A Hierarchical Framework for Estimating the Performance of an Aerial Network

Kamesh Namuduri[1(✉)], Amjad Soomro[2], and Srinivasa Kiran Gottapu[1]

[1] University of North Texas, Denton, USA
kamesh.namuduri@unt.edu
[2] Air Force Research Laboratory, Rome, NY, USA

Abstract. Dynamic networks such as airborne networks are characterized by fast changing topologies. Such networks require efficient strategies for estimating performance measures towards mission-specific objectives. Performance measures defined over a network will help choose optimal routes for information sharing between a pair of nodes.

This article presents a model and approach to estimate the performance of a dynamic network. First, it introduces *goodness* measures at three levels of hierarchy - link, path, and network, in terms of primitive metrics such as reliability, throughput, and latency. Second, it presents a strategy to estimate these goodness measures. The strategy is illustrated by applying it to find an optimal path between a pair of nodes in a network. Results presented on five benchmark networks illustrate the value of the proposed model.

Keywords: Aerial network · Adhoc network · Reliability
Throughput · Latency · Goodness measures · Configuration graph

1 Introduction

Often times, there is a need to find a reliable route between a pair of nodes in a network. At other times, it may be necessary to find a suitable node in a network to host a service, such as a controller in a software-defined network (SDN). Many solutions exist for finding optimal routes in wired networks as well as for wireless networks. However, finding optimal routes in extreme dynamic networks such as airborne networks is challenging and requires new strategies and solutions. Furthermore, in many practical scenarios, there may be multiple criteria for choosing an optimal route between a pair of nodes such as based on the shortest distance, reliability or security. At other times, it may be a combination of several metrics which define a suitable route for sharing information between a pair of nodes. Thus, there is a need for developing a framework and strategy for finding the best routes given performance metrics of interest in mission-critical dynamic networks.

This paper presents the results of our investigation into a hierarchical framework for evaluating *goodness* measures at various levels in a dynamic network. We define a goodness metric as a function of several primitive parameters in a

Y. Zhou and T. Kunz (Eds.): AdHocNets 2017, LNICST 223, pp. 119–130, 2018.
https://doi.org/10.1007/978-3-319-74439-1_11

hierarchical manner. This hierarchical model allows one to answer questions such as the following: which network topology makes the network the most efficient in terms of a set of given measures? Which routes are critical? Which routes are more reliable? Which mobility patterns make the network maintain connectivity and performance? Which topology maximizes the longest surviving path between two nodes? In which topology one link failure has minimal effect on the network performance? Which nodes have maximum impact on the network performance? How can the criticality of routes and their impact be minimized? The model is independent of any specific metrics and it is suitable for many types of networks. However, in this paper, we consider an aerial network as a specific scenario where the model could be applied to illustrate its application.

The rest of this paper is organized as follows. Section 2 provides a brief survey of related literature. Section 3 presents a general description of an aerial network. Section 4 defines metrics to measure the performance of an aerial network in terms of reliability, throughput, and latency. Section 5 defines goodness measures at three levels of hierarchy - link, path, and network. An algorithm based on goodness measures for generating optimal paths from source node to all other nodes in the network is presented. The implementation of the proposed strategies on benchmark graphs is discussed in Sect. 5.2. Section 6 concludes the paper with a summary.

2 Literature Survey

There is significant literature in the area of modeling and analysis of networks including wireless networks, wireless sensor networks, ad hoc networks, and vehicular networks among others. However, in the domain of extremely dynamic networks such as airborne networks, performance modeling is mostly done through simulations and to a certain extent through experimental analysis. Our work shares some commonalities with disruption-tolerant networks, wireless sensor networks and airborne networks. Concepts gathered from the literature in these three domains are briefly discussed below.

Evaluation of network resilience, survivability, and disruption tolerance in networks is analyzed in [1,2]. The authors describe a comprehensive methodology to evaluate network resilience using a combination of topology generation, mathematical analysis, simulations and experimental evaluation techniques with the goal of improving the resilience and survivability of a network. In [3], multilevel resilience of networks is investigated in terms of redundancy for fault-tolerance, diversity for survivability and connectivity for disruption tolerance.

A shortest path tree-based algorithm for relay placement in a wireless sensor network and its performance analysis is presented in [4]. The authors investigate the problem of designing a multihop wireless network for interconnecting sensors to a base station by deploying a minimum number of relay nodes at a subset of given potential locations while meeting the hop-count constraints.

A position-aware, secure and efficient routing strategy for airborne mesh networks is investigated in [5]. Cognitive radio technology is investigated as a means for communication and networking among unmanned aerial vehicles is investigated in [6]. The authors discuss the challenges associated with the integration of unmanned aerial vehicles and cognitive radio technology. An analysis of topology algorithms for commercial airborne networks is presented in [7]. The authors present an airborne network architecture based on free-space optical communications links that form a high-bandwidth mesh network. Evaluation of a multihop airborne IP network with heterogeneous radio technologies is presented in [8]. The authors discuss performance of link, radio-to-router interface, and multihop network they simulated using open source platforms.

There is also significant amount of research present in the literature on the trade-offs among the primitive measures such as throughput, reliability, and latency that are discussed in our work. A model to balance the relationship between throughput and latency for a multihop communication link is presented in [9]. Throughput, delay and reliability trade-offs are investigated in [10]. Their results suggest that single hop transmissions are optimal for maximizing the lower bound on the transmission capacity in the sparse network regime. A quality-of-service profile based on throughput, delay and reliability trade-offs in body area sensor networks is presented in [11]. This analysis is intended for time critical bio-medical applications. Throughput, delay and reliability trade-offs in multihop networks with random access are investigated in [12]. The authors characterized the trade-offs between the achievable throughput, end-to-end delay and reliability in wireless networks with random access.

The research discussed in our paper provides a generic framework for performance modeling and analysis of extremely dynamic networks. We present a novel algorithm to discover an optimal route between any two nodes in a network given a performance criteria represented by an arbitrary function. The algorithm is demonstrated to converge rapidly. This algorithm could be used to generate network routing tables in a centralized controller such as it would be in *Software Defined Networking* (SDN) paradigm.

3 Aerial Network

An aerial network is formed by aircraft deployed for a specific mission. The network may include manned and unmanned aircraft systems (UASs), ground vehicles, control stations and services, as illustrated in Fig. 1. In an aerial network nodes may travel at high speeds with range extending to hundreds of miles and with network topology constantly changing.

Successful deployment of aerial networks requires comprehensive modeling and simulation beforehand. Modeling and simulation of airborne networks, in turn, requires models of airborne vehicles, antenna propagation patterns, mobility models, terrain models, and weather patterns. Deployment of successful aerial networks also requires the implementation of information assurance strategies and their integration with network management and planning tools. An aerial network with its dynamic topology can best be represented as a random graph.

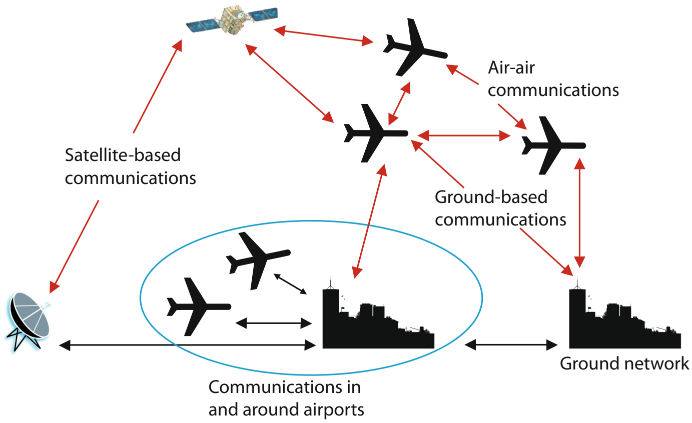

Fig. 1. An illustration of airborne network consisting of terrestrial, satellite, and RF links to connect to control stations on the ground and to other airplanes.

4 Aerial Network as a Random Graph

This section outlines the mathematical preliminaries of random graphs. We consider networks with two terminals: a source (s) node and a destination (t) node and follow the notation used in [13]. Let $G = (V, E, P)$ represent a probabilistic graph with a set of nodes $v_i \in V$, a set of edges $e_{ij} \in E$, and a link failure probability matrix $p_{ij} \in P$. Let $G_{st}(\mathrm{V}, E_{st}, P_{st})$ represent an overlay graph containing a path from s to t with its associated set of edges and probabilities (E_{st}, P_{st}). An overlay graph is created during the route discovery process (RDP); a process followed by a source node to find its destination node. Although either nodes or links may fail in a network, the scope of this analysis is limited to networks with link failures only, i.e., nodes are assumed to be failure-free. An edge e_{ij} represents a link connecting two adjacent nodes v_i and v_j. A path between two nodes v_i and v_j which is not adjacent to each other in G is defined as a sequence of distinct links connecting the two nodes. Information flows from one node to another as long as there is a path connecting the two nodes. A '$(s - t)$' cut divides the set of vertices V in the graph $G_{st}(\mathrm{V}, E_{st}, P_{st})$ into two disjoint subsets S and T such that $s \in S$ and $t \in T$. $C_{st}(i)$ represents a cut-set indexed by i in the overlay graph connecting the two nodes s and t (Table 1).

4.1 Reliability Analysis

This section outlines the concept of reliability in the context of an aerial network. It provides an approach to estimate the reliability of a link between a pair of nodes, a path between any source and destination nodes and the reliability of the entire network.

A link failure in a dynamic network could be due to link attributes such as mobility and orientation of a node. For example, a link failure may be temporary

Table 1. Terminology and notation used to represent a graph [13].

G(V, E, P)	A network with the set of nodes V, set of links E and link failure probability matrix P
s	A source node in the network G
t	A destination node in the network G
S	The set of all source nodes
T	The set of all destination nodes
NS	A set of network states
NS_i	Network state i
$G_{st}(\mathrm{V}, E_{st}, P_{st})$	An overlay network that contains a path from s to t with its associated $(\mathrm{V}, E_{st}, P_{st})$
n	Number of nodes, $\|V\|$
m	Number of edges, $\|E_{st}\|$
nc	Number of cut-sets in a graph
Fp	Probability that a network is disconnected
$s - t$	A cut in $G_{st}(\mathrm{V}, E_{st}, P_{st})$ where $s \in S$ and $t \in T$
$C_{st}(i)$	i^{th} cut-set of $G_{st}(\mathrm{V}, E_{st}, P_{st})$
c_{ij}	Capacity of the link e_{ij}
$c(S, T)$	Capacity of an $s - t$ cut in a static network
$c_p(S, T)$	Capacity of an $s - t$ cut in a probabilistic network
$R_{st}(G_{st})$	Reliability of route between s and t
R	Reliability of an entire network
$\Re_{st}$	Data flow between s and t
z_{st}	Probability that a data flow occurs between s and t
$l(i, j)$	Link latency between two nodes i and j
$L(s, t)$	Path latency between the source node s and its destination node t
F_p	Probability that the network gets disconnected

as the link may become active again when the node comes back within the range of another node which is connected to the network. On the other hand, if a node fails, it will be removed from the aerial network. The topology of the network might change when a node is disconnected from one node and is connected back again possibly to a different node. Hence, it is reasonable to assign a probability of failure to every link in the network.

An overlay network is created while a node s is discovering a path to its destination t. Although the graphs, in general, may be directed, we consider undirected graphs for simplicity of analysis. The model can easily be extended to directed graphs as well. While the probability of failures may be different from

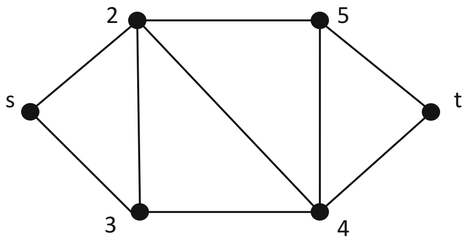

Fig. 2. An illustration of an overlay network [14]

one link to another, for simplification, it is assumed that the failure probabilities are the same for all the links, i.e., $p_{ij} = p$ and that they are independent of one another. For illustration purpose, let us consider a benchmark graph from among those given in [14] shown in Fig. 2. It represents a typical overlay network created during a route discovery process (RDP).

Reliability is a performance measure for the overlay network created during RDP between two nodes. Network reliability can be computed as a function link failure probabilities and cut-sets in the corresponding graph. The problem of enumerating all cut-sets in a graph is an NP-hard problem, for which a solution is proposed in [14]. The graph shown in Fig. 2 has the following cut-sets:

$$\begin{aligned} C_{st}(2) &= \{\{e_{s2}, e_{13}\}, \{e_{5t}, e_{4t}\}\} \\ C_{st}(3) &= \{\{e_{s2}, e_{23}, e_{34}\}, \{e_{25}, e_{24}, e_{34}\}, \{e_{25}, e_{54}, e_{4t}\}\} \\ C_{st}(4) &= \{\{e_{5t}, e_{54}, e_{24}, e_{34}\}, \{e_{s3}, e_{23}, e_{24}, e_{25}\}\} \\ C_{st}(5) &= \{\{e_{s2}, e_{23}, e_{24}, e_{45}, e_{4t}\}, \{e_{s3}, e_{23}, e_{24}, e_{54}, e_{5t}\}\} \end{aligned} \tag{1}$$

Each $C_{st}(i)$ above lists all the cut-sets in the graph that contain exactly i physical links. Assume that there are m physical links in a network between s and t, i.e., ($|E_{st}| = m$). Let p represent the probability of link failure. The failure probability of a network state NS_i with exactly i physical link failures, is $p^i(1-p)^{m-i}$. Let N_i be the number of disconnected states in NS_i with $|NS_i| = N_i$. Then, the probability that the network gets disconnected (F_p) is the sum of the probabilities over all disconnected states, i.e.,

$$F_p = \sum_{i=0}^{m} N_i p^i (1-p)^{m-i} \tag{2}$$

Reliability of a two-terminal network is defined as the probability of having atleast one path between the two nodes [15]. When viewed as the complement of the network failure probability, it can be expressed as follows:

$$R_{st}(G_{st}) = 1 - \sum_{i=0}^{m} N_i p^i (1-p)^{m-i}. \tag{3}$$

Network failure states (NS) can be completely characterized by cut-sets. With the use of cut-sets, reliability $R_{st}(G_{st})$ of the network $G_{st}(V, E_{st}, P_{st})$ [13] can be expressed in the following closed form:

$$R_{st}(G_{st}) = 1 - \sum_{nc} \sum_{i=0}^{m} |C_{st}(i)| p^i (1-p)^{m-i} \quad (4)$$

where $m = |E_{st}|$ is the cardinality of the edge set E_{st}, nc is the number of cut-sets, and $|C_{st}(i)|$ is the cardinality of cut-set with exactly i edges. The reliability of the entire overlay network can be defined as [13]

$$R = \frac{\sum_{s \in V} \sum_{t \in V, t \neq s} z_{st} R_{st}(G_{st})}{n(n-1)} \quad (5)$$

where $n = |V|$, and z_{st} is the probability that a data flow occurs between the two nodes s and t.

4.2 Throughput Analysis

Throughput of a network can be estimated using cut-sets of a graph that represents the network. The concept of max-flow min-cut strategy to estimate the throughput of a network was first introduced in [16]. This section extends this concept to probabilistic networks.

Definition 1. *Cut-set: An $s - t$ cut-set is a partition of V such that $s \in S$, $t \in T$, and S and T are disjoint subsets of V.*

Definition 2. *Capacity of a Cut-set: The capacity of a $s - t$ cut-set is defined as follows:*

$$c(S,T) = \sum_{(u,v) \in (S \times T), (i,j) \in E} c_{ij} d_{ij} \quad (6)$$

where c_{ij} is the capacity of the link e_{ij} and $d_{ij} = 1$ if $i \in S$ and $j \in T$, 0 otherwise. Minimum $s - t$ cut is obtained by minimizing $c(S,T)$.

Definition 3. *Max-flow min-cut: The max-flow min-cut theorem suggests that the maximum amount of data passing from the source (s) to the destination (t) in a network is equal to the amount of flow corresponding to the minimum $s - t$ cut [16].*

Throughput for a probabilistic network needs to take the reliability of the links into account. In its simplistic form, throughput of an unreliable link can be obtained by multiplying the amount of flow on the link with its reliability. Thus, the capacity of an $s - t$ cut in a probabilistic network can be expressed as follows:

$$c_p(S,T) = \sum_{(u,v) \in (S \times T), (i,j) \in E} c_{ij}(1 - p_{ij}) d_{ij} \quad (7)$$

where p_{ij} represents the failure probability of the link e_{ij}. The minimum $s - t$ cut for a probabilistic network will be different from a static network. Hence, the throughput of a probabilistic network could be different from the throughput of a static network.

4.3 Latency Analysis

Link latency ($l_{i,j}$) is a parameter that characterizes an aerial communication link (i, j) between two nodes i and j. If a path consisting of n number of nodes exists between a source s node and its destination (t) node, then, the path latency, $L(s, t)$, is the sum of the latencies corresponding to the sequence of links $\{(\mathrm{s}, 2), (\mathrm{s}, 3), \ldots, (\mathrm{i}, \mathrm{i}+1), \ldots, (\mathrm{n}-1, \mathrm{t})\}$ that constitute the path $(\mathrm{s}-\mathrm{t})$.

$$L(s,t) = l_{s,2} + \sum_{i=2}^{n-2} l_{i,i+1} + l_{n-1,t} \tag{8}$$

Path latency can be viewed as the end-to-end delay between the source and destination nodes assuming that there is no queuing delay. Latency is a deterministic parameter for a given path unlike throughput which is a function of the reliability of the communication links between the source and destination nodes.

4.4 Security Analysis

Security of a link ($S_{i,j}$) is a probabilistic parameter that characterizes an aerial communication link (i, j) between two nodes i and j. If a path consisting of n number of nodes exists between a source (s) node and its destination (t) node, then, the security of the path $(s - t)$ can be represented by $S(s, t)$. Detailed security analysis is beyond the scope of this paper.

5 Goodness Measures

This "goodness" determination is based on three levels of analysis. At the first level, goodness of a link can be estimated in terms of basic measures such as reliability, throughout, and latency of communication. At the second level, goodness of a path can be measured between a pair of nodes that need to share data and network control information. At the third level, goodness is measured for the entire network. Below, we develop a general hierarchical framework that includes these three levels of analysis.

5.1 First Level Analysis: Link Metrics

A link represents one hop communication channel between a pair of nodes. Metrics defined over a link represent the basic measures that characterize the quality of communication over the link. One can define a goodness measure for a communication link as a mapping (g) from the set of basic measures (M) defined on the link to a goodness function. This function assigns weights (W) to basic measures and combines the weighted measures in some form to estimate the goodness of a communication link.

$$g \colon M \mapsto f(M, W) \tag{9}$$

Link metrics may be deterministic (M_D) or probabilistic (M_P). There may be more than one link between a pair of communicating nodes. In this case, the mapping needs to take into account the metrics corresponding to all available links.

Goodness of a link ($g(i-j)$) can be formulated as a function of basic measures such as reliability ($R_{ij}(G_{ij})$), throughput, latency ($l_{i,j}$), and security ($S_{i,j}$) of that specific communication link. Out of these measures, throughput and latency are deterministic measures and form a subset M_D. Reliability and security are probabilistic measures and form a subset M_P.

In general, the subset M_P represents a collection of probabilistic measures $\{m_{p1}, m_{p2}, \ldots, m_{pn}\}$ and the subset M_D represents a collection of deterministic measures $\{m_{d1}, m_{d2}, \ldots, m_{dn}\}$ as described below.

$$\begin{aligned} M &= M_D \cup M_P,\ where\ \ M_D \cap M_P = \emptyset \\ M_D &= \{m_{d1}, m_{d2}, \ldots, m_{dn}\} \\ M_P &= \{m_{p1}, m_{p2}, \ldots, m_{pn}\} \end{aligned} \tag{10}$$

Thus, the goodness of a communication link can be estimated as a weighted function of M_D and M_P.

$$g(link) = f(M_D, M_P, W) \tag{11}$$

5.2 Second Level Analysis: Path Metrics

The link analysis discussed above can be extended to path level. At this level, each link is seen as a potential connection that facilitates information flow between a pair of nodes that it connects. Goodness of a path is an estimation of the connectivity between a pair of nodes that may be one or more hops away from each other. As a path represents a sequence of links, the mapping needs to take into account the metrics corresponding to the sequence of links that form the path. If a path consisting of n number of links exists between a source (s) node and its destination (t) node then the goodness of that path, represented by $g(path)$, is described as follows:

$$g(path) = f(g(link(1)), g(link(2)), \ldots, g(link(n))) \tag{12}$$

where ($link(1)$, $link(2)$, …, $link(n)$) constitutes the path. For illustration purposes, let us consider the benchmark graph shown in Fig. 2 as an example. The goodness function given in Eq. 12 may be used to compare goodness values of two different paths between a pair of nodes. For example, there are two paths from node s to node 2: $s-2$ and $s-3-2$ in the graph shown in Fig. 3. While $s-2$ is a direct path from node s to node 2 with just one link, $s-3-2$ includes two links. Even though $s-2$ is the one hop link, it may be possible that $g(s-2)$ may be worse than $g(s-3-2)$.

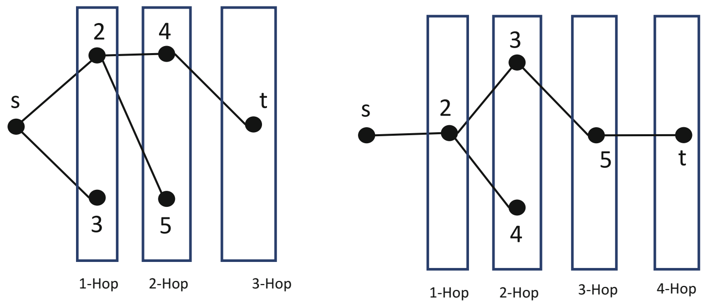

Fig. 3. Two possible configuration graphs q_1 and q_2 showing the best possible paths from the s to the rest of the nodes in the network

5.3 Third Level Analysis: Network Metrics

The network considered here is an overlay network, a partial network found by node s while it is trying to find possible routes to a destination node t. The third level analysis requires us to create a network configuration graph (q_1), a multi-layer graph starting from the source node to the destination node. In the configuration graph n^{th} layer represents the set of all nodes that can be reached from the source node in n hops. This process of generating configuration q_1 is described in Algorithm 1 below.

Algorithm 1. Algorithm for Generating the Configuration Graph

Initialization
Let $S = \{s, 2, 3, \ldots, t\}$ be the set of all nodes in the network and Let $S^{'}$=$\{\}$;
Move the source node (s) from S to $S^{'}$;
while there are nodes in the set S **do**
    for each node i in set S **do**
        identify the set of neighbors N_i of i
        for each node j in N_i **do**
            if the optimal path from s to j includes i, and $i \notin S^{'}$ **then**
                update the path from node s to j;
            end if
        end for
        Move the node i to $S^{'}$;
    end for
end while

Algorithm 1 outlines a systematic way to find optimal paths from a source (s) node to a destination (t) node. Starting from s, the algorithm enumerates the neighbors of s and finds the best routes to reach these neighbors in the first iteration. This process continues iteratively until all nodes are included in the configuration graph. In each iteration, the routes are refined taking into account the new neighbors added in each iteration. Figure 3 shows two possible configuration graphs that were generated using Algorithm 1. Configuration q_1 is generated when $g(s-2) < g(s-3-2)$ and $g(2-4) < g(2-3-4)$. Configuration q_2 is generated when $g(s-3) > g(s-2-3)$ and $g(2-4) > g(2-3-4)$.

6 Summary

This paper presented a hierarchical framework for computing goodness measures for links and paths in dynamic networks. A strategy for finding an optimal path between a pair of nodes is presented as an application for this hierarchical framework.

Acknowledgments. This research work was initially carried out at the Air Force Research Laboratory, Rome, NY, USA, as part of the visiting faculty research program during the summer 2016. It was continued at the University of North Texas with the support from the National Science Foundation through the smart and connected communities program, grant No. 1622978.

References

1. Sterbenz, J.P.G., Çetinkaya, E.K., Hameed, M.A., Jabbar, A., Qian, S., Rohrer, J.P.: Evaluation of network resilience, survivability, and disruption tolerance: analysis, topology generation, simulation, and experimentation. Telecommun. Syst. **52**(2), 705–736 (2013)
2. Çetinkaya, E.K., Broyles, D., Dandekar, A., Srinivasan, S., Sterbenz, J.P.G.: Modelling communication network challenges for future internet resilience, survivability, and disruption tolerance: a simulation-based approach. Telecommun. Syst. **52**(2), 751–766 (2013)
3. Sterbenz, J.P.G., Hutchison, D., Çetinkaya, E.K., Jabbar, A., Rohrer, J.P., Schller, M., Smith, P.: Redundancy, diversity, and connectivity to achieve multilevel network resilience, survivability, and disruption tolerance invited paper. Telecommun. Syst. **56**(1), 17–31 (2014)
4. Bhattacharya, A., Kumar, A.: A shortest path tree based algorithm for relay placement in a wireless sensor network and its performance analysis. Comput. Netw. **71**, 48–62 (2014)
5. Sbeiti, M., Goddemeier, N., Behnke, D., Wietfeld, C.: PASER: secure and efficient routing approach for airborne mesh networks. IEEE Trans. Wirel. Commun. **15**(3), 1950–1964 (2016)
6. Saleem, Y., Rehmani, M.H., Zeadally, S.: Integration of cognitive radio technology with unmanned aerial vehicles: issues, opportunities, and future research challenges. J. Netw. Comput. Appl. **50**, 15–31 (2015)
7. Newton, B., Aikat, J., Jeffay, K.: Analysis of topology algorithms for commercial airborne networks. In: 2014 IEEE 22nd International Conference on Network Protocols (ICNP), pp. 368–373. IEEE (2014)
8. Cheng, B.-N., Charland, R., Christensen, P., Veytser, L., Wheeler, J.: Evaluation of a multihop airborne IP backbone with heterogeneous radio technologies. IEEE Trans. Mobile Comput. **13**(2), 299–310 (2014)

9. Sparrow, R.D., Adekunle, A.A., Berry, R.J., Farnish, R.J.: Balancing throughput and latency for an aerial robot over a wireless secure communication link. In: 2015 IEEE 2nd International Conference on Cybernetics (CYBCONF), pp. 184–189. IEEE (2015)
10. Vaze, R.: Throughput-delay-reliability tradeoff in ad hoc networks. In: 2010 Proceedings of the 8th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), pp. 459–464. IEEE (2010)
11. Akbar, M.S., Yu, H., Cang, S.: Delay, reliability, and throughput based QOS profile: a MAC layer performance optimization mechanism for biomedical applications in wireless body area sensor networks. J. Sens. **2016**, 17 (2016)
12. Srinivasa, S., Haenggi, M.: Throughput-delay-reliability tradeoffs in multihop networks with random access. In: 2010 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton), pp. 1117–1124. IEEE (2010)
13. Caleffi, M., Ferraiuolo, G., Paura, L.: A reliability-based framework for multi-path routing analysis in mobile ad-hoc networks. Int. J. Commun. Netw. Distrib. Syst. **1**(4–6), 507–523 (2008)
14. Benaddy, M., Wakrim, M.: Cutset enumerating and network reliability computing by a new recursive algorithm and inclusion exclusion principle. Int. J. Comput. Appl. **45**, 22–25 (2012)
15. Lee, K., Lee, H.-W., Modiano, E.: Reliability in layered networks with random link failures. IEEE/ACM Trans. Netw. (TON) **19**(6), 1835–1848 (2011)
16. Elias, P., Feinstein, A., Shannon, C.: A note on the maximum flow through a network. IRE Trans. Inf. Theory **2**(4), 117–119 (1956)