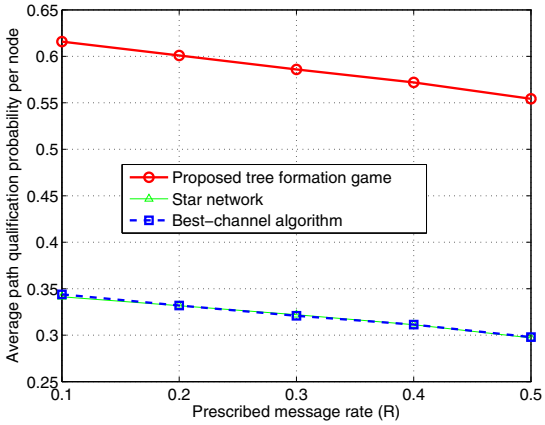


Fig. 7. Average path qualification probability per node as the prescribed message rate R varies for a network with $N = 15$ nodes and $K = 3$ eavesdroppers (case of statistical CSI knowledge).

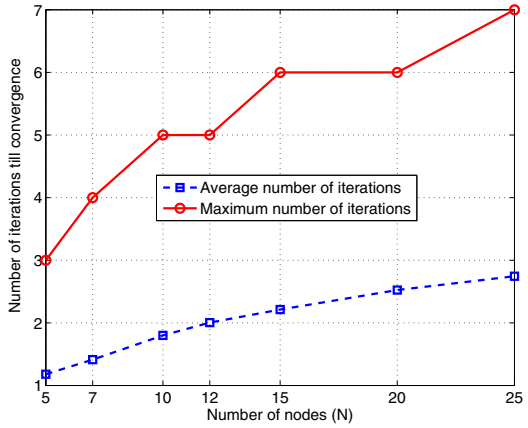


Fig. 8. Average and maximum number of iterations till convergence to a Nash network as the network size varies with $K = 3$ eavesdroppers (case of statistical CSI knowledge).

nodes are deployed, the possibility of finding a route to the base station which achieves the prescribed rate increases. In contrast, the performance of the best-channel algorithm and the star network is relatively constant as the network size varies. Fig 6 shows that the proposed game has a significant performance advantage at all network sizes, reaching up to 118.2% and 112% at $N = 25$ nodes, relative to the best-channel algorithm and the star network, respectively.

Figure 7 shows the average path qualification probability per node resulting from the proposed approach, the best-channel scheme, and the star network, for a network with $N = 15$ nodes and $K = 3$ eavesdroppers as the prescribed target secrecy rate R varies. In Figure 7, we can see that, as R increases, the average path qualification probability per node decreases for all schemes. This result stems from the fact that an increase in the prescribed message rate R implies a more stringent secrecy requirement and, thus, a lower path qualification probability. Figure 7 clearly shows that, at all rates, the proposed game yields significant performance gains, in terms of the average path qualification probability per node, reaching up to 86.6% and 86.1% at $N = 25$ nodes, relative to the best-channel algorithm and the star network, respectively.

Figure 8 shows the average and the maximum number of iterations needed till convergence of the proposed algorithm to a Nash network as the number of nodes N increases for a network with $K = 3$ eavesdroppers. In this figure, we can see that, as the number of nodes N increases, the total number of iterations needed for the convergence to a Nash network increases. This is due to the fact that, as N increases, the possibilities for performing multi-hop transmission increase, and, thus, more best response actions are needed prior to convergence. Figure 8 shows that the average and the maximum number of iterations vary, respectively, from 1.2 and 3 at $N = 5$ nodes up to 2.8 and 7 at $N = 25$ nodes. This result implies that, on the average, the speed of convergence of the proposed game is reasonable even for relatively large networks. In Figure 9, we show the average and the average maximum number of hops that govern the network architecture resulting from the proposed tree formation game for a network with $K = 3$ eavesdroppers as the number of nodes N increases, in the case of statistical CSI knowledge. Figure 9 shows that, as the network size N increases, both the average and the average maximum number of hops in the final Nash network tree structure increase. The average and the average maximum number of hops vary, respectively, from 1.9 and 2.5 at $N = 5$ nodes, up to 4.6 and 8 at $N = 25$ nodes. Figure 9 demonstrates that, as the network becomes larger, the nodes have an incentive to use multi-hop communication so as to optimize their secrecy.

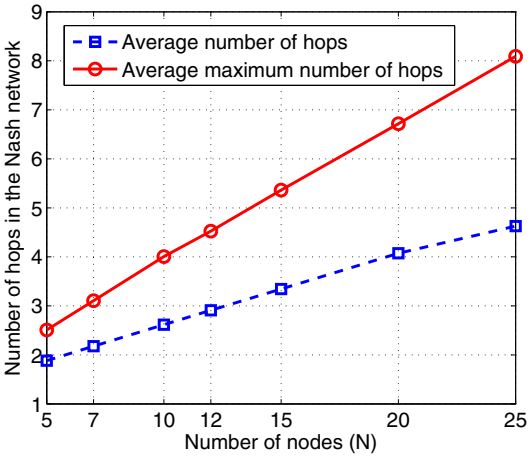


Fig. 9. Average and average maximum number of hops in the Nash network structures resulting from the proposed game as the network size varies with $K = 3$ eavesdroppers (case of statistical CSI knowledge).

In Figure 10, we evaluate how the proposed tree formation game enables the nodes to adapt to periodic mobility, in the case of statistical CSI knowledge. The chosen mobility model is a random walk scheme in which the nodes move at a constant speed in a random direction uniformly distributed between 0 and 2π. For both figures, in order to emphasize *solely* the impact of the changes of the nodes' locations due to mobility, we took fading to be constant over the whole duration.

Figure 10 shows, over a period of 5 minutes, the average total number of actions performed per node per minute for different node speeds for two network sizes in a network with $K = 3$ eavesdroppers. The nodes evaluate whether they need to change their strategies or not every 30 seconds. In Figure 10,

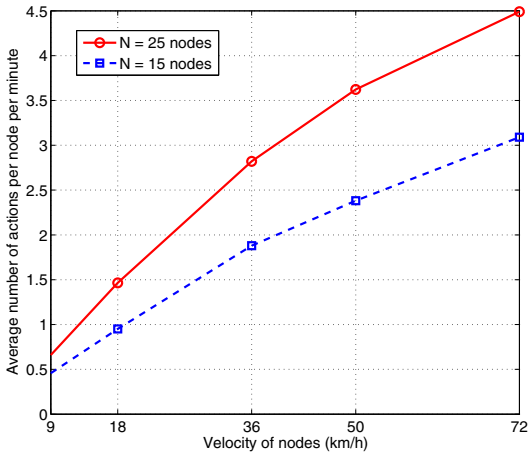


Fig. 10. Average number of actions performed per node per minute for a mobile network (with $K = 3$ eavesdroppers for different numbers of nodes) in which the nodes engage periodically in the proposed tree formation game.

we can see that, as the speed of the nodes increases, the average number of actions increases for both $N = 15$ nodes and $N = 25$ nodes. This implies that, as the environment changes faster, the nodes are more apt to change their tree formation strategies. Moreover, Figure 10 shows that for larger networks, the slope of increase is steeper due to the availability of more possible network paths. In fact, Figure 10 clearly demonstrates that the network with $N = 25$ nodes leads to an average number of actions per node that is larger than that of the network with $N = 15$ nodes. Hence, clearly, as the network becomes larger, the nodes are more prone to take a decision to change their links as reflected by the average number of actions. In this context, for $N = 15$ nodes, the average total number of actions per node per minute varies from around 0.5 at 9 km/h to around 3 at 85 km/h while for $N = 25$ nodes, this variation is from 0.7 at 9 km/h to around 4.5 at 85 km/h.

VII. Conclusions

In this paper, we have studied the problem of multi-hop communications in the presence of eavesdroppers. We have proposed a novel game-theoretic formulation that enables a number of wireless nodes to interact and optimize the security of their uplink transmissions. In the proposed game, the strategy of each node is to choose its preferred path to reach the base station, while optimizing physical layer security-related utilities. The type of adopted utility depends on the knowledge that the nodes have about the eavesdroppers' channels. To solve the game, we have proposed a distributed algorithm that enables the nodes to engage in pairwise negotiation so as to decide on the graph structure that will interconnect them. We have shown that the proposed algorithm converges to a Nash network and we have studied the properties of the resulting network. Simulation results have demonstrated that the proposed approach leads to significant performance gains in terms of both the average bottleneck secrecy rate per node and the average path qualification probability per node, relative to classical algorithms and the star network.

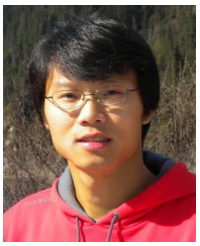
References

[1] A. D. Wyner, "The wire-tap channel," *Bell System Techn. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
[2] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.
[3] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4687–4698, Sep. 2008.
[4] A. O. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.
[5] P. Prada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. 2005 IEEE Int. Symp. Inf. Theory*, pp. 2152–2155.
[6] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," in *Proc. 46th Annual Allerton Conference on Communication, Control, and Computing*, 2008.
[7] S. Mathur, A. Reznik, Y. Chunxuan, R. Mukherjee, A. Rahman, Y. Shah, W. Trappe, and N. Mandayam, "Exploiting the physical layer for enhanced security," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 63–70, Oct. 2010.
[8] Y. S. Shiu, S. Y. Chang, H. C. Wu, S.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.
[9] Y. Sarikaya, O. Ercetin, and C. E. Koksal, "Wireless network control with privacy using hybrid ARQ," in *Proc. 2012 IEEE Int. Symp. Inf. Theory*.
[10] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, "Compound wire-tap channels," in *Proc. 45th Annual Allerton Conference on Communication, Control, and Computing*, 2007.
[11] S. Vasudevan, D. Goeckel, and D. Towsley, "Security-capacity trade-off in large wireless networks using keyless secrecy," in *Proc. 2010 ACM Int. Symp. Mobile Ad Hoc Networking and Computing*, pp. 21–30.
[12] O. O. Koyluoglu, C. E. Koksal, and H. El Gamal, "On secrecy capacity scaling in wireless networks," submitted. Available: http://arxiv.org/abs/0908.0898.
[13] M. Haenggi, "The secrecy graph and some of its properties," in *Proc. 2008 IEEE Int. Symp. Inf. Theory*, pp. 539–543.
[14] P. C. Pinto and M. Z. Win, "Continuum percolation in the intrinsically secure communications graph," in *Proc. 2010 IEEE Int. Symp. Inf. Theory and Its Applications*.
[15] The Relay Task Group of IEEE 802.16, "The p802.16j baseline document for draft standard for local and metropolitan area networks," 802.16j-06/026r4, Tech. Rep., June 2007.
[16] S. W. Peters, A. Panah, K. Truong, and R. W. Heath, "Relay architectures for 3GPP LTE-Advanced," *EURASIP J. Wireless Commun. and Networking*, vol. 2009, May 2009.
[17] T. Wirth, V. Venkatkumar, T. Haustein, E. Schulz, and R. Halfmann, "LTE-Advanced relaying for outdoor range extension," in *Proc. 2009 IEEE Vehicular Technology Conference – Fall*.
[18] O. Teyeb, V. V. Phan, B. Raaf, and S. Redana, "Dynamic relaying in 3GPP LTE-Advanced networks," *EURASIP J. Wireless Commun. and Networking*, vol. 2009, July 2009.
[19] D. Niyato, E. Hossain, and Z. Han, *Dynamic Spectrum Access and Management in Cognitive Radio Networks*. Cambridge University Press, 2009.
[20] B. Zhang, Y. Takizawa, A. Hasagawa, A. Yamaguchi, and S. Obana, "Tree-based routing protocol for cognitive wireless access networks," in *Proc. 2007 IEEE Wireless Communications and Networking Conf.*
[21] G.-M. Zhu, F. Akyildiz, and G.-S. Kuo, "STOD-RP: a spectrum-tree based on-demand routing protocol for multi-hop cognitive radio networks," in *Proc. 2008 IEEE Global Communication Conference*.
[22] B. Lin, P. Ho, L. Xie, and X. Shen, "Optimal relay station placement in IEEE 802.16j networks," in *Proc. 2007 International Conference on Communications and Mobile Computing*.
[23] D. Niyato, E. Hossain, D. Kim, and Z. Han, "Joint optimization of placement and bandwidth reservation for relays in IEEE 802.16j mobile multihop networks," in *Proc. 2009 IEEE Int. Conf. on Communications*.
[24] H. Min, W. Seo, J. Lee, S. Park, and D. Hong, "Reliability improvement using receive mode selection in the device-to-device uplink period underlaying cellular networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 413–418, Feb. 2011.
[25] B. Kaufman and B. Aazhang, "Cellular networks with an overlaid device to device network," in *Proc. 2008 Asilomar Conference on Signals, Systems and Computers*.
[26] C.-H. Yu, K. Doppler, C. B. Ribeiro, and O. Tirkkonen, "Resource sharing optimization for device-to-device communication underlaying

cellular networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2752–2763, Aug. 2011.
[27] A. Ghosh, J. Zhang, J. G. Andrews, and R. Muhamed, *Fundamentals of LTE*. Prentice-Hall, 2010.
[28] J. G. Andrews, A. Ghosh, and R. Muhamed, *Fundamentals of WiMAX*. Prentice-Hall, 2007.
[29] A. de Baynast, O. Gurewitz, and E. W. Knightly, "Cooperative strategies and optimal scheduling for tree networks," in *Proc. 2007 IEEE Conf. on Comp. Comm.*, pp. 1857–1865.
[30] B. Lin, P. Ho, L. Xie, and X. Shen, "Relay station placement in IEEE 802.16j dual-relay MMR networks," in *Proc. 2008 IEEE Int. Conf. on Communications*.
[31] 3GPP TR 36. 814 Technical Specification Group Radio Access Network, "Further advancements for E-UTRA, physical layer aspects," Tech. Rep.
[32] E. Visotsky, J. Bae, R. Peterson, R. Berryl, and M. L. Honig, "On the uplink capacity of an 802.16j system," in *Proc. 2008 IEEE Wireless Communications and Networking Conf.*
[33] V. Genc, S. Murphy, Y. Yu, and J. Murphy, "IEEE 802.16j relay-based wireless access networks: an overview," *IEEE Wireless Commun.*, vol. 15, no. 5, pp. 56–63, Oct. 2008.
[34] J. Camp and E. Knightly, "The IEEE 802.11s extended service set mesh networking standard," *IEEE Commun. Mag.*, vol. 46, Aug. 2008.
[35] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.
[36] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE. Trans. Inf. Theory*, vol. 55, no. 4, pp. 1575–1590, Apr. 2009.
[37] M. O. Jackson, "A survey of models of network formation: stability and efficiency," Working Paper 1161, California Institute of Technology, Division of the Humanities and Social Sciences, Nov. 2003.
[38] X. He and A. Yener, "Providing secrecy when the eavesdropper channel is arbitrarily varying: a case for multiple antennas," in *Proc. 48th Annual Allerton Conf. Commun. Control Comput.*, 2010, pp. 1228–1235.
[39] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks," submitted. Available: http://arxiv.org/abs/1001.3697.
[40] G. Demange and M. Wooders, *Group Formation in Economics: Networks, Clubs and Coalitions*. Cambridge University Press, 2005.
[41] J. Derks, J. Kuipers, M. Tennekes, and F. Thuijsman, "Local dynamics in network formation," in *Proc. 2008 Third World Congress of the Game Theory Society*.
[42] M. O. Jackson, *Social and Economic Networks*. Princeton University Press, 2010.
[43] R. Xian, J. Neville, and M. Rogati, "Modeling relationship strength in online social networks," in *Proc. 2010 ACM Int. Conference on World Wide Web*.
[44] C. S. R. Murthy and B. Manoj, *Ad Hoc Wireless Networks: Architectures and Protocols*. Prentice Hall, 2004.
[45] S. Vasudevan, D. Towsley, D. Goeckel, and R. Khalili, "Neighbor discovery in wireless networks and the coupon collector's problem," in *Proc. 2009 ACM Int. Conf. on Mobile Computing and Networking*.
[46] N. Mittal, Y. Zeng, and S. Venkatesan, "Neighbor discovery in wireless networks and the coupon collector's problem," in *Proc. 2011 ACM Int. Conf. on Distributed Computing Systems*.
[47] W. Saad, A. Hjørungnes, Z. Han, and T. Başar, "Network formation games for wireless multi-hop networks in the presence of eavesdroppers," in *Proc. 2009 International Workshop on Computational Advances in Multi-Sensor Adaptive Processing*.
[48] G. Gigerenzer and R. Selten, *Bounded Rationality: The Adaptive Toolbox*. Cambridge University Press, 2002.

Walid Saad (S'07, M'10) received his B.E. from the Lebanese University in 2004, his M.E. in Computer and Communications Engineering from the American University of Beirut in 2007, and his Ph.D. degree from the University of Oslo in 2010. From August 2008 till July 2009 he was a visiting scholar in the Coordinated Science Laboratory at the University of Illinois at Urbana Champaign. From January 2011 till July 2011, he was a Postdoctoral Research Associate at the Electrical Engineering Department at Princeton University.

Currently, he is an Assistant Professor at the Electrical and Computer Engineering Department at the University of Miami. His research interests span the areas of game theory, wireless networks, small cell networks, security, and smart grids. He is a co-author of a book on game theory in wireless and communication networks, published by Cambridge University Press in October 2011. He was the first author of the papers that received the Best Paper Award at the 7th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), in June 2009 and at the 5th International Conference on Internet Monitoring and Protection (ICIMP) in May 2010. He is a co-author of the paper that won the best paper award at the IEEE Wireless Communications and Networking Conference (WCNC) in 2012.



Xiangyun Zhou (S'08, M'11) is a lecturer at the Australian National University (ANU), Australia. He received the B.E. (hons.) degree in electronics and telecommunications engineering and the Ph.D. degree in telecommunications engineering from the ANU in 2007 and 2010, respectively. From June 2010 to June 2011, he worked as a postdoctoral fellow at UNIK - University Graduate Center, University of Oslo, Norway. His research interests are in the fields of communication theory, wireless communications and wireless networking. Dr. Zhou serves on the editorial board of *Security and Communication Networks Journal* (Wiley) and *Ad Hoc & Sensor Wireless Networks Journal*. He has also served as the TPC member of major IEEE conferences. He is a recipient of the Best Paper Award at the 2011 IEEE International Conference on Communications.

Behrouz Maham (S'07, M'10) received the B.Sc. and M.Sc in electrical engineering, from University of Tehran, in 2005 and 2007, respectively, and his PhD from the University of Oslo, Norway, in April 2010. He worked as a system engineer from 2006 till 2007 at Iran Telecommunication Research Center. From September 2008 to August 2009 he was with the Dept. of Electrical Engineering at Stanford University, USA. Currently, he is an Assistant Professor in the School of Electrical and Computer Engineering at the University of Tehran. He has held visiting appointments at Aalto University (formerly Helsinki University of Technology) and University of Oulu, Finland, and the Alcatel-Lucent Chair at SUPLEC in France. His fields of interest span the broad area of scalable wireless communication and networking, with emphasis on relay techniques, multiuser techniques, cognitive radio, interference alignment, and optimization theory. He has over 50 publications in major technical journals and conferences. Since April 2011, he has been serving as an Editor for Transactions on Emerging Telecommunications Technologies (formerly European Transactions on Telecommunications). He served as a technical program chair and technical program committee member of several major IEEE conferences.

Tamer Başar ((S'71-M'73-SM'79-F'83) is with the University of Illinois at Urbana-Champaign (UIUC), where he holds the positions of Swanlund Endowed Chair; Center for Advanced Study Professor of Electrical and Computer Engineering; Professor, Coordinated Science Laboratory; and Professor, Information Trust Institute. He received the B.S.E.E. degree from Robert College, Istanbul, and the M.S., M.Phil, and Ph.D. degrees from Yale University. He joined UIUC in 1981 after holding positions at Harvard University and Marmara Research Institute (Turkey). He is a member of the US National Academy of Engineering, Fellow of IEEE, Fellow of IFAC, Fellow of SIAM, a past president of Control Systems Society (CSS), the founding president of the International Society of Dynamic Games (ISDG), and past president of American Automatic Control Council (AACC). He has received several awards and recognitions over the years, including the highest awards of IEEE CSS, IFAC, AACC, and ISDG, and a number of international honorary doctorates and professorships. Dr. Başar has close to 600 publications in systems, control, communications, and dynamic games, including books on non-cooperative dynamic game theory, robust control, network security, and wireless and communication networks. He is the Editor-in-Chief of *Automatica* and editor of several book series. His current research interests include stochastic teams and games; routing, pricing, and congestion control in communication networks; control over wired and wireless networks; sensor networks; formation in adversarial environments; mobile and distributed computing; risk-sensitive estimation and control; mean-field game theory; game-theoretic approaches to security in computer networks, including intrusion detection and response; and cyber-physical systems.

H. Vincent Poor (S'72, M'77, SM'82, F'87) received the Ph.D. degree in EECS from Princeton University in 1977. From 1977 until 1990, he was on the faculty of the University of Illinois at Urbana-Champaign. Since 1990 he has been on the faculty at Princeton, where he is the Michael Henry Strater University Professor of Electrical Engineering and Dean of the School of Engineering and Applied Science. Dr. Poor's research interests are in the areas of stochastic analysis, statistical signal processing and information theory, and their applications in wireless networks and related fields including social networks and smart grid. Among his publications in these areas are the recent books *Classical, Semi-classical and Quantum Noise* (Springer, 2012) and *Smart Grid Communications and Networking* (Cambridge University Press, 2012).

Dr. Poor is a member of the National Academy of Engineering and the National Academy of Sciences, a Fellow of the American Academy of Arts and Sciences, and an International Fellow of the Royal Academy of Engineering (U. K). He is also a Fellow of the Institute of Mathematical Statistics, the Optical Society of America, and other organizations. In 1990, he served as President of the IEEE Information Theory Society, and in 2004-07 he served as the Editor-in-Chief of the IEEE TRANSACTIONS ON INFORMATION THEORY. He received a Guggenheim Fellowship in 2002, the IEEE Education Medal in 2005, and the Marconi and Armstrong Awards of the IEEE Communications Society in 2007 and 2009, respectively. Recent recognition of his work includes the 2010 IET Ambrose Fleming Medal for Achievement in Communications, the 2011 IEEE Eric E. Sumner Award, and honorary doctorates from Aalborg University, the Hong Kong University of Science and Technology, and the University of Edinburgh.