Vulnerabilities and Mitigation Methods in the NextGen Air Traffic Control System

Sachiko Sueki and Yoohwan Kim

Abstract The air traffic control (ATC) systems have been modernizing and standardizing the automation platforms in recent years in order to control increased number of flights. In 2004, FAA started transforming the nation's ground-based ATC system to a system which uses satellite-based navigation and other advanced technology, called NextGen. The NextGen system deploys Internet Protocol based network to communicate and heavily relies on computerized information system and digital data, which may introduce new vulnerabilities for exploitations. Many vulnerabilities of NextGen stem from the increased interconnection of systems through wireless networks. For instance, a critical part of the NextGen, Automatic Dependent Surveillance – Broadcast, which transfers essential information via wireless network without encryption, is an easy target for attackers. There have been some deployments of security measures but still lack in critical system. In this study, we present the potential vulnerabilities of the NextGen ATC systems and their possible solutions.

Keywords ATC · Automatic dependent surveillance – broadcast · Data communications · System wide information management · En route automation modernization and replacement · Terminal automation modernization and replacement

1 Introduction

In 2013, Presidential Policy Directive 21 identified 16 critical infrastructure sectors which provide essential services that are vital to the nation's safety, prosperity, and well-being. One of the sectors is transportation systems, which includes aviation such as aircrafts, air traffic control (ATC) systems, airports, and landing strips. Cyber systems including ATC, tracking, and communication systems provide a fundamental capability in keeping the nation's transportation system safe and operational [1].

S. Sueki(✉) · Y. Kim
Department of Computer Science, University of Nevada, Las Vegas, NV, USA
e-mail: suekis@unlv.nevada.edu, Yoohwan.Kim@unlv.edu

S. Latifi (ed.), *Information Technology New Generations*,
Advances in Intelligent Systems and Computing 448,
DOI: 10.1007/978-3-319-32467-8_19

The ATC systems have been modernizing and standardizing the automation platforms in recent years. Comprehensive ATC under the direction of the Federal Government started in 1936 in the United States [2]. The ATC system evolved as the number of flights increased. At present the so-called legacy system is managed based on a combination of radar and computer technology. Some of the technologies used in the legacy system were developed as far back as the 1940s [3]. The system is not capable of navigating in oceanic airspace and remote land regions because of its ground-based operations. In general, aircrafts operating in these regions follow inefficient procedural separation methods. These inefficient control systems are causing flight delays.

According to FAA long-range forecasts, aircraft operations are going to increase to approximately 81 million and 96 million in 2020 and 2030, respectively [4]. In order to control increased number of flights, in 2004, FAA started transforming the nation's ground-based ATC system to a system which uses satellite-based navigation and other advanced technology, called NextGen [5]. The improvements from the legacy system to the NextGen [6] are listed in Table 1. The NextGen system deploys Internet Protocol (IP)-based network to communicate and heavily relies on computerized information system and digital data, which may not be adequately secure and thus vulnerable to exploitations. The facilities, aircrafts and pilots communicate using point-to-point communication lines in the legacy system while in the NextGen they happen through system-wide interconnectivity. Furthermore, modern aircrafts increasingly rely on Internet for many purposes. Such interconnectivity in their information systems presents elevated cyber-attack opportunities.

There have been reported cyber-attack incidents in the ATC systems. For instance, in 2006, Federal Aviation Administration (FAA) ATC system was infected by a virus forcing it to shut down a portion of the ATC systems in Alaska. In 2008, an attacker took over the critical FAA network servers and gained an access to shut down the servers [7]. Earlier in 2015, FAA network was attacked with malicious software [8]. According to the report [7], more than 800 cyber incident alerts were issued to the Air Traffic Organization responsible for ATC operations during the Fiscal Year 2008. As the NextGen ATC systems replace the legacy systems, opportunities for cyber attackers can further increase. Even though FAA has taken steps to protect the systems from cyber-based threats, significant security control weaknesses still exist [5]. Therefore, it is crucial to understand and mitigate the vulnerabilities that exist in the ATC systems and its counter measures taken such as use of encryption and authentication technologies.

In this study, a literature review, surveys and analyses are being conducted to identify vulnerabilities that exist in the NextGen ATC systems and we suggest possible mitigation measures. First, a brief explanation of the NextGen air traffic control systems is given in section 2. Then, vulnerabilities and their possible solutions are discussed in sections 3 and 4, respectively. Finally, some promising mitigation methods are discussed in section 5.

Table 1 Improvements from the legacy system to the NextGen

Legacy System		NextGen
Voice Communication	→	Digital Communication
Ground-Based Navigation	→	Performance-Based Navigation
Radar Surveillance	→	Satellite-Based Surveillance
Constrained Automation	→	Flexible Automation, Decision-Support Tools
Disparate Point-to-Point System	→	Integrated System and Information Distribution

2 NextGen Air Traffic Control Systems

The NextGen ATC systems consist of six major programs, which are primarily FAA internal system upgrades that are necessary to deploy additional capabilities. The six programs are Automatic Dependent Surveillance – Broadcast (ADS-B), Data Communications (Data Comm), En Route Automation Modernization (ERAM), Terminal Automation Modernization and Replacement (TAMR) National Airspace System (NAS) Voice Switch (NVS), and System Wide Information Management (SWIM) [9].

ADS-B uses a Global Navigation Satellite System to determine aircraft's own position and broadcasts its position, speed and altitude to ground stations or other aircrafts in the vicinity over a radio frequency. On board GPS receiver gives aircraft's own position and velocity. Then, the transmitting subsystem, ADS-B Out, periodically broadcasts its information via a message. The ATC stations on the ground and nearby aircrafts equipped with the receiving subsystem, ADS-B In, can receive these messages. The ADS-B functions most likely are integrated into currently used 1090ES data link, which predominantly uses the 1090 MHz frequency for communications and data is transmitted by blocks utilizing pulse position modulation (PPM). ADS-B is the central component in the NextGen and ADS-B Out must be equipped in aircrafts by January 1, 2020 [9].

Data Comm communicates with digitally-delivered messages between ATC and pilots replacing radio voice communications. Routine instructions such as departure clearances and weather-avoiding reroutes are directly sent to the flight deck, reducing potential miscommunications. The initial en route services are expected in 2019 and full operational capability at air route traffic control centers in 2021 [9].

ERAM is a scalable system combining flight plan information with information from surveillance sources such as ADS-B data to automate many air traffic control functions and support controller decisions. ERAM serves as the platform of data sharing, digital communications and trajectory-based operation. The system will be used in air traffic controllers at the air route traffic control centers. Full deployment of ERAM is planned to be completed by 2015 [9]. Other air traffic facilities and government agencies such as airport towers, FAA command center, automated flight service stations, Department of Homeland Security, Department of Defense, and U.S. Customs and Border Protection, are now connected to the centers via ERAM.

The TAMR program converts the automation platforms for near airports and high altitude to a single automation platform called Standard Terminal Automation Replacement System (STARS). The system meets operational requirements for ADS-B and improves flight plan processing with a 4-D trajectory (lateral, vertical, horizontal and time). Full deployment of TAMR is planned for 2020 [9].

NVS uses router-based communications linked through the FAA Telecommunications Infrastructure network. NVS provides a capability of sharing communication resources unlike the current voice switches operated independently at individual facilities. The capability of NVS is still in development and NVS is currently on schedule to start operational test in Seattle in the fiscal year 2019 [9].

SWIM is the base for data-sharing and currently distributes weather and flight planning information to the NAS users through a single point of access. The SWIM program is to implement a set of information technology principles in the NAS and provides users with relevant and commonly understandable information. Raw surface data from airport towers are converted to accessible information via SWIM Terminal Data Distribution System (STDDS). The information is, then, available from Terminal Radar Approach Control (TRACON) to airlines and airports through SWIM messaging services. The SWIM Flight Data Publication Service (SFDPS) will improve flight data sharing using standard Flight Information Exchange Model with a Globally Unique Flight Identifier. SFDPS is currently available only in the SWIM research and development domain [9].

As NVS is still in the development phase, not much information is available, therefore NVS is excluded from the study. On the other hand, ADS-B is a critical part of the NextGen, which transfers essential information via wireless network. Therefore, there have been several studies in its vulnerabilities and mitigations as reported in [10]-[19]. The majority of vulnerabilities and solutions reported here is related to ADS-B.

3 Vulnerabilities

ADS-B has been developed without security in mind and its signals are public over a known frequency. Furthermore, transmissions are not encrypted or authenticated. Therefore, ADS-B is subject to various types of attacks. The attacks include eavesdropping, jamming, message injection, message deletion and message modification [11]. Eavesdropping is highly possible since the complexity of an attack is low and ADS-B sends unencrypted messages over a broadcast medium. Furthermore, as pointed out by [12], there are services to aid eavesdropping such as commercially available ADS-B receivers [20], digitized live ADS-B data available to public via the Internet [21], and open-source GNU radio module available for sophisticated traffic analysis [22]. Jamming is another simple attack that can cause denial-of-service (DOS) problems [13]. Jamming is a common problem to all wireless communication. However, the impact is severe because of importance and criticality of the transmitted data. Since ADS-B does not have any authentication measures, an attack with cheap and simple technological means can be used

to inject non-legitimate message into the communication system. Message injection can display ghost aircrafts on a cockpit display forcing the pilots to change their course and/or velocity. Injecting multiple messages can cause ghost aircrafts flooding which can lead to DOS of the controller's surveillance system [12]. Message deletion can be achieved by transmitting the inverse of the signal broadcast by a legitimate sender [11] or by causing large enough number of bit errors for the receiver to recognize a message as corrupted. Message deletion can cause aircraft disappearance. Message modification can be typically done by overshadowing or bit-flipping during transmission. Overshadowing is to replace part of the message by sending a high-powered signal. Bit-flipping is the signal converting by flipping bits from 1 to 0 or the other way around by superimposing the signal. By combining aforementioned attacks, attackers can achieve trajectory modification, indication of false alarms such as hijacking, and aircraft spoofing [14].

Data Comm allows controllers to electronically send instructions to the cockpit display with a push of a button. Instructions are sent via data link without any authentication, which can be susceptible to possible cyber-attacks [23]. The information is supposed to be seen by controllers and applicable pilots. However, hobbyists who have appropriate radio equipment can monitor and decode transferred information, making this vulnerable to cyber-attacks similar to the ADS-B messages.

The major vulnerability of SWIM is attributed from net-centric exchanges, which potentially increases the chance of the system to be compromised and damaged. Damage can potentially spread to other systems on the network when one of the systems connected to an IP network is compromised. Furthermore, SWIM is vulnerable to a man-in-the-middle attack since it does not provide any end-to-end confirmation that messages are sent or received on the network [24]. The other concern is the use of various software. Since SWIM does not include control information and safety-critical information such as surveillance data, any relatively inexpensive commercial software or internally developed software, and open source software can be used. Such software may have a list of widely known vulnerabilities that can increase opportunities for unauthorized access and malicious-code execution.

ERAM and TAMR are used for analyzing data within the centers. However, they also communicate with other facilities in order to obtain data or transfer information. Vulnerabilities of the programs are associated with the interconnectivity of systems, which can lead to an unauthorized access or a malicious code attack to the ATC system.

Finally, NextGen's potential vulnerability arises from the IP network connectivity. Approximately 36 percent of the ATC system in the NAS is connected to IP network and the connections are projected to grow to 50 to 60 percent by 2020 [5]. The legacy system's point-to-point connections, which co-exist with the NextGen system, can be also compromised because of increased connectivity with IP network.

4 Mitigation Methods

Most of the security mitigation is focused on ADS-B because of its importance in the NextGen System and an existence of several potential vulnerabilities. In order to secure ADS-B, there are two distinct approaches, secure broadcast authentication and secure location verification [15]. Secure broadcast authentication is to secure the communications and can be used to prevent and/or detect attacks in a unidirectional broadcast network. Node-based authentication (the authenticity of the hardware) includes non-cryptographic schemes on the physical layer and cryptography. Secure location verification authenticates the claimed location using data from the senders and other ADS-B participants. The techniques include multilateration, group verification, distance bounding, Kalman filtering, data fusion, and traffic modeling.

Non-cryptographic schemes such as fingerprinting are to identify suspicious activity in a network. Fingerprinting is to identify what they are based on the unique characteristics of devices such as operating system, drivers, clocks, and radio circuit [25]. ADS-B currently does not utilize the schemes to secure the system. However, there are three possible techniques that may be employed in ADS-B. The techniques are software-based fingerprinting, hardware-based fingerprinting, and channel/location-based fingerprinting [26]. Software-based fingerprinting uses distinctly different patterns or behavior of software operating on wireless equipment. Hardware-based fingerprinting is to identify devices based on unique hardware differences such as differences in turn-on/off transient, modulation of a radio signal, and clock skew. Another recent technique is physically unclonable functions (PUF) [27], which uses specifically implemented circuits to create unique and secure signatures. Channel/location-based fingerprinting is based on received signal strength, channel impulse response, or the carrier phase. Randomize/uncoordinated frequency hopping/spreading is one type of non-cryptographic schemes, which is different from fingerprinting. Such schemes use Uncoordinated Frequency Hopping, Uncoordinated Direct-Sequence Spread Spectrum or Randomized Differential Direct-Sequence Spread Spectrum [28]. By regularly changing communication frequencies of a sender and a receiver, they wait for a chance to be at the same communication channel.

Cryptography is one of the common methods to secure communication in wireless networks, which requires distribution of encryption keys to vast participants of ADS-B systems [15]. One of the proposed methods in [16] is the use of public key cryptography with challenge/response format. Retroactive key publication is a variation of public key cryptography, which sends a partial public key with every message [29]. The receivers who buffer all the messages can decrypt them using the collected public key. On the other hand, a recent study by [17] suggested the use of Staged Identity-Based Encryption, which uses receiving parties' identities as public keys for encryption.

Multilateration technique can geometrically calculate an unknown location from a precise distance between four or more known locations [18]. Currently a preferred method for location verification is multilateration by utilizing the time difference of arrival. Time difference of arrival can be obtained from several antennas in different locations that receive the same signal at different times. The other way of utilizing multilateration is group verification. Group verification is to verify the location claimed by a non-group aircraft in-flight using multilateration done by a group of aircrafts [15].

Distance bounding is to find the upper bound of locations by sending a challenge to the receiver and getting a response [15]. The upper bound is calculated based on the fact that electromagnetic waves do not travel faster than the speed of light. The actual location can be found via a difference in distance between the measurements from the various ground stations.

Kalman filtering is already used to filter and smoothen GPS position data in messages in ADS-B [19]. In every time step, the measured variables and the error covariance are projected. It then updates the estimations and error covariance with the actual measurements. The filtering is an important tool for sorting out noisy signals and smoothing over missing data for multilateration approach. The filter was also suggested to use in one of the distance bounding protocols.

Data fusion is to verify the data obtained within the system by comparing it with the data coming from other independent sources, e.g., the fusion of ADS-B and radar [19].

Traffic modeling can be created from historical data and machine learning methods to detect deviations from normal ADS-B behavior [15]. The technique can be also applied to establish red flags for intrusion detection system so that the technically and physically impossible data are reasonably dropped to reduce the strain on the ADS-B system and prevent spoofing and DOS attacks.

Similar to the ADS-B message protections, messages sent using Data Comm can be secured using cryptography such as Elliptical Curve Cryptography Asymmetric Public-Key Infrastructure. One such application suggested by [23] was the Protected Aircraft Communications Addressing and Reporting System (PACARS), which provides end-to-end message protection and/or authentication. PACARS uses Elliptical Curve Cryptography Asymmetric Public-Key Infrastructure.

SWIM provides a comprehensive set of technical security controls via its infrastructure and the Common Data Transport (CDT) security services implemented in the FAA telecommunications infrastructure [30]. The CDT provides firewalls that can defend unauthorized access, IP address spoofing, traffic rerouting, session hijacking, and some forms of DOS attacks. The CDT security also includes link and network layer cryptographic security providing authentication, integrity and confidentiality. The SWIM security provides identity and access management, which includes authentication, authorization and auditing. Authentication may be provided by Kerberos or Public Key Infrastructure. Kerberos is a network authentication protocol based on the shared-secret cryptography [31]. From a functional perspective, SWIM and CDT share an intrusion detection system, security information management and a public key infrastructure certificate authority to monitor events, keep event logs, and provide digital certificates.

In order to guard the overall IP-networked systems, an enterprise approach is being developed, which views IP-networked systems as subsystems within the large enterprise-wide system [5]. The subsystems can interoperate while enterprise-wide set of shared cybersecurity controls such as continuous monitoring, incident detection and response, internal policy enforcement, and identity and key management are available. However, in order to fully utilize an enterprise approach, a holistic threat model can be a valuable tool. A holistic threat model might provide a likely compromise and dangers associated with potential consequences [5].

The NextGen ATC systems' vulnerabilities and their solutions are listed in Table 2.

5 Advantages and Disadvantages of Methods

Mitigation methods must be adaptable to large-scale deployment in order to be implemented in the ATC systems. Furthermore, for practical purpose, the cost and the complexity of deployment need to be considered. Therefore, adding new hardware or modifying the existing systems is hard to implement. For instance, ADS-B is a unidirectional broadcast while many of the proposed methods such as PUF, channel/location-based fingerprinting, and distance bounding require bidirectional communication. Hardware-based fingerprinting with clock skew and data fusion require additional data while PUF and Randomize/uncoordinated frequency hopping/spreading require additional hardware.

Table 2 The NextGen ATC System's Vulnerabilities and Their Solutions

NextGen Program	Vulnerabilities	Mitigation Methods
ADS-B	Eavesdropping	Randomize/uncoordinated frequency hopping/spreading, Public key infrastructure
	Jamming	Randomize/uncoordinated frequency hopping/spreading
	Message Injection	Fingerprinting, Public key infrastructure, Multilateration, Distance bounding, Kalman filtering, Traffic modeling Group verification, Data fusion
	Message deletion	Randomize/uncoordinated frequency hopping/spreading
	Message modification	Fingerprinting, Randomize/uncoordinated frequency hopping/spreading, Public key infrastructure, Multilateration, Distance bounding, Kalman filtering, Traffic modeling Group verification, Data fusion
Data Comm	Cyberattack, Eavesdropping	PACARS (Elliptical Curve Cryptography Asymmetric Public key infrastructure)
SWIM	Network compromise (unauthorized access, spoofing, DOS, etc)	Common data transport security service, Public key infrastructure, Kerberos
	Man-in-middle attack	Public key infrastructure, Kerberos
	Commercial, internal, open source software	Timely installation of patches
Others	IP-networked system	Enterprise wide system, Holistic threat model

Multilateration and Kalman filtering appear to be promising methods to incorporate in ADS-B. Multilateration is currently in use in comparatively short distances while this technique still cannot fully utilize ADS-B because of decreased accuracy over long distances. Kalman filtering is already being used in ADS-B related systems but it is slightly difficult in positional claim verification of aircraft-to-aircraft systems. However it is feasible and highly scalable. For secure communications, one of the promising methods is retroactive key publication even though this technique can be susceptible to a memory-based DOS attack and requires a slight modification of data. A successful implementation of these three methods can provide protections from message injection and modification attacks. In order to address all possible vulnerabilities in ADS-B, new protocols or methods may be required.

Some security measures are already in place in SWIM but not in rest of the systems. Although those systems are not as crucial as ADS-B, it is important to mitigate their vulnerabilities. Therefore, further studies are needed.

6 Summary and Conclusions

The NextGen ATC systems' vulnerabilities come mainly from the increased interconnection of systems through wireless network. There have been some deployments of security measures such as in SWIM but not in other critical systems such as ADS-B. Even though there are many security measures proposed, their practical use is still questionable because of its broadcast nature and wide operational range. One solution cannot protect variety of attacks. Therefore, the system must be protected with a defense-in-depth and an enterprise approach.

References

1. Homeland Security: Transportation systems sector-specific plan, an annex to the national infrastructre protection plan (2010). http://www.dhs.gov/transportation-systems-sector (accessed September 15, 2015)
2. Federal Aviation Administration: FAA historical chronology, 1926–1996 (2011). https://www.faa.gov/about/history/chronolog_history/ (accessed October 3, 2015)
3. Federal Aviation Administration: Navigation programs – history (2015). https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/history/ (accessed October 3, 2015)
4. Federal Aviation Administration: FAA long-range aerospace forecasts, fiscal years 2020, 2025 and 2030 (2007). http://www.faa.gov/data_research/aviation/long-range_forecasts/media/long07.pdf (accessed October 3, 2015)
5. United States Government Accountability Office: Air Trafic Contorl, FAA needs a more comprehensive approach to address cybersecurity as agency transition to NextGen, Report to Congressional Requesters, GAO-15-370 (2015)
6. Bradford, S.: NextGen progress and ICAO. In: Integrated Communications, Navigation and Surveillance Conference (ICNS 2014), pp. 1–22, April 8–10, 2014

7. Office of Inspector General: Review of web applications security and intrusion detection in air traffic control systems, 2009. Audit Report, Report ID: FI-2009-049, p. 23 (2009)
8. Sternstein, A.: Exclusive: FAA computer systems hit by cyberattack earlier this year. In: Nextgov (2015). http://www.nextgov.com/cybersecurity/2015/04/faa-computer-systems-hit-cyberattack-earlier-year/109384/ (accessed October 3, 2015)
9. Federal Aviation Administration: NextGen implementation plane (2015). https://www.faa.gov/nextgen/media/NextGen_Implementation_Plan-2015.pdf (accessed October 3, 2015)
10. Danev, B., Zenetti, D., Capkun, S.: On physical-layer identification of wireless devices. ACM Computer Surveys **45**(1), 1–29 (2012)
11. Strohmeier, M., Lenders V., Martinovic, I.: Security of ADS-B: state of the art and beyond. arXiv preprint arXiv:1307.3664 (2013)
12. Schäfer, M., Lenders, V., Martinovic, I. (eds.): Experimental analysis of attacks on next generation air traffic communication. In: 11th International Conference on Applied Cryptography and Network Security. Lecture Note in Computer Sciences, pp. 253–271 (2013)
13. McCallie, D., Butts, J., Mill, R.: Security analysis of the ADS-B implementation in the next generation air transportation system. International Journal of Critical Infrastructure Protection **4**(2), 78–87 (2011)
14. Amin, S., Clark, T., Offutt, R., Serenko, K.: Design of a cyber security framework for ADS-B based surveillance systems. In: Systems and Information Engineering Design Symposium (SIEDS 2014), pp. 304–309, April 25, 2014
15. Strohmeier, M., Lenders, V., Martinovic, I.: On the security of the automatic dependent surveillance-broadcast protocol. IEEE Communications Surveys & Tutorials **17**(2), 1066–1087 (2015). Secondquarter 2015
16. Viggiano, M., Valovage, E., Samuelson, K., Hall, D.: Secure ADS-B authentication system and method, U.S. Patent 7730307 B2, June 1, 2010
17. Hableel, E., Baek, J., Byon, Y., Wong, D.S.: How to protect ADS-B: confidentiality framework for future air traffic communication. In: IEEE Conference of on Computer Communications Workshops (INFOCOM WKSHPS), April 26–May 1, 2015, pp. 155–160 (2015)
18. Nijsure, Y., Kaddoum, G., Gagnon, G., Gagnon, F., Yuen C., Mahapatra, R.: Adaptive air-to-ground secure communication system based on ADS-B and wide area multilateration. IEEE Transactions on Vehicular Technology **99**, 1. doi:10.1109/TVT.2015.2438171
19. da Silva, J.L.R., Brancalion, J.F.B., Fernandes, D.: Data fusion techniques applied to scenarios including ADS-B and radar sensors for air traffic control. In: 12th International Conference on Information Fusion, Fusion 2009, pp. 1481–1488, July 6–9, 2009
20. iPad Pilot News: Which ADS-B reciever should I buy? (2015). http://ipadpilotnews.com/2015/10/ads-b-receiver-buy-2/ (accessed November 10, 2015)
21. Flightrader24: Live Air Traffic. Available from http://www.flightradar24.com/
22. Sharan, R., West, N.: The comprehensive GNU radio archieve network. http://www.cgran.org/ (accessed November 10, 2015)
23. Storck, P.E.: Benefits of commercial data link security. In: Integrated Communications, Navigation and Surveillance Conference (ICNS 2013), pp. 1–6, April 22–25, 2013

24. Jaatun, M.G., Faegri, T.E.: Sink or SWIM: information security requirements in the sky. In: Eighth International Conference on Availability, Reliability and Security (ARES 2013), pp. 794–801, September 2–6, 2013
25. National Air Traffic Controllers Association: NextGen now. Quaterly E-Publication **1**(4) (2015). http://www.natca.org/safety.aspx?zone=Safety%20and%20Technology&pID=4586 (accessed October 25, 2015)
26. Zensg, K., Govindan, K., Mohapatra, P.: Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]. IEEE Wireless Communications **17**(5), 56–62 (2010)
27. Devadas, S., Suh, E., Paral, S., Sowell, R., Ziola, T., Khandelwal, V.: Design and Implementation of PUF-Based "Unclonable" RFID ICs for anti-counterfeiting and security applications. In: 2008 IEEE International Conference on RFID, pp. 58–64, April 16–17, 2008
28. Chengzhi, L., Huaiyu, D., Liang, X., Peng, N.: Analysis and optimization on jamming-resistant collaborative broadcast in large-scale networks. In: 2010 Conference Record of the Forty Fourth Asilomar Conference on Signals, Systems and Computers (ASILOMAR), pp. 1859–1863, November 7–10, 2010
29. Kwon, T., Hong, J.: Secure and efficient broadcast authentication in wireless sensor networks. IEEE Transactions Computer **59**(8), 1120–1133 (2010)
30. Stephens, B.: Security architecture for system wide information management. In: The 24th DASC 2005 Digital Avionics Systems Conference, vol. 2, p. 10, October 30–November 3, 2005
31. Neuman, C., Yu, T., Hartman, S., Raeburn, K.: The Kerberos network authentication service (V5), RFC4120 (July 2005)