INTERNATIONAL JOURNAL OF RECENT TRENDS IN ENGINEERING & RESEARCH
Impact Factor 4.101 ISSN -2455-1457
RECENT ADVANCES IN ELECTRONICS & COMMUNICATION ENGINEERING (RAECE-2K17)

ADS-B is Vulnerable to location Spoofing Attacks and Countermeasures

Murali Krishna Rayapu
Department of Electronics and Communications Engg.
NNRG College of Engineering, Hyderabad, India

Shilpa Samarla
Department of Electronics and Communications Engg
NNRG College of Engineering, Hyderabad, India

G. Indira Priya Darshini
Department of Electronics and Communications Engg
NNRG College of Engineering, Hyderabad, India

ABSTRACT
Multilateration techniques have been proposed to verify the integrity of unprotected location claims in wireless localization systems. A common assumption is that the adversary is equipped with only a single device from which it transmits location spoofing signals. In this paper, we consider a more advanced model where the attacker is equipped with multiple devices and performs a geographically distributed coordinated attack on the multilateration system. The feasibility of a distributed multi-device attack is demonstrated experimentally with a self-developed attack implementation based on multiple COTS software-defined radio (SDR) devices. We launch an attack against the OpenSky Network, an air traffic surveillance system that implements a time-difference-of-arrival (TDoA) Multilateration method for aircraft localization based on ADS-B signals.
Our experiments show that the timing errors for distributed spoofed signals are indistinguishable from the multilateration errors of legitimate aircraft signals, indicating that the threat of multi-device spoofing attacks is real in this and other similar systems. In the second part of this work, we investigate physical-layer features that could be used to detect multi-device attacks. We show that the frequency offset and transient phase noise of the attacker's radio devices can be exploited to discriminate between a received signal that has been transmitted by a single (legitimate) transponder or by multiple (malicious) spoofing sources. Based on that, we devise a multi-device spoofing detection system that achieves zero false positives and a false negative rate below 1%.

Overview

ADS-B is one of the emerging technology which is considered to be the emerging technology in civil aviation. ADS-B provided its positional information which is derived from satellites by means of GPS receiver and adds the additional information to it and then broadcasts. This information is use by other aircrafts, vehicles and by ground facilities. ADS-B isacronimed as Automatic Dependent Surveillance – Broadcast the elaborated meaning is as given below.

ADS-B and MLAT are being emerging concepts, which are meant for increasing the availability and detection of emitters and increase the system performance.

- The performance of the system depends upon the visibility of ground receiver station and also the analysis of the influence of each ground position on the system performance.
- The factors affecting the system degradation depends on poor visibility and less performance levels, this becomes the threat in giving the ability to detect.
- At installation of unit a validation, a more comprehensive maintenance set of analysis are required and these are provided by "**Quadrant's Control and Monitoring System (QCMS)".**

ADS-B explains about its advanced features and comes under the dependance category of surveillance as listedbelow.

- **Automatic:** The operation of the system is *automatic*, and manual intervention of neither ground staff nor pilot is required as every messaging is done automatically.
- **Dependent:** The accuracy of the system is dependent upon the on-board avionics. Navigation and other related data sources (e.g. FMS) for providing the data broadcast; this requires a co-operative/ friendly Aircraft.
- **Surveillance:** The broadcasted information is provided for air and ground *surveillance.*
- **Broadcast:** The system information is *broadcasted*. Originator who receives the data will be able to use the data without any specific 'contract' or interrogation scheduling.

In the present scenario ADS-B is mainly preferred due to following advantages:

1) Provides information about aircraft's
   a. Position
   b. Altitude
   c. Speed and heading
   d. Rate
   e. Aircraft identification

2) In the present scenario the integration of radar sources is very much essential. It has the following advantages.
   a. Presented at ATC controller working position
   b. All (known) target information via one interface
3) Commercial Aircrafts should be visible to ATC.

The Design parameters of ABS –B are as given below:

Coverage Volume:

1) The cubic volume defined according to the specifications and aircraft operates within the required specifications.
2) Accuracy.
3) The coverage is based on the difference between estimated and actual position of an aircraft.

Integrity:

1) This determines that the aircraft is flying in its pre-determined volume and cannot breach the volume. If it breaches the tunnel named as volume then system raises an indication is shown.
2) The update rate is also high.
3) Reliability of the system performance is high.
4) The continuity & Availability of the emitter is bound to be in the given specifications and its probability of failure is also less.

The performance rate is dependent on the operating time and is again related to the rated specifications.

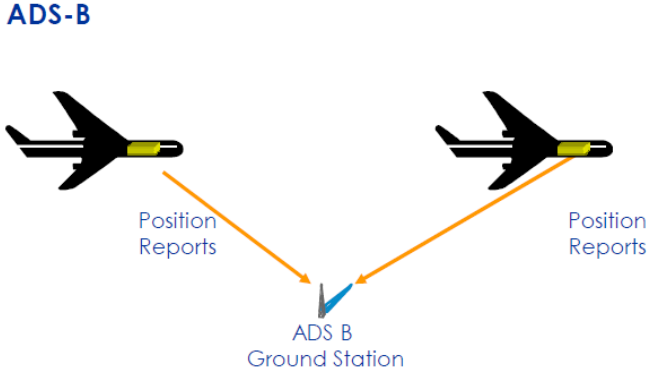

Figure 1 Automatic Dependant Surveillance

Future Surveillance System

The aspects of the future surveillance system should have the following advantages, these are as given below.

- High Performance & Competitive than SSR
- No RF emission
- Minimal power requirement (Approx. 10W per Sensor)
- Easy Installation
- Higher update rate - 2 positions per second
- Standalone or MLAT configuration
- Mandatory after 2017 in some countries
- Radar like separation at reduced cost
- It is Able to share data (Air-to-Air application).
- Can extend its own surveillance coverage area.
- Reduce coordination issues.
- Self-Separation and Free flight concept.

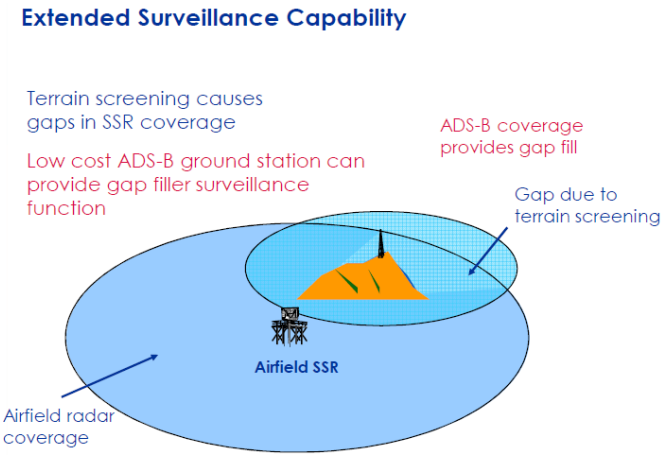

Figure 2 ADS-B Coverage

Efficiency of the system depends on the following:

- Affective utilization of airspace.
- Optimum flight levels accommodation i.e. number of Aircrafts in higher levels which results in fuel savings.
- In critical times like restricted areas activation and bad weather conditions the diversion will be smooth.
- The implementation cost is less and maintenance is easier.

Safety features of this system are as given below:

- Precise in Position & Velocity is broadcasted
- Range of Radar does not ADS-B accuracy as in conventional radar.
- It covers overseas air space.
- The response time is very high for rescue response.
- Its availability reduces the risk of collision.

Capacity of ADS-B is as given below:

- Same airspace can be used by many aircrafts at given time.
- Density in the non-radar region can be greatly increased.
- Reduces the take-off and landing time and so increases the flight movement greatly.

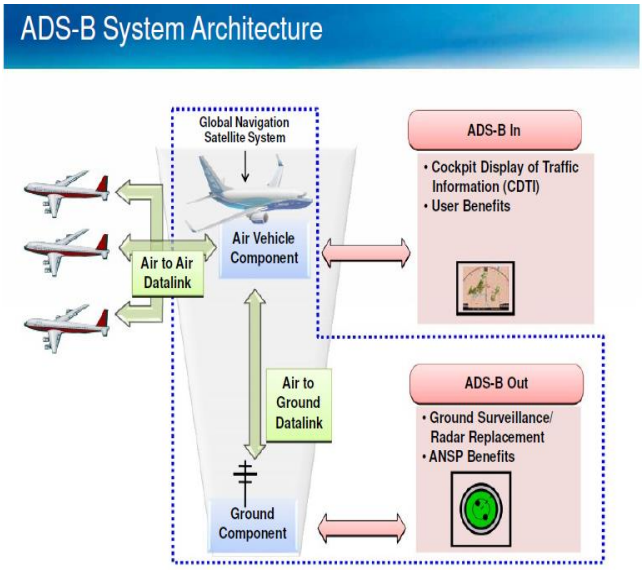

Figure 3 ADS-B Signal Flow

GPS RECEIVER:

One of the most important parts of ADS-B is GPS RECEIVER

The functions of receiver are as given below.

- The UTC time reference for internal high-stability time source is provided by GPS or NTP.
- In addition it provides position and altitude information which is used for operation.
- The distance between the GPS Receiver and the Sensor/ Low Power Site Monitor shall not exceed more than 5 meters.
- The system mainly uses the time derived from GPS Rx that in turn will be used for synchronisation, its system time and relevant timestamp where ever required.

The transmitter pipeline works as follows. The code on the PC (referred to as *multispoof*), takes as input from a master PC an arbitrary trajectory to be spoofed and generates the sequence of all ADS-B messages that a transponder should transmit according to the standard [30] when flying this trajectory. Important are the position messages which are sent twice per second including the spoofed locations. These messages are then transformed to a stream of digital IQ samples on the PC according to the pulse position modulation (PPM) of the Mode S data link. These computed IQ samples are then transferred to the USRP through the USRP Hardware Driver (UHD). However, the ADS-B signals are not immediately transferred over the radio front-end but first buffered in the internal memory of the USRPs. The transmission times of these buffered samples are different for each radio and carefully selected in order to mimic the time difference of arrivals between the Multilateration sensors for the claimed locations. The FPGAs on the USRPs then independently trigger the transmission of the samples of each ADSB message based on the times specified in the buffers.

Figure 4 GPS Receiver with connecting cable

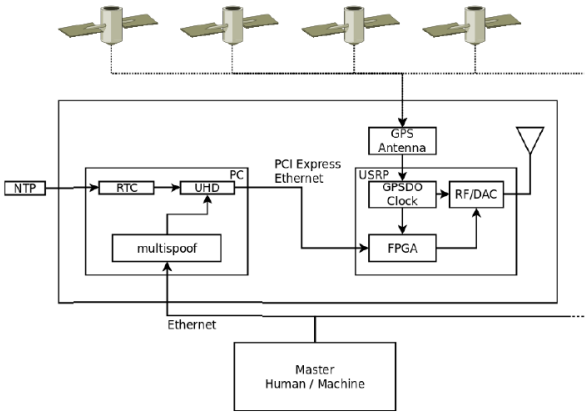

Figure 5 Software-defined radio architecture of the transponders for the attack. Time synchronization of the software-defined radios (USRP) is achieved using GPS disciplined oscillators

The last challenge to solve is the time synchronization among the USRPs. Classical software-defined radios such as the USRPs do not provide enough clock stability for the intended purpose because the clock used to trigger the FPGA is derived from a local oscillator which significantly drifts apart for different radios. Our approach to solving this problem was to replace the local oscillator of the USRPs with a GPS-disciplined oscillator (GPSDO). A GPSDO is an oscillator which is controlled by a tracking loop locked to the GPS signal. The GPS satellites are equipped with atomic clocks with very high time stability and therefore provide an excellent signal source for time synchronization. By locking the oscillators of the USRP to the GPS timing source, the USRP are now synchronized with very high accuracy and can trigger the transmissions at the correct times. The detailed schematics of the attacker setup are shown in Figure 5.

Equipped with the attacker setup described above, we demonstrate in the following the feasibility to perform multi-device location spoofing attacks in the Open Sky Network. In addition to demonstrating the feasibility of these attacks, we further aim at understanding the limiting factors for the attacker and therefore perform additional benchmarks which serve to quantify the impact of different factors on the spoofing accuracy.

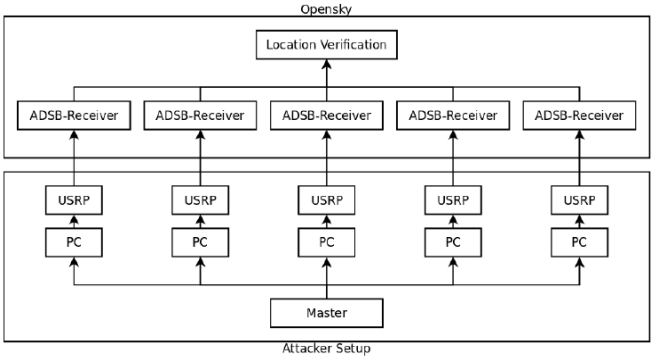

Figure 6 Overview of the Multilateration attack setup. A master node connected to five attacking devices (PC and USRP) controls the exact time at which the five Open Sky receivers receive the ADSB messages for Multilateration.

Performing an experimental over-the-air attack on a system like the Open Sky Network has some legal and safety implications, and we, therefore, have to be careful when designing the experiment. First, the 1090 MHz channel used to transmit ADS-B signals is licensed, and as such, only certified transponders are allowed to transmit in this frequency band. Second, the spoofed messages may be misinterpreted as legitimate signals by listening aircraft and ground controllers in the neighborhood leading to safety issues for the regular air traffic. To avoid legal and safety complications, we decided to minimize the risk of emitting spoofed messages to the outside world as much as possible and perform the experiments by transmitting the signals from the attacker to the receivers over shielded RF cables whenever possible. Only to study the impact of the channel conditions on the spoofing accuracy, we perform controlled over-the-air experiments with an antenna. Furthermore all the over-the-air experiments were conducted inside a large 7-floor concrete building with shielded windows to avoid any leakage to the outside world. We confirmed the same by measuring whether spoofed messages were received from the outside of the building.

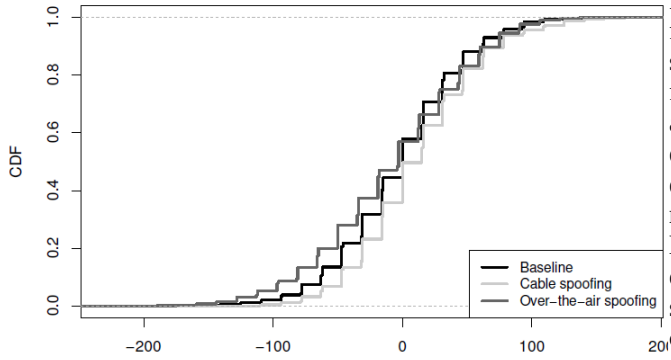

Figure 7 Distribution of the TDoA between packets sent by two spoofing devices. Over-the-air and cable experiments are close to the baseline.

Figure 7 shows the distribution of the TDoA for our three experimental setups when the spoofers are configured to produce a TDoA of zero at the two receivers. Several interesting conclusions can be made from the resulting distributions. First, the distribution for all three experiments shows a comparable standard deviation. While both cable-based measurements are distributed with standard deviation of about 50*ns*, the measurements over the air yielded a standard deviation of approximately 60*ns*. This indicates that the primary source of noise is not related to the synchronization error of the spoofer setup or the wireless channel but from the noise of the receivers themselves. The distribution of the mean TDoA values are also quite similar. The over-the-air experiments hold a mean deviation of *7:5*ns*, the spoofers over cable a mean of 11:4*ns*, while the baseline only differs *1:8*ns* from the expected mean of 0*ns*.

While both, the cable and over-the-air experiments do not perfectly match the signals of our baseline experiment, they do not add much additional error compared to the large uncertainty resulting from the high standard deviation of the TDoA measurements. These results confirm that an attacker can precisely time the TDoA at two receivers while using two separate spoofing devices.

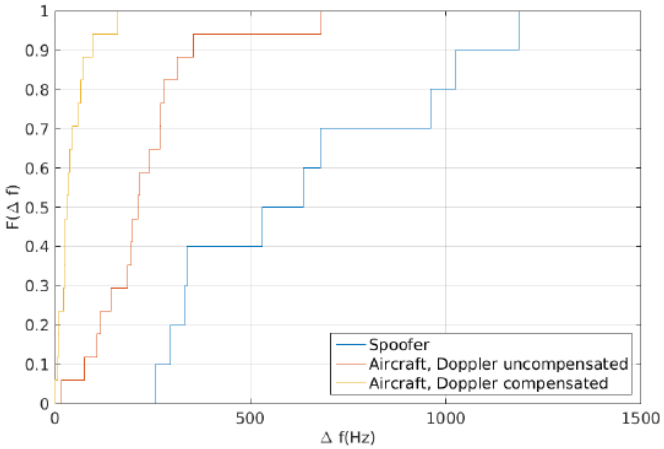

Figure 8 The CDFs show the medians of the frequency offsets of different spoofer and aircraft datasets. To the left we have the Doppler compensated and uncompensated aircraft signals; to the right the spoofer's frequency offsets.

Figure 8 shows the distributions of the medians of the frequency offsets in our datasets with multi-device spoofing signals and legitimate aircraft (see Section 5.1 for the details of the experimental setup). Since real aircraft are moving, the received signals at the sensors experience a Doppler shift which we compensate by extracting the speed of the aircraft from the ADS-B messages. As we can see, the signals from real aircraft are located nearer to an offset of zero, the spoofer's signal offsets lie further from zero and experience a much flatter slope. This separation, especially between the Doppler compensated and the spoofer's curve Figure 5: The CDFs show the medians of the frequency offsets of different spoofer and aircraft datasets. To the left we have the Doppler compensated and uncompensated aircraft signals; to the right the spoofer's frequency offsets. Highlight the applicability of this feature to discern spoofed signals originating from different attack devices. However, we recognize that an attacker might be able to counteract his device's frequency offset by measuring the offsets himself

and correct them in software prior to transmitting the spoofing signals. Additionally, the attacker may try to improve the stability and accuracy of the synchronization method and thus reduce his transmitter's frequency offsets. Nevertheless, a non-zero frequency offset is likely to remain given the imperfections in the hardware components used in the attacker's radio transmitters.

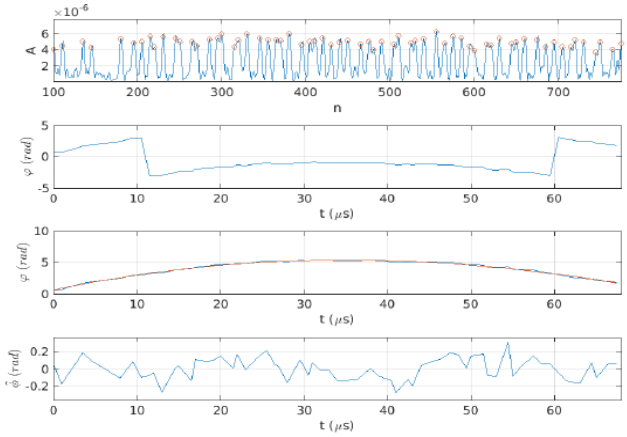

Figure 9 Phase extraction process for a sample message

The top plot reports the signal amplitude, followed by the instantaneous phase _. The third plot shows the instantaneous phase after unwrapping (blue line) and the corresponding regression (orange). The difference between the two represents the phase noise and is displayed in the bottom plot.

Figure 9 showes Phase extraction process for a sample message. The top plot reports the signal amplitude, followed by the instantaneous phase _. The third plot shows the instantaneous phase after unwrapping (blue line) and the corresponding regression (orange). The difference between the two represents the phase noise and is displayed in the bottom plot. Behavioral characteristics during the tuning process to the carrier frequency. Therefore, observing additional pulses of the recorded signal will not improve our detection of a multi-device spoofing attack.

The signals were captured using one sample per pulse. The phase noise for the first pulse is the first value in the phase noise vector ._u. This phase noise is extracted from a discrete-time signal u.

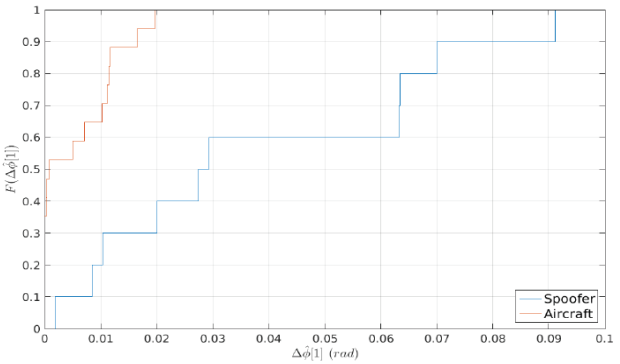

Fig 10 These CDFs show the distribution of the phase transient feature for real and spoofed signals.

As shown in Figure 10, even though both distributions for the spoofer and the aircraft's signals are well separated, they still exhibit an overlapping area. We therefore aggregate this feature's data at more than two receivers to extract meaningful results and for the final distinction between legitimate and spoofing signals.

Attack Detection Performance

As shown in the results for different configurations of the frequency and phase feature. Using the frequency offset, our IDS detects 96~ of attacks with zero false positives using the average 30 messages, making use of four receivers. With the same parameters, the phase feature accomplishes an attack detection rate of 92~ with again zero false positives. Using the average over 10 messages already skews our results aswe encounter false positive classifications immediately from the beginning. If our IDS only uses one message for decision making, the false positive rate starts to dominate the classification results.

CONCLUSIONS

This work has shown that a distributed multi-device attacker model is a realistic threat scenario to TDoA Multilateration systems. We have shown that using COTS software-defined radios with GPS synchronization, it is possible to generate spoofing signals with a sufficient synchronization over large areas such that the localization error of the Multilateration becomes indistinguishable from the error of legitimate signals. Given this result, we have analyzed the usage of physical-layer features to detect multi-device attacks against wireless Multilateration systems. We identified and evaluated a frequency-based and a phase-based feature which can be used to detect distributed attackers. These features are well suited to detect distributed spoofing attacks in air traffic surveillance scenarios because the attack detection is (i) purely passive, (ii) does not require any changes to the legacy data communication protocols, (iii) requires only limited exchange of information between the sensors, and (iv) works even when the Multilateration sensor locations are known by the attacker.

REFERENCES

[1] Radarcape. http://shop.jetvision.de/Radarcape. [Online: accessed 11/13/2015].

[2] X300 Product Page. http://www.ettus.com/product/details/X300-KIT. [Online; accessed 12/07/2014].

[3] Wide Area Multilateration, Report on EATMP TRS 131/04, Version 1.1. https://www.eurocontrol.int/sites/default/files/publication/files/surveilllance-report-wide-area-multilateration-200508.pdf, 2005. [Online; accessed 02/16/2015].

[4] Andrei Costin and Aurélien Francillon. Ghost is in the Air(traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. Black Hat USA, July 2012. White paper.

[5] K. Bauer, D. McCoy, E. Anderson, M. Breitenbach, G. Grudic, D. Grunwald, and D. Sicker. The directional attack on wireless localization -or- how to spoof yourlocation with a tin can. In *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, pages 1–6, Nov 2009.

[6] V. Brik, S. Banerjee, M. Gruteser, and S. Oh. Wireless device identification with radiometric signatures. In *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, MobiCom' 08, pages 116–127, New York, NY, USA, 2008. ACM.

[7] S. R. Bussolari and D. J. Bernays. Mode s data link applications for general aviation. In *Digital Avionics Systems Conference, 1995., 14th DASC*, pages 199–206. IEEE, 1995.

[8] S. Capkun, K. Bonne Rasmussen, M. Cagalj, and M. Srivastava. Secure location verification with hidden and mobile base stations. *Mobile Computing, IEEE Transactions on*, 7(4):470–483, April 2008.

[9] S. Capkun and J.-P. Hubaux. Secure positioning of wireless devices with application to sensor networks. In *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, volume 3, pages 1917–1928 vol. 3, March 2005.

[10] Y. Chen, W. Trappe, and R. Martin. Attack Detection in Wireless Localization. In *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, pages 1964–1972, May 2007.

[11] J. T. Chiang, J. J. Haas, J. Choi, and Y.-C. Hu. Secure Location Verification Using Simultaneous Multilateration. *IEEE Transactions on Wireless Communications*, 11(2), feb. 2012.

[12] Costin, Andrei and Francillon, Aurélien. Ghost is in the Air(traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. In *Black Hat USA*, July 2012.

[13] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy. Attacks on physical-layer identification. In *Proceedings of the Third ACM Conference on Wireless Network Security*, WiSec '10, pages 89–98, New York, NY, USA, 2010. ACM.

[14] B. Danev, D. Zanetti, and S. Capkun. On physical-layer identification of wireless devices. *ACM Comput. Surv.*, 45(1):6:1–6:29, Dec. 2012.

[15] W. Du, L. Fang, and P. Ning. Lad: Localization anomaly detection for wireless sensor networks. In *International Parallel and Distributed Processing Symposium - IPDPS*, page 874, 2005.

[16] K. J. Ellis and N. Serinken. Characteristics of radio transmitter fingerprints. *Radio Science*, 36(4):585–597, 2001.

[17] J. Hall. Enhancing intrusion detection in wireless networks using radio frequency fingerprinting. In *Proceedings of the 3rd IASTED International Conference on Communications, Internet and Information Technology* (CIIT), pages 201–206. Kranakis, 2004.

