POSTER: Localization of Spoofing Devices using a Large-scale Air Traffic Surveillance System

Kai Jansen
Ruhr-University Bochum
kai.jansen-u16@rub.de

Matthias Schäfer
University of Kaiserslautern
schaefer@cs.uni-kl.de

Vincent Lenders
armasuisse
vincent.lenders
@armasuisse.ch

Christina Pöpper
New York University
Abu Dhabi
christina.poepper@nyu.edu

Jens Schmitt
University of Kaiserslautern
jschmitt@cs.uni-kl.de

ABSTRACT

Systems relying on satellite positioning techniques such as GPS can be targeted by spoofing attacks, where attackers try to inject fake positioning information. With the growing spread of flying drones and their usage of GPS for localization, these systems become interesting targets of attacks with the purpose of hijacking or to distract air safety surveillance. The most recent development in air traffic surveillance is the automatic dependent surveillance – broadcast (ADS-B). Aircraft periodically broadcast their location, speed, or environmental measurements via ADS-B. The open research project OpenSky Network collects ADS-B reports and makes them available for research purposes.

This poster presents a concept to detect and localize spoofing devices by utilizing the information provided by a large-scale air traffic surveillance system. We utilize ADS-B reports collected by the OpenSky Network and provide first results on the effectiveness of localizing spoofing sources.

1. MOTIVATION

GPS is used in many applications that rely on positioning or timing information. However, the system is not secure, i. e., GPS signals sent by the satellites are neither authenticated nor encrypted [19]. Consequently, GPS is vulnerable to signal spoofing attacks, where an attacker transmits fake signals that imitate signals from satellites but at a higher power and at different time delays [5, 6]. GPS receivers will lock on to the fake signals instead of to the signals from the authentic satellites. This gives rise to attackers that try to inject fake positioning information in systems that, e. g., realize navigation for drones or in aircraft [8]. As a result, aircraft that are affected by this type of attack, will broadcast the false positioning information using ADS-B [2, 11, 17, 16]. Since the fake information contained in the ADS-B reports depend on the attacker-induced signals, we try to extract information to determine the attacker's location. This could help to shut down attacks faster to resolve potentially devastating incidents.

2. CONTRIBUTIONS

The poster will present a concept for detecting GPS spoofing attacks and for localizing the spoofing source using an existing infrastructure based on ADS-B reports. In particular, the poster will outline a novel technique for the localization of GPS spoofing devices via relating the fake positioning information reports contained in ADS-B messages. Finally, the poster will briefly foreshadow first simulation results based on real-world air traffic control data from the OpenSky Network [14, 15]. The results show that using the messages from at least four aircraft, it is possible to detect and localize spoofing devices by rapidly narrowing down a potential search radius.

3. METHOD

Our novel method leverages existing position advertisements that aircraft periodically broadcast for air traffic control purposes. We use the reported position information from the spoofed aircraft and the timestamps that are generated in the ground-based sensors. While other works [12, 13, 9, 7] focus on spoofing detection, we go further and explore the possibility of localizing the spoofing source. Further, we are considering moving targets like aircraft in the sense that both the target itself and the spoofed positions are non-stationary. Compared to other suggestions [1, 20, 10], our approach is lightweight and does not require modifications of the GPS receiving devices, and it uses already available data collected in real-time by air traffic control authorities and online flight tracking services. The reports collected by multiple ground-based sensors can be used to (i) detect GPS spoofing attacks and (ii) localize the spoofing source.

4. SPOOFING DETECTION

We can detect spoofing attacks on the logical level via cross-checking multiple position estimates from each aircraft or by checking the reported locations from multiple aircraft. The first approach checks if the actual position of the aircraft resolved by other means like RADAR or multilateration [4, 3] is within a certain range of the position reported

ASIA CCS '17 April 02-06, 2017, Abu Dhabi, United Arab Emirates

ACM ISBN 978-1-4503-4944-4/17/04.

DOI: http://dx.doi.org/10.1145/3052973.3055158

via ADS-B. A distance too far off can be an indication of a spoofing attack. The latter approach is based on a comparison of the position reports from multiple aircraft, which will be similar if the aircraft are affected by the same spoofing attack. A mutual distance that violates air traffic restrictions can point towards the presence of an ongoing spoofing attack.

5. SPOOFER LOCALIZATION

When we have successfully detected a spoofing attack, we need to trace the source in order to stop the spoofing attack. The localization approach is based on the following observations. A spoofer that affects multiple aircraft has different distances to each of the reached aircraft. Based on these distances, the aircraft have different positions on the moving track, which can be expressed as a function of the distance to the spoofing source and the velocity of the spoofed GPS track.

At the ground stations, we receive the ADS-B reports of all the affected aircraft. With these reports we can formulate relationships incorporating the actual position of the aircraft, the spoofed track velocity, and the current spoofer position. We can estimate the position of the aircraft via, e. g., multilateration and we can calculate the spoofed track velocity based on the time series of reported GPS positions. Considering these relationships, we can numerically solve multiple equations towards the spoofer position, which is assumed to be the same for all currently affected aircraft.

6. RESULTS

Our first results suggest that we can narrow down the spoofer location to a search space with a radius of a few kilometers. Taking the overall search space into consideration, which is every position an attacker can sent signals from, this represents a significant reduction. For instance, we were able to reduce the search radius to less than ten kilometers as compared to several hundreds or even thousands of square kilometers that is observed by the sensors. These initial results are based on conservative assumptions and are expected to improve further.

Additionally, we can state that our method only requires the fake signals of four aircraft to start narrowing down the potential spoofer location. We achieved reasonable search space reductions within a few minutes after the spoofing attack is launched.

7. RELATED WORK

GPS is known to be vulnerable to jamming and spoofing attacks [5, 6]. The requirements for successful GPS spoofing attacks are analyzed in [18]. In [1], the authors propose general techniques for detecting and localizing spoofing attacks in wireless networks. The same authors [20] extended the scheme to deal with attackers varying the transmission power. GPS spoofing detection approaches that employ multiple sensors at separated locations are discussed by Tippenhauer et al. [18, 7].

Even though these detection approaches do not require changes to the GPS infrastructure, they still have a crucial drawback. They assume more specialized GPS receivers increasing, e. g., the complexity and power requirements. This is potentially critical since aerial standardization processes take a very long time as compared to other industries.

8. REFERENCES

[1] Y. Chen, W. Trappe, and R. P. Martin. Detecting and Localizing Wireless Spoofing Attacks. In *IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, SECON '07, pages 193–202, San Diego, CA, USA, June 2007. IEEE.

[2] A. Costin and A. Francillon. Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. Technical report, Black Hat USA, July 2012.

[3] FlightAware. Multilateration (MLAT) Overview, 2016.

[4] Flightradar24. How We Track Flights with MLAT, 2015.

[5] T. E. Humphreys. Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing. Technical report, The University of Texas at Austin, July 2012. Submitted to the Subcommittee on Oversight, Investigations, and Management of the House Committee on Homeland Security.

[6] T. E. Humphreys. Statement on the Security Threat Posed by Unmanned Aerial Systems and Posssible Countermeasures. Technical report, The University of Texas at Austin, Mar. 2015. Submitted to the Subcommittee on Oversight and Management Efficiency of the House Committee on Homeland Security.

[7] K. Jansen, N. O. Tippenhauer, and C. Pöpper. Multi-Receiver GPS Spoofing Detection: Error Models and Realization. In *Annual Computer Security Applications Conference*, ACSAC '16, Los Angeles, CA, USA, Dec. 2016. ACM.

[8] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys. Unmanned Aircraft Capture and Control via GPS Spoofing. *Journal of Field Robotics*, 31(4):617–636, July 2014.

[9] D. Moser, P. Leu, L. Vincent, A. Ranganathan, F. Ricciato, and S. Čapkun. Investigation of Multi-device Location Spoofing Attacks on Air Traffic Control and Possible Countermeasures. In *ACM Conference on Mobile Computing and Networking*, MobiCom '16, New York, USA, Oct. 2016. ACM.

[10] A. Ranganathan, H. Ólafsdóttir, and S. Čapkun. SPREE: A Spoofing Resistant GPS Receiver. In *ACM Conference on Mobile Computing and Networking*, MobiCom '16, New York, USA, Oct. 2016. ACM.

[11] M. Schäfer, V. Lenders, and I. Martinovic. Experimental Analysis of Attacks on Next Generation Air Traffic Communication. In *International Conference on Applied Cryptography and Network Security*, ACNS '13, pages 253–271, Banff, Alberta, Canada, June 2013. Springer.

[12] M. Schäfer, V. Lenders, and J. Schmitt. Secure Track Verification. In *IEEE Symposium on Security and Privacy*, SP '15, pages 199–213, San Jose, CA, USA, May 2015. IEEE.

[13] M. Schäfer, P. Leu, V. Lenders, and J. Schmitt. Secure Motion Verification using the Doppler Effect. In *ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '16, pages 135–145, Darmstadt, Germany, July 2016. ACM.

[14] M. Schäfer, M. Strohmeier, V. Lenders, I. Martinovic,

and M. Wilhelm. Bringing up OpenSky: A Large-scale ADS-B Sensor Network for Research. In *ACM/IEEE International Conference on Information Processing in Sensor Networks*, IPSN '14, pages 83–94, Berlin, Germany, Apr. 2014. IEEE.

[15] M. Schäfer, M. Strohmeier, M. Smith, M. Fuchs, R. Pinheiro, V. Lenders, and I. Martinovic. OpenSky Report 2016: Facts and Figures on SSR Mode S and ADS-B Usage. In *IEEE/AIAA Digital Avionics Systems Conference*, DASC '16, Sacramento, CA, USA, Sept. 2016. IEEE.

[16] M. Strohmeier, V. Lenders, and I. Martinovic. On the Security of the Automatic Dependent Surveillance-Broadcast Protocol. *IEEE Communications Surveys & Tutorials*, 17(2):1066–1087, Oct. 2014.

[17] M. Strohmeier, M. Schäfer, V. Lenders, and I. Martinovic. Realities and Challenges of NextGen Air Traffic Management: The Case of ADS-B. *IEEE Communications Magazine*, 52(5):111–118, May 2014.

[18] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Čapkun. On the Requirements for Successful GPS Spoofing Attacks. In *ACM Conference on Computer and Communications Security*, CCS '11, pages 75–86, Chicago, IL, USA, Oct. 2011. ACM.

[19] U.S. Department of Defense. *Global Positioning System Standard Positioning Service Performance Standard*, 4th edition, Sept. 2008.

[20] J. Yang, Y. Chen, W. Trappe, and J. Cheng. Detection and Localization of Multiple Spoofing Attackers in Wireless Networks. *IEEE Transactions on Parallel and Distributed Systems*, 24(1):44–58, Jan. 2013.