Co-existence and Security White Paper

July, 2008

By Dr. Raju Pandey, CTO

1 Introduction

SynapSense wireless sensor network (WSN) solutions extend the enterprise IT infrastructure to key equipments, products, and facilities. They can monitor everything from specific equipments (such as power, vibration and utilization) to global environmental conditions (such as ambient temperature, humidity and air pressure). In addition, they provide application intelligence to characterize the state of the equipments or the environment, and to effectively adapt their behavior. The SynapSense wireless sensor network solution consists of two parts: (a) the *data collection* component provides a robust wireless mesh networking capability for instrumenting, collecting and transferring information to the analytics engine; and (b) the *analytics engine* analyzes the received data and provides intelligence about the monitored environment.

SynapSense sensor and networking devices use 802.15.4 based radios that operate in the 2.4 GHz industrial scientific and medical (ISM) unlicensed band. This white paper addresses the co-existence and security issues associated with SynapSense wireless products. Specifically, it addresses (i) co-existence of SynapSense wireless system with other wireless technologies that operate in the 2.4 GHz band, (ii) potential impact of operating SynapSense wireless devices on IT equipments, and (iii) security risks.

2 Co-existence

SynapSense sensor and gateway devices uses 802.15.4 based radios that operate in the 2.4 GHz industrial scientific and medical (ISM) unlicensed band. The ISM band is also used by IEEE 802.11b (WLAN), IEEE 802.15.1 (Bluetooth), wireless USB, and microwave ovens.
The table below summarizes the RF characteristics of the different 2.4 GHz technologies:

	Channel Width	# of Channels	Data Rate	Operating Range	Power
Wi-Fi (802.11b)	22 MHz	13	11 Mbps	~150 m	100 mw
Bluetooth	15 MHz	79	1 Mbps (v1.2)	~1 meter (Class 1)	2.5mw
			3 Mbps (v2)	~10 m (Class 2)	
				~100m (Class 3)	
Wireless USB	1 MHz	79	62.5 Kbps	~50 m	1mw
SynapSense	3 MHz	16	128 Kbps	~20-100 m	1 mw

Table 1: Radio Characteristics of different 2.4 GHz devices

2.1 Interference with Wi-Fi Devices

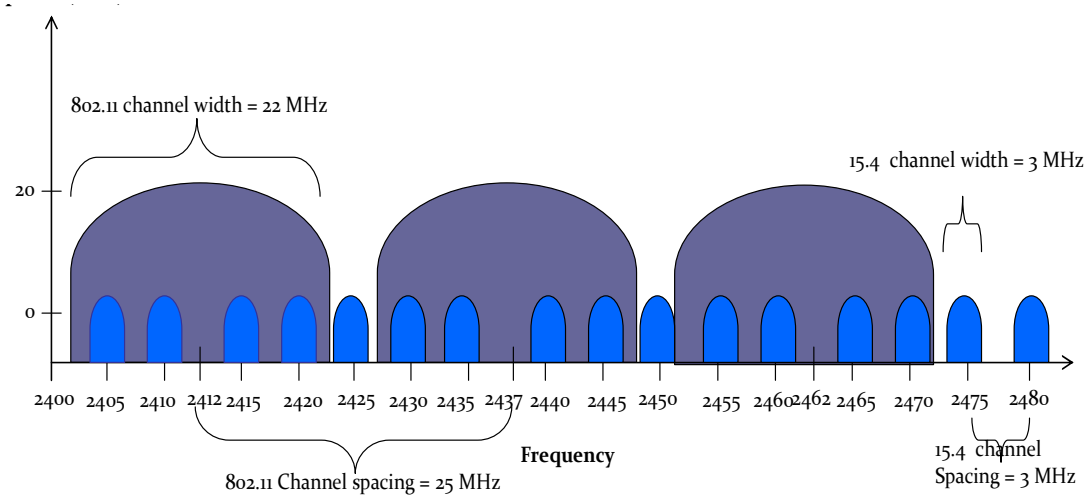


Figure 1: Frequency Overlap between 802.11 and 802.15.4 Channels

Wi-Fi uses the 2.4 GHz ISM band by dividing it into 14 possible channels, with each channel being 22 MHz wide, allowing up to three evenly-distributed concurrent channels. SynapSense devices use 16 channels that are 5 MHz apart. Figure 1 shows the three concurrent Wi-Fi channels along with the 16 channels defined for the SynapSense devices. The Y-axis shows the power differences between the 802.11 and 802.15.4 transmitters.

Several studies have been conducted to analyze the interference behavior of 802.11 and 802.15.4 technologies. In the first set of experiments, 802.11 and 802.15.4 radios are set to operate in overlapping frequency ranges - for instance, the 802.11 devices in channel 6 (2437 MHz) and the 802.15.4 devices in channel 16 (2440MHz). In such an environment, test results show that the majority of the 802.15.4 packets (> 90%) are destroyed by the 802.11 overlapping frames. However, some 15.4 packets survive, and able to use some of the unused 802.11 slots.

In another set of experiments, 802.15.4 and 802.11 devices were run on non-overlapping channels – for instance, the 802.11 devices on channel 4 (2427 MHz) and 802.15.4 devices on channel 16 (2440 MHz). The results show that as the distance between the channels used by the 802.11 and 802.15.4 devices increases, the rate of packet losses decreases. In the case when devices are operating in orthogonal channels, 15.4 devices have little or no losses.

These experiments indicate that 802.15.4 and 802.11 devices can co-exist by selecting non-overlapping channels. This selection can take place manually or adaptively through channel hopping. For instance, in a crowded 802.11 environment, SynapSense devices hop through different noisy channels until they can find non-overlapping channels.

Operation of 802.15.4 devices has small impact on 802.11 devices: when operating in overlapping frequency ranges, 802.11 devices have reduced signal to noise ratio in the narrow (5 MHz) overlapping band. Given that 802.11 devices use spread spectrum technology over the 22 MHz bandwidth, much of the 802.15.4 signal appears as a narrow band interference. Further, the output power of 802.15.4 devices is limited to 1 mw in comparison to 802.11 devices that operate at around 30mW.

2.2 Interference with Bluetooth Devices

Bluetooth is a short-range wireless technology, operating in the 2.4 GHz ISM band. It uses the spread spectrum, frequency hopping scheme. Bluetooth technology's adaptive

frequency hopping (AFH) capability hops among 79 frequencies at 1 MHz intervals to avoid interferences with other devices in the spectrum.

Tests have shown that about 1% of the 15.4 packets are destroyed due to interference. The losses occur when the 15.4 device and the Bluetooth device operate at the same time and on the same frequency. These tests show that Bluetooth devices do not interfere with SynapSense device operations, and can co-exist with them.

2.3 Interference with Microwave Ovens

Microwave ovens operate on the same 2.4 GHz ISM band. They also can be a source of interference with the 15.4 devices. Test studies have shown that if 15.4 devices are in close proximity (less than one meter) of a microwave oven, microwave operations have three kinds of effects on the 802.15.4 devices: The signal strength (RSSI) is reduced by a small amount; a small number (< 1%) of 15.4 packets are corrupted; and a small number (< 1%) 15.4 packets are completely destroyed. Over larger distances, there is no observable interference. In summary, microwave operation has negligible effect on SynapSense device operations.

2.4 Impact of operating SynapSense wireless devices on existing wireless devices

SynapSense systems use a number of techniques to ensure that SynapSense devices have minimal impact on other wireless systems and other IT equipment. These include the following:

- **Low power transmitters**: SynapSense devices use a low power transmitter (1 mw), which is significantly less than the other wireless devices in the same 2.4 GHz band.
- **Low duty cycle**: SynapSense devices operate in a very low duty cycle mode (< 1%). Also, they occur over a very small amount of time, typically in tens of milli seconds. This means that data transmissions are infrequent and are for a short duration.

- **Channel avoidance**: The SynapSense system uses the CSMA-CA scheme to sense the environment before transmitting any data in the air. This reduces the chances of interfering with any ongoing data transmission on the same channel.
- **Channel diversity**: SynapSense devices use the 16 available channels to send and receive data. This allows SynapSense systems to distribute their transmission schedule over the available channels, thereby reducing the amount of time specific channels are busy with SynapSense traffic.
- **Channel adaptation**: SynapSense devices use adaptive algorithms to determine specific channels that are free from any RF noise. This means that SynapSense network traffic can co-exist with other wireless devices by completely avoiding the channels that the other wireless devices are using.

2.5 Impact of SynapSense Devices on Data Center IT and Other Equipment

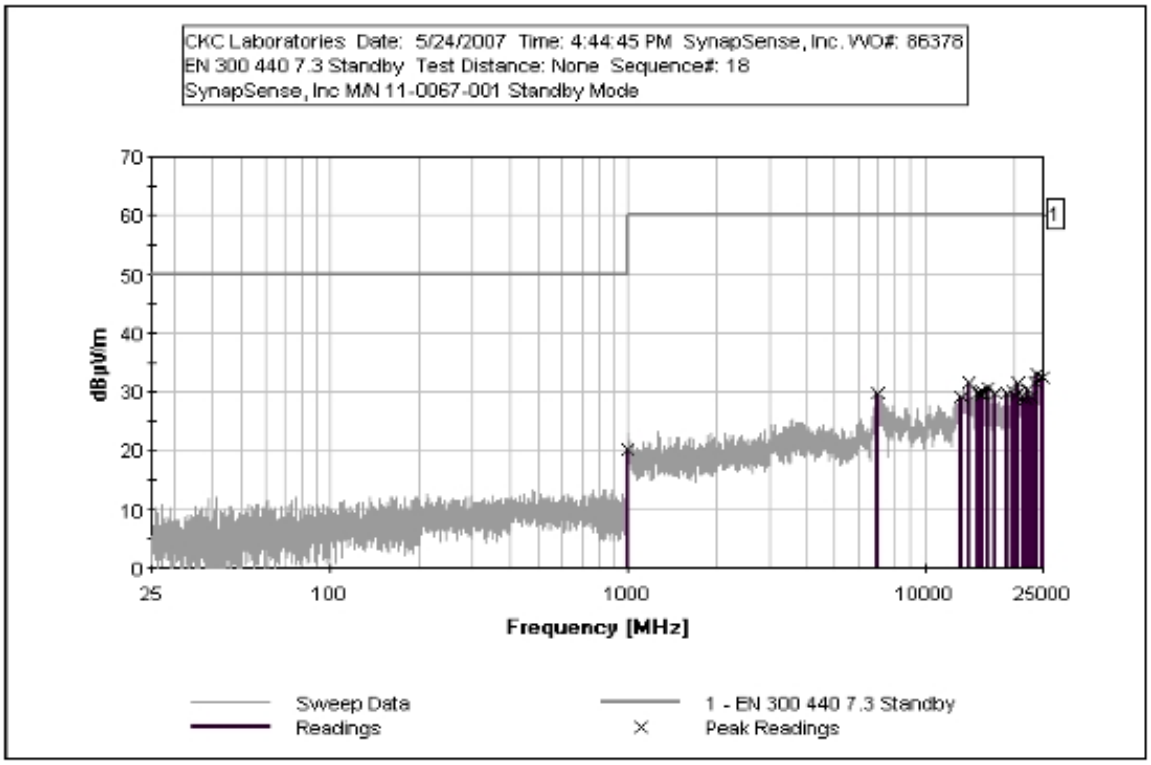
SynapSense wireless devices do not interfere with IT or other equipment in data centers due to the following:

- Ultra-low power transmissions (<1 mW)
- Ultra-low data transmission rate (<1%)
- Non-overlapping frequency range (2400 to 2485 MHz)

Independent testing (Report number ETS07-022A) has shown the transmission power of SynapSense radios is 0.28 mW (101.5 dBµV). This is 86% less than a typical 2 Watt cell phone. In addition, the duty cycle of SynapSense devices is less than 1%. The devices are not radiating power, of any sort, more than 99% of the time. In contrast, cell phones, walkie-talkies, and 802.11 devices radiate anytime they have data to transmit. A typical 802.11 device carries enough traffic in a business environment to radiate 1 Watt of power virtually all of the time.

The operating range of frequencies that the SynapSense device transmits into is from 2400.00 MHz to 2483.50 MHz. SynapSense is not aware of any servers that have non-wireless components that radiate in this frequency range. Out of band emissions, or

spurious emissions into other frequency ranges, are less than 282 nano watts (nW) or less than 71.5 dBµV.



SynapSense has found no evidence of SynapSense sensing devices and gateways causing any interference with the operation of IT equipment or other devices in the data center.

2.6 Summary

SynapSense 802.15.4 devices do not cause any problems with the operation of the existing 2.4 GHz devices in the data center. However, data centers that have multiple 802.11 channels will see 802.11 packets interfering with the operation of the SynapSense devices.

3 Security

SynapSense sensor, router and gateway devices use a mesh network topology to transfer information. This section describes the mechanisms that built into SynapSense systems to ensure protection again security risks.

3.1 Protection against rogue devices

Each SynapSense device is preconfigured with two numbers that associate the device with a specific deployment. The first is a 16-bit personal area network (PAN) identifier that is unique to each 15.4 logical network. The PAN id is used to isolate different PANs and to ensure that packets stay within a specific PAN. The second is a link-layer encryption key that is used to authenticate and encrypt.

Each device in the network is pre-programmed with the same PAN id and encryption key. A device becomes part of network by sending beacons to its neighbors. The beacon packet includes the id and the encryption key. Other devices in the neighborhood use the id and their own key to authenticate the beacon packet. If the beacon packet cannot be authenticated, the network devices do not provide any network infrastructure information to the incoming node. This ensures that devices that have not been pre-programmed with the PAN id and encryption key cannot be part of the network.

3.2 Protection against Snooping

The SynapSense networks use encryption to ensure that external agents cannot snoop the context of the communication on the 15.4 network. The encryption is based on 128-bit **Advanced Encryption Standard** (AES). AES is a popular algorithm used in symmetric key cryptography. SynapSense Stack uses AES in CTR mode for packet encryption from the end of the MAC header (start of NWK) to end of packet. Each packet is "signed" using AES in CBC-MAC mode with 32bits of signature. Devices that have a key programmed and security bits enabled (the default) require that every packet to have a correct CBC-MAC signature. The device will reject incorrect signatures and unsigned packets. In addition, the SynapSense MAC layer uses the link layer encryption key to decrypt the network layer and data payload to forward the information to the network layer.

3.3 Protection against IP-based Access, Intrusion, Passive or Active Attacks

The SynapSense wireless sensor, router and gateway devices do not support any IP-based protocols. They do not provide any support for IP connection initiation, connection establishment, data initiation, or data transfer. The SynapSense wireless networks are completely self-contained networks that are fully isolated from the wired or wireless IP-networks. They therefore cannot be used as an entry point into data center IP network. The integration with the IP-network takes place when the gateway is connected with a SynapSense application server. By fully securing the server that runs the SynapSense wireless data center solution, the overall system architecture ensures that SynapSense system cannot be used to intrude into a client environment.

3.4 Summary

The SynapSense wireless systems achieve security at multiple levels: First, SynapSense devices are not IP-enabled; they therefore are not susceptible to external IP-based passive and active attacks. Second, SynapSense network stack uses 128-AES cryptograph to provide authentication and data encryption, thereby providing security against rogue admissions and snooping.

About the Author:

Dr. Raju Pandey, SynapSense Co-Founder & Chief Technology Officer

He is an Associate Professor in the Department of Computer Science, at the University of California, Davis. While at UCD, Dr. Pandey led the SENSES project, which was funded in part under National Science Foundation grants. Dr. Pandey's research interests are in wireless sensor networks, distributed and parallel systems, system software, programming languages, security and software engineering. Dr. Pandey has authored over 40 papers on sensor networks and distributed computing and has several patents under review. Dr. Pandey holds a Ph.D. from the University of Texas, Austin, an M.S. from the University of Massachusetts, Amherst, and a Bachelor in Technology from the Indian Institute of Technology, Kharagpur.