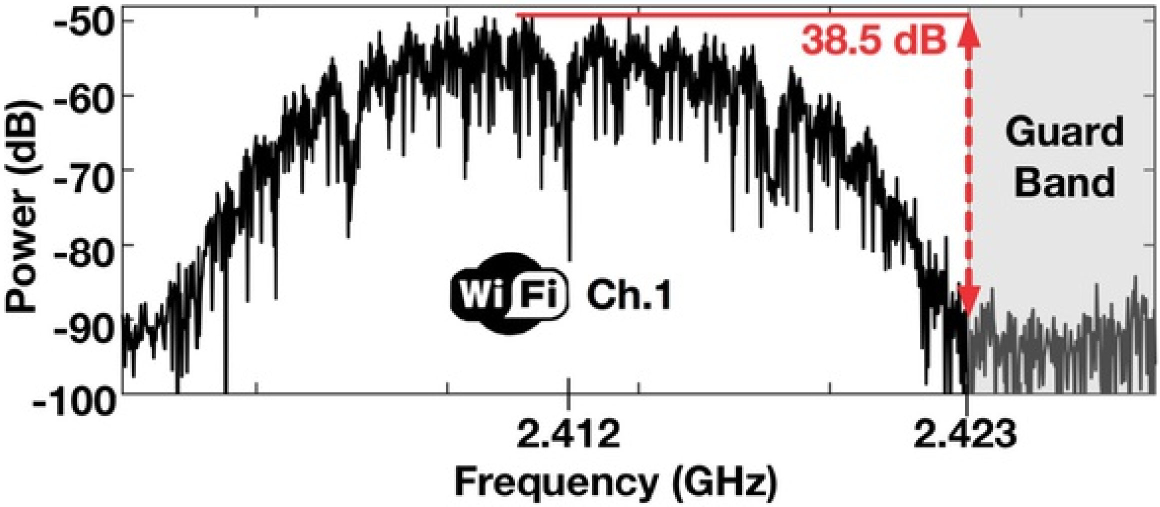
GEORGE MASON UNIVERSITY Department of Computer Science

New technique can enhance reliability for wireless device automation protocol



Researchers have devised a way to significantly improve wireless data transfer reliability.

by Johnny Pesavento

Researchers from George Mason University have devised a way to significantly improve wireless data transfer reliability for devices that use a networking protocol called ZigBee. When sharing a frequency spectrum for data transfer with a normal Wi-Fi network, the majority of data transmitted between ZigBee devices can become corrupted due to interference from unrelated devices on the Wi-Fi network. However, by taking advantage of a small, unused portion of the Wi-Fi network's frequency spectrum called a guard band, almost every ZigBee data packet can be transmitted without corruption even if the Wi-Fi network is experiencing heavy traffic.

How data can become corrupted

A packet is a small portion of data that can be sent over a wireless network to communicate with other devices. However, sometimes a sent packet is unable to be received by the intended device. This failure to communicate is called packet loss, and it can lead to data corruption for affected devices. To protect against this issue, ZigBee devices currently have to retransmit packets until they are successfully received, a very energy-expensive process.

Packet loss commonly occurs when there are many wireless devices in close proximity transmitting data on the same frequency band. The many signals being transferred at the same frequency can cause some packets to become lost after being sent. This is called signal interference.

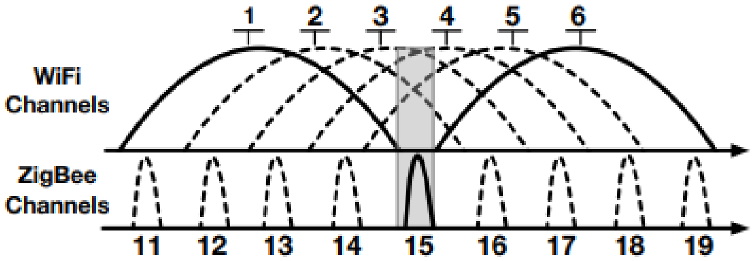
Signal interference with ZigBee

ZigBee is a wireless networking protocol, just like Wi-Fi and Bluetooth. Its main use is to connect devices in the Internet of things (IoT) with each other. The IoT is simply a network of everyday physical devices. For example, you could turn on a toaster in your kitchen by pressing a button in your bedroom when you wake up. When the button is pressed, it sends a signal to the toaster so that it turns on. ZigBee automation is not limited to the home. It can be used to automate procedures in factories, hospitals, and almost any other workplace.

Wi-Fi, Bluetooth, and ZigBee each use a frequency band around 2.4 GHz to send packets. These networks are often called heterogeneous because they connect different types of devices. Congestion on any one of these heterogeneous wireless networks can lead to packet loss for any 2.4GHz device within range due to signal interference no matter which protocol the device is using. This specific type of signal interference is called cross-technology interference.

Finding a solution

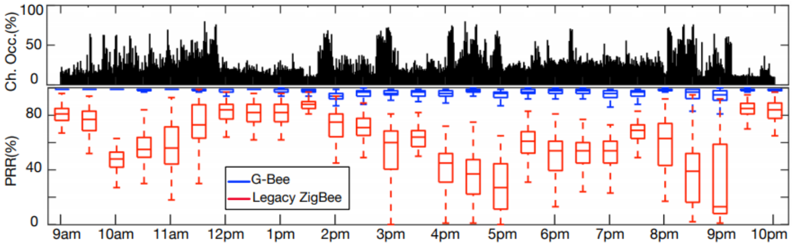
In order to eliminate cross-technology interference, PhD candidates Yoon Chae and Shuai Wang from George Mason University's Department of Computer Science and Prof. Song Min Kim invented a new technique called G-Bee. G-Bee detects nearby 2.4GHz Wi-Fi networks (802.11b/g/n) and establishes a ZigBee frequency range outside of the Wi-Fi's in what is called the guard band. The guard band is a small frequency range devoid of signals adjacent to but outside of Wi-Fi channels. Guard bands are a fraction of the size of the space needed to house a Wi-Fi channel; however, ZigBee channels are much smaller than Wi-Fi channels and are able to fit in guard bands. This solution effectively safeguards communication between ZigBee devices and decreases congestion on both the Wi-Fi and ZigBee networks.



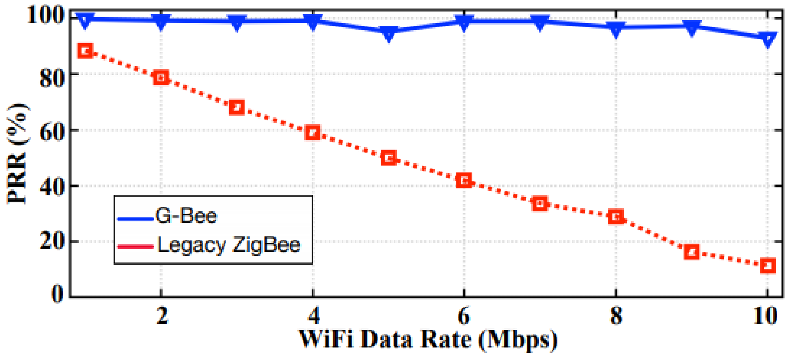
G-Bee works as an extension to ZigBee on the sender side. The technology experimentally determines the duration, frequency, and time of the guard band and then transmits signals on that channel. A robust process called narrowband decoding allows the device to gather information about the Wi-Fi network in real time and deduce information about the guard band. When compared to other solutions, this method is unique, as others generally rely on probability and prospective calculations.

Applying the technology

Implementing G-Bee drastically improves the duty cycle efficiency, data transmission speed, and packet reception rate for ZigBee devices even when an ambient Wi-Fi network is heavily saturated. When an experimental test was performed in a George Mason University library with a prototype G-Bee device, the percentage of packets received remained at or above 93% for the duration of the experiment (over 12 hours), whereas the percentage of legacy ZigBee packets received reached as low as 14%. Additionally, at times of heavy traffic, G-Bee's packet reception ratio (PRR) was up to 6.5 times more than legacy ZigBee's.



Several more tests were conducted to test the reliability of G-Bee in real world scenarios. When tested at a coffee shop in Washington, D.C., a shopping mall in Northern Virginia, and a residential area, the G-Bee data transfer speeds were consistently high enough to support nearly every IoT implementation even in the vicinity of saturated Wi-Fi networks. Another test also showed that G-Bee has the potential to save 83% more energy than legacy ZigBee, further demonstrating that G-Bee is practical and reliable for use in the real world.



The study, titled *Exploiting WiFi Guard Band for Safeguarded ZigBee*, was conducted by Yoon Chae, Shuai Wang, and Song Min Kim. It can be found at https://doi.org/10.1145/3274783.3274835.

Posted 2 weeks, 3 days ago

← Previous: Creating Foldable Polyhedral Nets

Next: Nine Undergraduates Participate in NSF REU Site at CS@Mason →