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

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

***Abstract*— It is usual to quantify the performance of communication networks in terms of achievable throughput or delay. However, as a result of the significant recent interest in safety-critical application scenarios for wireless networking, security and reliability concerns are gradually emerging at the forefront of wireless networking research. In light of this, it is increasingly crucial to consider secure communication capacity or delay as primary performance measures, and evolve theoretical frameworks that can allow for quantification of the trade-off between security and performance. In this paper, we argue for the need for comprehensive effort in this direction, and present an illustrative example of the same by describing asymptotic secure-capacity results for randomly deployed wireless network where each node is preloaded with a random subset of keys.**

I. Introduction

It is usual to quantify the performance of communication networks in terms of achievable throughput 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]. There is also a substantial body of work on characterising stable "throughput-optimal" schedulers [4].

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.

This research is supported in part by US Army Research Office grant W911NF-0710287, and a Vodafone Graduate Fellowship.

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 [5], [6]. There has also been work on quantifying secure capacity in an information-theoretic sense [7], including work on capacity of secure network coding [8]. However, further work on developing a theoretical structure is needed, especially in the context of analyzing and quantifying security-performance trade-offs.

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 revisited in a secure wireless network.

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. Security and Reliability Issues in Wireless Networks

While security and reliability are relevant in both wired and wireless networks, the distinct nature of wireless communication exposes wireless networks to additional attack models that are not encountered in wired networks. Typically, this is because the wireless medium is a *shared* broadcast medium, which easily allows for the possibility of (1) eavesdropping (2) disruption of legitimate communication via jamming, in addition to the possibility of message-tampering by malicious relay nodes. Of these, the issues of eavesdropping and tampering can be addressed via end-to-end encryption/authentication;

however for many scenarios, e.g., sensor networks, a public-key infrastructure may be too expensive to deploy. Thus, more lightweight solutions may be required.

It must be noted that though the broadcast nature of the medium gives rise to new attack models, it also provides new opportunities for detection and handling of malicious behavior. In this regard, recent results on Byzantine fault-tolerant broadcast in wireless networks (e.g., [9], [10], [11], [12], [13], [14]) are of significant interest, as these highlight some of the advantages as well as disdvantages of having a broadcast medium. They also provide insights into how reliable communication (in the sense of resilience from message tampering) can be achieved without public-key infrastructure, and expose some of the trade-offs in message-complexity and fault-tolerance.

To avoid eavesdropping, a lightweight approach involves link-layer encryption, whereby each pair of neighboring nodes shares a common key; packets exchanged by them are encrypted before transmission, and decrypted after receipt. Additional discussion on benefits and limitations of link-layer encryption is available in [15]. Providing all nodes with a single common key makes the system vulnerable, as the adversary only needs to compromise one node to be able to decrypt any communication in the network. Thus, various key pre-distribution schemes have been proposed, e.g., [16]. Key pre-distribution and associated performance trade-offs is the focus of this paper.

Other approaches involve exploiting physical layer diversity in the wireless network, e.g., in [17], the presence of multiple channels was used to facilitate post-deployment key distribution in the presence of non-colluding eavesdropping adversarial nodes. In [18], a scenario is considered where there are multiple channels, and the adversary can only jam one or few of these. Deterministic algorithms for an operation termed ε-gossip in such a scenario are described.

What is important in all these scenarios is that given the specific characteristics of the wireless physical layer, there are many interesting trade-offs that arise. Thus, from the viewpoint of a network designer who seeks to not only design suitable algorithms for a given network, but potentially decide what physical layer attributes/parameters would better facilitate secure protocols, it is extremely important to study these issues in detail. As stated in Section I, we provide an example of the same in this paper, by obtaining results for asymptotic secure connectivity and capacity in a key pre-distribution scenario.

III. Notation and Terminology

We use the following standard asymptotic notation [19]:

- $f(n) = O(g(n))$ means that $\exists c, N_o$, such that $f(n) \leq cg(n)$ for $n > N_o$
- $f(n) = o(g(n))$ means that $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$
- $f(n) = \omega(g(n))$ means that $g(n) = o(f(n))$
- $f(n) = \Omega(g(n))$ means that $g(n) = O(f(n))$
- $f(n) = \Theta(g(n))$means that $\exists c_1, c_2, N_o$, such that $c_1 g(n) \leq f(n) \leq c_2 g(n)$ 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 tend to be similar to those encountered in practice.

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.

Given the security requirement, the network is said to be connected if and only if each non-faulty node in the network is capable of sending a message to all other non-faulty nodes in a secure manner.

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

Per-flow secure capacity: Along similar lines, one may conceive of defining a notion of *secure capacity* which is similar to the definition of capacity, except that we now consider the achievable throughput for communication that satisfies the desired notion of *security* (which may vary depending on the context).

There are two different ways of viewing the notion of secure capacity. One may be termed as *pre-attack* or *quiescent* secure capacity, wherein the network is pre-configured to face certain attacks (at some cost), and the pre-attack secure capacity yields the per-flow secure throughput that can be guaranteed before any node is compromised. Thus, this definition allows one to quantify the cost of the *a priori* mechanisms that are in place.

Another way of viewing secure capacity is to seek to quantify the secure throughput that can be guaranteed to all (or a large fraction of) flows originating/terminating at uncompromised nodes, given that some nodes have indeed been compromised. This can be termed as *post-attack* secure capacity. This view also involves quantifying the number of node-compromises that can be effectively tolerated without making an acceptable level of security impossible to achieve. The nature of this definition requires a specific model of what is *acceptable* security.

Moreover, the above two notions of security also highlight the need to differentiate security-related mechanisms as *a priori* and *on demand* mechanisms. The former can degrade the pre-attack capacity, even in the absence of any attack, but may be easier to put into place. The latter are more desirable from the viewpoint of efficiency; but may require sophisticated approaches for detection of an attack, so that the on-demand mechanisms may be triggered. Thus, a practically desirable solution may involve a hybrid approach.

In this paper, we restrict our discussion to *pre-attack* secure capacity, which can be defined as the minimum per-flow throughput that can guaranteed to each flow while using the *a priori* mechanisms. Moreover, we consider a specific example scenario, where an adversary may attempt to overhear communication in the network. The *a priori* mechanism used is that of link-layer encryption, and to reduce the impact of one (or a few) nodes being compromized, random key pre-distribution is used. We discuss this further in the next section.

V. Random Key Pre-distribution

Random key pre-distribution for sensor networks was first proposed in [16]. 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 [16]. 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.

In [20], the issue of connectivity with random key pre-distribution is considered for random geometric graphs. They consider an approximate model wherein the keys are assigned *with replacement*. Since key assignment with replacement can only reduce connectivity for a certain key-set size, the sufficient condition obtained by them for the *with replacement* case is also a sufficient condition for the *without replacement* case.

There is a vast body of subsequent work on a wide range of key establishment and management techniques, e.g, [21], [22], [23].

In subsequent sections we establish necessary and sufficient conditions for connectivity and establish the pre-attack secure capacity for the random key pre-distribution scheme described in [16], by leveraging some of our prior work on multi-channel wireless networks with channel switching constraints [24], [25].

VI. Switching Constraints in a Multi-Channel Wireless Network

As was mentioned in the previous section, we leverage prior results regarding multi-channel wireless networks with channel switching constraints, in order to obtain results for scenarios with random key pre-distribution. In this section, we briefly discuss those multi-channel scenarios.

In recent work [24], [25], we have 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 node is equipped with a single (half-duplex) radio-interface. Each individual 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, where $c = O(\log n)$.

VII. Deriving Secure Capacity Results Using Multi-Channel Results

The multi-channel model discussed in Section VI 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, with $c = O(\log n)$. Thus the random (c, f) model of [24], [25] maps to pre-distribution of uniformly random f-subsets of keys (which we will refer to as random (c, f) key pre-distribution), and the results for the former can be mapped to results for the latter, as we discuss further.

The probability that any two nodes have at least one common key (channel) is given by $p_{rnd} = 1 - (1 - \frac{f}{c})(1 - \frac{f}{c-1})...(1 - \frac{f}{c-f+1})$. As was discussed in [25], $p_{rnd} \geq 1 - e^{-\frac{f^2}{c}}$. Thus, $f = \Omega(\sqrt{c}) \implies p_{rnd} = \Omega(1)$, i.e., there is a rapid convergence of p_{rnd} to 1. Such fast convergence (in the context of keys) was also empirically demonstrated in [16].

A. Connectivity

It is not hard to see that connectivity conditions and properties are the same for the case of both channels and keys. In the multi-channel scenario, two nodes within each others' range can communicate if and only if they can switch on some common channel. In the corresponding key scenario, two nodes within each others' range can communicate securely if and only if they share a common key that can be used to encrypt data transmitted between them.

In [24], the critical connectivity range [1] was shown to be $\Theta(\sqrt{\frac{\log n}{p_{rnd} n}})$ for random (c, f) assignment and $c = O(\log n)$.

[1] The critical range for connectivity is said to be $\Theta(f(n))$ if $\lim_{n\to\infty} \Pr[\text{network is connected}] = 1$ when the transmission range is at least $c_1 f(n)$ (for a suitable constant c_1), but $\lim_{n\to\infty} \Pr[\text{network is connected}] < 1$ if the transmission range is less than or equal to $c_2 f(n)$ (for another suitable constant $c_2 < c_1$).

Thus, it follows that the critical range for secure connectivity with random (c, f) key pre-distribution is also $\Theta(\sqrt{\frac{\log n}{p_{rnd} n}})$.

B. Upper Bound on Capacity

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 (c, f) key pre-distribution is $O(W\sqrt{\frac{p_{rnd}}{n \log n}})$.

C. Lower Bound on Capacity

It is easy to see that a route that is valid for multi-hop communication with random (c, f) assignment is also a valid route for secure communication in the corresponding key-based scenario. This is because each pair of consecutive nodes on that route are guaranteed to share at least one common channel, which maps to sharing a common key in the key-based scenario. Thus the data on each hop can be encrypted using the shared key.

However, there is one difference in the two scenarios: in the multi-channel scenario, there are c channels of bandwidth $\frac{W}{c}$ each, while in the corresponding key-based scenario, there is only one channel spanning all the available bandwidth W. We now describe how one may easily obtain a feasible schedule for the key scenario from a schedule for the channel scenario:

Given a network instance, construct a feasible random (c, f) schedule as described in [25]. Constructing this schedule involves partitioning the network into cells. As per the description in [25], this schedule is two-level:

The schedule comprises rounds; 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 in that cell get scheduled.

We construct a schedule for the key scenario as follows:

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 multi-channel schedule:

In the multi-channel schedule, each sub-slot can have at most c concurrent transmissions going on at rate $\frac{W}{c}$ each. In the key schedule, we divide each sub-slot further into c equal sub-sub-slots. Each transmission is exclusively assigned one sub-sub-slot, and occurs at rate W (since there is a single channel that supports data-rate W). Thus, we serialize these transmissions. This serialization is depicted in Fig. 1.

It is not hard to see that this is a feasible schedule for the key pre-distribution scenario. Thus, one can obtain a capacity lower bound with keys which is the same as the capacity lower bound for the corresponding multi-channel scenario, i.e., $\Omega(W\sqrt{\frac{p_{rnd}}{n \log n}})$ [25].

D. Capacity with Random (c, f) Key Pre-distribution

In Section VII-B and Section VII-C, we established upper and lower bounds on capacity with random (c, f) key pre-distribution, by drawing on the multi-channel results presented in [24], [25]. It follows from the upper and lower bounds that the capacity with random (c, f) key pre-distribution, when $c = O(\log n)$ is $\Theta(W\sqrt{\frac{p_{rnd}}{n \log n}})$. When $f = \Omega(\sqrt{c})$, $p_{rnd} = 1$ and one achieves pre-attack capacity of the same asymptotic order as with $f = c$, or without random key pre-distribution.

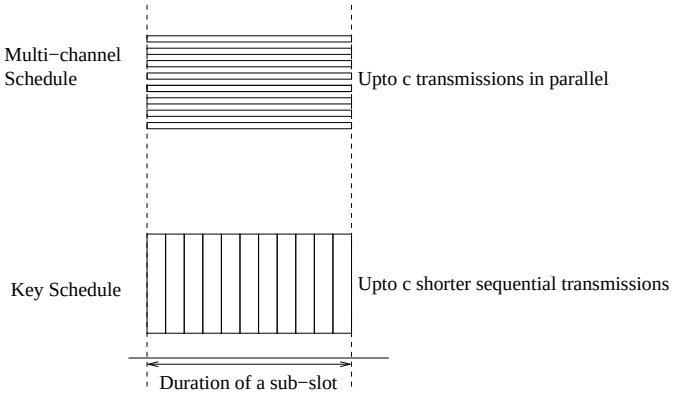

Fig. 1. Obtaining a schedule for key scenario by serializing transmissions in multi-channel schedule

VIII. Insights on Routing

We described in the previous section how the construction used in [25] to achieve capacity for random (c, f) assignment is also valid for a random (c, f) key pre-distribution scenario, with some modification to the schedule. Moreover, the routes that are valid for one are valid for the other. The routing strategy provides insights into the routing issues that arise in such networks due to the fact that two nodes that are in range cannot communicate securely unless they share a key. This issue has not been carefully studied in prior work on random key pre-distribution. While [22] discusses the notion of replacing a direct neighbor link with multiple hops in a key-predistribution scenario, they do not consider the implications for network-wide routing.

In the routing construction for random (c, f) assignment described in [25], 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 $(S, R_1), (R_1, R_2), ..., (R_l, D)$ can operate on at least one common channel (to ensure a sequence of feasible links); 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 S to D (i.e., the route that passes through cells traversed by the straight-line from S to D', with a possible additional last hop to D (Fig. 2)) 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 made to pass through a sufficient number of cells by taking a *detour* (Fig. 3). Routing with keys would also require similar detour strategies, and possibly

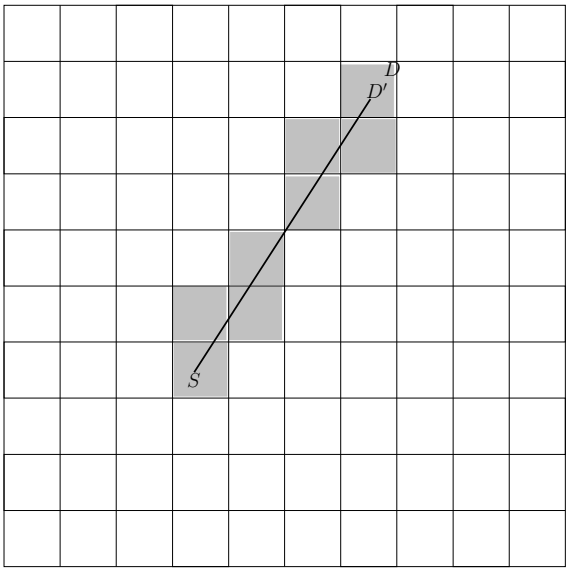

Fig. 2. Routing along a straight line

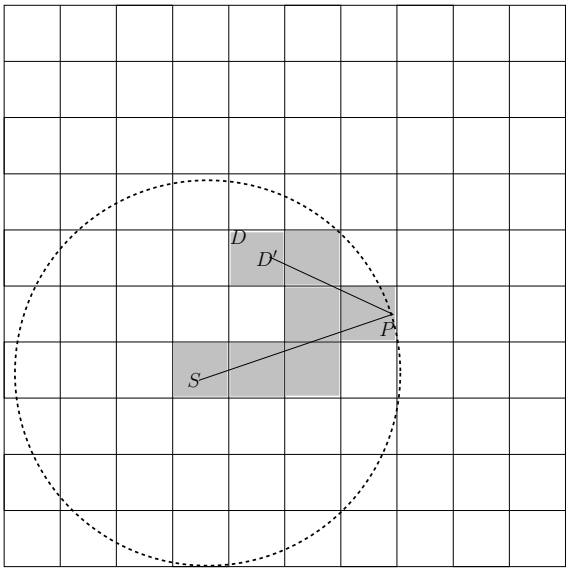

Fig. 3. Illustration of detour routing

longer-than-usual routes, to ensure an end-to-end secure path from source to destination.

IX. Discussion on Security-Performance Trade-off

The capacity results established in Section VII provide insight into the trade-off between security (i.e., resilience to key-compromise) and performance. Since each node is equipped with a random subset of f keys, an adversary can gain access to f keys by compromising a single node. Thus, it would be desirable to keep f small to improve security characteristics. However, since capacity scales as $\Theta(W\sqrt{\frac{p_{rnd}}{n\log n}})$, and is an increasing function of f, the quiescent or pre-attack capacity is adversely affected if f is small. Hence, performance (throughput) dictates a large value of f. This interplay introduces a trade-off, and f must be suitably chosen to achieve the appropriate balance. The asymptotic capacity results help quantify this trade-off.

Moreover, it is to be noted that in the capacity construction, the common transmission range can be chosen to maximize capacity. This essentially means that there is no power constraint on the nodes. In a practical deployment, very high transmission power may not be feasible, particularly for battery-powered sensor nodes. Thus, given the largest transmission power that one is willing to use, the transmission range is upper-bounded, and so f must be chosen to be large enough to provide good connectivity for that range. Results on critical range for connectivity can help guide this decision.

This discussion highlights that there are many requirements and constraints on a practical network, and the value of f must be appropriately chosen to achieve the desired operating point. Formal theoretical analysis can be useful in providing rigorous insights regarding the trade-offs. In particular, there is need to formulate models for post-attack secure capacity, as was discussed in Section IV.

X. 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 shed light on the routing implications and issues in such scenarios, as well as the trade-off between resilience to key-compromise and performance. They also serve as an illustration of a theoretical approach to quantifying security-performance trade-offs in wireless networks.

XI. Acknowledgement

We thank Matthew Miller who first drew our attention to the 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] L. Tassiulas and A. Ephremides, "Stability properties of constrained queueing systems and scheduling policies for maximum throughput in multihop radio networks," *IEEE Transactions on Automatic Control*, vol. 37, no. 12, pp. 1936–1948, Dec. 1992.

[5] 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.

[6] ——, "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.

[7] J. Barros, "Physical layer security," Short Course offered at UIUC, Sept. 2007.

[8] J. Feldman, T. Malkin, C. Stein, and R. Servedio, "On the capacity of secure network coding," in *Proc. 42nd Annual Allerton Conference on Communication, Control, and Computing*, 2004.

[9] C.-Y. Koo, "Broadcast in radio networks tolerating byzantine adversarial behavior," in *PODC '04: Proceedings of the twenty-third annual ACM symposium on Principles of distributed computing*. ACM Press, 2004, pp. 275–282.

[10] A. Pelc and D. Peleg, "Broadcasting with locally bounded byzantine faults," *Information Processing Letters*, vol. 93, no. 3, pp. 109–115, Feb 2005.

[11] V. Bhandari and N. H. Vaidya, "On reliable broadcast in a radio network," in *PODC '05: Proceedings of the twenty-fourth annual ACM SIGACT-SIGOPS symposium on Principles of distributed computing*. ACM Press, 2005, pp. 138–147.

[12] A. Pelc and D. Peleg, "Feasibility and complexity of broadcasting with random transmission failures," in *PODC '05: Proceedings of the twenty-fourth annual ACM SIGACT-SIGOPS symposium on Principles of distributed computing*, 2005, pp. 334–341.

[13] C.-Y. Koo, V. Bhandari, J. Katz, and N. H. Vaidya, "Reliable broadcast in radio networks: The bounded collision case," in *Proceedings of ACM PODC 2006*, 2006.

[14] S. Gilbert, R. Guerraoui, and C. Newport, "Of malicious motes and suspicious sensors," in *Proc. of OPODIS*, 2006.

[15] C. Karlof, N. Sastry, and D. Wagner, "Tinysec: a link layer security architecture for wireless sensor networks," in *SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems*. ACM, 2004, pp. 162–175.

[16] 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.

[17] M. J. Miller and N. H. Vaidya, "Leveraging channel diversity for key establishment in wireless sensor networks," in *Proc. of IEEE Infocom*, Apr. 2006, pp. 1–12.

[18] S. Dolev, S. Gilbert, R. Guerraoui, and C. Newport, "Gossiping in a multi-channel radio network (an oblivious approach to coping with malicious interference)," in *Proc. of DISC*, 2007.

[19] T. H. Cormen, C. E. Leiserson, and R. L. Rivest, *Introduction to Algorithms*. MIT Press, 1990.

[20] R. D. Pietro, L. V. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan, "Connectivity properties of secure wireless sensor networks," in *SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*. New York, NY, USA: ACM, 2004, pp. 53–58.

[21] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *SP '03: Proceedings of the 2003 IEEE Symposium on Security and Privacy*. IEEE Computer Society, 2003, p. 197.

[22] 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.

[23] H. Chan and A. Perrig, "Pike: peer intermediaries for key establishment in sensor networks," in *INFOCOM*, 2005, pp. 524–535.

[24] 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.

[25] ——, "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.