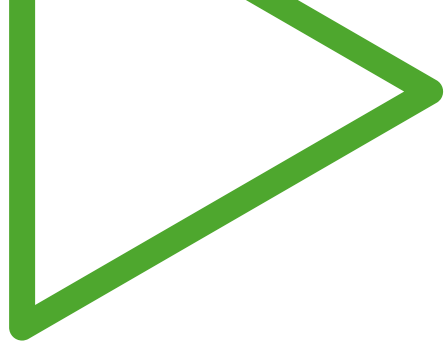
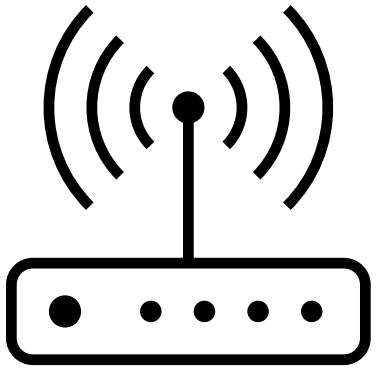
Hackers with Radios

Security and the Physical Layer

Presented by: Mark Megarry, 2I0OMW





Agenda


Introduction
Threat modelling
Eavesdropping
Replay attack
•Hardware
•Replay protection
Relay attack
Attack mitigations/wrap-up

Speaker profile

- PhD student with QUB's Centre for Secure Information Technologies (CSIT)
- Project: Security of 6G Open Radio Access Networks (O-RAN)
- How did I get here:
  - Interest in radio science and comms engineering from classes
  - Internship and Masters project involving antenna array design
  - General interest hardware security

QUEEN'S UNIVERSITY BELFAST | CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Disclaimer: Please don't break the law

THIS IS NOT LEGAL ADVICE

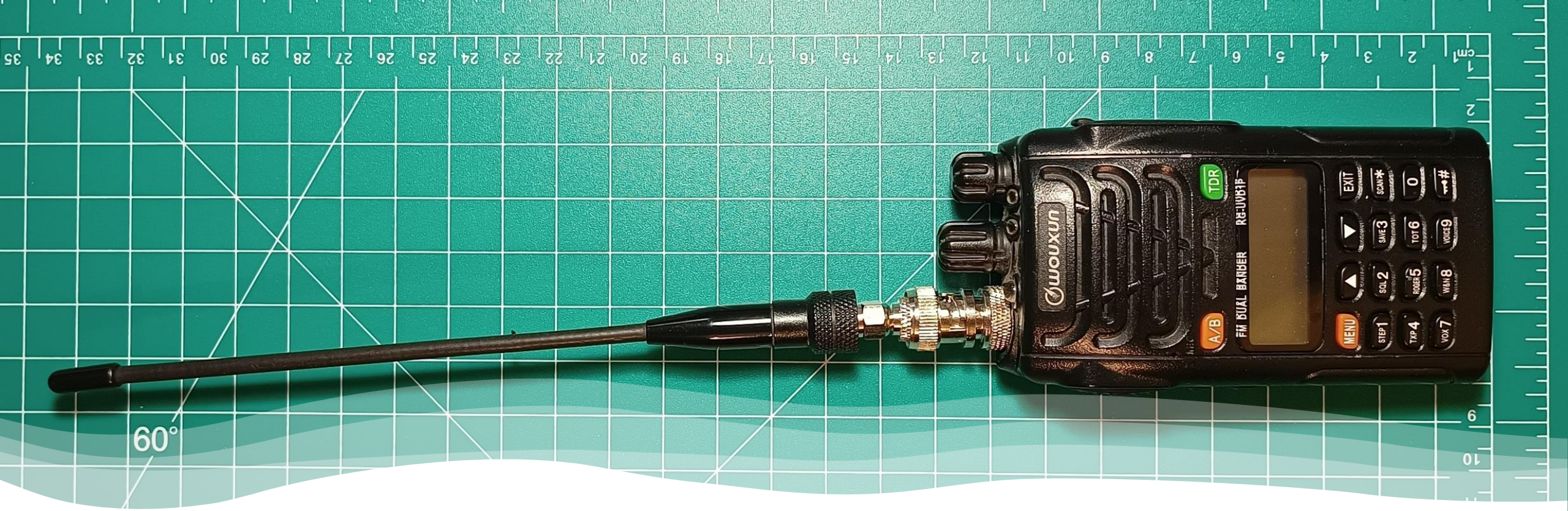
Cybercrime

- Criminal Justice Act 2017 offences include [1]:
  - Intercepting transmission of data without lawful authority
  - Interfering with data without lawful authority
  - Accessing information systems without lawful authority
- Penalties include prison sentences

Spectrum law

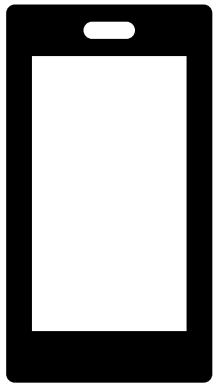
- The radio spectrum is a shared resource
- ComReg govern how it's shared in Ireland
- Know what frequencies you can transmit on, and how you should be transmitting on them!

[1] Government of Ireland, "Criminal Justice (Offences Relating to Information Systems) Act 2017 ." Available: https://www.irishstatutebook.ie/eli/2017/act/11/enacted/en/print.html (Accessed May 18, 2025)

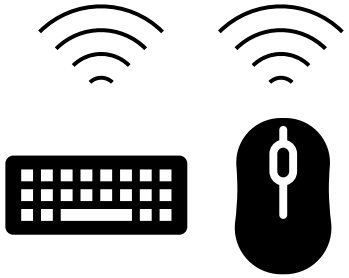


Radios: They’re everywhere!

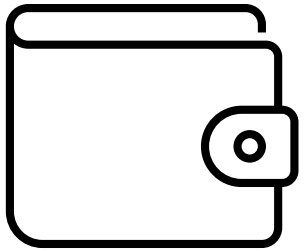
Radios: They’re everywhere!



- Wi-Fi: 2.4GHz, 5GHz
- Bluetooth: 2.4GHz
- Cellular (4G and 5G)
- GPS: 1227.6MHz, 1575.42MHz



Wireless mice and keyboards: 2.4GHz



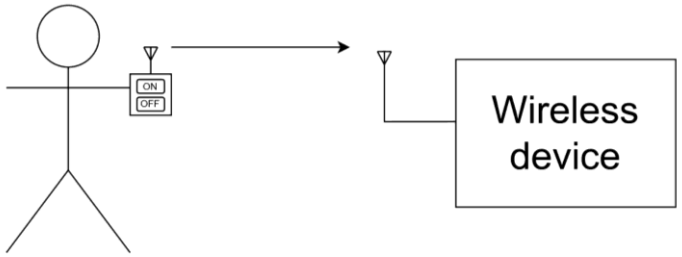
- Contactless payment: 13.56MHz
- Employee ID: 13.56MHz

- Remote keyless entry: 433.92MHz (UK)
- Passive keyless entry: 125KHz, 433.92MHz
- Transponder: 125KHz

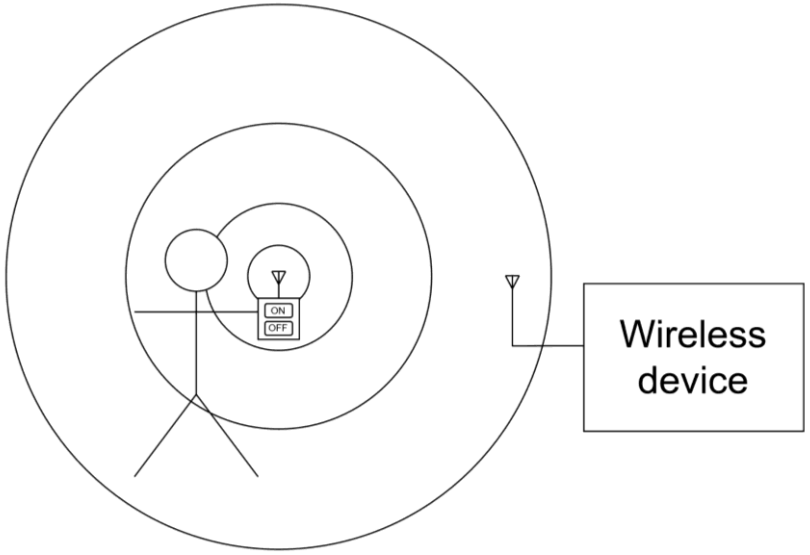
- Smart home Zigbee devices: Often 2.4GHz

Note: Omnidirectional transmission

Radio links in the system diagram



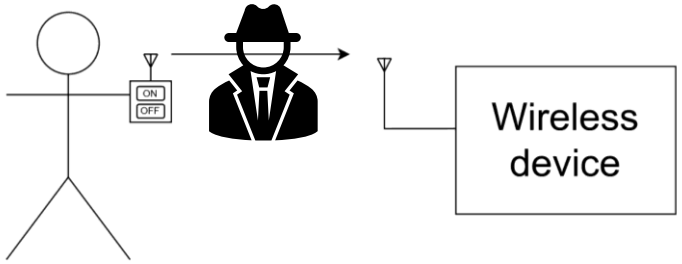
Radio links in reality (but not always!)



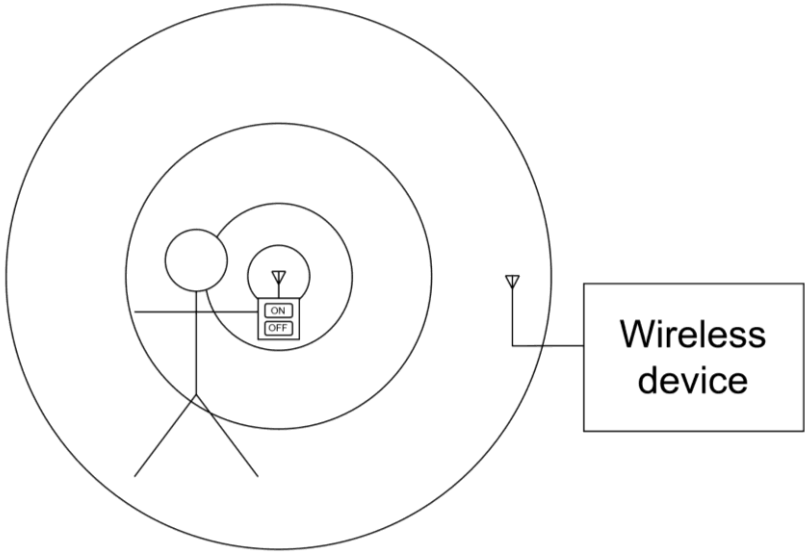
(Artist’s impression)

Note: Omnidirectional transmission

Radio links in the system diagram



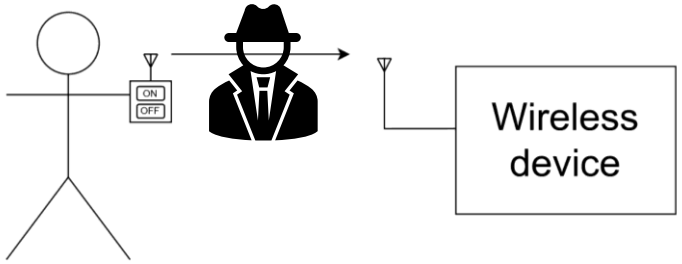
Radio links in reality (but not always!)



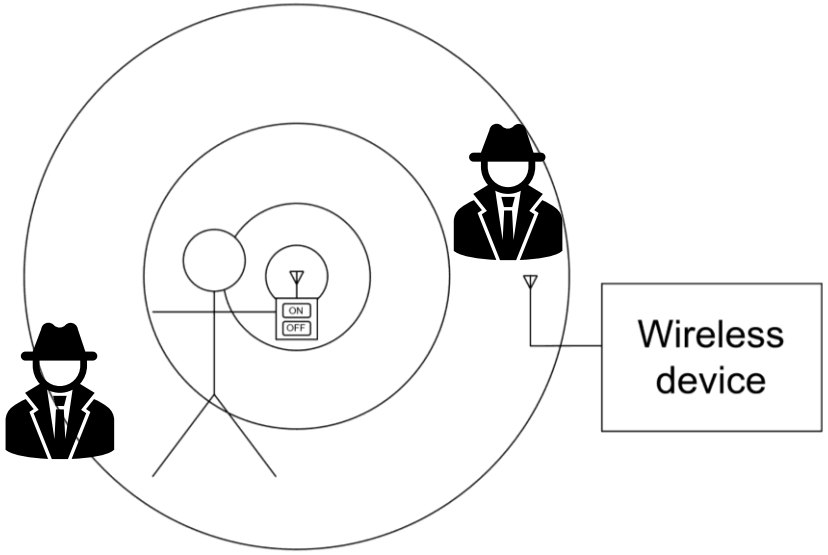
(Artist’s impression)

Note: Omnidirectional transmission

Radio links in the system diagram



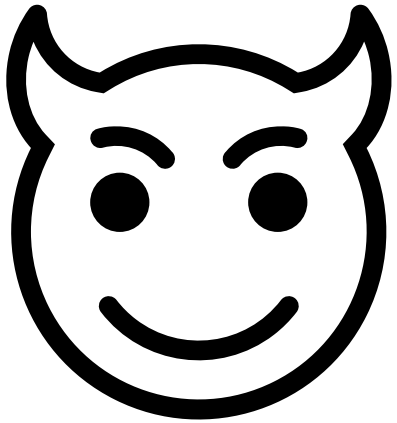
Radio links in reality (but not always!)



Threat Modelling: Radio Adversary

Transmit new messages

Block messages



Eavesdrop on messages

Modify messages

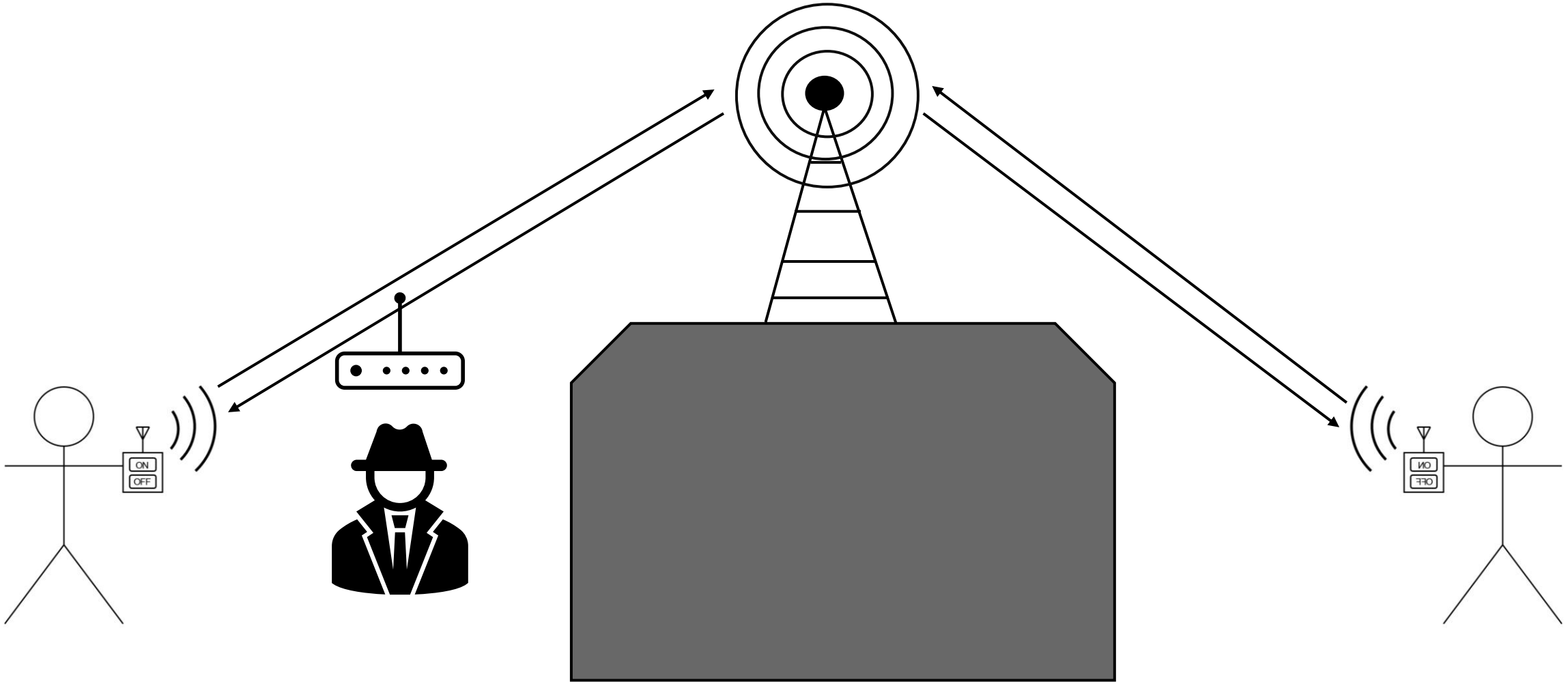
We must assume the channel itself is hostile!

Inspired by the Dolev-Yao adversary model, see:

V. Sundararajan, “Formal modeling of cryptographic protocols: Dolev-Yao model.” Accessed: Nov. 21, 2024. [Online]. Available: https://www.cmi.ac.in/~spsuresh/teaching/security17/lectures/basicdolevyao.pdf

Eavesdropping

Eavesdropping: Amateur radio example



Bob
Callsign: 2I0***

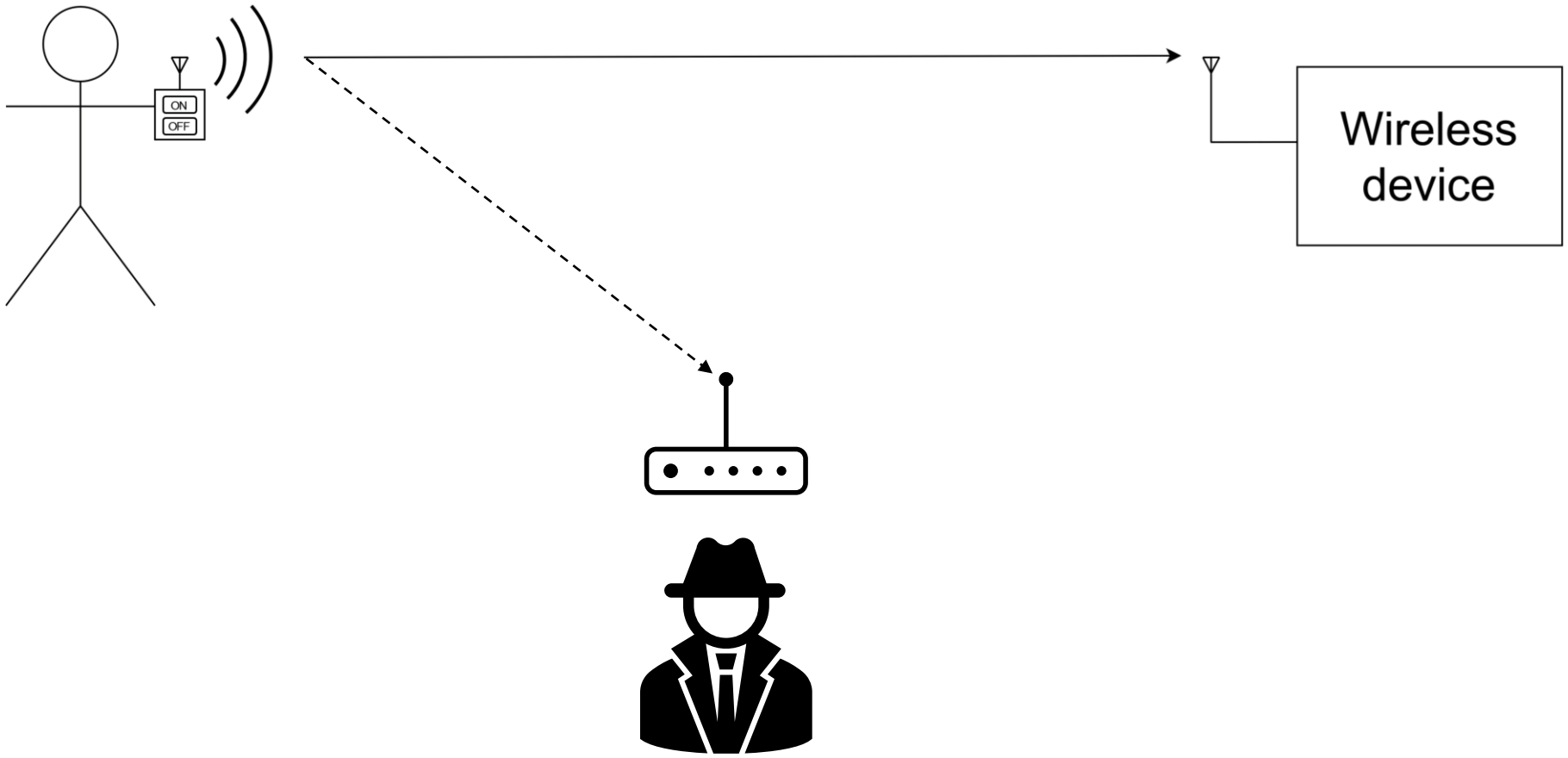
Repeater
Callsign: GB***

Alice
Callsign: *****

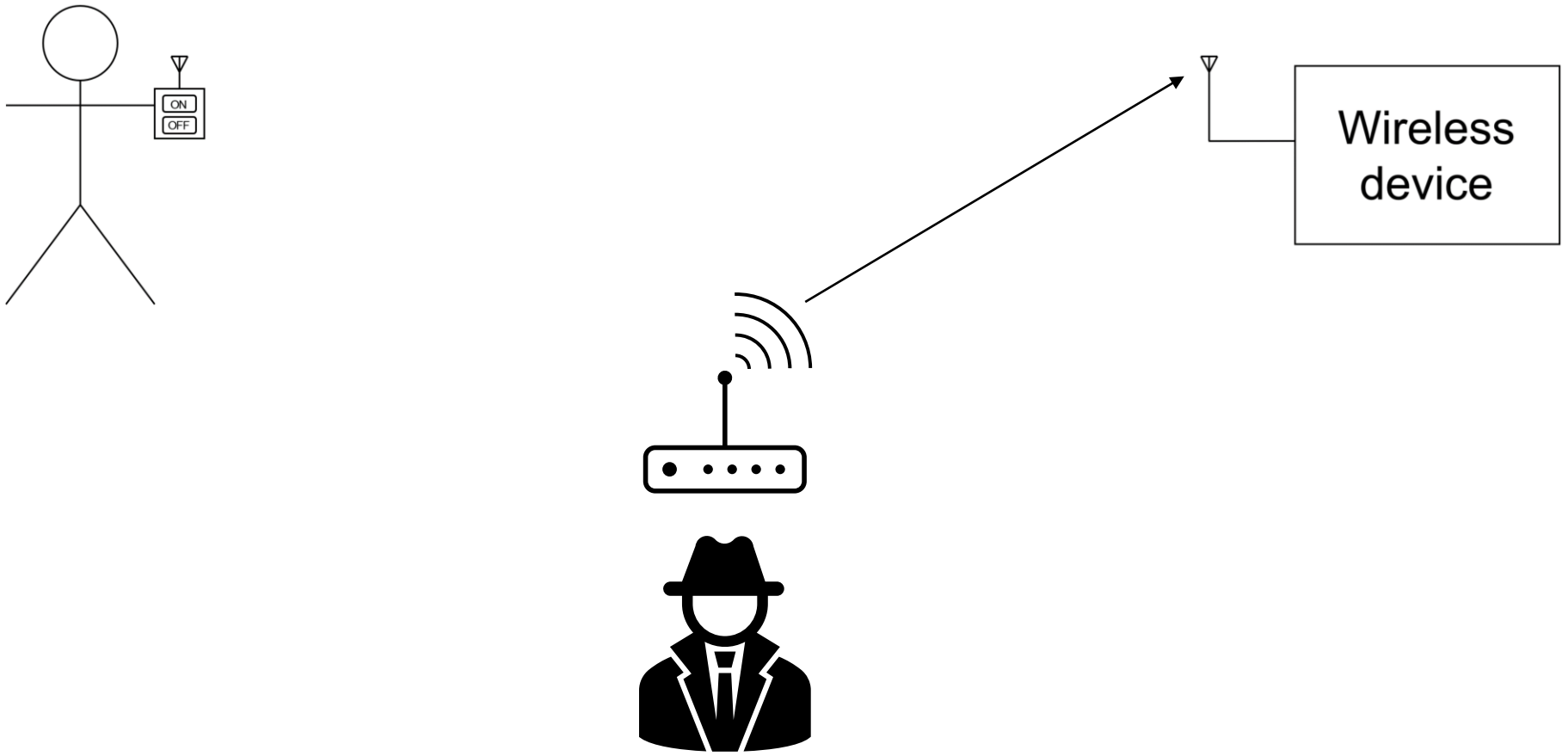
Replay attacks

Replay attacks: Concept

Replay attacks: Concept

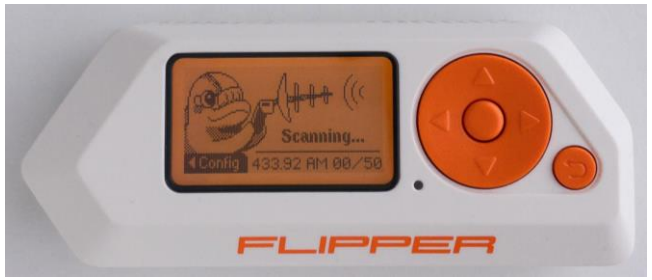


Replay attacks: Concept



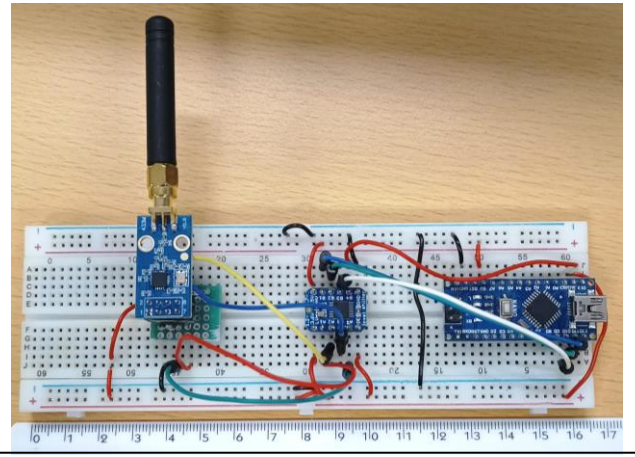
Replay attacks: Some hardware options

HackRF One
- Frequency range: 1MHz to 6 GHz [1]
- Price: €274.80 [2]

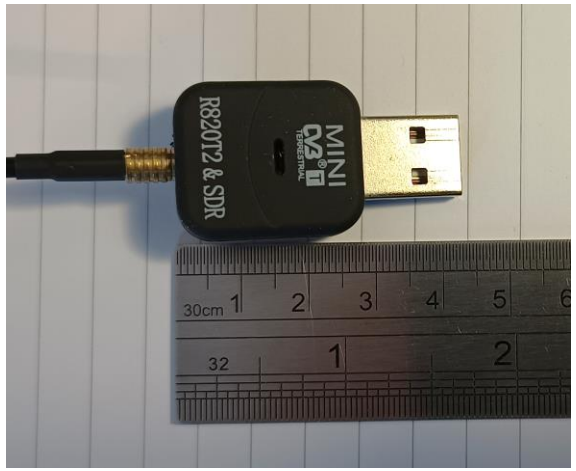


Flipper Zero image courtesy of Turbospok [5]

Flipper Zero
- Frequency range: < 1GHz and a number of other bands/protocols [3]
- Price: €229.00 [4]



TI CC1101 with dev board
- Frequency range: 300-348MHz, 387-464MHz, 779-928MHz [6]
- Price: <£30.00



RTL2832U-based SDR
- Frequency: 25MHz - 1750MHz [7]
- **Cannot transmit!**
- Price: €34.34 [7]

Hardware comparison references

[1] Great Scott Gadgets, “HackRF One.” Available: https://greatscottgadgets.com/hackrf/one/ (accessed Sep. 11, 2024).

[2] Martin Lynch and Sons, “Great Scott Gadgets HackRF One”, 2025. Available: https://www.hamradio.co.uk/sdr/great-scott-gadgets/great-scott-gadgets-hackrf-one-pd-7799 (accessed May 18, 2025).

[3] Flipper Devices Inc., “Flipper Zero Documentation.” Available: https://docs.flipper.net/ (accessed May 18, 2025)

[4] Flipper Devices Inc., “Flipper Zero.” Available: https://shop.flipperzero.one/ (accessed May 18, 2025).

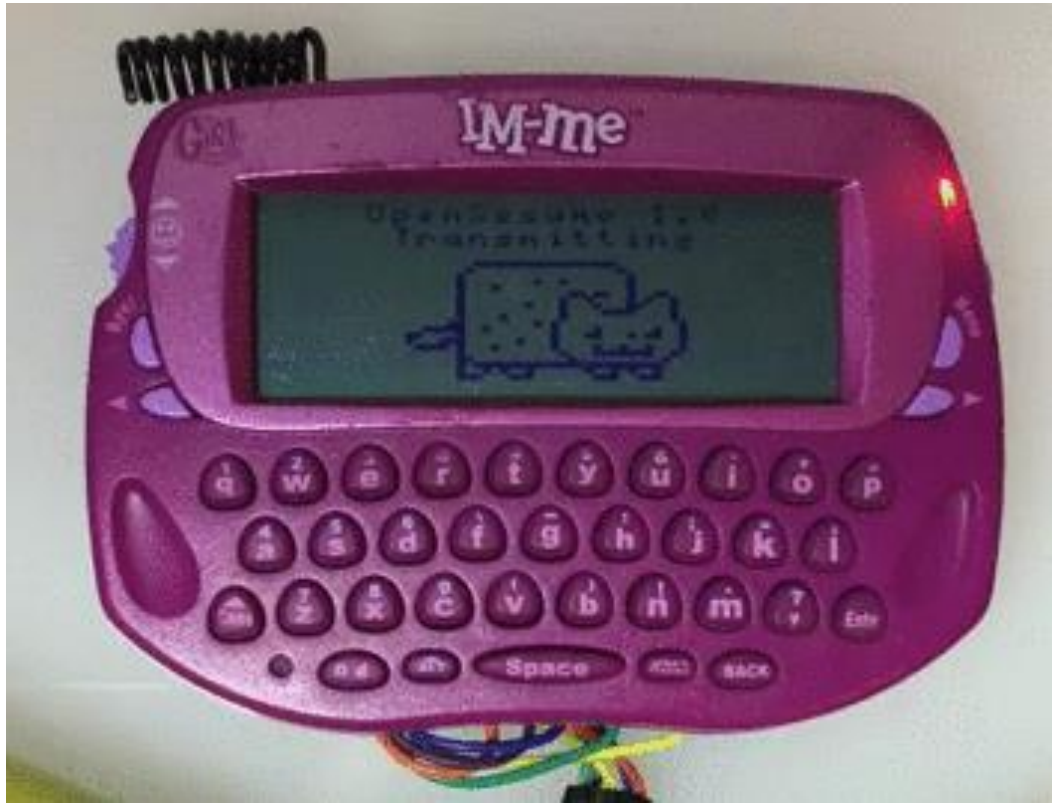
[5] Turbospok, “Flipper Zero.jpg”, Wikimedia. Available: https://commons.wikimedia.org/wiki/File:Flipper_Zero.jpg#/media/File:Flipper_Zero.jpg (accessed: Sep. 11, 2024).

[6] Texas Instruments, “CC1101.” Available: https://www.ti.com/product/CC1101 (accessed Sep. 11, 2024).

[7] Nooelec, “Nooelec NESDR Nano 2: Tiny RTL-SDR USB Set w/ R820T2 Tuner & Antenna.” Available: https://www.nooelec.com/store/nesdr-nano2.html (accessed May 18, 2025).

Honorable mention: The Girl Tech IM-me

- Original purpose: Instant messaging
- Toy features a Texas Instruments CC1110 sub-1GHz microcontroller [1][2]
- Has been used with Kamkar's OpenSesame to hack a garage door opener [1]
- Has been used to demonstrate jamming of P25 (secure) radios [3]
- Retailed for 64.99 USD in 2007 [4]
- Costs around £100 on eBay now

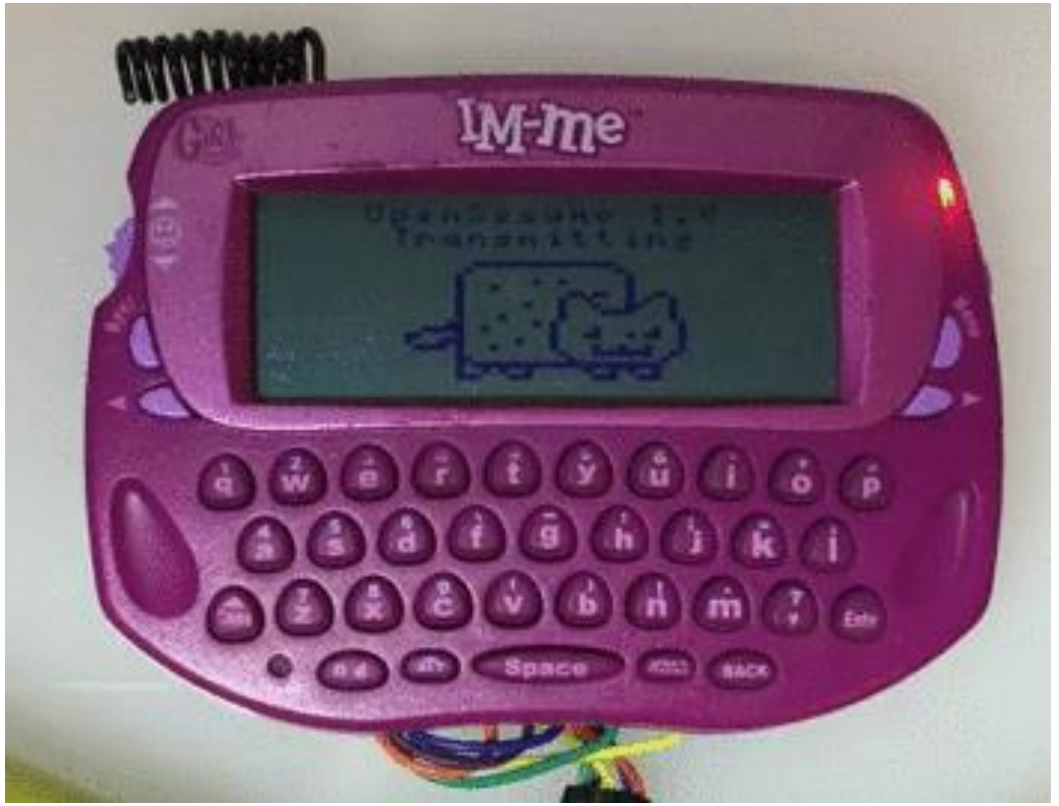


Kamkar's modified Girl Tech IM-me [1]

[1] S. Kamkar, "OpenSesame: hacking garages in seconds." Available: http://samy.pl/opensesame/ (accessed Sep. 10, 2024).
[2] Texas Instruments, "CC1110-CC1111," 2022. Available: https://www.ti.com/product/CC1110-CC1111 (accessed Sep. 10, 2024).
[3] S. Clark, T. Goodspeed, P. Metzger, Z. Wasserman, K. Xu, and M. Blaze, 'Why (Special Agent) Johnny (Still) Can't Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System', in *USENIX Security Symposium*, 2011, vol. 2011, pp. 8–12.
[4] A. Gelfand, "It's Like a Walkie-Talkie, Only You Type Into It," WIRED, Feb. 13, 2007. Available: https://www.wired.com/2007/02/its-like-a-walk/ (accessed Sep. 10, 2024).

Honorable mention: The Girl Tech IM-me

- Original purpose: Instant messaging
- Toy features a Texas Instruments CC1110 sub-1GHz microcontroller [1][2]
- Has been used with Kamkar's OpenSesame to hack a garage door opener [1]
- Has been used to demonstrate jamming of P25 (secure) radios [3]
- Retailed for 64.99 USD in 2007 [4]
- Costs around £100 on eBay now

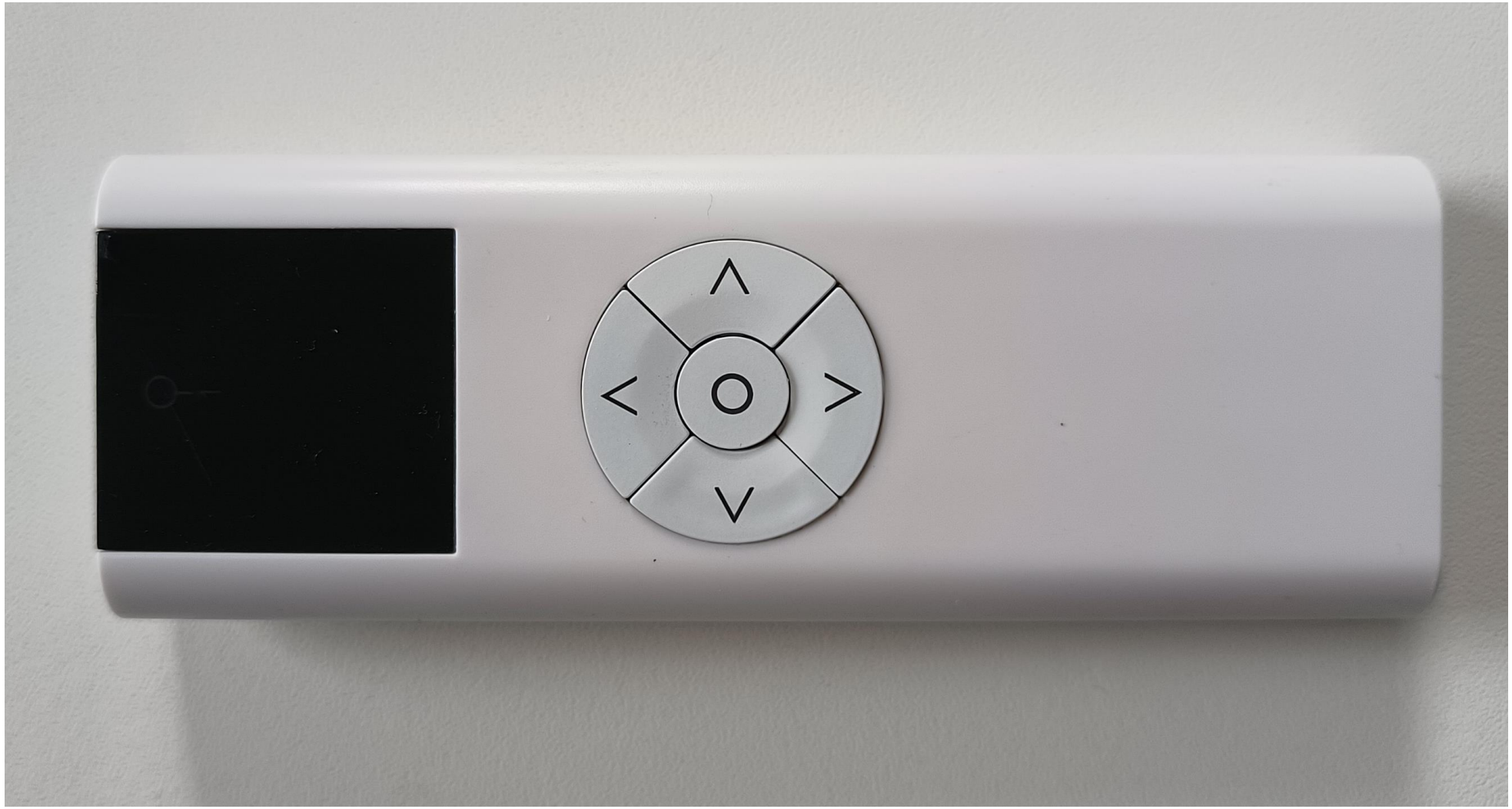


Kamkar's modified Girl Tech IM-me [1]

[1] S. Kamkar, "OpenSesame: hacking garages in seconds." Available: http://samy.pl/opensesame/ (accessed Sep. 10, 2024).
[2] Texas Instruments, "CC1110-CC1111," 2022. Available: https://www.ti.com/product/CC1110-CC1111 (accessed Sep. 10, 2024).
[3] S. Clark, T. Goodspeed, P. Metzger, Z. Wasserman, K. Xu, and M. Blaze, 'Why (Special Agent) Johnny (Still) Can't Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System', in *USENIX Security Symposium*, 2011, vol. 2011, pp. 8–12.
[4] A. Gelfand, "It's Like a Walkie-Talkie, Only You Type Into It," WIRED, Feb. 13, 2007. Available: https://www.wired.com/2007/02/its-like-a-walk/ (accessed Sep. 10, 2024).

Simple replay attack: Projector screen motor

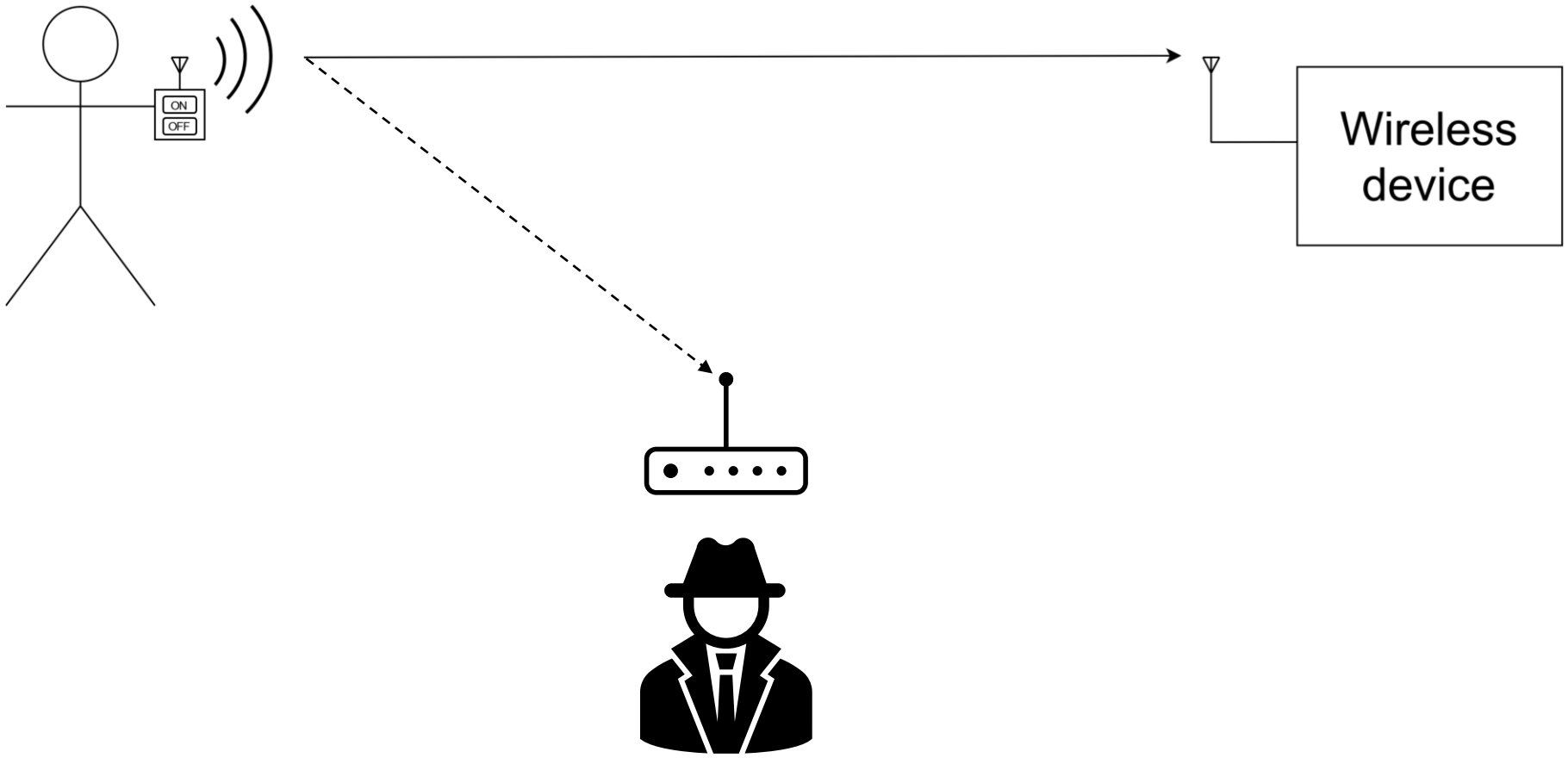
Simple replay attack: Projector screen motor



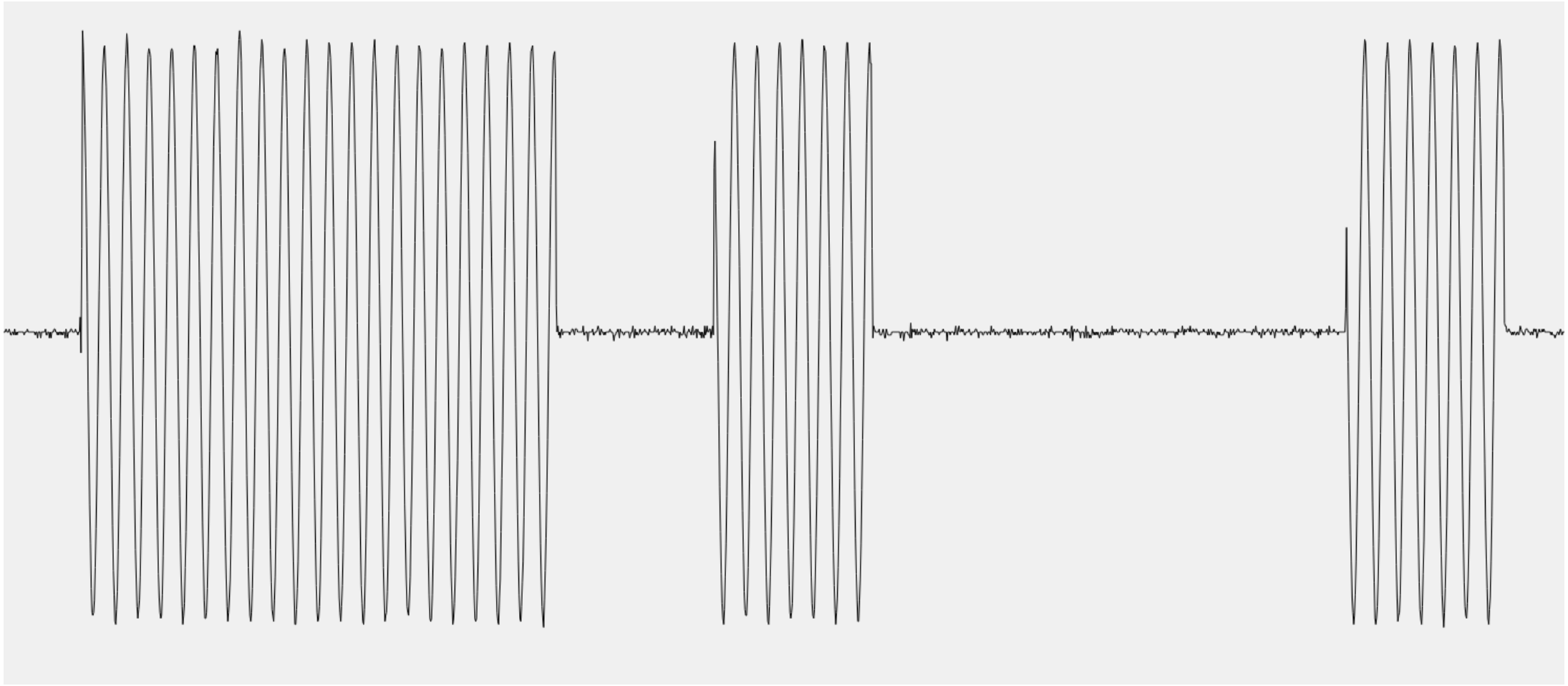
Simple replay attack: Projector screen motor

Simple replay attack: Projector screen motor

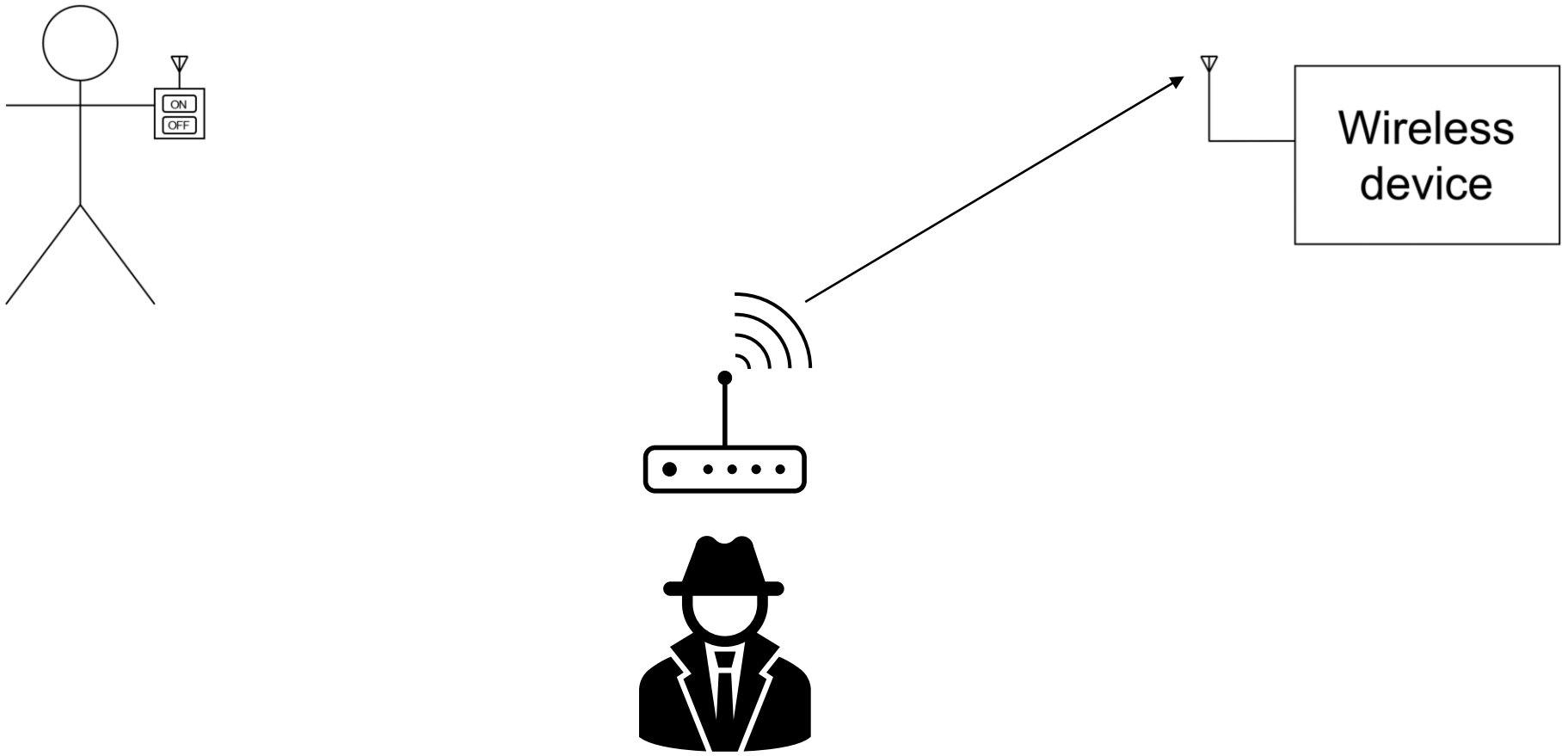
Simple replay attack: Projector screen motor

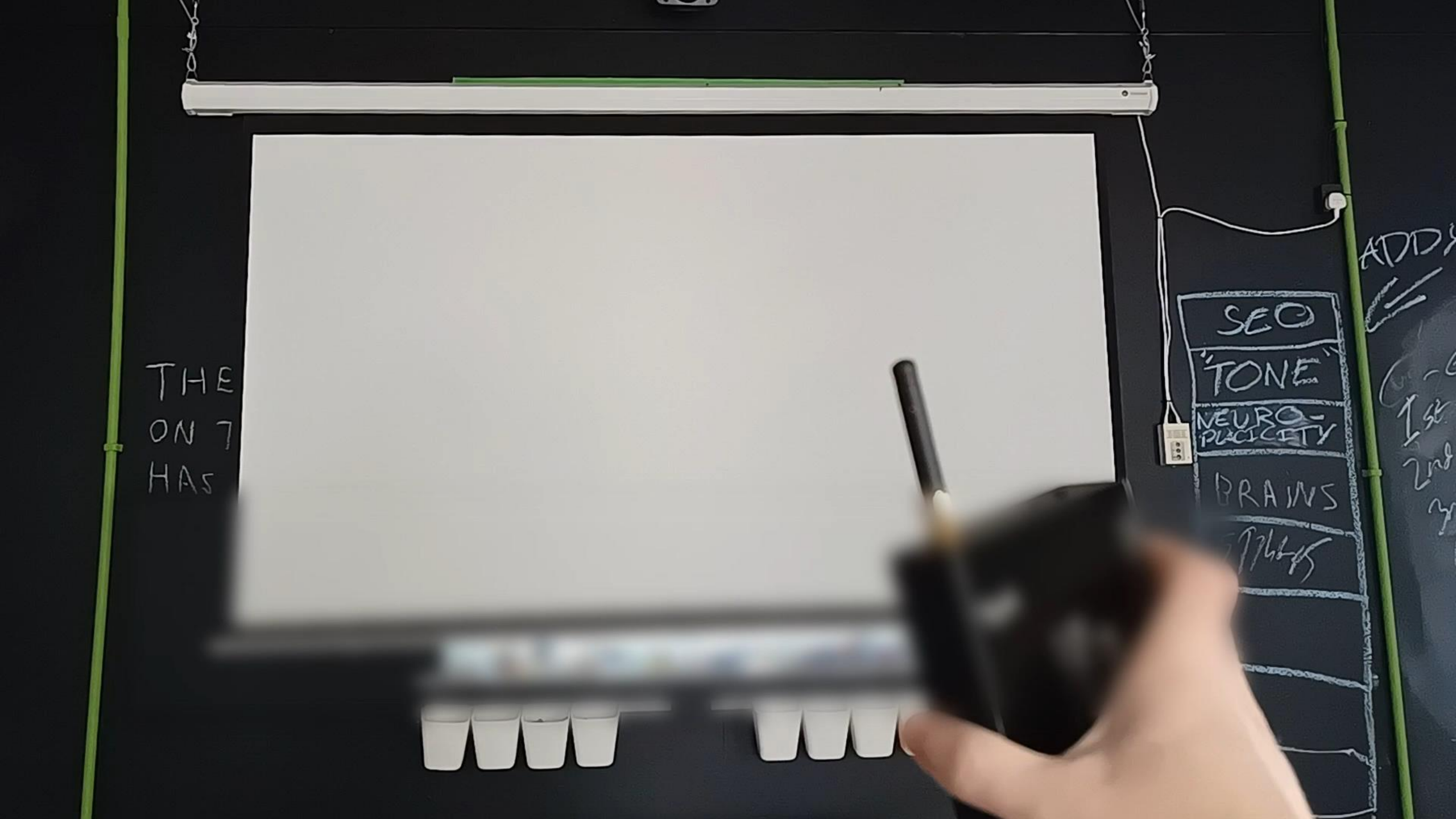


Simple replay attack: Projector screen motor



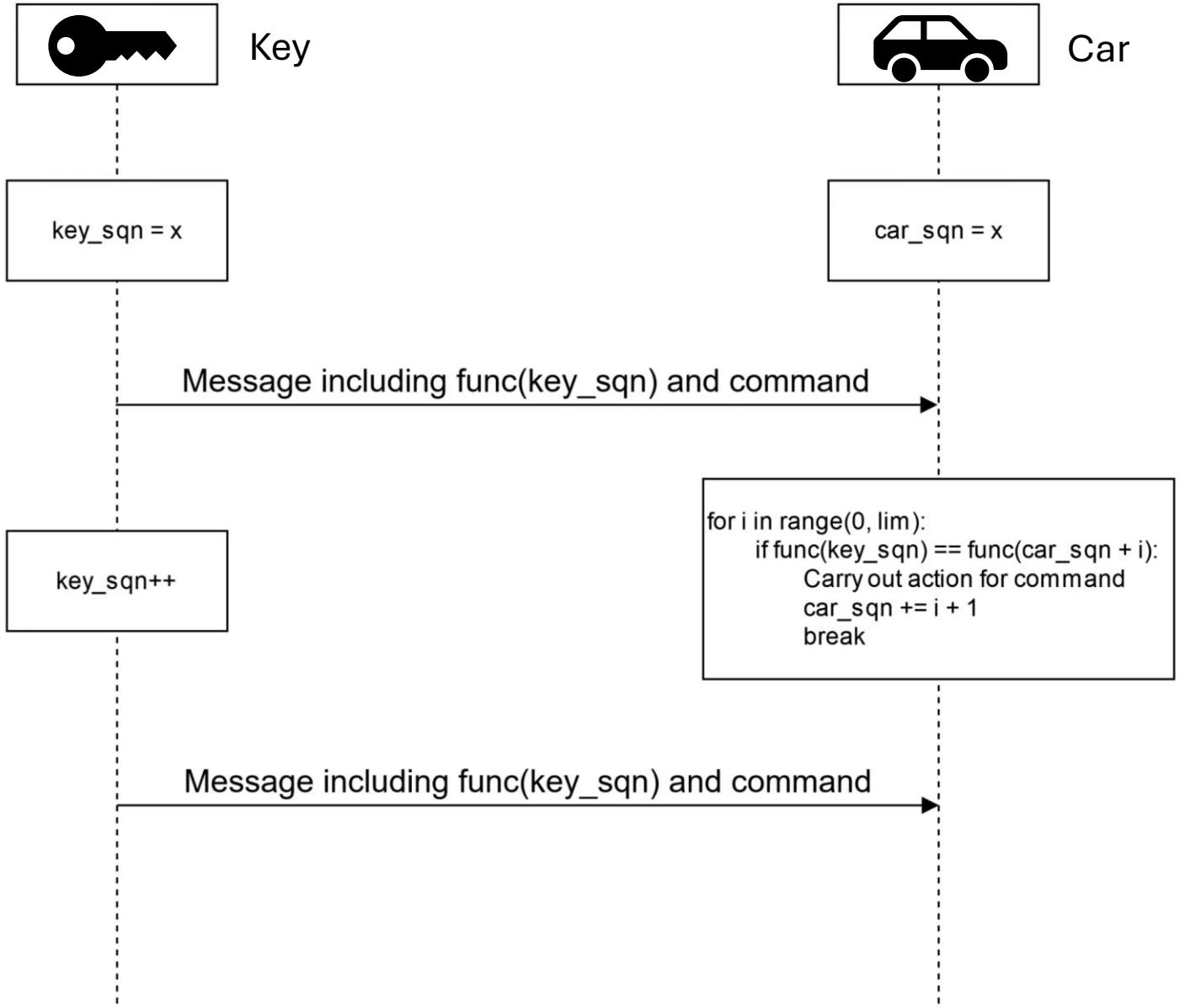
Simple replay attack: Projector screen motor

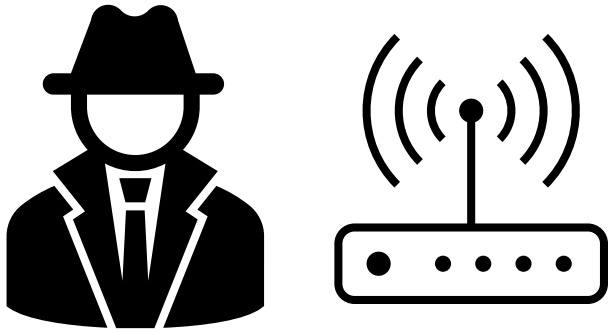



THE
ON 7
HAS
SEO
TONE
NEURO-
PLASTICITY
BRAINS

A reasonable next step...

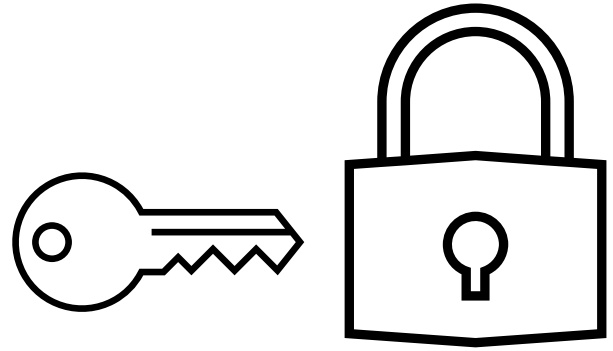
Rolling code: Pseudocode





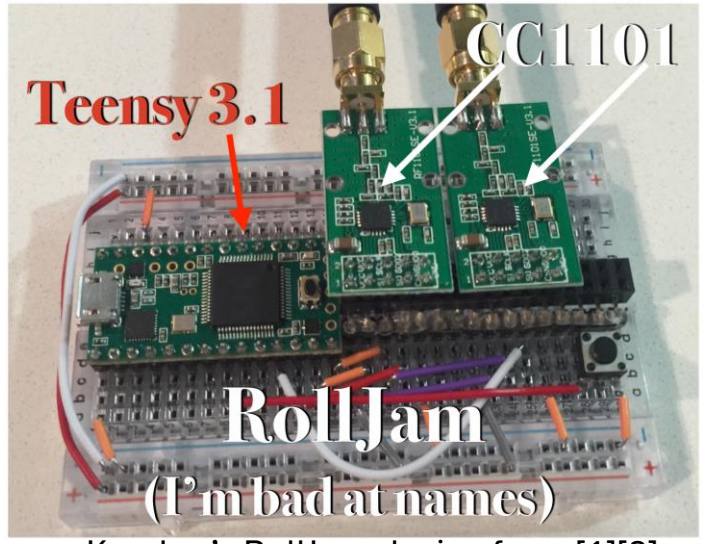
Does that mean my car can’t be unlocked by an attacker?

(This is now a cryptography problem)

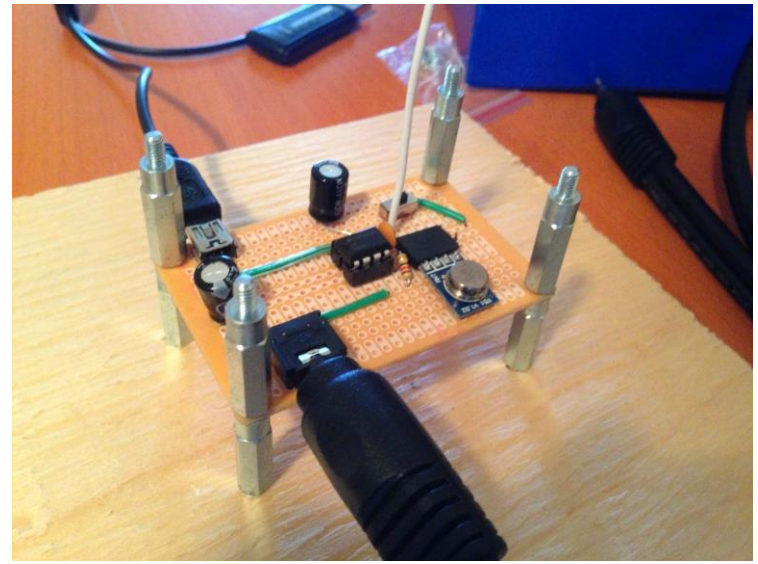


Rolljam: Keeping one step ahead

- Attack presented by Samy Kamkar at Defcon 23 (2015) [1][2]
- Kamkar is also known for:
  - MySpace Samy worm [3]
  - Drone hacking (SkyJack) [4]
  - Many other pieces of automotive security research
- Kamkar's hardware included [1][2]:
  - Teensy 3.1 (ARM Cortex development board)
  - 2 x Texas Instruments CC1101 modules (Same IC used in the Flipper Zero!)

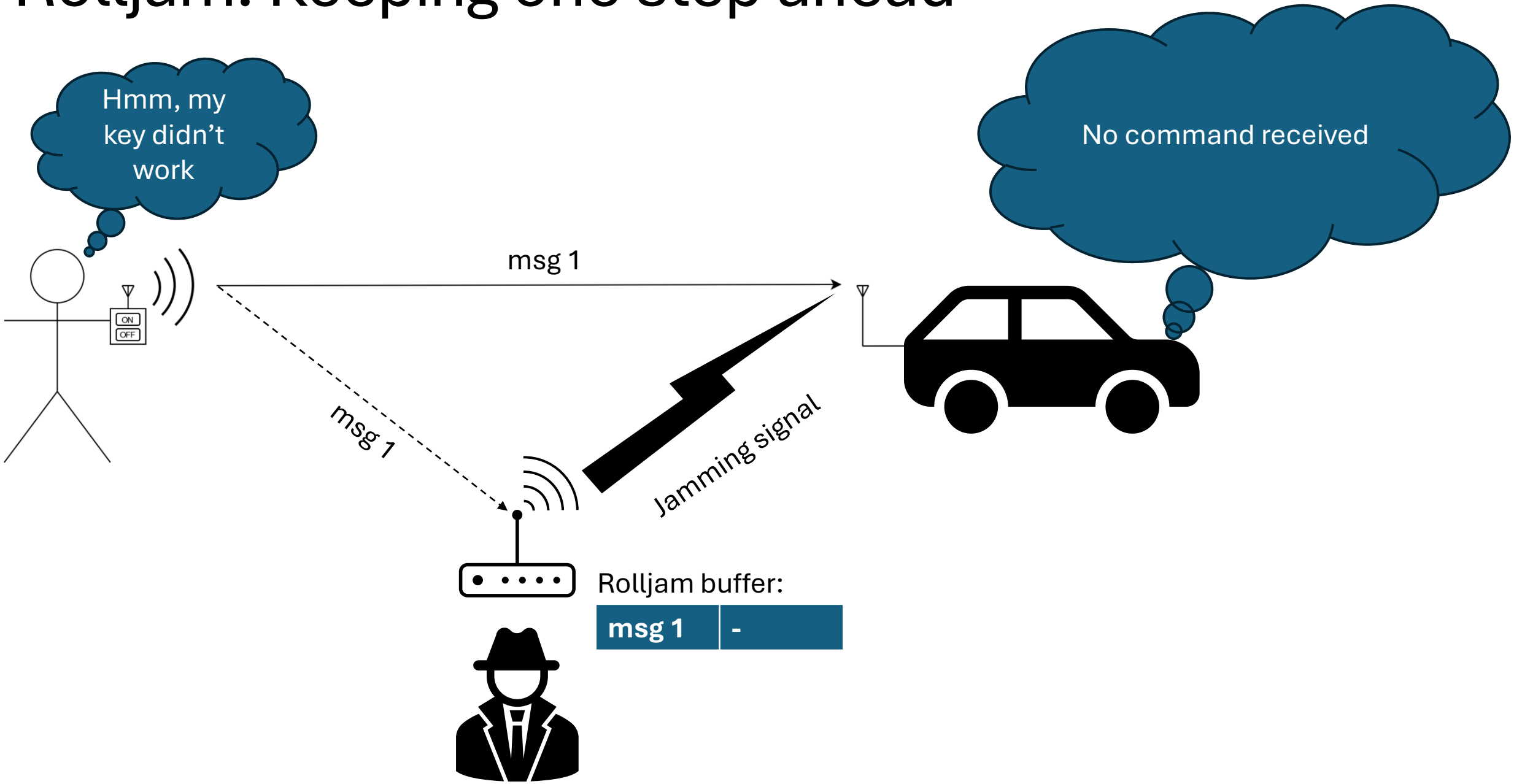


Kamkar's RollJam device from [1][2]

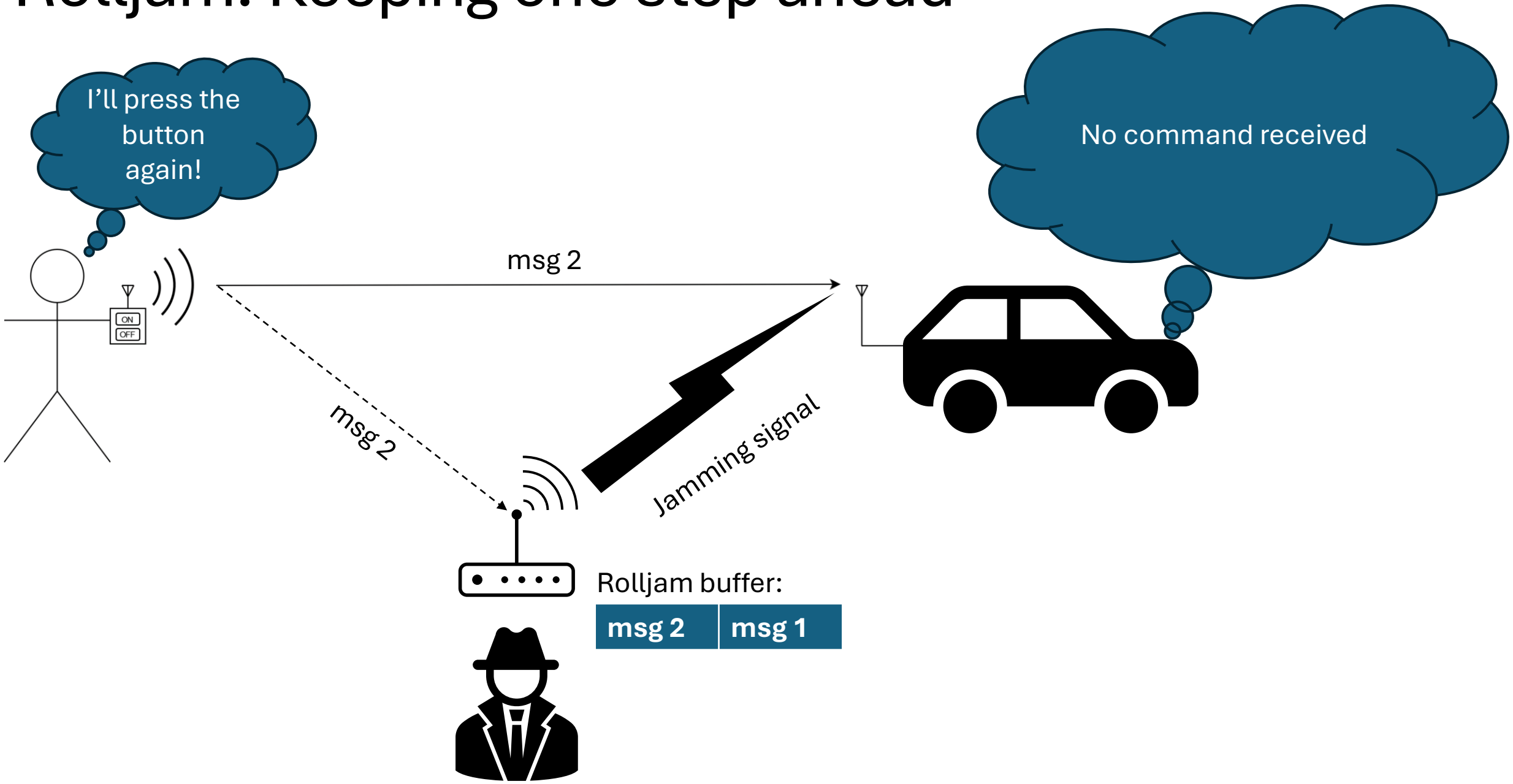

Whyte's RollJam device from [5]

[1] S. Kamkar, "Drive it like you Hacked it," presented at Def Con 25 [Online], 2015. Available: https://samy.pl/defcon2015/2015-defcon.pdf (accessed Sep. 11, 2024).
[2] DEFCONConference, "DEF CON 23 - Samy Kamkar - Drive it like you Hacked it: New Attacks and Tools to Wireles," *YouTube* [Online], Dec. 02, 2015. Available: https://www.youtube.com/watch?v=UNgvShN4USU (accessed Aug. 29, 2024).
[3] S. Kamkar, "MySpace Worm Explanation." Available: https://samy.pl/myspace/tech.html (accessed Sep. 11, 2024).
[4] S. Kamkar, "SkyJack: autonomous drone hacking." Available: https://samy.pl/skyjack/ (accessed Sep. 11, 2024).
[5] S. Whyte, "Jam Intercept and Replay Attack against Rolling Code Key Fob Entry Systems using RTL-SDR," Aug. 29, 2024. Available: http://spencerwhyte.blogspot.com/2014/03/delay-attack-jam-intercept-and-replay.html?m=1 (accessed Aug. 29, 2024).

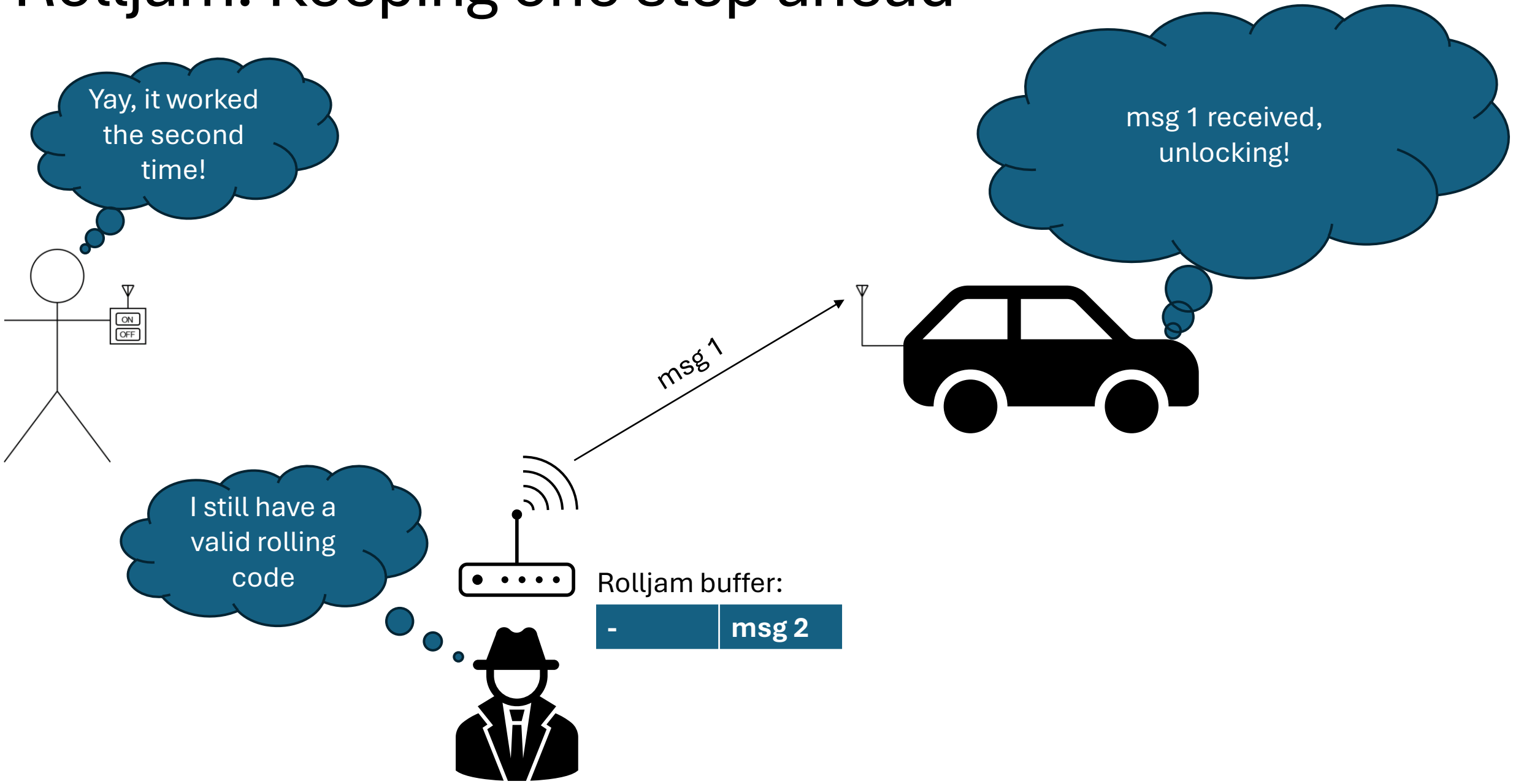
Rolljam: Keeping one step ahead



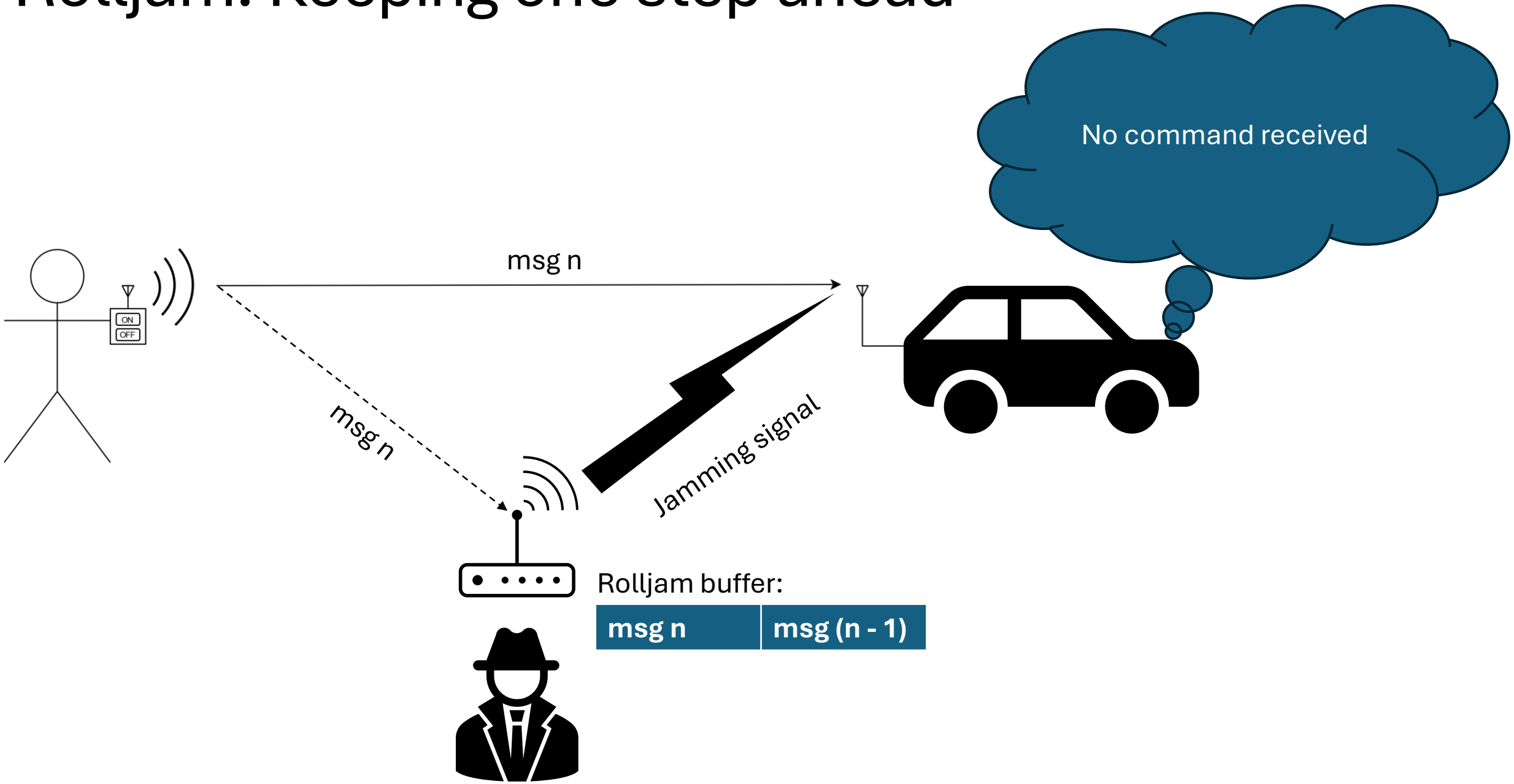
Rolljam: Keeping one step ahead



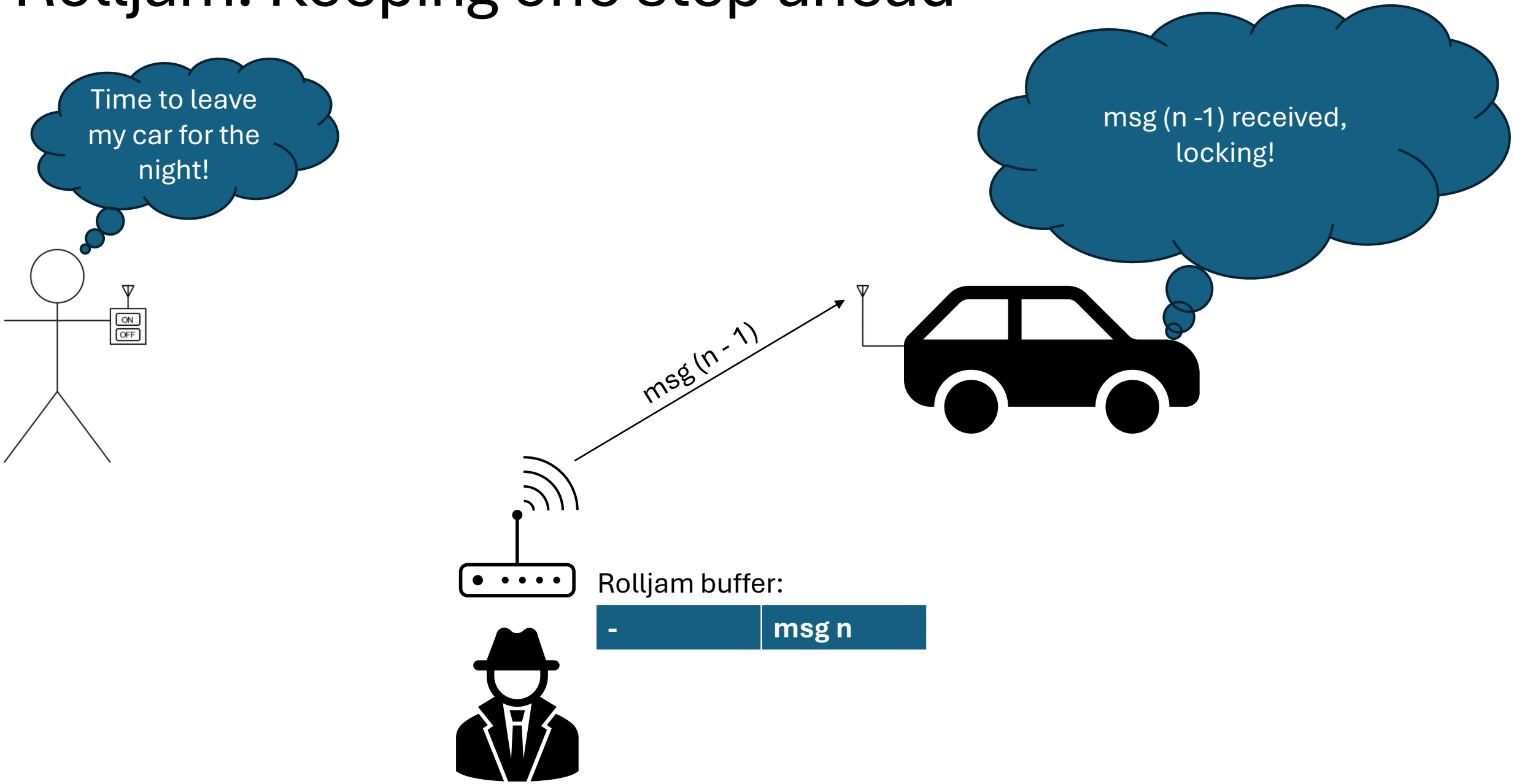
Rolljam: Keeping one step ahead



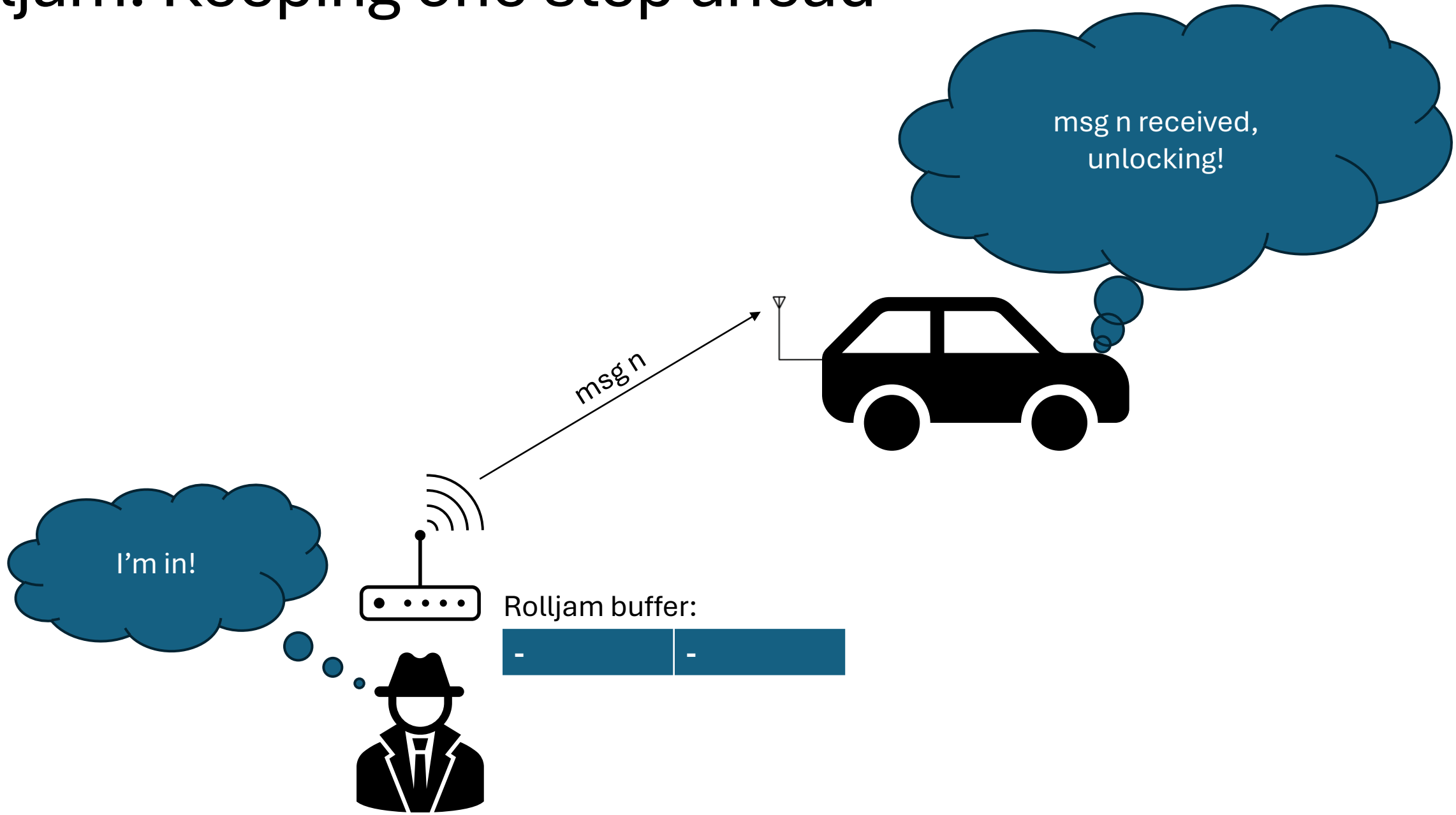
Rolljam: Keeping one step ahead



Rolljam: Keeping one step ahead



Rolljam: Keeping one step ahead



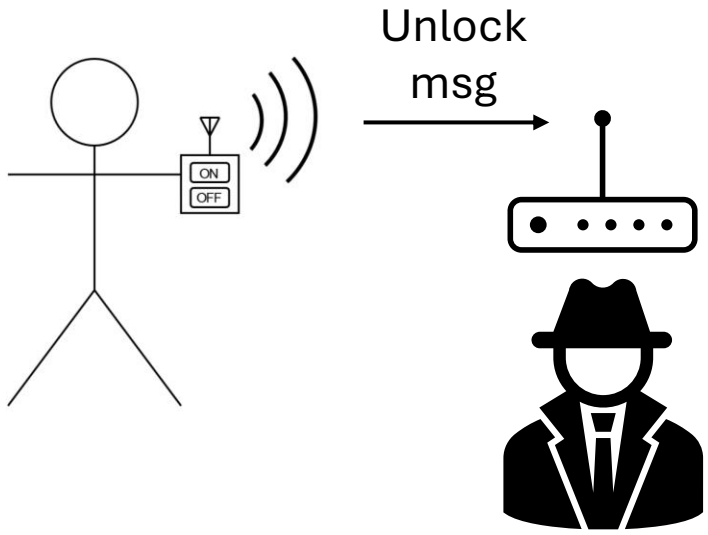
Radio jamming is (usually) illegal!

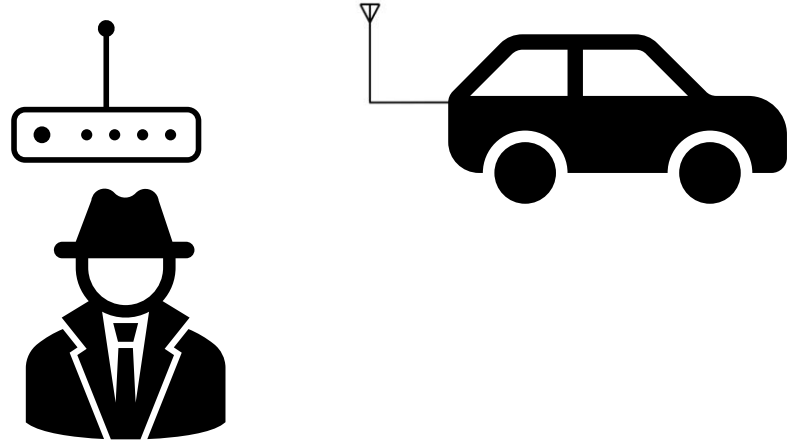
Let’s recreate another attack to avoid breaking the law

Relay attack: Concept

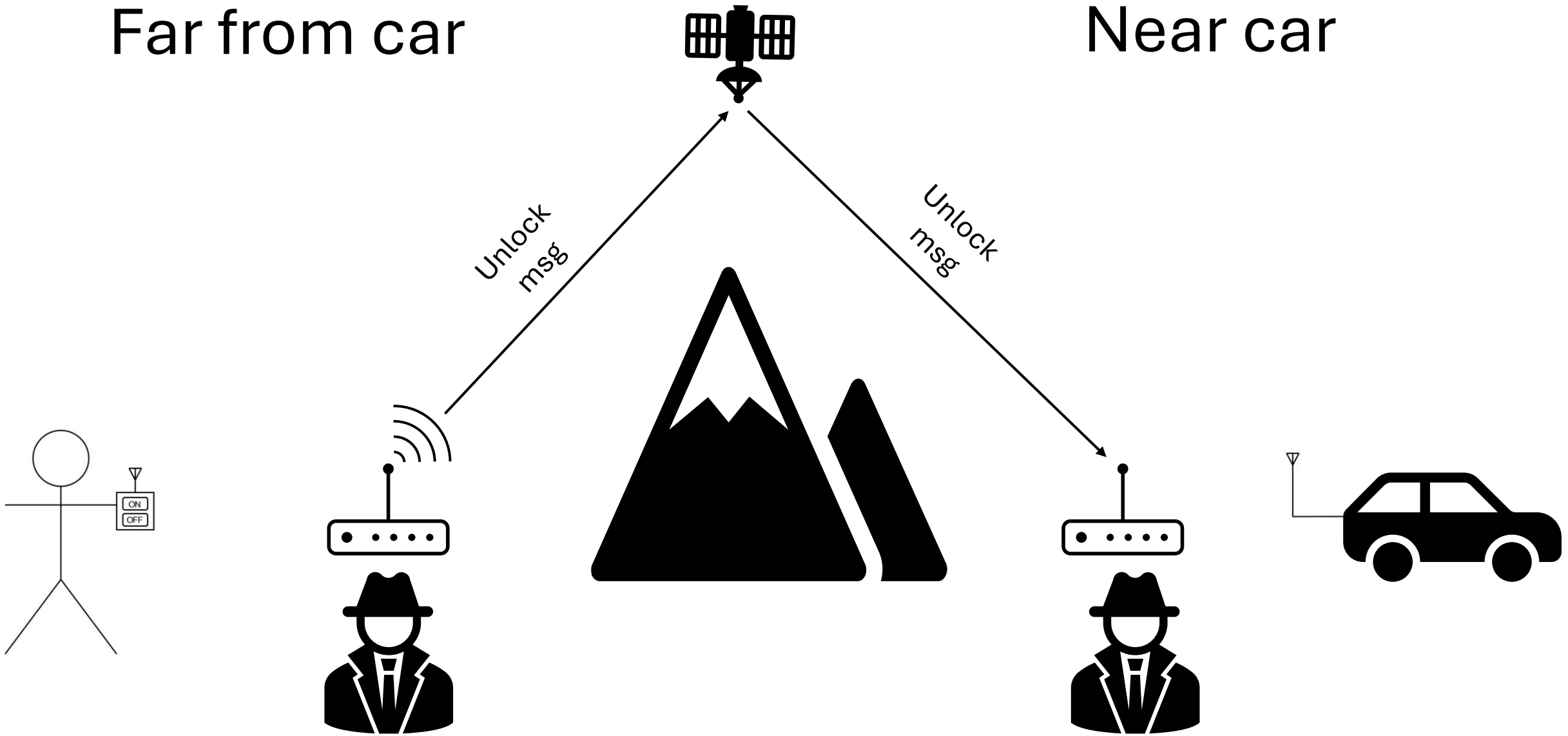
Far from car

Near car





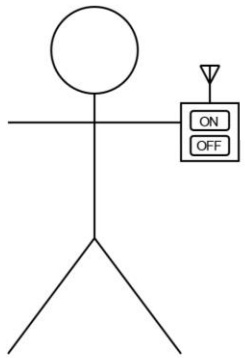
Relay attack: Concept

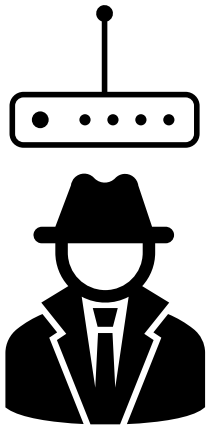


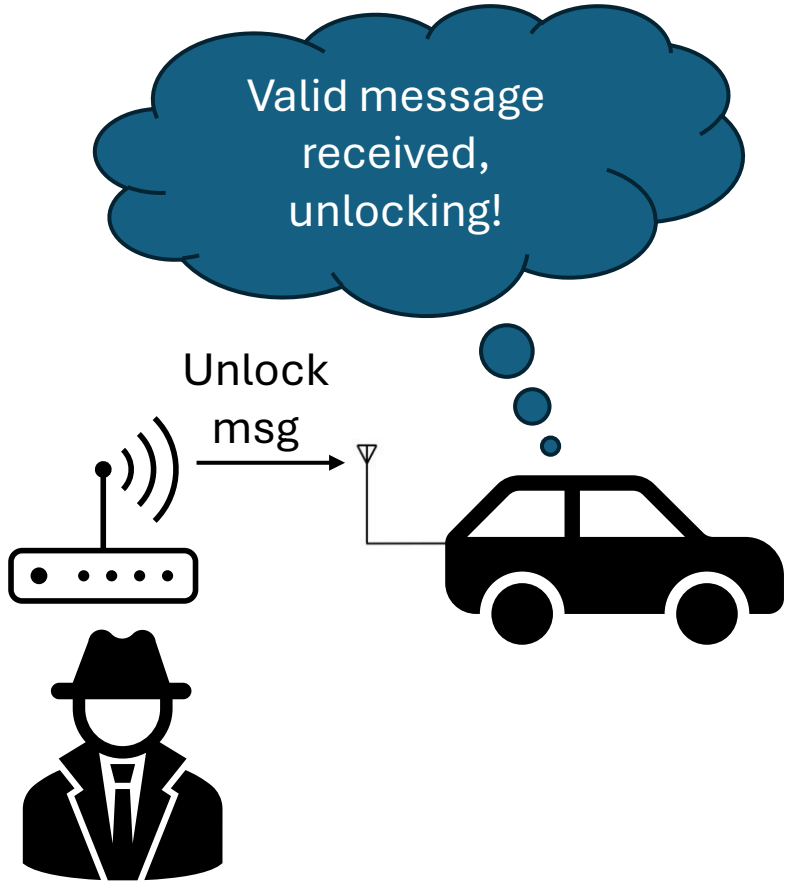
Relay attack: Concept

Far from car

Near car

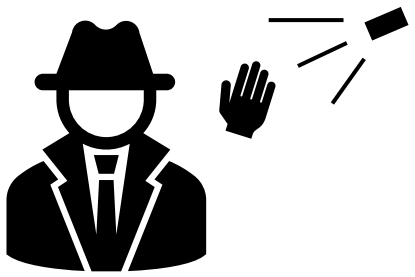




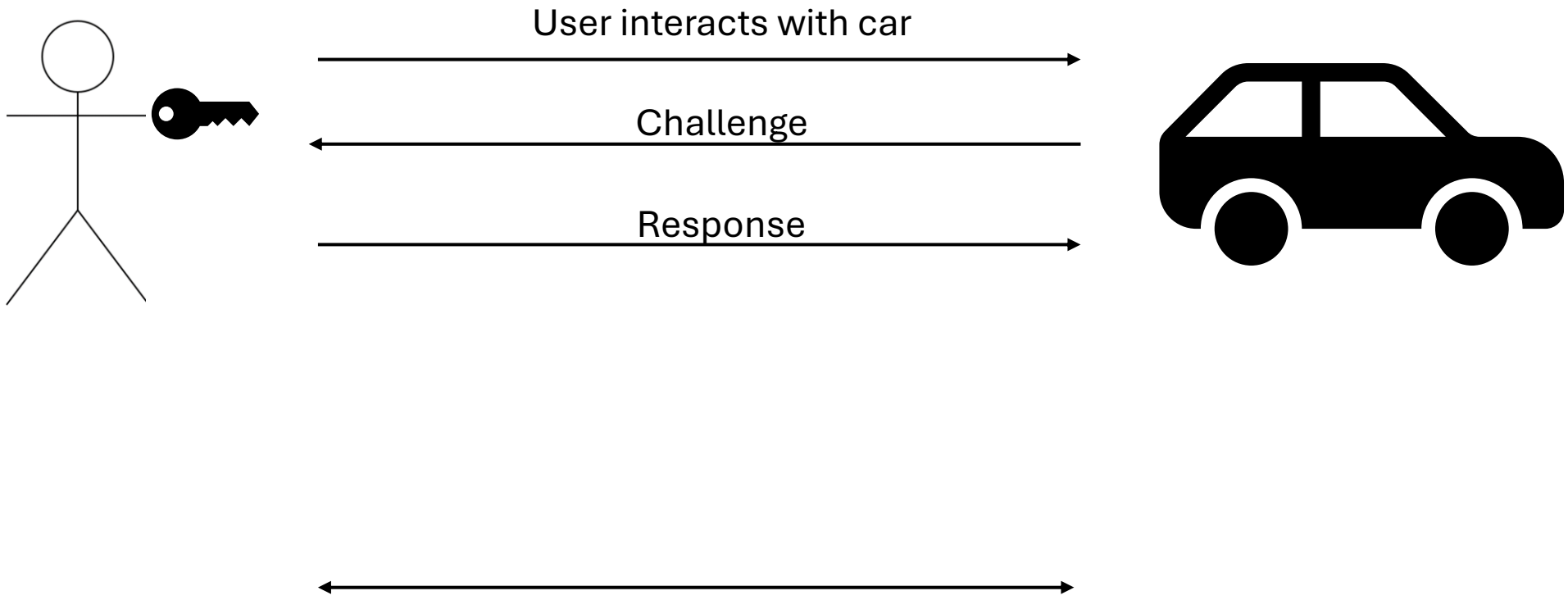


Relay attack demo

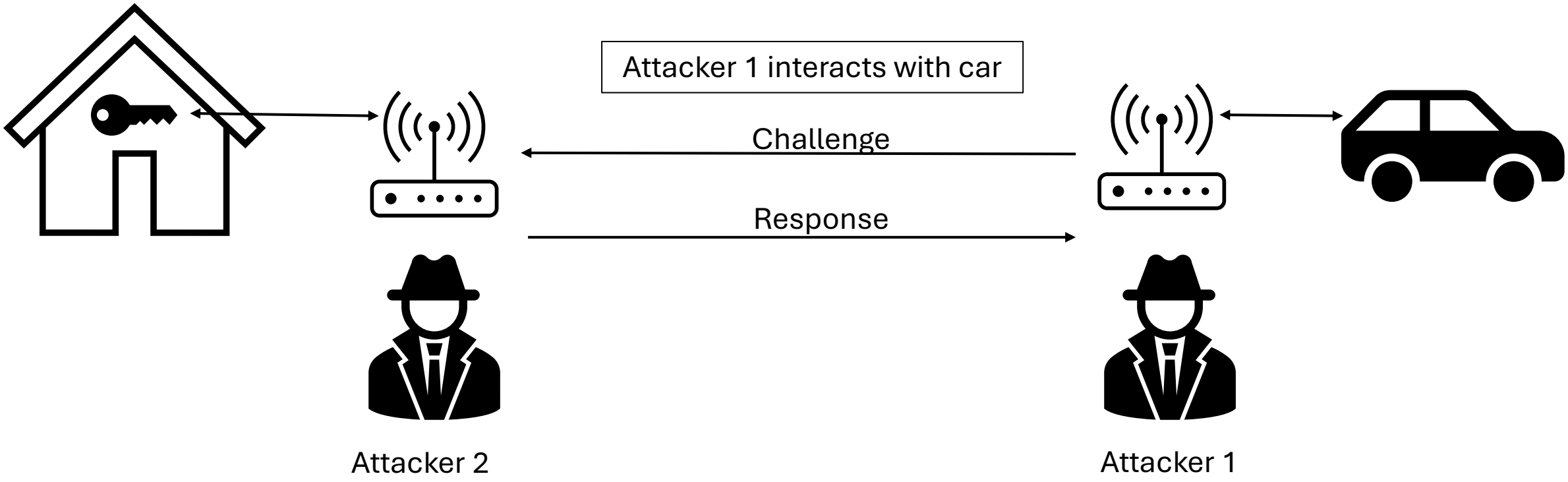
So is this attack practical?



Passive keyless entry/start: Concept



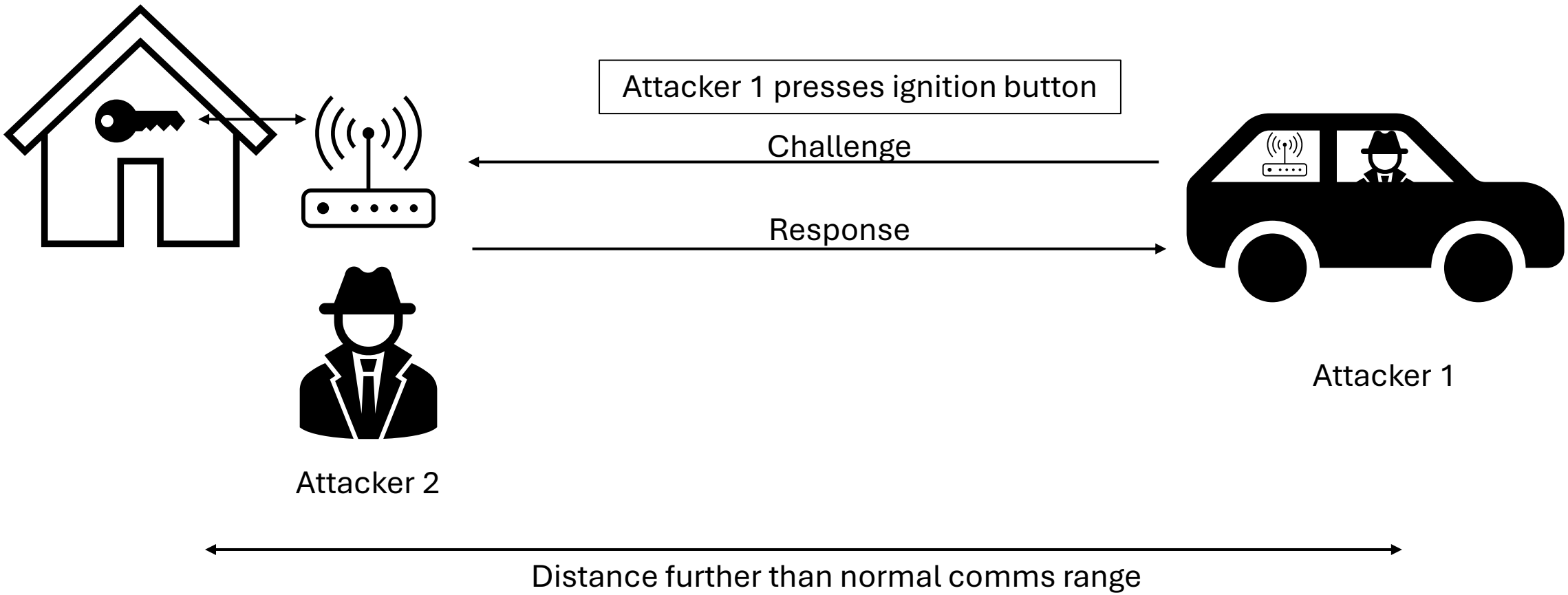
Passive keyless entry/start: Two-thief attack



Distance further than normal comms range
Attackers amplify signals to increase comms range
Little knowledge of involved protocols required

[1] A. I. Alrabady and S. M. Mahmud, "Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs," in *IEEE Transactions on Vehicular Technology*, vol. 54, no. 1, pp. 41-50, Jan. 2005, doi: 10.1109/TVT.2004.838829.

Passive keyless entry/start: Two-thief attack



[1] A. I. Alrabady and S. M. Mahmud, "Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs," in *IEEE Transactions on Vehicular Technology*, vol. 54, no. 1, pp. 41-50, Jan. 2005, doi: 10.1109/TVT.2004.838829.

Attack Mitigation

Mitigation: Users [1]

[1] PSNI, "Preventing Keyless Car Theft". Available: https://www.psni.police.uk/safety-and-support/roads-and-driving/preventing-car-and-vehicle-theft/preventing-keyless-car-theft (accessed Sep. 11, 2024).

Mitigation: Some proposed solutions

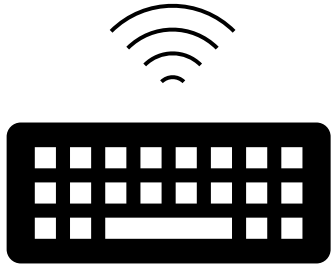
- Use encoded timestamps
  - Radio signals propagate at the speed of light in a vacuum
  - We securely encode time of transmission in each message
  - Receiving a signal a few seconds after it was sent from close proximity is suspicious
  - In 2015, Kamkar suggested the use of Dual KeeLoq protocol [1]
  - Challenge: Synchronising timing between key and car
- Machine learning techniques for fingerprinting signals [2]
- Use of physical metrics (e.g., RSSI, RTT, GPS coordinates) to identify proximity [3]

[1] S. Kamkar, “Drive it like you Hacked it,” presented at Def Con 25, 2015. Available: https://samy.pl/defcon2015/2015-defcon.pdf (accessed Sep. 11, 2024).
[2] K. Joo, H. J. Jo and W. Choi, "Securing Passive Keyless Entry and Start System in Modern Vehicles Based on LF-Band Signal Analysis," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2024.3453920.
[3] J. Wang, K. Lounis and M. Zulkernine, "CSKES: A Context-Based Secure Keyless Entry System," 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), Milwaukee, WI, USA, 2019, pp. 817-822, doi: 10.1109/COMPSAC.2019.00120.

Takeaways

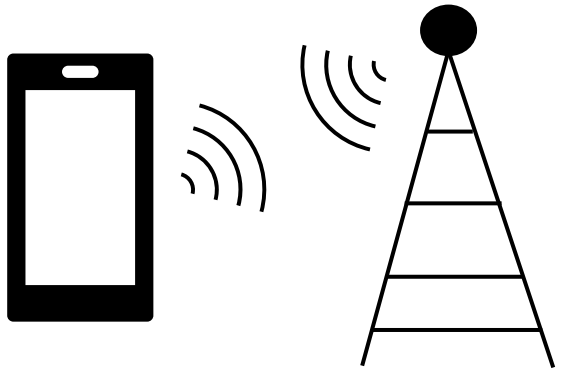
- When you broadcast a message from a wireless device, you generally can't control who receives it – only who can read it
- Security in hardware can be a balancing act
- Have a think – Do we need to have higher expectations regarding wireless and hardware security testing?
- Interested beginner? Check out a foundation amateur radio course on the Radio Society of Great Britain (RSGB) website: https://rsgb.org/main/clubs-training/for-students/online-training-resources-for-students/
  - Post-conference note: The above is only relevant for UK amateur radio. Please refer to information provided by an amateur radio society in the country you wish to operate in, e.g., the Irish Radio Transmitters Society (IRTS) in Ireland.

Other topics I want to mention



Wireless keyboards/mice

Phone phreaking/blue boxing



5G RAN and core network security

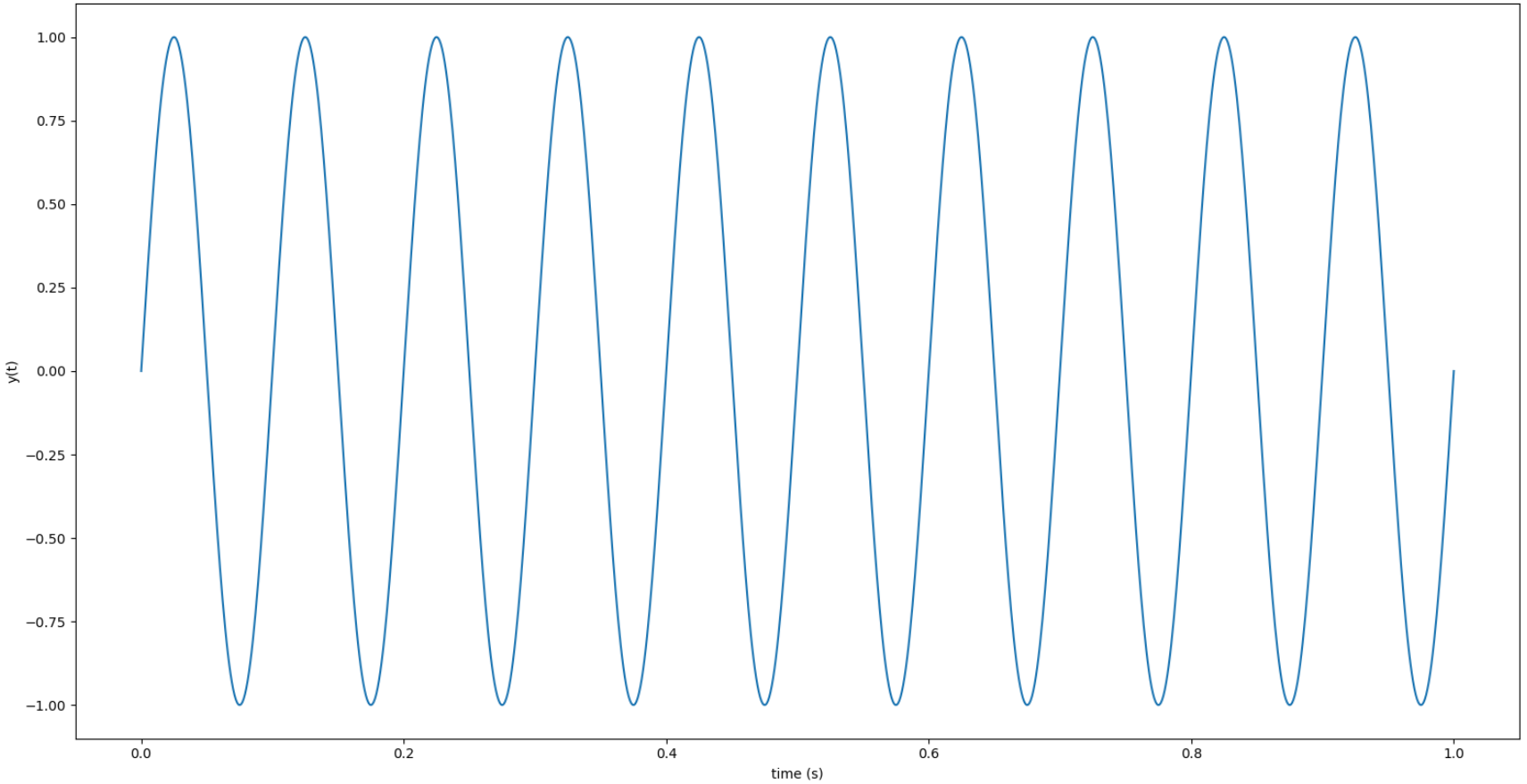
Thank you!

- And a special thank you to:
- **Grant (@brains933)** for lending me his HackRF One
- **John Megarry** for filming me breaking into my car
- **Farset Labs** for letting me play with their projector screen
- **Samy Kamkar** for inspiring this talk

Follow me/get in touch

Unused slides

Sending a Message: What dials can we turn?



$$y(t) = \boldsymbol{A} \cdot \sin(2\pi \boldsymbol{f} t + \boldsymbol{\phi})$$

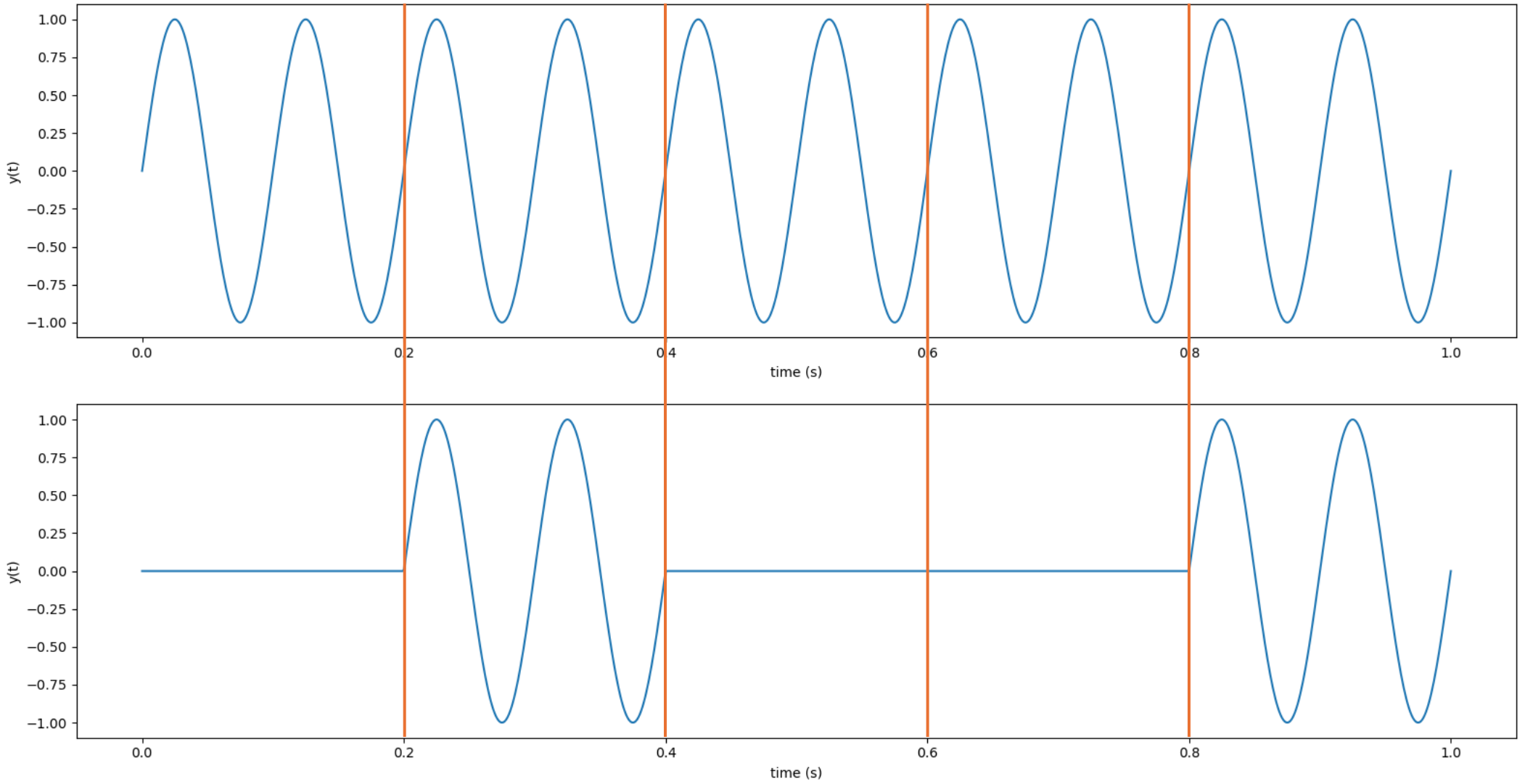
A: Amplitude
f: Frequency
ϕ: Phase

What do these modulation schemes look like?

Modulation: Amplitude Shift Keying

As used in car keys and Christmas light remotes!

0 1 0 0 1



Carrier wave

ASK waveform

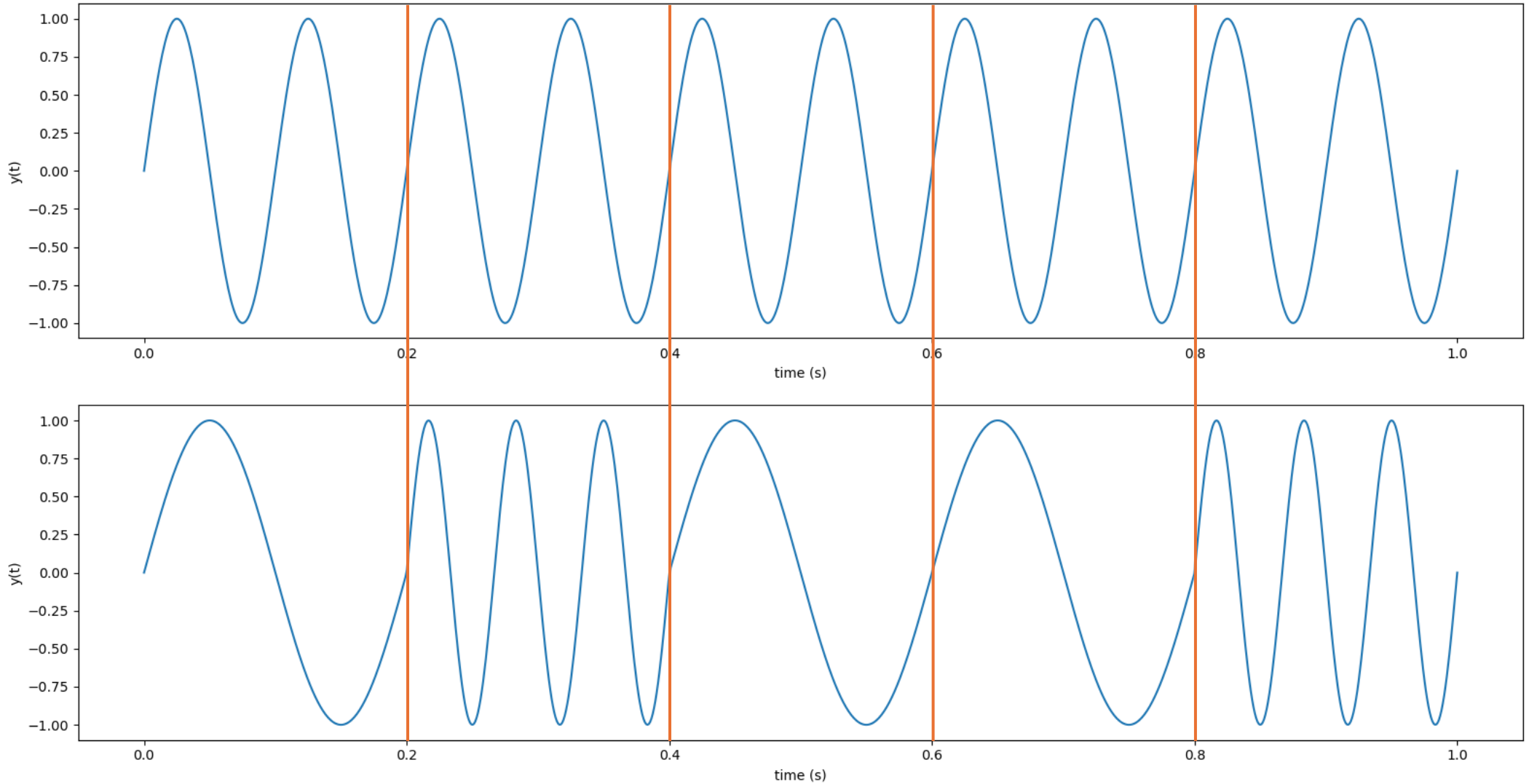
Created using a variation of Bill Buchanan's digital modulation code [2]

[1] W. J. Buchanan, "ASK, FSK and PSK," 2024. Available: https://asecuritysite.com/comms/plot03 (accessed Sep. 10 2024).

Modulation: Frequency Shift Keying

Used in weather balloon radiosondes [1]

0 1 0 0 1



Carrier wave

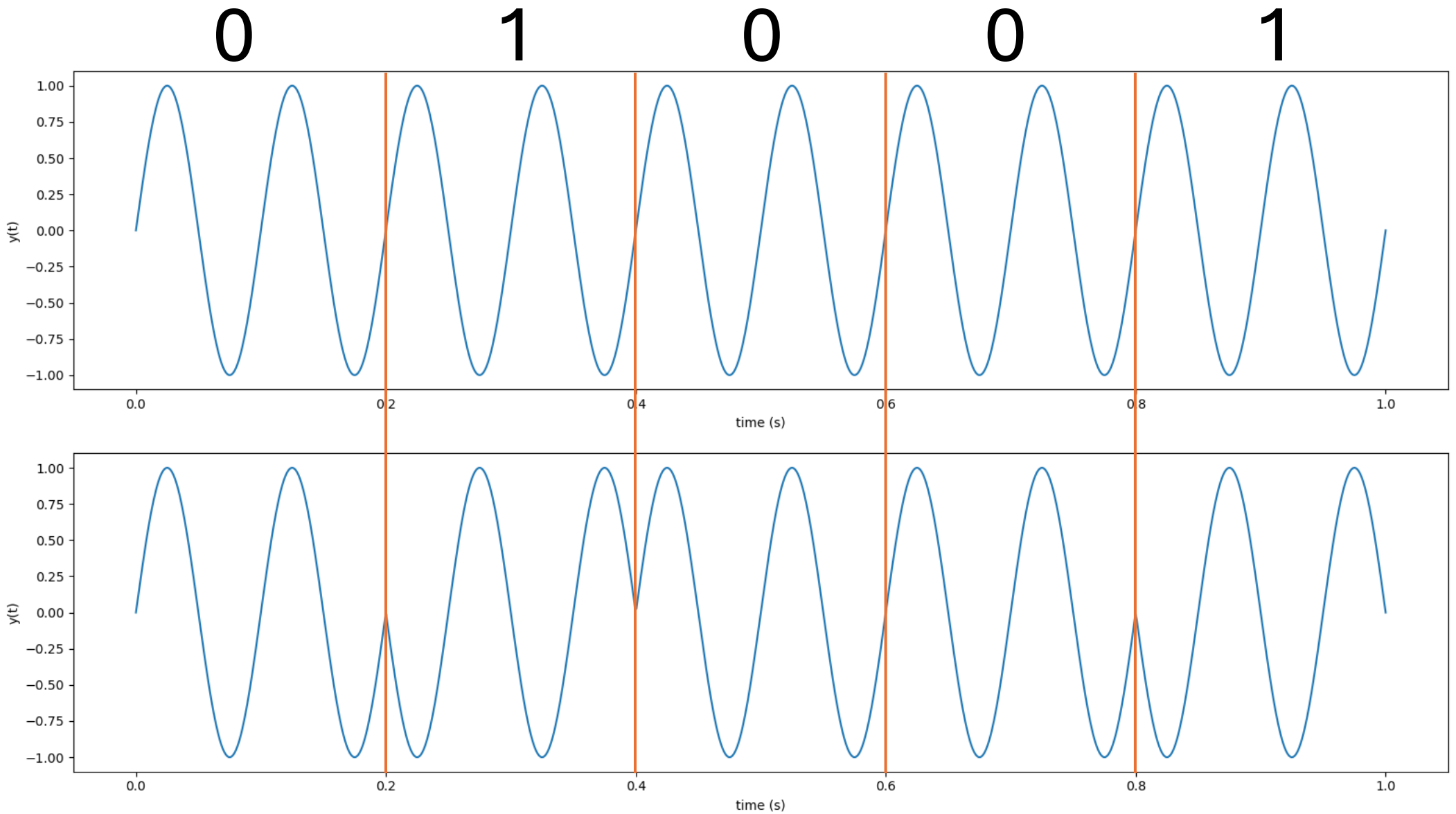
FSK waveform

Created using a variation of Bill Buchanan's digital modulation code [2]

[1] bazjo, "RS41_Decoding," GitHub [Online] 2019. Available: https://github.com/bazjo/RS41_Decoding (accessed Sep. 11, 2024).
[2] W. J. Buchanan, "ASK, FSK and PSK," 2024. Available: https://asecuritysite.com/comms/plot03 (accessed Sep. 10 2024).

Modulation: Phase Shift Keying

A variant is used in GSM [1]



Carrier wave

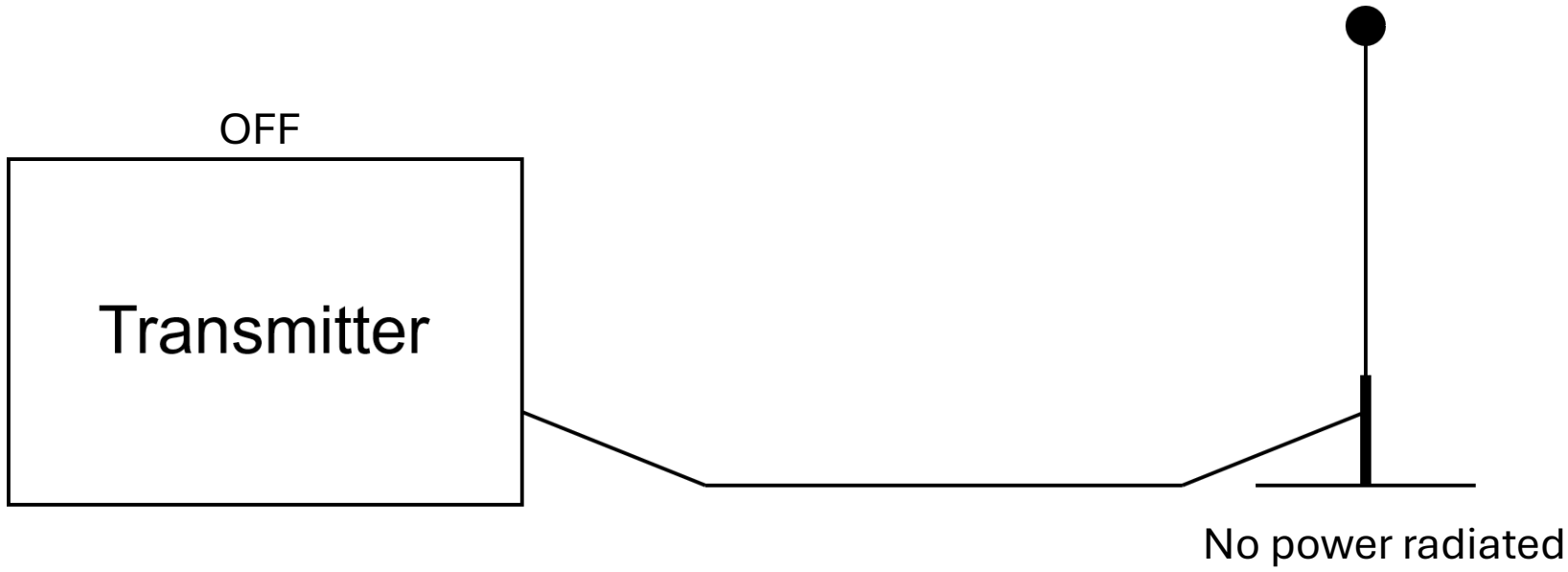
PSK waveform

Created using a variation of Bill Buchanan's digital modulation code [2]

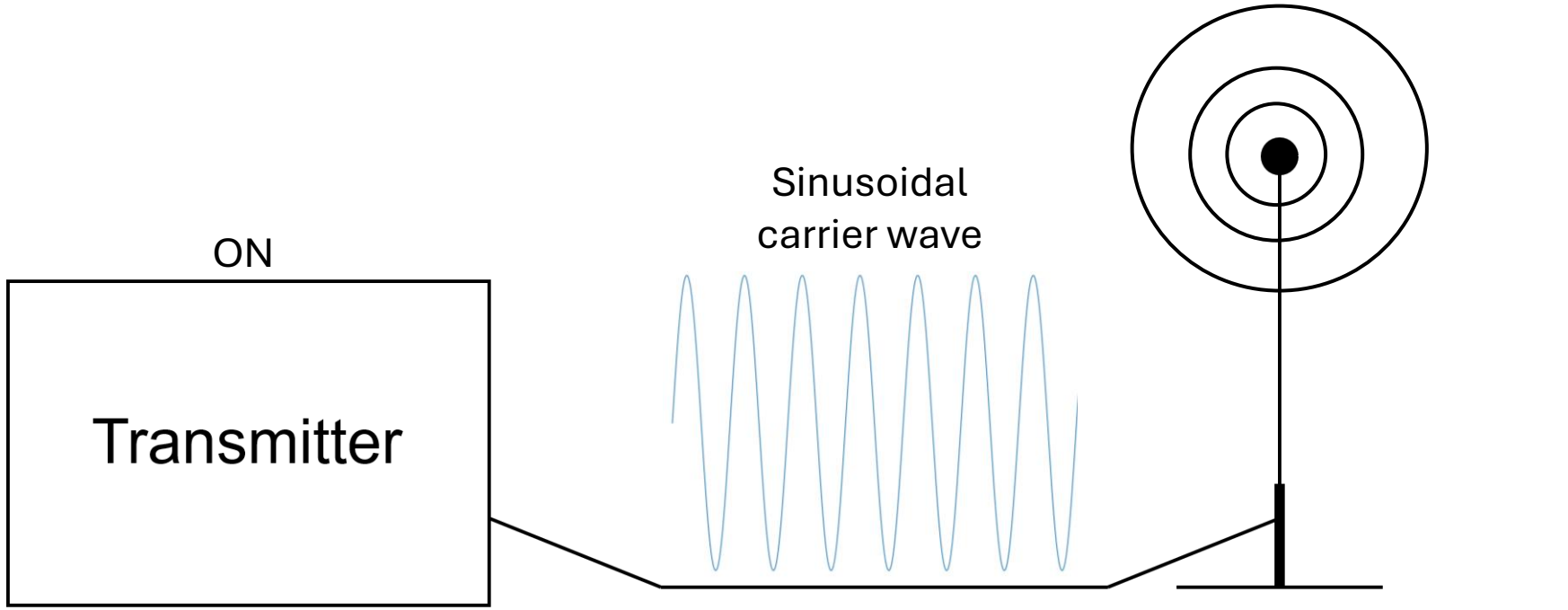
[1] ETSI, "2nd Generation (GERAN)," [Online]. https://www.etsi.org/technologies/mobile/2g?jjj=1725834216070 (accessed Sep. 11, 2024).
[2] W. J. Buchanan, "ASK, FSK and PSK," 2024. Available: https://asecuritysite.com/comms/plot03 (accessed Sep. 10 2024).

Sending a message: The carrier wave

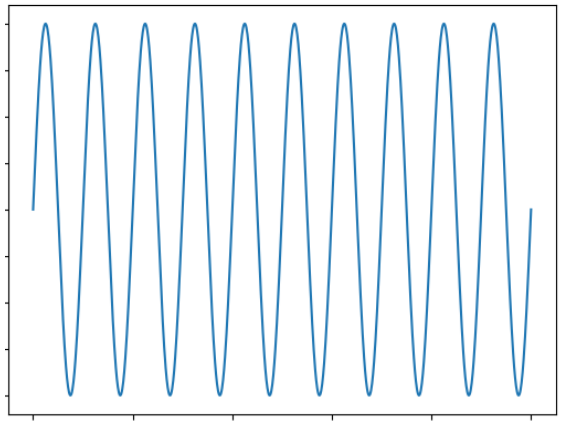
Sending a Message: The carrier wave



Sending a Message: The carrier wave



Sending a Message: Modulation

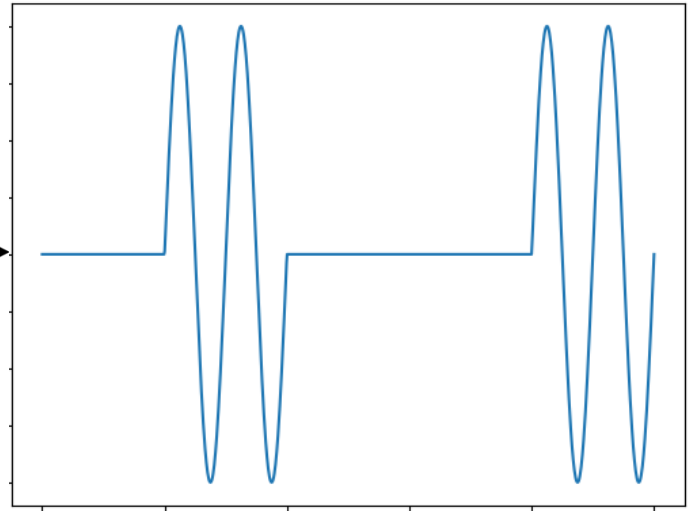


Carrier wave

Modulation

...0,1,0,0,1...

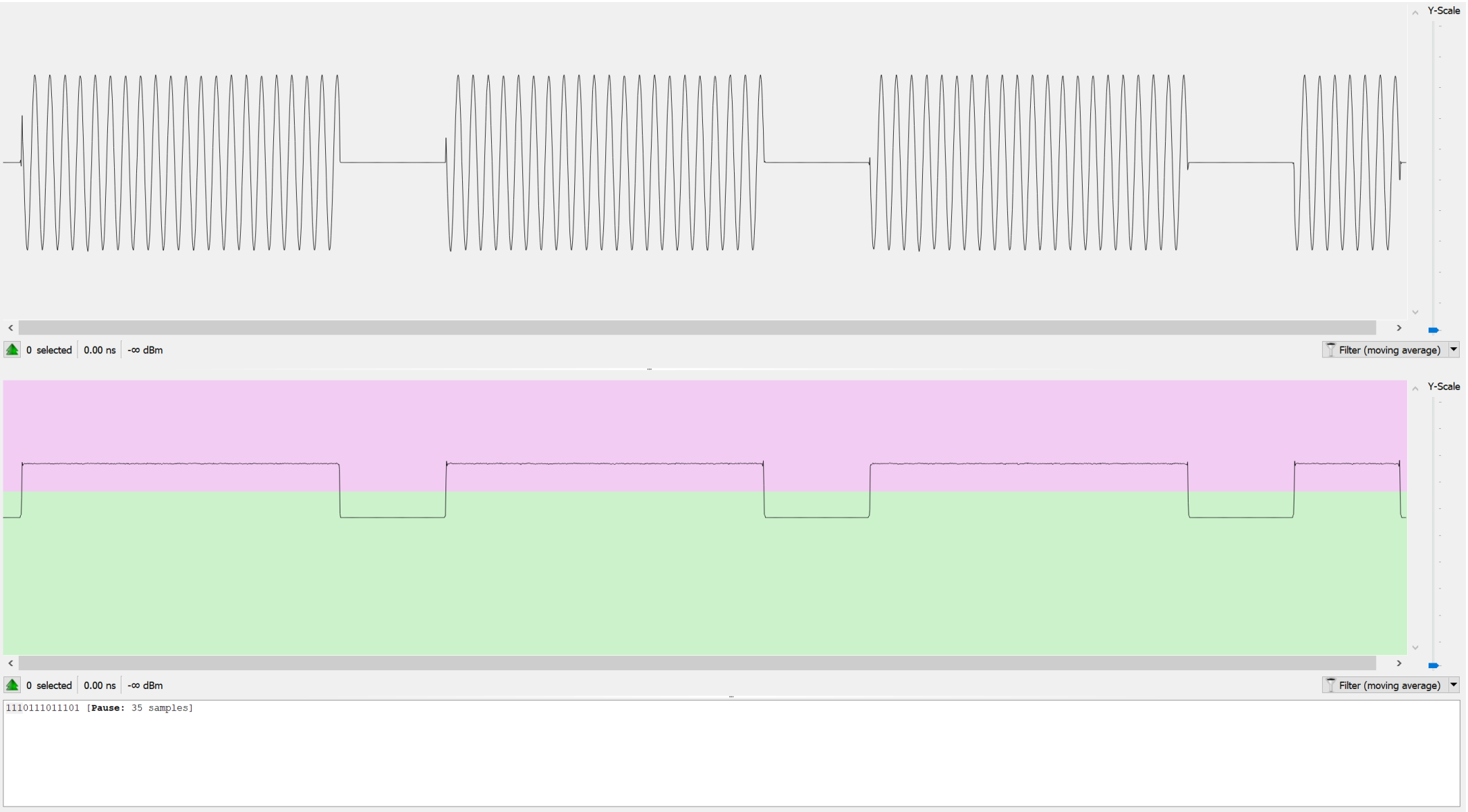
Data



Modulated waveform
(Amplitude shift keying [1])

[1] W. J. Buchanan, “ASK, FSK and PSK,” 2024. Available: https://asecuritysite.com/comms/plot03 (accessed Sep. 10 2024)

Received ASK-modulated Signal



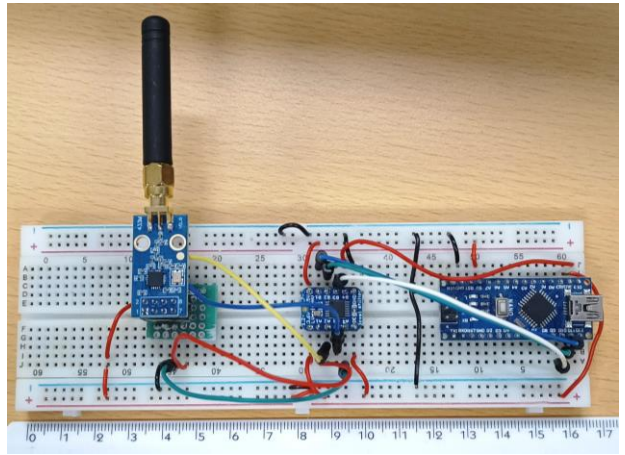
Received signal

Demodulated signal
Red: 1, green: 0

Demodulated data:
1110111011101

Interpretation screen in Universal Radio Hacker

Quick Hardware Comparison

	Flipper Zero	SDR (e.g., HackRF One, USRP)	TI CC1101 with dev board (e.g., Arduino or Raspberry Pi)
Price	£165.00 [1]	£219.70 [2]	< £30.00
Flexibility	Swiss army knife – Covers a broad range of wireless domains	Extremely flexible within its frequency range	Moderate – Has a finite list of supported modulation schemes
Ease of use	Straightforward for supported use cases	Depends on software, but starting is easy	DIY
Frequency range	< 1GHz and a number of other bands/protocols [3]	HackRF One: 1MHz to 6 GHz [4]	300-348MHz, 387-464MHz, 779-928MHz [5]
Image	 Flipper Zero image courtesty of Turbospok [6]		

Threat Modelling: My opinion

Threat	Goal	Applicability of RF attacks against car security
Opportunistic valuables thief	Steal any valuables from the vehicle	• Cheaper, easier and more convenient to use a brick or similar to smash a window rather than hack the car
Car thief	Steal the vehicle itself	• Must have a way to start engine once inside car • Gaining entry via a smashed window requires much less preparation time than executing discussed attacks
Investigator/stalker	Covertly plant a tracking/listening device in vehicle	• Previous attacks allow for tracking device to be placed inside car without arousing suspicion • Carrying out these attacks requires more preparation than placing tracker on car exterior