# Security and Reliability of Wireless LAN Protocol Stacks Used in Control Systems

Jacob Brodsky, PE and Anthony McConnell, PE
Washington Suburban Sanitary Commission
Laurel, Maryland
{jBrodsk, aMcconn}@wsscwater.comm

Marco Cajina, Dale Peterson
Digital Bond, Inc.
Sunrise, Florida
{cajina, peterson}@digitalbond.com

**Abstract:** Wireless LAN technology offers some important benefits for control systems including easier and lower cost deployment and topology changes. However this wireless LAN technology can be more accessible to an attacker than wired LAN technology. To address this potential increased risk, industry groups have been working on wireless security standards. One of the more popular efforts is ISA 100.11a.

Most of the discussions regarding hacking and protecting ISA 100.11a and other wireless LAN efforts have focused on source and data integrity and confidentiality in the form of detailed cryptographic protocols. The third leg of the security triad, availability, has received less attention particularly from malicious attempts to affect availability of the wireless signal, such as jamming.

ISA 100 and other wireless standards leverage IEEE 802.15.4 for the layer two protocol. Brodsky and McConnell showed in a 2009 S4 [1] paper that the Clear Channel Assessment (CCA) feature in IEEE 802.15.4 made this signal easy to jam using very low cost equipment. However, that test only occurred on one channel and not on ISA 100.11a radios. After the paper was released, there was uncertainty on whether this jamming attack would be prevented by some measures in the ISA 100.11a protocol stack. This year, the authors expanded the jamming equipment and testing to include all 16 channels in the 2.4GHz range, and the authors tested an actual ISA 100.11a radio.

The Nivis ISA 100.11a [2] protocol stack, the only stack for that protocol available at the time of the testing, was obtained and deployed for testing. The results from the jamming were mixed and discussed in the paper. The radios were more resistant than the IEEE 802.15.4 radios tested last year, but there performance and reliability issues remained, especially in establishing connections when jamming was taking place.

**Keywords:** Clear Channel Assessment, IEEE 802.15.4, ISA 100.11a, Jamming, Wireless LAN

# 1 Introduction

At the 2009 S4, Brodsky and McConnell presented a paper showing how to interfere with an IEEE 802.15.4 signal. That paper showed how a single channel of an IEEE802.15.4 low power network could be attacked using inexpensive hardware to inhibit traffic by using the CCA feature to prohibit communication attempts. Following that presentation, several attendees and commenters contended that ISA 100.11a, even though it is based upon IEEE 802.15.4, does not use CCA.

This paper documents follow-up testing with equipment capable of simultaneous jamming of all 16 channels in the 2.4GHz range in the standard and an actual ISA 100.11a radio.

# 2 Test Platform and Jamming Equipment

To move from intellectual disagreements and theory to real world testing and results, the Nivis 100.11a integration kit was obtained and deployed. In 2009, Nivis had the only ISA 100.11A protocol stack, and at the time of the testing all ISA 100.11A products were using the Nivis protocol stack. The integration kit included:

- 4 field devices/sensors
- 1 router (base station/gateway)
- 1 system manager PC

The Nivis products were very easy to deploy. All hardware and software came pre-configured with specific IP's and account settings, enabling the setup of the system to require minimum effort by means of setting up a network switch to the configured LAN subnet. Additionally, instructions were provided on how to make changes to the configuration of the system, such as NTP server and IP addresses. All field devices were pre-provisioned to only communicate and join the network controlled by the system manager provided with the integration kit.

The RF jamming equipment used in this paper was custom built by the authors. One of the gating factors was to limit the cost to US$200 and the components to easily procured items to mimic an enterprising but financially limited attacker. A well-funded attacker could develop or purchase a more capable jammer, but even with this limited funding the authors were able to put a signal on all 16 channels used by the protocol.

The jamming equipment used a linearized Voltage Controlled Oscillator (VCO) to generate a wideband frequency modulated signal in the 2.4GHz spectrum. The modulation frequency was typically 1.0MHz, though frequencies as low as 500 kHz and as high as 5 MHz were used without issue. The VCO output was measured at +8 dBm (decibel comparison to one milliwatt) and was amplified to as high as +30 dBm using two amplifiers. Additionally, attenuators were available to test at the lower power levels. The equipment was used to generate a signal with sidebands guaranteed to be on each channel in the 2.4 GHz spectrum within the passband of the receiver.

The jamming equipment generated a signal from 2400 to 2480 MHZ to ensure that all 16 channels were flooded with interference.

Most parts came from Mini-Circuits Inc. This firm is well established and deals with orders both large and small. The VCO was a model ZX95-2490+. The amplifiers we used were TAMP-272LN surface mount modules. We soldered them together using solder paste and a toaster oven to Mini-Circuit's standard test fixture model TB-468+. These models have a 1 dB compression output (the output level at which the gain drops by 1 decibel) of typically 19.5 dBm. The 802.11b amplifier used was inexpensive and purchased on E-Bay. Lastly, we used a microwave power meter to measure a power output of +29.5 dBm, just shy of one watt. A picture of the jamming platform is shown in Figure 1.


*Figure 1 – Jamming Test Platform*

## 3 Testing Scenarios

Three different test scenarios were included in the testing discussed in this paper.

1. Test scenario 1: Establish communications between the sensors and router/gateway. Then with established communications, enable jamming signal, on all 16 channels.
2. Test scenario 2: Enable jamming signal, on all 16 channels, then attempt to establish a connection including a sensor's registration process with the router/gateway.
3. Test scenario 3: Enable jamming signal to interfere with only the even channels, then attempt to establish a connection including a sensor's registration process with the router/gateway.

## 3.1 Test Scenario 1

In our first scenario, the effects of beginning a jamming effort on a fully running system were tested. Once the system was up and running and with the sensors actively transmitting data to the router/gateway, the jamming signal was started on all 16 possible channels.

The system was monitored for several minutes with no adverse side effects detected. This appears to indicate that CCA had been disabled on the Nivis sensors and gateway/router. However, after a prolonged period of time two out of the three sensors in the test were no longer registered with, or stopped transmitting data to, the router/gateway. One of devices came back online once the jamming signal was disabled, and the other one did not. It is unclear if this was a result of what is discussed in Test Scenario 2 or for some other reason.

## 3.2 Test Scenario 2

In second test scenario, the sensor registration process was tested for reliability under simple jamming conditions. Specifically, how would the sensor react in a hostile environment at different VCO output levels when attempting to initially synchronize with the router/gateway.

1. The first attempt was performed at +30 dBm. At this level, the sensor was unable to register with the router/gateway.
2. The second attempt was performed at 0 dBm. Again, the sensor was unable to register with the router/gateway.
3. The third attempt was performed at -20 dBm. Again, the sensor was unable to register with the router/gateway.

When the jamming signal was disabled, the sensor would register automatically within a few minutes.

Additionally, the sensor appears to erroneously indicate that it has registered when in the presence of the jamming signal, even when the router/gateway was turned off.

## 3.3 Test Scenario 3

This scenario was similar to Test Scenario 2, where the ability to prevent registration was tested, except only the even channels were being jammed, and only the 0 dBm jamming signal was tested. This was accomplished by setting the jamming signal frequency to 2440MHz and set the signal to a 10MHz input.

The jamming in this scenario caused a delay in registration, but the sensor eventually registered itself on an odd numbered channel. Also, once the sensor was registered, it functioned normally, on the channel with the jamming signal was present. This was the expected result and consistent with Test Scenario 1 results.

# 4 Results/Conclusion

The authors believe the testing in this paper indicates the reliability of ISA 100.11A when subjected to simple and low cost jammers is an open question. While the apparent results of CCA being disabled in established communications in the Nivis system makes jamming more difficult, the testing did show that a jammer could prevent registration or the establishment or re-establishment of sensor to router/gateway communications.

It is unclear whether the issues identified in this paper are due to a flaw in the ISA 100.11A specification, the Nivis implementation, or both. Furthermore, this may not even be considered a flaw if the specification is not designed to be jam resistant.

What is needed is additional testing of ISA 100.11A compliant sensors and router/gateways to determine precisely the jamming-resistance and jamming-risk. It is the dearth of this information that is of great concern and can lead to an unknown and unintended introduction of risk by owner/operators that decide to deploy wireless systems based on this protocol.

---

**About the Author** – Jacob Brodsky and Anthony McConnell are Registered Control Systems Engineers at the Washington Suburban Sanitary Commission, with a combined experience of 45 years.

Mr. Brodsky began his career there in 1986 as a Tele-Communications Technician while attending evening classes at the Johns Hopkins University. He earned his Bachelors Degree in Electrical Engineering in 1990.

Mr. McConnell has many years of various telecommunications experience ranging from in-car cameras for NASCAR, police and fire radio communications, radio paging networks, and utility communications networks.

Marco Cajina is a Security Researcher at Digital Bond. He is a key contributor to the Dept. of Energy funded Bandolier project that creates security audit files for control system components. Marco is also a technical lead on Digital Bond's control system security assessments.

Dale Peterson is the founder of Digital Bond and has been involved in computer security for more than twenty years. He began his career as a cryptanalyst at the US National Security Agency. For the last ten years Dale has focused on control system security and has led numerous research projects, consulting engagements as well as writing and speaking on the subject.

# References:

[1] J. Brodsky and A. McConnell, Jamming and Interference Induced Denial of Service Attacks on IEEE 802.15.4 Based Wireless Networks, 2009 Proceedings of the SCADA Security Scientific Symposium, Digital Bond Press

[2] http://www.nivis.com/NivisISAIntegrationKit/Default.aspx