Secure Capacity of Multi-Hop Wireless Networks with Random Key Pre-distribution

Technical Report (December 2007)

Vartika Bhandari
Dept. of Computer Science, and
Coordinated Science Laboratory
University of Illinois at Urbana-Champaign
vbhandar@uiuc.edu

Nitin H. Vaidya
Dept. of Electrical and Computer Eng., and
Coordinated Science Laboratory
University of Illinois at Urbana-Champaign
nhv@uiuc.edu

I. Introduction

It is usual to quantify the performance of communication networks in terms of achievable throughout or delay. The past decade or so has also seen the gradual evolution of a theoretical structure for analysis of the scaling of wireless network performance. Gupta and Kumar [1] established the necessary and sufficient conditions for connectivity in a randomly deployed network. Subsequently, in their seminal paper [2] they defined a notion of transport capacity and established capacity results for arbitrary and random networks. Since then there have been a plethora of capacity results for wireless networks under different models and assumptions. Simultaneously, there have been efforts at quantification of the performance of wireless networks in the non-asymptotic regime, e.g., [3].

It is to be noted that these results have focused on traditional measures of performance, viz., throughput (capacity) (and/or in some cases delay), without taking into consideration the possible need to secure communication against failure/subversion/disruption. *As security and reliability concerns gradually emerge at the forefront of networking research, it is increasingly crucial to consider secure communication capacity/delay as primary performance measures*. Inherent in this argument is the recognition that security has a cost. Securing communication against subversion or disruption will typically require more resources (in terms of bandwidth and/or hardware capabilities); traditional performance measures fail to take this into account.

While quantifying the impact of security has general relevance, it is particularly significant in the case of wireless networks, where the medium is shared, and resources (e.g. energy) are often scarce. Thus wireless protocol design must carefully take into account the performance degradation expected as a result of improving the security characteristics. The impact of security on wireless network performance has been studied empirically in some past work [4], [5]. There has also been work on quantifying secure capacity in an information-theoretic sense. However, further work on developing a theoretical structure is needed, especially in the context of analyzing protocol performance.

A formal quantification of the cost of security can be quite beneficial, as it can facilitate evaluation of the desirability of specific security solutions. It can also allow for exploration of suitable trade-offs between security and efficiency, and enable protocol designers to reason about desirable operating points that balance both concerns. To this effect, performance measures need to be redefined in a secure wireless network. The notion of network connectivity also requires a fresh definition.

As an illustration of the same, we obtain a result for secure asymptotic connectivity and capacity of randomly deployed wireless networks in a scenario where each node is loaded with a random subset of keys prior to deployment, and nodes can securely communicate only with neighbors with whom they share at least one common key.

II. Defining Secure Connectivity

As per the traditional definition of connectivity, a network is said to be connected if and only if each pair of nodes in the network is connected via at least one path.

Another way to view connectivity is to say that if a node wishes to broadcast a message to all other nodes in the network, it is indeed possible to do so. If the network is connected then broadcast is possible. If broadcast is possible, then the network must be connected. Thus, connectivity is equivalent to achievability of broadcast.

This alternative definition of connectivity is useful when one seeks to extend the notion to a network where there may be attempts at subverting communication. In such a network, connectivity may be defined thus: *the network is said to be connected if and only if each pair of non-faulty nodes in the network can communicate reliably (securely) with each other*.

This research is supported in part by NSF grant CNS 06-27074, US Army Research Office grant W911NF-05-1-0246, and a Vodafone Graduate Fellowship.

III. Notation and Terminology

We use the following asymptotic notation:

- $O(g(n)) = \{f(n) | \exists c, N_o, \text{ such that } f(n) \leq cg(n) \text{ for } n > N_o\}$
- $o(g(n)) = \{f(n) | \lim_{n\to\infty} \frac{f(n)}{g(n)} = 0\}$
- $\omega(g(n)) = \{f(n) | g(n) = o(f(n))\}$
- $\Omega(g(n)) = \{f(n) | g(n) = O(f(n))\}$
- $\Theta(g(n)) = \{f(n) | \exists c_1, c_2, N_o, \text{ such that } c_1 g(n) \leq f(n) \leq c_2 g(n) \text{ for } n > N_o\}$

Whenever we use a term $\log(x)$, we are referring to the natural logarithm of x.

IV. The Model

In this section, we describe the model that we use for the secure capacity results in this paper. We adopt the approach of asymptotic capacity analysis which was introduced in the seminal paper by Gupta and Kumar [2]. In this approach, the goal is to investigate how network performance scales as we increase the node population in the network. Asymptotic results can be useful in that apart from helping to understand scaling behavior of very large networks, they also provide useful insights into the issues encountered, many of which are common to networks at all scales. Moreover, the general trends obtained from asymptotic analysis have often be very similar to those encountered in practice, e.g., it was found in [3] that the general trends for multi-channel capacity established in [6] conformed to trends observed for smaller-scale networks.

We consider a network of *n single-interface* nodes randomly deployed over a unit torus. Each node is the source of exactly one flow. As in [2], each source S selects a destination by first fixing on a point D' uniformly at random, and then picking the node D (other than itself), that is closest to D'. All communication occurs over a single channel of bandwidth W. All multi-hop communication is assumed to occur via the store-and-forward paradigm.

Per-flow Capacity: As per the definition introduced in [2], the per-flow capacity is said to be $\Theta(f(n))$ if there exist constants c_1, c_2 such that:

1) $\lim_{n\to\infty} Pr[$ each flow can be given throughput $c_1 f(n)] = 1$
2) $\lim_{n\to\infty} Pr[$ each flow can be given throughput $c_2 f(n)] < 1$

Per-flow secure capacity: Along the lines of the definition of secure connectivity, we can define a notion of *secure capacity* as follows: the per-flow capacity is said to be $\Theta(f(n))$ if there exist constants c_1, c_2 such that:

1) $\lim_{n\to\infty} Pr[$ each flow can securely communicate data with throughput $c_1 f(n)] = 1$
2) $\lim_{n\to\infty} Pr[$ each flow can securely communicate data with throughput $c_2 f(n)] < 1$

V. Secure Capacity with Random Key Pre-distribution

Random key pre-distribution for sensor networks was first proposed in [7]. In this model, sensor nodes are pre-loaded with a random subset of cryptographic keys, and then deployed. Thereafter, two neighboring nodes can commmunicate securely only if they share at least one common key. Thus, if an adversary gains control of a single node (or a few nodes), it only gains access to a subset of the keys, and cannot eavesdrop on all ongoing communication in the network.

Some results analyzing network connectivity when each node is assigned a random subset of keys have been presented in [7]. However, instead of a precise formulation for random geometric graphs, these rely on using results for random graphs, and assume the communication probability for each node-pair to be independent (it actually exhibits correlation, e.g., suppose A and B have the same set of keys; if C shares a key with A, it is guaranteed to share a key with B). Moreover, the issue of multi-hop routing in such scenarios has not been formally analyzed.

Some recent work by us [8], [9] has studied the capacity of multi-channel wireless networks where radios are subject to *switching constraints*. In these scenarios, there are c channels of equal bandwidth available. Each individual (half-duplex) radio-interface is pre-assigned a subset of f channels out of c. Thereafter it can only switch on these f channels. The a priori assignment of f channels could occur in many different ways, and some constraint models were proposed to capture some such scenarios. One of the considered constraint models was termed random (c, f) assignment. In this model, each radio is pre-assigned f channels uniformly at random out of c available channels.

These multi-channel results can be interpreted in this context by viewing the ability to switch on a channel as being equivalent to having a certain key. Each node is pre-loaded with a subset of f keys out of c. Thus the random (c, f) model of [8], [9] maps to pre-distribution of uniformly random f-subsets of keys. Connectivity conditions and properties are the same for the case of both channels and keys. In [8], the critical connectivity range was shown to be $\Theta(\sqrt{\frac{\log n}{p_{rnd} n}})$ for random (c, f) assignment and $c = O(\log n)$, and the same continues to hold for this case.

As was first shown in [2], a transmission range of $r(n)$ imposes a capacity upper bound of $O(\frac{W}{nr(n)})$ by limiting the maximum number of concurrent transmissions possible. Thus we obtain that the capacity with random key pre-distribution is $O(W\sqrt{\frac{p_{rnd}}{n \log n}})$.

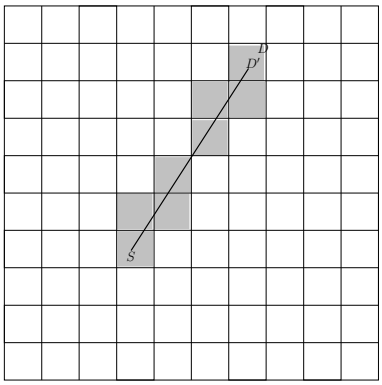

Fig. 1. Routing along a straight line

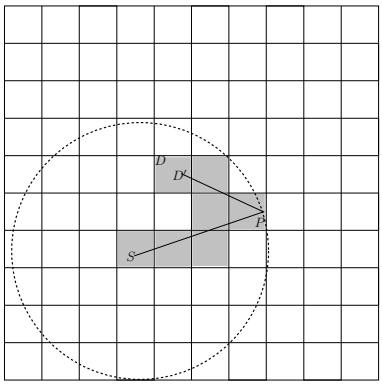

Fig. 2. Illustration of detour routing

Moreover, a route that is valid for multi-hop communication with random (c, f) assignment, is valid in the corresponding key-based scenario. But the capacity outlook is different in that there is only one channel spanning all the available bandwidth. However, it is easy to obtain a feasible schedule for the key scenario from a schedule for the channel scenario as follows:

Given a network instance, construct a feasible random (c, f) schedule as described in [9]. As per the description in [9], this schedule is two-level, i.e., each round is divided into a constant number of cell-slots, and each cell gets one slot per round for its transmissions. Each cell-slot is further divided into sub-slots in which individual packet transmissions get scheduled.

The key schedule retains the assignment of cells to slots. However, the scheduling within a cell-slot is obtained via a *serialization* of the scheduling in the corresponding cell-slot of the random (c, f) schedule, as follows: divide each sub-slot further into c equal sub-sub-slots. In the random (c, f) schedule, each sub-slot could have at most c concurrent transmissions going on at rate $\frac{W}{c}$ each. Now each such transmission is exclusively assigned one sub-sub-slot, and occurs at rate W (since there is one channel that supports data-rate W).

It is easily seen that this is a feasible schedule for the key pre-distribution scenario. Thus, one can deduce that capacity with keys is $\Omega(W\sqrt{\frac{p_{rnd}}{n\log n}})$. An upper bound was established using the necessary conditions for connectivity. Then, from the multi-channel results presented in [8], [9], it can be deduced that the capacity with a random (c, f) key pre-distribution, with $c = O(\log n)$ is $\Theta(W\sqrt{\frac{p_{rnd}}{n\log n}})$. When $f = \Omega(\sqrt{c})$, $p_{rnd} = 1$ and one achieves order-optimal capacity.

Of particular interest is the construction used in [9] to achieve this capacity, which provides insights into routing in such networks. While [10] discusses the notion of replacing a direct neighbor link with multiple hops, they do not consider global routing. In the routing construction for random (c, f) assignment, each route must traverse a certain minimum number of intermediate hops. The need for this can be intuitively explained as follows: it is possible that a source S and its destination D may not switch on any common channel. Thus one needs to find a sequence of nodes $S, R_1, R_2, ..., R_l$ such that each consecutive pair of nodes $(S, R_1), (R_1, R_2), ..., (R_l, D)$ has one common channel; thus S can send packets on one of its f channels, and the destination will be able to receive them on one of its f channels. If the straight-line route from source to destination (Fig. 1) provides the required minimum number of hops, then the straight-line route is taken. However if S and D are very close to each other, the straight-line route may be too short, and the route is artificially made longer by taking a *detour* (Fig. 2). Routing with keys would also require similar detour strategies to ensure and end-to-end secure path from source to destination.

VI. Conclusion

We have established secure capacity results for wireless networks with random key pre-distribution, based on past work by us on multi-channel wireless networks with channel-switching constraints. These results also shed light on the routing implications and issues in such scenarios.

VII. Acknowledgement

We thank Matthew Miller who first drew our attention to the potential similarity between our multi-channel switching constraint models and random pre-distribution of cryptographic keys.

References

[1] P. Gupta and P. R. Kumar, "Critical power for asymptotic connectivity in wireless networks," in *Stochastic Analysis, Control, Optimization and Applications: A Volume in Honor of W.H. Fleming*, W. M. McEneany, G. Yin, and Q. Zhang, Eds. Boston: Birkhauser, 1998, pp. 547–566.

[2] ——, "The Capacity of Wireless Networks," *IEEE Transactions on Information Theory*, vol. IT-46, no. 2, pp. 388–404, March 2000.

[3] M. Kodialam and T. Nandagopal, "Characterizing the capacity region in multi-radio multi-channel wireless mesh networks," in *MobiCom '05: Proceedings of the 11th annual international conference on Mobile computing and networking*. ACM Press, 2005, pp. 73–87.

[4] A. K. Agarwal and W. Wang, "Measuring performance impact of security protocols in wireless local area networks," in *Proc. of 2nd IEEE International Conference on Broadband Networks– Broadband Wireless Networking Symposium*, Oct. 2005.
[5] ——, "On the impact of quality of protection in wireless local area networks with ip mobility," *Mob. Netw. Appl.*, vol. 12, no. 1, pp. 93–110, 2007.
[6] P. Kyasanur and N. H. Vaidya, "Capacity of Multi-channel Wireless Networks: Impact of Number of Channels and Interfaces," in *MobiCom '05: Proceedings of the 11th annual international conference on Mobile computing and networking*. ACM Press, 2005, pp. 43–57.
[7] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *CCS '02: Proceedings of the 9th ACM conference on Computer and communications security*. ACM Press, 2002, pp. 41–47.
[8] V. Bhandari and N. H. Vaidya, "Connectivity and Capacity of Multichannel Wireless Networks with Channel Switching Constraints," in *Proceedings of IEEE INFOCOM*, Anchorage, Alaska, May 2007, pp. 785–793.
[9] ——, "Capacity of multi-channel wireless networks with random (c, f) assignment," in *MobiHoc '07: Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing*. ACM Press, 2007, pp. 229–238.
[10] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," *ACM Trans. Inf. Syst. Secur.*, vol. 8, no. 2, pp. 228–258, 2005.