Secrecy Throughput of MANETs Under Passive and Active Attacks

Yingbin Liang, *Member, IEEE*, H. Vincent Poor, *Fellow, IEEE*, and Lei Ying, *Member, IEEE*

***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. A model under passive attack is first studied, in which the malicious nodes are assumed to be eavesdroppers that only listen to transmission without actively injecting signals. An information-theoretic approach for security is applied to achieve secure communication among legitimate nodes in MANETs with transmissions being kept perfectly secure from eavesdroppers. 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 optimal secrecy throughput equals that of MANETs without malicious nodes, i.e., the impact of the presence of malicious nodes on the network throughput is negligible; and when $m = \Omega\left(\sqrt{nD}\text{poly}(n)\right)$, i.e., $\lim_{n\to\infty} m/\left(\sqrt{nD}\text{poly}(n)\right) \geq c$ for a positive constant c, the optimal secrecy throughput is limited by the number of malicious nodes. A model under active attack is further studied, in which the malicious nodes actively attack the network by transmitting modified packets to the destination nodes. It is shown that to guarantee the same throughput as the model under passive attack, the model under active attack needs to satisfy more stringent condition on the number of malicious nodes.**

***Index Terms*—Erasure channel, mobile *ad hoc* network (MANET), mobility model, secrecy, throughput scaling, wiretap channel.**

I. Introduction

MOBILE *ad hoc* networks (MANETs) represent one of the most innovative emerging networking technologies, with broad potential applications in personal area networks, emergency and rescue operations, military applications, etc. The unique features of MANETs, such as mobility and peer-to-peer connectivity, make MANETs a very flexible technology for establishing communication in areas with limited infrastructure. However, providing secure communication over MANETs using traditional cryptographic methods presents significant challenges due to: 1) the open nature of the wireless medium, which allows eavesdroppers and attackers to intercept information transmission (in particular, transmission of secret keys) or to degrade transmission quality; 2) the lack of infrastructure, which makes key distribution and management required for traditional symmetric-key cryptographic approaches difficult; and 3) energy and complexity limitations at terminals that may prohibit the use of alternative cryptographic methods, such as public key cryptography. New approaches to achieving security in MANETs are thus of considerable interest.

In this paper, we propose to achieve secure communication over MANETs via an approach developed based on information-theoretic security. The idea is to apply the powerful secure coding developed in information-theoretic security to preprocess messages being transmitted through the network to guarantee secure communication in the presence of malicious nodes. The contributions of this paper are summarized below.

- We identify equivalent wiretap models for MANETs with malicious nodes, which facilitate the application of the information-theoretic security approach for securing MANETs, and the corresponding theoretical analysis of fundamental secrecy rate limits.
- The messages transmitted securely between legitimate nodes can be viewed as secret keys, and hence symmetric keys are established between legitimate nodes over MANETs. This solves the open problem of key distribution for MANETs under a two-dimensional (2-D) independent and identically distributed (i.i.d.) mobility model [1], [9].
- The fundamental limits of the secrecy rate can be characterized in terms of the order of the numbers of legitimate and malicious nodes in networks. These limits apply to all possible secure transmission schemes, including those implemented via cryptographic approaches.
- The information-theoretic approach we proposed provides *provable* secure transmission (or key distribution) over MANETs.

More specifically, the MANET model we consider consists of a number of legitimate nodes transmitting information among themselves, and also a number malicious nodes, which can receive information that is transmitted between the legitimate nodes. We assume that the malicious nodes follow the same mobility behavior as legitimate nodes. For MANETs, a virtual (or an equivalent) channel representation was developed

Manuscript received May 20, 2010; revised December 21, 2010; accepted May 26, 2011. Date of current version October 07, 2011. The work of Y. Liang was supported by a National Science Foundation CAREER Award under Grant CCF-10-26565 and by the National Science Foundation under Grant CCF-10-26566. The work of H. V. Poor was supported by the National Science Foundation under Grant CNS-09-05398. The work of L. Ying was supported by the National Science Foundation under Grant CNS-09-53165, and by the Defense Threat Reduction Agency (DTRA) under Grants HDTRA1-08-1-0016 and HDTRA1-09-1-0055. The material in this paper was presented in part at the IEEE International Symposium on Information Theory, Seoul, South Korea, June–July 2009.

Y. Liang is with the Department of Electrical Engineering and Computer Science, Syracuse University, Syracuse, NY 13244 USA (e-mail: yliang06@syr.edu).

H. V. Poor is with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: poor@princeton.edu).

L. Ying is with the Department of Electrical and Computer Engineering, Iowa State University, Ames, IA 50011 USA (e-mail: leiying@iastate.edu).

Communicated by R. A. Berry, Associate Editor for Communication Networks.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2011.2165800

in [1] to model the impact of mobility on packet delivery via an erasure channel, in which the erasure probability at the receiver corresponds to the probability that a packet could not get close enough to its destination before its deadline. The virtual channel representation enables a holistic information-theoretic view for the design of capacity-achieving algorithms in MANETs [1]. In this paper, we show that the behavior of malicious nodes can also 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 a wiretap channel with a destination (legitimate) receiver and an eavesdropper as studied in [2] and [3]. A review of information-theoretic security can be found in [4].

We first consider the passive attack model, in which the malicious nodes are assumed to be passive eavesdroppers, which do not send signals over the communication channels. In this case, the equivalent model is an erasure wiretap channel, in which both the channels to the destination and to the eavesdropper are erasure channels, i.e., each bit is successfully transmitted with a certain probability and otherwise gets erased (lost). Using information-theoretic approaches, the best secrecy rate (i.e., the secrecy capacity) at which information can be transmitted successfully while being kept secret from an eavesdropper in the basic wiretap channel is characterized in [2], and coding schemes designed to achieve this rate are developed in [5] and [6]. Thus, these coding schemes can be applied to achieve secure communication in MANETs, and the secrecy capacity of the wiretap channel provides a way to characterize the fundamental limits on the secrecy throughput in MANETs. The goal of this paper is to explore these information-theoretic approaches to investigate MANETs.

Although the performance limits of MANETs in terms of performance bounds on throughput and delay have been extensively studied (e.g., in [1] and [7]–[17]), performance limits of MANETs under secrecy constraints have not been studied much before although with exceptions [18]–[21]. This is in general a challenging problem, because traditional cryptographic approaches are not easy to quantify for optimality analysis. In this paper, we first explore information-theoretic approaches to provide an upper bound on the secrecy throughput, which is the largest throughput possible over the network under secrecy constraints no matter what kind of schemes are used for achieving security. Hence, this upper bound also provides a fundamental performance limit for approaches based on encryption. We then propose joint coding, scheduling, and routing schemes to achieve this upper bound. Our results demonstrate that the scaling of throughput is separated into two regimes characterized by how the number of legitimate nodes n compares with the number of malicious nodes m, and correspondingly two different transmission schemes need to be implemented for these two regimes. The two regimes are separated by a threshold on $m = o(\sqrt{nD})$,[1] where D denotes the delay constraint and scales with n. In particular, we show that when $m = o(\sqrt{nD})$, the secrecy throughput equals the throughput of MANETs without malicious nodes and can be achieved by a multihop secrecy scheme; and when $m = \Omega\left(\sqrt{nD}\text{poly}(n)\right)$, the secrecy throughput is limited by the number of malicious nodes, and can be achieved by a single-hop scheme.

We then extend our approach to study the active attack model, in which the malicious nodes can transmit modified packets to the destination nodes in addition to eavesdropping. We first show that this model is equivalent to a wiretap channel with the channel to the legitimate receiver being a binary symmetric erasure channel (i.e., each bit may be successfully received with a certain probability, modified with a certain probability and erased otherwise) and the channel to the eavesdropper being an erasure channel. Hence, the active attack is characterized by the properties of the legitimate receiver's channel in the equivalent wiretap channel, while the passive attack is characterized by the eavesdropper's channel. By applying the secrecy rate and achievable secrecy schemes for the wiretap channel, we also characterize the secrecy throughput for the active attack model for MANETs in two regimes. Compared to the passive attack model, the difference lies in that, to guarantee the same throughput, the model under active attack needs to satisfy more stringent condition on the number of malicious nodes. However, when $m = \Omega\left(\sqrt{nD}\text{poly}(n)\right)$ holds, the same secrecy throughput is achieved as the passive model because the single-hop scheme dominates the contribution to the secrecy throughput.

We would like to comment that the secrecy throughput of *static ad hoc* wireless networks has recently been studied in [18]–[21]. In particular, Koyluoglu *et al.* [18] show that if the eavesdropper density is on the order of $O(1/(\log n)^2)$, then the secrecy rate scales as $1/\sqrt{n}$. The network model we consider assumes the nodes are mobile, and hence the network has dynamic structure. In a static *ad hoc* wireless network, multihop transmissions (routing) are needed to deliver packets from sources to their corresponding destinations; while in mobile *ad hoc* networks, the mobiles can physically carry the packets to their destinations instead of using routing. Therefore, both the transmissions strategies and throughput scaling of MANETs are fundamentally different from those of static *ad hoc* networks. The results and analysis of this paper, hence, are different from those in [18]–[21]. For example, compared to [18], our model allows the density of eavesdroppers to be larger than 1, and the secrecy throughput depends on not only n and m, but also D, the delay constraint.

The paper is organized as follows. In Section II, we introduce the MANET model with the secrecy constraint on the system. In Section III, we introduce the basic concepts and definitions of information-theoretic security, and provide the main result on the secrecy capacity of the block erasure wiretap channel, which is very useful for analyzing the secrecy throughput of MANETs. In Sections IV and V, we provide the main results on MANETs under passive attacks. In Section VI, we provide the results for MANETs under active attacks. Finally, in Section VII, we give a few concluding remarks.

[1] We adopt the following notation in the paper. For nonnegative 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.

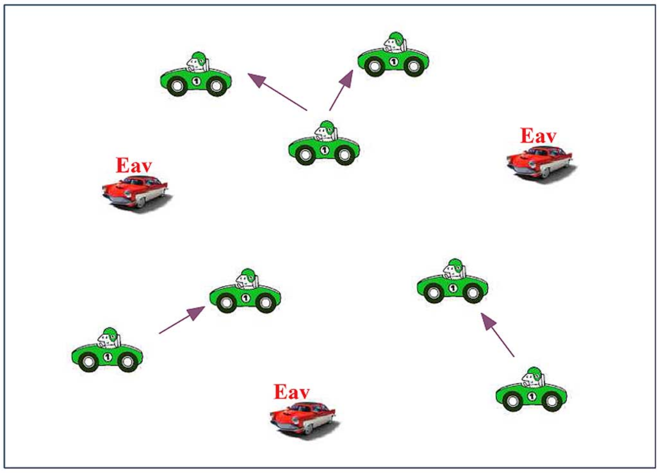

Fig. 1. An example MANET with eavesdroppers.

II. MANET Model

In this section, we describe our models for network configuration, communications, and security attacks. We consider a wireless MANET that consists of n legitimate wireless nodes and m malicious nodes positioned in a unit square (see Fig. 1 for an illustration). We assume the legitimate nodes know the value of m or at least the order of m. We adopt the 2-D i.i.d. mobility model [1], [9]. As such, each node is uniformly, randomly positioned in the unit 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 that of 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 well-known protocol model [22] to model transmissions between nodes in the network. We assume that all mobile nodes use a common transmission radius L. Let $\mathrm{dist}(i,j)$ denote the Euclidean distance between node i and node j. Node i can successfully transmit to node j if $\mathrm{dist}(i,j) \leq L$ and $\mathrm{dist}(k,j) \geq (1+\Delta)L$ for each node $k \neq i$ which transmits at the same time, where Δ is a protocol-specified guard zone whose purpose is to prevent interference. We further assume a fast mobility model [1] in which only one-hop transmissions are feasible and each transmission can send B bits, which is independent of n.

We study both passive and active attacks in this paper. The first model considers passive attacks, in which 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, in this case, 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. The second model considers active attacks, in which a malicious node not only can receive packets as assumed for passive attacks, but also can modify and deliver the packets to a destination if the destination is within transmission radius of this malicious node. We note that the secrecy capacity of static *ad hoc* networks with colluding eavesdroppers has been studied in [19] and [20], which, however, is fundamentally different from the problem considered in this paper.

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 information bits being successfully delivered to node i in time interval $[0,T]$ and being kept perfectly secret from the malicious nodes (the definition of *perfect secrecy* will be given in Section III). A secrecy throughput λ per S–D pair is said to be *achievable* 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 joint coding, scheduling, and routing algorithm such that

$$\lim_{T\to\infty} \Pr\left(\frac{\Lambda_i[T]}{T} \geq \lambda,\ \forall\, i\right) = 1.$$

The goal of this paper is to characterize how the secrecy throughput scales with the numbers of legitimate nodes and malicious nodes.

III. Information-Theoretic Security

In this section, we provide some basic background on information-theoretic security including the basic wiretap 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 *wiretap channel* introduced and studied by Wyner [2]. This channel includes a source node that wishes to transmit a message W to a destination node (legitimate receiver) and wishes to keep this message as secret as possible from an eavesdropper (see Fig. 2 for an illustration). The channel is characterized by a transition probability distribution $P_{YZ|X}$, where X denotes the channel input, and Y and Z denote 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

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

where Z^l denotes the outputs at the eavesdropper for codeword length l. The equivocation rate indicates the eavesdropper's uncertainty about the message W given the information available to it. Hence, the larger is the equivocation rate, the higher is the level of secrecy.[2]

A rate R is achievable with perfect secrecy if there exists a block coding and decoding scheme such that the average error

[2] We note that the secrecy defined based on the equivocation rate in (1) is referred to as weak secrecy in the sense that information is secure at the level of the (encoding) block, i.e., encoded messages. There is also a notation of strong secrecy [23] that concerns security at the level of the transmission bit. This paper focuses only on weak secrecy. The problems considered in this paper can also be studied in the sense of strong secrecy.

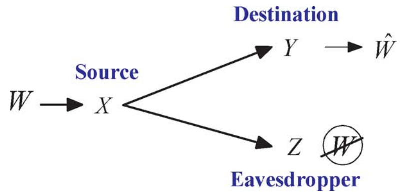

Fig. 2. The wiretap channel.

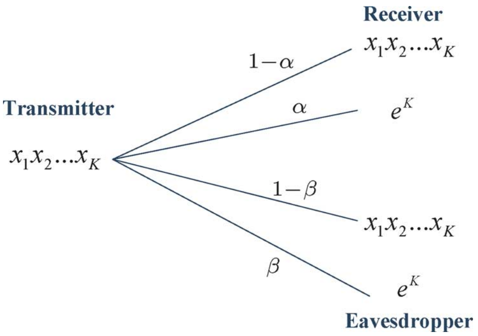

Fig. 3. A block transmission of the block erasure wiretap channel.

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 wiretap channel is characterized by Csiszár and Körner [3], 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 $U \to X \to (Y, Z)$.

Based on the result (3), we now study the secrecy capacity of the block erasure wiretap channel, which will be useful for studying MANETs. For the block erasure wiretap channel, each channel input symbol takes values in $\{0, 1\}$. A block of input $X^K = (X_1, \ldots, X_K)$ may be successfully received at the receiver with probability $1 - \alpha$, and may be erased completely with probability α, where $0 \leq \alpha \leq 1$. Hence, the distribution of a block channel output Y^K for any given input x^K is

$$P(Y^K | x^K) = \begin{cases} x^K, & \text{with probability } 1 - \alpha \\ e^K, & \text{with probability } \alpha \end{cases}$$

where e^K denotes K erased bits. From one block to another, channel inputs are erased independently with the same parameter α. The channel to an eavesdropper is assumed to be the same as that to the legitimate receiver, but with a different erasure parameter β. An illustration of this channel for one block is given in Fig. 3. This channel models packet transmission in practice with each packet contains a block of coded information bits.

Theorem 1: The secrecy capacity of the block erasure wiretap channel with block length K 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.

Proof: We view a block of transmission as one channel use, and hence the input alphabet takes 2^K values $(x_1^K, \ldots, x_{2^K}^K)$. Assume we choose the input probability distribution to be $P(X^K = x_j^K) = q_j$ for $j = 1, \ldots, 2^K$, where $\sum_{j=1}^{2^K} q_j = 1$. We first note that if $\beta \leq \alpha$, the receiver's channel is stochastically degraded with respect to the eavesdropper's channel, and hence the secrecy capacity is zero. If $\beta > \alpha$, the eavesdropper's channel is stochastically degraded with respect to the receiver's channel. In this case, choosing $U = X$ in (3) is optimal. We hence compute

$$I(X^K;Y^K) - I(X^K;Z^K) = \left(- \sum_{j=1}^{2^K} q_j \log q_j \right) (\beta - \alpha). \tag{5}$$

The above rate is maximized by choosing $q_j = \frac{1}{2^K}$ for $j = 1, \ldots, 2^K$, i.e., the uniform input distribution. We further normalize the rate computed above and obtain the desired secrecy capacity given by

$$C_s^E = \beta - \alpha$$

which concludes the proof. □

It is clear that the block erasure wiretap channel has the same secrecy capacity as the erasure wiretap channel (with blocklength 1). Hence, correlation between bits within blocks does not affect the secrecy capacity of the erasure wiretap channel. Thus, in this paper, we do not specifically distinguish between the two channels in terms of the secrecy capacity. One way to achieve the secrecy capacity of the block erasure channel is to apply interleaving, i.e., assigning symbols within each block to different codewords so that each bit in one codeword sees an independent erasure channel. In this way, secure coding design for the erasure wiretap channel (with the blocklength as the channel parameter $K = 1$) can be applied.

Secure coding design to achieve the secrecy capacity for the binary erasure wiretap channel with $\alpha = 0$ was first studied by Ozarow and Wyner [5], in which a nested code structure was proposed. Based on this structure, Thangaraj *et al.* [6] provided an explicit code design to achieve the secrecy capacity for the binary erasure wiretap channel. For the passive attack model, we will explore the secrecy capacity given in (4) to study the secrecy throughput for MANETs, and we will also propose strategies to apply the secure codes given in [6] to achieve the secrecy throughput.

IV. MANETs Under Passive Attacks

In this section, we study MANETs under passive attacks. We first characterize the secrecy throughput of MANETs in this case, and then present a heuristic argument to illustrate the intuition of our result. We delegate the rigorous proof to Section V.

Theorem 2: For the MANET model under passive attacks described in Section II, if $m = o(\sqrt{nD})$ and

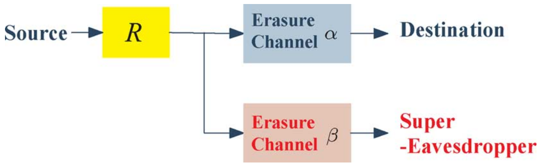

Fig. 4. An equivalent wiretap channel representation.

$D = \omega(\sqrt[3]{n})$, then the optimal secrecy throughput of MANETs is $\Theta(\min\{\sqrt{D/n}, 1\})$, and if $m = \Omega\left(\sqrt{nD}\mathrm{poly}(n)\right)$, then the optimal secrecy throughput of MANETs is $\Theta\left(\frac{1}{m}\right)$.

Remark 1: From this theorem, 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, which is at the same order as the one without malicious nodes. Thus, the presence of malicious nodes has negligible impact on the network throughput. ii) When the number of malicious nodes is $\Omega\left(\sqrt{nD}\mathrm{poly}(n)\right)$, the secrecy throughput is limited by the number of malicious nodes.

Remark 2: The additional constraint 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.

A. 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 Theorem 2. 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 Fig. 4), in which R is the rate at which a source can send out packets. The system also includes two erasure channels, one to the destination with erasure probability α, and the other to a super-eavesdropper with erasure probability β. The erasure channel at the bit level is shown in Fig. 5. 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 an erasure wiretap channel. From Section III, it is clear that the secrecy capacity of the erasure wiretap channel is the largest communication rate achievable with perfect secrecy, and hence can be applied to derive the fundamental secrecy throughput for the corresponding MANET.

To derive the secrecy throughput, we classify the packets sent out from a source into the following two types, respectively corresponding to single-hop and multihop transmissions, and hence respectively corresponding to two virtual erasure wiretap channels. Furthermore, these two type of packets correspond to major contributions to secrecy throughput in two network regimes, respectively.

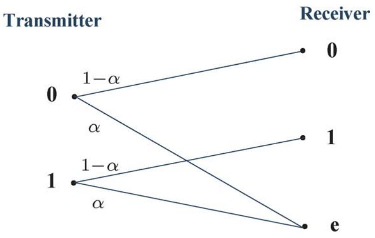

Fig. 5. An erasure channel.

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

We next heuristically compute the erasure probabilities α and β for the above two types of packets, and analyze the corresponding secrecy throughputs.

1) Secrecy Throughput of Type-I Packets: 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, $\alpha = 0$. Such 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 $1-\beta = 1-(1-\pi L^2)^m$. Furthermore, the probability that an S–D pair is within the communication range is πL^2, which implies that the rate at which the source can send out a Type-I packet is given by $R = \pi L^2$.

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

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

2) Secrecy Throughput of Type-II Packets: The delivery of a Type-II packet contains three phases:

- the packet is transmitted from the source to one or multiple relays;
- the mobile relays physically carry the packet near the destination;
- 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 deliverable 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 being delivered, so the erasure probability of the super-eavesdropper is upper bounded by

$$\beta = \left(1 - \pi L^2\right)^m.$$

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

$$C_{s,\mathrm{II}} = \max_L \frac{1}{\pi n L^2}\left(\left(1 - \pi L^2\right)^m - \left(1 - \pi L^2\right)^{\pi L^2 nD}\right). \tag{6}$$

By further analyzing (6), we obtain the following lemma on the secrecy throughput of Type-II packets.

Lemma 1: 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

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

Proof: See the Appendix. □

3) Total Secrecy Throughput: To combine the secrecy throughputs of Type-I and Type-II packets, we note that the total throughput satisfies

$$C_s \le C_{s,\mathrm{I}} + C_{s,\mathrm{II}}$$

and we need $D \cdot C_s = \Omega(1)$ to guarantee that the throughput is achievable for Type-II packets. Thus, we conclude that if $m = o\left(\sqrt{nD}\right)$, then

$$C_s \doteq C_{s,\mathrm{II}} = \begin{cases} \Theta\left(\sqrt{\frac{D}{n}}\right), & D = \Omega(\sqrt[3]{n}) \\ 0, & \text{otherwise} \end{cases}$$

where $a \doteq b$ denotes equality in the sense of being of the same order. Otherwise, if $m = \Omega\left(\sqrt{nD}\right)$, we have that

$$C_s \doteq C_{s,\mathrm{I}} = \Theta\left(\frac{1}{m}\right).$$

Hence, 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 $C_s = \Theta\left(\frac{1}{m}\right)$.

We note that the above argument is heuristic. For example, $1 - \alpha$ is the probability that a packet becomes deliverable. However, it is not equal to the probability that the packet is actually delivered because when multiple packets to the same destination become deliverable at the same time, one packet is delivered. Nevertheless, the heuristic argument still reveals some important information that will guide our mathematical proofs given in the next section, in which we will first prove that the above heuristic results are upper bounds on the secrecy throughput, and we will then present algorithms that achieve the upper bounds and hence achieve the optimal secrecy throughput under certain conditions.

V. Proof of Theorem 2

The proof of Theorem 2 consists of three parts: an upper bound and two achievable algorithms for two network regimes with $m = o(\sqrt{nD})$ and $m = \Omega\left(\sqrt{nD}\mathrm{poly}(n)\right)$, respectively.

A. Upper Bound

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

Lemma 2 (Upper Bound): If $m = o(\sqrt{nD})$, then the secrecy throughput of MANETs is $O(\min\{\sqrt{D/n}, 1\})$; and if $m = \Omega\left(\sqrt{nD}\mathrm{poly}(n)\right)$, then the secrecy throughput of MANETs is $O\left(\frac{1}{m}\right)$.

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

We first consider Type-I packets transmitted between a specific S–D pair. Assume that the source sends out X_{I} Type-I packets during a time period of T time slots such that $\pi L^2 T = \omega(1)$. We also note that the probability that a S–D pair is within the communication range at a given time slot is πL^2, and the source can send B/S_p packets in one time slot, where S_p is the packet size. Without loss of generality, we assume that $S_p = B$, so the source can send one packet per time slot. Hence, by the Chernoff bound, we obtain that

$$\Pr\left(X_{\mathrm{I}} \le (1+\epsilon)\pi L^2 T\right) \ge 1 - e^{-\epsilon \pi L^2 T}$$

which converges to 1 as T goes to infinity. Thus, we have that

$$\begin{aligned} C_{s,\mathrm{I}} &\le \max_L (1+\epsilon)\pi L^2 \left(1 - \pi L^2\right)^m \\ &= (1+\epsilon)\frac{1}{m+1}\left(1 - \frac{1}{m+1}\right)^m \\ &\to \frac{(1+\epsilon)e^{-1}}{m+1} \\ &= \Theta\left(\frac{1}{m}\right). \end{aligned} \tag{7}$$

We next consider Type-II packets. We further classify Type-II packets into the following two subtypes:

1) Type-II-1 packets have more than $(1+\epsilon)\pi L^2 n$ relay copies;
2) Type-II-2 packets have no more than $(1+\epsilon)\pi L^2 n$ relay copies.

Note that to generate a Type-II-1 packet, the source needs to have more than $(1+\epsilon)\pi L^2$ relays in its communication range when the source sends out the packet. This event occurs with probability no more than $e^{-\epsilon\pi L^2 n}$. Thus, the probability that there are more than $(1+\epsilon)Te^{-\epsilon\pi L^2 n}$ Type-II-1 packets for a specific source over T time slots is lower bounded by

$$1 - e^{-\epsilon T e^{-\epsilon\pi L^2 n}}.$$

The probability that there are no more than $(1+\epsilon)nTe^{-\epsilon\pi L^2 n}$ Type-II-1 packets is lower bounded by

$$\left(1 - e^{-\epsilon T e^{-\epsilon\pi L^2 n}}\right)^n$$

which converges to one as T goes to infinity. We note that each Type-II-1 packet has at most n relay copies, and the probability that a Type-II-1 packet becomes deliverable before its deadline is no more than $1-(1-\pi L^2)^{nD}$, and each packet will be heard with probability $1-(1-\pi L^2)^m$ by one of the malicious nodes (i.e., the super-eavesdropper). Thus, defining $C_{s,\text{II}-1}$ to be the secrecy throughput per S–D pair contributed from Type-II-1 packets, we have

$$\begin{aligned} C_{s,\text{II}-1} &\le \frac{(1+\epsilon)Tne^{-\epsilon\pi L^2 n}\left((1-\pi L^2)^m-(1-\pi L^2)^{nD}\right)}{Tn} \\ &= (1+\epsilon)e^{-\epsilon\pi L^2 n}\left((1-\pi L^2)^m-(1-\pi L^2)^{nD}\right). \end{aligned} \tag{8}$$

To guarantee that the equation above is positive, $nD = \Omega(m)$, and hence we have

$$C_{s,\text{II}-1} = O\left(e^{-\epsilon n}\right) = O\left(e^{-\frac{m}{D}}\right). \tag{9}$$

We next consider Type-II-2 packets. The probability that a Type-II-2 packet becomes deliverable before its deadline is no more than $1-(1-\pi L^2)^{(1+\epsilon)\pi L^2 nD}$. With transmission radius L, at most $\frac{1}{\pi L^2}$ packets can be transmitted sources during one time slot. Thus, the number of Type-II-2 packets in the network is upper bounded by $\frac{T}{\pi L^2}$. Therefore, defining $C_{s,\text{II}-2}$ to be the secrecy throughput per S–D pair contributed from Type-II-2 packets, we have

$$\begin{aligned} C_{s,\text{II}-2} &\le \frac{T\left((1-\pi L^2)^m-(1-\pi L^2)^{(1+\epsilon)\pi L^2 nD}\right)}{\pi L^2 Tn} \\ &= \frac{(1-\pi L^2)^m-(1-\pi L^2)^{(1+\epsilon)\pi L^2 nD}}{\pi L^2 n}. \end{aligned} \tag{10}$$

To guarantee that the right-hand side of the equation above is positive, we require $\pi L^2 = \Omega\left(\frac{m}{nD}\right)$, and hence we obtain

$$C_{s,\text{II}-2} = O\left(\frac{D}{m}e^{-\frac{m^2}{nD}}\right). \tag{11}$$

We also note that we need $D \cdot C_{s,\text{II}-i} = \Omega(1)$ for $i = 1, 2$ to guarantee that the secrecy throughput is achievable. Comparing (9) and (11) with (7), we conclude that (7) provides the dominant term for the secrecy throughput for the case when $m = \Omega\left(\sqrt{nD}\text{poly}(n)\right)$, which concludes the proof. □

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

In this section, we describe secure communication algorithms for the case in which $m = o(\sqrt{nD})$. To create an equivalent discrete memoryless erasure wiretap channel, we need to guarantee that symbols in one codeword (that encodes one message) see independent erasure channels. This requires: 1) symbols in one codeword must be in different packets; and 2) relay copies that contain symbols from one codeword 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 codeword to different super-time-slots. We outline our algorithm as follows.

---

1) *Stochastic secure coding and message interleaving:* We apply the secure codes [6] and stochastic encoding schemes proposed in [2] for the erasure wiretap channel to encode each message. In particular, each message corresponds to a set of codewords. If a message is chosen to be sent to its destination, one of the codewords in the set is randomly selected to be sent. Such a stochastic encoding process is implemented to confuse the eavesdropper. We let the codeword length be K bits. Group $X = D\sqrt{D}B/(16\sqrt{n})$ 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 $X = D\sqrt{D}B/(16\sqrt{n})$ bits. We then break each super-packet into $D\sqrt{D/n}$ packets, each with $B/16$ bits. An illustration is depicted in Fig. 6. We note that each codeword in the figure is the randomly selected one under the stochastic encoding schemes.

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 minislots, and at minislot 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 $K \cdot D$ time-slots, where we group every set of D time slots into a super-time-slot. Thus, we have K super-time-slots. At the zth super-time-slot, the packets belonging to the zth 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 zth super-packet,

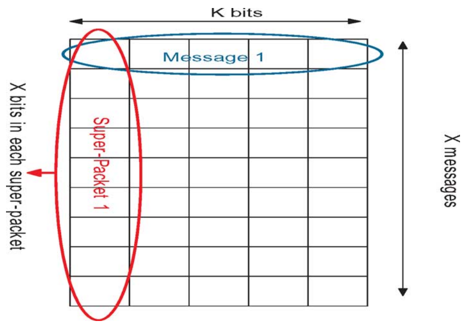

Fig. 6. An illustration of message interleaving.

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 each cell to transmit during each 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. Namely, the destination groups the gth bit from all super-packets, and then decodes the gth source message.

The probability of 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 following lemma specifies the secrecy throughput achieved by the above scheme.

Lemma 3 (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 S–D pair can communicate X messages within D time slots with perfect secrecy.

Proof: We consider the probability that a packet is received by one of the malicious nodes (the super-eavesdropper). Under the secure communication algorithm, each packet will be transmitted at most twice, and each transmission will be heard by a malicious node with probability πL^2. Thus, the probability that a packet is not received by the super-eavesdropper, i.e., the erasure probability of the virtual channel between the source and malicious nodes, is given by

$$\lim_{n\to\infty} \beta = \lim_{n\to\infty} (1-\pi L^2)^{2m} = 1$$

where we have used the assumption that $m = o(\sqrt{nD})$ and $L = \Theta\left(1/\sqrt[4]{(nD)}\right)$. As shown in [1], $\Theta(\sqrt{D/n})$ is achievable and α is a constant when $L = \Theta\left(1/\sqrt[4]{(nD)}\right)$. Hence, the existence of the malicious nodes does not change the order of the throughput. □

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

In this section, we consider the case in which $m = \Omega(\sqrt{nD}\mathrm{poly}(n))$. We consider only Type-I packets, which dominate the secrecy throughput. We describe our algorithm as follows.

---

1) *Stochastic secure coding and message interleaving:* Each message is coded into K bits using secure codes and is transmitted via stochastic encoding. Group $B/16$ coded messages and generate K super-packets (each with $B/16$ bits) similar to the procedures in step 1) of 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 groups the gth bit of all super-packets and decodes the gth source messages.

We specify the secrecy throughput achieved by the above algorithm in the following lemma.

Lemma 4 (Lower Bound II): If $m = \Omega(\sqrt{nD}\mathrm{poly}(n))$, then there exists $K = \Theta(1)$ such that each S–D pair can communicate $B/16$ messages within $\Theta(m)$ time slots with perfect secrecy.

Proof: We choose $X = \frac{nD^3}{m^3}e^{-\frac{10m^2}{\pi nD}}$, $K = \frac{nD^3}{m^3}$ and $L = \sqrt{\frac{5m}{\pi nD}}$. We consider a specific S–D pair within a fixed super-time-slot.

It is clear that based on Algorithm II, the corresponding erasure probability of the channel to the destination is zero. We also note that the eavesdropper can obtain a packet during the broadcast phase or the delivery phase. The probability that packet k is obtained by the eavesdroppers is lower bounded by

$$1-(1-\pi L^2)^{2m}.$$

Thus, the secrecy throughput is given by

$$\max_L \pi L^2(1-\pi L^2)^m = \Theta\left(\frac{1}{m}\right). \qquad \square$$

We comment that due to the i.i.d. mobility assumption, the probability of successful delivery of a packet depends on the number of relays that carry the packet, and is independent of which nodes are the relays. Therefore, it is sufficient to consider single-hop or two-hop transmissions because a source can broadcast a packet to sufficiently many relays using one broadcast instead of using multiple-hop transmissions.

VI. MANETs Under Active Attacks

We now consider the MANET model under active attacks, in which the m malicious nodes not only can receive the packets that are transmitted in their reception range, but also can modify and deliver the packets to the destination if the destination is within its transmission range. We assume that the malicious nodes modify every bit in the codewords, which can be argued to be the best active attack strategy, given that message interleaving is adopted by the transmitters. This is because different bits in a packet belong to different codewords, and hence are independent. Therefore, modifying every bit in a packet maximally reduces decodability at the destination.

In the rest of this section, we will first provide a heuristic argument on the secrecy throughput for the model under active attacks. We will then present the main theorem on the secrecy throughput followed by a proof. Similar to the passive attack model, we identify an equivalent wiretap channel for the active attack model. We first note that bit modification affects only destinations, and hence packet reception of malicious nodes (i.e., the super-eavesdropper) is the same as that for the passive attack model and can be modeled as an erasure channel with erasure probability β. To model packet delivery at legitimate destinations, we assume that when multiple copies of a coded packet are received by a destination, the destination keeps only the first one and drops the others. Similarly to the passive attack model, we consider Type-I and Type-II packets. For Type-I packets, which are directly sent to their destinations, it is clear that active attacks do not affect packet delivery, because these packets are directly sent from source nodes and are the first copies received by the corresponding destinations. Hence, the packet delivery at destinations can be modeled as a perfect channel, i.e., an erasure channel with erasure probability zero, which is the same as the passive attack model.

We next focus on Type-II packets, which are first sent to relay nodes, and are then delivered to their destinations via relay nodes. Unlike the passive attack model, the malicious nodes can modify received packets and deliver them to destinations. 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 with a high probability $\pi L^2 n$ relay (legitimate) copies and $\pi L^2 m$ modified (by malicious nodes) copies in the network. We have the following (heuristic) observations.

- For the $\pi L^2 n$ relay (legitimate) copies of a packet, each copy becomes deliverable at time t with probability πL^2. Thus, the probability that the packet is delivered correctly in one of the D time slots is at most
$$p_1 = 1 - \left(1 - \pi L^2\right)^{\pi L^2 nD}.$$
- For the $\pi L^2 m$ modified copies of a packet, each copy becomes deliverable at time t with probability πL^2. Thus, the probability that the modified packet is delivered in one of the D time slots is at most
$$p_2 = 1 - \left(1 - \pi L^2\right)^{\pi L^2 mD}.$$

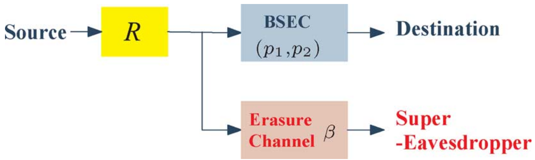

Fig. 7. An equivalent wiretap channel representation for active attacks.

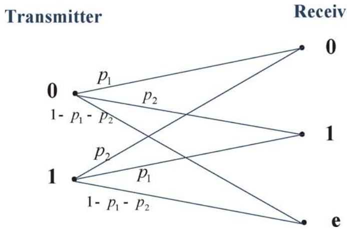

Fig. 8. A binary symmetric erasure channel.

- If none of relay (legitimate) and modified copies of a packet are delivered at the destination within D time slots, the packet is erased with probability $\alpha = 1 - p_1 - p_2$.
- 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
$$R = \frac{1}{\pi L^2 n}.$$
- Each packet has to be transmitted at least once before being delivered, so the erasure probability of the super-eavesdropper is upper bounded by
$$\beta = \left(1 - \pi L^2\right)^m.$$

In summary, the MANET under active attack can be modeled as an equivalent wiretap channel as depicted in Fig. 7. The channel to the super-eavesdropper (all malicious nodes) can be modeled as an erasure channel with erasure probability β, and the channel to the legitimate receiver can be modeled as a binary symmetric erasure channel (BSEC), in which an input symbol may be correctly received with probability p_1, modified with probability p_2, and erased with probability $\alpha = 1 - p_1 - p_2$. The BSEC at the bit level is depicted in Fig. 8. We note that although malicious nodes can perform active attacks by modifying the packets, the equivalent model has only a passive eavesdropper, in which the active attack is modeled into the statistics of the channel to the legitimate receiver.

The secrecy capacity of the above wiretap channel can be derived by using (3). The channel input X is binary, and the auxiliary random variable U has a cardinality constraint. Hence, the optimal joint input distribution P_{UX} can be obtained numerically to compute the secrecy capacity. However, it is difficult to obtain any analytical properties from such numerical results. We will hence approach this in a different way. Namely, we will first compute an achievable secrecy rate obtained by choosing

$U = \phi$ and a uniform distribution for P_X, and then show that this special choice of the input distribution does not affect the optimality in terms of the order of nodes.

Based on (3), an achievable secrecy rate is given by

$$\begin{aligned} R_s &= \max_L \frac{1}{\pi n L^2} \left(I(X;Y) - I(X;Z) \right) \\ &= \max_L \frac{1}{\pi n L^2} \left[(1-\alpha) \left(1 - H\left(\frac{p_1}{p_1+p_2} \right) \right) - (1-\beta) \right] \\ &= \max_L \frac{1}{\pi n L^2} \left[\beta - \alpha - H\left(\frac{p_1}{p_1+p_2} \right) (1-\alpha) \right] \end{aligned} \tag{12}$$

where $H(x) = -x \log x - (1-x)\log(1-x)$ is the binary entropy function. We then have the following theorem based on (12).

Theorem 3: If $m = o(\sqrt{nD}) \cap o(n)$ and $D = \omega(\sqrt[3]{n})$, then the optimal secrecy throughput of MANETs is $\Theta(\min\{\sqrt{D/n}, 1\})$, and if $m = \Omega\left(\sqrt{nD}\text{poly}(n)\right)$, then the optimal secrecy throughput of MANETs is $\Theta\left(\frac{1}{m}\right)$.

Proof: We first note that the upper bound obtained in Lemma 2 continues to be an upper bound.

We now consider achievable schemes. If $m = o(\sqrt{nD}) \cap o(n)$ and $D = \omega(\sqrt[3]{n})$, then $p_1/p_2 \rightarrow \infty$ and hence $H(p_1/(p_1+p_2)) = o(1)$. Thus, applying an algorithm similar to the achievable scheme proposed in Section V-B (with the secure coding scheme designed for the BSEC wiretap channel), it can be shown that $\beta \rightarrow 1$ as $n \rightarrow \infty$, which implies that

$$R_s = \max_L \frac{1}{\pi n L^2} (1-\alpha) = O(\min\{\sqrt{D/n}, 1\}). \tag{13}$$

Now if $D = \omega(m)$, then we apply the algorithm proposed in Section V-C, in which all packets are directly transmitted from sources to destinations. Since each destinations accepts only the first copy when multiple copies of a packet are received, the network is immune to active attacks under this scheme. The secrecy throughput $\Theta\left(\frac{1}{m}\right)$ is hence achievable. □

If we compare our results for the models under passive and active attacks, it is clear that the secrecy throughput is the same when the number of malicious nodes is large. This is a little counterintuitive, because having a large number of malicious nodes would seem to strengthen active attacks. However, this is not true, because in this case, the dominant contribution to the secrecy throughput is via single-hop transmissions from sources to destinations directly, which avoid active attacks in the first place. The difference between the models under passive and active attacks lies in the case when the number of malicious nodes is small. In this case, the dominant contribution to the secrecy throughput is via two-hop transmissions, during which malicious nodes may send modified packets to destinations. Therefore, to guarantee the same throughput as the model under passive attacks, the model under active attacks needs to satisfy a more stringent condition on the number of malicious nodes.

VII. Conclusion

In this paper, we have studied the secrecy throughput of MANETs with malicious nodes under both passive attacks and active attacks. For the model with passive attacks, we have modeled communication in MANETs by the erasure wiretap channel, and have applied the secrecy capacity of the wiretap channel to characterize the secrecy throughput for MANETs. We have then explored secure coding design for the erasure wiretap channel to construct secure communication algorithms to achieve the optimal secrecy throughput. For the model under active attacks in addition to passive attacks, we have modeled communication in MANETs by the BSEC wiretap channel, and obtained the secrecy throughput via an approach similar to the model under passive attacks. We have also compared the secrecy throughput of the two models, and discussed the connections and differences between the two.

In this paper, we have considered a simple mobility model: the 2-D i.i.d. mobility model, in which the nodes are independently reshuffled at the beginning of each time slot. This mobility model assumes that the mobiles move fast enough such that they can move from one location to any other location in one time slot. This simple mobility model enables us to connect network transmissions under security constraints to an equivalent discrete memoryless wiretap channel in order to quantify the scaling behavior of the secrecy throughput. One future research problem of interest is to investigate the secrecy throughput of more realistic mobility models such as the random walk model and the random waypoint model. The approach adopted in this paper may be applicable for these models if correlation in mobility models decays as time increases so that a block-memoryless wiretap channel may be a good approximation. Alternatively, more complicated wiretap models may need to be developed for studying these more realistic mobility models.

Appendix
Proof of Lemma 1

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

$$m < \pi L^2 n D. \tag{14}$$

To further analyze $C_{s,\text{II}}$, we first note that

$$\left(1 - \frac{1}{n}\right)^{f(n)} \rightarrow \begin{cases} 1 - \dfrac{f(n)}{n}, & \text{if} \lim_{n\rightarrow\infty} f(n)/n = 0 \\ e^{-\dfrac{f(n)}{n}}, & \text{if} \lim_{n\rightarrow\infty} f(n)/n \geq A \end{cases}$$

where A is a positive constant.

Assuming inequality (14) holds and defining

$$C(L) = \frac{1}{\pi n L^2} \left(\left(1 - \pi L^2\right)^m - \left(1 - \pi L^2\right)^{\pi L^2 n D} \right)$$

we evaluate $C(L)$ for the following three cases:

Case 1) $\left(\pi L^2\right)^2 nD = o(1)$, which implies that $\pi L^2 m = o(1)$ due to (14). We then obtain

$$C(L) \approx \frac{1}{n} \left(\pi L^2 n D - m \right).$$

Case 2) $\left(\pi L^2\right)^2 nD = \Omega(1)$ and $\pi L^2 m = o(1)$. We obtain

$$C(L) \approx \frac{1}{\pi n L^2} \left(1 - \pi L^2 m - e^{-\left(\pi L^2\right)^2 nD} \right).$$

Case 3) $\pi L^2 m = \Omega(1)$, which implies that $(\pi L^2)^2 nD = \Omega(1)$. We obtain

$$C(L) \approx \frac{1}{\pi n L^2}\left(e^{-\pi L^2 m} - e^{-\left(\pi L^2\right)^2 nD}\right).$$

It can be shown that if $m = O\left(\sqrt{nD}\right)$, then all of the above three cases are feasible and the secrecy throughput is given by

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

Otherwise, if $m = \omega\left(\sqrt{nD}\right)$, then only Case 3 is feasible, and the secrecy throughput is given by

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

References

[1] L. Ying, S. Yang, and R. Srikant, "Optimal delay-throughput tradeoffs in mobile ad hoc networks," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4119–4143, Sep. 2008.

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

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[4] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, no. 4–5, pp. 355–580, 2008.

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

[6] A. Thangaraj, S. Dihidar, A. Calderbank, S. McLaughlin, and J.-M. Merolla, "Application of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

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

[8] S. N. Diggavi, M. Grossglauser, and D. Tse, "Even one-dimensional mobility increases ad hoc wireless capacity," in *Proc. IEEE Int. Symp. Inf. Theory*, Palais de Beaulieu, Lausanne, Switzerland, 2002, DOI: 10.1109/ISIT.2002.1023624.

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

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

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

[12] A. El Gamal, J. Mammen, B. Prabhakar, and D. Shah, "Optimal throughput-delay scaling in wireless networks—Part I: The fluid model," *IEEE Trans. Inf. Theory*, vol. 52, no. 6, pp. 2568–2592, Jun. 2006.

[13] A. El Gamal, J. Mammen, B. Prabhakar, and D. Shah, "Optimal throughput-delay scaling in wireless networks—Part II: Constant-size packets," *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 5111–5116, Nov. 2006.

[14] G. Sharma, R. Mazumdar, and N. Shroff, "Delay and capacity tradeoffs in mobile ad hoc networks: A global perspective," in *Proc. IEEE INFOCOM*, Bacelona, Catalunya, Spain, Apr. 2006, DOI: 10.1109/INFOCOM.2006.144.

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

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

[17] S. Zhou and L. Ying, "On delay constrained multicast capacity of large-scale mobile ad-hoc networks," in *Proc. IEEE INFOCOM Mini-Conf.*, San Diego, CA, Apr. 2010, DOI: 10.1109/INFCOM.2010.5462257.

[18] O. O. Koyluoglu, C. E. Koksal, and H. El Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, Apr. 2010, submitted for publication.

[19] O. O. Koyluoglu, C. E. Koksal, and H. El Gamal, "On the effect of colluding eavesdroppers on secrecy capacity scaling," in *Proc. Eur. Wireless Conf.*, Lucca, Italy, 2010, pp. 790–795.

[20] P. C. Pinto, J. Barros, and M. Z. Win, "Wireless physical-layer security: The case of colluding eavesdroppers," in *Proc. IEEE Int. Symp. Inf. Theory*, Seoul, Korea, 2009, pp. 2442–2446.

[21] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks," 2010 [Online]. Available: arXiv:1001.3697, to be published

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

[23] U. M. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Advances in Cryptology-Eurocrypt 2000*, ser. Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, May 2000, pp. 351–368.

Yingbin Liang (S'01–M'05) received the Ph.D. degree in electrical engineering from the University of Illinois at Urbana-Champaign, Urbana, in 2005.

In 2005–2007, she was working as a Postdoctoral Research Associate at Princeton University, Princeton, NJ. In 2008–2009, she was an Assistant Professor at the Department of Electrical Engineering, University of Hawaii. Since December 2009, she has been an Assistant Professor at the Department of Electrical Engineering and Computer Science, Syracuse University, Syracuse, NY. Her research interests include communications, wireless networks, information theory, and machine learning.

Dr. Liang was a Vodafone Fellow at the University of Illinois at Urbana-Champaign during 2003–2005, and received the Vodafone-U.S. Foundation Fellows Initiative Research Merit Award in 2005. She also received the M. E. Van Valkenburg Graduate Research Award from the Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, in 2005. In 2009, she received the National Science Foundation CAREER Award, and the State of Hawaii Governor Innovation Award.

H. Vincent Poor (S'72–M'77–SM'82–F'87) received the Ph.D. degree in electrical engineering and computer science from Princeton University, Princeton, NJ, in 1977.

From 1977 until 1990, he was on the faculty of the University of Illinois at Urbana-Champaign, Urbana. Since 1990, he has been on the faculty at Princeton, where he is the Dean of Engineering and Applied Science, and the Michael Henry Strater University Professor of Electrical Engineering. His research interests are in the areas of stochastic analysis, statistical signal processing and information theory, and their applications in wireless networks and related fields. Among his publications in these areas are *Quickest Detection* (Cambridge Univ. Press, 2009), coauthored with O. Hadjiliadis, and *Information Theoretic Security* (Now Publishers, 2009), coauthored with Y. Liang and S. Shamai.

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, in 2004–2007 as the Editor-in-Chief of the these TRANSACTIONS, and in 2009 as General Co-Chair of the IEEE International Symposium on Information Theory, held in Seoul, South Korea. He received a Guggenheim Fellowship in 2002 and the IEEE Education Medal in 2005. Recent recognition of his work includes the 2010 IET Ambrose Fleming Medal for Achievement in Communications, the 2011 IEEE Eric E. Sumner Award, the 2011 IEEE Information Theory Paper Award, and an honorary D.Sc. from the University of Edinburgh, conferred in 2011.

Lei Ying (M'08) received the B.E. degree from Tsinghua University, Beijing, China, in 2001 and the M.S. and Ph.D. degrees in electrical engineering from the University of Illinois at Urbana-Champaign, Urbana, in 2003 and 2007, respectively.

During fall 2007, he worked as a Postdoctoral Fellow at the University of Texas at Austin, Austin. He is currently an Assistant Professor at the Department of Electrical and Computer Engineering, Iowa State University, Ames. His research interest is broadly in the area of information networks, including wireless networks, mobile *ad hoc* networks, P2P networks, and social networks.

Dr. Ying received a Young Investigator Award from the Defense Threat Reduction Agency (DTRA) in 2009, NSF CAREER Award in 2010, and is named The Northrop Grumman Assistant Professor (formerly the Litton Industries Assistant Professor) at the Department of Electrical and Computer Engineering at Iowa State University for 2010–2012.