Generalized Delay-Secrecy-Throughput Trade-offs in Mobile Ad-Hoc Networks

Saurabh Shintre[1], Lucile Sassatelli[2], João Barros[1] *

Abstract — **In this paper, we first present a theoretical framework aimed at generalizing the scaling laws of delay, secrecy and throughput in mobile ad-hoc networks for various network models and scheduling policies available in the literature. We derive scaling laws for throughput-delay tradeoffs for new routing policies such as Spray-and-Wait. A model based on threshold secrecy constraint is developed and it is shown that scaling laws are not impacted provided the eavesdropper density is lower than the node density.**

1 Introduction

Gupta and Kumar in [1], showed that the per-user throughput of a static wireless ad-hoc network scales to zero with increasing node density (N). Grossglauser and Tse in [2], however showed that, the per-user throughput can be maintained constant with N, provided the nodes are mobile and large delay D is permitted in the data delivery.

The delay and throughput trade-off in MANETs was studied by Neely and Modiano in [3]. Using a cellular spatial division scheme [3] showed that the delay of the two-hop routing of [2], increases with node-density. The delay can be reduced by introducing redundant data in the network which, in turns, reduces the throughput. The fundamental delay-throughput trade-off was discovered to be $\lambda = \mathcal{O}(D/N)$, where λ is the per-user throughput and D is average delay. Ying *et al.* improved this trade-off by scaling the transmission radius inversely to the permissible delay [4]. The achievable trade-off resulted in $\lambda = \mathcal{O}(\sqrt{D/N})$.

Apart from throughput and delay, security is a major performance bottleneck in MANET deployment. The broadcast nature of wireless links makes interception of transmission extremely easy and the lack of centralized infrastructure hinders implementation of admission control policies or distribution of secret keys. In such a scenario, it is important to exploit security opportunities at all levels of the system. (For an introduction to physical layer security refer to [10].)

The delay-throughput performance of MANETs in the presence of passive and active attacks was studied by Liang *et al.* in [5] which extends the framework in [4]. It was shown that performance of MANETs can be divided in two regimes according to the density of eavesdroppers (M). For passive colluding attackers, if $M = o(\sqrt{ND})$, the same delay throughput performance can be guaranteed as [4]. If $M = \Omega(\sqrt{ND poly(N)})$, then the throughput is $\mathcal{O}(1/M)$. For active attackers, the same throughput was achieved but with more stringent conditions on the densities.

The paper makes the following contributions:

Generalized Framework: We first present a theoretical framework aimed at characterizing the scaling laws of delay, secrecy and throughput in mobile ad-hoc networks. The framework extracts important system parameters which code for the eavesdropping intensity and the scheduling policy. This allows to use mean field approximations and queuing theory tools to get results depending on the system parameters only, thereby encompassing previous results [3, 4, 5].

Tradeoffs for two-hop routing and Spray-and-Wait: We derive new scaling laws for secrecy-throughput-delay tradeoffs for other routing policies such as Spray-and-Wait. The results are given in terms of the redundancy allowed per packet in the system, both for two-hop routing and Spray-and-Wait. We show that two-hop routing gives better trade-off however Spray-and-Wait must be used to improve delay beyond certain threshold. The throughput costs are then much higher.

2 Network Model and Preliminaries

The network consists of N legitimate and M eavesdropping nodes. Each legitimate node serves as the source and destination for equal amount of traffic. All nodes move according to a uniform i.i.d mobility (independent among users as well as time-slots). A maximum of one-hop transmissions can be done in a time-slot (Fast Mobility). In this paper, "routing" only refers to opportunistic forwarding with possible packet replication. All order notation is borrowed from [4]

*[1] Instituto de Telecomunicações, Departamento de Engenharia Electrotécnica e de Computadores, Faculdade de Engenharia da Universidade do Porto, 4200-465, Porto, Portugal, e-mails: {saurabh.shintre, jbarros} .fe.up.pt. [2] Laboratoire I3S, Université de Nice Sophia Antipolis - CNRS, 06903 Sophia Antipolis Cedex - France, e-mail: sassatelli@i3s.unice.fr

This work was partly supported by the Fundação para a Ciência e Tecnologia (Portuguese Foundation for Science and Technology) under grant SFRH/BD/71350/2010, and the Wireless Information Theoretic Security (WITS) project (Grant PTDC/EIA/71362/2006)

Definition 1 ***Per-user Throughput**: Let, $\Lambda_i(T)$ be the number of unique packets received (decoded, in case coding is used) by node i during the time duration $(0, T)$. Then, per-user throughput λ is said to be feasible if: $\lim_{T\to\infty} P\left(\Lambda_i(T)/T \geq \lambda, \forall i\right) = 1$ The average per-user throughput, we defined it as λ such that $\lambda_i \geq \lambda$ for all i.*

Definition 2 ***Delay**: Let D_i be the time taken by a packet to reach the destination from its arrival at the top of source buffer. Delay D would denote the delay averaged over all packets in the system.*

Delay in [5] is measured from the point of first transmission of the packet and does not include waiting time for the first transmission. D' will refer to the average delay using such definition.

Eavesdroppers, if present, are passive and are assumed not to collude. This means that the aim of a secret code is to protect the information from eavesdroppers individually. We now define the important model parameters which allow to account for various scheduling policies and eavesdropping intensity and use mean field approximations.

R: The maximum number of copies of a packet (redundancy) allowed to be created by the routing policy, including the source.

σ: Given a pair of nodes A and B, consider the probability that transmission from A to B is possible according to the chosen transmission criterion (defined in the next section). The average of such probability over all node locations is denoted by σ.

δ: Given that node A carries a packet to be relayed by B, consider the probability that A is scheduled as a transmitter in that time-slot and the transmission criterion is met (B can hear A) and B selects A over all other transmitters that B can hear (B listens to A). δ is the average probability over all node locations.

η: Given that A holds a packet destined to B, consider the probability that A is scheduled as a transmitter at that time-slot and the transmission criterion is met (B can hear A) and B selects A over all the transmitters B can hear (B listens to A). The average of such probability over all node locations is denoted by η.

Note: R is dependent on the routing policy only, σ is dependent on the network parameters only (N and M), while δ and η are dependent of the scheduling policy. For example, with perfect scheduling $\eta = \sigma$ (entailing that some infrastructure is available or some feedback is feasible), otherwise $\eta = \delta$ when the destination has no means to select the source with a packet for it other than randomly.

In the following section, we calculate the value of these parameters for a special Maximum Secrecy Rate based model. Note that probability of having threshold MSR from the intended receiver to the transmitter (for feedback) does not not vary with N, and thus feedback mechanisms are assumed to be available for the model as scaling is not impacted.

3 MSR Model

The N nodes and M eavesdroppers are present in a unit disc (radius $1/\sqrt{\pi}$). Mobility model is as described above. Based on a scheduling policy Π, in a given slot, certain set of nodes N_T are assigned as potential transmitters and others as receivers. Let $\mathcal{T}$ be the set of all designated transmitters and $\mathcal{R}$ be the set of all designated receivers.

Channel gain between two nodes (U_i, U_j) located distance d apart is denoted by $\gamma(U_i, U_j) = d^{-\alpha}$. We assume that all transmitters transmit with unit power, and therefore, the received signal power from U_i to U_j equals $\gamma(U_i, U_j)$ and has the following distribution: $P(\gamma(U_i, U_j) \geq z) = \pi z^{-2/\alpha}$.

Interference is caused at a receiver R_i which is scheduled to receive data from designated transmitter $T_i \in \mathcal{T}$, owing to concurrent transmission. $I(T_i, R_i) = \sum_{T_j \in \mathcal{T}\setminus\{T_i\}} \gamma(T_j, R_i)$ represents the interference caused to the transmission $T_i \to R_i$.

In the absence of eavesdroppers, the transmission criteria for a transmitter-receiver pair (T_i, R_i) is based on a threshold SINR ($S(T_i, R_i)$), that is given by $S(T_i, R_i) = \frac{\gamma(T_i,R_i)}{N_0 + I(T_i,R_i)}$.

Lemma 1

$$P(S(T_i, R_i) \geq y) = y^{-2/\alpha}\Theta(1/N).$$

Proof: SINR is equivalent to the ratio of one random variable with the sum of N identical and independent random variables (each one with a Pareto distribution). Distribution of I can be approximated by a stable distribution with appropriate scaling and the result can be readily derived.

Secure communication can be ensured if and only if none of the eavesdroppers has a better channel (SINR) than the receiver because eavesdroppers are assumed not to collude. This criteria is defined in terms of *Maximum Secrecy Rate*, defined for a transmitter-receiver pair (T, R) as:

$$MSR(T_i, R_i) = \frac{1}{2}\left[\log\frac{(1 + S(T_i, R_i)}{\max_{E_j \in \mathcal{E}}(1 + S(T_i, E_j))}\right],$$

where, $\mathcal{E}$ is the set of all eavesdropper and has cardinality M.

Theorem 1 *For sufficiently small ρ,*

$$\sigma = P(MSR(T_i, R_i) \geq \rho) = \Theta\left(\frac{1}{\max(M, N)}\right).$$

Proof: SINR for legitimate receivers or eavesdroppers have the same distribution. If the $M = o(N)$, then the probability of threshold MSR is limited by the probability of threshold SINR (hence, $\Theta(1/N)$). If $N = o(M)$, then the probability of threshold MSR is limited by the maximum SINR for M eavesdroppers and can be proven to be $\Theta(1/M)$.

4 Analysis of end-to-end delay

In order to derive the minimum end-to-end delay, we first consider the case where a single packet is delivered over an empty network. We build on [6, 7] to derive the approximate end-to-end delay in each case. We assume that, at each transmission, all the receivers not carrying the packet yet are potential targets.

4.1 Two-hop routing

Theorem 2 *When two-hop forwarding is used and the number of possible copies is not limited, then the mean end-to-end delay verifies:*

$$\mathbb{E}[D] \leq \Theta\left(\frac{1}{\delta\sqrt{N}}\right) .$$

For the MSR model described in Section III, this gives

$$\mathbb{E}[D] = \begin{cases} \Theta\left(\sqrt{N}\right) & \text{when } N = \max(N, M) \\ \Theta\left(\frac{M}{\sqrt{N}}\right) & \text{when } M = \max(N, M) \end{cases}$$

Proof: Defining δ and η allows us to use the results of Benaïm and Le Boudec [6] to express the mean field limit of the fraction $\mu_1(t)$ of nodes holding the packet, as the branching process we are looking at has a vanishing intensity.

$$\mu_1(t) = 1 - (1 - \frac{1}{N})\exp(-\delta t) \ . \qquad (1)$$

We use the lower-bound η: $\eta \geq \delta$ to express the cumulative distribution function (CDF) of the delay for the packet to reach the destination, in a similar way as Zhang *et al.* [7] did for sparse networks without interference.

Corollary 1 *With two-hop routing, when the number of copies is limited to R, then the end-to-end delay satisfies* $\mathbb{E}[\mathit{delay}] \leq T_1(R) + T_2(R)$ *where*

$$T_1(R) = -\frac{1}{\delta}\log\left(\frac{N-R}{N-1}\right), \quad T_2(R) = \frac{1}{\eta R} \ .$$

Proof: $T_1(R)$ stands for the mean number of time slots required for the source to disseminate R copies, and T_2 for the mean time required for the destination to get the packet, once there are already R copies in the network. Hence, we have $\mathbb{E}[\text{delay}] \leq T_1(R) + T_2(R)$. From eq. (1), $T_1(R) = \frac{1}{\delta}\log\left(\frac{N-1}{N-R}\right)$. And the expression of the CDF of the delay: $P(t) = 1 - \exp\left(-N\eta\int_0^t \mu_1(s)ds\right)$ gives $T_2(R)$ by computing the mean time for reception.

Remark 1: For $R = \sqrt{N}$, we thereby obtain $\mathbb{E}[\text{delay}] \leq \Theta(\frac{1}{\delta\sqrt{N}})$. Limiting $R = \sqrt{N}$ achieves minimum delay. This is the same result found by Neely and Modiano in [3], Lemma 1.

Remark 2: We consider the D' definition of delay to draw a connection with [5]. The transmission radius L is adapted so that the range includes R nodes on average (the nodes in the transmission range of a transmitter are assumed to be silent). Therefore $D' = T_2(R)$. We can get the same optimal transmission range L by solving $\frac{1}{\eta R} = D'$. Owing to the so-called cell-scheduling in [5], $\eta = \sigma$ and the results follow.

4.2 Epidemic forwarding

Theorem 3 *When epidemic forwarding, a.k.a. flooding, is used and the number of possible copies is not restricted, then the mean delay achieved is:* $\mathbb{E}[\mathit{delay}] \leq \frac{\log(N)}{(N-1)\delta}$.

For the MSR model described in Section III, this gives

$$\mathbb{E}[D] = \begin{cases} \Theta\left(\log(N)\right) & \text{when } N = \max(N, M) \\ \Theta\left(\frac{M}{N}\log(N)\right) & \text{when } M = \max(N, M) \end{cases}$$

Proof: The proof is based on the same arguments as proof of Theorem 2, except that we have to distinguish between process with non-vanishing and vanishing intensities. Specifically, we get $\mu_1(t) = \frac{1}{1+(N-1)\exp(-N\delta t)}$

4.3 Spray-and-Wait

In the same way as for two-hop, we will consider epidemic routing under the constraint of a maximum number of copies per packet, i.e., Spray-and-Wait [9] introduced by Spyropoulos *et al.* with $R \leq N-1$. If $R = N-1$, then Spray-and-Wait boils down to flooding. It has been shown that Spray-and-Wait achieves the lowest end-to-end delay for given R [9].

Corollary 2 *With Spray-and-Wait routing, when the number of copies is limited to R, then the end-to-end delay satisfies* $\mathbb{E}[\mathit{delay}] \leq T_1(R) + T_2(R)$ *where,* $T_1(R) = \frac{1}{N\delta}\log\left(\frac{N-1}{N/R-1}\right), \quad T_2(R) = \frac{1}{\eta R}$.

5 Throughput analysis

In this section, we analyze what the throughput can be for such minimum delay when all sessions are active. Equalities are in order sense in what follows.

5.1 Two-hop routing with R redundancy

Lemma 2 *For two-hop routing with R copies per-packet, each user experiences the above-mentioned minimum delay, provided that* $\lambda \le \Theta\left(1/T_1(R)\right)$

Proof: $\frac{1}{T_1(R)}$ is the average rate at which the source can introduce the packets to the network, and rate of reception can not be greater than the rate of transmission. To show that this bound is tight, we resort to feedback in case it is achievable, or declare a deadline of $D > 2T_2$ for each packet. Using Markov inequality one can prove that reduction in throughput caused by dropped packets is fractional.

From Corollary 1, we have $T_1(R) = \frac{1}{\delta}\log\left(\frac{N-1}{N-R}\right)$, $T_2 = \frac{1}{\delta R}$ For $R = o(N)$, $T_1(R) = \frac{R}{\delta N}$. So we have throughput $\lambda(R) = \frac{\delta N}{R}$ and mean end-to-end delay $D(R) \le T_1(R) + T_2(R)$.

Comparison with [4]: from Remark 2 in Section IV, we have $R = \sqrt{N/D'}$, and $\delta = \frac{L^2}{L^2 N}$, whereby $T_1(R) = \frac{R}{\delta N} = L^2 N = \sqrt{(N/D)}$, to get back the result of Ying *et al.* [4] for per-user delay and throughput. Comparison with [5] is non-trivial as their transmission criteria is end-to-end (allowing for colluding eavesdroppers).

5.2 Spray-and-Wait with R redundancy

Theorem 4 *For Spray-and-Wait with a maximum of R copies per packet, each user experiences at most a delay mentioned in Corollary 2, provided the per-user throughput is no greater than*

$$\lambda_R \le \Theta\left(\frac{1}{RT_1(R)}\right) = \Theta\left(\frac{N\delta}{R}\left[\log\frac{N-1}{N/R-1}\right]^{-1}\right)$$

Proof: The network is seen by the N sessions as N/R servers with service time $T_1(R)$ each. Buffer size is maintained constant due to equal intensity of meeting the source and the destination.

With the model described in Section III, a constant (with N) fraction of nodes are scheduled as transmitters or receivers at each time-slot. Thus $\delta = \sigma$ and $\sigma = P(MSR > \rho)$. Therefore we get when $R = o(N)$: $\lambda_R = \frac{1}{RT_1(R)} = \frac{\delta N}{R\log(R)} = \frac{\min(1,N/M)}{R\log(R)}$. Under such algorithm, the end-to-end delay of a source packet is still $D \le T_1(R) + T_2(R)$. The particular case of $R = N-1$ corresponds to flooding and gives $\lambda = \Theta\left(\frac{1}{\max(M,N)\log N}\right)$.

6 Delay-Throughput trade-off

Let us now express a bound on the trade-off between delay and throughput. This bound relies on the framework described in Section II, and allows to unify all transmission schemes based on hop-by-hop criterion, such as [3, 4] and our MSR model of Section III.

Theorem 5 *Under delay D, the per-session throughput cannot be greater than* $\lambda \le \delta\eta N D$.

Proof: The number of replicas sent by all sessions within a time-slot is λRN. The average number of nodes receiving a packet (replica) at that time-slot is $\Theta(\delta NN)$. Whereby $\lambda R \le \delta N$. Moreover, since $T_2(R) = \frac{1}{\eta R}$ and $D(R) \ge T_2(R)$, we get the result.

7 Conclusions

We have developed a framework that generalizes the study of scaling laws of MANETs. Important parameters were identified and a uniform analysis was performed for secrecy, throughput and delay, specifically, for previously unexplored Spray-and-wait routing. A model based on MSR is studied with this framework and analyzed under various routing schemes.

References

[1] P. Gupta, and P. R. Kumar, "The capacity of wireless networks", IEEE Trans. on Information Theory, Vol. 46, No. 2, Pg. 388-404, Mar 2000.

[2] M. Grossglauser and D. N. C. Tse, "Mobility increases the Capacity of Ad Hoc Wireless Networks", IEEE/ACM Trans. on Networking, Vol. 10, No. 4, Pg. 477-486, Aug 2000.

[3] M. Neely and E. M. Modiano, "Capacity and Delay Tradeoffs for Ad-Hoc Mobile Networks", IEEE Transactions on Information Theory, Vol. 51, No. 6, Pg. 1917-1936, Jun 2005.

[4] , L. Ying, S. Yang and R. Srikant, "Optimal Delay-Throughput Trade-offs in Mobile Ad Hoc Networks", IEEE Transactions on Information Theory, Vol. 54, No. 9, Sep 2008.

[5] Y. Liang, H. Poor, H. and L. Ying, "Secrecy Throughput of MANETs with Malicious Nodes", Proc. IEEE International Symposium on Information Theory, Jun 2009.

[6] M. Benaïm, and J. -Y. Le Boudec, "A Class Of Mean Field Interaction Models for Computer and Communication Systems", Performance Evaluation, Vol. 65, No. 11-12, Pg. 823-838, 2008.

[7] X. Zhang, G. Neglia, J. Kurose and D. M. Towsley, "Performance modeling of epidemic routing", Computer Networks, Vol. 51, Pg. 2867-2891, 2007.

[8] T. G. Kurtz, "Solutions of ordinary differential equations as Limits of Pure Jump Markov Processes", Journal of Applied Probability, Vol. 7, No. 1, Pg. 49-58, Apr 1970.

[9] T. Spyropoulos, K. Psounis and C. Raghavendra , "Efficient routing in intermittently connected mobile networks: the multi-copy case", ACM/IEEE Trans. on Networking, Vol. 16, Pg. 77-90, Feb 2008.

[10] M. Bloch and J. Barros, "Physical-Layer Security: From Information Theory to Security Engineering",To Appear: Cambridge University Press , 2011.