Airborne network: A cyber–physical system perspective

Conference Paper · January 2012
DOI: 10.1145/2248326.2248340

CITATIONS
7

READS
130

4 authors, including:

K. Namuduri
University of North Texas
125 PUBLICATIONS 923 CITATIONS
SEE PROFILE

Mahadevan Gomathisankaran
University of North Texas
46 PUBLICATIONS 113 CITATIONS
SEE PROFILE

Ravi Pendse
Brown University
117 PUBLICATIONS 402 CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Aerial Base Stations View project

All content following this page was uploaded by Mahadevan Gomathisankaran on 18 February 2014.

The user has requested enhancement of the downloaded file. All in-text references underlined in blue are added to the original document and are linked to publications on ResearchGate, letting you access and read them immediately.
Airborne Network: A Cyber-physical System Perspective

Kamesh Namuduri
Department of Electrical Engineering
University of North Texas
kamesh.namuduri@unt.edu

Yan Wan
Department of Electrical Engineering
University of North Texas
yan.wan@unt.edu

Mahadevan Gomathisankaran
Department of Computer Science and Engineering
University of North Texas
mgomathi@unt.edu

Ravi Pendse
Department of Computer Science and Electrical Engineering
Wichita State University
ravi.pendse@wichita.edu

ABSTRACT
An airborne network is a cyberphysical system (CPS) in which there is an intense interaction between the physical and cyber components. While computation, communication and networking elements form the cyber components of the system, flight-paths, manoeuvre geometries, and multi-mode resources including ground-based nodes and control stations form the physical components of the CPS. The synergy between the cyber and physical components, if explored and exploited, will significantly enhance the safety and security capabilities of Next Generation (NextGen) air transportation systems. In this paper, we characterize airborne networks based on their mobility patterns, path predictability, and model complexity. We discuss mobility models suitable for airborne networks, analytical models for estimating the link/path duration in airborne networks, and strategies for information assurance in airborne networks.

Categories and Subject Descriptors
C.2.1 [Network Architecture and Design]: Network Communications

Keywords
Cyber-Physical System, Airborne Networks

1. INTRODUCTION
Enhanced safety and security are the primary objectives for the Next Generation (NextGen) air transportation systems (Fig. 1). Although significant progress has been made in many dimensions of air transportation systems (e.g. airspace management, data link capability), there is a definite need to enhance the safety and security capabilities (e.g. sense and avoid, safe navigation, and secure communication) of NextGen transportation systems. One approach towards achieving these objectives is through airborne networking.

Airborne networks (ANs) are a class of autonomous mobile ad-hoc networks (MANETs) consisting of several subnets of nodes making connections as they fly by the existing subnets. Airborne networks are unique and significantly different from vehicular networks involving only ground vehicles, in many perspectives. Classical mobility models and security strategies designed for MANETs and ground vehicular networks are not suitable for airborne networks. Mobility models that take into account the unique characteristics such as smooth turns, and high-level information assurance, authentication and integrity verification strategies that can meet the minimum latency requirements are needed for airborne networks.

In this paper, we first characterize airborne networks in terms of connectivity, randomness, and path predictability. Then, we discuss and mobility models suitable for airborne networks, and analytical models for path duration estimation in airborne networks. Finally, we discuss mechanisms for confidentiality and integrity protection and remote integrity verification strategies for verifying the dynamic state of airborne nodes and validate their trustworthiness.

The organization of this paper is as follows: Section 2 presents the cyber-physical system perspective of an airborne network. Section 3 discusses mobility models for airborne networks. Section 4 outlines path duration estimation in airborne networks. Section 5 discusses secure information sharing strategies. Section 6 concludes the paper.

2. AIRBORNE NETWORK FROM A CYBER-PHYSICAL SYSTEM PERSPECTIVE
An airborne network is a cyber-physical system (CPS) in which there is an intense interaction between its physical and cyber components. While computation, communication and networking elements form the cyber components of the system, flight-paths, manoeuvre geometries, and multi-mode resources including ground-based nodes and control stations form the physical components of the CPS (Fig. 2).

The fundamental challenge for airborne networks is to bring the synergistic interactivity between its cyber and physical components. This synergy, if successfully explored...
and exploited, will immensely benefit the NextGen air transportation systems. For example, predicting the trajectories of airborne vehicles within the neighborhood (say, 1000 square mile region), forming a trusted network with friendly nodes, reconfiguring the network as its topology changes, and sharing audio and video streaming data securely over the air among the pilots, will significantly improve the situational awareness of an airborne vehicle, and enhance the safety capabilities of the air transportation system. However, fundamental design principles which are needed to explore this synergy between the cyber and physical dimensions do not exist and experimental datasets which are needed to develop such design principles are beyond the reach of academic community.

Figure 1: Cross-cutting themes in Next Generation air transportation systems. (Source: NextGen focus group meeting held at NSF, in Nov. 2010). NAS: National Air Space.

Figure 2: Cyber-physical perspective of airborne network: fundamental and multidisciplinary engineering design principles of an airborne network.

Figure 3 illustrates a network consisting of few airborne and ground nodes. Node altitudes and distances between the nodes are expected to be highly variable in airborne networks. The nodes in an airborne network may be static or move at speeds of over 1000 MPH, leading to extremely dynamic topological changes in the network. Factors that need to be considered in designing high-performance airborne networks include timeliness and integrity of information being shared, high bandwidth usage, and scalability.

3. MOBILITY MODELS

Mobility models provide a framework for connectivity studies, network performance evaluation, and eventually the design of reliable routing protocols [12]. In particular, mobility models capture the random movement pattern of each network agent, based on which rich information related to the varying network structure can be estimated, such as node distribution and the statistics of link and path lifetime. In order to provide accurate predictions to facilitate airborne networking, it is crucial to develop realistic and tractable mobility models for ANs. Some mobility models have received extensive studies in the literature, such as random direction (RD), and random waypoint (RWP) [6, 32, 8, 17]. The RWP model assumes that an agent chooses a random destination (waypoint) and traveling speed; upon the arrival, it pauses before traveling to the next destination. The extended version of RD model assumes that an agent chooses a speed and direction randomly after a randomly selected traveling time [14, 13]. The stochastic properties of these common models such as their spatial distributions can be found in e.g., [6, 24, 17, 8].

The widely used RWP and RD models are well suited to describe the random activity of mobile users in MANETs; however, they lack the capability to describe features that are unique to airborne vehicles. For example, it is easy for mobile users/ground vehicles to slow down, make sharp turns, and travel in an opposite direction (see an enhanced random mobility model that captures such movement [5]). However, airborne vehicles tend to maintain the same heading speed and change direction by making turns with a large radius. This unique feature is caused by the mechanical and aerodynamical constraints for airborne vehicles and reflected in the correlation in acceleration along spatial and temporal dimensions. Capturing this smooth-turn feature into mobility models can significantly improve path estimation and connectivity analysis for airborne networks. There is a need to develop a thorough theoretical study of realistic models that capture such features unique to airborne networks, and whereas simple and tractable enough to facilitate connectivity analysis and routing design.

In order to facilitate the theoretical study, we first char-
acterize airborne networks based on their mobility patterns, path predictability, and model complexity. Fig. 4 shows one such characterization driven by real-world applications. Such categorization explains the need for the design, analysis, and development of realistic mobility models suitable for airborne networks.

4. PATH DURATION ESTIMATION IN AIRBORNE NETWORKS

Design models and tools for MANETS that exist today are mostly empirical or simulation-based. Although there are few analytical methods which provide insights into mobility aspects, they are incomplete and address only parts of the problem. For example, mobility models and path duration analysis applicable for MANETS and ground vehicles [9, 33, 31, 7] are available in the literature. However, they do not consider high mobility and frequent link failures that characterize airborne networks. Delay-tolerant computing [2] and resilient networking [3] models, although share some common features with airborne networking, they are not applicable for low latency applications.

Path duration statistics are investigated in [28, 4, 16, 21, 9, 22, 23]. The problem with the shortest path and the phenomenon called “edge effect” that occurs at a high node density are discussed in [22]. In explaining the edge effect, the authors point out that when the node density is high, the probability of finding relay nodes at the edges of transmission radius is very high. In such a situation, even a small movement of nodes will lead to link breakage and ultimately to path breakage. In [9], the authors point out that the shortest path is not the best path when the path duration is taken into account and point out that the lifetime estimation of links is essential for finding routes that can last for a longer time. The correlation between average path duration, throughput, and overhead of the reactive routing protocols is investigated in [28]. Even though the authors identified node density as an important parameter that influences path duration, they didn’t attempt to derive this relationship. The lack of appropriate analytical models that are capable of estimating path duration is the motivation for this proposal.

Also of relevance to our study, the behavior of communication links is discussed in [19, 11, 18, 29, 22, 10, 15], mobility metrics and performance analysis are discussed in [30, 20, 27, 10], and adaptive routing protocols are discussed in [26, 11, 9]. Link distances and their relationship with hop count are examined in [11], assuming that the selection of a relay node is a function of the least remaining distance (LRD) to destination. Optimal transmission radius for radio terminals has been investigated in [18]. An ad-hoc routing protocol based on stability and hop count has been proposed in [29].

We developed a probabilistic model for predicting the average path duration based on the known network parameters [25]. We established the impact of network density (along with other parameters such as transmission range, maximum velocity, and number of hops) on path duration. This model was simulated in NS-2 by varying the following parameters: velocity (1800 KMPH to 18000 KMPH), transmission range (100 KM to 400 KM), number of nodes (10 to 90), number of hops (1 to 4), and area (1000 KM x 1000 KM). The results are compared with those obtained from MATLAB implementation of the analytical model. As shown in Fig. 5, 6, 7 and 8, the theoretical predictions agree with the simulated values demonstrating the validity of the analytical model.

Fig. 5 shows a plot between transmission range and average path duration. This plot suggests that the average path duration increases almost linearly with increase in transmission range. Fig. 6 shows the plot between average velocity of nodes and average path duration. The plot suggests that the average path duration exponentially drops as the speed increases. Such exponential relationship between node velocity and path duration has also been observed through simulations in [28, 19]. Fig. 7 shows a plot between number of hops and average path duration. The plot shows that the duration is much longer for one hop link, and there is a steep fall in the path duration when the number of hops increase. The distribution can be approximated to exponential distribution for hops > 2 as suggested in [28]. Fig. 8 shows a plot between node density and average path duration. The plot shows that an increase in node density is potentially beneficial, but the returns are very minimal as the density gets higher.

![Figure 4: Mobility Models for airborne networks with applications to next generation air transportation systems](image)

![Figure 5: Transmission range versus average path duration](image)
5. SECURE INFORMATION SHARING IN AIRBORNE NETWORKS

Airborne networks pose unique challenges in terms of information sharing and information security in airborne networks. Fast moving nodes create constant topological changes in the network resulting in frequent disconnections and disruptions in the network. In an airborne network, each node is viewed as an autonomous embedded system with local and network level resource constraints. As the autonomous system evolves by interacting with its environment, it also becomes vulnerable to malicious control by adversaries. Thus, it is imperative that an airborne network requires security strategies that can protect the integrity of its embedded systems and allow for its verification so as to make the system trustworthy. Classical security solutions like TPM [1] are unsuitable for airborne networks due to their heavy-weight computations and long latencies.

Desirable security characteristics of an airborne network and its embedded systems include (1) confidentiality - which assures that valuable assets such as passwords, secret keys, intellectual property captured in software algorithms, hardware design or content are not revealed to an unauthorized observer, (2) integrity - which assures that critical data and programs - of users, system, firmware, and hardware are not tampered with to produce undesirable, adversarial behavior. The attack space, as shown in Figure 9, is expanded to include an adversary with physical possession of the device. This allows an adversary to observe board level buses, measure side-channels such as $V_{dd}$ pin based power. A state sponsored well funded adversary can even reverse engineer transistor level geometry of the chip and observe data using electron microscope and other devices.

6. CONCLUSIONS

Suggesting that an airborne network is a cyber-physical system, we characterized airborne networks based on their mobility patterns, path predictability, and model complexity. We discussed mobility models suitable for airborne networks analytical models for estimating the link/path duration in airborne networks, and secure strategies for information sharing in airborne networks.

7. REFERENCES