Secrecy Throughput of MANETs with Malicious Nodes

Yingbin Liang
Department of Electrical Engineering
University of Hawaii at Manoa
Honolulu, HI 96822, USA
Email: yingbinl@hawaii.edu

H. Vincent Poor
Department of Electrical Engineering
Princeton University
Princeton, NJ 08544, USA
Email: poor@princeton.edu

Lei Ying
Department of Electrical
and Computer Engineering
Iowa State University
Ames, IA 50011, USA
Email: leiying@iastate.edu

***Abstract*—The secrecy throughput of mobile ad-hoc networks (MANETs) with malicious nodes is investigated. The MANET consists of n legitimate mobile nodes and m malicious nodes. Transmissions between legitimate nodes are subject to a delay constraint D. An information theoretic approach for security is applied to achieve secure communication among legitimate nodes in MANETs with transmissions being kept perfectly secure from malicious nodes. A critical threshold on the number of malicious nodes (m) is identified such that when $m = o(\sqrt{nD})$, i.e., $\lim_{n\to\infty} m/\sqrt{nD} = 0$, the secrecy throughput equals the throughput of MANETs without malicious nodes, i.e., the impact of the presence of malicious nodes on the network throughput is negligible; and when $m = \Omega\left(\sqrt{nD}\mathbf{poly}(n)\right)$, i.e., $\lim_{n\to\infty} m/\left(\sqrt{nD}\mathbf{poly}(n)\right) \geq c$ for a positive constant c, the secrecy throughput is limited by the number of malicious nodes.**

I. Introduction

MANETs represent one of the most innovative emerging networking technologies, with broad potential applications in personal area networks, emergency and rescue operations, military battlefield applications, etc. The unique features of MANETs, such as mobility and wireless communication, make MANETs a very flexible technology for establishing communication in areas with limited infrastructure. However, protecting MANETs from security attacks is a challenging task because of the dynamic topology of MANETs, strict delay constraints in military and emergency operations, and physical layer uncertainty.

The performance limits of MANETs, in particular, performance bounds on throughput and delay have been extensively studied (e.g., in [1]–[11]). There are two fundamental constraints limiting the performance of MANETs:

- Wireless interference: network capacity is limited because of the interference caused by simultaneous transmissions.
- Mobility: mobile trajectories determine the communication opportunities between two mobiles.

These two fundamental constraints have been bridged together using a virtual channel representation developed in [11]. The key idea is to model the impact of mobility on packet delivery via an erasure channel, in which the erasure probability corresponds to the probability that a packet could not get close enough to its destination before its deadline.

In this paper, we consider MANETs with malicious nodes, which follow the same mobility behavior as legitimate nodes, and hence their reception of packets also has a certain erasure probability. The malicious nodes are assumed to be passive eavesdroppers, which do not send signals over the communication channels. In this paper, we show that the behavior of malicious nodes can be included in the virtual channel representation by introducing an additional eavesdropper, and hence the entire system of MANETs with malicious nodes is modeled by an erasure wire-tap channel studied in [13], [14]. Thus, coding schemes designed for the wire-tap channel can be applied to achieve secure communication in MANETs, and the secrecy capacity of the wire-tap channel provides a way to characterize the fundamental secrecy throughput in MANETs. The goal of this paper is to explore these information theoretic approaches to investigate MANETs.

In this paper, we first provide an upper bound on the secrecy throughput and then show that the upper bound is achievable for two cases. Our results demonstrate that the throughput scales differently with the number of legitimate nodes n and the number of eavesdroppers m for these two regimes, which are separated by a threshold on $m = o(\sqrt{nD})$,[1] where D denotes the delay constraint. In particular, we show that when $m = o(\sqrt{nD})$, the secrecy throughput equals the throughput of MANETs without malicious nodes; and when $m = \Omega\left(\sqrt{nD}\text{poly}(n)\right)$, the secrecy throughput is limited by the number of malicious nodes.

II. MANET Model

We describe the network and communication models in this section. Consider a wireless MANET that consists of n legitimate wireless nodes and m malicious nodes positioned in a unit square. We adopt the two-dimensional independent and identically distributed (i.i.d.) mobility model [3], [11]. As such, each node is uniformly, randomly positioned in the unit

[1]We adopt the following notation in the paper. For non-negative functions $f(x)$ and $g(x)$, $f(x) = O(g(x))$ means there exist positive constants c and a such that $f(x) \leq cg(x)$ for all $x \geq a$; $f(x) = \Omega(g(x))$ means there exist positive constants c and a such that $f(x) \geq cg(x)$ for all $x \geq a$; $f(x) = \Theta(g(x))$ means that both $f(x) = \Omega(g(x))$ and $f(x) = O(g(x))$ hold; $f(x) = o(g(x))$ means that $\lim_{x\to\infty} f(x)/g(x) = 0$; $f(x) = \omega(g(x))$ means that $\lim_{x\to\infty} g(x)/f(x) = 0$; and $f(x) = \text{poly}(x)$ means that $f(x)$ is a polynomial in x.

square, and the node position changes independently across time slots. The positions of different nodes are independent. That the mobility behavior of malicious nodes is the same as the legitimate nodes is justified by the fact that the malicious nodes can be easily detected if they behave differently. We assume that there are n source-destination (S-D) pairs in the network, and each legitimate node is both a source and a destination. Without loss of generality, we assume that the destination of node i is node $i+1$, and the destination of node n is node 1.

We adopt the protocol model [12] in this paper. We assume that all mobiles use a common transmission radius L. Let dist(i,j) denote the Euclidean distance between node i and node j. Node i can successfully transmit to node j if dist$(i,j) \leq L$ and dist$(k,j) \geq (1+\Delta)L$ for each node $k \neq i$ which transmits at the same time, where Δ is a protocol-specified guard-zone to prevent interference. We further assume a fast mobility model [11] where only one-hop transmissions are feasible and each transmission can send W bits, which is independent of n. We assume that the malicious nodes do not transmit in the network, but can receive packets transmitted between legitimate nodes. A malicious node can successfully receive a packet from a transmitter if it is within the transmitter's transmission radius. We consider the worst-case scenario, in which all malicious nodes collaborate to decode messages transmitted in the network by exchanging their received outputs. Hence, the malicious nodes can be viewed as one super-eavesdropper, which receives a packet as long as one of the malicious nodes receives this packet.

Given a delay constraint D, a packet is said to be successfully delivered if the destination obtains the packet within D time slots after it is sent out from the source. Let $\Lambda_i[T]$ denote the number of bits successfully delivered to node i in time interval $[0,T]$. A secrecy throughput λ per S-D pair is said to be *feasible* under the delay constraint D and loss probability constraint $\epsilon > 0$ if there exists n_0 such that for every $n \geq n_0$, there exists a coding/routing/scheduling algorithm such that $\lim_{T\to\infty} \Pr\left(\frac{\Lambda_i[T]}{T} \geq \lambda,\ \forall\, i\right) = 1$ and transmitted information between all S-D pairs is kept perfectly secret from the malicious nodes. The definition of perfect secrecy will be given in Section III.

III. Preliminary on Information Theoretic Security

In this section, we provide the basic background in information theoretic security including the basic channel model, definitions and information theoretic characterization of secrecy capacity, which are useful in our study of MANETs.

The basic model to study information theoretic security is the wire-tap channel introduced and studied by Wyner in [13]. This channel includes a transmitter that wishes to transmit a source signal (a message) W to a legitimate receiver and wishes to keep this message as secret as possible from an eavesdropper. The channel is characterized by a transition probability distribution $P_{YZ|X}$, where X denotes the channel input and Y and Z denotes respective channel outputs at the legitimate receiver and the eavesdropper. The secrecy level of the message W at the eavesdropper, is measured by the *equivocation rate* defined as

$$R_e^{(l)} = \frac{1}{n} H(W|Z^l), \tag{1}$$

where Z^l denotes the outputs at the eavesdropper for l channel users. The equivocation rate indicates the eavesdropper's uncertainty about the message W given the information available to it. Hence the larger the equivocation rate, the higher the level of secrecy.

A rate R is *achievable with perfect secrecy* if there exists a block coding and decoding scheme such that the average error probability converges to zero as the codeword length l goes to infinity and

$$R \leq \liminf_{l\to\infty} R_e^{(l)}. \tag{2}$$

The *secrecy capacity* C_s is the largest rate achievable with perfect secrecy.

The general form of the secrecy capacity for the wire-tap channel is characterized by Csiszár and Körner in [14], and is given by

$$C_s = \max_{P_{UX} P_{YZ|X}} [I(U;Y) - I(U;Z)], \tag{3}$$

where the maximization is taken over all joint distributions P_{UX} between the channel input X and an auxiliary random variable U satisfying the Markov chain condition $U \to X \to (Y,Z)$.

We now consider the binary erasure wire-tap channel, in which the input alphabet is $\{0,1\}$, the channel to the legitimate receiver is a binary erasure channel with erasure probability α (i.e., the input symbol is lost with probability α, and is correctly received with probability $1-\alpha$), and the channel to the eavesdropper is also a binary erasure channel with erasure probability β. The secrecy capacity of the erasure wire-tap channel can be obtained from (3), and is given by

$$C_s^E = [(1-\alpha) - (1-\beta)]^+ = [\beta - \alpha]^+ \tag{4}$$

where $[x]^+$ equals x if $x > 0$ and equals 0 otherwise.

Secure coding design to achieve the secrecy capacity for the binary erasure wire-tap channel with $\alpha = 0$ was first studied by Ozarow and Wyner in [15], where a nested code structure was proposed. Based on this structure, [16] provided an explicit code design to achieve the secrecy capacity for the binary erasure wire-tap channel. In this paper, we will explore the secrecy capacity given in (3) to study the secrecy throughput for MANETs, and we will also propose strategies to apply the secure codes given in [16] to achieve the secrecy throughput.

IV. A Heuristic Argument

In this section, we provide a heuristic argument to demonstrate the main idea of achieving secure communication and analyzing secrecy throughput for MANETs, which provides key intuition for the main results that we present in the

next section. We also demonstrate the interplay of security, throughput and delay in MANETs.

Consider a packet sent out by its source node. With some probability, say probability $1-\alpha$, the packet is delivered to its destination. At the same time, the packet may also be heard by the eavesdroppers with a certain probability, say probability $1-\beta$. Thus, we model each S-D pair as a virtual system (see Figure 1), in which R is the rate at which a source can send out packets. The system then includes two erasure channels, one to the destination with erasure probability α, and the other to a super-eavesdropper with erasure probability β. As we mentioned earlier, the super-eavesdropper sees outputs of all eavesdroppers since all eavesdroppers collaborate. Hence a packet is erased at the super-eavesdropper only when none of the eavesdroppers receive the packet. Clearly the two erasure channels form the erasure wire-tap channel. From Section III, it is clear that the secrecy capacity of the erasure wire-tap channel is the largest communication rate achievable with perfect secrecy, and hence provides the fundamental secrecy throughput for the corresponding MANET.

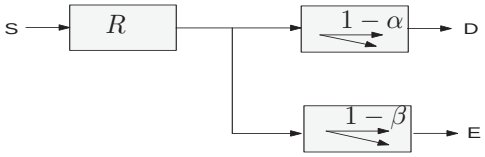

Fig. 1. A virtual channel representation

Next, we heuristically compute the erasure probabilities α and β to obtain the secrecy throughput of the MANET. We classify the packets sent out from a source into two types:

- Type-I packets: packets that are directly sent to their destinations;
- Type-II packets: packets that are sent to their destinations via relay nodes.

A. Secrecy Throughput of Type-I Packets

In this subsection, we consider Type-I packets. We say that a packet is obtained by the super-eavesdropper if the packet is heard by at least one of the malicious nodes. The probability of this event is given by $1-\beta = 1-(1-\pi L^2)^m$. According to the definition of Type-I packet, the source node sends out a Type-I packet only when the corresponding destination is in the communication range of the source node. Hence $1-\alpha = 1$. Furthermore, the probability that an S-D pair is within the communication range is πL^2, which implies that $R = \pi L^2$.

We let $C_{s,\mathrm{I}}$ denote the secrecy throughput of Type-I packets. Based on the secrecy capacity of the erasure wire-tap channel given in (4), we obtain

$$C_{s,\mathrm{I}} = R\left[\beta-\alpha\right]^+ = \max_L \pi L^2(1-\pi L^2)^m = \Theta\left(\frac{1}{m}\right).$$

B. Secrecy Throughput of Type-II Packets

In this subsection, we consider Type-II packets. The delivery of a Type-II packet contains three phases:

(1) The packet is transmitted from the source to one or multiple relays;
(2) The mobile relays physically carry the packet near the destination;
(3) Some mobile relay transmits the packet to the destination.

We consider a super-time-slot consisting of D time slots, and assume that each source sends out X packets over the super-time-slot. We note that each broadcast generates $\pi L^2 n$ relay copies in the network with a high probability. We say a packet is deliverable if it is within distance L from the destination. We have the following observations:

- Assume that there are $\pi L^2 n$ relay copies for each packet. Each copy becomes deliverable at time t with probability πL^2. Thus, the probability that the packet is delivered in one of the D time slots is at most $1-\alpha = 1-\left(1-\pi L^2\right)^{\pi L^2 nD}$.
- Each packet has to be transmitted at least once before delivered, so the erasure probability of the super-eavesdropper is upper bounded $\beta = \left(1-\pi L^2\right)^m$.
- At each time slot, the network can support at most $\frac{1}{\pi L^2}$ simultaneous transmissions. Thus, during one super-time-slot, at most $\frac{D}{\pi L^2}$ packets can be sent out from the sources. Then the rate R for each S-D pair is upper bounded by $R = \frac{1}{\pi L^2 n}$.

Based on the secrecy capacity of the erasure wire-tap channel given in (4), we obtain the following approximate (in fact, upper bound on) secrecy throughput of the Type-II packets:

$$C_{s,\mathrm{II}} = \max_L \frac{1}{\pi n L^2}\left(\left(1-\pi L^2\right)^m - \left(1-\pi L^2\right)^{\pi L^2 nD}\right). \quad (5)$$

To guarantee that $C_{s,\mathrm{II}} > 0$, L must satisfy the following condition:

$$m < \pi L^2 nD. \quad (6)$$

It can be shown that if $m = o\left(\sqrt{nD}\right)$, the secrecy throughput is given by

$$C_{s,\mathrm{II}} = \max_L C(L) = \Theta\left(\sqrt{\frac{D}{n}}\right);$$

otherwise, if $m = \omega\left(\sqrt{nD}\right)$, then the secrecy throughput is given by

$$C_{s,\mathrm{II}} = \max_L C(L) = \Theta\left(\frac{D}{m}e^{-\frac{m^2}{nD}}\right).$$

C. Total Secrecy Throughput

Combining the secrecy throughput for Type-I and Type-II packets, we conclude that if $m = o\left(\sqrt{nD}\right)$, then $C_s = \Theta\left(\sqrt{\frac{D}{n}}\right)$; otherwise, if $m = \Omega\left(\sqrt{nD}\mathrm{poly}(n)\right)$, then $C_s = \Theta\left(\frac{1}{m}\right)$.

In the rest of this paper, we prove that the heuristic results in this section are upper bounds on the secrecy throughput.

Furthermore, we also present algorithms that achieve the upper bounds and hence achieve the optimal secrecy throughput under certain conditions.

V. Main Results: Secrecy Throughput of MANETs

We characterize the secrecy throughput of MANETs in the following theorem.

Theorem 1: If $m = o(\sqrt{nD})$, the feasible secrecy-throughput of MANETs is $O(\min\{\sqrt{D/n}, 1\})$, which is achievable when $D = \omega(\sqrt[3]{n})$; and if $m = \Omega\left(\sqrt{nD}\text{poly}(n)\right)$, the feasible secrecy-throughput of MANETs is $O\left(\frac{1}{m}\right)$, which is achievable when $D = w(m)$.

Remark 1: From the theorem above, it can be seen that the behavior of the secrecy throughput of MANETs falls into two different cases: (i) when the number of malicious nodes is $o(\sqrt{nD})$, the secrecy throughput is a function of the number of nodes n and the delay constraint D. The presence of malicious nodes has negligible impact on the network throughput; and (ii) when the number of malicious nodes is $\Omega\left(\sqrt{nD}\text{poly}(n)\right)$, the secrecy throughput is limited by the number of malicious nodes. The intuition is that in the second case, only Type-I packets can be received securely.

Remark 2: The additional constraints on achievability is to guarantee that $\lambda D = \omega(1)$, i.e., the number of bits that can be transmitted within D time slots (the delay constraint) is at least a constant number, so that the throughput has a practical meaning.

The proof of Theorem 1 consists of three parts: upper bound, achievable algorithm for $m = o(\sqrt{nD})$, and achievable algorithm for $m = \Omega\left(\sqrt{nD}\text{poly}(n)\right)$. We will briefly outline our proof for these three parts in the following three subsections.

A. Upper Bound

We state an upper bound on the secrecy throughput in the following lemma.

Lemma 1: (Upper Bound) If $m = o(\sqrt{nD})$, then the secrecy-throughput of MANETs is $O(\min\{\sqrt{D/n}, 1\})$; and if $m = \Omega\left(\sqrt{nD}\text{poly}(n)\right)$, then the secrecy-throughput of MANETs is $O\left(\frac{1}{m}\right)$.

Proof: It follows from [11] that $\Theta(\min\{\sqrt{D/n}, 1\})$ is the maximum throughput for MANETs without malicious nodes, and it hence serves as an upper bound on the secrecy throughput. For the case when $m = \Omega\left(\sqrt{nD}\text{poly}(n)\right)$, we separately bound the throughputs of Type-I and Type-II packets. The details are omitted due to space limitations. ■

B. Achievable Algorithm I for $m = o(\sqrt{nD})$

In this subsection, we propose secure communication algorithms that for the case in which $m = o(\sqrt{nD})$. To create an equivalent discrete memoryless erasure wire-tap channel, we need to guarantee that symbols in one message (hence one codeword) see independent erasure channels. This requires: (1) symbols in one message must be in different packets; and (2) relay copies that contain symbols from one message do not collide to transmit to the same destination. The first condition is guaranteed by message interleaving and the second condition is guaranteed by scheduling relay copies that contain symbols from one super-time-slots. We outline our algorithm as follows.

(1) **Message interleaving and coding:** We apply the secure codes [16] for the erasure wire-tap channel to encode each message. Let the codeword length be K bits. Group $X = D\sqrt{D}W/(16\sqrt{n})$ codewords (corresponding to X messages) for interleaving, i.e., generate K super-packets with each super-packet consisting of one symbol from each codeword. Hence, each super-packet contains $X = D\sqrt{D}W/(16\sqrt{n})$ bits. We then break each super-packet into $D\sqrt{D/n}$ packets, each with $W/16$ bits. See Figure 2 for an illustration.

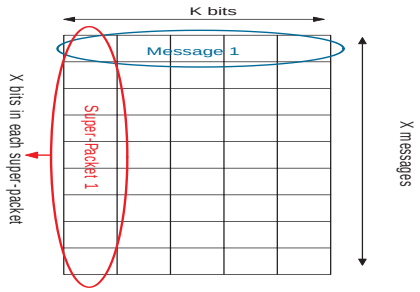

Fig. 2. An illustration of message interleaving

(2) **Cell scheduling:** We set the transmission radius of each node to be $L = 1/\sqrt[4]{nD}$. The unit torus is divided into cells such that the side-length of each cell is L. We group every 4×4 set of cells into a super-cell, and index the cells from 1 to 16. We divide each time slot into 16 mini-slots, and at mini-slot i, the cells with index i are chosen to be active. If a cell is active, one mobile in the cell is selected to transmit. It is easy to verify that under this cell scheduling algorithm, simultaneous transmissions do not cause interference under the protocol model.

(3) **Two-hop transmission scheme:** Consider KD time-slots, where we group every set of D time slots into a super-time-slot. Thus, we have K super-time-slots. At z^{th} super-time-slot, the packets belonging to the z^{th} super-packet are transmitted using the following scheme:

(a) **Broadcasting:** This step consists of $D/2$ time slots. At each time slot, in each cell, we randomly choose a mobile. The mobile checks other mobiles within its transmission radius. If there are more than $9\pi nL^2/10$ mobiles in the cell, and the selected mobile has not broadcast all packets belonging to the z^{th} super-packet, then a packet that was not previously sent is broadcast in the cell. Recall that our choice of packet size and cell scheduling allow one node in every cell to transmit during every time slot.

(b) **Receiving:** This step consists of the remaining $D/2$ time slots. At each time slot, each destination checks whether there are deliverable packets within its cell. During the minislot allocated to a certain cell, if there is only one deliverable packet in the cell, then the packet is transmitted

to the destination using a one-hop transmission. At the end of this step, all undelivered packets are dropped.

(4) **Decoding:** Each destination decodes the K super-packets. Then the destination groups the g^{th} bit of every super-packet, and then decodes the g^{th} data message.

The probability of the packet loss for the legitimate destination can be computed, which corresponds to the erasure probability for the channel from the source to the destination. The super-eavesdropper (all malicious nodes) may get hold of packets in the broadcasting and receiving steps in the two-hop transmission scheme. The probability of the packet loss for the super-eavesdropper based on the above scheme can be computed as well. These two erasure probability parameters are used to design the secure code to encode the messages so that perfect secrecy can be guaranteed. The details are omitted due to space limitations. We conclude the achievable result shown in this subsection in the following lemma.

Lemma 2: (Lower Bound I) If $m = o(\sqrt{nD})$ and $D = \omega(\sqrt[3]{n})$, then there exist $X = \Theta(D\sqrt{D/n})$ and $K = \Theta(1)$ such that each source-destination pair can communicate X messages within D time slots with perfect secrecy.

C. Achievable Algorithm II for $m = \Omega(\sqrt{nD}\text{poly}(n))$

In this subsection, we consider the case in which $m = \Omega(\sqrt{nD}\text{poly}(n))$. We consider only Type-I packets, and outline our algorithm as follows.

(1) **Message interleaving and coding:** Each message is coded into K bits using secure codes. Group $W/16$ coded messages and generate K super-packets (each with $W/16$ bits) similar to procedures in step (1) of achievable Algorithm I.

(2) **Cell scheduling:** We set the transmission radius of each node to be $\frac{1}{\sqrt{m}}$. The unit torus is divided into cells such that the side-length of each cell is $\frac{1}{\sqrt{m}}$. The cell scheduling is the same as that in Algorithm I.

(3) **One-hop transmission scheme:** At each time slot, each destination checks whether its source is within its cell. During the minislot allocated to a certain cell, if there is only one S-D pair within the cell, then the packet is transmitted to the destination directly from the source.

(4) **Decoding:** Each destination decodes the g^{th} bit of every super-packet to recover the g^{th} data messages.

It is clear that based on Algorithm II, the corresponding erasure probability of the channel to the destination is zero, and the erasure probability of the channel to the super-eavesdropper can be computed. We conclude the achievable result we show in this subsection in the following lemma.

Lemma 3: (Lower Bound II) If $m = \Omega(\sqrt{nD}\text{poly}(n))$ and $D = \omega(m)$, there exists $K = \Theta(1)$ such that each S-D pair can communicate $W/16$ messages within $\Theta(m)$ time slots with perfect secrecy.

VI. Conclusion

In this paper, we have studied the secrecy throughput of MANETs with malicious nodes. We have modeled communication in MANETs by an erasure wire-tap channel, and applied the secrecy capacity of the wire-tap channel to characterize the secrecy throughput for MANETs. We have also explored secure coding and practical coding design for the wire-tap channel to construct secure communication algorithms to achieve the optimal secrecy throughput.

Acknowledgment

The work of Y. Liang was supported by the National Science Foundation CAREER Award under Grant CCF-08-46028. The work of H. V. Poor was supported by the National Science Foundation under Grant CNS-06-25637. The work of L. Ying was supported by the Defense Threat Reduction Agency under Grant HDTRA1-08-1-0016.

References

[1] M. Grossglauser and D. Tse, "Mobility increases the capacity of ad-hoc wireless networks," in *Proc. IEEE Infocom.*, vol. 3, San Francisco, CA, April 2001, pp. 1360–1369.

[2] S. N. Diggavi, M. Grossglauser, and D. Tse., "Even one-dimensional mobility increases ad hoc wireless capacity," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Palais de Beaulieu, Lausanne, Switzerland, 2002, p. 352.

[3] M. Neely and E. Modiano, "Capacity and delay tradeoffs for ad-hoc mobile networks," *IEEE Trans. Inform. Theory*, vol. 51, no. 6, pp. 1917–1937, 2005.

[4] S. Toumpis and A. J. Goldsmith, "Large wireless networks under fading, mobility, and delay constraints," in *Proc. IEEE Infocom.*, vol. 1, Hong Kong, 2004, pp. 619–627.

[5] X. Lin and N. Shroff, "Towards achieving the maximum capacity in large mobile wireless networks," *J. Commun. and Networks*, no. 4, pp. 352–361, 2004.

[6] A. E. Gammal, J. Mammen, B. Prabhakar, and D. Shah, "Optimal throughput-delay scaling in wireless networks - part I: The fluid model," *IEEE Trans. Inform. Theory*, vol. 52, no. 6, pp. 2568–2592, June 2006.

[7] ——, "Optimal throughput-delay scaling in wireless networks - part II: Constant-size packets," *IEEE Trans. Inform. Theory*, vol. 52, no. 11, pp. 5111–5116, November 2006.

[8] G. Sharma, R. Mazumdar, and N. Shroff, "Delay and capacity trade-offs in mobile ad hoc networks: A global perspective," in *Proc. IEEE Infocom.*, Bacelona, Catalunya, Spain, April 2006, pp. 1–12.

[9] X. Lin, G. Sharma, R. R. Mazumdar, and N. B. Shroff, "Degenerate delay-capacity trade-offs in ad hoc networks with Brownian mobility," *Joint Special Issue of IEEE Transactions on Information Theory and IEEE/ACM Transactions on Networking on Networking and Information Theory*, vol. 52, no. 6, pp. 2777–2784, June 2006.

[10] J. Mammen and D. Shah, "Throughput and delay in random wireless networks with restricted mobility," *IEEE Trans. Inform. Theory*, vol. 53, no. 3, pp. 1108–1116, March 2007.

[11] L. Ying, S. Yang, and R. Srikant, "Optimal delay-throughput trade-offs in mobile ad hoc networks," *IEEE Trans. Inform. Theory*, vol. 54, no. 9, September 2008.

[12] P. Gupta and P. Kumar, "The capacity of wireless networks," *IEEE Trans. Inform. Theory*, vol. 46, no. 2, pp. 388–404, 2000.

[13] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[14] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, pp. 339–348, May 1978.

[15] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *Bell Syst. Tech. J.*, vol. 63, pp. 2135–2157, Dec. 1984.

[16] A. Thangaraj, S. Dihidar, A. Calderbank, S. McLaughlin, and J.-M. Merolla, "Application of LDPC codes to the wiretap channel," *IEEE Trans. Inform. Theory*, vol. 53, pp. 2933–2945, Aug. 2007.