Manipulating the Five V's in the Next Generation Air Transportation System

Dustin Mink[1(✉)], William Bradley Glisson[1], Ryan Benton[1], and Kim-Kwang Raymond Choo[2,3]

[1] School of Computing, University of South Alabama, 150 Jaguar Drive, Suite 2101, Mobile, Al 36688, USA
dmm1521@jagmail.southalabama.edu, {bglisson,rbenton}@southalabama.edu
[2] Department of Information Systems and Cyber Security, The University of Texas at San Antonio, San Antonio, TX 78249-0631, USA
[3] School of Information Technology and Mathematical Sciences, University of South Australia, Adelaide, SA 5095, Australia
Raymond.Choo@fulbrightmail.org

Abstract. The U.S. Next Generation Air Transportation System (NextGen) is designed to increase the capacity, safety and efficiency of the air traffic control via the integration of past experiences and advances in technology. However, the system is expected to greatly increase the amount and types of data generated as well as the knowledge to be managed. Additionally, as with all new technology, U.S. NextGen opens the specter of the potential impacts created by cyberattacks. Given this, it appears logical to view the U.S. NextGen system from the lens of Big Data. This study evaluates the U.S. NextGen system using the five differentiated qualitative characteristics of big data: Volume, Velocity, Variety, Veracity and Value. The results indicate that U.S. NextGen system has several big data challenges that must be addressed in order to obtain its maximal potential.

Keywords: NextGen · ADS-B · IoT · Big data · Cybersecurity

1 Introduction

The impact of the aviation industry in today's globally integrated societies is evident from both economic and governmental perspectives. A 2016 report by the U.S. FAA indicates U.S. Gross Domestic Product (GDP) will increase from $16.3 trillion U.S. dollars in 2015 to $26.2 trillion in 2036 [1]. Furthermore, the world GDP is forecasted to increase from 74.4 trillion U.S. dollars in 2015 to $136.3 trillion in 2036.

While the issue of funding security is always challenging particularly in a tight fiscal climate [2], the escalation of cyber-security concerns in the aviation environment, from the government perspective, is very visible through legislative activities like the Senate subcommittee approving a bill to investigate aviation security and cybersecurity [3]. An article on the World Economic Forum highlights the fact that the proliferation and equalization of technology accessibility increases the potential number of attackers [4].

X. Lin et al. (Eds.): SecureComm 2017 Workshops, LNICST 239, pp. 271–282, 2018.
https://doi.org/10.1007/978-3-319-78816-6_19

It also goes on to note that the integration of cyber and physical environments not only create new vulnerabilities but, potentially, has extensive impacts in the aviation industry. The importance of cybersecurity is reinforced in incidents such as those involving Brussels' airport [5], MH17 in the Ukraine [6] and the missing Malaysia Flight ML370 [7].

In an attempt to mitigate security concerns, the U.S. Government Accountability Office [8] states that the aviation industry is in the process of rolling out the U.S. Next Generation (NextGen) Air Traffic System. While all of the U.S. NextGen component programs are at various stages of development, they are targeted to be operational no later than the 2020 [8]. U.S. Government Accountability Office (US GAO) indicates that the U.S. NextGen system is, currently, comprised of six parts, namely: Automatic Dependent Surveillance Broadcast (ADS-B), Collaborative Air Traffic Management Technologies (CATMT), Data Communication, National Airspace System Voice System, U.S. NextGen Air Transportation System Weather, and System Wide Information Management. According to the US GAO, a major element of this system is the ADS-B capability, which is directed to be the future of air traffic control through advancements in aircraft tracking and flow management. They also state that the U.S. NextGen ADS-B messages are sent continually every five seconds. Furthermore, there are three different ADS-B message types, namely: position messages, velocity messages, and identification messages. CATMT is the program that is responsible for enhancing the existing traffic flow management system and subsequently will have to handle the volume of data the ADS-B will be producing [8]. Complicating matters, there are documented exploitations of ADS-B system [9–11]. Hence, spoofing aircraft with fake ADS-B messages is a viable concern. Fingerprinting aircraft transponders transmitting ADS-B and cross referencing with aircraft equipment transponders allows for the inference of airline communications. This environment prompted the idea that the ADS-B message system should be examined from the perspective of the five differentiated qualitative characteristics of big data, namely: Volume, Variety, Velocity, Variability, and Value [12]. In this environment, each aircraft can be thought of as a very complex device or node that communicates with other aircraft and Air Traffic Control Facilities (ATCF). The goals are two-fold. First, identify the big data issues within the U.S. NextGen Air Transportation System architecture. Second, understand which of the five differentiated qualitative characteristics apply to the unique U.S. NextGen Air Transportation System to categorize big data issues.

The next section summarizes the relevant works within a big data and the U.S. NextGen Air Transportation System context. In Sect. 3, we discuss the hypothesis: *Does the U.S. NextGen Air Transport System have unaddressed big data issues?* Section 4 examines each of the five-differentiated qualitative big data characteristics within the context of the U.S. NextGen architecture. Finally, the last section presents conclusions and identifies future U.S. NextGen system research from a big data perspective.

2 Relevant Literature

The increasing amalgamation of technology into the aviation industry is stimulating research interest into the possible risk associated with the U.S. NextGen Air Traffic

System. Interest in this area is being encouraged through the continued escalation of residual data in legal environments [13, 14] along with an absence of clarity on conducting aircraft forensics investigations [15]. Coupling this with the increasing capabilities of technology that allow a single entity/node to generate vast volumes of data quickly, U.S. NextGen Air Traffic System starts to resemble a big data problem, especially when multiple entities/nodes are considered from a real-world perspective. This is supported further when one considers the variety of research interests pertaining to NextGen, which range from *communication* data flow [16] and *encryption* [17], to *cyber-physical systems*, to the *Internet of Things (IoT)* [18], to *big data* applications [19], to *defense-in-depth* [20], and so on.

From a *communication* perspective, many researchers agree that the ADS-B system is the most important program out of the ten programs that make up the configuration of the U.S. NextGen Air Transport System [17, 21–23]. Aircraft will be required to be equipped with ADS-B systems to transmit messages to other aircraft and Air Traffic Control Centers. The unencrypted structure of the ADS-B system means the National Airspace System is susceptible to breath of cyber-physical attacks. As He, et al. [17] noted, an important objective of the ADS-B system is the security of the National Airspace System by 2020. To address both authentication and integrity issues they proposed a "three-level hierarchical identity-based signature" solutions. However, a key limitation in the scheme of He et al. [17] is the sending of identities in plaintext, which could be exploited by attackers.

The *unencrypted structure* of the ADS-B system means the national airspace system is susceptible to variety of cyber-physical attacks [11]. OpenSky is a sensor network in Central Europe, which can capture 30% of the European air traffic communications on ADS-B. The ADS-B system can augment traditional means of surveillance: radar and transponders. Radars can indicate there is something in the sky the same size as an aircraft, while a transponder will broadcast or squawk the identity of the aircraft when activated. An ADS-B message field can contain information on traffic, weather, and flight information. ADS-B vulnerabilities transgress confidentiality, integrity, and availability. First, anyone with an ADS-B radio can transmit and receive messages showing no signs of confidentiality. Data integrity is affected by attacks such as Ghost Aircraft Injection, Aircraft Disappearance, Virtual Trajectory Modification, and Aircraft Spoofing. Ghost Aircraft Injection occurs when an ADS-B radio transmits a fake message and other aircraft now believe there is an aircraft that does not really exist. Aircraft Disappearance happens when skillfully timed malformed ADS-B messages are sent with a real aircraft's identification, resulting in ADS-B messages with the particular aircraft to be disregarded. In other words, the remaining aircrafts do not believe this particular aircraft exists. Virtual Trajectory Modification is the act of jamming an aircraft or ground station to create false alarms. Aircraft Spoofing is simply using another aircraft's identification to send ADB-S message with false information. Finally, availability is loss associated with Ground Station and Ghost Aircraft Flooding. Ground Station Flooding occurs when ground-based radios are jammed. Ghost Aircraft Flooding happens when a large number of fake ADB-S messages are sent that there are too many real and fake aircrafts that nothing is distinguishable. No solutions were presented on how to address the unencrypted structure of the ADS-B system.

From an *IoT* perspective, Varga et al. [18] presented a solution for a real-time air traffic monitoring and tracking system that is based upon the ADS-B system. The solution is implemented via a software defined radio, integrating hardware and software into a high-performance wireless communication system. The software defined radio solution, however, does not allow for the use of multiple radios or the correlation of data between systems.

From a *big data* perspective, researchers are beginning to investigate architectural solutions for analyzing ADS-B records. Boci and Thistlethwaite [19] developed a Hadoop-based solution that can be used to analyze billions of ADS-B radio messages in approximately 35 min. The results of their research are visualized using density maps. However, the maps produced are very busy. It would be beneficial, from a security (or forensic) perspective, to be able to filter the messages on key words or phrases to reduce noise [24]. As the authors noted, a reduction in computational times would assist with enormous data asset as well as assisting with real time processing aspirations [19, 24].

Other researchers are beginning to look at U.S. NextGen Air Transportation systems from the perspective of *defense-in-depth* [20]. The research recommends the Flight Information Exchange Model based on experience with the Mini Global II for the advancement of the U.S. Federal Aviation Administration NextGen Air Transportation System Wide Information Management. The research is to extend the Flight Information Exchange Model beyond the 3.0 version for the benefit of the public and private organizations. The Mini Global II is part of the Federal Aviation Administration and international aviation community to unite sharing of flight, weather, and aeronautical data. The research demonstrates how the International Civil Aviation Organization Flight and Flow Information for a Collaborative environment could be leveraged to share information on a global scale to the Air Navigation Service Providers and Air Transportation Operators. The research version of the Mini Global II (e.g. Flight Information Exchange Model) includes the Weather Exchange Information Model and Aeronautical Information Exchange Model. The expanded Global Enterprise Messaging Services Support Air Navigation Service Providers' Flight Operations Centers. The simulated global environment allows for the testing of the Flight Information Exchange Model for data collection and exchange. The results indict development needs to use of the exchange model for flight objects.

While existing literature on U.S. NextGen security focuses to a large degree on communications, cyber-physical vulnerabilities, and IoT perspectives, there is minimal research investigating U.S. NextGen air transportation systems from a big data perspective.

3 Methodology

In order to investigate the U.S. NextGen system from a big data perspective, we use a case study research strategy. Specifically, this involves a documentation data generation method along with quantitative data analysis, as defined by Oates [25]. Key concepts in big data defined by Katal et al. [12] are the five characteristics, also known as the 5 v's of big data, namely: volume, variety, velocity, veracity, and value.

- Data volume measures the scale of the data within the system;
- Data variety refers to the different structures and sources of data;
- Data velocity is the analyzation of the data as the data is generated;
- Data veracity illustrates the uncertainty of the data; and
- Data value is the evaluation of the impact the data has on research.

We posit that the U.S. Next Generation Air Transport System has unaddressed big data issues; thus, we seek to obtain a better understanding of the following research challenges.

Q1: Can the combined ADS-B messages within the U.S. National Airspace system be stored with current storage technologies?

Q2: Can the combined ADS-B messages within the U.S. National Airspace system be processed with current processing technologies?

Q3: Are there too many ADS-B message formats, which creates undue complexity of the processing unit?

Q4: Are there cybersecurity issues with the ADS-B that create uncertainty about the data being transmitted?

Q5: Is the U.S. NextGen system capable of providing timely analysis in order to meet its maximum potential in enhancing public safety of air transportation?

4 Analysis and Results

The research results are described using the five considerations of big data, namely: volume, velocity, variety, veracity, and value.

4.1 Volume

The volume is calculated for the ADS-B system using the size of the message, the rate messages are sent, the amount of aviation flight hours, and a conversion factor from hours to seconds. The ADS-B systems uses fixed length 112 Bytes messages [26], and averages 6.2 messages every second from an individual aircraft. In 2015, U.S. recorded 18,103,000 general aviation flight hours [27]. Finally, there are 3,600 s in one hour. This results in 41TiB per a one year time frame, as seen in the following calculation:

$$\begin{aligned}(112\,\text{Bytes/Message}) * (6.2\,\text{Messages/Second}) * (3,600\,\text{Second/Hour}) \\ * (18,103,000\,\text{Flight Hours/Year}) = 41\,\text{TiB/Year}\end{aligned} \tag{1}$$

The combined ADS-B messages within the U.S. National Airspace system can be stored with current storage technologies. It should be noted, however, that another study [19], processed CAT033 messages that were generated from ADB-S signals received by 71 radio stations in March 2014. Compressed, this dataset size was approximately 4 TB. Given that the stations only cover a small part of the country, there does seem to be a mismatch in data generated and data stored. This could be due to the adding of additional meta-data, overlap of stations and so forth. While still in bounds with conventional storage, it does point to potential issues of assuming that the source transmittions

are indicative of archival size. It should also be noted that the data collection, to our knowledge, assumes that the data is trustworthy and accurate.

Additionally, it should be noted that simply storing data does not facilitate data analysis. Hence, while the storage of the raw information can be achieved with current technologies, it is important to ensure the data is stored in a means to facilitate analysis (the rationale behind Big Data). Marsh and Ogaard [28] noted much of the information stored in the ADS-B data they received was not relevant to their analysis. Moreover, the data they received were organized in files based upon the receiving stations; hence, to track a flight, it would be often necessary to search through multiple files. To extract the relevant data, and preprocess it to be amendable to analysis, took approximately three hours; the raw data was approximately 22 gigabytes in size. Thus, in order to facilitate timely access and retrieval of the ADS-DB data for analysis, the data will need to be stored in databases, with various fields (and combination of fields) being indexed to support anticipated types of analysis. Other precomputed operations may include the ability to search and retrieve based upon aggregation of certain data elements. This, of course, adds to the storage and other costs.

4.2 Velocity

The velocity is calculated for the ABS-D system by using the size of the message, the rate message is sent, the average amount of flights in the National Air Space at any given time. An average of 7,000 flights in the U.S. National Air Space at any given time [27] results in 404,058,960,000 messages per year, as shown in the next two equations.

$$\begin{aligned}&(6.2\ \text{Messages/Second}) * (60\ \text{Seconds/Minutes}) * (60\ \text{Minutes/Hour})\\ &* (18{,}103{,}000\ \text{Flights Hours/Year}) = (404{,}058{,}960{,}000\ \text{Messages/Year})\end{aligned} \tag{2}$$

$$\begin{aligned}&(404{,}058{,}960{,}000\ \text{Messages/Year})/\Big((365\ \text{Days/Year}) * (24\ \text{Hours/Day})\\ &* (60\ \text{Minutes/Hour}) * (60\ \text{Seconds/Minute})\Big)\\ &= (\sim 13\ \text{Messages/Millisecond})\end{aligned} \tag{3}$$

The combined ADS-B messages within the U.S. National Airspace system cannot be processed efficiently in real-time with existing standard processing technologies. A proposed ADS-B Data Lake Architecture used to process one month of messages covering the en route air traffic for Boston, New York, and Washington DC [19] took over 35 min. This dealt with approximately 17 million ADS-B messages sent at the 1090 channel; or approximately only 0.001% of the total expected volume of ADS-B messages. Assuming there is any real-time need to collect, process, compare and transmit results to other locations, this can become a true bottleneck in the process.

4.3 Variety

One means in which variety is shown within the U.S. NextGen Air Transportation is through the multitude of message type [17, 18, 29]. The message types of U.S. NextGen Air Transportation are Mode A, Mode C, Mode S, and ADS-B In and Out. Mode S, in

turn, has three message types, which are (a) Data Block Surveillance Interrogation and Reply Message Format, (b) Data Block Surveillance and Communication Interrogation and Reply-Communication-A and Communication-B Message Format, and (c) Data Block Surveillance Communication Interrogation and Reply-Extended Length Message Format. The ADS-B system inherits its message types from Mode S; hence, ADS-B has three different message types.

The Mode S Data Block Surveillance Interrogation and Reply Message Format comprises of three parts, which is displayed in Table 1. The three parts are Format Number, Surveillance and Communication Control, and Address and Parity; the format is also displayed in Table 1. The Format Number is a 5-bit message representing the sequence number of the message. The Surveillance and Communication Control is a 27-bit message, which includes commands and flight information. The Address and Parity is a 24-bit message intended to represent a unique aircraft identifier.

Table 1. Mode S data block surveillance interrogation and reply message format.

Format number	Surveillance and communication control	Address and parity
5-bits	27-bits	24-bits

The Mode S Data Block Surveillance and Communication Interrogation and Reply-Communication-A and Communication-B Message Format comprises four parts, which are shown in Table 2. The four parts of the Mode S Data Block Surveillance and Communication Interrogation and Reply-Communication-A and Communication-B Message Format are Format Number, Surveillance and Communication Control, Message Field, and Address and Parity.

Table 2. Mode S data block surveillance and communication interrogation and reply – communication–A and communication-B message format.

Format number	Surveillance and communication control	Message field	Address and parity
5-bits	27-bits	56-bits	24-bits

The Format Number is a 5-bit message representing the sequence number of the message. The Surveillance and Communication Control is a 27-bit message, which includes commands and flight information. The Message Field is a 56-bit that contains additional flight information. The Address and Parity is a 24-bit message intended to represent a unique aircraft identifier.

The Mode S Data Block Surveillance Communication Interrogation and Reply-Extended Length Message Format comprise four parts: Format Number, Communication Control, Message Field, and Address and Parity (see Table 3). The Format Number is a 2-bit message representing the sequence number of the message. The Communication Control is a 6-bit message, which includes commands. The Message Field is an 80-bit contains additional flight information. The Address and Parity is a 24-bit message intended to represent a unique aircraft identifier.

Table 3. Mode S data block surveillance communication interrogation and reply – extended length message format.

Format number	Communication on control	Message field	Address and parity
2-bits	6-bits	80-bits	24-bits

While the varying length message format is an asset where data transmission and storage is concerned, the varying length message formats creates additional complexity for processing, similar to that of the Complex Instruction Set Architecture (CISC). CISC uses varying length instruction, while Reduced Instruction Set Architecture (RISC) uses fixed length instructions. CISC saves on the storage of the instructions, but additional complexity resides within the processor to decode the varying length instructions. The fixed length instructions of the RISC processor suffer from internal fragmentation because of the unused space within the instruction format. However, the processor only processes a one size instruction, reducing the complexity on the processor. In this case, the ADS-B protocol favored optimizing storage over reducing complexity.

Aside from the variability in the messages themselves, it has been noted that the formats used to store ADS-B formats vary. As noted earlier, the study conducted by [19] used CAT033 messages that contained ADS-B data. Marsh and Ogaard [28] received ADS-B data from around the world. However, they noted the three storage formats received were "Comma-Separated Value (CVS), Extensible Markup Language (XML) and the binary format used by Garmin GDL 90 ADS-B transceiver". Hence, the Automatic Dependent Surveillance system can be viewed as having multiple tiers of variety.

4.4 Veracity

The veracity is depicted by the known and peer-reviewed security vulnerabilities within the ADS-B protocol. The vulnerabilities to the ADS-B system include ground station flooding, ghost aircraft injection or flooding, aircraft disappearance, virtual trajectory modification or false alarm attack, and aircraft spoofing [11, 30]. Ground station flooding is the jamming of the 1090 MHz frequency. The exploitation of the ground station flooding vulnerability has a low level of difficulty. The attacker is required to have a signal power greater than the legitimate communications to the Area Control Center. The exploitation would require the Area Control Center to use a legacy system incapable of handling high density airspaces. Ghost aircraft injection or flooding is the insertion of an ADS-B message spoofing an existing aircraft. The scaling of ghost aircraft injection into many ghost aircraft injections is called ghost aircraft flooding. The injected messages are indistinguishable from the legitimate communications. The ghost aircraft flooding causes a denial of service. Aircraft disappearance is caused by the deletion of all ADS-B messages sent from a legitimate aircraft. Virtual trajectory modification or false alarm attack is achieved by combining an illegitimate message with illegitimate modified trajectory date with the legitimate and valid 24-bit International Civil Aviation Organization identifier. Aircraft spoofing is accomplished by combining the illegitimate message with the valid 24-bit International Civil Aviation Organization identifier of the legitimate aircraft being spoofed.

Hence, it is safe to conclude that there are cybersecurity issues with the ADS-B system such as the lack of integrity demonstrated by the vulnerabilities to the ADS-B. This creates uncertainty about the data being transmitted, which in turn, indicates that veracity is an issue. It should also be noted, in this case, that the volume of the data and velocity of data, as well as the distributed nature of the collection and storage, exasperate the problem of verifying the data veracity. Attempts to mitigate the veracity concerns include two mitigation solutions: intrusion detection [9, 31] and cryptographic solution implementation [32–34]. However, the problem is still not definitively solved.

4.5 Value

The value is shown through the lens of public safety. U.S. NextGen Air Transportation aims to improve safety, increase efficiency and capacity. Aviation Safety Information Analysis and Sharing creates an aggregate of data from industry and government. One use of the aggregate data is to detect safety tendencies. Aviation Safety Information Analysis and Sharing is used by incident responders to replay the events leading to an incident. The data points are derived from surface monitoring systems. System Safety Management and Transformation allows for visualization of safety trends and further analysis is used for forecasting. The System Wide Information Management system creates an interconnection between otherwise unshared information, which could enhance public safety of air transportation.

A key issue in value is the timeliness of the analysis. Hence, for the air traffic controller, determining that a contact is a matter of Ghost Aircraft Injection requires a system that can analyze, within seconds, the array of historical and current, to determine the likelihood of the contact actually being true. In the case of determining if a Ghost Aircraft Injection occurred as a postmortem of a security alert, the value of the analysis does not decrease if it take a few minutes. Thus, the question if the Next Generation Air Transportation has a value problem, in terms of big data, becomes a rather complex determination of what questions need to be answered, when they need to be answered and by whom needs the data. Given this complexity, at present, the question is not resolvable at this time.

Not all Big Data considerations were addressed by the U.S. NextGen Air Transportation System, as shown in Table 4.

Table 4. Results from the characteristics of big data.

Characteristics of big data	Results
Volume	(41 TiB/Year)
Velocity	(~13 Message/ms)
Variety	Mode A, Mode C, and Mode S
Veracity	No encryption
Value	Public safety

While the 41 TiB per year volume is manageable, the results only address existing ADS-B systems. One would expect more volume from a voice system, which will be

provided by the U.S. NextGen Air Transportation System Data Communication. Unlike Twitter, the Federal Aviation Agency would have to address and processes voice communication. There is variety within variety for the U.S. NextGen Air Transportation System.

5 Conclusions and Future Work

In this paper, we explained the unaddressed big data issues in the U.S. NextGen Air Transport System. For example, We pointed out that the System Wide Information Management does not address the veracity of the data received via the ADS-B protocol, which is untrustworthy due to the lack of encryption for both confidentiality and integrity. Potential mitigation solutions include intrusion detection and Public Key Infrastructure implementation. The goal of the research, to identify Big Data issues with the U.S. NextGen Air Transport System, was achieved by identifying issues with the velocity, variety, and veracity of the U.S. NextGen Air Transport System.

Future work will investigate the creation of a U.S. NextGen Air Transportation System command and control model to address the outlined big data issues, namely: velocity, variety, and veracity. In order to add in command and control models, each of the remaining five parts of the U.S. NextGen system, plus the overall system, will be analyzed from the Big Data perspective. The research will need to identify combinations that pose unique challenges and problems from the 5 V perspective. In addition, the applicability of these newly created command and control models will need to be examined for automobile and drone environments. As the U.S. Department of Transportation progresses in its effort to automate automobiles, many of the lessons learned within the U.S. NextGen Air Transportation System may be applicable to ground transportation infrastructures. Future research will also examine the viability of adopting these command and control models to Unmanned Arial Vehicles (UAV) environments.

Another potential research agenda is to integrate forensic requirements and techniques into the design of the U.S. NextGen Air Transportation System. Such an approach, coined forensic-by-design [35], can facilitate the identification, collection and analysis of data during forensic investigations on a cybersecurity incident [36, 37].

References

1. U.S. Department of Transportation: Fact Sheet - FAA Forecast Fact Sheet-Fiscal Years 2016–2036, 2017 (2016)
2. Gillen, D., Morrison, W.G.: Aviation security: costing, pricing, finance and performance. J. Air Transp. Manage. **48**, 1–12 (2015)
3. Committee on Appropriations: FY2017 Homeland Security Appropriations Bill Cleared for Committee Debate, 2017 (2016)
4. Kaspersen, A.: Four threats to aviation security – and four responses, 2017 (2016)
5. BBC News: Brussels explosions: what we know about airport and metro attacks, 2017 (2016)
6. BBC News: MH17 Ukraine plane crash: what we know, 2017 (2016)
7. AirlineReporter: Updated: Malaysia Airlines Flight 370 Has Likely Crashed But Where? 2017 (2014)

8. United States Government Accountability Office: FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen, 2017 (2015)
9. Strohmeier, M., Martinovic, I.: On passive data link layer fingerprinting of aircraft transponders. In: Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy, pp. 1–9. ACM, Denver (2015)
10. Costin, A.: Ghost is in the air (traffic): on insecurity of ADS-B protocol and practical attacks on ADS-B devices. Black Hat USA (2012)
11. Strohmeier, M., Schafer, M., Lenders, V., Martinovic, I.: Realities and challenges of nextgen air traffic management: the case of ADS-B. IEEE Commun. Mag. **52**, 111–118 (2014)
12. Katal, A., Wazid, M., Goudar, R.H.: Big data: issues, challenges, tools and good practices. In: 2013 Sixth International Conference on Contemporary Computing (IC3), pp. 404–409 (2013)
13. Berman, K., Glisson, W.B., Glisson, L.M.: Investigating the impact of global positioning system (GPS) evidence in court cases. In: Hawaii International Conference on System Sciences (HICSS-48). IEEE, Kauai (2015)
14. McMillan, J., Glisson, W.B., Bromby, M.: Investigating the increase in mobile phone evidence in criminal activities. In: Hawaii International Conference on System Sciences (HICSS-46). IEEE, Wailea (2013)
15. Mink, D., Yasinsac, A., Choo, K.-K.R., Glisson, W.B.: Next generation aircraft architecture and digital forensic. In: Americas Conference on Information Systems (AMCIS). Americas Conference on Information Systems, San Diego (2016)
16. Moallemi, M., Castro-Peña, C.A., Towhidnejad, M., Abraham, B.: Information security in the aircraft access to system wide information management infrastructure. In: 2016 Integrated Communications Navigation and Surveillance (ICNS), pp. 1A3-1–1A3-7 (2016)
17. He, D., Kumar, N., Choo, K.K.R., Wu, W.: Efficient hierarchical identity-based signature with batch verification for automatic dependent surveillance-broadcast system. IEEE Trans. Inf. Forens. Secur. **12**, 454–464 (2017)
18. Varga, M., Polgár, Z.A., Hedeşiu, H.: ADS-B based real-time air traffic monitoring system. In: 2015 38th International Conference on Telecommunications and Signal Processing (TSP), pp. 215–219 (2015)
19. Boci, E., Thistlethwaite, S.: A novel big data architecture in support of ADS-B data analytic. In: 2015 Integrated Communication, Navigation and Surveillance Conference (ICNS), pp. C1-1–C1-8 (2015)
20. Li, W., Kamal, P.: Integrated aviation security for defense-in-depth of next generation air transportation system. In: 2011 IEEE International Conference on Technologies for Homeland Security (HST), pp. 136–142 (2011)
21. Samuelson, K., Valovage, E., Hall, D.: Enhanced ADS-B research. In: IEEE Aerospace Conference, pp. 1–7 (2006)
22. Robinson, R.V., Sampigethaya, K., Li, M., Lintelman, S., Poovendran, R., Oheimb, D.V.: Secure network-enabled commercial airplane operations: it support infrastructure challenges. In: First CEAS European Air Space Conference, pp. 1–10 (2007)
23. Kacem, T., Wijesekera, D., Costa, P.: Integrity and authenticity of ADS-B broadcasts. In: IEEE Aerospace Conference, pp. 1–8 (2015)
24. Tassone, C.F.R., Martini, B., Choo, K.-K.R.: Visualizing digital forensic datasets: a proof of concept. J. Forensic Sci. **62**, 1197–1204 (2017)
25. Oates, B.J.: Researching Information Systems and Computing (2006)
26. Dong, X.L., Srivastava, D.: Big data integration. In: IEEE 29th International Conference on Data Engineering (ICDE), pp. 1245–1248 (2013)

27. U.S. Department of Transportation's Bureau of Transportation Statistics: Transportation Statistics Annual Report 2016 (2016)
28. Marsh, R., Ogaard, K.: Mining heterogeneous ADS-B data sets for probabilistic models of pilot behavior. In: IEEE International Conference on Data Mining Workshops, pp. 606–612 (2010)
29. Finke, C., Butts, J., Mills, R.: ADS-B encryption: confidentiality in the friendly skies. In: Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop, pp. 1–4. ACM, Oak Ridge (2013)
30. Chen, T.-C.: An authenticated encrption scheme for automatic dependent surveillance-broadcast. IEEE Commun. Mag. (2012)
31. Baek, J., Young-jj, B., Hableel, E., Al-Qutavri, M.: Making air traffic surveillance more reliable: a new authentication framework for automatic dependent sureillance-broadcast (ADS-B) based on online/offline identity-based signature. Secur. Commun. Netw. **8**, 740–750 (2015)
32. Lauf, A.P., Peters, R.A., Robinson, W.H.: A distributed intrusion detection system for resource-constrained devices in ad-hoc networks. Ad Hoc Netw. **8**, 253–266 (2010)
33. Mitchell, R., Chen, I.-R.: A survey of intrusion detection techniques for cyber-physical systems. ACM Comput. Surv. (CSUR) **46**, 55 (2014)
34. Wesson, K.D., Humphreys, T.E., Evans, B.L.: Can cryptography secure next generation air traffic surveillance. IEEE Secur. Priv. Mag. (2014)