DETECTING MALICIOUS PACKET DROPPING USING TRAFFIC PATTERNS IN MANET

R. Rao and G. Kesidis

Abstract - Ad hoc networks are gaining presence with the proliferation of cheap wireless devices and the need to keep them connected. Individual applications and larger missions, such as those of tactical sensor networks, require secure data transmission among wireless devices. Security remains a major challenge for such networks. Current protocols employ encryption and authentication techniques for secure message exchange, but given the limitations and innately insecure nature of ad-hoc networks, such mechanisms may not suffice. A security breach can, for example, be a network-level denial-of-service (DoS) attack, passive eavesdropping, or physical layer jamming to degrade communication channels. In a multihop network, an intruder node can degrade communication quality by simply dropping packets that are meant to be relayed (forwarded). The network could then misinterpret the cause of packet loss as congestion instead of malicious activity. In this paper, we suggest that traffic transmission patterns be selected to facilitate verification by a receiver. Such traffic patterns are used in concert with suboptimal MAC that preserves the statistical regularity from hop to hop. This general technique for intrusion detection is therefore suitable for networks that are not bandwidth limited but have strict security requirements, e.g., certain kinds of tactical sensor networks.

Keywords: MANET, Intrusion Detection, Packet Dropping.

Resumo: O barateamento de dispositvos para redes sem fio tem proporcionado a proliferação de redes Ad hoc. Aplicações nestas redes, tais como aplicações em missões táticas, necessitam de mecanismos que assegurem a segurança da comunicação. Protocolos atuais empregam criptografia e autenticação, porém não são suficientes dada a natureza destas redes. Uma opção viável é prover mecanismos contra ataques de negação de serviço, o que poderia evitar, por exemplo, a interpretação errônea da perda maciça de pacotes geradas por um intruso. Neste artigo, introduz-se uma técnica baseada na interpretação de padrões de tráfego em redes cujo protocolo de acesso ao meio preserva a regularidade estatística do tráfego. A técnica introduzida aqui são próprias para redes que necessitam de segurança e que não são limitadas pela disponibilidade de banda passante, tais como redes de sensores.

Palavras-chave: MANET, Detecção de Intrusos, Descarte de Pacotes.

1. INTRODUCTION

Ad hoc networks can be defined as dynamic networks of wireless devices that have no a priori infrastructure support. The devices in ad hoc networks, referred herein as "nodes", dynamically establish connections when they are in radio range of each other. Nodes in radio range exchange information directly, but nodes out of radio range depend on intermediate nodes to forward their packets. Thus, nodes can simultaneously act as sources, sinks and relays for packets. Ad hoc networks are employed in, for example, emergency response (disaster relief) and tactical battlefield environments including mission-customized mobile wireless sensor networks.

Resource efficient routing for mobile multihop ad hoc networks has been a major area of research [1-6]. More recently, secure packet routing protocols have been proposed [10-12]. Certain routing issues can be resolved by encrypting the routing information. Encryption requires private keys or hash functions that are known only to the receiver and sender requiring, in turn, a mechanism for secure key distribution. In some cases, it is possible to assign private symmetric keys to each pair of nodes before they are deployed in the field. Secure key distribution would, of course, be required in more dynamic deployment situations.

One approach to secure exchange of symmetric private keys is a public key encryption system [15]. Each node is assigned a public key known to all nodes and a private key known only to the node under consideration. Nodes can employ the more complex public key encryption to exchange keys and continue future communication using private symmetric keys. In turn, private keys can be used to exchange less computationally complex symmetric hash functions. The Internet's public key system employs a certification authority that authenticates user identities by issuing digital certificates for use in the public key distribution process. Similar systems for key management and distribution have been proposed for ad hoc networks [7,8]. In the following, we assume that key management and key distribution issues are resolved.

There are ways of undermining the communication of the network that data encryption alone cannot mitigate. Since nodes depend on intermediates to relay packets, an *intruder* node can disrupt a session for which it is a relay by simply dropping packets on a regular basis instead of forwarding them. The end nodes can easily mistake the cause of the resulting packet loss as congestion. This issue was previously examined for TCP connections in the Internet [13].

We propose to control the traffic transmission pattern of the source node such that it is possible for the destination node to gain information about the actual congestion at an intermediate relay node from the statistics of interpacket arrival times. Such traffic patterns will be used in concert with certain medium access control (MAC) mechanisms

R. Rao is a student at Penn State University. He is persuing his doctoral degree in Electrical Engineering. G. Kesidis is Associate Professor at Penn State University, Electrical Engineering and Computer Science Engineering department.
E-mails: rnr115@psu.edu, kesidis@engr.psu.edu.

that preserve statistical properties of the traffic from hop to hop. Clearly, under such mechanisms, optimal throughput levels for the ad hoc network cannot be reached. Therefore, our proposed approach is applicable to situations where defense against hijacked nodes is important or where the network has low traffic volume, i.e., the network is not bandwidth limited. Examples include certain kinds of tactical networks of sensors that individually generate little traffic volume, e.g., temperature or wind direction readings or target identification. Also, individual sensors that substantially process and compress data (video, audio, etc) may also fall into this category because the resulting traffic generated will only amount to the alerts and commands associated with target tracking missions (however, this traffic will be latency critical).

The balance of this paper is organized as follows. In Section 2, we discuss a specific network model designed to help a receiver detect any abnormally high amount of packet loss and specify the decision rules. Section 3 explains the simulation setup and presents the simulation results. Conclusions are drawn in section 4.

2. NETWORK MODEL

2.1 NETWORK MODEL

We consider an ad hoc network model with multihop routes. Intermediate nodes receive packets and forward them to destination nodes based on the destination addresses in the packet headers. If an intermediate node is hijacked, it can drop packets at random to degrade communication. This activity may drastically reduce the effective communication bandwidth of the network. The sender and receiver can easily mistake the cause of missing packets for network congestion. The only way that malicious packet dropping can be detected is by finding the true level of congestion at the intruder node. Furthermore, only a non-compromised node in radio range of an "intermediate" (potentially hijacked) node experiencing higher that normal packet loss can monitor traffic flow to help determine the true level of congestion at the intermediate node.

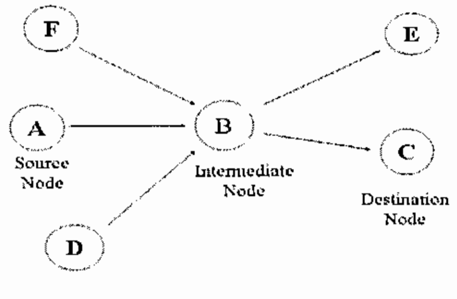

Figure 1. Ad hoc network.

Specifically consider the two-hop network shown in Figure 1 and focus on the session from node *A* to node *C*. Nodes *A* and *C* share a symmetric key (or hash function) to encrypt the packet payloads as necessary. Packet sequence numbers for the session and source (*A*) and destination (*C*) addresses are encrypted and stored in each packet header. Of course, the destination address is present unencrypted to enable basic packet forwarding. Node *B* is the intermediate traffic node forwarding the packets and is also an intruder (hijacked) node that drops packets at random. Note that node B cannot change the packet sequence number as it is encrypted.

We further assume that *B* is a bottleneck node. So, even if *B* does maliciously drop packets, *A* must still forward through *B* to get to *C* in the short term, i.e., before mobility and other environmental conditions create an alternative path to *C* that can be used by the distributed routing algorithm in place.

Suppose node *A* transmits packets according to a Poisson process at an average rate of λ packets/s. The packet length is assumed to be constant. The aggregate arrival process to *B* has rate Λ ≥ λ. All the flows transmitting to node *B* follow a poisson process. Thus to total flow rate is also poisson with mean rate Λ. The mean service rate of node *B* is μ packets/s. For stability we assume μ > Λ. We assume all nodes receiving packets from node *B* are aware of the buffer size (K packets) of node *B*. Finally, we assume that node B participates in an ALOHA-type (exponential back-off) medium access mechanism so that the packet arrival and departure processes of *B* are Poisson.

2.2 GROUNDS FOR SUSPICION

Let the sequence number of the i^{th} packet received by *C* be *r(i)* and the time of its arrival to *C* be $T_{r(i)}$. The first packet arrives at time T_1 (the implicit assumption *r(1) = 1* can be relaxed). Node *C* estimates λ using the following equation,

$$\hat{\lambda} = \frac{r(i)-1}{T_{r(i)} - T_1} \tag{1}$$

The sequence number *r(i)* also includes packets lost in transmission. Therefore, *r(i)* ≥ *i*. Despite the fact that $T_{r(i)}$ does not necessarily give the time of arrival of i^{th} packet, (1) still gives an unbiased estimator for the arrival rate λ at the destination node for a general stationary model of the network buffer. Since node *C* keeps track of the actual sequence numbers of the packets constituting its session with *C*, it is aware of packets lost during transmission.

The number of packets lost at time $T_{r(i)}$ is given by *r(i) – i*. The empirical probability of packets lost is given by

$$P_e = \frac{r(i)-i}{r(i)} \tag{2}$$

Node *C* knows the buffer capacity of the queue at node *B* is K and the queues average service rate is μ packets/s. We assume that the total traffic arriving at node *B* is also known to *C*, c.f., Section 2.3. Using the estimated λ and the above assumptions, node *C* can estimate the probability of packet loss due to buffer overflow (i.e., natural congestion) using the rule that Poisson arrivals see time averages (PASTA) [9]:

$$\hat{P}_e = \frac{\hat{\lambda}}{\hat{\Lambda}} \cdot \frac{(\hat{\Lambda}/\mu)^K}{\sum_{j=0}^{K} (\hat{\Lambda}/\mu)^j} \qquad (3)$$

This equation is derived from modelling the single queue as CTMC. We consider the queue at node *B* as an /M/M/1/K system with estimated arrival rate given by $\hat{\Lambda}$ and service rate is μ. From CTMC modelling the probability that system is in state *l* (*Queue length* = *l*) is given by

$$P\{QL = l\} = \frac{(\hat{\Lambda}/\mu)^l}{\sum_{j=0}^{j=K} (\hat{\Lambda}/\mu)^j} \qquad (3a)$$

From PASTA, the probability that a Poisson arrival will see the system in state *l* is also given by (3a). Thus packets arriving at queue see the system in state *l* with probability given by (3a). Probability that arriving packets find buffer full (*Queue length* = *K*) is given by

$$P\{QL = K\} = \frac{(\hat{\Lambda}/\mu)^K}{\sum_{j=0}^{j=K} (\hat{\Lambda}/\mu)^j} \qquad (3b)$$

This is also the probability that a packet arriving at queue is dropped. Since we have all the flows to the queue system as poisson, the sum also being poisson, the probability that a packet from a particular flow of rate $\hat{\lambda}$ is dropped is given by the fraction of the total flow rate, i.e.

$$P_e = \frac{\hat{\lambda}}{\hat{\Lambda}} \frac{(\hat{\Lambda}/\mu)^K}{\sum_{j=0}^{j=K} (\hat{\Lambda}/\mu)^j}$$

This is equation (3).

Now if we consider a single flow then Λ = λ and this equation reduces to:

$$\hat{P}_e = \frac{(\hat{\lambda}/\mu)^K}{\sum_{j=0}^{K} (\hat{\lambda}/\mu)^j} \qquad (3c)$$

Again, these expressions give an estimate of what the probability of packet loss due to natural congestion at *B* ought to be. Node *C* can compare them with the empirical value derived from (2) to determine whether *B* is dropping excessively.

To make such a comparison statistically significant, the measured confidences node C has in these estimates, i.e., the sample standard deviations σ_e and $\hat{\sigma}_e$, need to be involved. Node *C* can therefore deem the intermediate node *B* to be an intruder if the confidence "intervals" do not overlap, i.e., if

$$P_e - \alpha\sigma_e > \hat{P}_e + \alpha\hat{\sigma}_e \qquad (4)$$

for a fixed constant $\alpha \geq 1$ typically.

Clearly, it is desirable to apply the test (4) only if there is sufficient confidence in the individual estimates, i.e., only if the relative errors

$$\frac{\hat{\sigma}_e}{\hat{P}_e} \text{ and } \frac{\sigma_e}{P_e} \qquad (5)$$

are sufficiently small (significantly less than 1). In our simulation results, however, we apply test (4) on a packet-by-packet basis to study the performance of our detection mechanism as a function of the number of received packets.

Note that if computation costs of sample standard deviations are too high for the nodes, an alternative test for (4) to deem that the intermediate node is maliciously dropping packets could be

$$P_e > (1+\alpha)\hat{P}_e \qquad (6)$$

2.3 MULTIPLE FLOW CASE AND INVESTIGATION PROTOCOL

If node *C* suspects that an intermediate node *B* is maliciously dropping packets where node *B* is handling multiple flows, then *C* needs to ascertain the true *total* traffic load Λ that *B* is experiencing. To do this, we propose the following protocol initiated by *C*.

Node *C* dispatches a message to *B* requesting that *B* contact all of its tributaries to request that they send a message to *C* containing their recent traffic transmission rate to *B*. This information will be sent in both unencrypted and encrypted format, the latter using the symmetric private keys shared by *C* and the tributaries of *B*. Upon receipt of these messages from the tributaries of *B*, *C* will authenticate each one and tally the component transmission rates to obtain Λ.

Note that many of the tributaries of the suspect intermediate node *B* may need to use *B* itself to communicate with node *C*. However, note that it is in the best interest of the intermediate node *B* to honestly cooperate with C's investigation otherwise *C* may underestimate the total load on B and therefore more likely conclude that B is maliciously dropping.

Clearly, we are assuming throughout that the intermediate node *B* is not aware of the private keys of any other nodes, in particular those of its tributaries, so that it cannot spoof any other node. Also, we assume that *no two* proximal nodes have been hijacked and are cooperating to undermine communication in the network.

2.4 FALSE ALARM AND MISDETECTION

The value of the fixed parameter α in the decision criterion (4) critically affects the detection performance. This performance is quantified by false alarm and misdetection rates. A false alarm occurs when an intruder is not present and equation (4) holds, i.e., the receiver concludes there is an intruder when there is none. Misdetection occurs when an intruder is present at B but (4) is false, i.e., the receiver fails to detect an intruder when one is present. Intuitively, the probahility of false alarm is an increasing function of α but the probability of misdetection is a decreasing function of α.

3. SIMULATION

The simulation model considers a single queue and single flow at node B as shown in Figure 2.

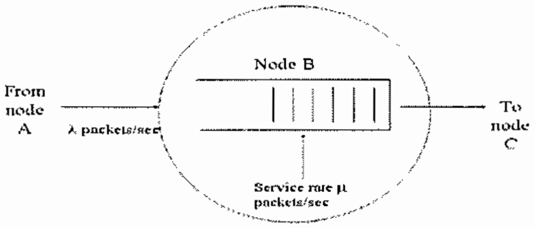

Figure 2. Single queue network model.

Since only a single flow is considered, $\Lambda = \lambda$ and $\lambda < \mu$. The simulations were performed for different values of α and for fixed value of traffic intensity ($\rho = \lambda/\mu$). The achieved confidence interval is 95%, 19 times out of 20 [14].

The difficulty in detecting an intruder maliciously dropping packets is increased with the traffic intensity. Therefore, we focus on the case $\rho = 0.9$. For lower values of traffic intensity, our detection strategy will have improved performance than that reported below.

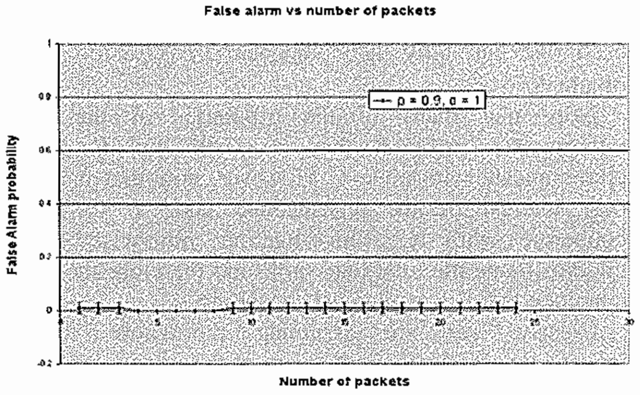

Figure 3. False alarm vs. number of packets.

Figure 3 shows a plot of false alarm probability for different number of packets. This simulation ignores equation (5) and uses (4) to make the comparison. In this simulation, no packet is dropped and we note the number of times the receiving node C concludes that there is a packet drop. This gives us the probability of false alarm. Here note that false alarm is negligible for any given number of packets.

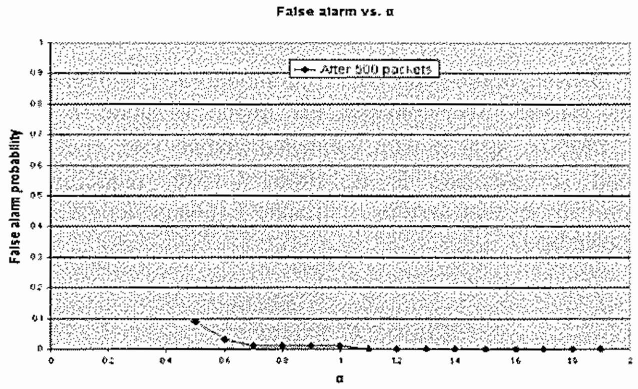

Figure 4 - False alarm vs. α

Figure 4 shows the change in false alarm rate for different values of α. As the value of α increases, the false alarm rate decreases as expected.

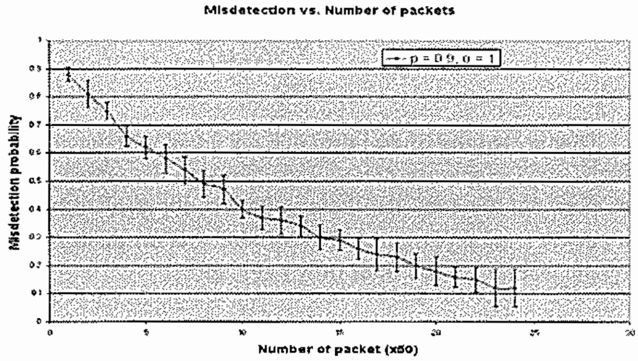

Figure 5. Misdetection vs. number of packets.

Figure 5 shows the misdetection probability for different numbers of packets. The packets are randomly dropped by the intermediate node B with probability 0.1 in the simulation. As the number of packets increases, the misdetection rate decreases because the accuracy in the estimation of $\hat{p}_c$ improves.

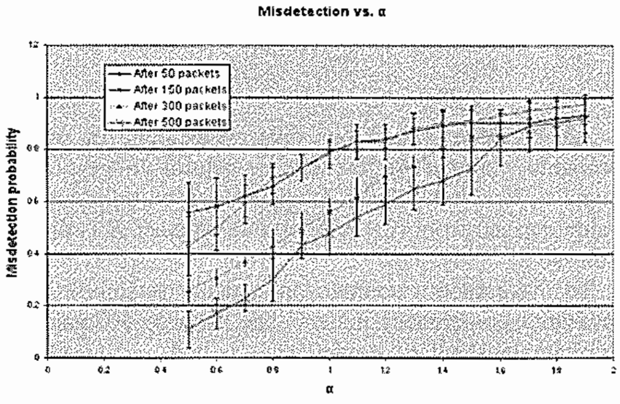

Figure 6. Misdetection vs. α.

Figure 6 plots misdetection rates for different values of α and for different numbers of packets. The misdetection probability increases with increasing α as expected.

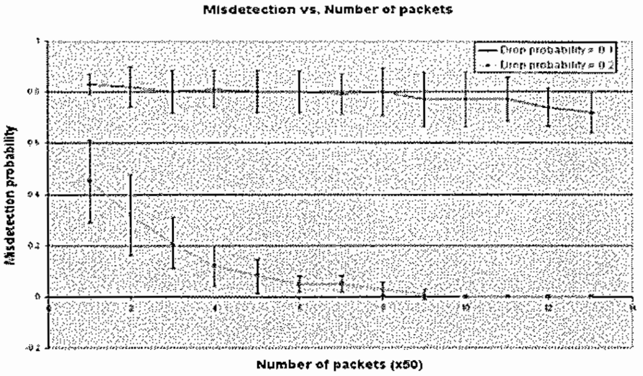

Figure 7. Misdetection vs. number of packets for constant service time.

Thus far we bave assumed that there exists a traffic model (e.g., Poisson traffic transmission pattern together with ALOHA-type medium access) to which nodes adhere so that intrusion detection at a destination node (*C*) is facilitated. A natural question is: What happens if an intruder node does not follow a prescribed traffic model? Figure 7 sbows a plot of misdetection for different numbers of packets when the intruder has a constant service time instead of exponentially distributed service time. We note that the misdetection probability does not monotonically decrease with increasing numbers of received packets demonstrating limits to detection performance due to "model error". However, note that tbe misdetection probability drops considerably as the probability of malicious packet dropping by the intruder increases. This suggests that if an intruder does not follow the prescribed traffic model but drops packets aggressively, it can still be detected.

4. CONCLUSIONS

The plots in Section 3 show the dependence of false alarm and misdetection rates on the number of packets processed and the value of parameter α in the intruder decision rule (4). As the number of packets increase, the estimate of the loss probability improves. This is seen as the decrease in botb the false alarm and misdetection probabilities. Tbere is a trade-off, however, in the choice of the parameter α: the probability of false alarm decreases with increasing α, but the probability of misdetection increases with increasing α. The value of α should be chosen according to any specified requirements on false alarm and misdetection rates. Finally, we studied misdetection performance in the presence of model error in the medium access.

REFERENCES

[1] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," *Comp. Commun. Rev.*, pp. 234-244, Oct 1994.

[2] C.-C. Chiang, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel," *Proc. IEEE SICON '97*, pp. 197-211, Apr. 1997.

[3] S. Murthy and J. J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks," *ACM Mobile Networks and Application J., Special Issue on Routing in Mobile Communication Networks*, pp. 183-197, Oct. 1996.

[4] V. D. Park and M. S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," *Proc. INFOCOM '97*, Apr. 1997.

[5] C.-K. Toh, "A Novel Distributed Routing Protocol to Support Ad-Hoc Mobile Computing", *Proc. 1996 IEEE 15th Annual Int'l. Phoneix Conf. Comp. and Commun.*, pp. 480-486. Mar. 1996.

[6] R. Dube et al., "Signal Stability based Adaptive Routing (SSA) for Ad Hoc Mobile Networks", *IEEE Personal Communication*, pp. 36-45, Feb. 1997.

[7] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks", *IEEE Networks*, volume 13, no. 16, pp 24-30 Nov-Dec, 1999.

[8] H. Hubaux, L. Buttyan and S. Capkun, "The Quest for Security in Mobile Ad Hoc Networks", pp 146-155, *Proceedings of ACM MobiHoc* 2001.

[9] R. W. Wolff, *Stochastic modeling and the theory of queues*, Prentice-Hall International, 1989.

[10] P. Papadimitrator and Z. J. Haas, "Secure Routing for Mobile Ad Hoc Networks," *Proc. SCS Comm. Netw. And Distributed Sys. Modeling and Sim. Conf.* (CNDS 2002), Jan 2002.

[11] S. Yi, P. Naldurg, R. Kravets, "Security Aware Ad Hoc Routing for Wireless Networks," *Technical Report UIUCDCS-R-2001-2241, UILU-ENG-2001-1748*, University of Illinois at Urbana Champaign, August 2001.

[12] B. Dahill, B. N. Levine, E. Royer, C. Shields, "A Secure Routing Protocol for Ad Hoc Networks," *Technical Report, UM-CS-2001-037*, University of Massachusetts, Amherst, 2001.

[13] X. Zhang, S. Wu, Z. Fu and T. Wu, "Malicious Packet Dropping: How it Might Impact the TCP Performance and How we can Detect It", *IEEE ICNP* 2000.

[14] Sheldon Ross, *Simulation*, Academic Press, 3rd edition, Dec 01.

[15] W. Diffie and M. E. Hellman, "*New Direction in Cryptography*", IEEE Tran. on Info. Theory, Vol. IT-22, pp. 644-654, 1976.

Rajesh N. Rao received his bachelors degree from BMS College of Engineering, Bangalore University in Electronics and Communication. He got his MS from Penn State University in Electrical Engineering. He is currently a PhD student with Dr. George Kesidis at Penn State University. His area of research is in mobile ad-hoc networks and includes, energy efficient routing, mobility management of nodes and intrusion detection.

George Kesidis received his M.S. and Ph.D. in EECS from U.C. Berkeley in 1990 and 1992 respectively. He was a professor in the E&CE Dept of the University of Waterloo, Canada, from 1992 to 2000. Since April 2000, he has been an associate professor in both the EE and CS&E Depts of the Pennsylvania State University. In

1999, he took a sabbatical with Nortel Networks, Ottawa, to work, in particular, on low-complexity traffic measurement and estimation and on bandwidth scheduling for MPLS. In 2001, he was part time member of technical staff at Mahi Networks working on embedding algorithms in the data plane of their multi-protocol router. In addition to a book on ATM networking, Prof. Kesidis has authored papers on the following topics related to communication networks: effective bandwidths and traffic modeling, quick simulation, traffic multiplexing (scheduling) algorithms, traffic shaping, traffic measurement and estimation, network resources provisioning for QoS, TCP-friendly active queue management (AQM), network pricing and billing, and modeling and traceback of malicious behavior (network security). His current research also includes the following problems in wireless ad hoc networking: network self-organization, energy efficient routing, energy efficient medium access control and scheduling, mobility management for sensor networks, and intrusion detection. Currently, he is on the technical program committees of 2004 IEEE INFOCOM (Hong Kong) and 2004 IEEE ICC (Paris) and he will be TPC co-chair of INFOOCM 2007. George Kesidis is a senior member of the IEEE.