Secure Information Transfer Between Nearby Wireless Devices

Timothy J. Pierson, Reza Rawassizadeh, Ronald Peterson, David Kotz
Department of Computer Science, Dartmouth College
Hanover, NH, USA 03755

ABSTRACT

Securely transferring data between two devices that have never previously met nor shared a secret is a difficult task. Previous solutions to the problem are susceptible to well-known attacks or may require extensive infrastructure that may not be suitable for wireless devices such as Internet of Things sensors that do not have advanced computational capabilities.

We propose a new approach: using jamming to thwart adversaries located more than a few centimeters away, while still allowing devices in close physical proximity to securely share data. To accomplish this secure data transfer we exploit MIMO antennas and the Inverse-Square Law.

ACM Reference format:
Timothy J. Pierson, Reza Rawassizadeh, Ronald Peterson, David Kotz
Department of Computer Science, Dartmouth College
Hanover, NH, USA 03755
. 2017. Secure Information Transfer Between Nearby Wireless Devices. In *Proceedings of S317, October 20, 2017, Snowbird, UT, USA., ,* 3 pages.
DOI: http://dx.doi.org/10.1145/3131348.3131355

1 INTRODUCTION

Analysts predict *billions* of everyday devices will soon become "smart" with the addition of wireless communication capabilities [7]. These newly connection-enabled Internet of Things (IoT) devices are envisioned to share data and actuator control information between themselves; with new mobile devices entering and exiting a particular environment on a regular, but difficult to predict basis. Additionally, some of the information the devices share may be privacy sensitive or have security implications. This situation implies that devices that have never met, nor shared a secret, must somehow have a way to securely communicate.

We propose using jamming from a multiple-antenna device to cover information exchanged with a target device in close physical proximity as shown in Figure 1. Here a multi-antenna device uses antenna A_1 to send a data signal to the target device located at distance d_1, while using a second antenna A_2 located d_2 from the target to transmit barrage jamming (random noise).

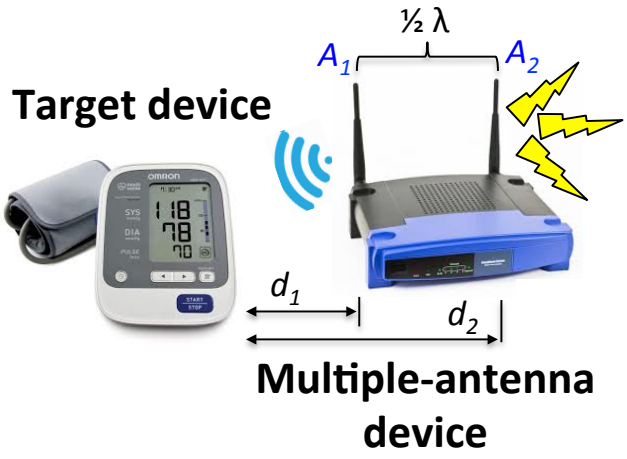

Figure 1: A multiple-antenna device uses antenna A_1 to send a data signal to a target device located at distance d_1, while antenna A_2 located d_2 from the target transmits barrage jamming.

While Figure 1 depicts a multi-antenna router communicating with a single-antenna blood pressure monitor, multiple antennas are becoming common in mobile devices, and in fact multiple antennas are required to take advantage of some of the more advanced features such as beam forming in Multiple-Input, Multiple-Output (MIMO) configurations of 802.11n and 802.11ac [4]. To perform effective beam forming, antennas are typically separated on devices by one-half wavelength [6].

The idea is to leverage existing MIMO radio chains and antennas to create a situation where the legitimate target device is able to correctly receive the transmitted data, despite the presence of jamming, while denying a more distant adversary the ability to recover the data. In the next section we review some background information useful to understanding our approach to this problem.

2 BACKGROUND

Our approach to overcoming jamming for devices in close physical proximity with each other relies on the fact that radio waves attenuate proportionally with the square of the distance between the transmitter and receiver. This relationship, driven by the Inverse-Square Law, is captured by the Friis transmission model [6] which states:

$$P_r = P_t G_t G_r \left(\frac{\lambda}{4\pi d}\right)^2 \quad (1)$$

S3'17, , October 20, 2017, Snowbird, UT, USA.
 ISBN 978-1-4503-5145-4/17/10...$15.00
DOI: http://dx.doi.org/10.1145/3131348.3131355

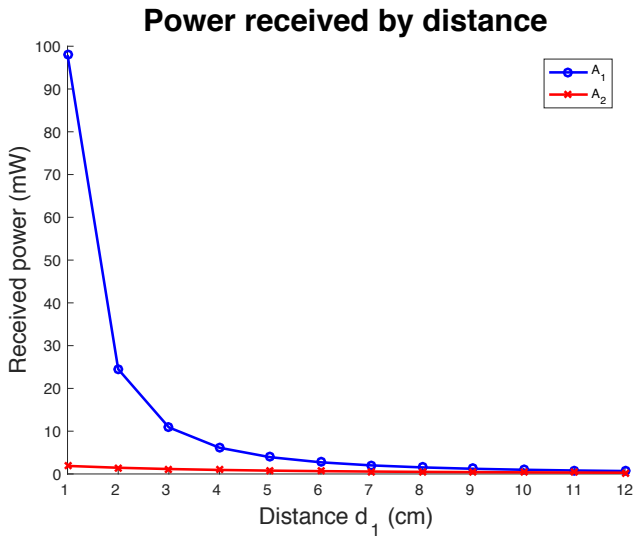

Figure 2: Expected power received from two transmitting antennas, each sending a 20 dBm signal, with antenna A_1 located at distance d_1 cm from the receiver and antenna A_2 located $d_2 = d_1 + \lambda/2$ cm from the receiver.

where P_r is the power (in mW) at the receiving antenna, P_t is the power transmitted, G_t is the gain of the transmitting antenna, G_r is the gain of the receiving antenna, λ is the wavelength of the signal, and d is the distance between the transmitting and receiving antennas. From Equation (1) it is clear that if the distance d between transmitter and receiver is reduced by one-half, then the received power is increased by a factor of four.

The relationship between distance and received power is particularly stark when a receiver is in close proximity to a transmitter. Figure 2 shows the expected received power according to Equation (1), where a transmitting antenna A_1 is located d_1 cm away from a receiver, and a second transmitting antenna A_2 transmits a signal of equal magnitude to the signal from A_1 but is located at distance d_2. Here d_2 is one-half wavelength farther away from the receiver than A_1 (e.g., $d_2 = d_1 + \lambda/2$). In Figure 2 we model a 20 dBm Wi-Fi signal transmitted on channel 1's center frequency of 2.412 GHz, which has wavelength $\lambda \approx 12.5$ cm.

We see in Figure 2 that when a receiver is very close to a transmitter (say A_1 is 4 cm away), it receives a significantly stronger signal than a signal from a transmitter located only one-half wavelength farther away (about 10 cm $\approx$ 4 cm + 12.5/2 cm, which is roughly 2.5 times farther than A_1 in this example). When the devices are farther away from the receiver (A_1 is more than about 7 cm away), the received signal strength from each transmitter is virtually identical.

We use this difference in signal strength to provide secure communications to a nearby legitimate target device while denying a more distant adversary the ability to recover the data.

3 APPROACH

In this paper we focus on Wi-Fi to illustrate our concept, although other protocols could be used as well. We begin by positioning a target device's antenna in close physical proximity to a multiple-antenna device's antenna A_1, aligned so that A_2 is maximally distant from the target, as shown in Figure 1. Because multiple antennas on a device are typically separated by a fixed distance of one-half wavelength, $d_2 = d_1 + \lambda/2$.

Once the multiple-antenna device senses a clear Wi-Fi channel, it begins to transmit barrage jamming from antenna A_2. After jamming has been initiated, the multiple-antenna device uses antenna A_1 to send normal Wi-Fi frames to transfer data to the target device. Once all frames have been transmitted, the multiple-antenna device terminates jamming on A_2. In this way, all frames are sent under the cover of jamming. Figure 2 shows that the Wi-Fi frame will be received by the nearby target with much higher energy than the jamming, but an adversary located more than about 7 cm will receive approximately equal signal strength from each antenna.

The key to success is to ensure that there is enough separation in signal strength between the data and jamming signals at the nearby target so that target can recover the data, while the roughly equal strength of data and jamming signals ensures a more distant adversary cannot recover the data. Models have been developed to estimate the Bit Error Rate (BER) expected in the presence of noise (natural background noise plus our jamming in this case). These models involve estimating the energy per bit, E_b, of the data transmitted, the noise power spectral density, N_0, which represents the amount of noise per Hertz of bandwidth, and the Modulation and Coding Scheme (MCS) used for data transmission.

Wi-Fi has a number of modulation options it can employ to send data, including Binary Phase Shift Keying (BPSK), Quadrature Phase Shift Keying (QPSK), and Quadrature Amplitude Modulation (QAM). Additionally, Wi-Fi can use convolutional coding to send redundant copies of bits to boost reception reliability at the expense of throughput (e.g., duplicate copies mean a higher likelihood a data bit is correctly received, but fewer data bits are sent per fixed period of time). The most basic MCS in Wi-Fi is BPSK with 1/2 coding. In this case each transmitted symbol represents one bit, and each bit is duplicated (e.g., the data rate is 1/2 because each bit has two copies in the transmitted message).

We can use the expected received power given by Equation (1) to estimate E_b, and assuming an Additive White Gaussian Noise (AWGN) channel, we can model the expected BER for various Wi-Fi MCS types. For BPSK the expected BER is [2]:

$$P_s = P_b = Q\left(\sqrt{\frac{2E_b}{(N_0 + N_j)}}\right) \quad (2)$$

where P_s is probably of a symbol error, P_b is the probably of a bit error (same as P_s because each symbol represents one bit in BPSK), E_b is the energy per bit, N_0 is the noise power

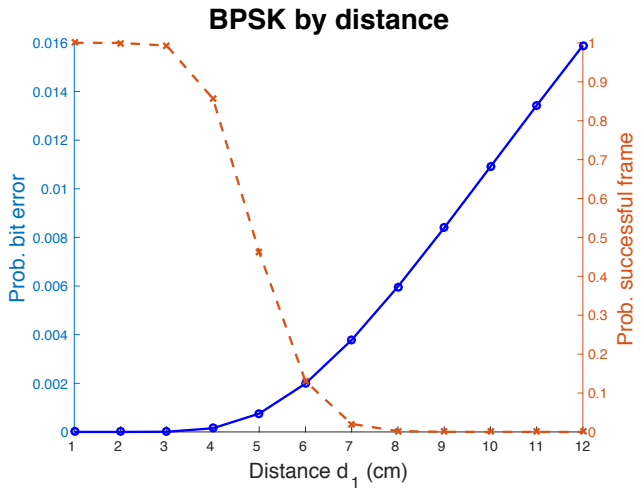

Figure 3: (Left) Expected bit error rate with antenna A_1 sending BPSK Wi-Fi frames located at distance d_1 from a target device while antenna A_2 located at distance $d_2 = d_1 + \lambda/2$ sends a jamming signal. (Right) Estimated probability a frame is received with no bit errors.

spectral density of the environment, N_j is the power spectral density of the jamming signal, and where the Q function is:

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{x^2}{2}} dx. \quad (3)$$

Using the estimated power received from a data signal sent by antenna A_1 located at distance d_1 to estimate E_b and a jamming signal sent by antenna A_2 at distance d_2 to estimate N_j, Equation (3) yields Figure 3. Examining the left axis, we see that the probability of a bit error is low while the multiple-antenna device and the target are physically close together (e.g., d_1 is small), but increases rapidly as d_1 increases. Assuming a Wi-Fi frame contains 1,024 bits of data, the probability that a frame is received with no errors is plotted on the right axis.[1] We see the probability that a frame is successfully received with no errors is extremely low as d_1 increases beyond about 7 cm. These estimates suggests a physically close target device should be able to reliably receive Wi-Fi BPSK encoded frames while a more distant adversary cannot.

4 RELATED WORK

Data transmission in the presence of noise and intentional jamming has been well studied. While there are many uses for jamming, "friendly jamming" attempts to use jamming to accomplish a specific purpose such as secure data transfer. Al-Mefleh and Al-Kofahi published a comprehensive survey of friendly jamming covering 182 academic papers [1]. One paper in particular is close to our approach. Gollakota developed a system called *Shield* that uses a necklace-worn friendly jammer to protect implanted medical devices from accepting outside commands [3]. Our system is different in that it conveys information to a nearby device rather than preventing the target from receiving potentially malicious data.

Separately, Pierson et al. presented a project called *Wanda* that exploits the difference in signal strength between two nearby antennas to securely transmit data to a target device [5]. Wanda, however, can only transmit *one bit* with each Wi-Fi packet, whereas our proposal can send a much larger data payload – 2,304 *bytes* in each Wi-Fi packet [4] – making it more than 18,000 times faster than Wanda.

[1] Forward Error Correction (FEC) may be able to correct some erroneous bits.

5 CONCLUSION

We believe that as the number of deployed IoT devices grows, securely transferring data between them will become an increasingly difficult problem. Manually entering secret keys on each device will likely become extraordinarily cumbersome if predictions of the number of IoT devices coming soon are even remotely accurate. To alleviate that problem, we intend to explore the approach presented here more fully in future work.

6 ACKNOWLEDGEMENT

This research results from a research program at the Institute for Security, Technology, and Society at Dartmouth College, supported by the National Science Foundation under award number CNS-1329686.

The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the sponsors.

REFERENCES

[1] Haithem Al-Mefleh and Osameh Al-Kofahi. Taking advantage of jamming in wireless networks: A survey. *Computer Networks*, 99:99–124, 2016. DOI doi.org/10.1016/j.comnet.2016.02.011.

[2] Marvin Frerking. *Digital signal processing in communications systems*. Springer Science & Business Media, 2013.

[3] Shyamnath Gollakota, Haitham Hassanieh, Benjamin Ransford, Dina Katabi, and Kevin Fu. They can hear your heartbeats: non-invasive security for implantable medical devices. *SIGCOMM Computer Communication Review*, 41(4):2–13, August 2011. DOI 10.1145/2018436.2018438.

[4] Institute of Electrical and Electronics Engineers. 802.11 standard. Online at http://standards.ieee.org/about/get/802/802.11.html, visited 7/12/2017.

[5] Timothy J. Pierson, Xiaohui Liang, Ronald Peterson, and David Kotz. Wanda: securely introducing mobile devices. In *IEEE International Conference on Computer Communications (INFOCOM)*, pages 1–9, April 2016. DOI 10.1109/INFOCOM.2016.7524366.

[6] Theodore S. Rappaport. *Wireless communications: principles and practice*. Prentice Hall, 2002.

[7] Rob van der Meulen. Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015. Online at http://www.gartner.com/newsroom/id/3165317, visited 7/12/2017.