Volume 2, Issue 5, May 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Optimal Anti Jamming Traffic Allocation for Multipath Source Routing

D.SaiKrishna[#1], **G.Prasad**[#2], **D.Sagar**[#3]
[#] *Department of Computer Science& JNT University*
[1] saikrishna.dharmapuri@gmail.com

Abstract—**Multiple-path source routing protocols allow a data source node to distribute the total traffic among available paths. In this paper, we consider the problem of jamming-aware source routing in which the source node performs traffic allocation based on empirical jamming statistics at individual network nodes. We formulate this traffic allocation as a lossy network flow optimization problem using portfolio selection theory from financial statistics. We show that in multisource networks, this centralized optimization problem can be solved using a distributed algorithm based on decomposition in network utility maximization (NUM). We demonstrate the network's ability to estimate the impact of jamming and incorporate these estimates into the traffic allocation problem. Finally, we simulate the achievable throughput using our proposed traffic allocation method in several scenarios.**

Index Terms—**jamming, multiple-path routing, network utility maximization (NUM), optimization, portfolio selection theory.**

I.NTRODUCTION

JAMMING point-to-point transmissions in a wireless mesh network [1] or underwater acoustic network [2] can have debilitating effects on data transport through the network. The effects of jamming at the physical layer resonate through the protocol stack, providing an effective denial-of-service (DoS) attack [3] on end-to-end data communication. The simplest methods to defend a network against jamming attacks comprise physical layer solutions such as spread-spectrum or beamforming, forcing the jammers to expend a greater resource to reach the same goal. However, recent work has demonstrated that intelligent jammers can incorporate cross-layer protocol information into jamming attacks, reducing resource expenditure by several orders of magnitude by targeting certain link layer and MAC implementations [4]–[6] as well as link layer error detection and correction protocols [7]. Hence, more sophisticated antijamming methods and defensive measures must be incorporated into higher layer protocols, for example channel surfing [8] or routing around jammed regions of the network [6]. The majority of antijamming techniques make use of diversity. For example, antijamming protocols may employ multiple frequency bands, different MAC channels, or multiple routing paths. Such diversity techniques help to curb the effects of the jamming attack by requiring the jammer to act on multiple resources simultaneously. In this paper, we consider the antijamming diversity based on the use of multiple routing paths. Using multiple-path variants of source routing protocols such as Dynamic Source Routing (DSR) [9] or Ad Hoc On-Demand Distance Vector (AODV) [10], for example the MP-DSR protocol [11], each source node can request several routing paths to the destination node for concurrent use. To make effective use of this routing diversity, however, each source node must be able to make an intelligent allocation of traffic across the availablepaths while considering the potential effect of jamming on the resulting data throughput. In order to characterize the effect of jamming on throughput, each source must collect information on the impact of the jamming attack in various parts of the network. However, the extent of jamming at each network node depends on a number of unknown parameters, including the strategy used by the individual jammers and the relative location of the jammers with respect to each transmitter–receiver pair. Hence, *the impact of jamming is probabilistic from the perspective of the network*,1 and the characterization of the jamming impact is further complicated by the fact that the jammers' strategies may be dynamic and *the jammers themselves may be mobile*.2 In order to capture the nondeterministic and dynamic effects of the jamming attack, we model the packet error rate at each network node as a random process. At a given time, the randomness in the packet error rate is due to the uncertainty in the jamming parameters, while the time variability in the packet error rate is due to the jamming dynamics and mobility. Since the effect of jamming at each node is probabilistic, the end-to-end throughput achieved by each source–destination pair will also

1. We assume that the network does not rely on a jamming detection, localization, or tracking infrastructure.
2. We note that factors other than jamming that similarly impact throughput can be included as well. We focus on jamming in this work as it is likely the prominent source of packet loss. be nondeterministic and, hence, must be studied using a stochastic framework.

In this paper, we thus investigate the ability of network nodes to characterize the jamming impact and the ability of multiple source nodes to compensate for jamming in the allocation of traffic across multiple routing paths. Our contributions to this problem are as follows.

- We formulate the problem of allocating traffic across multiple routing paths in the presence of jamming as a lossy network flow optimization problem.We map the optimization problem to that of asset allocation using portfolio selection theory [12], [13].
- We formulate the centralized traffic allocation problem for multiple source nodes as a convex optimization problem.

- We show that the multisource multiple-path optimal traffic allocation can be computed at the source nodes using a distributed algorithm based on decomposition in network utility maximization (NUM) [14].
- We propose methods that allow individual network nodes to locally characterize the jamming impact and aggregate this information for the source nodes.
- We demonstrate that the use of portfolio selection theory allows the data sources to balance the expected data throughput with the uncertainty in achievable traffic rates.

The remainder of this paper is organized as follows. In Section II, we state the network model and assumptions about the jamming attack. To motivate our formulation, in Section III, we present methods that allow nodes to characterize the local jamming impact. These concepts are required to understand the traffic allocation optimization and the mapping of this problem to Portfolio selection. In Section IV, we formulate the optimal multiple path traffic allocation problem for multisource networks. In Section V, we evaluate the performance of the optimal traffic allocation formulation. We summarize our contributions in Section VI.

II.SYSTEM MODEL AND ASSUMPTIONS

The wireless network of interest can be represented by a directed Graph G = (N , €). The vertex set N represents the network nodes, and an ordered pair (i , j) of nodes is in the edge set € if and only if node can receive packets directly from node I We assume that all communication is unicast over the directed edges in , i.e., each packet transmitted by node i€N is intended for a unique node j€ N. (i,j)€N The maximum achievable data rate, or capacity, of each unicast link (i,j)€N in the absence of jamming is denoted by the predetermined constant rate c_{ij} in units of packets per second.3Each source node in a subset S C N generates data for a single destination node d_s € N. We assume that each source node constructs multiple routing paths to d_s using a route request process similar to those of the DSR [9] or AODV [10] protocols. We let $P_s = \{P_{s1} \ldots\ldots\ldots P_s L_s\}$ denote the collection of L_s loop-free routing paths for source , noting that these paths need not be disjoint as in MP-DSR [11]. Representing each path P_{sl}

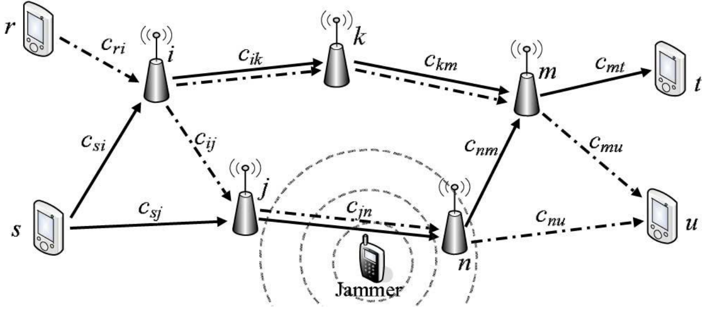

Fig. 1. Example network with sources s={r,s}Each unicast link (I,j) € €
is labeled with the corresponding link capacity. by a subset of directed link set , the subnetwork of interest to source is given by the directed subgraph

$$G_s = \left(N_s = \cup_{l=1}^{Ls} \{j : (i,j) \in p_{sl}\}, \varepsilon_s = \cup_{l=1}^{Ls} p_{sl} \right)$$

of the graph G.

Fig. 1 illustrates an example network with sources S = {r,s}. The subgraph G_r consists of the two routing paths

$$p_{r1} = \{(r,i),(i,k),(k,m),(m,u)\}$$

$$P_{r2} = \{(r,i),(i,j),(j,n),(n,u)\}$$

and the subgraph G_s consists of the two routing paths

$$p_{s1} = \{(s,i),(i,k),(k,m),(m,t)\}$$

$$P_{s2} = \{(s,j),(j,n),(n,m),(m,t)\}$$

In this paper, we assume that the source nodes in S have no prior knowledge about the jamming attack being performed. That is, we make no assumption about the jammer's goals, method of attack, or mobility patterns. We assume that the number of jammers and their locations are unknown to the network nodes. Instead of relying on direct knowledge of the jammers, we suppose that the network nodes characterize the jamming impact in terms of the empirical packet delivery rate. Network nodes can then relay the relevant information to the source nodes in order to assist in optimal traffic allocation. Each time a new routing path is requested or an existing routing path is updated, the responding nodes along the path will relay the necessary parameters to the source node as part of the reply message for the routing path. Using the information from the routing reply, each source node S is thus provided with additional information about the jamming impact on the individual nodes.

III.CHARACTERIZING THE IMPACT OF JAMMING

In this section, we propose techniques for the network nodes to estimate and characterize the impact of jamming and for a source node to incorporate these estimates into its traffic allocation. In order for a source node to incorporate the jamming impact in the traffic allocation problem, the effect of jamming on transmissions over each link (i,j) € $€_s$ must be estimated and relayed to . However, to capture the jammer mobility and the dynamic effects of the jamming attack, the local estimates

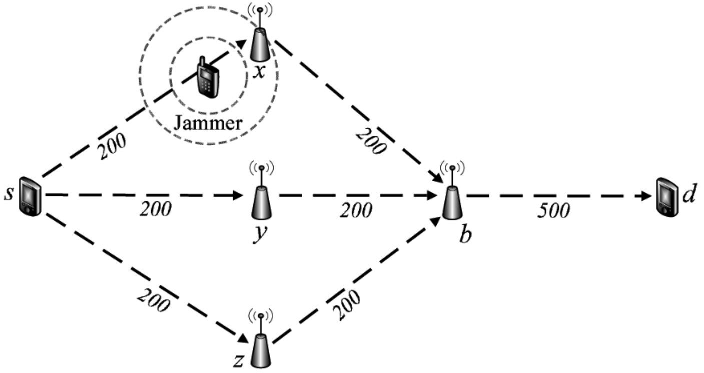

Fig. 2. Example network that illustrates a single-source network with three routing paths. Each unicast link (I,j) is labeled with the corresponding link capacity c_{ij} in units of packets per second. The proximity of the jammer to nodes

x and y impedes packet delivery over the corresponding paths, and the jammer mobility affects the allocation of traffic to the three paths as a function of time.

Need to be continually updated. We begin with an example to illustrate the possible effects of jammer mobility on the traffic allocation problem and motivate the use of continually updated local estimates.

A. Illustrating the Effect of Jammer Mobility on Network Throughput

Fig. 2 illustrates a single-source network with three routing Paths p1 = {(s,x),(x,b),(b,d)}, p3 = {(s,y),(y,b),(b,d)},p3 = {(s,z),(z,b),(b,d)}. The label on each edge (i,j) is the link capacity c_{ij} indicating the maximum number of packets per second (pkts/s) that can be transported over the wireless link. In this example, we assume that the source is generating data at a rate of 300 pkts/s. In the absence of jamming, the source can continuously send 100 pkts/s over each of the three paths, yielding a throughput rate equal to the source generation rate of 300 pkts/s. If a jammer near node is transmitting at high power, the probability of successful packet reception, referred to as the *packet success rate*, over the link (s,x) drops to nearly zero, and the traffic flow to node reduces to 200 pkts/s. If the source node becomes aware of this effect, the allocation of traffic can be changed to 150 pkts/s on each of paths p2 and p3 thus recovering from the jamming attack at node .However, this one-time reallocation by the source node does not adapt to the potential mobility of the jammer. If the jammer moves to node , the packet success rate over (s,x) returns to 1, and that over (s,y) drops to zero, reducing the throughput to node to 150 pkts/s, which is less than the 200 pkts/s that would be achieved using the original allocation of 100 pkts/s over each of the three paths. Hence, each node must relay an estimate of its packet success rate to the source node , and the source must use this information to reallocate traffic in a timely fashion if the effect of the attack is to be mitigated. The relay of information from the nodes can be done periodically or at the instants when the packet success rates change significantly. These updates must be performed at a rate comparable to the rate of the jammer movement to provide an effective defense against the mobile jamming attack. Next, suppose the jammer continually changes position between nodes x and y, causing the packet success rates over links (s,x) and (s,y) to oscillate between zero and one. This behavior introduces a high degree of variability into the observed packet

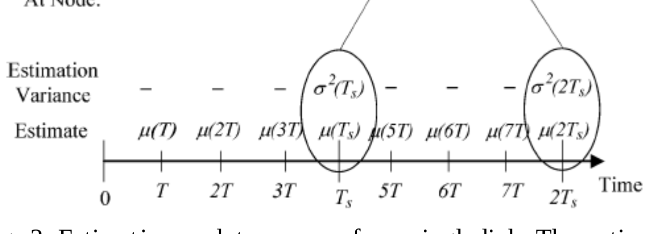

Fig. 3. Estimation update process for a single link. The estimate u_{ij} (t) is updated

every T s, and the estimation variance (t) is computed only every s.Both values are relayed to relevant source nodes every T_s s.

Success rates, leading to a less certain estimate of the future success rates over the links (s,x) and (s,y). However, since the packet success rate over link (s,z) has historically been more steady, it may be a more reliable option. Hence, the source can choose to fill p3 to its capacity and partition the remaining 100 pkts/s equally over p1 and p2. This solution takes into account the historic variability in the packet success rates due to jamming mobility. In the following section, we build on this example, providing a set of parameters to be estimated by network nodes and methods for the sources to aggregate this information and characterize the available paths on the basis of expected throughput.

B. Estimating Local Packet Success Rates

We let $x_{ij}(t)$ denote the packet success rate over link at time , noting that $x_{ij}(t)$ can be computed analytically as a function of the transmitted signal power of node , the signal power of the jammers, their relative distances from node , and the path loss behavior of the wireless medium. In reality, however, the locations of mobile jammers are often unknown, and, hence, the use of such an analytical model is not applicable. Due to the uncertainty in the jamming impact, we model the packet success rate as a random process and allow the network nodes to collect empirical data in order to characterize the process.We suppose that each node j maintains an estimate of the packet success rate $x_{ij}(t)$ as well as a variance parameter to characterize the estimate uncertainty and process variability.4

We propose the use of a recursive update mechanism allowing each node to periodically update the estimate $U_{ij}(t)$ as a function of time. As illustrated in Fig. 3, we suppose that each node updates the estimate $U_{ij}(t)$ after each *update period T* of s and relays the estimate to each relevant source node after each *update relay period* of $T_s \geq T$ s. The shorter update period of Ts allows each node to characterize the variation $x_{ij}(t)$ in over the update relay period of Ts, a key factor in . PDR in a similar manner. Furthermore, we propose to average the empirical PDR values over time to smooth out the relatively short-term variations due to noise or fading. During the update period represented by the time interval [t-T,t], each node j can record the number r_{ij} ([t-T,t]), of packets received over link (i,j) and the number v_{ij} ([t-T,t]) ≤ r_{ij} ([t-T,t]), of valid packets that pass an error detection check.5 The PDR over link(i,j) for the update period ([t-T,t]),, denoted PDR_{ij}([t-T,t]), is thus equal to the ratio

$$\mathrm{PDR}_{ij}\,([\mathrm{t}-T,\,\mathrm{t}]) = \frac{vij\,([t-T,t])}{rij\,([t-T,t])},$$

This PDR can be used to update the estimate $U_{ij}(t)$ at the end of the update period. In order to prevent significant variation in the estimate $U_{ij}(t)$ and to include memory of the jamming attack history, we suggest using an exponential weighted moving average (EWMA) [16] to update the estimate $U_{ij}(t)$ as a function of the previous estimate U_{ij}(t-T) as

$$\mu_{ij}(t) = \alpha\mu_{ij}(t-T) + (1-\alpha)\mathrm{PDR}_{ij}([\mathrm{t}-\mathrm{T},\mathrm{t}])$$

Where α € [0,1] is a constant weight indicating the relative preference between current and historic samples. We use a similarEWMAprocess to update the variance at the end of each update relay period of Ts. Since this variance is intended to capture the variation in the packet success rate over the last Ts, we consider the sample variance v_{ij} ([t-T,t]) of the set of packet delivery ratios computed using (1) during the interval ([t-T,t]) as

$$V_{ij}([t - T_s,t]) = V_{ar}\{PDR_{ij}([t - kT,t - kT + T]):$$

$$K=0,\dots,[T_s/T] - 1\}.$$

The estimation variance is thus defined as a function of the previous variance as

$$\sigma_{ij}{}^2(t) = \beta\sigma^2{}_{ij}(t - T_s) + (1- \beta)V_{ij}([t - T_s,t])$$

where β=[0,1]is a constant weight similar α to in (2).

The EWMA method is widely used in sequential estimation processes, including estimation of the round-trip time (RTT) in TCP [17].We note that the parameters in (2) and in (4) allow for design of the degree of historical content included in the parameter estimate updates, and these parameters can themselves be functions α(t) and β(t) of time. For example, decreasing the parameter α allows the mean $U_{ij}(t)$ to change more rapidly with the PDR due to jammer mobility, and decreasing the parameter allows the variance to give more preference to variation in the most recent update relay period over historical variations. We further note that the update period T and update relay period T_s between subsequent updates of the parameter estimates have significant influence on the quality of the estimate. In particular, if the update period T_s is too large, the relayed estimates $U_{ij}(t)$ and will be outdated before the subsequent update at time t + T_s. Furthermore, if the update period at each node is too large, the dynamics of the jamming attack may be averaged out over the large number of samples r_{ij}([t-T,t]). The update periods T and T_s must thus be short enough to capture the dynamics of the jamming attack. However, decreasing the update period T_s between successive updates to the source node necessarily increases the communication overhead of the network. Hence, there exists a tradeoff between performance and overhead in the choice of the update period T_s. We note that the design of the update relay period T_s depends on assumed path-loss and jammer mobility models. The application-specific tuning of the update relay period T_s is not further herein.

Using the above-mentioned formulation, each time a new routing path is requested or an existing routing path is updated, the nodes along the path will include the estimates $U_{ij}(t)$ and as part of the reply message. In what follows, we show how the source node s uses these estimates to compute the end-to-end packet success rates over each path.

C. Estimating End-to-End Packet Success Rates

Given the packet success rate estimates $U_{ij}(t)$ and for the links(i,j) in a routing path P_{sl}, the source needs to estimate the effective end-to-end packet success rate to determine the optimal traffic allocation. Assuming the total time required to transport packets from each source s to the corresponding destination d_s is negligible compared to the update relay period T_s, we drop the time index and address the end-to-end packet success rates in terms of the estimates U_{ij} and . The end-to-end packet success rate for y_{sl} path P_{sl} can be expressed as the product

$$Y_{sl} = \prod_{(i,j)\in psl} x_{ij}$$

Which is itself a random variable6 due to the randomness in each?

x_{ij} We let y_{sl} denote the expected value of y_{sl} , and w_{slm} denote the covariance of y_{sl} and y_{sm} for paths , P_{sl} P_{sm} € P_s Due to the computational burden associated with in-network inference of correlation between estimated random variables, we let the source node assume the packet success rates x_{ij} as mutually independent, even though they are likely correlated. We maintain this independence assumption throughout this work, yielding a feasible approximation to the complex reality of correlated random variables, and the case of in-network inference of the relevant correlation is left as future work. Under this independence assumption, the mean y_{sl} of y_{sl} given in (5) is equal to the product of estimates U_{ij} as

$$\gamma_{sl} = \prod_{(i,j)\in psl} \mu ij$$

and the covariance w_{slm} = E[y_{sl} y_{sm}] - E[y_{sl}]E[y_{sm}] is similarly given by

$$\omega_{slm} = \prod_{(i,j)\in psl \oplus psm} \mu_{ij} \prod_{(i,j)\in psl \cap psm} (\sigma^2{}_{ij} + \mu^2{}_{ij}) - \gamma_{sl}\gamma_{sm.}$$

In (7), θdenotes the exclusive-OR set operator such that an element is in A θ B if it is in either A or B but not both. The covariance formula in (7) reflects the fact that the end-to-end packet success rates Y_{sl} and Y_{sm} of paths P_{sl} and P_{sm} with shared links are correlated even when the rates x_{ij} are independent.We note that the variance $W^2{}_{sl}$ of the end-to-end rate Y_{sl} can be computed using (7) with l = m. Let γ denote the L_s X 1 vector of estimated end-to-end packet success rates computed using (6), and let denote the L_s X L_s covariance matrix with (l,m) entry computed using (7). The estimate pair provides the sufficient statistical characterization of the end-to-end packet success rates for source to allocate traffic to the paths in P_a. Furthermore, the off-diagonal elements in denote the extent of mutual overlap between the paths in P_s.

IV .OPTIMAL JAMMING-AWARE TRAFFIC ALLOCATION

In this section, we present an optimization framework for jamming-aware traffic allocation to multiple routing paths P_s in for each source node s € S. We develop a set of constraints imposed on traffic allocation solutions, and then formulate a utility function for optimal traffic allocation by mapping the problem to that of portfolio selection in finance. Letting denote the traffic rate allocated to path P_{sl} by the source node , the problem of interest is thus for each source to determine the optimal L_s X 1 rate allocation vector subject to network flow capacity constraints using the available statistics and of the end-to-end packet success rates under jamming.

V.CONCLUSION

In this paper, we studied the problem of traffic allocation in multiple-path routing algorithms in the presence of jammers whose effect can only be characterized statistically. We have presented methods for each network node to probabilistically characterize the local impact of a dynamic jamming attack and for data sources to incorporate this information into the routing algorithm. We formulated multiple-path traffic allocation in multisource networks as a lossy network flow optimization problem using an objective function based on portfolio selection theory from finance. We showed that this centralized optimization problem can be solved using a distributed algorithm based on decomposition in network utility maximization (NUM).We presented simulation results to illustrate the impact of jamming dynamics and mobility on network throughput and to demonstrate the efficacy of our traffic allocation algorithm. We have thus shown that multiple-path source routing algorithms can optimize the throughput performance by effectively incorporating the empirical jamming impact into the allocation of traffic to the set of paths.

REFERENCES

[1] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: A survey," *Comput. Netw.*, vol. 47, no. 4, pp. 445–487, Mar. 2005.

[2] E. M. Sozer, M. Stojanovic, and J. G. Proakis, "Underwater acoustic networks," *IEEE J. Ocean. Eng.*, vol. 25, no. 1, pp. 72–83, Jan. 2000.

[3] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. New York: Wiley, 2001.

[4] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," in *Proc. USENIX Security Symp.*, Washington, DC, Aug. 2003, pp. 15–28.

[5] D. J. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11 b and other networks," in *Proc. 25th IEEE MILCOM*, Washington, DC, Oct. 2006, pp. 1–7.

[6] A. D.Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, Oct. 2002.

[7] G. Lin and G. Noubir, "On link layer denial of service in data wireless LANs,"*Wireless Commun. Mobile Comput.*, vol. 5, no. 3, pp. 273–284, May 2005.

[8] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," *IEEE Netw.*, vol. 20, no. 3, pp. 41–47, May/Jun. 2006.

[9] D. B. Johnson, D. A. Maltz, and J. Broch, *DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks*. Reading, MA: Addison-Wesley, 2001, ch. 5, pp. 139–172.

[10] E. M. Royer and C. E. Perkins, "Ad hoc on-demand distance vector routing," in *Proc. 2nd IEEE WMCSA*, New Orleans, LA, Feb. 1999, pp. 90–100.

[11] R. Leung, J. Liu, E. Poon, A.-L. C. Chan, and B. Li, "MP-DSR: A QoS-aware multi-path dynamic source routing protocol for wireless ad-hoc networks," in *Proc. 26th Ann. IEEE LCN*, Tampa, FL, Nov. 2001, pp. 132–141.

[12] H. Markowitz, "Portfolio selection," *J. Finance*, vol. 7, no. 1, pp. 77–92, Mar. 1952.

[13] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[14] D. P. Palomar and M. Chiang, "A tutorial on decomposition methods for network utility maximization," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 8, pp. 1439–1451, Aug. 2006.

[15] M. Evans, N. Hastings, and B. Peacock, *Statistical Distributions*, 3rd ed. New York: Wiley, 2000.

[16] S. W. Roberts, "Control chart tests based on geometric moving averages," *Technometrics*, vol. 42, no. 1, pp. 97–101, Feb. 2000.

[17] V. Paxson and M. Allman, "Computing TCP's retransmission timer," RFC 2988, Nov. 2000 [Online]. Available: http://www.ietf.org/rfc/ rfc2988.txt

[18] I. R. James, "Products of independent beta variables with applications to Connor and Mosimann's generalized dirichlet distribution," *J. Amer. Stat. Assoc.*, vol. 67, no. 340, pp. 910–912, Dec. 1972.

[19] W. F. Sharpe, *Investors and Markets: Portfolio Choices, Asset Prices, and Investment Advice*. Princeton, NJ: Princeton Univ. Press, 2007.