

MOBI-CLIQUEES FOR IMPROVING ERGODIC SECRECY IN FADING WIRETAP CHANNELS UNDER POWER CONSTRAINTS

Dionysios S. Kalogerias and Athina P. Petropulu

Department of Electrical & Computer Engineering
Rutgers, The State University of New Jersey, Piscataway, NJ 08854, USA

ABSTRACT

We consider a cooperative secret communication scenario, in which a group of mobile and power constrained nodes, acting as relays, cooperatively transmit to a destination in the presence of an eavesdropper; both destination and eavesdropper are assumed stationary. The cooperative scheme entails motion control and optimal communication, in order to achieve a prescribed level of ergodic secrecy rate. The group of motion-controlled cooperating relays is here termed as *mobi-clique*. Under this setting, a novel, decentralized motion control scheme is derived, which effectively drives the relays to a formation configuration, so that a prescribed expected secrecy requirement is met, while at the same time the utilization of network resources is maximized. The effectiveness of the proposed approach is verified both theoretically and through numerical simulations.

Index Terms— Secrecy Rate, Secrecy Capacity, Physical Layer Security, Network Mobility Control, Cooperative Networks

1. INTRODUCTION

As the use of wireless devices is becoming ubiquitous, maintaining secrecy of wireless transactions has been drawing a lot of attention. Physical layer secrecy has emerged as an alternative to cryptography, targeting the degradation of the information that leaks to eavesdroppers by exploiting the characteristics of the wireless channel. Physical layer secrecy was first introduced and studied in the context of a single user memoryless wiretap channel [1], and later in the broadcast [2] and the scalar Gaussian wiretap channels [3]. For single-antenna source, destination and eavesdropper (single-input single-output (SISO) channel), when an eavesdropper's channel is a degraded version of the legitimate channel, the source and the destination can achieve a positive secrecy rate. With the use of multiple antennas positive secrecy rate can be ensured even when the SISO methods fail [4, 5]. For scenarios in which a multi-antenna source has access to only statistical channel state information (CSI), the ergodic secrecy rate of Gaussian multiple-input single-output (MISO) channels was studied in [6] and relevant ergodic capacity were presented more recently in [7].

It is well known that mobility improves the capacity of multiuser ad hoc wireless networks with random relay-assisted source-destination pairs [8]. Recently, mobility control has been combined with optimal transmit beamforming in order to minimize the transmit power while maintaining Quality of Service (QoS) in multiuser cooperative networks [9]. In the context of network security, distributed network mobility has been employed in [10, 11] for achieving specific operational network goals, such as the adaptation of

network topologies to jamming attacks. In the more specialized context of information theoretic secrecy, decentralized mobility control has been recently jointly combined with noise nulling and cooperative jamming for secrecy rate maximization in mobile, jammer assisted cooperative communication networks with one source, one destination and multiple jammers [12].

In this paper, we consider a cooperative communication scenario, in which a user enlists multiple network nodes (relays) to help deliver the information to the destination in the presence of a passive eavesdropper; the node first distributes the signal to neighboring relays and, subsequently, the relays cooperate to transmit the signal in a beamforming fashion. The relays have the ability to move, forming a *mobi-clique*, which is defined as a set of cooperative, motion-controlled nodes in the network, whereas the destination and eavesdropper are assumed stationary. The relays have strict power constraints, and have only statistical information on the channel. The goal of the relays is to cooperate jointly in the space of communications and motion controls, in order to achieve a prescribed level of ergodic secrecy. Our contribution is summarized in deriving a novel, formation preserving, decentralized motion control scheme, effectively driving the relays to a formation configuration, so that a prescribed expected secrecy requirement is met, while at the same time the utilization of network resources are maximized. The proposed scheme fully exploits the transmission capabilities of all relays in the network, and distributes the total power consumption to multiple nodes, thus extending the lifetime of the network.

2. SYSTEM MODEL & PROBLEM FORMULATION

In the following, we will study the problem after the point at which the information to be transmitted has been distributed to the *mobi-clique*. Suppose there are N single antenna mobile cooperating nodes (Alices) on the plane, with antenna locations denoted as $\mathbf{p}_{Ai} \in \mathbb{R}^2, i \in \mathbb{N}_N^+ \equiv \{1, 2, \dots, N\}$, ultimately intending to cooperatively transmit confidential information to the destination (Bob), in the presence of an eavesdropper (Eve). Bob and Eve are assumed to be stationary and are located at $\mathbf{p}_i \in \mathbb{R}^2, i \in \{B, E\}$.

During a transmission, Alice i transmits the signal $\sqrt{P_s} w_i x$, where $P_s \in \mathbb{R}_+$ denotes the *sum* transmission power budget for all Alices, $x \in \mathbb{C}$ denotes the symbol to be transmitted, modeled as an arbitrary zero mean complex random variable with $\mathbb{E}\{|x|^2\} \equiv 1$ and $w_i, i \in \mathbb{N}_N^+$ denote complex, power and phase adjusting weights, chosen such that $\sum_{i \in \mathbb{N}_N^+} |w_i|^2 \triangleq \|\mathbf{w}\|_2^2 \equiv 1$.

Under this setting, the received signals at Bob and Eve can be expressed as $y_j \triangleq \sqrt{P_s} (\mathbf{h}_j^H) \mathbf{w} x + n_j \in \mathbb{C}, j \in \{B, E\}$, where $\mathbf{h}_j^H \triangleq \left[\left\{ h_j^i(\mathbf{p}_{Ai}) \right\}_{i \in \mathbb{N}_N^+} \right]^T$, with $(h_j^i(\mathbf{p}_{Ai}))^* \in \mathbb{C}, i \in \mathbb{N}_N^+$ de-

This work is supported by the National Science Foundation (NSF) under Grant CNS-1239188

noting the position dependent time quasistatic (for one symbol period) communication channel gains from the respective Alice to Bob and Eve, respectively; $\mathbf{p} \triangleq \left[\left\{ \mathbf{p}_{Ai}^T \right\}_{i \in \mathbb{N}_N^+} \right]^T \in \mathbb{R}^{2N \times 1}$; and $n_B \in \mathbb{C}$ and $n_E \in \mathbb{C}$ constitute complex AWGN quantities at the respective reception points, with variances $\mathbb{E} \left\{ |n_B|^2 \right\} \equiv \mathbb{E} \left\{ |n_E|^2 \right\} \triangleq N_0$. The secrecy rate of the system is given by

$$R_{MW}^{\mathbf{p}, \mathbf{w}} \triangleq \left(\log \left(\frac{1 + \rho \mathbf{w}^H \mathbf{R}_B^{\mathbf{p}} \mathbf{w}}{1 + \rho \mathbf{w}^H \mathbf{R}_E^{\mathbf{p}} \mathbf{w}} \right) \right)^+ \quad (1)$$

where $\rho \triangleq P_s/N_0$ denotes the SNR and $\mathbf{R}_B^{\mathbf{p}} \triangleq \mathbf{h}_B^{\mathbf{p}} (\mathbf{h}_B^{\mathbf{p}})^H \in \mathbb{C}^{N \times N}$ and $\mathbf{R}_E^{\mathbf{p}} \triangleq \mathbf{h}_E^{\mathbf{p}} (\mathbf{h}_E^{\mathbf{p}})^H \in \mathbb{C}^{N \times N}$ are rank-1 matrices.

Under these assumptions and using Jensen's inequality, the jointly position and beamforming weight dependent *expected* secrecy rate of the system is lower bounded by the quantity

$$ER_{MW}^{\mathbf{p}, \mathbf{w}} \triangleq \left(\mathbb{E} \left\{ \log \left(\frac{1 + \rho \mathbf{w}^H \mathbf{R}_B^{\mathbf{p}} \mathbf{w}}{1 + \rho \mathbf{w}^H \mathbf{R}_E^{\mathbf{p}} \mathbf{w}} \right) \right\} \right)^+ \quad (2)$$

since the operator $(\cdot)^+ : \mathbb{R} \rightarrow \mathbb{R}^+$ is convex. Therefore, we can leverage this lower bound to define an ergodic secrecy rate as in (2) and use this as our objective stochastic secrecy cost functional. We are now in position to state our problem of interest as follows.

Problem. Given a prescribed level of expected secrecy $c > 0$, jointly adjust the beamforming vector \mathbf{w} and control each Alice in space, such that, at the goal positions $\mathbf{p}_{Ai}^{goal}, i \in \mathbb{N}_N^+$ paired with the respectively determined \mathbf{w}^o , the ergodic secrecy rate of the system will be lower bounded as $ER_{MW}^{\mathbf{p}_{Ai}^{goal}, \mathbf{w}^o} \geq c$.

The wireless channels are assumed to be flat fading. Assuming a rich scattering, obstacle free environment [9], the baseband equivalent channel gain between a mobile node at position \mathbf{p}_i and a stationary receiver at position \mathbf{p}_j can be modeled as $c_j(\mathbf{p}_i, t) \triangleq \alpha(t) \beta_j(\mathbf{p}_i) \exp(\mathfrak{I} \cdot 2\pi d_{ij}/\lambda)$, where $\mathfrak{I} \triangleq \sqrt{-1}$; t denotes time (transmission cycle); λ denotes the carrier wavelength; $\beta_j(\mathbf{p}_i) \triangleq \|\mathbf{p}_i - \mathbf{p}_j\|_2^{-\mu/2}$; $\mu > 0$ denotes the path loss exponent; $d_{ij} \triangleq \|\mathbf{p}_i - \mathbf{p}_j\|_2$; and $\alpha(t) \sim \mathcal{CN}(0, \sigma_R^2/2), \forall t > 0$.

3. SISOSE CAPACITY ACHIEVING OPTIMAL POWER ALLOCATION

Invoking results presented in [6], the ergodic secrecy rate $ER_{MW}^{\mathbf{p}, \mathbf{w}}$, as defined in Section 2, equals

$$ER_{MW}^{\mathbf{p}, \mathbf{w}} = \left(F_1 \left(\rho \mathbf{w}^H \mathbf{\Sigma}_B^{\mathbf{p}} \mathbf{w} \right) - F_1 \left(\rho \mathbf{w}^H \mathbf{\Sigma}_E^{\mathbf{p}} \mathbf{w} \right) \right)^+, \quad (3)$$

where $F_1(x) \triangleq e^{1/x} E_1(1/x)$ is an increasing function, with $E_1 : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ denoting the exponential integral, and $\mathbf{\Sigma}_j^{\mathbf{p}} \triangleq \text{diag} \left(\left\{ \sigma_R^2 \beta_j^2(\mathbf{p}_{Ai}) \right\}_{i \in \mathbb{N}_N^+} \right), j \in \{B, E\}$ are the covariance matrices of $\mathbf{h}_B^{\mathbf{p}}$ and $\mathbf{h}_E^{\mathbf{p}}$, respectively.

For any fixed positions of the Alices on the plane, let us consider the program

$$\text{maximize}_{\mathbf{w}} ER_{MW}^{\mathbf{p}, \mathbf{w}} \quad \text{subject to} \quad \|\mathbf{w}\|_2^2 \equiv 1. \quad (4)$$

Then, using, for instance, the KKT conditions, one can easily prove the following lemma, characterizing the optimal solution to (4).

Lemma 1. For fixed positions of the nodes, the optimal power allocation policy maximizing the ergodic secrecy rate of the system amounts to assigning all the available power to Alice $i^o \in \mathbb{N}_N^+$, such that $i^o \in \arg \max_{i \in \mathbb{N}_N^+} F_1 \left(\rho \sigma_R^2 \beta_B^2(\mathbf{p}_{Ai}) \right) - F_1 \left(\rho \sigma_R^2 \beta_E^2(\mathbf{p}_{Ai}) \right)$.

Consequently, we readily see that, in general, cooperation among *stationary* Alices does not offer any benefit in terms of secrecy rate maximization, of course under the important assumption that all Alices are able to transmit at maximum power P_s (in fact, under the assumption of power constrained Alices, Lemma 1 constitutes a hypothetical ‘‘upper bound’’ solution to (4)). Leveraging Lemma 1, the maximum achievable ergodic secrecy rate of the system is given by

$$ER_{MW}^{\mathbf{p}, \mathbf{w}^o} = \left(\mathbb{E} \left\{ \log \left(\frac{1 + \rho |h_B^{i^o}(\mathbf{p}_{Ai^o})|^2}{1 + \rho |h_E^{i^o}(\mathbf{p}_{Ai^o})|^2} \right) \right\} \right)^+ \triangleq EC_{W^{Ai^o}}^{\mathbf{p}, \mathbf{w}^o}. \quad (5)$$

Of course, $ER_{MW}^{\mathbf{p}, \mathbf{w}^o} > 0$ if and only if $|h_B^{i^o}(\mathbf{p}_{Ai^o})| > |h_E^{i^o}(\mathbf{p}_{Ai^o})|$. In fact, using the results presented in [7], one can readily show that the above ergodic rate actually coincides with the ergodic secrecy capacity of the SISOSE (Single-Input-Single-Output-Single-Eavesdropper) wiretap channel and that the following holds.

Theorem 1. For fixed positions of the nodes of the network, optimal power allocation achieves the ergodic secrecy capacity of the equivalent fading SISOSE wiretap channel model.

However, as we show in the next section, by allowing the Alices to move, the ergodic secrecy capacity can be both *at least nearly* achieved and improved using cooperative transmission, fully exploiting the power resources of the network.

4. IMPROVING SECRECY VIA MOTION CONTROL

We assume that the area spanned by each network node i constitutes a disc¹ of radius $r_i \in \mathbb{R}_{++}$ and center (antenna) located at \mathbf{p}_i , where $i \in \left\{ \{Aj\}_{j \in \mathbb{N}_N^+}, B, E \right\}$. We also assume that $r_{k \in \{B, E\}} \gg r_{AN} \equiv r_{Aj} \triangleq r_A, \forall j \in \mathbb{N}_{N-1}^+$. Concerning kinematics, each Alice i reacts to the continuous time control input $\mathbf{u}_i(t) \in \mathbb{R}^2$ and its motion evolves according to the first order differential equation

$$\dot{\mathbf{p}}_i(t) = \mathbf{u}_i(t). \quad (6)$$

Under this setting, our goal will be to determine the motion controller(s) \mathbf{u}_i , that will ensure steering the respective Alice to a position that satisfies the respective secrecy constraint of interest.

4.1. Noncooperative Case

The main conclusion of Section 3 is that if the best (in the sense of Lemma 1) Alice is assigned all the available transmission power, optimal pseudo-beamforming is (SISOSE) capacity achieving. However, if we allow the Alices to move, then, the particular choice of an Alice is completely irrelevant. In fact, if motion is not considered expensive, we should just pick an Alice (say Alice i^o , without risk of confusion) and then steer her to a position such that the secrecy

¹Of course, these discs could also define reachability constraints for a network node. The interpretation depends clearly on the desirable context.

capacity is lower bounded by our prescribed secrecy level c , as long as c is feasible.

From (5) and recalling that $F_1(x)$ is an increasing function, it can be easily verified that the capacity of the system is positive when Alice i° is closer to Bob than to Eve and that it increases as Alice i° moves closer to Bob. In fact, it is true that as $\mathbf{p}_{Ai^\circ} \rightarrow \mathbf{p}_B$, $EC_W^{\mathbf{p}_{Ai^\circ}} \rightarrow \infty$.

However, the geometries of Alice i° , Bob and Eve place a natural upper bound on the achievable improvement on the secrecy capacity. First, observe that we can simplify the assumed geometric models by equivalently considering Alice i° as a single point in \mathbb{R}^2 and Bob and Eve as discs with augmented radii $\tilde{r}_{k \in \{B, E\}} \triangleq r_{k \in \{B, E\}} + r_A$, respectively. Then, the maximum possible value of the secrecy capacity will correspond to a point on the boundary of Bob's disc. This point is necessarily the one that lies on the line connecting $\mathbf{p}_B \triangleq [x_B \ y_B]^T$ and $\mathbf{p}_E \triangleq [x_E \ y_E]^T$ and at the same time is the most distant from \mathbf{p}_E . We will call such a point an *exceptional* one and denote it as $\mathbf{p}_{ex} \triangleq [x_{ex} \ y_{ex}]^T$. If the equation $y = ax + b$ describes the aforementioned line, where a and b can be trivially determined, then, using elementary geometry, it can be easily shown that

$$x_{ex} = x_B + \text{sign}(x_B - x_E) \frac{\tilde{r}_B}{\sqrt{1 + a^2}}. \quad (7)$$

For simplicity, we do not consider collision avoidance among the Alices. Then, similarly to [12], it suffices to define a quadratic artificial potential $\phi_B^{att} : \mathbb{R}^2 \rightarrow \mathbb{R}_+$, attractive to the exceptional point \mathbf{p}_{ex} , as $\phi_{ex}^{att}(\mathbf{p}_{Ai^\circ}) \triangleq \|\mathbf{p}_{Ai^\circ} - \mathbf{p}_{ex}\|_2^2$, and two repulsive (collision) potentials $\phi_j^{rep} : \mathbb{R}^2 \rightarrow \mathbb{R}_+, j \in \{B, E\}$ as $\phi_j^{rep}(\mathbf{p}_{Ai^\circ}) \triangleq 1/(\gamma_j^\nu(\mathbf{p}_{Ai^\circ}) - 1, \nu > 0$ [13], where

$$\gamma_j(\mathbf{p}_{Ai^\circ}) \triangleq \left(1 - \xi \frac{\left(\|\mathbf{p}_{Ai^\circ} - \mathbf{p}_j\|_2^2 - \tilde{r}_j^2 \right)^2}{1 + \left(\|\mathbf{p}_{Ai^\circ} - \mathbf{p}_j\|_2^2 - \tilde{r}_j^2 \right)^2} \right)^\zeta, \quad (8)$$

with $\xi \triangleq (1 + \tilde{r}_j^4)/\tilde{r}_j^4$ and $\zeta \triangleq \frac{1}{2}(1 - \text{sign}(\|\mathbf{p}_{Ai^\circ} - \mathbf{p}_j\|_2 - \tilde{r}_j))$.

Then, defining the potential sum $\phi(\mathbf{p}_{Ai^\circ}) \triangleq \phi_{ex}^{att}(\mathbf{p}_{Ai^\circ}) + \phi_B^{rep}(\mathbf{p}_{Ai^\circ}) + \phi_E^{rep}(\mathbf{p}_{Ai^\circ})$, the desired motion controller for Alice i° is readily obtained as $\mathbf{u}_{Ai^\circ}(t) \triangleq -A \nabla_{\mathbf{p}_{Ai^\circ}} \phi(\mathbf{p}_{Ai^\circ}(t))$, where $A \in \mathbb{R}_{++}$ constitutes a user defined acceleration scaling factor, leading to the closed loop system

$$\dot{\mathbf{p}}_{Ai^\circ}(t) = -A \nabla_{\mathbf{p}_{Ai^\circ}} \phi(\mathbf{p}_{Ai^\circ}(t)). \quad (9)$$

During her movement, Alice continuously evaluates the ergodic capacity $EC_W^{\mathbf{p}_{Ai^\circ}(t)}$ for its given position on the plane and when $EC_W^{\mathbf{p}_{Ai^\circ}(t^*)} \geq c$ for some $\mathbf{p}_{Ai^\circ}(t^*)$ (of course c should be feasible), then she stops moving and starts communicating with Bob.

4.2. Nearly Capacity Achieving Cooperative Transmission

Assume that there is a "leader" Alice (say Alice i°) in the network. Then, while she moves towards the exceptional point according to the motion control scheme described in the previous subsection, the remaining Alices track their leader and adaptively form a tight, well defined formation around her. In such a case, all Alices will be eventually colocated. Therefore, if r_A is sufficiently small², they will

all be approximately equidistant from Bob and Eve. Consequently, from (3), it will be true that

$$ER_{MW}^{\mathbf{p}, \mathbf{w}} \cong \left(F_1 \left(\rho \sigma_R^2 \beta_B^2(\mathbf{p}_{Ai^\circ}) \right) - F_1 \left(\rho \sigma_R^2 \beta_E^2(\mathbf{p}_{Ai^\circ}) \right) \right)^+,$$

that is, beamforming is nearly capacity achieving for *any* admissible choice of the beamforming vector \mathbf{w} . This means that if each Alice transmits with an individual power budget, where all budgets sum to P_s , all Alices should transmit at maximum power. Obviously, if all Alices are identical, then the optimal power allocation policy must be the uniform one.

Based on the previous subsection, the "tracking the leader" control scheme can be derived as follows. First, without loss of generality, assume that Alice 1 is the leader, with motion dynamics defined by (9). Then, for each Alice $i \geq 2$, it suffices to define a mixed, time varying potential, consisting of two components, a static one and a dynamic one, as $\phi_i^{fol}(\mathbf{p}_{Ai}, t) \triangleq \phi_i^{st}(\mathbf{p}_{Ai}, t) + \phi_i^{dyn}(\mathbf{p}_{Ai}, t), \forall i \in \mathbb{N}_N^2 \equiv \{2, \dots, N\}$. The static potential prevents collisions between the respective Alice and Bob and Eve, respectively, and is defined as $\phi_i^{st}(\mathbf{p}_{Ai}) \triangleq \phi_B^{rep}(\mathbf{p}_{Ai}) + \phi_E^{rep}(\mathbf{p}_{Ai})$. The dynamic potential steers the respective Alice towards her "reserved" position in the formation, which should be a function of the time evolving position of her leader, denoted as $\mathbf{p}_{Ai(A1)}$, while avoiding collisions with her as well as the rest of the Alices, whose positions are also time evolving, and can be defined as $\phi_i^{dyn}(\mathbf{p}_{Ai}, t) \triangleq \phi_{Ai(A1)}^{att}(\mathbf{p}_{Ai}, t) + \phi_{A1}^{rep}(\mathbf{p}_{Ai}, t) + \sum_{j=2}^{i-1} \phi_{Aj}^{rep}(\mathbf{p}_{Ai}, t), \forall i \in \mathbb{N}_N^2$, where $\phi_{Ak}^{rep}(\mathbf{p}_{Ai}, t)$ is defined as in (8), but replacing \mathbf{p}_j and \tilde{r}_j with \mathbf{p}_{Ak} (which is time evolving) and $2r_A$, respectively. The desired motion controllers for the following Alices are thus obtained as $\mathbf{u}_{Ai}(t) \triangleq -\nabla_{\mathbf{p}_{Ai}} \phi_i^{fol}(\mathbf{p}_{Ai}(t), t), i \in \mathbb{N}_N^2$, leading to the set of closed loop time varying systems

$$\dot{\mathbf{p}}_{Ai}(t) = -\nabla_{\mathbf{p}_{Ai}} \phi_i^{fol}(\mathbf{p}_{Ai}(t), t), \quad i \in \mathbb{N}_N^2. \quad (10)$$

Assuming that global node positioning is available for all Alices, the proposed formation preserving control scheme can be considered decentralized.

During motion evolution, the leader Alice continuously evaluates the ergodic rate $ER_{MW}^{\mathbf{p}(t), \mathbf{w}}$ and when $ER_{MW}^{\mathbf{p}^*(t^*), \mathbf{w}} \geq c$ for some $\mathbf{p}^*(t^*)$, then all Alices stop and start communicating with Bob at full power. If the Alices' formation has indeed been created before reaching c (this is also related to the acceleration factor A), then, for sufficiently small r_A , $ER_{MW}^{\mathbf{p}^*(t^*), \mathbf{w}}$ will be nearly equal to $EC_W^{\mathbf{p}_{Ai^\circ}(t^*)}$ (see previous subsection) and, in this case we have a great improvement in the (SISOSE equivalent) secrecy capacity of the system. If c is reached earlier, that is, before the Alices' formation has been created, then an improvement in the rate $ER_{MW}^{\mathbf{p}(t), \mathbf{w}}$ can only be assured. However, in any case, c is reached through cooperation, effectively exploiting the transmission power capabilities of the network and improving secret communication, which is the main objective in this paper.

The situation we are dealing with here is directly equivalent to the MISOSE (Multiple-Input-Single-Output-Single-Eavesdropper) wiretap channel model with orthogonal channels, as studied in [6, 7]. Since our scheme is ultimately SISOSE capacity achieving, the same will happen with the MISOSE model too. The following is also true, as an interesting side result of our investigation.

Theorem 2. *The ergodic secrecy capacity of the fading MISOSE wiretap channel with orthogonal channels coincides with that of the fading SISOSE wiretap channel.*

² But at the same time sufficiently large, such that there are (approximately) no correlations among the channels from the Alices to Bob and Eve, respectively.

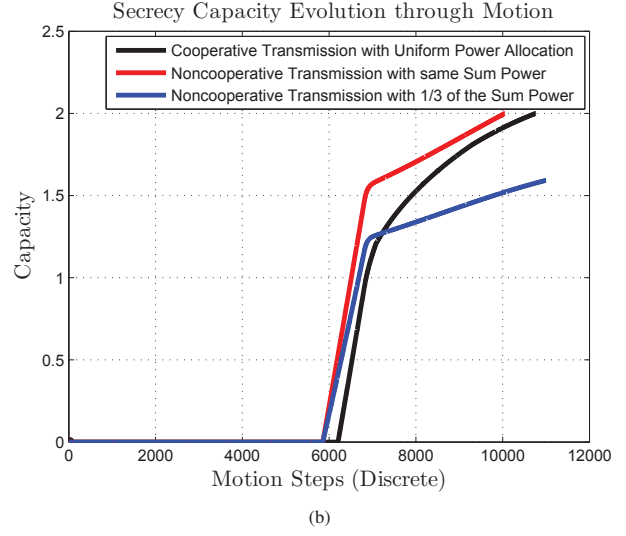
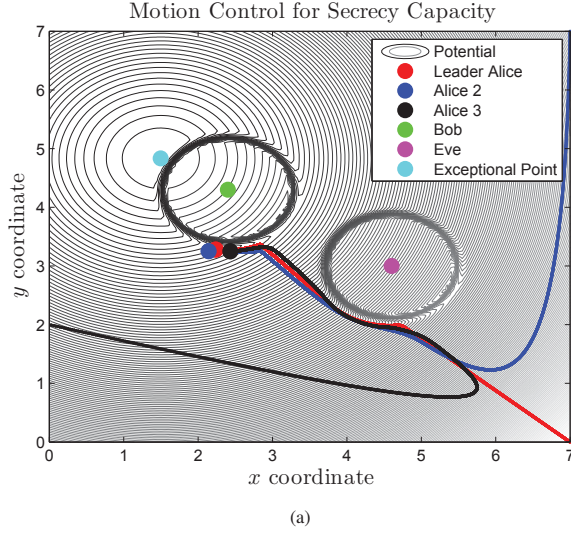


Fig. 1: Improving the Secrecy Rates via Motion Control.

Theorem 2 can be justified by analytically computing the capacity expression of Theorem 2 in [7], using results presented in [6]. Also, it is obvious that the motion control scheme proposed in Subsection 4.1 can be directly applied to MISOSE model, almost as is.

5. NUMERICAL SIMULATIONS

In this section, we confirm the proposed cooperative secrecy improving control scheme, presented in Section 4, through non trivial numerical simulations.

We consider a wireless network consisting of 3 *identical* mobile transmitters (Alices), a legitimate destination (Bob) and an eavesdropper (Eve), both assumed stationary. All network nodes are on a (7×7) (all distances are measured in meters) rectangular plane. Bob and Eve both occupy circular areas on the plane with common radius $r_B \equiv r_E \equiv 1$, with antennas located at $(2.4, 4.3)$ and $(4.6, 3)$, respectively and the common radius of all Alices is set as $r_A \equiv 0.05$, with initial positions of Alice 1,2 and 3 being $(7, 0)$, $(7, 7)$ and $(0, 2)$, respectively. We assume that Alice 1 is the leader of the transmitting nodes in the network and that $A \equiv 0.1$. The target formation among the Alices is defined by eventually steering the antennas of Alices 2 and 3 to the (time evolving) points $\mathbf{p}_{A1} + [-2r_A \ 0]^T$ and $\mathbf{p}_{A1} + [+2r_A \ 0]^T$, respectively. Regarding communication related parameters, we choose $\sigma_R^2 \equiv 1$, $\mu \equiv 3.5$ and $\lambda \equiv 2r_A/2 \equiv 0.05 \text{ m}$ (that is a carrier frequency of 6 GHz), in order to safely ensure communication channel approximate uncorrelatedness. The SNR with respect to the sum power budget of the network P_s is fixed at $\sim 14.8 \text{ dB}$ and the target secrecy rate c is set to 2 nats/s/Hz . Since the 3 Alices are identical, the maximum transmission power for each one of them equals $P_s/3$ (uniform power allocation).

Fig. 1(a) shows the motion trajectories of the mobi-clique. We observe that the target formation is created quickly and smoothly (while at the same time avoiding collisions). The formation is then driven gradually towards the (unique) exceptional point depicted in cyan in Fig. 1(a), until finally fulfilling the rate requirement c .

Fig. 1(b) shows comparatively the evolution through motion of the achievable rates for three cases of interest, that is, when uniform power allocation is employed (see right above) (black), when the whole available power is hypothetically assigned to Alice 1 (red) and when only Alice 1 is controlled and intends to transmit at its maximum power $P_s/3$ (blue). For the two latter SISOSE scenarios, the respective secrecy rates are actually capacities. We observe that all rates benefit greatly by employing motion control. It is also apparent that, in the cooperative case, the achievable rate approaches the secrecy capacity of the SISOSE equivalent network, validating the effectiveness of the proposed approach, formulated in Subsection 2 of Section 4. Clearly, the gap between the black and red curves of Fig. 1(b) is due to the geometric constraints present among the members of the mobi-clique, directly related to the value of the Alices' radii, r_A .

6. CONCLUSION

In this paper, we have addressed the problem of improving the secrecy rate in multiple source, single-destination, single-eavesdropper networks by exploiting source mobility. We have proposed a novel, decentralized, formation preserving motion control scheme, which ensures the achievability of user defined expected secrecy requirements, while at the same time maximizing the utilization of network resources. Specifically, under the assumption of Rayleigh fading channel modeling, we have shown that motion control can greatly improve the ergodic secrecy in the network and, more importantly, that motion control enables cooperation among the transmitting sources, making it feasible to nearly achieve the highest possible ergodic secrecy rate of the system in a completely systematic way, which might have been impossible without mobility exploitation. The effectiveness of the proposed scheme has also been verified through numerical simulations. Our work draws very promising directions for further research, such as the extension of the results presented here for more complicated and challenging communication scenarios.

7. REFERENCES

- [1] A. D. Wyner, "The wiretap channel," *Bell Systems Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.
- [2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [3] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inform. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
- [4] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inform. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.
- [5] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *IEEE International Conference on Acoustics, Speech and Signal Processing, (ICASSP)*, Apr. 2009, pp. 2437–2440.
- [6] J. Li and A. P. Petropulu, "On ergodic secrecy rate for Gaussian MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1176–1187, Apr. 2011.
- [7] S. C. Lin and P. H. Lin, "On ergodic secrecy capacity of multiple input wiretap channel with statistical CSIT," <http://arxiv.org/pdf/1201.2868.pdf>, 2012.
- [8] M. Grossglauser and D. N. C. Tse, "Mobility increases the capacity of ad hoc wireless networks," *IEEE/ACM Trans. on Networking*, vol. 10, no. 4, August 2002.
- [9] N. Chatzipanagiotis, Y. Liu, A. Petropulu, and M. M. Zavlanos, "Controlling groups of mobile beamformers," in *IEEE Conference on Decision and Control*, Hawaii, 2012.
- [10] K. Ma, Y. Zhang, and W. Trappe, "Mobile network management and robust spatial retreats via network dynamics," in *IEEE International Conference on Mobile Adhoc and Sensor Systems*, 2005.
- [11] K. Ma, Y. Zhang, and W. Trappe, "Managing the mobility of a mobile sensor network using network dynamics," *IEEE Trans. Parallel and Distributed Systems*, vol. 19, pp. 106 – 120, 2008.
- [12] D. S. Kalogerias, N. Chatzipanagiotis, A. P. Petropulu, and M. M. Zavlanos, "Mobile jammers for secrecy rate maximization in cooperative networks," in *38th IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2013)*, Vancouver, Canada, May 2013.
- [13] M. M. Zavlanos and G. J. Pappas, "Potential fields for maintaining connectivity of mobile networks," *IEEE Transactions on Robotics*, vol. 23, no. 4, pp. 812 – 816, 2007.