Minimizing Eavesdropping Risk by Transmission Power Control in Multihop Wireless Networks

Jung-Chun Kao, *Student Member*, *IEEE*, and Radu Marculescu, *Member*, *IEEE*

Abstract—To defend against reconnaissance activity in ad hoc wireless networks, we propose transmission power control as an effective mechanism for minimizing the eavesdropping risk. Our main contributions are given as follows. First, we cast the wth-order eavesdropping risk as the maximum probability of packets being eavesdropped when there are w adversarial nodes in the network. Second, we derive the closed-form solution of the first-order eavesdropping risk as a polynomial function of the normalized transmission radius. This derivation assumes a uniform distribution of user nodes. Then, we generalize the model to allow *arbitrary* user nodes distribution and prove that the uniform user distribution minimizes the first-order eavesdropping risk. This result plays an essential role in deriving analytical bounds for the eavesdropping risk given *arbitrary* user distributions. Our simulation results show that, for a wide range of *nonuniform* traffic patterns, the difference in their eavesdropping risk values from the corresponding lower bounds is 3 dB or less.

Index Terms—Wireless network security, transmission power control, wireless ad hoc networks.

1 Introduction

An ad hoc wireless network consists of a collection of autonomous nodes, all capable of transmitting and receiving packets. Such a network can operate in a standalone fashion (with the ability of self-configuration) or can connect to the Internet. Minimal configuration time and quick deployment make ad hoc networks suitable for emergency situations like natural or human-induced disasters, military conflicts, emergency situations, and so forth. In addition, the migration of wireless networks from hot spots to multihop ad hoc networks is an important step toward self-organized global routing [1], [2].

During data transmission, a node dissipates a finite amount of energy to send packets over wireless channels. Due to the existence of noise and interference in the wireless environment (for example, the signal-to-interference-plus-noise ratio), the *transmission range* cannot be infinitely large. A node can receive a packet only if it is located within the transmission range of the sending node.

Although most of the autonomous nodes in an ad hoc network are *user nodes*, *adversarial nodes* may also exist. If an adversarial node intercepts the transmitted packets, it can attack the network and produce damage, depending on the actual information contained in the eavesdropped packets. In fact, according to US-CERT, reconnaissance activity is the most frequent incident on computer networks since 2002 [3] and many attacks (including DoS attacks and unauthorized access incidents) are preceded by reconnaissance activity [4].

• *The authors are with the Department of Electrical and Computer Engineering, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213-3890. E-mail: {jckao, radum}@cmu.edu.*

Manuscript received 13 Nov. 2006; revised 1 Apr. 2007; accepted 12 Apr. 2007; published online 30 Apr. 2007.
For information on obtaining reprints of this article, please send e-mail to: tc@computer.org, and reference IEEECS Log Number TC-0433-1106.
Digital Object Identifier no. 10.1109/TC.2007.1066.

Reconnaissance activity can be classified into active scanning and passive eavesdropping. Scanning activity may perform port scanning and probing, looking for vulnerable services to attack or ways to gain a detailed map of available hosts and open ports. Firewalls, intrusion-detection systems, and early warning systems (for example, Recon [5]) can usually detect the scanning activity. On the contrary, the eavesdropping activity is *not* detectable. It is important to note that the information gathered from the eavesdropped packets (for example, identity and privacy information) can be of critical importance since it can be used later to compromise the network by identifying potential victims, conducting target-specific attacks, or breaking the cryptographic key in use. Such follow-up attacks (referred to as *hear-and-fire attacks*) result in what we call *eavesdropping risk*.

Eavesdropping risk causes a more severe security problem in ad hoc wireless networks compared to single-hop wireless networks or fixed wired networks. Indeed, due to the absence of an underlying communication infrastructure, the source and destination nodes in ad hoc wireless networks heavily rely on the intermediate nodes to relay their data. This makes the nodes more susceptible to attacks based on the information contained in the eavesdropped packets.

The existing defense mechanisms against the hear-and-fire attacks in ad hoc wireless networks can be categorized into cryptographic techniques, secure routing, and anonymous routing. Recent research on cryptographic techniques [6] focuses on developing a robust efficient cryptosystem for protecting the data confidentiality under resource constraints. Important issues in designing such cryptosystems include key management [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], authentication [18], hash functions, and encryption/decryption algorithms [19].

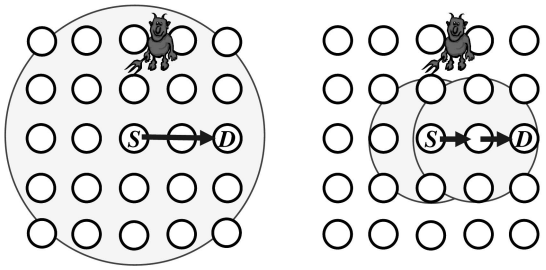


Fig. 1. An example illustrating that controlling the transmission range helps reduce the probability of a packet being eavesdropped. (a) The case when a packet is transmitted using the maximum transmission range. Due to its location within the transmission range, the adversary can eavesdrop the packet. On the contrary, the adversary in (b) (where the packet is forwarded via multiple hops at small transmission range) cannot sniff the packet since this adversary lies outside any transmission range.

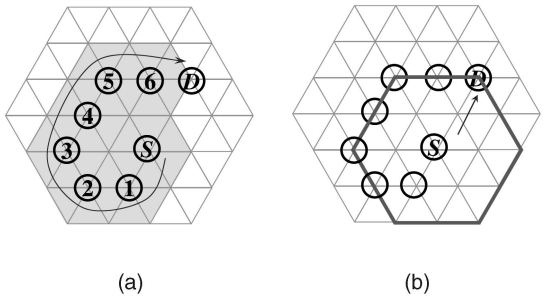


Fig. 2. A counterexample disproving the intuition that minimizing transmission power always reduces the probability of a packet being eavesdropped. When a packet is sent from node S to node D at minimum transmission power (say, the transmission radius $R = 1$), it is relayed via nodes $1, 2, \ldots, 6$ and an adversary residing in the green shadow can eavesdrop the packet. When the transmission radius is doubled (that is, $R = 2$), the packet arrives at the destination directly and an adversary can intercept the packet only if it resides in the red hexagon. The ratio of these two areas is 30:24, which is contrary to the intuition described above. For clarity reasons, we use triangle cells (equivalently, the *hexagonal* transmission range), but the same idea can be illustrated with the circular or square transmission ranges.

These cryptographic techniques facilitate the design of secure and anonymous routing protocols in the presence of adversarial nodes. The adversarial nodes may compromise the network operation by exhibiting a *Byzantine* behavior [20] while being able to corrupt, replay, and fabricate the routing packets. A secure routing protocol (for example, [21]) is one that not only ensures data confidentiality but also prevents the attacks mounted by the adversarial nodes from disrupting the connections between source-destination $(S\text{-}D)$ pairs.

Conceptually, anonymous routing can be regarded as an extension of secure routing. In addition to guaranteeing successful data transmission from source to destination in the presence of adversarial nodes, an anonymous routing protocol in a loose sense (for example, [22], [23], [24]) needs to preserve identity privacy. In a strict sense, an anonymous routing protocol requires preserving identity privacy, location privacy, and route anonymity (see [25] for the definitions of these three terms).

Unlike previous cryptography-based work that causes high overhead in terms of processing delay [22], packet size [26], and energy consumption [27], we propose the use of transmission power control as an effective mechanism for improving the network security. This security improvement is achieved by decreasing the *eavesdropping risk* probability. The basic idea is to adapt the transmission range in a way that helps to reduce sniffing. More precisely, as illustrated in Fig. 1, instead of directly sending a packet from source to destination using the maximum transmission range, a better way that makes the adversaries less likely to eavesdrop the packet is to forward the packet via multiple hops, each of them using a smaller transmission range.

However, assessing the impact of transmission power control on the eavesdropping risk is *not* a trivial problem. The simple intuition that using the smallest transmission power minimizes the probability of a random packet being eavesdropped is *not* true in general. Indeed, the actual distribution of user nodes has a significant impact on how a transmission power control scheme affects the eavesdropping risk. Contrary to Fig. 1, which shows that, given the uniform user distribution, using minimum transmission range makes an adversary less likely to sniff the transmitted packet, Fig. 2 shows a counterexample where sending a packet at the minimum transmission power actually makes it easier for an adversary to intercept the transmitted packet; this is due to the long detour during packet transmission.

By mentioning the complex nature of transmission power control on a *single packet*, we point out the inherent difficulty of investigating the impact of transmission power control on the *entire network* in terms of eavesdropping risk. This leads to the need for a rigorous analysis since intuitive explanations are insufficient and may appear contradicting to each other.

In practice, the power amplifiers used in commercial transceivers—even those designed for short-range and low-power communication standards like Bluetooth [28] and ZigBee [29]—have the capability of controlling the output power. This transmission power control capability is necessary for connectivity and energy conservation, but, at the same time, this provides an opportunity for improving the network security.

Our proposal for transmission power control for security improvement has beneficial side effects on throughput, energy conservation, and quality-of-service support. At the same time, the techniques targeting the network performance improvement (for example, [30], [31], [32], [33], [34], [35], [36], [37]) usually also reduce the eavesdropping risk. This is because the techniques that improve spatiotemporal reuse of wireless channels usually help to reduce interference and transmission power, and vice versa. For example, the COMPOW protocol [36], which transmits packets at the lowest possible power for throughput purposes, actually enhances the network security, in a statistical sense, according to our quantitative analysis.

As the main theoretical contribution, we analyze the impact of transmission power control on the eavesdropping risk as follows:

- First, given an arbitrary geographical distribution of user nodes, we define the $w\text{th-order}$ eavesdropping risk as the maximum probability of packets being

eavesdropped when there are w adversarial nodes in the ad hoc wireless network. The eavesdropping risk is defined as a "maximum" probability because we assume that the adversarial nodes are able to move around for maximizing the probability of listening to packets transmitted over the wireless channels.

- Second, in order to simplify the multiple access control problem, we use the unit torus model that is a generalization of El Gamal et al.'s model [38].[1] Similarly to El Gamal et al.'s model, our model is able to capture the geographical structure and interference properties of the ad hoc wireless networks. Under the unit torus model, we consider a random network of uniformly distributed nodes and then derive a closed-form solution of the first-order eavesdropping risk as a function of the transmission radius.
- Finally, we generalize the user distribution to allow for *arbitrary* distributions and study their impact on the eavesdropping risk. To this end, we prove that the uniform user distribution minimizes the first-order eavesdropping risk. Therefore, the uniform user distribution represents the *best-case scenario* for reducing the eavesdropping risk. As shown later in this paper, the best-case analysis not only helps future security research based on power-controlled topology synthesis in ad hoc wireless networks but also plays a crucial role in deriving the first known bounds for the eavesdropping risk.

The remainder of this paper is organized as follows: In Section 2, we formulate the problem of eavesdropping risk. We present analytical results on the relationship between transmission power control and the eavesdropping risk in Section 3 and simulation results in Section 4. Finally, in Section 5, we present some concluding remarks.

2 The Eavesdropping Risk Problem

The main objective of this section is to formulate the eavesdropping risk problem in ad hoc wireless networks. To this end, we first introduce the model of the parameterized cell-partitioned unit torus, abbreviated as the *unit torus model*. This model is a generalization of El Gamal et al.'s model proposed in [38] in the sense that the user nodes can be *arbitrarily distributed*; it also allows the use of *directional* antennas.

2.1 The Unit Torus Model

As shown in Fig. 3, the network region described as a parameterized cell-partitioned unit torus is divided into several cells. A cell is a square of area $a(n)$ containing a set of distinct nodes, where n is the total number of user nodes. The user nodes can be arbitrarily distributed as long as each cell in the unit torus has at least one user node, thus guaranteeing successful transmission. Each user node has a randomly chosen destination. Each cell can support at most one active link transmission per time slot and a node can only transmit (or listen) to the nodes within the same cell or in its adjacent cells.

1. Similar models are used for investigating other important issues (for example, network capacity, delay, power/rate allocation, energy minimization, and coverage) in [38], [39], [40], [41], [42].

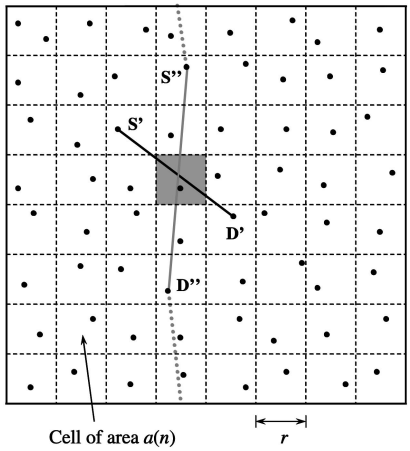


Fig. 3. As in El Gamal et al.'s model, the unit torus is divided into cells of size $a(n)$. Several S-D lines passing through the shaded cell are shown using solid lines.

Unlike El Gamal et al.'s model, which assumes that the packets are transmitted omnidirectionally, we allow the directional broadcast mode. In practice, all antennas have directional properties and, therefore, they do not radiate power in all directions equally. For example, a typical Yagi antenna radiation pattern is drawn in Fig. 4 (reproduced from [43]), which contains a main lobe and several side lobes. Figs. 5a and 5b illustrate that, for a directional broadcast to either an orthogonally neighboring cell or a diagonally neighboring cell, it is reasonable to assume that only the nodes within the cell(s) where either the transmitter or receiver resides can hear the directional broadcast.

Therefore, one can define the *normalized transmission range* as the cell area $a(n)$ and the *normalized transmission radius* $r = \sqrt{a(n)}$ as the square root of the transmission range.[2] Note that both the normalized transmission range and normalized transmission radius are fractional numbers in the interval $(0, 1]$. The extreme case, $a(n) = 1$, corresponds to a configuration in which any node can reach all other nodes directly.

We assume that the packets originating from the source nodes always *pass through* the route(s) with the least number of hops when traveling toward their destinations. For instance, the S′-D′ pair in Fig. 3 is two hops away, whereas the S″-D″ pair is four hops away. It is possible to have multiple routes with the smallest hop count between any S-D pair. For example, the solid and the dotted routes between the S″-D″ pair have the same number of hops. In such a case, a route is randomly chosen with an equal probability ρ. Hence, the probability of the S′-D′ pair passing through the shaded cell in Fig. 3 is $\rho = 1$, whereas the probability of the S″-D″ pair passing through the shaded cell is $\rho = 1/2$.

2.2 Problem Formulation

A packet will be eavesdropped if and only if it passes through cells where adversarial nodes reside. An S-D pair

2. Other possible definitions can make the normalized transmission range a multiple of the cell area and the normalized transmission radius a multiple of the square root of the transmission range.

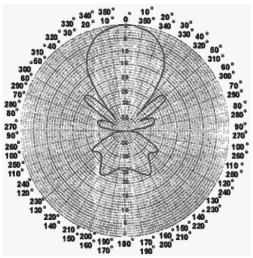


Fig. 4. This is a polar plot of the 10-element Yagi antenna and shows the side lobes of the antenna relative to the main beam in decibels (from [43]).

may be eavesdropped in cell i if and only if there is an adversarial node located in cell i and the S-D pair passes through cell i with a probability greater than zero. In general, the probability that an S-D pair passes through a certain cell can be 0, 1, or a fraction between 0 and 1. This is because, although an S-D pair can have multiple routes with a minimal number of hops, only a few of these routes may actually pass through cell i.

Now, we give the definitions of the passing volume and the probability of packets being eavesdropped.

Definition 1. *Given an arbitrary user/adversary distribution, the* probability of packets being eavesdropped *is defined as the number of packets that pass through any of the cells with one (or more) adversarial node divided by the total number of (originating) packets.*

Definition 2. *Given an arbitrary user/adversary distribution, the* passing volume *is defined as the probability of packets being eavesdropped multiplied by the number of S-D pairs.*

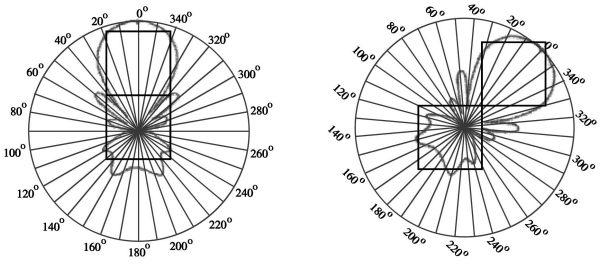
Proposition 1. *If the traffic volume of all S-D pairs follows a common distribution (for example, Gaussian, exponential, and so forth), then the passing volume is equal to the sum of probabilities of the S-D pairs passing through any of the cells with adversarial node(s).*

We note that the adversarial nodes are allowed to move around in order to maximize the traffic volume they can eavesdrop. Since each S-D pair is assumed to have an identical traffic pattern in a statistical sense, maximizing the eavesdropped traffic volume then becomes equivalent to maximizing the probability of packets being eavesdropped; this, in turn, is equivalent to maximizing the probability of S-D pairs being eavesdropped. This equivalence relationship allows us to define the wth-*order eavesdropping risk problem* as follows:

Given *an arbitrary user distribution and w adversarial nodes present in an ad hoc wireless network,* ***find*** *the adversary distribution such that the probability of packets being eavesdropped is maximized.*

Definition 3. *Given an arbitrary user distribution, the* wth eavesdropping risk *is defined as the maximum probability of packets being eavesdropped for all possible distributions of w adversarial nodes in an ad hoc wireless network.*

Definition 4. *Given an arbitrary user distribution, the* wth-order eavesdropping volume *is defined as the wth-order eavesdropping risk multiplied by the number of S-D pairs.*



(a) (b)

Fig. 5. This figure shows that, for a directional broadcast to a node in any neighboring cell, it is reasonable to assume that only the nodes within the cell(s) in which either the transmitter or receiver resides can hear the directional broadcast. (a) The directional broadcast to one of the four orthogonally nearest cells. (b) The directional broadcast to one of the four diagonally nearest cells.

Proposition 2. *If the traffic volume of all S-D pairs follows a common distribution, then the wth-order eavesdropping volume is equal to the maximum passing volume for all possible distributions of w adversarial nodes in an ad hoc wireless network.*

One should note that the larger the wth-order eavesdropping risk is, the more likely the adversarial nodes eavesdrop the packets transmitted over the wireless channels. Whereas the adversarial nodes are able to move around in order to maximize the eavesdropping risk, for security concerns, the user nodes tend to minimize the eavesdropping risk by relying on some basic defense mechanisms. For example, two such mechanisms for reducing the eavesdropping risk are transmission power control and topology optimization.

Although of potential interest, physical-layer techniques (for example, frequency hopping and spread spectrum communication) are not considered in this paper. These techniques do not improve the network security under the assumption that, compared to a user node, an adversarial node uses an identical transceiver and has better computational capabilities. Routing may help reduce the eavesdropping risk, but the complexity of optimizing a routing algorithm is exponential. Therefore, in this paper, we focus on the analysis of the transmission range.

3 Analytical Results

The main objective of this section is to analyze the impact of transmission power control on the eavesdropping risk. Our approach is described as follows: We first consider a uniform distribution of user nodes, which is a common assumption [38], [39], [44], [45] in ad hoc wireless networks, and derive the closed-form solution for the first-order eavesdropping risk as a function of the *normalized transmission radius*. This uniform case is then generalized to allow for *arbitrary* node distributions. We prove that the result derived for the uniform case provides a lower bound for such general scenarios. The tightness of this lower bound will be investigated later, in Section 4, by simulations over a

wide range of traffic patterns and a wide range of node distributions.

3.1 Uniform Distribution of User Nodes

Theorem 1 below gives the closed-form formula of the first-order eavesdropping risk when user nodes are uniformly deployed.

Theorem 1. *In a random network consisting of n nodes distributed independently and uniformly over a unit torus whose normalized transmission radius is r, the first-order eavesdropping risk is given as follows:*

1. *If s is odd, then the first-order eavesdropping risk is $R_1^*(r) = \frac{s^2+3s-1}{3s^3} = \frac{1}{3}r + r^2 - \frac{1}{3}r^3$ and*
2. *if s is even, then the first-order eavesdropping risk is $R_1^*(r) = \frac{s^2+3s+\frac{1}{2}}{3s^3} = \frac{1}{3}r + r^2 + \frac{1}{6}r^3$,*

where $s = 1/r$ is the number of cells along a single edge of the unit torus.

Proof. Consider an arbitrary S-D pair, say, S-D pair j, where $1 \le j \le n(n+1)/2$.[3] Let H_j and D_j be the number of hops and the displacement between S-D pair j, respectively. The displacement is defined as $D_j = 0$ if the two ends of S-D pair j are within the same cell; otherwise, the displacement is equal to the hop count, that is, $D_j = H_j$. Define the Bernoulli random variables Y_j^h for any hop h, $0 \le h \le H_j$, to be equal to 1 if and only if hop h of S-D pair j ends at a cell where an adversarial node resides.[4] Note that, for all $h' \neq h$ $(1 \le h', h \le H_j)$, the event $Y_j^{h'} = 1$ is mutually exclusive to the event $Y_j^h = 1$; this is because a single adversarial node cannot reside in two cells. Define the random variable Y_j as $Y_j^0 + \sum_{h=1}^{D_j} Y_j^h$. Due to mutual exclusion, the event $Y_j = 1$ is equivalent to the event that S-D pair j is eavesdropped by the adversarial node. Therefore, the (conditional) probability that S-D pair j is eavesdropped, given its displacement D_j, is

$$\begin{aligned}\mathbf{E}[Y_j|D_j] &= \mathbf{E}\left[Y_j^0 + \sum_{h=1}^{D_j} Y_j^h \Big| D_j\right] \\ &= \sum_{h=0}^{D_j} \mathbf{E}[Y_j^h] = (D_j+1)\cdot\mathbf{E}[Y_j^1] = (D_j+1)\cdot a(n),\end{aligned} \tag{1}$$

where the third equality follows from the fact that, due to the symmetry of the torus, each hop of an S-D pair is equally likely to end at the cell in which an adversarial node resides.

Note that, since the user nodes are randomly deployed with uniform distribution, the conditional probabilities $Y_j|D_j$s, $1 \le j \le n(n+1)/2$, are identically distributed. Since S-D pair j is arbitrarily chosen, the first-order eavesdropping risk $R_1^*(r)$ is equal to the (unconditional) probability of S-D pair j being eavesdropped:

$$\begin{aligned}R_1^*(r) &= \mathbf{E}[Y_j] = \mathbf{E}_{D_j}[\mathbf{E}[Y_j|D_j]] \\ &= \mathbf{E}_{D_j}[(D_j+1)\cdot a(n)] = a(n)\cdot(\mathbf{E}[D_j]+1),\end{aligned} \tag{2}$$

where the third equality follows from (1).

The only thing left to complete this proof is to find the value of $\mathbf{E}[D_j]$. We calculate $\mathbf{E}[D_j]$ as follows:

1. When s is odd, the probability that the displacement associated with S-D pair j is d is[5]

$$\Pr(D_j = d) = \begin{cases} \frac{1}{s^2} & \text{if } d = 0 \\ \frac{8d}{s^2} & \text{if } d = 1, 2, \ldots, \frac{s-1}{2} \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, the expectation of D_j is

$$\mathbf{E}[D_j] = \sum_{d=0}^{\frac{s-1}{2}} d\cdot\Pr[D_j = d] = \frac{s^2-1}{3s}.$$

By using (2), the eavesdropping risk is

$$R_1^*(r) = a(n)\cdot(\mathbf{E}[D_j]+1) = \frac{s^2+3s-1}{3s^3}. \tag{3}$$

2. When s is even, similarly to the odd case, we get

$$\Pr(D_j = d) = \begin{cases} \frac{1}{s^2} & \text{if } d = 0 \\ \frac{8d}{s^2} & \text{if } d = 1, 2, \ldots, \frac{s}{2}-1 \\ \frac{2s-1}{s^2} & \text{if } d = \frac{s}{2} \\ 0 & \text{otherwise,} \end{cases}$$

$$\mathbf{E}[D_j] = \frac{s^2+\frac{1}{2}}{3s},$$

and

$$R_1^*(r) = \frac{s^2+3s+\frac{1}{2}}{3s^3}. \tag{4}$$

By substituting s with $1/r$ in both (3) and (4), we prove this theorem. □

3.2 Arbitrary Distribution of User Nodes

The next step is to generalize the node distribution and allow for *arbitrary* distributions. In this section, we prove that the results provided in Theorem 1 actually serve as lower bounds for *arbitrary* distributions of user nodes. This implies that the uniform case represents the best-case scenario of the eavesdropping problem.

Before delving into details, it is important to note that the following naive justification of the best case scenario—if the distribution of the users is not uniform, then the attacker(s) will go to the most crowded cell(s) to intercept the highest volume of communication and, therefore, the uniform distribution of user nodes minimizes the eavesdropping risk—is simply wrong. Fig. 6 shows a counterexample of why this intuition is wrong. Assume that there are $2m$ user nodes residing in each dark-gray cell, m user nodes in each light-gray cell, and 0 user node in other cells. By this intuition, the attacker maximizes the eavesdropping

3. The destination node is allowed to be the source node. Therefore, the total number of S-D pairs is $n(n-1)/2 + n = n(n+1)/2$.

4. Although hop 0 does not exist physically, we define that hop 0 ends at the source node.

5. Without loss of generality, $\Pr(D_j = d)$ can be computed by assuming that the source node is given. The total number of cells in the unit torus is s^2. In order to have a displacement of d, where $d = 1, 2, \ldots, \frac{s-1}{2}$, the destination node must reside in one of $(2d+1)^2 - (2d-1)^2 = 8d$ cells. Therefore, $\Pr(D_j = d) = 8d/s^2$.

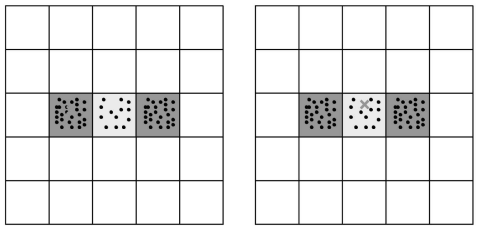


Fig. 6. A counterexample to disprove the naive intuition that the reason for uniform user distribution minimizing the eavesdropping risk is because otherwise the attacker will go to the most crowded cell to intercept the most communication.

volume (in terms of the number of S-D pairs eavesdropped by the adversarial node) by moving to a dark-gray cell. However, in doing so, the first-order eavesdropping volume $(2m)^2/2 + (2m)(m+2m) = 8m^2$ is *not* maximal because an attacker residing in a light-gray cell can eavesdrop $m^2/2 + m(4m) + (2m)(2m) = 8.5m^2$ S-D pairs.[6] This shows that we need a rigorous proof, as given below for Theorem 3.

As we discuss later, the eavesdropping risk problem given an arbitrary node distribution is very complex from a mathematical point of view. Even the (simplest) first-order eavesdropping risk has the form of a min-max formula consisting of a large number of quadratic multivariable polynomials. For clarity, we present the proof in the following manner: We first study the corresponding problem using 1D torus, instead of dealing with the ordinary 2D torus directly. The proof consists of a combination of algebraic and geometric techniques. With minimal modifications, these techniques can be also applied to the 2D torus.

3.2.1 Notation

To give a rigorous proof, we first introduce a few terms defined over a unit torus. Consider a network consisting of n user nodes and w adversarial nodes. The network is modeled by the unit torus model and partitioned into cells of area $a(n)$. Let us number the cells $0, 1, \ldots, k-1$ in a left-to-right and, then, top-to-bottom manner, where $k = 1/a(n)$ is the total number of cells in the network.

A *user distribution* is denoted by the k-tuple $N = (n_0, n_1, \ldots, n_{k-1})$, where n_i, $0 \le i \le k-1$, is the number of user nodes located in cell i. Define $\mathbb{N}_n^k$ as the set of all k-tuples of natural numbers (excluding 0) whose k components sum up to n. Because n user nodes are distributed over k cells and each cell has at least one user node, N is a valid user distribution if and only if $N \in \mathbb{N}_n^k$.

Similarly, we can denote an *adversary distribution* by the k-tuple $W = (w_0, w_1, \ldots, w_{k-1})$, where w_i is the number of adversarial nodes located within cell i. Note that, under the unit torus model, multiple adversarial nodes within a cell cannot eavesdrop more S-D pairs than a single adversarial node in the same cell. Therefore, for any cell i, w_i is set to either 0 or 1.

The *normalized user distribution* $X = (x_0, x_1, \ldots, x_{k-1})$ is defined as $x_i = n_i/n$ for $0 \le i \le k-1$. The property of x_is summing up to 1 implies that $X \in \mathbb{F}_1^k$, where $\mathbb{F}_1^k$ is defined as the set of all k-tuples of fractional numbers in $(0, 1)$ whose k components sum up to 1.

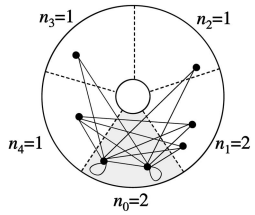


Fig. 7. An example of the 1D torus, which is topologically a ring. In this example, the ring is partitioned into $k = 5$ segments, each represented by a fan-shaped sector. n_i is the number of user nodes in segment i. All of the S-D pairs passing through segment 0 (the shaded one) are drawn as lines or self-loops. If the adversarial node resides in segment 0, it can hear all of these communications passing through segment 0.

Given a specific user distribution N (and, thus, k), the wth-order eavesdropping risk and the wth-order eavesdropping volume are denoted by $R_w^X(k)$ and $V_w^N(k)$, respectively. When the user distribution is not specified but n and k are given, the *best-case scenario* is defined as the user distribution that minimizes the eavesdropping risk without any prior knowledge of the adversary distribution. We denote the wth-order eavesdropping risk for the best-case scenario by $R_w^*(k)$ without explicitly showing the parameter n. Similarly, we also denote the wth-order eavesdropping volume for the best-case scenario by $V_w^*(k)$.

3.2.2 Eavesdropping Risk for the 1D Torus

A 2D torus can be constructed from a rectangle by gluing the opposite edges together. Observing a torus only along one dimension, say, the x-axis, makes the 2D torus degenerate into a 1D torus that is, topologically speaking, a ring. We note that a segment on the ring corresponds to a cell in the ordinary torus. The remaining terminology defined over a ring (for example, passing volume, probability of packets being eavesdropped, eavesdropping risk, and so forth) is based on definitions similar to the ones used for the ordinary 2D torus. By analogy with the torus model, the nodes on a ring can only transmit packets to the nodes on the same segment or adjacent segments.

We illustrate the first-order eavesdropping risk problem over a ring by using a simple example shown in Fig. 7. Consider a ring consisting of five segments ($k = 5$) and a set of user nodes with the geographical distribution $N = (n_0, n_1, n_2, n_3, n_4)$. If the adversarial node is located on segment 0, then the passing volume is $n_0(n - n_0) + \binom{n_0}{2} + \binom{n_0}{1} + n_1 n_4 = n_0 n - \frac{1}{2}n_0^2 + \frac{1}{2}n_0 + n_1 n_4$. [7] All of the S-D pairs that pass through segment 0 in this example are drawn in Fig. 7 as lines or self-loops. Similarly, we can get the respective passing volumes when the adversarial node resides on segments 1, 2, 3, and 4. Because the adversarial node is able to detect the user distribution, it will move to some segment such that the passing volume is maximized. Therefore, the first-order eavesdropping volume is calculated as the maximum over the five passing volumes:

6. For simplicity of exposition, we only present the highest-order terms.

7. We assume here that the source node can transmit packets to itself.

$$V_1^N(5) = \max\Big(n_0 n - 0.5n_0(n_0-1) + n_1 n_4,\; n_1 n - 0.5n_1(n_1-1) + n_2 n_0,\; n_2 n - 0.5n_2(n_2-1) + n_3 n_1,\; n_3 n - 0.5n_3(n_3-1) + n_4 n_2,\; n_4 n - 0.5n_4(n_4-1) + n_0 n_3\Big).$$

The best-case scenario is the case when the user distribution minimizes the first-order eavesdropping volume without any knowledge of the precise locations of adversarial nodes. Therefore, for this simple example, one can express the first-order eavesdropping volume under the best-case scenario as

$$V_1^*(5) = \min_{N\in\mathbb{N}_n^5} \max\Big(n_0 n - 0.5n_0(n_0-1) + n_1 n_4, n_1 n - 0.5n_1(n_1-1) + n_2 n_0, \ldots, n_4 n - 0.5n_4(n_4-1) + n_0 n_3\Big).$$

As shown above, even for such a simple example, the first-order eavesdropping risk problem is difficult to solve because $V_1^*(5)$ has the form of a min-max formula consisting of five quadratic multivariable polynomials. To solve the general case of the first-order eavesdropping risk under the best scenario over a ring, that is, $R_1^*(k)$, where k is an arbitrary natural number, we first divide the eavesdropping risk problem into two categories—one for an odd number of segments and the other one for an even number of segments—and solve them separately. Then, we take a geometrical approach and treat each category as a graph in a $(k-1)$-dimensional space. This way, we are able to prove the existence and uniqueness of the local minimum of the graph. Due to its uniqueness, the local minimum also represents the global minimum. Since this global minimum point corresponds to the uniform distribution, we prove that the uniform user distribution is indeed the best-case scenario. The closed-form solution of the first-order eavesdropping risk under the best scenario is simply the value of this global minimum.

Lemma 1 below deals with the case of an odd number of segments on a ring, whereas Lemma 2 targets the case of an even number of segments. These two lemmas give the closed-form solutions of $R_1^*(k)$ and show that the uniform user distribution minimizes the first-order eavesdropping risk over a ring. We present in detail the proof of Lemma 1 and only sketch the proof of Lemma 2 due to their similarity.

Lemma 1. *Given n user nodes, the first-order eavesdropping risk over a ring with an odd number k of segments is greater than or equal to*

$$R_1^*(k) = \alpha\frac{k^2+4k-1}{8k^2},$$

where $\alpha = \frac{2n^2}{n(n+1)}$. The equality holds when $n_i = n/k$ for $0 \le i \le k-1$. That is, when the ring is partitioned into an odd number of segments, the uniform user distribution minimizes the first-order eavesdropping risk.

Proof. *Step 1.* Consider the first-order eavesdropping risk problem over a ring with the user distribution N and an odd number k of segments. Because the packets exchanged between any S-D pair are transmitted along the route with the least number of hops, any S-D pair is at most $t = \lfloor k/2 \rfloor$ hops away. If the adversarial node is located on segment i, then the passing volume is[8]

$$n_i n - 0.5n_i(n_i-1) + \sum_{a=1}^{t-1}\sum_{b=1}^{t-a} n_{i+a}n_{i-b}. \tag{5}$$

Given N, the first-order eavesdropping volume $V_1^N(k)$ is the maximum passing volume over all possible adversary distributions. Since the first-order eavesdropping volume for the best-case scenario $V_1^*(k)$ is the minimum of $V_1^N(k)$ over all possible user distributions $N \in \mathbb{N}_n^k$, we get

$$V_1^*(k) = \min_{N\in\mathbb{N}_n^k} \max\Big(n_0 n - 0.5n_0(n_0-1) + \sum_{a=1}^{t-1}\sum_{b=1}^{t-a} n_a n_{0-b},\; n_1 n - 0.5n_1(n_1-1) + \sum_{a=1}^{t-1}\sum_{b=1}^{t-a} n_{1+a}n_{1-b},\; \ldots,\; n_i n - 0.5n_i(n_i-1) + \sum_{a=1}^{t-1}\sum_{b=1}^{t-a} n_{i+a}n_{i-b},\; \ldots,\; n_{k-1} n - 0.5n_{k-1}(n_{k-1}-1) + \sum_{a=1}^{t-1}\sum_{b=1}^{t-a} n_{k-1+a}n_{k-1-b}\Big).$$

Define $f_i(X)$ as the probability of packets being eavesdropped when the normalized user distribution is X and the adversarial node resides on segment i. Dividing the corresponding passing volume in (5) by the total number of S-D pairs $n(n-1)/2 + n = n(n+1)/2$, we get

$$f_i(X) = \alpha\left(x_i - 0.5x_i^2 + \sum_{a=1}^{t-1}\sum_{b=1}^{t-a} x_{i+a}x_{i-b}\right),$$

where $\alpha = \frac{2n^2}{n(n+1)}$. The above equation neglects $0.5x_i/n$ because it equals 0 as $n \to \infty$. Similarly, dividing $V_1^*(k)$ by $n(n+1)/2$, we get the first-order eavesdropping risk for the best-case scenario:

$$R_1^*(k) = \frac{V_1^*(k)}{n(n+1)/2} = \min_{X\in\mathbb{F}_1^k} \max(f_0(X), f_1(X), \ldots, f_{k-1}(X)).$$

Step 2. Denote

$$g(X) = \max(f_0(X), f_1(X), \ldots, f_{k-1}(X)).$$

It is obvious that $R_1^*(k) = \min_{X\in\mathbb{F}_1^k} g(X)$. In other words, $R_1^*(k)$ is the global minimum of $g(X)$ in the domain $\mathbb{F}_1^k$. Note that $x_{k-1} = 1 - \sum_{a=0}^{k-2} x_a$ and $g(X)$ is a function of $k-1$ arguments $x_0, x_1, \ldots, x_{k-2}$; however, we keep the notation x_{k-1} in formulas for simplicity of exposition. In this step, we present some important properties of $f_i(X)$

8. For simplicity of exposition, the "*modulo k*" operation applies to the subscripts of the symbols n_i and x_i unless otherwise stated. For instance, n_{-k+1} and x_{2k-2} mean n_1 and x_{k-2}, respectively.

and give a geometric interpretation, which will help find the global minimum of $g(X)$ in the next two steps.

We first prove that, for $0 \le i \le k-1$, there exists no point $X \in \mathbb{R}_1^k$ such that the gradient[9] of f_i at X is equal to $\vec{0}$, where $\vec{0}$ is defined as the k-tuple of all zeros, and $\mathbb{R}_1^k$ is the set of k-tuples of real numbers whose components sum up to 1:

1. For $0 \le i \le t-2$, we can write $f_i(X)$ as

$$f_i(X) = \alpha\left(x_i - 0.5x_i^2 + x_{k-1}\sum_{a=i+1}^{t-1} x_a + Remainder\right),$$

where $Remainder$ collects all of the terms not containing x_i and x_{k-1}. Note that x_{i+t} does not appear in $Remainder$ because it does not appear in $f_i(X)$ either. Taking the partial derivatives of $f_i(X)$ and using the fact that $\frac{\partial x_{k-1}}{\partial x_i} = -1$ for all $0 \le i \le k-2$, we get

$$\frac{\partial f_i(X)}{\partial x_i} = \alpha\left(1 - x_i - \sum_{a=i+1}^{t-1} x_a\right)$$

and

$$\frac{\partial f_i(X)}{\partial x_{i+t}} = -\alpha\left(\sum_{a=i+1}^{t-1} x_a\right).$$

The above two partial derivatives of $f_i(X)$ cannot both be equal to 0. Therefore, $\nabla f_i(X) \neq \vec{0}$ for $0 \le i \le t-2$.

2. For $t-1 \le i \le k-t-1$, $f_i(X)$ does not have any term containing x_{k-1}. Therefore,

$$\frac{\partial f_i}{\partial x_i} = \alpha(1 - x_i) > 0$$

and we know that $\nabla f_i(X) \neq \vec{0}$ for $t-1 \le i \le k-t-1$.

3. For $k-t \le i \le k-2$, we can write $f_i(X)$ in the form of

$$f_i(X) = \alpha\left(x_i - 0.5x_i^2 + x_{k-1}\sum_{a=k-t-1}^{i-1} x_a + Remainder\right).$$

For the same reason as in the case where $0 \le i \le t-2$, the $Remainder$ is a function not containing x_i, x_{k-1}, and x_{i-t}. Taking the partial derivatives of $f_i(X)$, we get

$$\frac{\partial f_i(X)}{\partial x_i} = \alpha\left(1 - x_i - \sum_{a=k-t-1}^{i-1} x_a\right)$$

and

$$\frac{\partial f_i(X)}{\partial x_{i-t}} = -\alpha\left(\sum_{a=k-t-1}^{i-1} x_a\right).$$

The above two partial derivatives of $f_i(X)$ cannot both be equal to 0. Therefore, the gradient $\nabla f_i(X) \neq 0$ for $k-t \le i \le k-2$.

4. For $i = k-1$, $f_i(X)$ has one term containing x_{k-1}, but has no term containing x_{t-1}. Therefore,

$$\frac{\partial f_i(X)}{\partial x_{t-1}} = -\alpha(1 - x_i) < 0$$

and $\nabla f_i(X) \neq \vec{0}$ for $i = k-1$.

Based on the above arguments, we proved that, for $0 \le i \le k-1$, $\nabla f_i(X) \neq \vec{0}$ in the domain $\mathbb{R}_1^k$. Therefore, $f_i(X)$ has no critical point (extreme or saddle points). Because $\mathbb{F}_1^k$ is a subset of $\mathbb{R}_1^k$, this result also applies to $f_i(X)$ in domain $\mathbb{F}_1^k$.

Here, we give the geometrical interpretation of the nonexistence of the critical point (extreme or saddle point). Consider the graph $z = f_i(X)$ in a $(k-1)$-dimensional space ($x_0, x_1, \ldots, x_{k-2}$ for the $k-1$ dimensions). Because $f_i(X)$ has no local extremum, a contour (also called a *level* or *equipotential curve*) of $f_i(X)$, $0 \le i \le k-1$, does not form a closed curve. Because of the nonexistence of saddle points, a contour of $f_i(X)$ does not cross over any other contour.

We note a useful property of $f_i(X)$ in the domain of $\mathbb{F}_1^k$. That is, each $\nabla f_i(X)$ has at least one component keeping its sign regardless of the value of X. For example, $\frac{\partial f_i(X)}{\partial x_i} > 0$ for $0 \le i \le k-2$ and $\frac{\partial f_{k-1}}{\partial x_{t-1}} < 0$ within the domain $\mathbb{F}_1^k$. We call this property *polarity persistency*. We will use this property to prove the uniqueness of the minimum of $g(X)$ inside the domain $\mathbb{F}_1^k$ in Step 4.

Step 3 (Existence of a local minimum). Because $g(X)$ is defined as the maximum of $f_i(X)$s, $0 \le i \le k-1$, we can consider the graph $z = g(X)$ consisting of patches. Each *patch* is simply a part of the graph $z = f_i(X)$, which takes a value greater than or equal to all other $f_j(X)$s, $0 \le j \le k-1$. We note two properties of $g(X)$: 1) $g(X)$ is continuous and so are the contours of $g(X)$ and 2) $g(X)$ has no saddle point. The former property holds true due to the continuity of each $f_i(X)$. The latter property follows from the fact that the contours of $f_i(X)$ do not cross over each other. Any one of the $f_i(X)$s has no extremum in the domain $\mathbb{R}_1^k$; however, $g(X)$ may have local extrema because a set of patches may enclose a local extremum point.

If $g(X)$ has one (or more) local extremum, that local extremum point must be at the intersections of patches. (This is because each $f_i(X)$ has the property of polarity persistency.) In other words, $g(X)$ has an extremum at X, only if there exist some i and j such that $f_i(X) = f_j(X)$, $i \neq j$. Actually, the intersection of any less than k patches cannot identify an extremum point of $g(X)$ because $g(X)$ has $k-1$ variables (that is, $x_0, x_1, \ldots, x_{k-2}$) and needs all of the $k-1$ equalities $f_0(X) = f_1(X) = f_2(X) = \cdots = f_{k-1}(X)$ to determine the extreme point.

9. In a Cartesian coordinate with bases $x_0, x_1, \ldots, x_{n-1}$, the gradient of a function f is given by $\nabla f = (\frac{\partial f}{\partial x_0}, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_{n-1}})$.

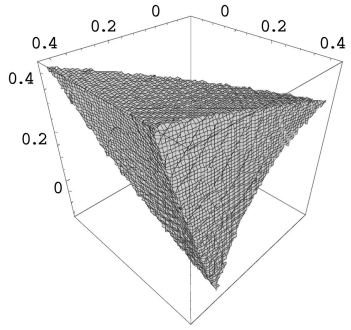


Fig. 8. The contour of $g(X) = 0.4\alpha$ in a ring with four segments. The axes are x_0, x_1, and x_2. The contour forms a closed surface surrounding the minimum point $X^* = (0.25, 0.25, 0.25)$.

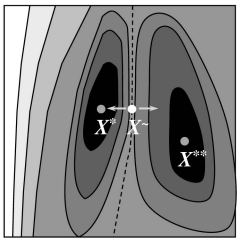


Fig. 9. This figure illustrates a contour plot with two local minimum points X^* and X^{**}. The darker the color is, the smaller the value it represents. The dotted curve is a common contour shared by the left contours enclosing X^* and the right contours enclosing X^{**}. $X^{\sim}$ is a point lying on the dotted curve. The left arrow and the right arrow represent the gradient at $X^{\sim}$ approaching from the left-hand side and the gradient at $X^{\sim}$ approaching from the right-hand side, respectively.

Now, consider the point $X^* = (1/k, 1/k, \ldots, 1/k)$. It is straightforward to show that X^* is at the intersection of all k patches because $f_0(X^*) = f_1(X^*) = \cdots = f_{k-1}(X^*)$. Since $\frac{\partial f_i(X^*)}{\partial x_i}$ is positive and $\frac{\partial f_{k-1}(X^*)}{\partial x_i}$ is negative for $0 \le i \le k-2$, we know that $g(X^*)$ is smaller than the neighbors of X^* in the $+x_i$ directions and $-x_i$ directions, $0 \le i \le k-2$. Because the contours of $g(X)$ are continuous and do not cross over to each other, this fact ensures that $g(X)$ has a local minimum at X^*.

Step 4 (Uniqueness of the local minimum in the domain $\mathbb{F}_1^k$). So far, we have proved the existence of a local minimum at $X^* = (1/k, 1/k, \ldots, 1/k)$. Now, let us prove that $g(X^*)$ is the only local minimum in the domain $\mathbb{F}_1^k$.

Note that a contour surrounding a local minimum point must be closed; otherwise, there exists a point in the hole of the contour surface such that the value of $g(X)$ at that point is less than the local minimum value, and this would contradict the definition of the local minimum. To give an illustration, Fig. 8 shows the contour of $g(X) = 0.4\alpha$ in the case of $k = 4$, which forms a closed surface surrounding the minimum point $X^* = (0.25, 0.25, 0.25)$, where $g(X^*) = 0.25\alpha$.

Now, let us assume that there exists more than one local minimum point in the domain $\mathbb{F}_1^k$ and denote the minimum point closest to X^* by X^{**}. Because X^* is a local minimum point, each contour of $g(X)$ around X^* forms a closed surface. For the same reason, this closure property of contours surrounding X^{**} holds as well. The level value of contours is gradually increasing when contours move away from the local minimum point X^* (and X^{**}). Because of the continuity of the contours of $g(X)$, there exist two contours—each moving away from X^* and X^{**}—merging into a single contour somewhere in between X^* and X^{**}; this is shown as the dotted curve in Fig. 9. Consider some point $X^{\sim}$ on the dotted curve that is lying on a patch, say, a fraction of the graph $z = f_i(X)$. It is obvious that $\nabla g(X^{\sim})$ approaching from one side (shown as an arrow in Fig. 9) is the negative of $\nabla g(X^{\sim})$ approaching from the other side (shown as the other arrow in Fig. 9). However, a contradiction occurs because this violates the property of polarity persistency of $f_i(X)$ in $\mathbb{F}_1^k$. Therefore, $g(X)$ has a unique local minimum $X^* = (1/k, 1/k, \ldots, 1/k)$ in the domain $\mathbb{F}_1^k$. This minimum value $g(X^*) = \alpha\frac{k^2+4k-1}{8k^2}$ is the first-order eavesdropping risk $R_1^*(k)$ for the best-case scenario over a ring with an odd number of segments. □

Lemma 2. *Given n user nodes, the first-order eavesdropping risk over a ring with an even number k of segments is greater than or equal to*

$$R_1^*(k) = \alpha\frac{k(k+4)}{8k^2},$$

where $\alpha = \frac{2n^2}{n(n+1)}$. The equality holds when $n_i = n/k$. That is, the uniform user distribution minimizes the first-order eavesdropping risk over a ring when the ring is partitioned into an even number of segments.

Proof. Similarly to the previous case when a ring is partitioned into an odd number of segments, the first-order eavesdropping risk over a ring with an even number k of segments is bounded below by that for the best-case scenario:

$$R_1^*(k) = \min_{X \in \mathbb{F}_1^k} \max(f_0(X), f_1(X), \ldots, f_{k-1}(X)),$$

where

$$f_i(X) = \alpha\left(x_i - 0.5x_i^2 + \sum_{a=1}^{t-1}\sum_{b=1}^{t-a}\rho(a+b)x_{i+a}x_{i-b}\right)$$

and

$$\rho(z) = \begin{cases} 1 & \text{if } 2 \le z \le t-1 \\ \frac{1}{2} & \text{if } z = t \\ 0 & \text{otherwise.} \end{cases}$$

Using a similar approach to Lemma 1, we can prove that all of the properties introduced in the proof of Lemma 1 also hold when k is even. These properties are sufficient to prove the existence and uniqueness of the local minimum point $X^* = (1/k, 1/k, \ldots, 1/k)$ in the domain $\mathbb{F}_1^k$. Therefore, we can follow Steps 3 and 4 in Lemma 1 above and get the following closed-form formula:

$$\begin{aligned} R_1^*(k) &= R_1^{X^*}(k) \\ &= \alpha\frac{k(k+4)}{8k^2}, \end{aligned}$$

which is a lower bound for the first-order eavesdropping risk over a ring with an even number of segments. □

Lemmas 1 and 2 lead to the following theorem:

Theorem 2. *Given n user nodes, the first-order eavesdropping risk over a ring is minimized under the uniform user distribution.*

3.2.3 Eavesdropping Risk for the 2D Torus

Now, we are ready to study the eavesdropping risk for the unit torus model. First, we prove that the uniform user distribution minimizes the first-order eavesdropping risk over a torus.

Theorem 3. *Given n user nodes, which are deployed arbitrarily, the first-order eavesdropping risk in the unit torus model is minimized when user nodes are uniformly deployed.*

Proof. *Step 1.* In this step, we derive the formula of eavesdropping risk given the user distribution N.

Consider the first-order eavesdropping risk problem in a unit torus with the distribution N of user nodes and the cell area $a(n)$. Since the total area of a unit torus is 1, the total number of cells in a unit torus is $k = 1/a(n)$. Assuming that the adversarial node is located in cell i, the passing volume is

$$n_i n - 0.5n_i^2 + 0.5n_i + \sum_{\substack{0\le a<b\le k-1\\ a,b\neq i}} \rho_i(a,b) n_a n_b,$$

where $\rho_i(a,b)$ is the probability of S-D pairs passing through cell i, given that cell a and cell b are the two ends of the S-D pairs. If these S-D pairs have (at least) one route with the least number of hops passing through cell i, $\rho_i(a,b)$ is positive and less than or equal to 1. Otherwise, $\rho_i(a,b)$ is equal to 0.

Similarly to the 1D torus case, given the normalized distribution X of user nodes, the probability of packets being eavesdropped when the adversarial node resides in cell i can be derived as follows:

$$f_i(X) = \alpha\left(x_i - 0.5x_i^2 + \sum_{\substack{0\le a<b\le k-1\\ a,b\neq i}} \rho_i(a,b) x_a x_b\right),$$

where $\alpha = \frac{2n^2}{n(n+1)}$ is the total number of S-D pairs divided by n^2. Obviously, the first-order eavesdropping risk given the normalized distribution X of user nodes,

$$R_1^X(k) = \max(f_0(X), f_1(X), \ldots, f_{k-1}(X)),$$

is bounded below by the eavesdropping risk for the best-case scenario:

$$R_1^*(k) = \min_{X\in\mathbb{F}_1^k} \max(f_0(X), f_1(X), \ldots, f_{k-1}(X)).$$

Note that x_{k-1} is not a variable because $x_{k-1} = 1 - \sum_{a=0}^{k-2} x_a$; however, we keep the notation x_{k-1} in this proof for reasons of simplicity.

Step 2. The main goal of this step is to extend the results derived for the 1D torus and prove that the two properties of $f_i(X)$—the nonexistence of critical points and polarity persistency—also hold on a (regular) torus.

Assume that the adversarial node resides in cell i and consider the S-D pairs originating from (or having destination at) cell i', where

$$i' = i + t + t\sqrt{k} \pmod k$$

and $t = \lfloor \sqrt{k}/2 \rfloor$. Because the packets exchanged in any S-D pair are always transmitted along the route with the smallest hop count, the two ends of any S-D pair in a unit torus are at most t hops away from each other. Since cell i is t hops away from cell i', any S-D pair originating from (or having destination at) cell i' does not pass through cell i unless cell i is the other end of that S-D pair. Hence, $f_i(X)$ does not have any term containing $x_{i'}$.

Similarly to the 1D torus case, for $0 \le i \le k-2$, we can calculate the two partial derivatives $\frac{\partial f_i(X)}{\partial x_i}$ and $\frac{\partial f_i(X)}{\partial x_{i'}}$ as follows by using the fact that $x_{k-1} = 1 - \sum_{a=0}^{k-2} x_a$ and $\frac{\partial x_{k-1}}{\partial x_i} = -1$:

$$\frac{\partial f_i(X)}{\partial x_i} = \alpha\left(1 - x_i - \sum_{\substack{0\le a\le k-2\\ a\neq i}} \rho_i(a,k-1)x_a\right),$$

$$\frac{\partial f_i(X)}{\partial x_{i'}} = -\alpha \sum_{\substack{0\le a\le k-2\\ a\neq i}} \rho_i(a,k-1)x_a.$$

Since $\frac{\partial f_i(X)}{\partial x_i}$ and $\frac{\partial f_i(X)}{\partial x_{i'}}$ cannot both be equal to 0, we have proved that $\nabla f_i(X) \neq \vec{0}$. Therefore, $f_i(X)$ has no critical point in the domain $\mathbb{R}_1^k$.

If we narrow down the domain of interest to $\mathbb{F}_1^k$ for $0 \le i \le k-2$, $f_i(X)$ satisfies the property of polarity persistency because $\frac{\partial f_i(X)}{\partial x_i} > 0$ in the domain $\mathbb{F}_1^k$. Indeed,

$$\frac{\partial f_i(X)}{\partial x_i} = \alpha\left(1 - x_i - \sum_{\substack{0\le a\le k-2\\ a\neq i}} \rho_i(a,k-1)x_a\right) \ge \alpha\left(1 - x_i - \sum_{\substack{0\le a\le k-2\\ a\neq i}} x_a\right) > 0.$$

For $i = k-1$, $f_i(X)$ has one term containing x_{k-1} but has no term containing $x_{i'}$. The partial derivative,

$$\frac{\partial f_i(X)}{\partial x_{i'}} = -\alpha,$$

is negative. Therefore, $f_i(X)$ has no critical point and is polarity persistent.

From the above arguments, it results that $f_i(X)$ has no critical point and satisfies the polarity persistency for $0 \le i \le k-1$.

Steps 3 and 4. We omit here the details of the approach we use to prove the existence and uniqueness of the local minimum in the domain $\mathbb{F}_1^k$ because it is similar to the approach used in the 1D torus case. (Please see Steps 3 and 4 in the proof of Lemma 1 for details.)

We have proved that the uniform user distribution minimizes the first-order eavesdropping risk in the unit torus model. □

We believe that, when the total number of user nodes and the total number of cells are large, the uniform user distribution also minimizes the higher order eavesdropping risks. This conjecture is based on the fact that the more random the traffic between user nodes is, the less benefit

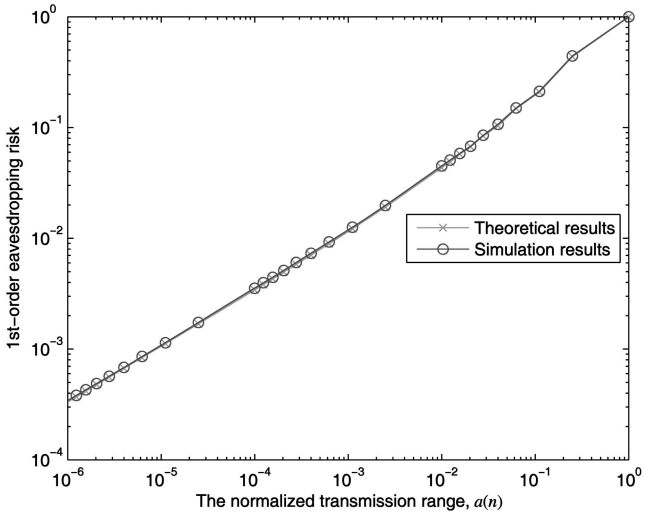


Fig. 10. This figure shows the consistency between the theoretical first-order eavesdropping risks under uniform traffic and the corresponding simulation results. In this log-log scale plot, the curve rises linearly when $a(n)$ is small enough. This is because, as $a(n) \to 0$, the first-order eavesdropping risk approximates to $1/3\sqrt{a(n)}$. Note that, as implied in Fig. 2, the increasing property under uniform user distributions is not necessarily applicable to nonuniform user distributions. However, the derived lower bound can be applied to all user distributions.

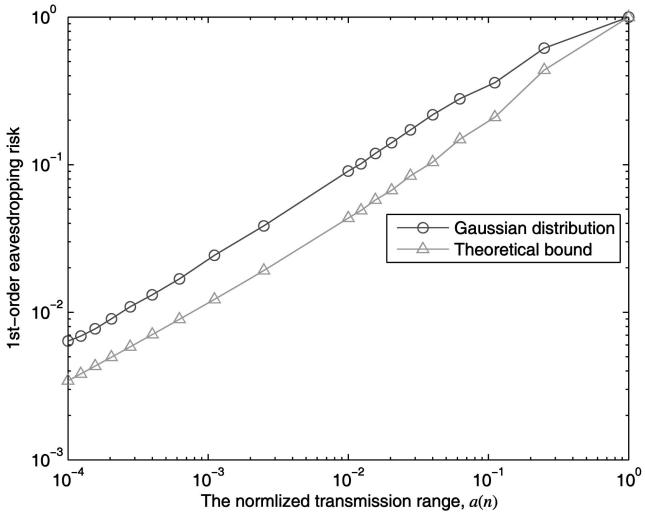


Fig. 11. This figure shows the first-order eavesdropping risk for the 2D Gaussian distribution with zero mean and $\sigma = 0.25$. Although the bell-shaped Gaussian distribution is different from the uniform distribution, the eavesdropping risk for the Gaussian distribution can be reasonably approximated by our proposed lower bound (with a difference of about 3 dB).

the adversarial nodes can gain by changing their locations in order to maximize the traffic volume they can listen to. The formal proof is left for future research.

Theorem 3 proves that the uniform user distribution minimizes the first-order eavesdropping risk and Theorem 1 gives its closed-form formulas. Combining these two theorems together results in the following general theorem.

Theorem 4. *In a random network consisting of n nodes deployed arbitrarily, the first-order eavesdropping risk is bounded below by $\frac{1}{3}\sqrt{a(n)}$, where $a(n)$ is the normalized transmission range.*

Proof. Since $s = 1/\sqrt{a(n)}$ is always greater than or equal to 1, both $s^2 + 3s - 1$ and $s^2 + 3s + \frac{1}{2}$ are greater than s^2. Therefore, by using (3) and (4), we know that $R_1^*(k) > \frac{s^2}{3s^3} = \frac{1}{3}\sqrt{a(n)}$. □

4 Simulation Results

4.1 The First-Order Eavesdropping Risk Given Uniform User Distribution

In this section, we show that, for the first-order eavesdropping risk, the theoretical bounds and the simulation results under uniform traffic are consistent with each other. The simulation configurations are as follows: In each iteration, an S-D pair is chosen at random. Then, a packet of unit size is transmitted from the source node to the destination node along a least hop count route. (In case there are multiple shortest routes, one of them is chosen randomly.) This route is recorded. At the end of simulation, the simulator identifies the cell where an adversarial node can grab the maximum number of packets and calculates the values of the first-order eavesdropping risks.

The total number of iterations is set to be proportional to the number of cells, but has an upper limit, 10^8. This limit helps us get reasonably accurate results while bounding the simulation time by a threshold.

As one can see in Fig. 10, the simulated first-order eavesdropping risk values under uniform traffic are very close to their corresponding theoretical counterparts. Fig. 10 also shows that a significant reduction in the eavesdropping risk can be achieved by decreasing the normalized transmission range. This justifies the idea of using transmission power control to improve the network security, especially in a large-scale ad hoc wireless network where the normalized transmission range is very small.

4.2 Nonuniform Distributions

Theorem 3 proves that the uniform distribution minimizes the first-order eavesdropping risk. In other words, nonuniformity increases the eavesdropping risk. In this section, we consider a few nonuniform distributions and investigate their quantitative impact on the eavesdropping risk. We start with the 2D Gaussian distribution (Section 4.2.1), which can be regarded as a distribution with a single cluster, and then move to distributions with multiple clusters (Section 4.2.2). The simulation results also validate the correctness of our proposed lower bounds (in addition to the mathematical proof in Section 3) and show how close our derived lower bound can be when the user nodes are deployed nonuniformly.

4.2.1 Nonuniform Cases with 2D Gaussian Distribution

We first investigate the impact of the 2D Gaussian distribution on the eavesdropping risk. In this simulation setup, a number of nodes are Gaussian distributed around a center with zero mean and a covariance matrix $\sigma^2\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$, where the location of the center is randomly chosen.

As shown in Fig. 11, regardless of the transmission range, the eavesdropping risk for the 2D Gaussian distribution is never smaller than the theoretical lower bound. This shows the correctness of the theoretical bound. In addition,

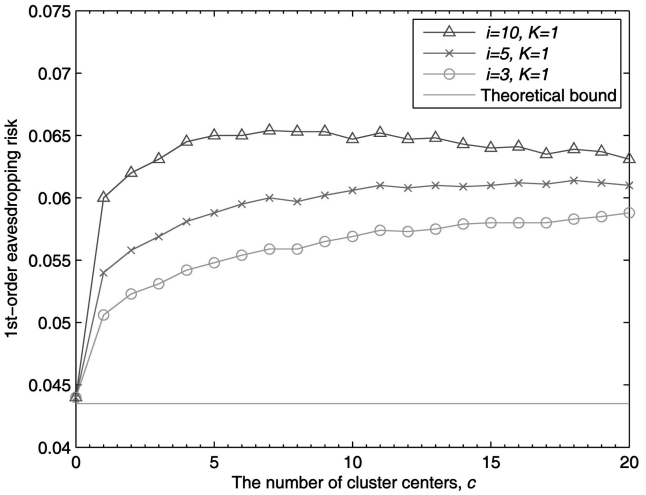


Fig. 12. This figure shows the first-order eavesdropping risk for the cluster distributions with the number of cluster centers $c = \{0, 1, \ldots, 20\}$, the cluster intensity $i = \{3, 5, 10\}$, and the spreading factor $K = 1$ in a 10×10 unit torus network. Although the user distributions in this simulation setup are different from the uniform distribution, the eavesdropping risk for cluster distributions can be reasonably approximated by our proposed lower bound (with a difference up to 1.8 dB).

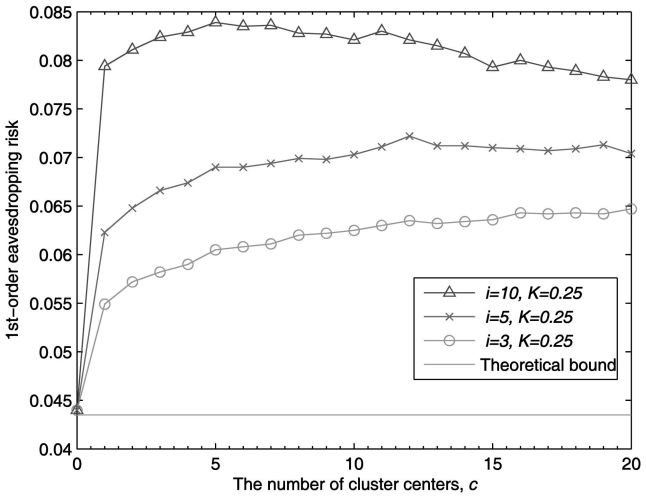


Fig. 13. This figure shows the first-order eavesdropping risk for the cluster distributions with the number of cluster centers $c = \{0, 1, \ldots, 20\}$, the cluster intensity $i = \{3, 5, 10\}$, and the spreading factor $K = 0.25$ in a 10×10 unit torus network. Although the user distributions in this simulation setup are different from the uniform distribution, the eavesdropping risk for cluster distributions can be reasonably approximated by our proposed lower bound (with a difference up to 2.9 dB).

although the Gaussian distribution is different from the uniform distribution, the eavesdropping risk can be reasonably approximated by the theoretical bound with a 3 dB difference.

4.2.2 Nonuniform Cases with Cluster Distribution

In this simulation setup, we focus on a 10×10 unit torus (that is, its normalized transmission range is $a(n) = 0.01$). In addition to the user nodes that are deployed uniformly and independently, we add a few extra nodes around c cluster centers. The locations of these c cluster centers are chosen randomly. The number of the extra nodes are Poisson distributed with a mean equal to $i - 1$ times the number of nodes per cell that were deployed uniformly (where the cluster intensity i is a measure of the relative node density of the regions around the cluster centers compared to the regions far away from the cluster centers). Moreover, the displacements of these extra nodes from their cluster centers follow an uncorrelated Gaussian distribution with a mean of zero and a covariance matrix $K^2 a(n) \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, where the spreading factor K determines how scattered the extra nodes are. For simplicity of exposition, we call this a *cluster distribution* with three parameters: the number of cluster centers c, the cluster intensity i, and the spreading factor K. Note that, when $c = 0$ or $i = 1$, the cluster distribution degenerates to a uniform distribution.

In order to assess the impact of cluster distributions on the eavesdropping risk, we simulate the individual eavesdropping risk for cluster distributions with different parameters, as shown in Figs. 12 and 13. It is observed that the first-order eavesdropping risk increases rapidly as c starts to increase. This is because the more concentrated the network nodes are, the easier the sniffing activity becomes. In other words, the nonuniformity of node distribution increases the eavesdropping risk. For the same reason, increasing the cluster intensity i and decreasing the spreading factor K result in the increase of the eavesdropping risk. However, further increasing the value of c makes the eavesdropping risk saturated (or even creates ripples) because randomly adding an exceedingly high number of clusters into the 100-cell torus actually smooths out the aggregate node distribution.

As we see in Figs. 12 and 13, the eavesdropping risk for various cluster distributions is never smaller than the theoretical lower bound. This shows the correctness of the theoretical bound. Moreover, the difference of the simulated eavesdropping risk values under various cluster distributions from the derived lower bound is less than 3 dB, although the cluster distributions are *not* uniform. From the above arguments, we conclude that our proposed lower bound is sufficiently tight for a wide range of node distributions.

4.3 Traffic with Various Batch Sizes

As explained in Section 4.2, nonuniformity is a major factor in determining the eavesdropping risk value. In general, there are two main sources of nonuniformity: the node distribution over the network and traffic pattern per S-D pair. Whereas Section 4.2 has represented the quantitative impact of node distributions on the eavesdropping risk value, the main objective of this section is to investigate the impact of the traffic patterns among S-D pairs on the eavesdropping risk.

Scaling up/down the traffic volume of all S-D pairs linearly does not affect the eavesdropping risk value because the linear factor will be canceled out during computing the eavesdropping risk. On the contrary, the *variation* of traffic volume among S-D pairs does matter. In one extreme case where only one S-D pair communicates and other pairs keep quiet, the first-order eavesdropping risk value is equal to the maximum value 1 because an adversarial node residing in the same cell where the source node resides can eavesdrop all the packets. In the other extreme case, where all S-D pairs

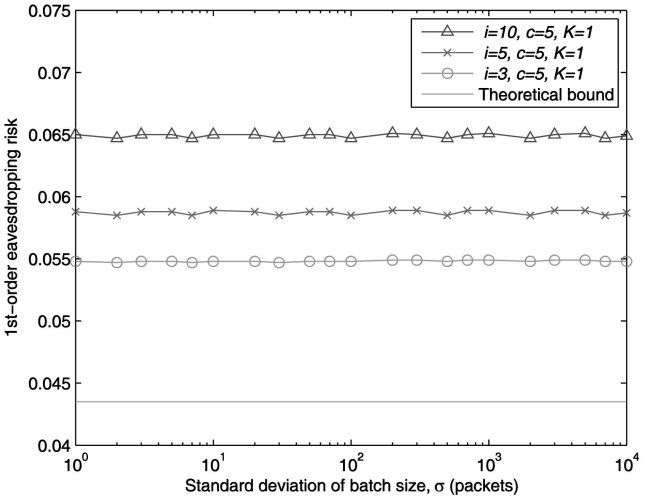


Fig. 14. This figure shows the first-order eavesdropping risk (for cluster distribution) under Gaussian traffic in a 10×10 unit torus network (that is, $a(n) = 0.01$). Please note that the eavesdropping risk in this simulation setup can be appropriately approximated by our proposed lower bound (with a difference up to 1.8 dB).

communicate at a constant traffic volume, the eavesdropping risk is minimized, as proven in Theorem 3. In practice, any node is allowed to communicate with any other node. Therefore, we concentrate our investigation in this section on the cases when the traffic volume of all S-D pairs follows a common distribution. More specifically, since the absolute value of traffic volume does not matter, we study the impact of the traffic *burstiness* on the eavesdropping risk by simulation.

In this simulation setup, we focus on a 10×10 unit torus. The batch size per S-D pair (in terms of the number of packets sent from source to destination) is modeled as a Gaussian variable with a mean of $\mu = 100$ packets and a standard deviation σ ranging from 1 to 10,000.[10] A batch of packets is transmitted to the destination node along the same path. The larger the standard deviation is, the more bursty the traffic patterns are. For each given standard deviation value, we generate 500 network instances according to the cluster distributions with various parameters. For each network instance, a large number of batches of packets are injected into the network instance according to the common Gaussian distribution. The individual eavesdropping risk values are computed over these 500 network instances in order to observe how the traffic burstiness impacts the eavesdropping risk.

One might think that the traffic burstiness increases the eavesdropping risk because large batches have a greater impact than the small batches have. However, our simulation results show that this guess is *not* true. As shown in Fig. 14, when a large number of batches are injected into the network, the impact of the traffic burstiness is insignificant because, regardless the standard deviation of the batch size, the eavesdropping risk values are almost identical. To assert this observation with stronger evidence, we list in Table 1 not only the mean of the simulated eavesdropping risk values but also their entropy[11] and central moments of several orders.

TABLE 1
When Nodes Are Deployed According to Cluster Distributions with Parameters $c = 5$, $i = \{3, 5, 10\}$, and $K = 1$, and the Size of Batches of Packets Varies with a Standard Deviation (σ)

i	σ	μ	μ_2	μ_3	H
3	0	0.05481	$9.205 \cdot 10^{-6}$	$2.343 \cdot 10^{-8}$	3.516
	10^0	0.05481	$9.144 \cdot 10^{-6}$	$2.324 \cdot 10^{-8}$	3.522
	10^1	0.05484	$9.421 \cdot 10^{-6}$	$2.305 \cdot 10^{-8}$	3.536
	10^2	0.05476	$8.518 \cdot 10^{-6}$	$1.986 \cdot 10^{-8}$	3.435
	10^3	0.05490	$9.475 \cdot 10^{-6}$	$2.483 \cdot 10^{-8}$	3.546
	10^4	0.05483	$9.245 \cdot 10^{-6}$	$2.151 \cdot 10^{-8}$	3.542
5	0	0.05884	$1.741 \cdot 10^{-5}$	$4.528 \cdot 10^{-8}$	4.027
	10^0	0.05884	$1.734 \cdot 10^{-5}$	$4.476 \cdot 10^{-8}$	4.029
	10^1	0.05885	$1.848 \cdot 10^{-5}$	$6.696 \cdot 10^{-8}$	4.031
	10^2	0.05851	$1.860 \cdot 10^{-5}$	$1.114 \cdot 10^{-7}$	3.951
	10^3	0.05887	$1.749 \cdot 10^{-5}$	$4.478 \cdot 10^{-8}$	4.029
	10^4	0.05874	$1.867 \cdot 10^{-5}$	$6.738 \cdot 10^{-8}$	4.028
10	0	0.06502	$4.275 \cdot 10^{-5}$	$3.063 \cdot 10^{-7}$	4.575
	10^0	0.06503	$4.262 \cdot 10^{-5}$	$3.049 \cdot 10^{-7}$	4.556
	10^1	0.06503	$4.526 \cdot 10^{-5}$	$3.337 \cdot 10^{-7}$	4.629
	10^2	0.06467	$3.844 \cdot 10^{-5}$	$2.610 \cdot 10^{-7}$	4.548
	10^3	0.06506	$4.368 \cdot 10^{-5}$	$3.162 \cdot 10^{-7}$	4.583
	10^4	0.06417	$4.037 \cdot 10^{-5}$	$2.801 \cdot 10^{-7}$	4.509

This table lists the mean (μ), the second and third-order central moments (μ_2 and μ_3), and the entropy (H) of the simulated eavesdropping risk over 500 network instances. Because all of these metrics are very close, it is observed that the variation of batch size does not affect the eavesdropping risk when batch size per S-D pair follows a common distribution. This observation holds true for cluster distributions with different parameters; however, the statistics are omitted here to save space.

An explanation of the above phenomenon is given as follows: Having packets transmitted in short uneven spurts affects the *transient behavior* of a network. However, since the total traffic volume per S-D pair from a *long-run* perspective is independent of traffic burstiness, the traffic burstiness does not affect the eavesdropping risk. This phenomenon is analogous to the fact that, in an M/G/1 queue, the variation of service time affects queuing delay but does not affect throughput.

As shown in Fig. 14, the eavesdropping risk for all traffic patterns is greater than the theoretical lower bound. This shows the correctness of the theoretical bound. Moreover, the simulated eavesdropping risk values have the same order of magnitude as the derived lower bound, although their traffic patterns are very different compared to the uniform traffic. From the above arguments, we conclude that our proposed lower bound is tight for a wide range of traffic patterns.

4.4 Higher Order Eavesdropping Risk

In this section, we consider the *higher order* eavesdropping risk under uniform traffic. In this simulation setup, a packet originates from a randomly chosen source node and has a random destination node, according to the uniform user distribution. Each eavesdropped packet is counted only once. This is because each eavesdropped packet has an equal contribution to the eavesdropping risk, regardless of how many adversarial nodes actually eavesdrop it. The simulation results of first to fourth-order eavesdropping risk are shown in Fig. 15.

10. If the Gaussian variable takes a value greater than 1, the batch size is rounded to the nearest integer. Otherwise, the batch size is set to 1.

11. We first group the 500 simulated eavesdropping risk values into bins of interval length 0.001 and then calculate the entropy of these bins.

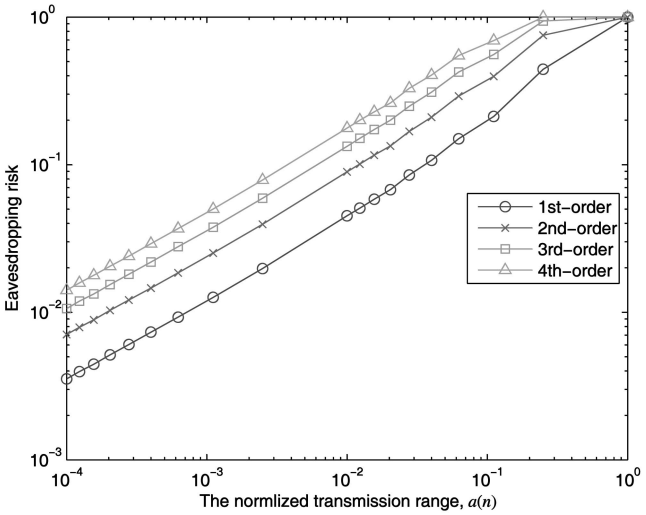


Fig. 15. Higher order eavesdropping risks under uniform traffic. This figure shows that, although the eavesdropping risk gets higher when the order gets larger, decreasing the transmission range can reduce the eavesdropping risk for all possible values of the order. It is also observed that, when $a(n)$ is small, the eavesdropping risk increases approximately linearly as the number of adversarial nodes (that is, the order) increases.

As observed in Fig. 15, the wth-order eavesdropping risk is an increasing function with respect to w, but its value is at most w times as large as the first-order eavesdropping risk. This is because the more adversarial nodes exist, the more packets can be eavesdropped. Actually, when the normalized transmission range is large (that is, close to 1), a small set of adversarial nodes can receive all packets transmitted over the wireless network. On the contrary, given $w \in \mathbb{N}$, decreasing the normalized transmission range reduces the wth-order eavesdropping risk significantly. Our simulations also show that, when the normalized transmission range is small enough, the wth-order eavesdropping risk is approximately w times larger than the first-order eavesdropping risk. This (approximately) linear dependency supports the idea of using transmission power control in a wide large-scale ad hoc wireless network where multiple adversarial nodes exist.

5 Conclusion

In this paper, the issue of transmission power control for security improvement in ad hoc wireless networks has been addressed. In particular, we have analyzed the impact of the transmission range and user distribution on the eavesdropping risk when there are one or more adversarial nodes.

As a main contribution, we have defined the wth-eavesdropping risk as the probability of packets being eavesdropped when there are w adversarial nodes in a network. We have derived a closed-form formula for the first-order eavesdropping risk under uniform traffic as a function of normalized transmission radius. For nonuniform traffic, we have identified the best-case scenario (in terms of the first-order eavesdropping risk) and proved a lower bound over all possible user distributions. Furthermore, our simulation results show the tightness of this lower bound for a wide range of user distributions and traffic patterns. We have also shown that adjusting the transmission range reduces the eavesdropping risk significantly.

In a more general context, transmission power control can not only help to better protect the network security by reducing the probability of packets being eavesdropped but also improve the network throughput, energy conservation, and quality of service. Whereas related work in the literature attempts to improve either the network security by cryptography-based approaches (at the cost of considerable overhead) or the network performance by transmission power control (without taking security into consideration), our results provide the first analytical treatment of using transmission power control as a defense mechanism against the reconnaissance activity.

Acknowledgments

The authors thank the anonymous reviewers for their many helpful suggestions. This research was supported by Carnegie Mellon University (CMU) CyLab Army Research Office (ARO) under Grant 9097.60.5 and by a Frank J. Marshall Graduate Fellowship for Jung-Chun Kao.

References

[1] J.-P. Hubaux, T. Gross, J.-Y.L. Boudec, and M. Vetterli, "Toward Self-Organized Mobile Ad Hoc Networks: The Terminodes Project," *IEEE Comm. Magazine,* vol. 39, no. 1, pp. 118-124, Jan. 2001.

[2] S. Weber, V. Cahill, S. Clarke, and M. Haahr, "Wireless Ad Hoc Network for Dublin: A Large-Scale Ad Hoc Network Test-Bed," *ERCIM News,* no. 54, pp. 34-35, July 2003.

[3] United States Computer Emergency Readiness Team, *Statistics on Federal Incident Reports,* http://www.us-cert.gov/federal/statistics/, Feb. 2006.

[4] T. Grance, K. Kent, and B. Kim, "Computer Security Incident Handling Guide," Nat'l Inst. Standards and Technology (NIST) Special Publications 800-61, Jan. 2004.

[5] S.J. Stolfo, "Worm and Attack Early Warning: Piercing Stealthy Reconnaissance," *IEEE Security and Privacy Magazine,* vol. 2, no. 3, pp. 73-75, May-June 2004.

[6] A. Perrig, J. Stankovic, and D. Wagner, "Security in Wireless Sensor Networks," *Comm. ACM,* vol. 47, no. 6, pp. 53-57, June 2004.

[7] C.K. Wong, M. Gouda, and S.S. Lam, "Secure Group Communications Using Key Graphs," *IEEE/ACM Trans. Networking,* vol. 8, no. 1, pp. 16-30, Feb. 2000.

[8] R.-H. Gau, "Performance Analysis of Multicast Key Backbone for Secure Group Communications," *IEEE Comm. Letters,* vol. 10, no. 7, July 2006.

[9] L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," *Proc. ACM Conf. Computer and Comm. Security (CCS '02),* pp. 41-47, Nov. 2002.

[10] W. Du, J. Deng, Y.S. Han, S. Chen, and P.K. Varshney, "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge," *Proc. IEEE INFOCOM '04,* pp. 586-597, Mar. 2004.

[11] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," *Proc. IEEE Symp. Security and Privacy,* pp. 197-213, May 2003.

[12] M. Abdalla, Y. Shavitt, and A. Wool, "Key Management for Restricted Multicast Using Broadcast Encryption," *IEEE/ACM Trans. Networking,* vol. 8, no. 4, pp. 443-454, Aug. 2000.

[13] R. Poovendran and J.S. Baras, "An Information-Theoretic Approach for Design and Analysis of Rooted-Tree-Based Multicast Key Management Schemes," *IEEE Trans. Information Theory,* vol. 47, no. 7, pp. 2824-2834, Nov. 2001.

[14] M. Li, R. Poovendran, and C. Berenstein, "Design of Secure Multicast Key Management Schemes with Communication Budget Constraint," *IEEE Comm. Letters,* vol. 6, no. 3, pp. 108-110, Mar. 2002.

[15] S. Capkun, L. Buttyan, and J.-P. Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," *IEEE Trans. Mobile Computing,* vol. 2, no. 1, pp. 52-64, Jan.-Mar. 2003.

[16] M.F. Younis, K. Ghumman, and M. Eltoweissy, "Location-Aware Combinatorial Key Management Scheme for Clustered Sensor Networks," *IEEE Trans. Parallel and Distributed Systems,* vol. 17, no. 8, pp. 865-882, Aug. 2006.

[17] Y. Mao, Y. Sun, M. Wu, and K.J.R. Liu, "Jet: Dynamic Join-Exit-Tree Amortization and Scheduling for Contributory Key Management," *IEEE/ACM Trans. Networking,* vol. 14, no. 5, pp. 1128-1140, Oct. 2006.

[18] W. Liang and W. Wang, "A Quantitative Study of Authentication and QoS in Wireless IP Networks," *Proc. IEEE INFOCOM '05,* pp. 1478-1489, Mar. 2005.

[19] D.R. Stinson, *Cryptography Theory and Practice,* third ed. CRC Press, Nov. 2005.

[20] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," *ACM Trans. Programming Languages and Systems,* vol. 4, no. 3, pp. 382-401, July 1982.

[21] P. Papadimitratos and Z.J. Haas, "Secure Routing for Mobile Ad Hoc Networks," *Proc. SCS Comm. Networks and Distributed Systems Modeling and Simulation Conf. (CNDS '02),* Jan. 2002.

[22] J. Kong and X. Hong, "ANODR: Anonymous on Demand Routing Protocol with Untraceable Routes for Mobile Ad-Hoc Networks," *Proc. ACM MobiHoc '03,* pp. 291-302, June 2003.

[23] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks," *Proc. IEEE Int'l Conf. Local Computer Networks,* pp. 618-624, Nov. 2004.

[24] X. Wu and B. Bhargava, "AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol," *IEEE Trans. Mobile Computing,* vol. 4, no. 4, pp. 335-348, July-Aug. 2005.

[25] B. Zhu, Z. Wan, M.S. Kankanhalli, F. Bao, and R.H. Deng, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," *Proc. IEEE Int'l Conf. Local Computer Networks,* pp. 102-108, Nov. 2004.

[26] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "Recommendation for Key Management," Nat'l Inst. of Standards and Technology (NIST) Special Publication 800-57, May 2006.

[27] D.W. Carman, P.S. Kruus, and B.J. Matt, "Constraints and Approaches for Distributed Sensor Network Security," technical report, NAI Labs, Sept. 2000.

[28] *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs),* IEEE Standard 802.15.1, 2005.

[29] *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs),* IEEE Standard 802.15.4, 2006.

[30] J.P. Monks, V. Bharghavan, and W.-M.W. Hwu, "A Power Controlled Multiple Access Protocol for Wireless Packet Networks," *Proc. IEEE INFOCOM '01,* pp. 219-228, Apr. 2001.

[31] N. Bambos and S. Kandukuri, "Power-Controlled Multiple Access Scheme for Next-Generation Wireless Packet Networks," *IEEE Wireless Comm. Magazine,* vol. 9, no. 3, pp. 58-64, June 2002.

[32] T. ElBatt and A. Ephremides, "Joint Scheduling and Power Control for Wireless Ad-Hoc Networks," *IEEE Trans. Wireless Comm.,* vol. 3, no. 1, pp. 74-85, Jan. 2004.

[33] A. Behzad and I. Rubin, "Multiple Access Protocol for Power-Controlled Wireless Access Nets," *IEEE Trans. Mobile Computing,* vol. 3, no. 4, pp. 307-316, Oct.-Dec. 2004.

[34] V. Kawadia and P.R. Kumar, "Power Control and Clustering in Ad Hoc Networks," *Proc. IEEE INFOCOM '03,* pp. 459-469, Mar. 2003.

[35] R. Ramanathan and R. Rosales-Hain, "Topology Control of Multihop Wireless Networks Using Transmit Power Adjustment," *Proc. IEEE INFOCOM '00,* pp. 404-413, Mar. 2000.

[36] S. Narayanaswamy, V. Kawadia, R.S. Sreenivas, and P.R. Kumar, "Power Control in Ad Hoc Networks: Theory, Architecture, Algorithm, and Implementation of the COMPOW Protocol," *Proc. European Wireless Conf.,* pp. 156-162, Feb. 2002.

[37] S. Singh, M. Woo, and C.S. Raghavendra, "Power-Aware Routing in Mobile Ad Hoc Networks," *Proc. ACM/IEEE Int'l Conf. Mobile Computing and Networking,* pp. 181-190, Oct. 1998.

[38] A. El Gamal, J. Mammen, B. Prabhakar, and D. Shah, "Throughput-Delay Trade-Off in Wireless Networks," *Proc. IEEE INFOCOM '04,* pp. 464-475, Mar. 2004.

[39] M.J. Neely and E. Modiano, "Capacity and Delay Tradeoffs for Ad Hoc Mobile Networks," *IEEE Trans. Information Theory,* vol. 51, no. 6, pp. 1917-1937, June 2005.

[40] M.J. Neely, E. Modiano, and C.E. Rohrs, "Dynamic Power Allocation and Routing for Time-Varying Wireless Networks," *IEEE J. Selected Areas in Comm.,* vol. 23, no. 1, pp. 89-103, Jan. 2005.

[41] M.J. Neely, "Energy Optimal Control for Time-Varying Wireless Networks," *IEEE Trans. Information Theory,* vol. 52, no. 7, pp. 2915-2934, July 2006.

[42] S. Shakkottai, R. Srikant, and N. Shroff, "Unreliable Sensor Grids: Coverage, Connectivity and Diameter," *Proc. IEEE INFOCOM '03,* pp. 1073-1083, Mar. 2003.

[43] J.H. Reisert, "Understanding and Using Antenna Radiation Patterns," http://www.astronwireless.com/radiation_patterns.html, Aug. 2006.

[44] P. Gupta and P.R. Kumar, "The Capacity of Wireless Networks," *IEEE Trans. Information Theory,* vol. 46, no. 2, pp. 388-404, Mar. 2000.

[45] M. Grossglauser and D. Tse, "Mobility Increases the Capacity of Ad Hoc Wireless Networks," *IEEE/ACM Trans. Networking,* vol. 10, no. 4, pp. 477-486, Aug. 2002.

Jung-Chun Kao received the BS degree from National Taiwan University in 1999 and the MS degree from the University of Southern California in 2003, both in electrical engineering. He is currently a PhD student at Carnegie Mellon University, Pittsburgh, Pennsylvania. His research interests include analysis and optimization techniques in networked systems, ambient intelligence, wireless ad hoc networks, and wireless sensor networks. He is a student member of the IEEE.

Radu Marculescu received the PhD degree in electrical engineering from the University of Southern California in 1998. He is currently an associate professor in the Department of Electrical and Computer Engineering at Carnegie Mellon University, Pittsburgh, Pennsylvania. He was a recipient of the US National Science Foundation Faculty Early Career Development (CAREER) Award in 2001 in the area of design automation of electronic systems. He received the 2005 *IEEE Transactions on Very Large Scale Integration Systems* Best Paper Award from the IEEE Circuits and Systems (CAS) Society, two best paper awards from the Design Automation and Test in Europe (DATE) Conference in 2001 and 2003, and a best paper award from the Asia and South Pacific Design Automation Conference (ASP-DAC) in 2003. He was also awarded the Carnegie Institute of Technology Ladd Research Award in 2002. His current research focuses on developing design methodologies and software tools for system-on-chip design, on-chip communication, and ambient intelligence. He is a member of the IEEE and the ACM.