Eavesdropping Minimization via Transmission Power Control in Ad-Hoc Wireless Networks

Jung-Chun Kao and Radu Marculescu
Carnegie Mellon University
Pittsburgh, PA 15213
{*jungchuk,radum*}*@ece.cmu.edu*

***Abstract*— Reconnaissance activity is the most frequent incident on computer networks since 2002. In fact, most attacks (including DoS attacks) are usually preceded by reconnaissance activity. In order to defend against reconnaissance activity in ad-hoc wireless networks, we propose to use transmission power control as an effective mean to minimize the eavesdropping risk. Our main contributions are as follows: First, we cast the w-th 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 1st order eavesdropping risk as a 3rd-order polynomial function of *normalized transmission radius*. This derivation is based on the recently proposed model by El Gamal which 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 actually minimizes the 1st order eavesdropping risk. This result plays an essential role in deriving the first analytical bounds for the eavesdropping risk given *arbitrary* user distribution. Our simulation results show that for a wide range of *non-uniform* traffic patterns, the eavesdropping risk has the same order of magnitude as the corresponding uniform traffic cases.**

1. Introduction

An ad-hoc wireless network consists of a collection of autonomous nodes, all capable of transmitting and receiving user packets. Most of these nodes are *user nodes*, but *adversarial nodes* may also exist. During data transmission, a node consumes a finite amount of energy to broadcast packets over a wireless channel. Due to the existence of noise and interference in the wireless environment (e.g. the signal-to-interference-plus-noise ratio), the *transmission range* is finite.

This research is supported by CMU CyLab ARO under grant no. 9097.60.5 and by Frank J. Marshall Graduate Fellowship for Jung-Chun Kao.

A node, either user or adversarial node, can receive a packet only if it is located within the transmission range of the sending node. If an adversarial node intercepts the transmitted packet, it can attack the network and produce damage depending on the actual information contained in the eavesdropped packet. In fact, according to US-CERT [1], [2], the reconnaissance activity is the most frequent reported incident since 2002 and many attacks (including DoS attacks and unauthorized access incidents) are preceded by reconnaissance activity. These attacks (referred as to *hear-and-fire attacks*) result in what we call *eavesdropping risk*.

The eavesdropping risk causes a more severe security problem in ad-hoc wireless networks, compared to single-hop wireless networks or fixed wired networks. Due to the absence of an underlying communication infrastructure, the source and destination nodes in ad-hoc wireless networks rely heavily 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. It is important to note that this information (e.g. identity and privacy information) can be of critical importance since it can be used to identify the potential victims, conduct target-specific attacks, or break the cryptographic key in use.

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 [3], [4] focuses on developing a robust, efficient cryptosystem for protecting the data confidentiality under resource constraints. Important issues in designing such cryptosystems include key management, authentication and encryption/decryption algorithms.

These cryptographic techniques facilitate the design of secure and anonymous routing protocols in the presence of adversarial nodes. The adversarial nodes may com-

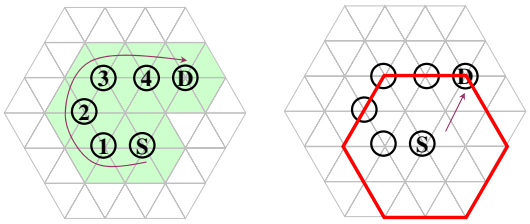

Fig. 1. A counterexample disproving the intuition that minimizing transmission power reduces the probability of a packet being eavesdropped. When a packet is sent from node S to node D at minimum transmission power (say the transmission radius $R = 1$), it is relayed via node $1, 2, \ldots, 4$ and an adversary residing in the green shadow can eavesdrop the packet. When the transmission radius is doubled ($R = 2$), 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 $26 : 24$, which is contrary to the intuition described above. For clarity reasons, we use triangle cells but the same idea can be illustrated with circular or square cells.

promise the network operation by exhibiting a *Byzantine* behavior [5], while being able to corrupt, replay and fabricate the routing packets. A secure routing protocol (e.g. [6]) is one which not only ensures data confidentiality, but also prevents the attacks mounted by the adversarial nodes from disrupting the connections between source-destination (*S-D*) pairs.

Conceptually, the 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 (e.g. [7]–[9]) needs to preserve the identity privacy. In a strict sense, an anonymous routing protocol requires preserving the identity privacy, location privacy and route anonymity (see [10] for the definitions of these three terms).

Unlike previous cryptography-based work, we propose the use of *transmission power control* in ad-hoc wireless networks as an effective approach for improving the network security by decreasing the *eavesdropping risk* probability. This is because smaller transmission range usually makes an adversary less likely to be able to eavesdrop packets. However, assessing the impact of transmission power control on the eavesdropping risk is *not* a trivial problem. For example, the simple intuition that minimizing the transmission power reduces the probability of a random packet to be eavesdropped is *not* true, in general. Figure 1 illustrates a counterexample where sending a packet at minimum transmission power actually makes an adversary easier to intercept the transmitted packets due to a long detour during packet transmission.

Interestingly enough, transmission power control can be used together with a cryptography-based technique to further protect the network security. One should also note that our proposal for transmission power control has a set of beneficial side effects such as improving network throughput, energy conservation, and quality-of-service support (e.g. [11]–[18]).

As main theoretical contribution, we study 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-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 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 El Gamal's model in [19] which assumes a uniform distribution of user nodes. This model is able to capture the geographical structure and interference properties of the ad-hoc wireless networks. Under the El Gamal's model, we derive a closed-form solution of the 1st order eavesdropping risk as a function of the transmission radius.
- Finally, we generalize the El Gamal's model to allow *arbitrary user* distributions and study their impact on the eavesdropping risk. To this end, we prove that the uniform user distribution minimizes the 1st order eavesdropping risk. So the uniform user distribution represents the *best-case scenario*. 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 bounds for the eavesdropping risk.

The remaining part 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 the 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 El Gamal's model [19]. Although the model assumes a uniform distribution

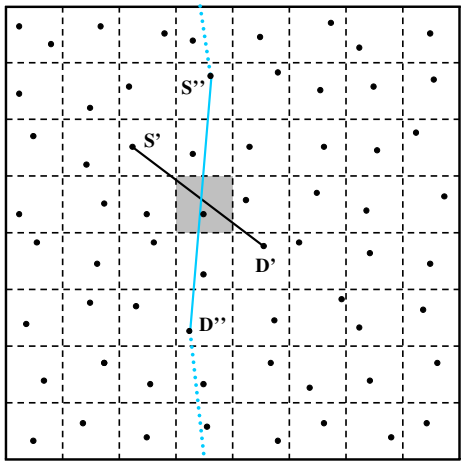

Fig. 2. In the El Gamal's model, the unit torus is divided into cells of size $a(n)$. Several S-D lines passing through the shaded cell are shown using solid lines.

of user nodes, we later relax this assumption so the definition used for the eavesdropping risk in this section can be applied to arbitrary user distributions.

2.1 The El Gamal's Model

In the model proposed by El Gamal (as illustrated in Figure 2), the network region described as a parameterized cell-partitioned unit torus (also referred to as 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. 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. So 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.[1] Note that both the normalized transmission range and the normalized transmission radius are fractional numbers in the interval (0,1]. The extreme case, $a(n) = 1$, corresponds to a configuration with a user node located one hop away from all other user nodes.

The packets originating from the source nodes always *pass through* the routes with the least number of hops when traveling towards their destinations. The *distance* between a S-D pair is defined as the number of hops of a minimal route from one end to the other end. For instance, the S'-D' pair in Figure 2 is 3 hops away, while the S"-D" pair is 4 hops away. It is possible to have multiple routes with the least number of hops between any S-D pair. For example, the solid and the dotted routes between the S"-D" pair in Figure 2 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 Figure 2 is $\rho = 1$, while the probability of the S"-D" pair passing through the shaded cell is $\rho = 1/2$.

The following theorem (reproduced from [19]) shows that each cell in the unit torus model will have at least one node with high probability (*whp*), thus guaranteeing successful transmission along every S-D pair. (Refer to El Gamal's paper [19] for the proof.)

Theorem 1: In a random network consisting of n nodes distributed independently and uniformly over a unit torus and cells with area $a(n)$ each, the following properties hold:

- $a)$ If $a(n) \geq 2\log n/n$, then all cells contain at least one node *whp*.[2]
- $b)$ For $a(n) = \Omega(\log n/n)$, each cell contains $na(n) \pm \sqrt{2na(n)\log n}$ nodes *whp*. In particular, if $a(n) = \omega(\log n/n)$ then each cell has $na(n) \pm o(na(n))$ nodes.
- $c)$ Let $a(n) = 1/n$ and let $c_k(n), k \geq 0$, be the fraction of cells with k nodes. Then *whp*, $c_k(n) = e^{-1}/k!$

2.2 Eavesdropping Risk

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

Now we give the definitions of the probability of packets being eavesdropped.

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

We note that the adversarial nodes 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 becomes then equivalent

[1]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.

[2]In this paper, *whp* means with probability $\geq 1 - 1/n$

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 *w-th 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 2: The *w-th eavesdropping risk* is defined as the maximum probability of packets being eavesdropped in the w-th eavesdropping risk problem.

One should note that the value of the w-th order eavesdropping risk is between 0 and 1. The larger this value is, the more likely the adversarial nodes eavesdrop the packets transmitted over the wireless channels. While 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 to reducing the eavesdropping risk are transmission power control and topology optimization.

Although of potential interest, physical-layer techniques (e.g. frequency hopping and spread spectrum communication) are not considered in this paper. These techniques do not improve network security under the assumption that, compared to a user node, an adversarial node uses a identical transceiver and has a 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 impact of 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 as follows: First, under the El Gamal's model, we derive the closed-form solution for the 1st order eavesdropping risk as a function of the normalized transmission radius. Then we generalize the El Gamal's model to allow *arbitrary* node distributions and prove that the uniform case provides a lower bound for such general scenarios. We will also show that this bound is tight for a wide range of traffic patterns (Section 4).

Theorem 2 below gives the closed-form formula of the 1st order eavesdropping risks under the El Gamal's model.

Theorem 2: In a random network consisting of n nodes distributed independently and uniformly over a unit torus, the 1st order eavesdropping risk for the best-case scenario is as follows:

a) If s is odd, then the 1st order eavesdropping risk for the best-case scenario is $R_1^*(r) = \frac{s^2+3s-1}{3s^3} = \frac{1}{3}r + r^2 - \frac{1}{3}r^3$

b) If s is even, then the 1st order eavesdropping risk for the best-case scenario 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 be the distance between S-D pair j (in terms of the number of hops). Define the Bernoulli random variables Y_j^h, for hops $0 \le h \le H_j$, to be equal to 1 if hop h of S-D pair j is located in a cell where an adversarial node resides.[4] Note that for all $h' \neq h$, the event of $Y_j^{h'} = 1$ is mutually exclusive to the event of $Y_j^h = 1$; this is because a single adversarial node cannot reside in two cells. Define the random variable Y_j as $\sum_{h=1}^{H_j} Y_j^h$. Due to mutual exclusion, the event of $Y_j = 1$ 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 the distance H_j between S-D pair j, is

$$\mathbf{E}[Y_j|H_j] = \mathbf{E}\left[\sum_{h=0}^{H_j} Y_j^h | H_j\right] = \sum_{h=0}^{H_j} \mathbf{E}[Y_j^h]$$
$$= (H_j+1)\cdot \mathbf{E}[Y_j^1] = (H_j+1)\cdot a(n) \quad (1)$$

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

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

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

[4]Hop 0 is the source node and hop H_j is the destination node.

eavesdropped:

$$R_1^*(r) = \mathbf{E}[Y_j] = \mathbf{E}_{H_j}[\mathbf{E}[Y_j|H_j]] \\ = \mathbf{E}_{H_j}[(H_j+1)\cdot a(n)] = a(n)\cdot(\mathbf{E}[H_j]+1) \quad (2)$$

where the third equality follows from equation (1).

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

a) When s is odd, the probability of the distance of S-D pair j being a hops away is

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

So the expectation of H_j is $\mathbf{E}[H_j] = \sum_{a=0}^{\frac{s-1}{2}} a \cdot \Pr[H_j = a] = \frac{s^2-1}{3s}$. By using equation (2), the eavesdropping risk is

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

b) When s is even, similarly to the odd case, we get:

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

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

and

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

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

The next step is to generalize the El Gamal's model to allow for *arbitrary* distributions. We prove that the functions provided in Theorem 3 actually serve as lower bounds under *any* distribution of user nodes.

Before delving into details, it is important to note that the following naive justification of Theorem 3—if the distribution of the users is not uniform, the attacker(s) will go to the most crowded cell(s) to intercept most communication and therefore the uniform distribution of user nodes minimizes the eavesdropping risk—is plain wrong. Figure 3 shows a counterexample of why this intuition is wrong.[5] This necessitates a rigorous proof as given below for Theorem 3.

[5]For simplicity of exposition, Figure 3 only represents the highest-order terms.

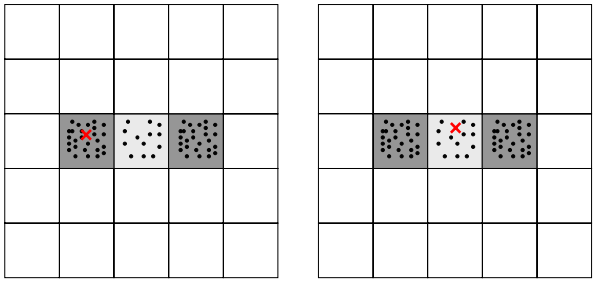

Fig. 3. A counterexample to disprove the naive intuition that the uniform user distribution minimizes the eavesdropping risk because otherwise the attacker will go to the most crowded cell to intercept most communication. Assume there are $2n$ user nodes residing in each dark grey cell, n user nodes in each light grey cell and 0 user node in other cells. By this intuition, the attacker maximizes the eavesdropping volume (in terms of the number of eavesdropping S-D pairs) by moving to a dark grey cell. However, if doing so, the eavesdropping volume $(2n)^2/2+(2n)(n+2n) = 8n^2$ is *not* maximal because an attacker residing in a light grey cell can eavesdrop $n^2/2+n(4n)+(2n)(2n) = 8.5n^2$ S-D pairs.

Theorem 3: Given n arbitrarily deployed user nodes, the 1st order eavesdropping risk is minimized under the uniform geographic distribution of user nodes.

Proof: Because the rigorous proof is too lengthy, we sketch its main steps but omit the details. In Step 1, the 1st order eavesdropping risk is formulated in a min-max form. Denoting the total number of cells by $k = 1/r^2$ and the distribution of user nodes by a vector $N = (n_0, n_1, \ldots, n_{k-1})$ where n_i is the number of user nodes in cell i, the 1st order eavesdropping risk can be derived as:

$$R_1^*(r) = \min_{N \in N_k^n} \max(f_0(N), f_1(N), \ldots, f_{k-1}(N))$$

where N_k^n is the set of k-dimensional vectors whose components sum up to n,

$$f_i(N) = \frac{2}{n(n+1)}\left(n_i n + \sum_{\substack{0\le a<b\le k-1 \\ a,b\neq i}} \rho_i(a,b) n_a n_b\right)$$

is the probability of packets being eavesdropped when an adversary resides in cell i, and $\rho_i(a,b)$ is the probability that a packet sent from node a to node b passes through cell i.

Obviously, the 1st order eavesdropping risk is non-linear and multivariate. Because of the intractability of solving the min-max formula from an algebraic perspective, we take a hybrid approach that uses both algebra and geometry. In Step 2, we discover that each f_i satisfies the property of *polarity persistency*; that is, its

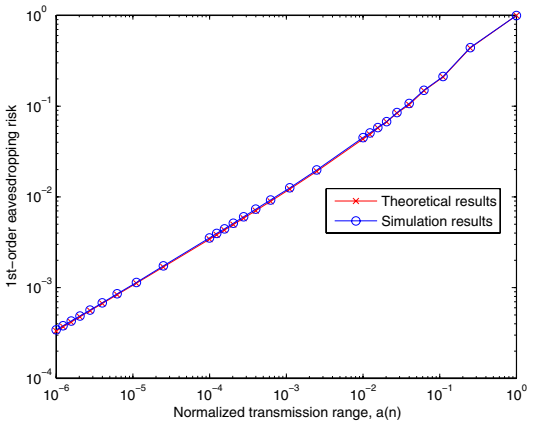

Fig. 4. This figure shows the consistency between the theoretical 1st order eavesdropping risks under uniform traffic and the corresponding simulation results.

gradient $\nabla f_i(N)$ has at least one component keeping its sign within the domain of interest N_k^n. In Step 3, we use this geometric property to prove that $R_1^*(r)$ has a local minimum at $N = (n/k, n/k, \ldots, n/k)$ which corresponds to the uniform distribution of user nodes. In Step 4, we take an algebraic approach to prove that this local minimum is the global minimum within the domain of interest N_k^n. ■

Theorem 3 proves that the uniform user distribution minimizes the 1st order eavesdropping risk, while Theorem 2 gives its closed-form formulae. Combining these two theorems together results into the following general theorem:

Theorem 4: In an arbitrary random network consisting of n nodes, the 1st order eavesdropping risk is bounded below by $\frac{1}{3}r$, where r is the normalized transmission radius.

Proof: By Theorem 3, we know that the formulae given in Theorem 2 are lower bounds. Since $0 < r \leq 1$, both $r^2 - \frac{1}{3}r^3$ and $r^2 + \frac{1}{6}r^3$ are greater than 0. Therefore, in either odd or even cases, $R_1^*(r) \geq \frac{1}{3}r$. ■

4. Simulation Results

4.1 The 1st Order Eavesdropping Risk

In this section, we show that for the 1st order eavesdropping risk, the theoretical values and the simulation results under uniform traffic are consistent with each other. The simulation configurations are as follows: In each iteration, a S-D pair is chosen at random. Then, a packet is transmitted from the source node to the destination node along the route with the least number of hops. (In case there are multiple shortest routes, one of them is chosen randomly.) 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 1st order eavesdropping risks.

The total number of iterations is set to be proportional to the number of cells but has a 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 Figure 4, the simulated 1st order eavesdropping risk values under uniform traffic are very close to their corresponding theoretical counterparts. Indeed, the difference between them is always less than 3.79% in this simulation setup. [6] Figure 4 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 Non-Uniform Traffic

Unlike Section 4.1 where the traffic volume between any S-D pair is identical, in this section, we first use the Gaussian traffic to validate the correctness of our proposed lower bounds (in addition to the mathematical proof in Section 3). Second, we try to see whether or not the eavesdropping risk under a wide range of traffic patterns can be reasonably approximated with the theoretical bounds.

In this simulation setup, we focus on a 10-by-10 unit torus (*i.e.* its normalized transmission range is $a(n) = 0.01$). The traffic volume 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 100 packets and a standard deviation ranging from 1 to 10000. For each Gaussian traffic with a given standard deviation, we generate 20 samples and simulate the individual eavesdropping risk.

As shown in Figure 5, 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.

[6] Actually, increasing the number of iterations can further reduce this difference.

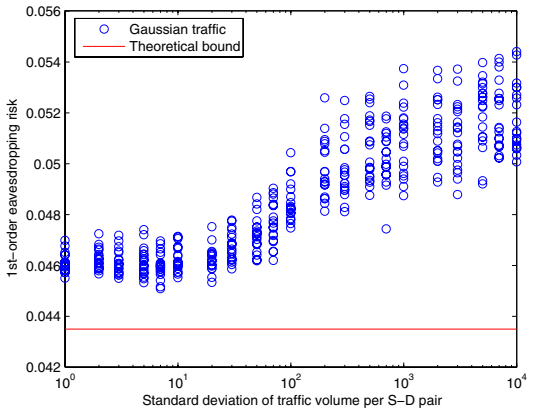

Fig. 5. This figure shows the 1st order eavesdropping risk under Gaussian traffic in a 10-by-10 unit torus network (*i.e.* $a(n) = 0.01$). Each circle represents an individual result without being averaged. Please note that the eavesdropping risk under Gaussian traffic can be appropriately approximated by our proposed lower bound within the same order of magnitude.

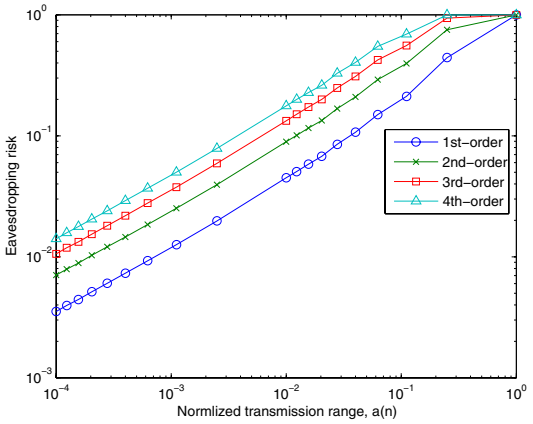

Fig. 6. Higher order eavesdropping risks under uniform traffic

4.3 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. Note that each eavesdropped packet has an equal contribution to the eavesdropping risk, regardless of how many adversarial nodes actually eavesdrop it. In other words, each eavesdropped packet is counted only once. The simulation results are shown in Figure 6.

As observed in Figure 6, the w-th order eavesdropping risk is an increasing function with respect to w, but its value is at most w times as large as the 1st 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 (*i.e.* 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 w-th order eavesdropping risk significantly. Our simulations also show that when the normalized transmission range is small enough, the w-th order eavesdropping risk is approximately w times as large as the 1st order eavesdropping risk. This (approximately) linear dependency supports that the idea of using transmission power control in a wide, large-scale ad-hoc wireless network where multiple adversarial nodes can exist.

5. Conclusion

In this paper, we have analyzed the impact of the transmission range and user distribution on the eavesdropping risk, when there is one or more adversarial nodes in an ad-hoc wireless network.

As main contributions, we have defined the w-th 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 1st order eavesdropping risk under uniform traffic as a function of normalized transmission radius. For non-uniform traffic, we have identified the best-case scenario (in terms of the 1st order eavesdropping risk) and proved a lower bound given arbitrary traffic patterns. Furthermore, our simulation results show the tightness of this lower bound for a wide range of traffic patterns. We have also shown that adjusting transmission range can result in a significant reduction of the eavesdropping risk.

In a more general context, transmission power control can not only help to better protect the network security, but also improve the network throughput, energy conservation and quality-of-service. While 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 with no consideration of security, our results provide the first analytical treatment of using transmission power control as a defense mechanism against the reconnaissance activity.

References

[1] United States Computer Emergency Readiness Team. (2006, Feb.) Statistics on federal incident reports. [Online]. Available: http://www.us-cert.gov/federal/statistics/

[2] NIST Special Publications 800-61, "Computer security incident handling guide," announced by Nat'l Inst. of Standards and Technology, Jan. 2004.

[3] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53–57, June 2004.
[4] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in *Proc. IEEE INFOCOM*, Hong Kong, Mar. 2004, pp. 586–597.
[5] 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.
[6] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks," in *Proc. SCS Communication Networks and Distributed Systems Modeling and Simulation Conf. (CNDS)*, San Antonio, USA, Jan. 2002.
[7] J. Kong and X. Hong, "ANODR: Anonymous on demand routing protocol with untraceable routes for mobile ad-hoc networks," in *Proc. ACM MobiHoc*, Annapolis, USA, June 2003, pp. 291–302.
[8] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: A secure distributed anonymous routing protocol for wireless and mobile ad hoc networks," in *Porc. IEEE Intl. Conf. on Local Computer Networks*, Tampa, USA, Nov. 2004, pp. 618–624.
[9] 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.
[10] B. Zhu, Z. Wan, M. S. Kankanhalli, F. Bao, and R. H. Deng, "Anonymous secure routing in mobile ad-hoc networks," in *Proc. IEEE Intl. Conf. on Local Computer Networks*, Tampa, USA, Nov. 2004, pp. 102–108.
[11] J. P. Monks, V. Bharghavan, and W.-M. W. Hwu, "A power controlled multiple access protocol for wireless packet networks," in *Proc. IEEE INFOCOM*, Anchorage, USA, Apr. 2001, pp. 219–228.
[12] N. Bambos and S. Kandukuri, "Power controlled multiple access scheme for next-generation wireless packet networks," *IEEE Wireless Commun. Mag.*, vol. 9, no. 3, pp. 58–64, June 2002.
[13] T. ElBatt and A. Ephremides, "Joint scheduling and power control for wireless ad-hoc networks," *IEEE Trans. Wireless Commun.*, vol. 3, no. 1, pp. 74–85, Jan. 2004.
[14] 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.
[15] T. J. Kwon and M. Gerla, "Clustering with power control," in *Proc. IEEE Military Communications Conf.*, Atlantic City, USA, Oct. 1999, pp. 1424–1428.
[16] R. Ramanathan and R. Rosales-Hain, "Topology control of multihop wireless networks using transmit power adjustment," in *Proc. IEEE INFOCOM*, Tel-Aviv, Israel, Mar. 2000, pp. 404–413.
[17] 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," in *Proc. European Wireless Conf.*, Florence, Italy, Feb. 2002, pp. 156–162.
[18] S. Singh, M. Woo, and C. S. Raghavendra, "Power aware routing in mobile ad hoc networks," in *Proc. ACM/IEEE Intl. Conf. on Mobile Computing and Networking*, Dallas, USA, Oct. 1998, pp. 181–190.
[19] A. E. Gamal, J. Mammen, B. Prabhakar, and D. Shah, "Throughput-delay trade-off in wireless networks," in *Proc. IEEE INFOCOM*, Hong Kong, Mar. 2004, pp. 464–475.