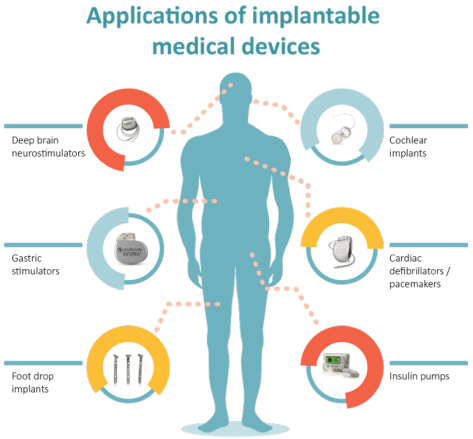
Countering Cross-technology Jamming Attack

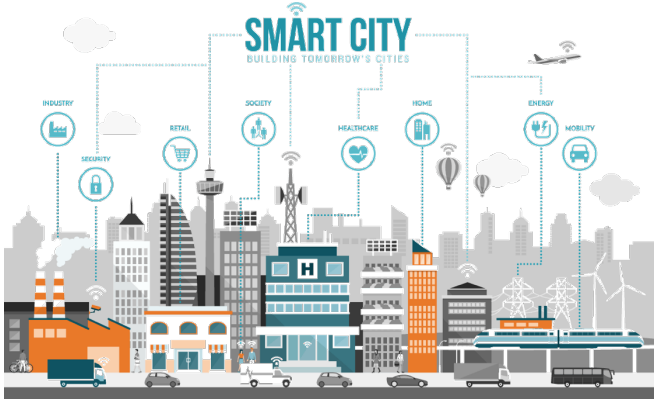
Zicheng Chi[1], Yan Li[1], Xin Liu[1], Wei Wang[1], Yao Yao[1], Ting Zhu[1], and Yanchao Zhang[2]

University of Maryland, Baltimore County[1]

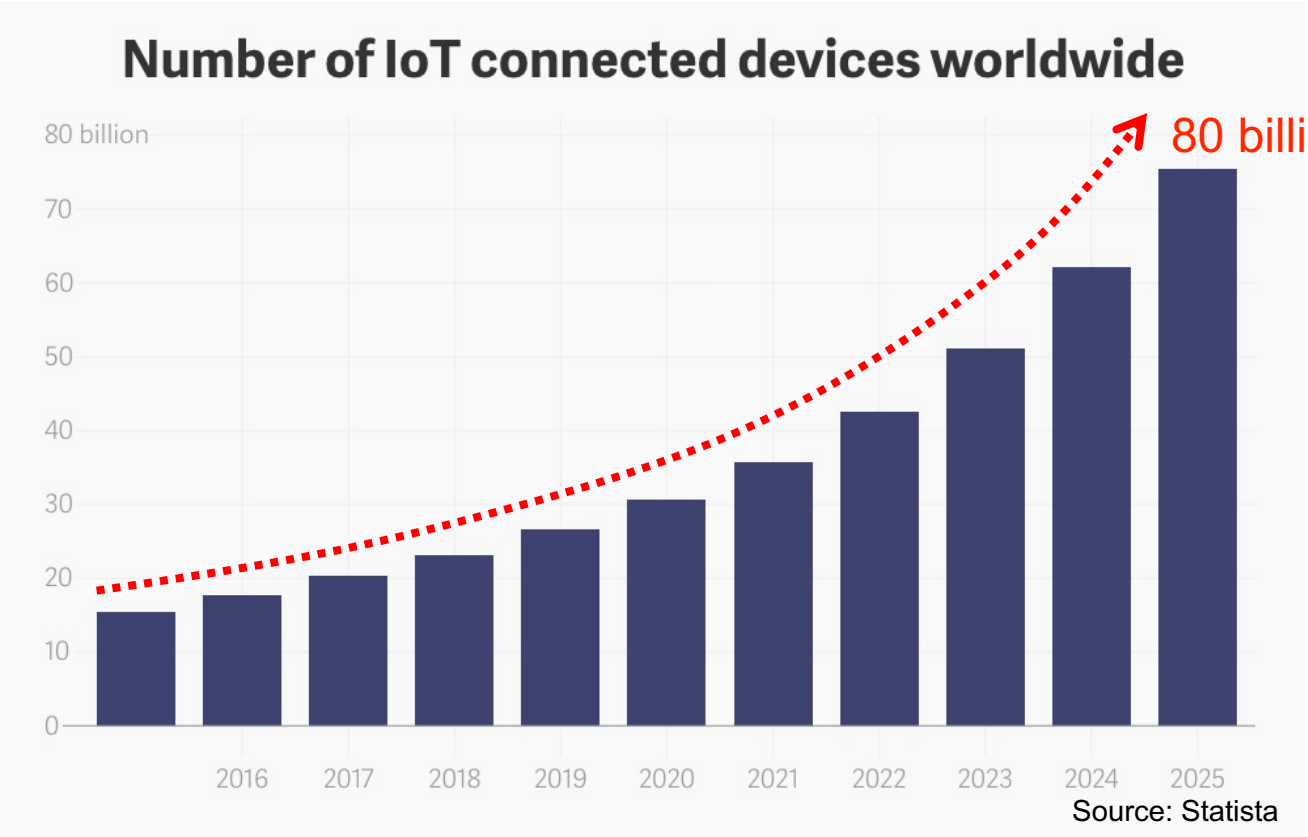
Arizona State University[2]

The Internet of things is changing the world





The Rapidly Growing Trend of IoT Devices



Spectrum is shared by IoT Devices

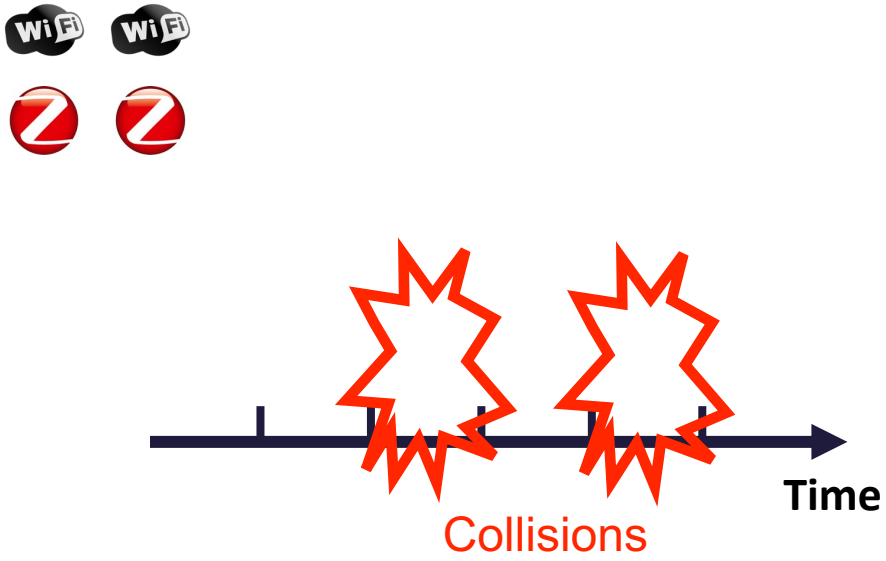
WiFi

Bluetooth

2.4 GHz ISM band

ZigBee

To share the spectrum and avoid collision, we use CSMA



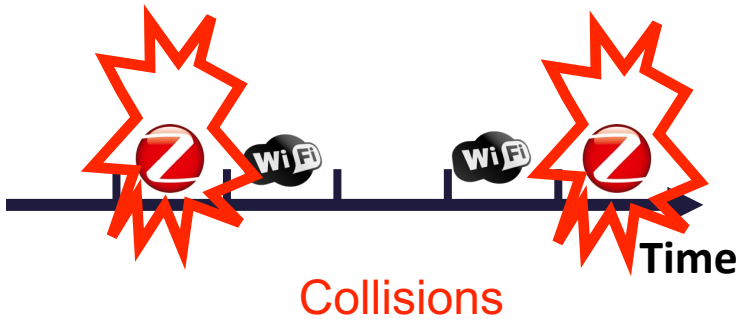
To share the spectrum and avoid collision, we use CSMA

- Carrier-sense multiple access **(CSMA)**

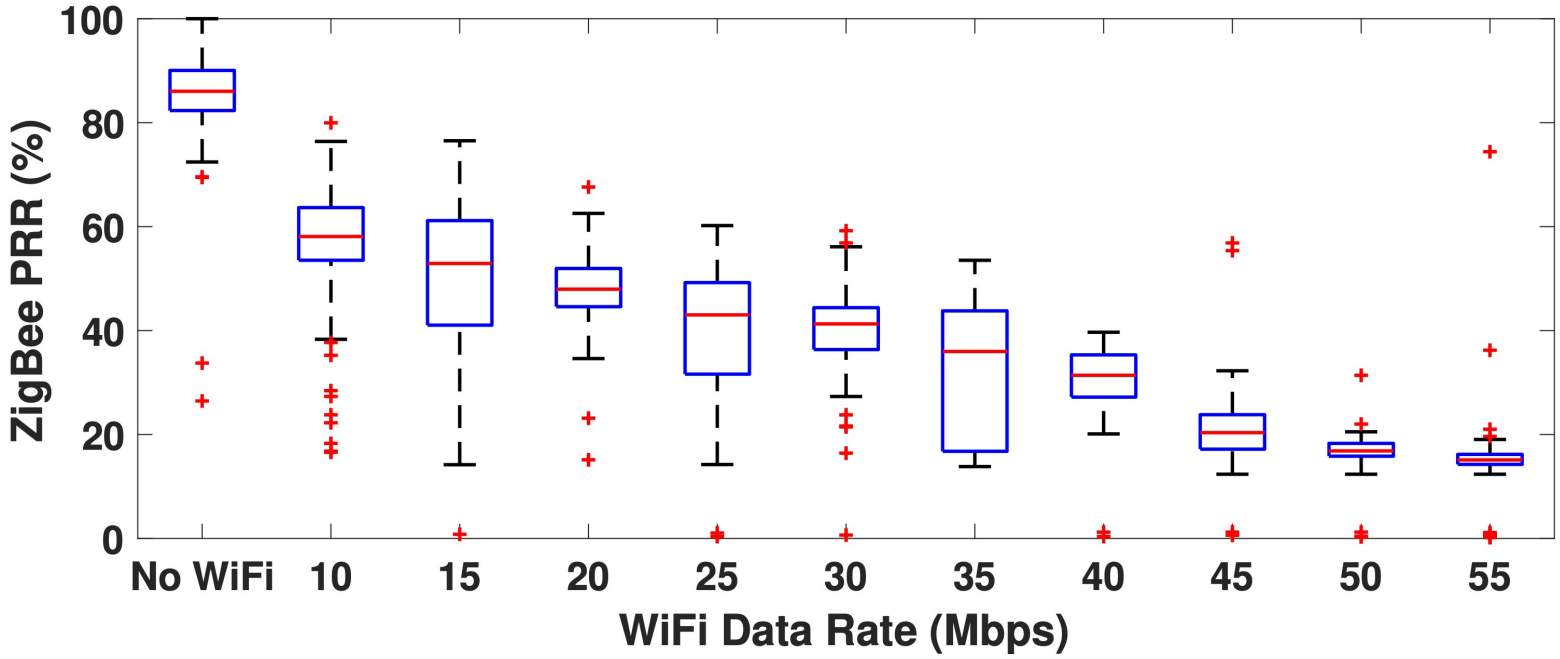
What if a malicious WiFi device intentionally disables CSMA?

ZigBee device is concealed jammed by WiFi device

- Channel Overlapping
- Wider Bandwidth
- WiFi is everywhere



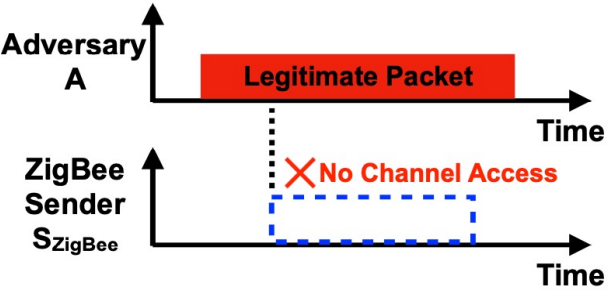
ZigBee Packet Reception Ratio (PRR) under concealed jamming

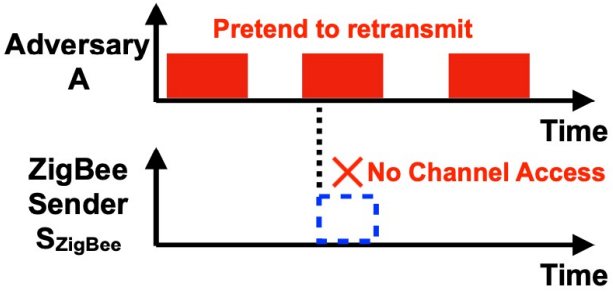


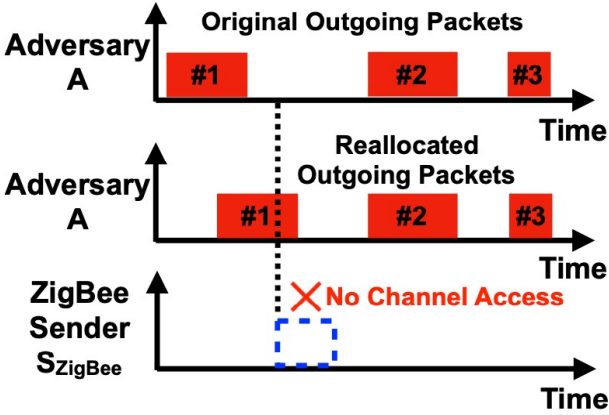
Impact on popular IoTs

Brand	Model	Type	ZigBee Profile	Power source	Required Gateway	Jamming Impact
Bosch	ISW-ZPR1-WP13	Pro-Grade Motion Detector	Home Automation	AA Battery	SmartThings Hub	Severe
Centralite	3310-G	Temp & Humidity Sensor	Home Automation	CR-2 Battery	SmartThings Hub	Moderate
Centralite	3323-C	Door Sensor	Home Automation	CR-2450 Battery	SmartThings Hub	Severe
Centralite	3315-C	Water Leak Sensor	Home Automation	CR-2 Battery	SmartThings Hub	Severe
Centralite	3155-wC	Smart Switch	Home Automation	Wall-Powered	SmartThings Hub	Mild
GE	45856GE	Smart Switch	Home Automation	Wall-Powered	Amazon Echo Plus	Mild
GWi	G4-MG-SE-GM-V2	Gas Meter	Smart Energy	Lithium Battery	Smart Energy Hub	Mild
IKEA	50383505	Motion SENSOR	Light Link	CR-2032 Battery	Hue Bridge	Severe
LEVITON	DL6HD-1BZ	DECORA Smart Dimmer	Smart Energy	Wall-Powered	SmartThings Hub	Mild
LEVITON	ZSS10-N0Z	DECORA Smart Switch	Smart Energy	Wall-Powered	SmartThings Hub	Mild
Philips	464602	Motion SENSOR	Light Link	AAA Battery	Hue Bridge	Severe
Samsung	F-IRM-US-2	Motion Sensor	Home Automation	CR-2477 Battery	SmartThings Hub	Severe
Samsung	F-ARR-US-2	Arrival Sensor	Home Automation	CR-2032 Battery	SmartThings Hub	Moderate
Samsung	F-MLT-US-2	Door/Window Sensor	Home Automation	CR-2450 Battery	SmartThings Hub	Severe
Samsung	F-WTR-US-2	Water Leak Sensor	Home Automation	CR-2 Battery	SmartThings Hub	Severe
Samsung	HSR761H	Smoke & CO Sensor	Home Automation	Wall-Powered	SmartThings Hub	Severe
SYLYANIA	E21266	Motion Sensor	Light Link	CR-2 Battery	Wink Hub	Severe
SYLYANIA	SYL-74388	Contact Temperature Sensor	Light Link	CR-2450 Battery	Wink Hub	Moderate
Visonic	MCT-340	Door Window Sensor	Home Automation	CR-2035 Battery	SmartThings Hub	Severe
Visonic	MP-841	PIR Detector	Home Automation	CR-123A Battery	SmartThings Hub	Severe
Visonic	GB-540	Acoustic Glass-break Detector	Home Automation	CR-123A Battery	SmartThings Hub	Severe

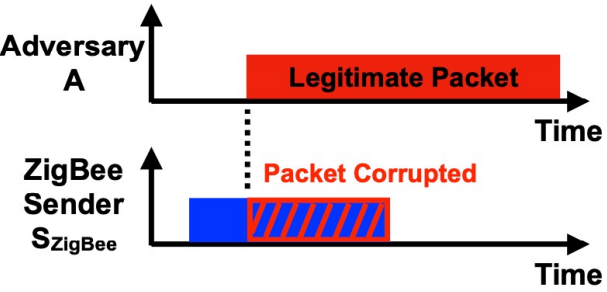
Attack model 1: Channel Access Prevention

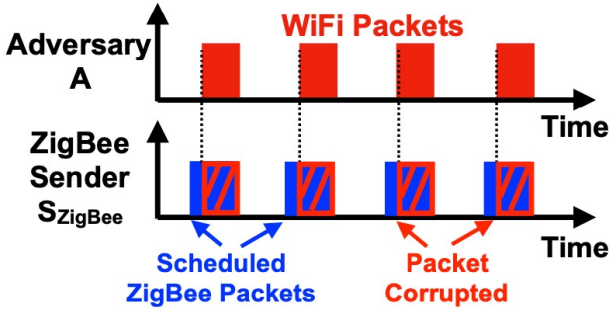


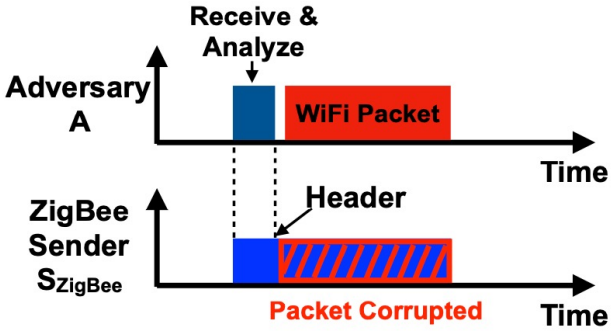




Attack model 2: Packet Corruption







Basic Idea of defense

- Instead of dropping WiFi and ZigBee collided signals, we disentangle the combined signals to extract ZigBee signal

Observation

WiFi Symbol Rate: the WiFi subcarriers (312.5 KHz) of the OFDM signal carry data at the symbol rate of 250,000 symbols per second.
ZigBee Chip Rate: the ZigBee's OQPSK-DSSS modulation scheme carries data at the chip rate of 2,000,000 chips per second.

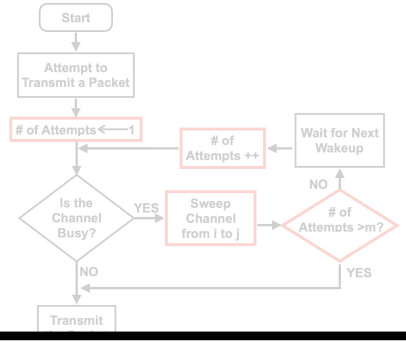
WiFi symbol rate and ZigBee chip rate reveal signal varying speed in WiFi and ZigBee signals, respectively. By utilizing this property, it is possible to disentangle the two signals if they are collided with each other.

ZigBee Signal Recovering

- **First**, utilizing the diverse chip/symbol rate of ZigBee and symbol to implement a band-stop filter bank.
- **Second**, the distorted ZigBee signals can be compensated by the robust DSSS scheme.
- **Third**, using FEC to increase the probability of correct receptions

Other Challenges

Concealed Jamming Detection



Handling Partially Collided Packets

Algorithm 1 Correlation Module

Input: $R[n]$, $G_{WiFi}[n]$ $n \in [0, T_{WiFi\_symbol}]$, and $G_{ZigBee}[n]$ $n \in [0, T_{ZigBee\_symbol}]$.
Output: $S_{ZigBee}[n]$ and $S_{Jam}[n]$.

1: $C_{WiFi} = \max_{k \in [0, T_{WiFi\_symbol}]} \sum_{n=0}^{\infty} G_{WiFi}[n-k]y[n]$;
2: $C_{ZigBee} = \max_{k \in [0, T_{ZigBee\_symbol}]} \sum_{n=0}^{\infty} G_{ZigBee}[n-k]y[n]$;
3: **if** $C_{WiFi} > C_{ZigBee}$ **then**
4: $S_{Jam}[n] = R[n]$;
5: **else**

Please refer to our paper for details

Handling an Adversary using a Different WiFi Channel

Experimental Setup

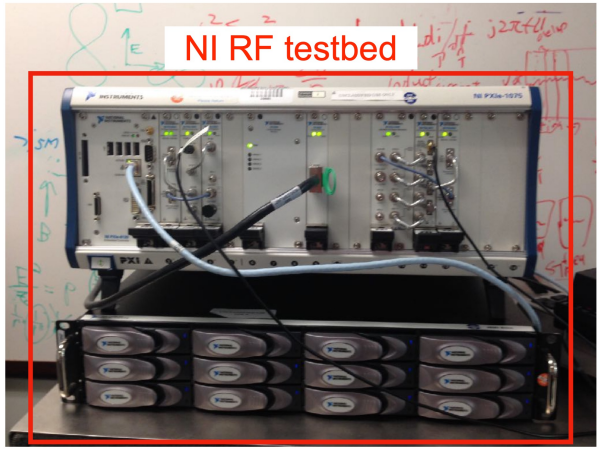
Baseline:

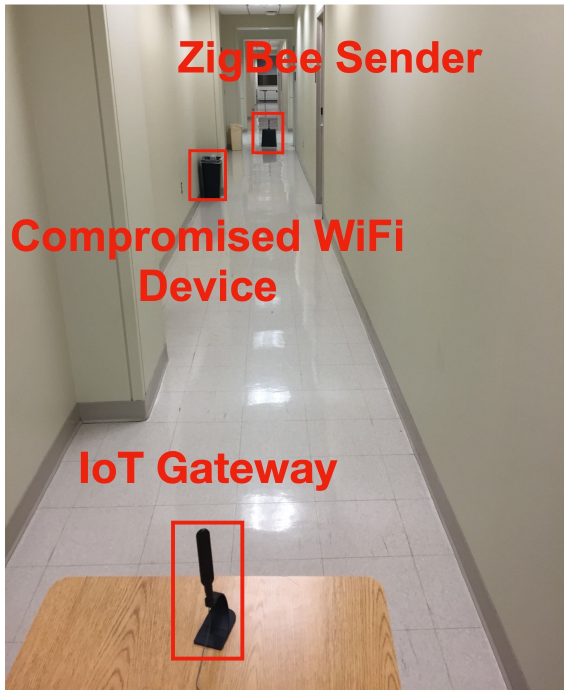
- No Attack
- Victim

Protege: our defending scheme

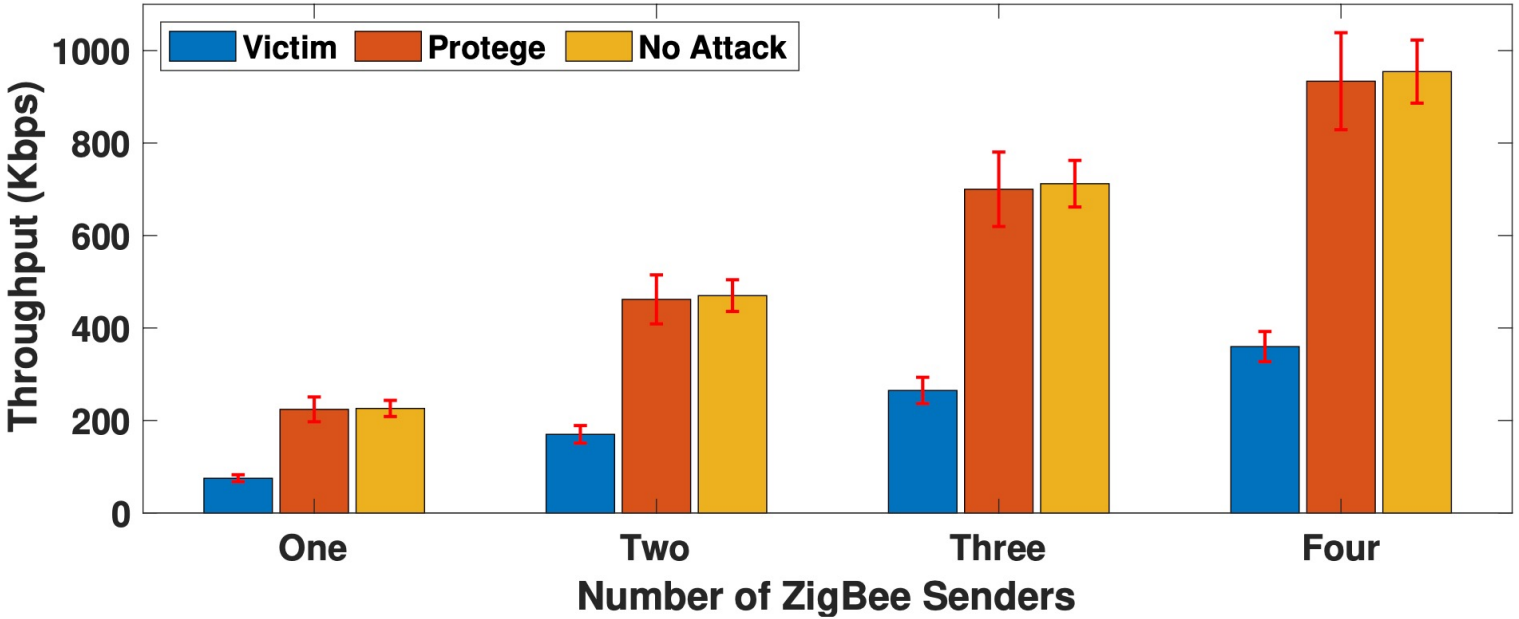
Metrics:

- Throughput
- Latency
- Bit Error Rate
- Packet Reception Ratio



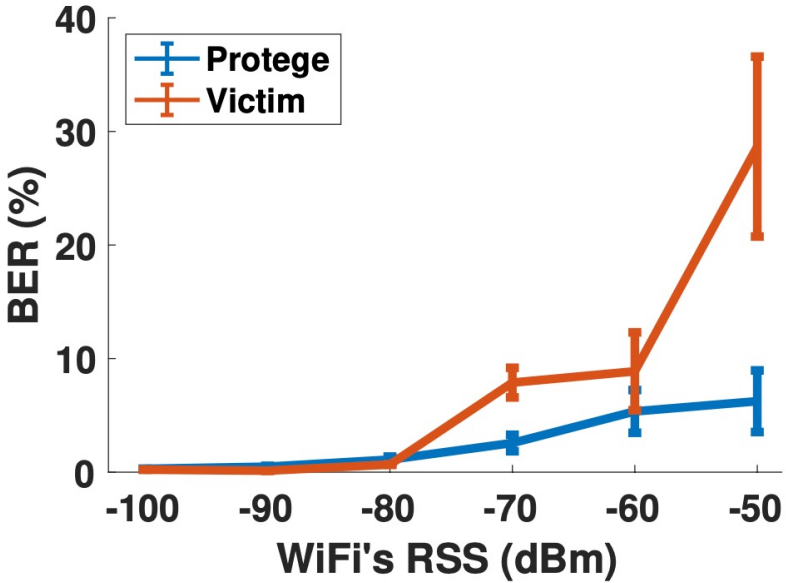


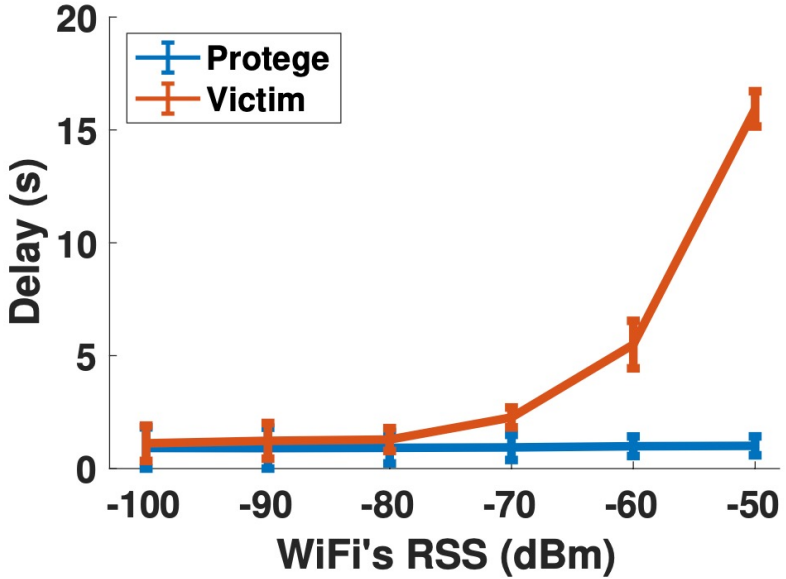
Overall throughput performance



- Our defense scheme shows much better performance than “victim” and very similar to “no attack”.

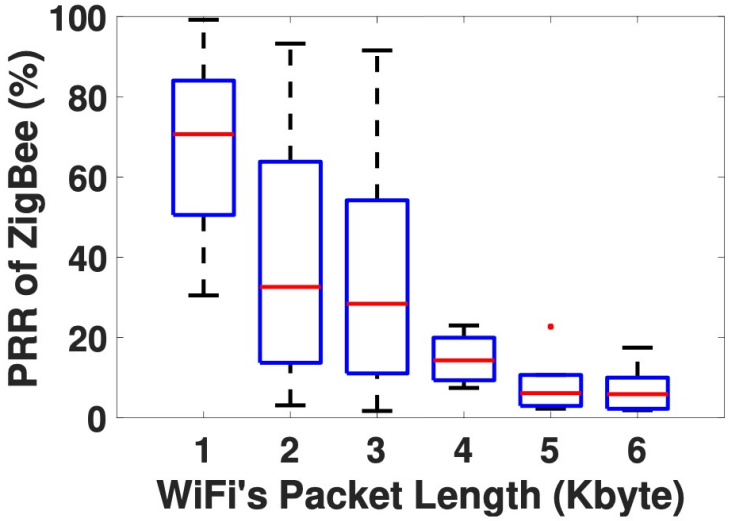
Impact of WiFi Signal Strength



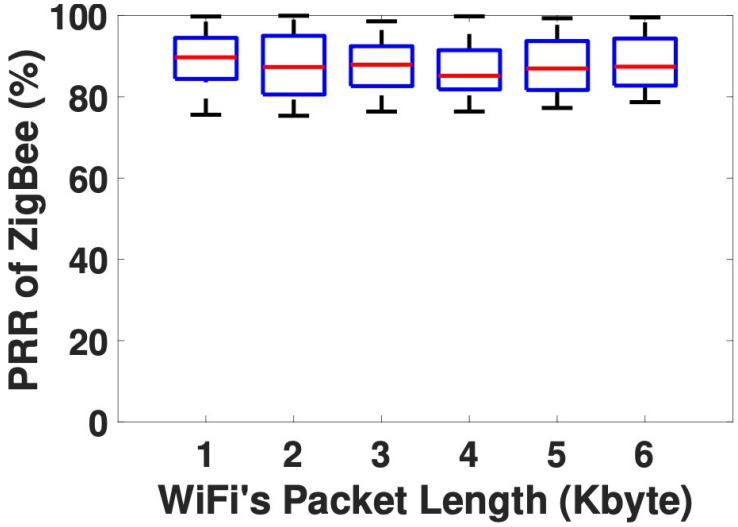


- Higher WiFi signal strength affects “victim” more while “protege” keeps stable

Overall throughput performance



(a) Victim



(b) Protege

- "Victim" is vulnerable to longer WiFi packets while "protege" is stable.

Conclusion

- We discovered a new set of attacks: concealed jamming attack in IoT networks.
- We proposed methods to defend against these attacks. Our generic scheme has the potential to be applied to defend from attacks among other spectrum sharing devices.
- Our extensive evaluation shows the packet reception delay can be reduced by a factor of 16 while the jammed device is protected by using our proposed method.

Q & A

Thanks!