SDNs in the Sky: Robust End-to-End Connectivity for Aerial Vehicular Networks

Gökhan Seçinti, Parisa Borhani Darian, Berk Canberk, and Kaushik R. Chowdhury

The authors propose an aerial network management protocol built on top of an SDN architecture. Unique to their design, each UAV becomes an SDN switch that performs under directives sent by a centralized controller. Using a novel 3D spatial coverage-related metric, the controller calculates diverse multiple paths among UAVs so that isolated and localized failures do not interrupt the overall network performance.

Abstract

Unmanned aerial vehicles allow rapidly deploying a multihop communication backbone in challenging environments with applications in public safety, search and rescue missions, crowd surveillance, and disaster area monitoring. Due to environmental obstructions in the above scenarios or intentional jamming, the communication links between peer unmanned aerial vehicless are susceptible to outages. This necessitates resiliency measures to be closely integrated into the network design. To address the needs of efficient and robust end-to-end data relaying, we propose an aerial network management protocol built on top of an SDN architecture. Unique to our design, each unmanned aerial vehicle becomes an SDN switch that performs under directives sent by a centralized controller. Using a novel 3D spatial coverage-related metric, the controller calculates diverse multiple paths among unmanned aerial vehicles so that isolated and localized failures do not interrupt the overall network performance. The controller issues directives to the unmanned aerial vehicle switches through flow entries in Openflow v1.5 protocol for immediate and effective switching to the best available path. Results reveal that the proposed multi-path routing algorithm reduces the average end-to-end outage rate by 18 percent while increasing the average end-to-end delay by 12 percent when compared to the traditional multi-path routing algorithms.

Introduction

In the last decade, unmanned aerial vehicles (UAVs) have seen deployments in various public safety applications, including search and rescue missions, advance reconnaissance for first responders, and detecting wildlife and marine predators for avoiding attacks on humans [1]. Typical UAV applications may involve forwarding time-critical data either generated from ground-users or collected via onboard sensors to remote pickup points. A reliable communication infrastructure among the UAVs becomes critical in maintaining this connected network for the data relaying tasks. However, traditional protocols and algorithms responsible for end-to-end (e2e) operation do not fully meet the challenges of the dynamic environments where UAVs operate. This article takes some important steps in this aspect by considering both the per-link connectivity as well as the holistic e2e performance. We first identify the limitations of UAV deployment, where UAVs are capable of utilizing different types of wireless standards such as LTE and WiFi for short-range access, including 802.11ac and 802.11ad. As wireless interfaces become smaller, lighter, and cheaper, it is only expected that future UAVs will be equipped with multiple interfaces adhering to the above standards. Each link access type will have implications on the range, error resiliency, and connectivity, which so far has not been studied in dynamic 3D environments.

The e2e connectivity becomes challenging as low-flying deployments of UAVs may encounter periodic disruptions. First, the characteristics of the environment may impact the quality of the communication links. For example, the rich signal reflection, blockages, and multi-path within the urban environment affect wireless links that are highly dependent on line of sight (LOS) conditions. Second, malicious users may choose to jam specific regions and portions of the spectrum. Thus, ensuring that resiliency is considered within the design of communication protocols for such networks is a key need. Our main approach in addressing these issues rests on a software defined networking (SDN) paradigm, which not only exerts control directives to adapt the network operations on demand, but also describes a generic networking framework for various applications that need reliable e2e performance.

Challenges in UAV Deployment

Figure 1 presents an overview of the major challenges in deploying UAV networks from a communications viewpoint. Also, how an SDN architecture may address some of them is shown and explained in detailed below:

Route determination: The unstable operational environment of UAVs impacts the operation of short-range wireless standards. When multiple link access standards exist, the neighborhood graph becomes dependent on the choice of the standard; that is, 802.11ac-based links reach farther than 802.11ad links, although the effective data rate in the former is fractional compared to 802.11ad. Thus, e2e routes must factor in the advantages and trade-offs associated with the choice of the link access technology between pairwise UAVs.

Limited onboard resources: Power and proces-

This work was completed during a research visit by G.Secinti at Northeastern University in 2016–2017.

Digital Object Identifier: 10.1109/MCOM.2017.1700456

Gökhan Seçinti and Berk Canberk are with Istanbul Technical University; Berk Canberk is also an adjunct associate professor at Northeastern University; Parisa Borhani Darian and Kaushik R. Chowdhury are with Northeastern University.

sor limitations impact not only the UAV's ability to handle real-time data but also the computational needs of identifying the e2e paths. Thus, relaying the acquired data from the sensors to a dedicated server via a communication backbone is necessary [2].

Frequent link disconnections: The 3D propagation environment may cause drastic changes in the signal-to-noise ratio (SNR), leading to frequent disconnection of the link between UAV peers. Some of the recent WiFi standards, such as 802.11ad, require beamforming, with the associated advantages of massive bandwidth available in the 60 GHz band. However, the links so formed are highly susceptible to outages caused by loss of LOS, which can result in a cascading effect on the entire data path.

Intentional disruption: The UAV network may face malicious attacks that blanket out a mission-critical area by intentional jamming/disruption. Several UAVs may be affected within this disruption radius concurrently, which may fully disconnect the e2e path. Thus, leveraging multiple paths between common endpoints to provide redundancy is no longer an option, but becomes a practical need in these circumstances.

To fully address the challenges above, we believe that limited centralized control that facilitates collaboration and communication is important. This is also important for future extensibility, when new link access standards become available. A network architecture design with UAVs must allow the ability to perform complex mission-based and standards-based trade-offs. Furthermore, the architecture itself must be isolated from the specific choice of the deployed wireless standard today, as the latter can rapidly evolve with time.

Vision of an SDN-Based UAV Network

SDNs provide an elastic and programmable network infrastructure that facilitates the management of various dissimilar protocols. It decouples the control and data mechanisms of the network, and treats the data plane entities as dummy devices subject to orchestration via a software controller [3]. The basic features of an SDN network are shown in Fig. 1, and their advantages are mapped to the aforementioned limitations of UAV networks. First, introduction of a software-defined centralized controller provides a global view of the network and enables formulating e2e strategies using the higher offsite computational power not available onboard the UAVs. This extensible paradigm allows offloading of future network functions, policies, and algorithms, such as complex data fusion/estimation that is needed in most application environments. Also, this decoupling allows implementing or modifying network protocols and policies without any change at the data plane infrastructure. Last, virtualization helps to maintain different functions and applications without necessitating additional changes in the UAV hardware. Thus, the same UAV can transition to a pure aerial sensor from an alternate role of data relaying with simple command directives.

Our proposed SDN-based UAV architecture (SD-UAV) has support for these features and is implemented using SDN-standards-compliant

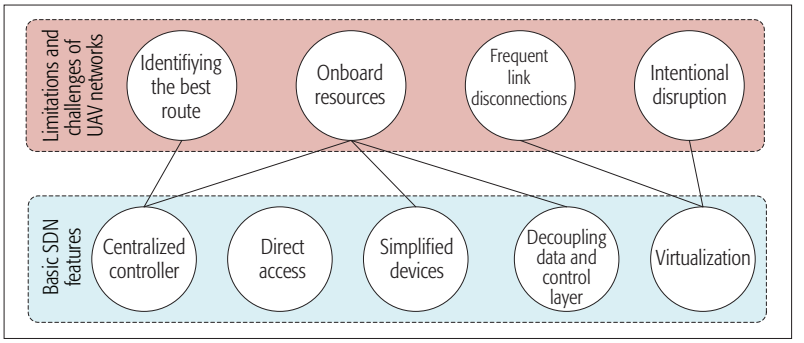

Figure 1. UAV networks with an overlay SDN architecture.

control protocols. As the first step, this article proposes an e2e routing protocol for multi-interface-enabled UAVs with improved resiliency of the network, where malicious jammers may disrupt the communication network. The proposed architecture is a general example of a UAV network, where each UAV acts as a software-defined switch, with the capability of configuring various radio access technologies (RATs) and computing resilient and diverse multi-path routes for data. The key algorithmic idea is that these multi-path routes are disjoint (i.e., they do not utilize any common UAV among their paths). Through a 3D separation heuristic, the controller also ensures spatial diversity of the routes. The goal is to dynamically form and switch the routes to make it impossible to totally disrupt an e2e connection by targeted jamming. The main contributions of this article include the following:

- We design a software defined architecture to address the limitations of UAVs.
- We introduce a centralized, graph theoretic approach that allows selection among different classes of wireless standards such as LTE, 802.11ad, and 802.11ac, as well as e2e paths that optimize data relaying subject to latency and throughput constraints.
- We propose a resilient multi-path routing metric that minimizes the impact of malicious jammers.

The rest of this article is organized as follows. The related work is given in the following section. Then the SD-UAV network architecture is described. We explain resilient multi-path routing protocol, and finally, we conclude the article.

Related Work

While there are various studies on e2e routing for ad hoc and vehicular networks, UAV networks are still in a nascent stage with many open challenges [4]. At a general level, neither resiliency of the network nor the implementation of software-defined approaches to UAV networks have been covered so far. Reference [5] proposes a speed-aware routing algorithm that is applied in the context of high-speed UAVs. This algorithm focuses on calculating optimal paths among UAVs using a traditional networking approach by estimating single-interface link conditions over the network. Furthermore, [6] proposes a fountain-code-based routing protocol where UAVs forward packets based on a metric that estimates the future positions of the given and neighboring UAVs to decide whether to forward the packet to a specific neighbor. This approach is

The UAVs act as software defined OpenFlow switches with a remote centralized controller [12] that coordinates with the deployed nodes via the OpenFlow v1.5 [13] south-bound protocol. All south-bound communications flow through a dedicated control channel between controller and UAVs. Each UAV is equipped with a GPS unit and various RATs such as LTE, 802.11ad, 802.11ac to communicate with each other.

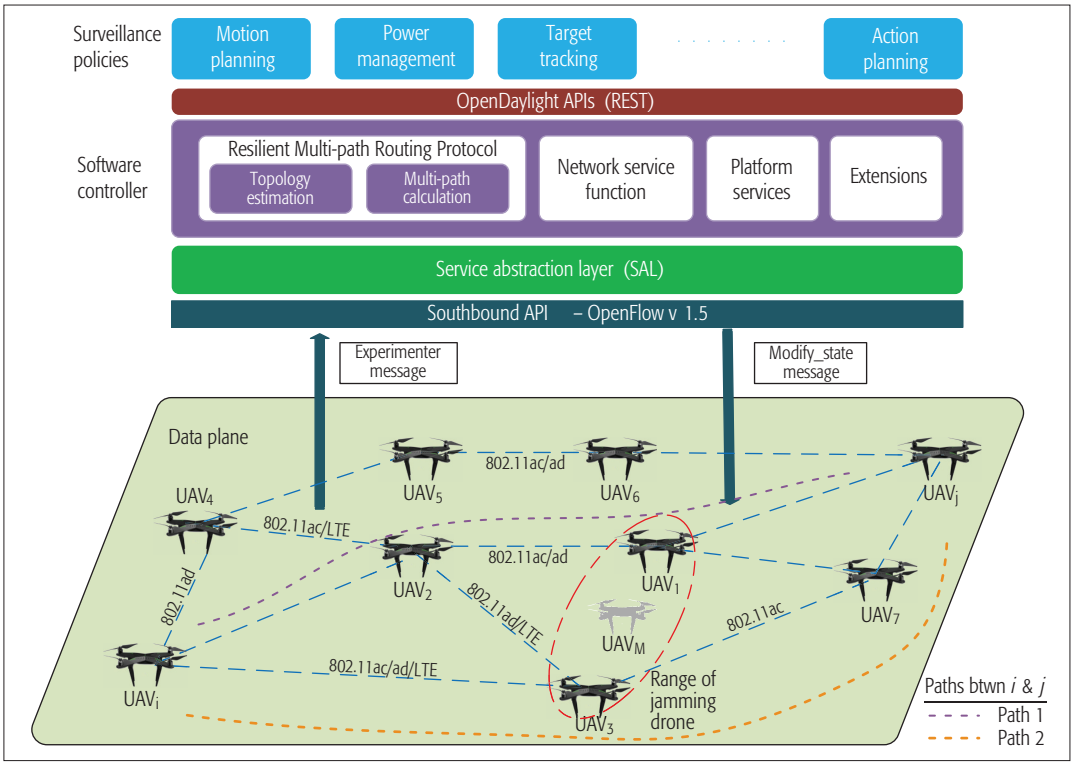

Figure 2. Proposed SD-UAV network architecture.

improved in [7] with queuing models for deciding the optimal choice of UAVs to forward packets. However, in the aforementioned studies, the routing decisions are made by the myopic information that a UAV is able to aggregate from its neighbors. Thus, none of them utilizes the global view of the network and addresses the resiliency of communication in UAV networks from a holistic viewpoint. Reference [8] describes the issues in the network layer communication for UAVs in traffic surveillance. Here, UAVs wirelessly receive control instructions from the base station and send back images, video, and data. Consequently, the issues considered in this work are high-bandwidth requirements, asymmetric data communications, and integration with ground sensors. Finally, [9] classifies the multi-UAV system as flying ad hoc networks while pointing out that such a network has different characteristics from classical ad hoc networks in terms of node mobility, node density, frequency of topology change, radio propagation, and communication challenges. These key considerations also motivate our own work.

Additionally, the challenge of ensuring path resilience has been explored in a different context in terrestrial wired communication networks [10], where multi-path Internet routing for connecting the ISP backbones is proposed using a metric that measures physical diversity of the paths. Such redundant paths provide reliability for sudden loss of e2e connectivity resulting from a sudden node failure. However, as mentioned earlier, simply calculating various disjoint paths is not an effective solution given the dynamic 3D nature of UAV networks. Finally, [11] addresses the integration of cognitive radio with UAV networks by emphasizing issues and challenges for each layer of the network protocol stack.

SD-UAV Network Architecture and Design

The UAVs act as software defined OpenFlow switches with a remote centralized controller [12] that coordinates with the deployed nodes via the OpenFlow v1.5 [13] southbound protocol. All southbound communications flow through a dedicated control channel between the controller and UAVs. Each UAV is equipped with a GPS unit and various RATs such as LTE, 802.11ad, and 802.11ac to communicate with each other.

OpenFlow protocol messages such as `Experimenter` and `Modify_State` are used both to acquire necessary information from the data plane and to implement multi-path routes among UAVs for providing resilient e2e connections, as shown in Fig. 2.

First, the software controller acquires 3D location and channel availability information from the data plane for each UAV through the payload contained in the `Experimenter` messages. Then the software controller aggregates the information sent by UAVs to estimate a snapshot of the network topology. The multi-path routing algorithm uses this snapshot to determine diverse routes using our spatial diversity metric. These snapshots are updated frequently enough to cover any changes in the topology. Thus, the issues that may occur upon the snapshot updates are not covered in this study. After generating the topology, each link between UAVs is represented by the estimated transmission time (*ETT*). We note that the *ETT* changes with the choice of wireless standard. Thus, the controller creates a map of every possible interface connection between a pair of UAVs, with the weight of the connecting edge defined by the *ETT*. During algorithm execution, one of these edges is chosen per active

connection between UAVs, which also decides the specific choice of wireless technology to be used in that link. In this manner, *ETT* is a function of both packet error rate and data rate of various available RATs [14].

Both packet error rate and the data rate for a specific RAT are estimated by using the physical distance and angular position between UAVs, based on their respective GPS-defined locations. The process of *ETT* calculation for a given link choice is simple: the expected packet retransmission count is estimated by using the packet error rate. Then *ETT* is calculated with the data rate and expected transmission count [14]. In order to calculate the *ETT* for each wireless standard, we perform comprehensive simulations in MATLAB. Table 1 shows the *ETT* for a typical scenario where the distance and the noise level for each of the technologies is assumed to be equal to 0.5 km and –93 dB, respectively. We use free space path loss, and then the transmission power is set to achieve the required SNR. Lastly, calculated ETT according to the modulation and the coding rate of each technology with respect to the estimated SNR is utilized to determine optimal paths by the proposed routing algorithm, described later.

After the routing algorithm calculates the multiple paths among UAVS, the group table capabilities are utilized for implementing multi-path routing protocols to orchestrate flow entries over OpenFlow-capable SD-UAVs. The flow tables and the related group action buckets are configured by `Modify_State` messages from the controller. A flow entry is implemented for each e2e connection, and their actions are set as `go_to_group_table` where groups tables hold the information of multi-path routing configuration. More specifically, the calculated multi-path routes are implemented by using fast failure recovery group tables, in which each diverse route is defined as an action bucket. Thus, when a link fails in an e2e connection, a UAV is capable of choosing an alternative route that is already defined as a different action bucket without consulting the controller. This ensures minimum disruption time for the network.

Resilient Multi-Path Routing Protocol

The physically diverse paths are calculated by using the snapshot of the network in order to define resilient e2e connections. We adopt the modified Dijkstra algorithm with a vertex splitting method [15] to calculate various diverse paths between any source and destination optimally. However, solely utilizing disjoint optimal multi-paths between two nodes without considering spatial separation distances between the UAVs on different paths is not enough; in fact, it provides an opportunity for a single jamming attack to disrupt multiple paths concurrently.

An example scenario is given in Fig. 2. There are two physically diverse paths defined between UAV_i and UAV_j. *Path1* utilizes UAVs <*i*, 2, 1, *j*>, while *Path2* utilizes UAVs <*i*, 3, 7, *j*> in order to connect the source to the destination. Assume that these paths are optimal in terms of overall ETTs in order to minimize e2e delay. However, a malicious UAV, say UAV_M, is able to jam the communication of UAVs (1 and 3) in both paths and disrupt e2e connection between UAV_i and

Standard	Freq. (GHz)	Modulation	Rate (Mb/s)	ETX	*ETT* (ms)
802.11ad	60	64-QAM	6237	1.06	5.4697
LTE	2.69	64-QAM	302.4	1.01	26.69
802.11ac	5	QPSK	1404	1.08	20.05

Table 1. *ETT* for different RATs at distance 0.5 km and coding rate of 3/4 and target SNR = 22.

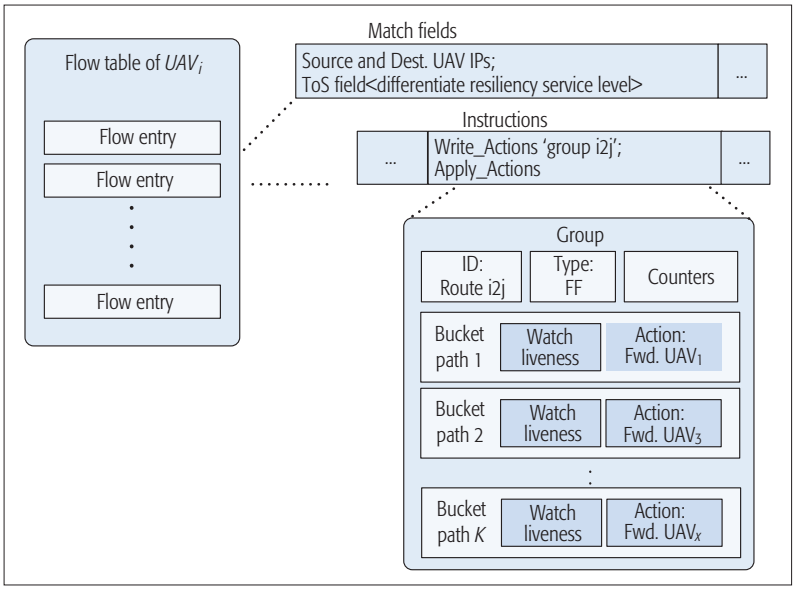

Figure 3. Flow table and group action definitions.

UAV_j. This undesirable situation nullifies the benefit of multi-path routes. To mitigate this situation, we enhance the disjoint multi-path algorithm [15] with our proposed heuristic γ. γ is used to multiply *ETT* values calculated for the links of those UAVs that are physically close to the UAVs in the already finalized paths. To do so, we assume that all UAVs in the network have the same range as the jamming source, and we aim to minimize the intersection of ranges between UAVs that belong to a different route. A malicious jamming source within the intersecting spheres may disrupt multiple UAVs on different routing paths, and thus nullify the redundancy advantage of multi-path routing. Hence, γ is defined as a natural exponential function that takes in the volume of intersecting ranges of UAVs on different paths as the parameter, and then computes a multiplier to scale the ETT values. As described earlier in the example in Fig. 2, we assume that the shortest path between *i* and *j* is <*i*, 2, 1, *j*>. Thus, this is the first path obtained for the network. Then the proposed algorithm utilizes the metric γ to increase *ETT* values of all links of the UAVS that have intersecting range with UAV_1 or UAV_1. In this manner, we aim to deter selection of physically closer paths to avoid them being disrupted by a single jamming source.

The flowchart of the proposed routing algorithm is given in Fig. 4. The algorithm calculates *K* number of disjoint paths for a pair of UAVs. Thus, the given algorithm runs for every UAV pair in the data plane individually. The shortest path is calculated first between pre-defined source and destination UAVs. Then the vertex splitting

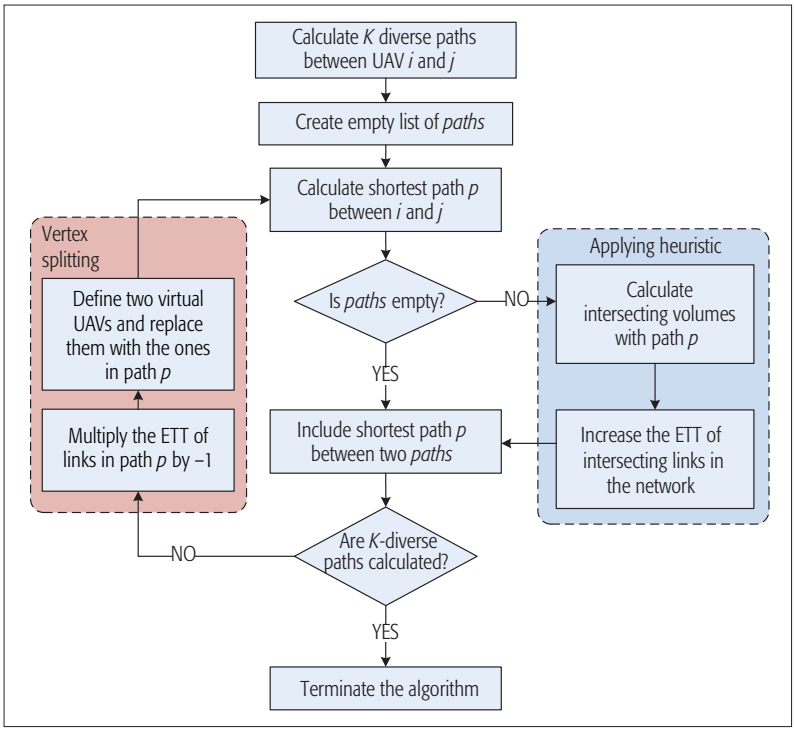

Figure 4. Flow chart of the proposed routing algorithm.

method [15] is applied on the path before calculating another diverse path between source and destination. This method consists of two internal steps as follows. First, the bidirectional edges on the path are re-defined as arcs (directed edges) by reversing their directions from the destination to the source and their initial weight (i.e., *ETT*) values are multiplied by –1. Second, the vertices that represent the UAVs on the path are split into two distinct vertices in such a way that one of them only contains incoming edges while the other one only contains outgoing edges. After these two steps, another shortest path may be calculated on this graph in order to obtain diverse paths. Further details of the vertex splitting method are given in [15]. As an enhancement to the algorithm, after updating the graph with vertex splitting, we apply the proposed metric γ to multiply the weight of all the edges that have intersecting volumes with the ones in the path. The heuristic is a natural exponential function that utilizes intersecting volumes between UAVs as an input. These individual volume values are normalized by dividing the maximum possible volume. Last, the algorithm repeats the steps explained above to calculate an additional path in every run until it calculates K diverse paths between UAV-peers. Thus, the algorithm poses $O(K \cdot (V\log V + E))$ asymptotic complexity to calculate all e2e paths from one UAV to others where V and E are the number of UAVs and the number of edges between UAVs.

Performance Evaluation

The performance of the proposed resilient multi-path routing protocol is evaluated with a random topological configuration that consists of 50 UAVs in 1 km^3 space where the jammers are positioned randomly. Furthermore, we assume that the jammers are able to disrupt all available wireless standards within its range as a worst case scenario. The e2e outage rate of the proposed algorithm is evaluated by comparing it to a traditional shortest path algorithm and shortest multi-path algorithms for two diverse paths (K = 2), since these two algorithms are able to calculate the optimal paths in fully known graphs. The first algorithm in the evaluation performs poorly in terms of e2e outage, since it only calculates the shortest path and provides a single route, making the network vulnerable with a single jammer. The second algorithm calculates two diverse routes between each pair. However, this algorithm aims to determine an optimal solution in terms of e2e delay without considering actual physical distances between routes. Thus, it performs worse than our proposed multi-path routing algorithm when there are malicious jammers. As seen in Fig. 5, our approach outperforms the other algorithms by providing lower e2e outage ratio under various numbers of jammers. However, as the number of jammers increases in the network, e2e outage difference diminishes between the proposed and shortest multi-path algorithms. Since the competing approaches only provide two distinct routes (K = 2), as the number of jammers grows, providing two such paths becomes an ineffective solution. Instead, the number of alternative paths (K) should be increased in proportion. Finally, since the proposed algorithm aims to diverge from optimal paths for the sake of reducing e2e outage ratio by eliminating intersecting ranges of UAVs on different routes, our algorithm performs slightly worse in terms of average e2e delay.

Conclusion

In this article, we propose an SD-UAV network architecture that utilizes multiple wireless link access technologies such as LTE, 802.11ad, and 802.11ac. Furthermore, we devise a resilient multi-path routing protocol that identifies multiple disjoint routes for UAV pairs in order to improve resiliency of the network. Our approach, used in conjunction with a spatial resiliency metric, reduces the outage rate of end-to-end connections in the presence of malicious UAVs. Finally, we show that the proposed framework performs better in terms of end-to-end outage with moderate reduction in end-to-end delay compared to traditional algorithms. As future work, we aim to enhance this study through a system-level implementation in a real 3D environment. Then the proposed algorithm will be evaluated further under various mobility and traffic patterns. We will also extend the algorithm to cover battery limitations of UAVs while determining the optimal routes.

Acknowledgment

This work was supported by the U.S. Office of Naval Research under grant number N000014-17-1-20416.

References

[1] M. Erdelj *et al.*, "Help from the Sky: Leveraging UAVs for Disaster Management," *IEEE Pervasive Computing*, vol. 16, no. 1, Jan 2017, pp. 24–32.
[2] N. H. Motlagh, M. Bagaa, and T. Taleb, "UAV-Based IoT Platform: A Crowd Surveillance Use Case," *IEEE Commun. Mag.*, vol. 55, no. 2, Feb. 2017, pp. 128–34.
[3] I. F. Akyildiz *et al.*, "Research Challenges for Traffic Engineering in Software Defined Networks," *IEEE Network*, vol. 30, no. 3, May 2016, pp. 52–58.

[4] L. Gupta, R. Jain, and G. Vaszkun, "Survey of Important Issues in UAV Communication Networks," *IEEE Commun. Surveys & Tutorials*, vol. 18, no. 2, 2016, pp. 1123–52.
[5] S. Rosati *et al.*, "Speed-Aware Routing for UAV Ad-Hoc Networks," *IEEE GLOBECOM Wksps.*, Dec 2013, pp. 1367–73.
[6] Y. Zhu *et al.*, "Design and Evaluation of Airborne Communication Networks," *7th Int'l. Conf. Ubiquitous and Future Networks*, July 2015, pp. 277–82.
[7] C. Yin *et al.*, "Enhanced Routing Protocol for Fast Flying UAV Network," *IEEE Int'l. Conf. Commun. Sys.*, Dec 2016, pp. 1–6.
[8] A. Puri, *A Survey of Unmanned Aerial Vehicles (UAV) for Traffic Surveillance*, Ph.D. dissertation, Dept. Comp. Sci. and Eng., Univ. South Florida, 2005.
[9] I. Bekmezci, O. K. Sahingoz, and Ş. Temel, "Flying Ad-Hoc Networks (FANETs): A Survey," *Ad Hoc Networks*, vol. 11, no. 3, 2013, pp. 1254–70.
[10] J. P. Sterbenz *et al.*, "Evaluation of Network Resilience, Survivability, and Disruption Tolerance: Analysis, Topology Generation, Simulation, and Experimentation," *Telecommun. Sys.*, vol. 52, no. 2, Feb. 2013, pp. 705–36.
[11] Y. Saleem, M. H. Rehmani, and S. Zeadally, "Integration of Cognitive Radio Technology with Unmanned Aerial Vehicles: Issues, Opportunities, and Future Research Challenges," *J. Network and Comp. App.*, vol. 50, 2015, pp. 15–31.
[12] The Linux Foundation Projects, "OpenDaylight — An Open Source Software Defined Networking Platform," 2013; https://www.opendaylight.org/.
[13] ONF, "OpenFlow Switch Specification v. 1.5.0," tech. rep. ONF TS-020, 2014.
[14] R. Draves, J. Padhye, and B. Zill, "Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks," *Proc. 10th Annual Int'l. Conf. Mobile Computing and Networking*, 2004, pp. 114–28.
[15] R. Bhandari, *Survivable Networks: Algorithms for Diverse Routing*, Kluwer, 1998.

Biographies

Gökhan Seçinti [S'13] (secinti@itu.edu.tr) received his Ph.D. degree from Istanbul Technical University in 2017. He serves as a reviewer for *IEEE Communications Magazine*, *IEEE Transactions on Vehicular Technology*, *IEEE Transactions in Wireless Communications*, *The International Journal of Communication Systems*, and *The International Journal of Computer and Telecommunications Networking*. He was a recipient of the IEEE INFOCOM Best Poster Paper Award (2015) and the IEEE CAMAD Best Paper Award (2016). His current research includes software-defined networking and performance analysis of 5G networks.

Parisa Borhani Darian received her B.S. and M.S. degrees in computer engineering from Azad University, Iran, in 2008 and 2013, respectively. She is currently pursuing a Ph.D. degree in computer engineering at Northeastern University, Boston, Massachusetts. Her research interestsnclude communication of UAVs and SDNs.

Berk Canberk [S'03, M'11, SM'16] (canberk@itu.edu.tr) is an associate professor at the Computer Engineering Department at ITU. Since 2016, he has also been an adjunct associate professor with the Department of Electrical and Computer Engineering at Northeastern University. He was a recipient of the IEEE CAMAD Best Paper Award (2016), the Royal Academy of Engineering (UK) NEWTON Research Collaboration Award (2015), and the IEEE INFOCOM Best Poster Paper Award (2015). His current research areas include software-defined networking, 5G network performance analysis and modeling, and cognitive radio networks.

Kaushik R. Chowdhury [M'09, SM'15] is an associate professor in the Electrical and Computer Engineering Department at Northeastern University. He was awarded the Presidential Early Career Award for Scientists and Engineers (PECASE) in January 2017, the DARPA Young Faculty Award (2017), the Office of Naval Research Director of Research Early Career Award (2016), and the NSF CAREER award (2015). His current research areas include networked robotics, dynamic spectrum access, RF energy harvesting sensors, and intra-body implant communication.

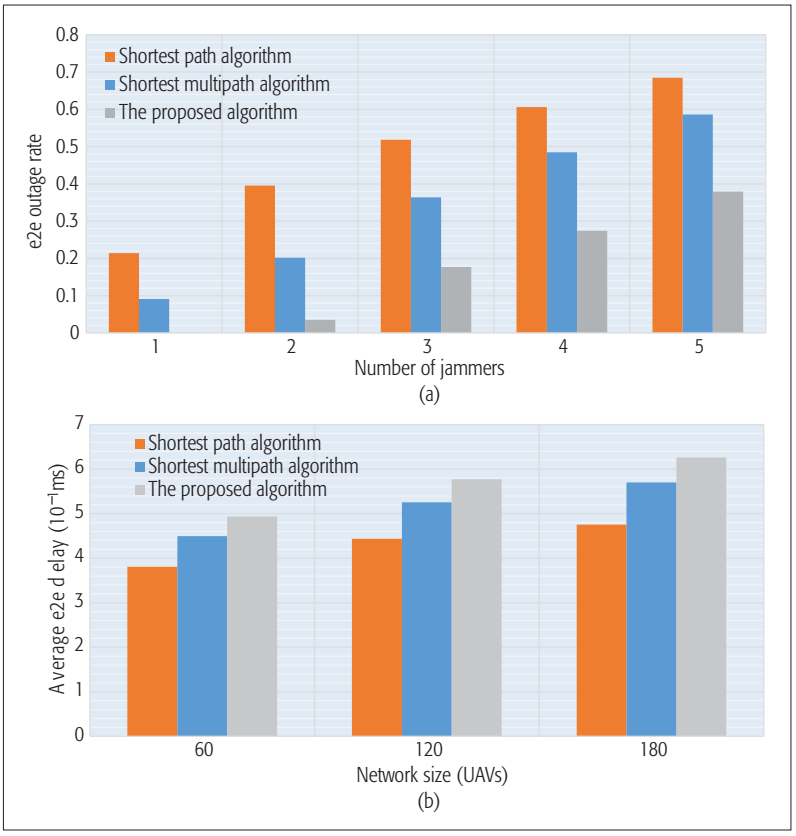

Figure 5. Performance evaluation: a) e2e outage ratio; b) average e2e delay.