Ghost Peak:

Practical Distance Reduction Attacks Against HRP UWB Ranging

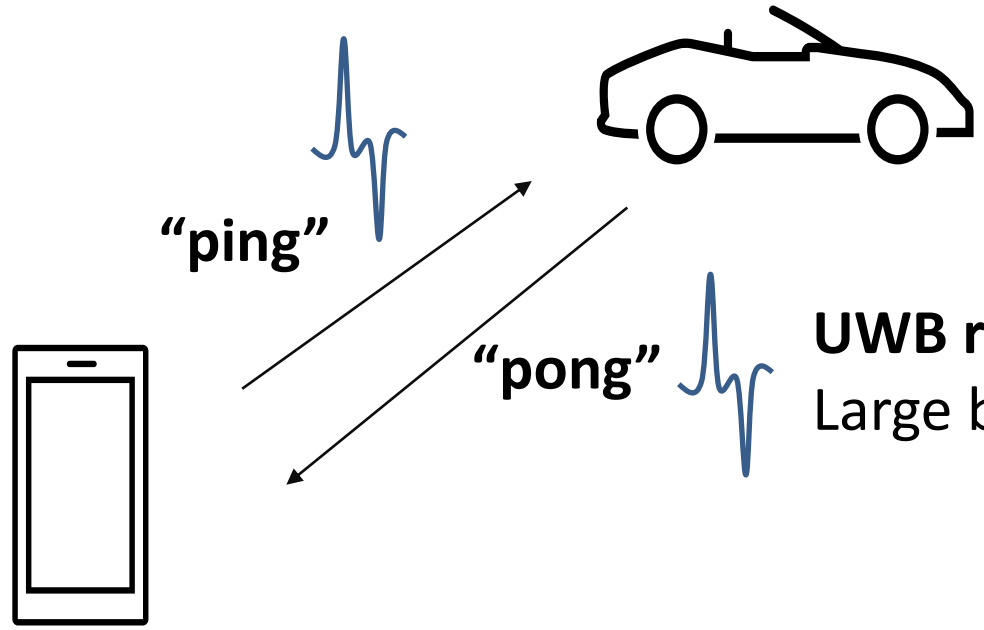
P. Leu[1*], G. Camurati[1*], A. Heinrich[2], M. Roeschlin[1], C. Anliker[1],
M. Hollick[2], S. Capkun[1], J. Classen[2]

[1] ETH zürich [2] SEEMOO SECURE MOBILE NETWORKING TECHNISCHE UNIVERSITÄT DARMSTADT

[*]Equal contribution

https://securepositioning.com/ghost-peak/
https://github.com/seemoo-la/uwb-sniffer

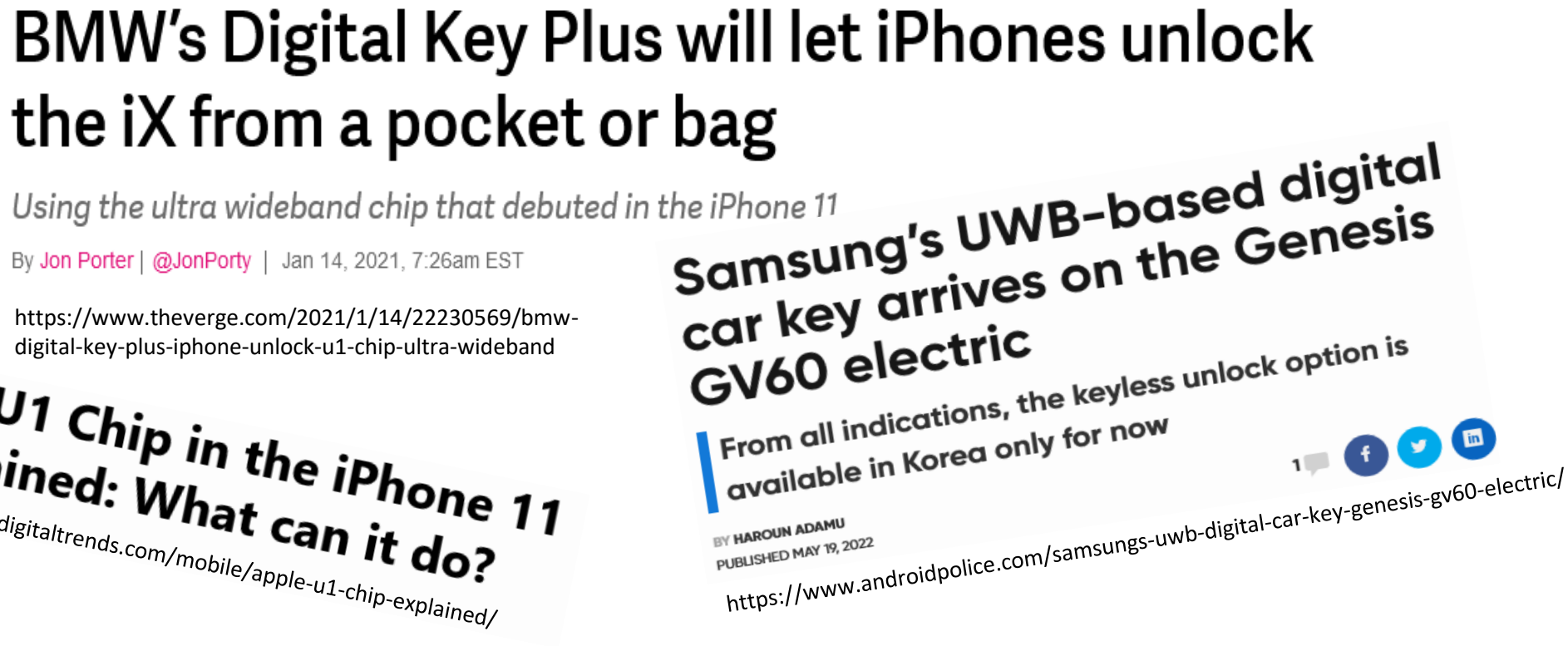
Background: Ultra Wide Band (UWB) ranging in a nutshell



UWB radio pulses
Large bandwidth => high time/distance accuracy

Distance = time-of-flight x speed-of-light

IEEE802.15z High-Repetition Pulse (HRP) UWB is now in your phone, watch, car…



BMW's Digital Key Plus will let iPhones unlock the iX from a pocket or bag

Using the ultra wideband chip that debuted in the iPhone 11

By Jon Porter | @JonPorty | Jan 14, 2021, 7:26am EST

https://www.theverge.com/2021/1/14/22230569/bmw-digital-key-plus-iphone-unlock-u1-chip-ultra-wideband

The U1 Chip in the iPhone 11 explained: What can it do?

https://www.digitaltrends.com/mobile/apple-u1-chip-explained/

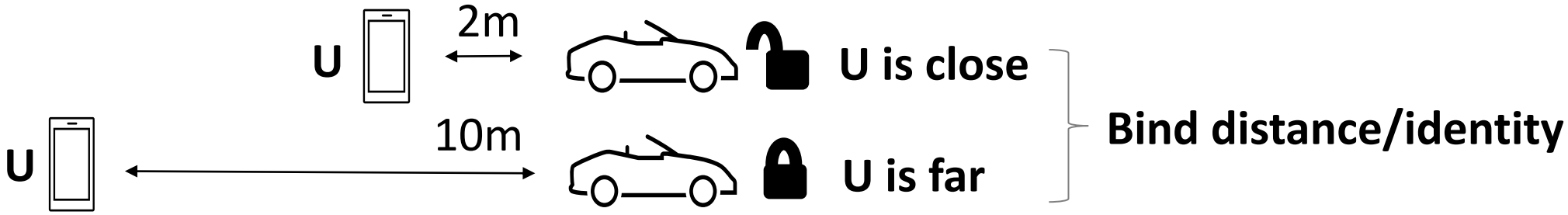
Samsung's UWB-based digital car key arrives on the Genesis GV60 electric

From all indications, the keyless unlock option is available in Korea only for now

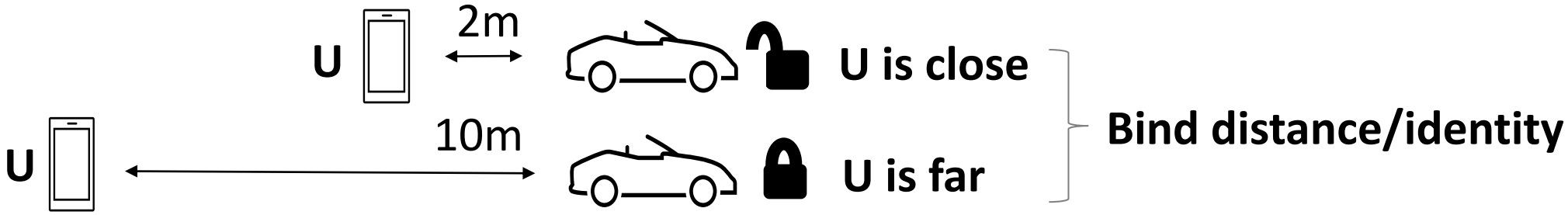
BY HAROUN ADAMU
PUBLISHED MAY 19, 2022

https://www.androidpolice.com/samsungs-uwb-digital-car-key-genesis-gv60-electric/

Motivation: ideal secure ranging and previous solutions

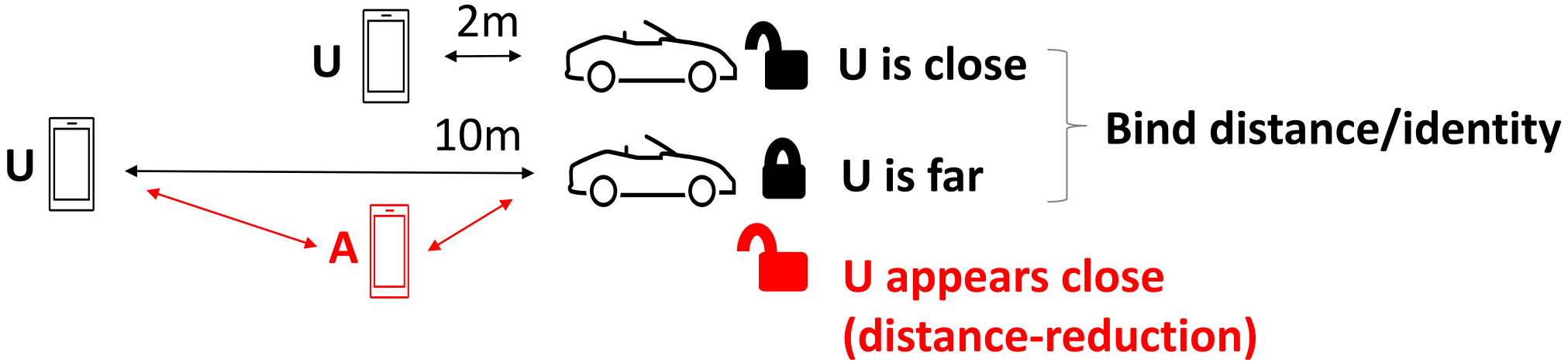


Motivation: ideal secure ranging and previous solutions



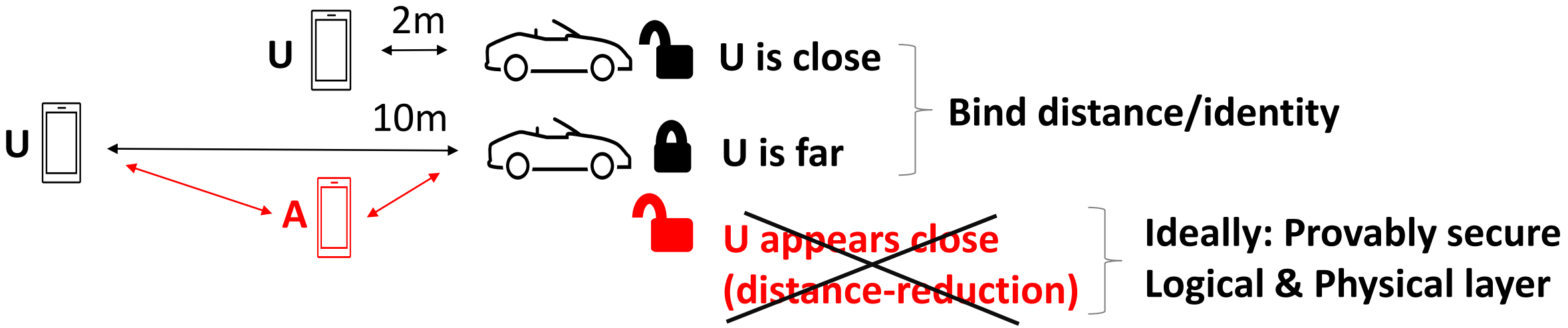
Applications: access control, mobile payments, tracking, automation, …

Motivation: ideal secure ranging and previous solutions



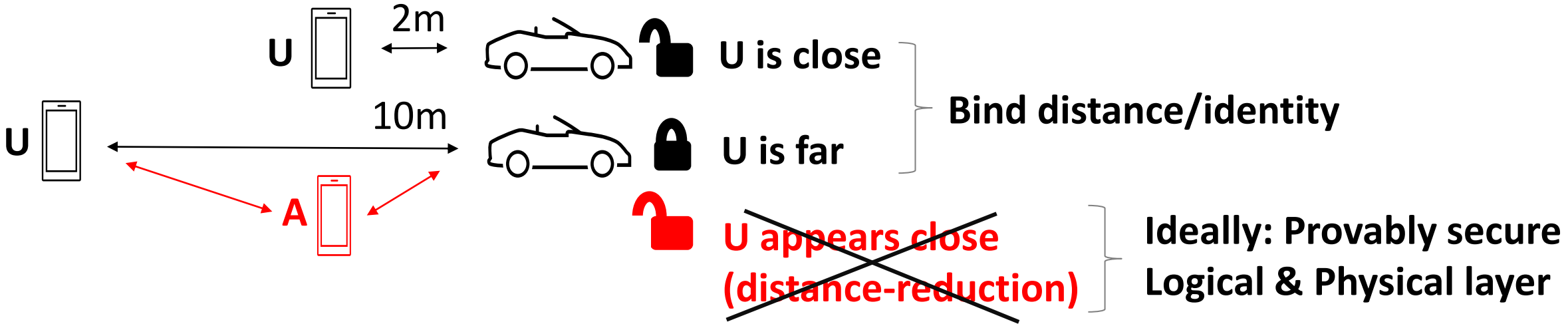
Applications: access control, mobile payments, tracking, automation, …

Motivation: ideal secure ranging and previous solutions



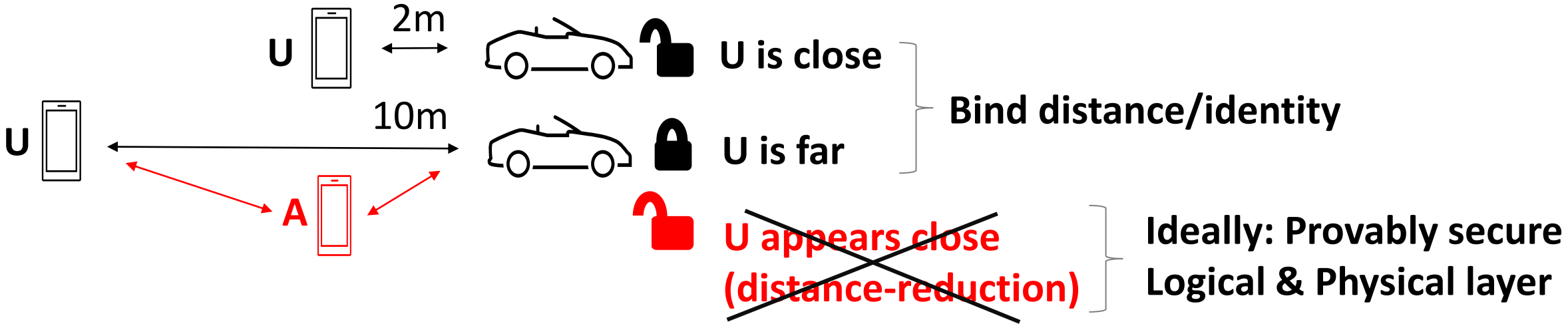
Applications: access control, mobile payments, tracking, automation, …

Motivation: ideal secure ranging and previous solutions



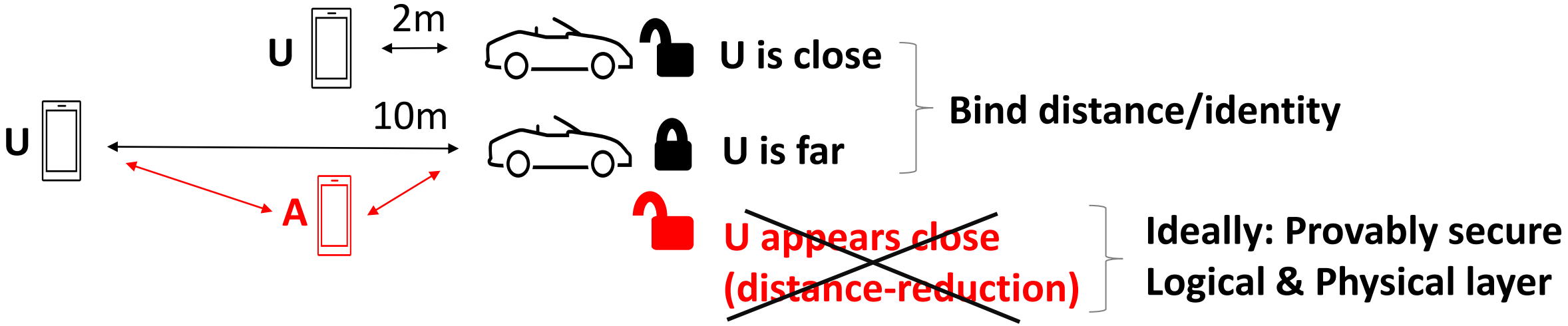
Applications: access control, mobile payments, tracking, automation, …
Insecure solutions: e.g., signal strength (RSSI)

Motivation: ideal secure ranging and previous solutions



Applications: access control, mobile payments, tracking, automation, …
Insecure solutions: e.g., signal strength (RSSI)
Secure solutions: e.g., low-repetition pulse (LRP) ultra wide band (UWB)

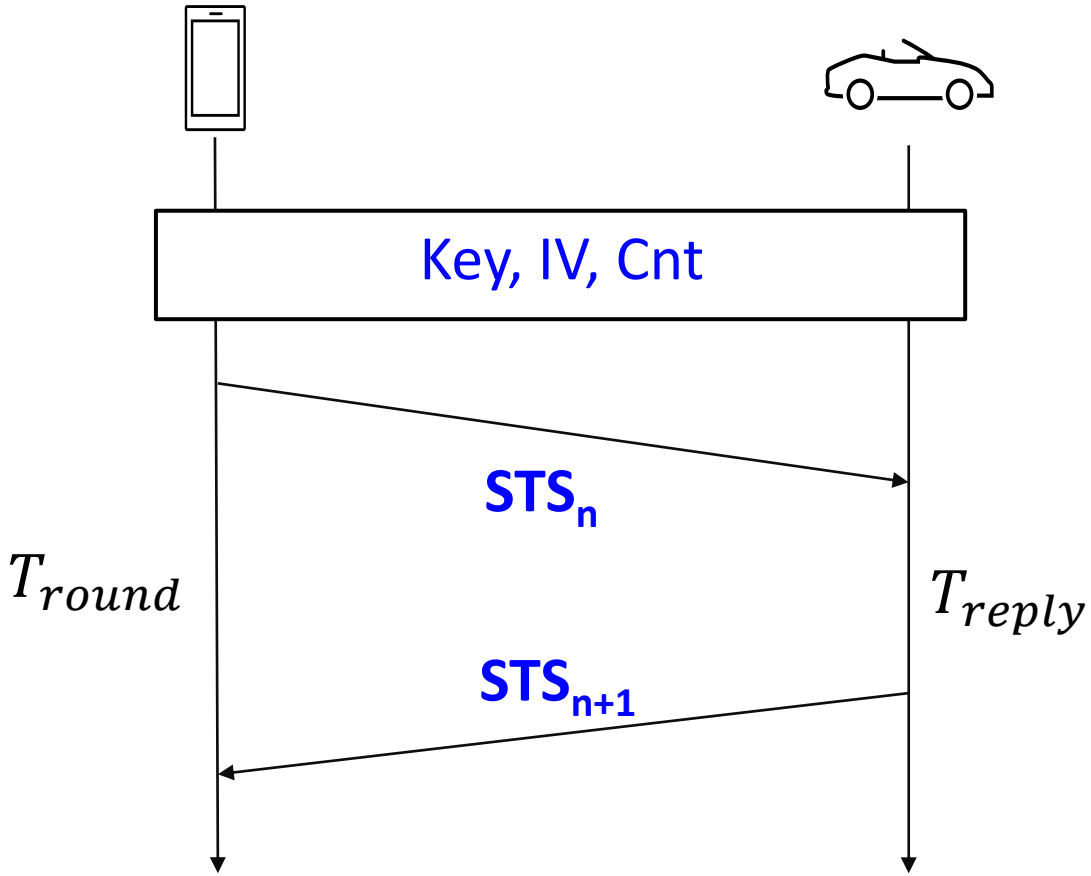
Motivation: ideal secure ranging and previous solutions



Applications: access control, mobile payments, tracking, automation, …
Insecure solutions: e.g., signal strength (RSSI)
Secure solutions: e.g., low-repetition pulse (LRP) ultra wide band (UWB)

What about HRP UWB? Is it secure?

Background: IEEE802.15z HRP UWB logical layer (simplified)

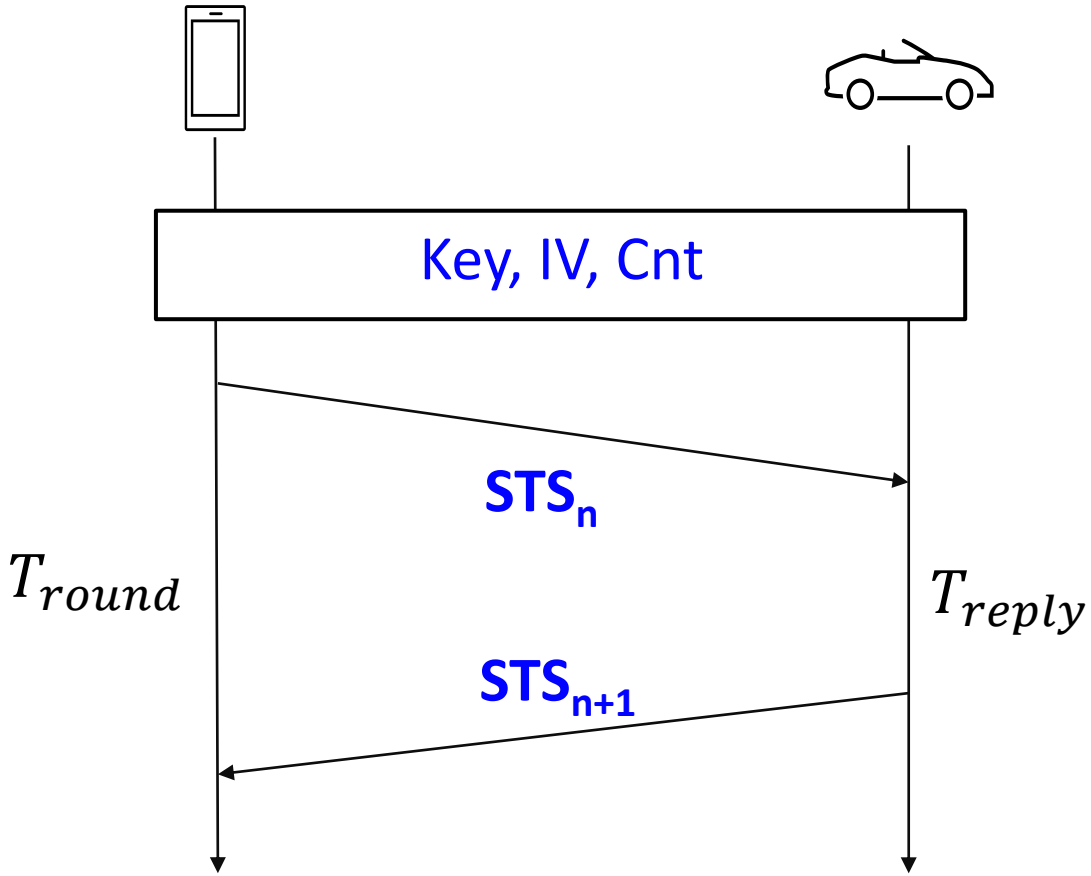


$$d = c\,(T_{round} - T_{reply})/2$$

STS = Scrambed Time Sequence

- E.g., 4096 pulses
- Cryptographycally secure sequence
- AES in counter mode

Background: IEEE802.15z HRP UWB logical layer (simplified)



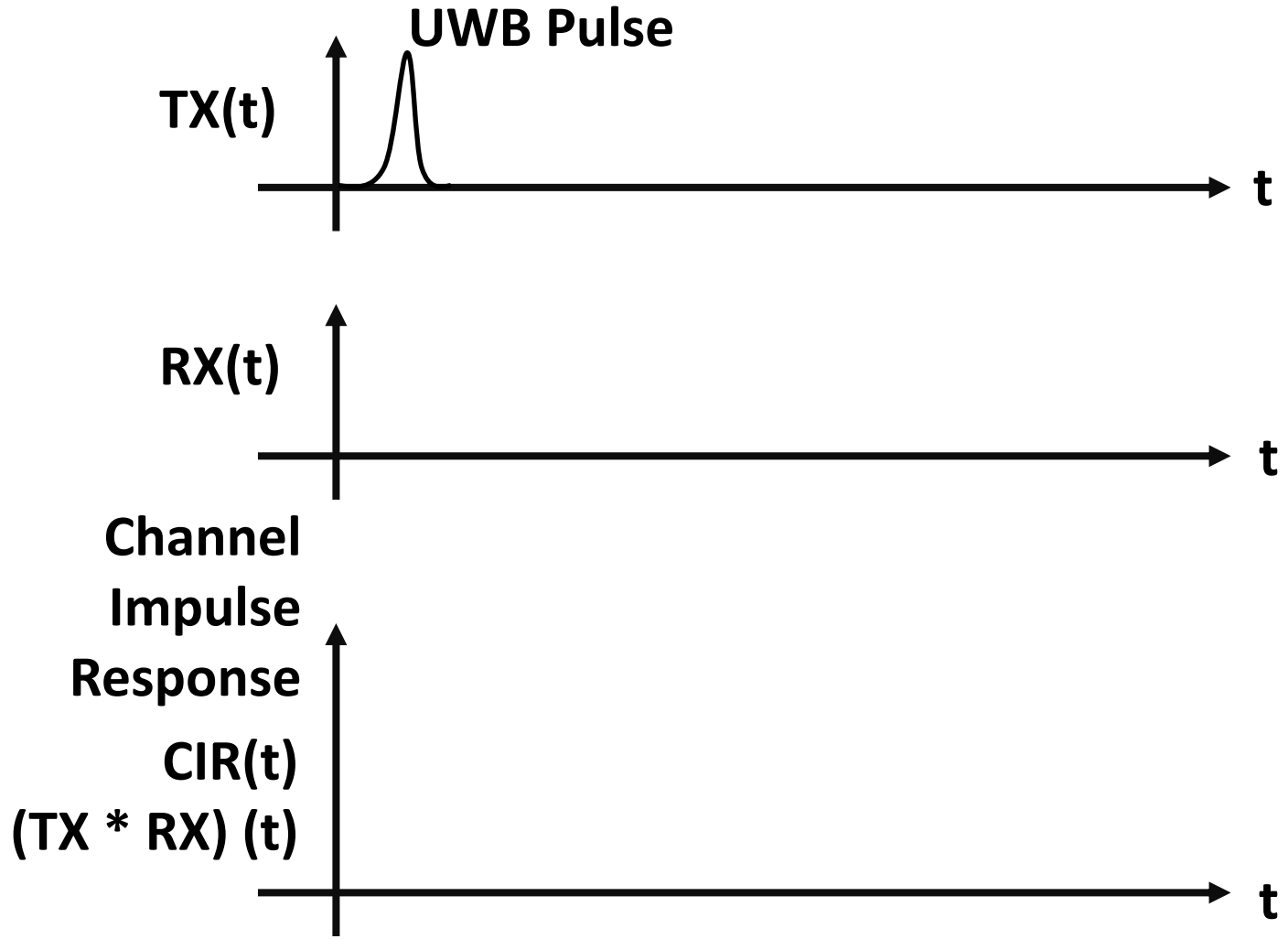
$$d = c\,(T_{round} - T_{reply})/2$$

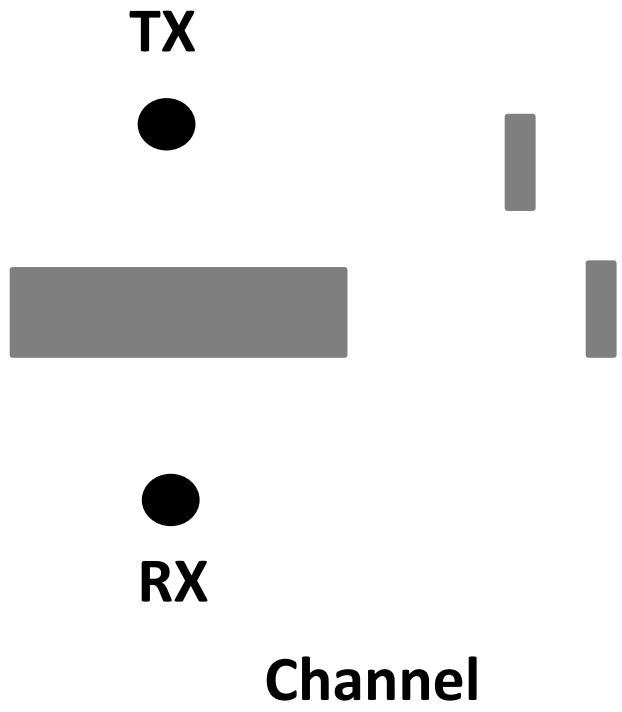
STS = Scrambed Time Sequence

- E.g., 4096 pulses
- Cryptographycally secure sequence
- AES in counter mode

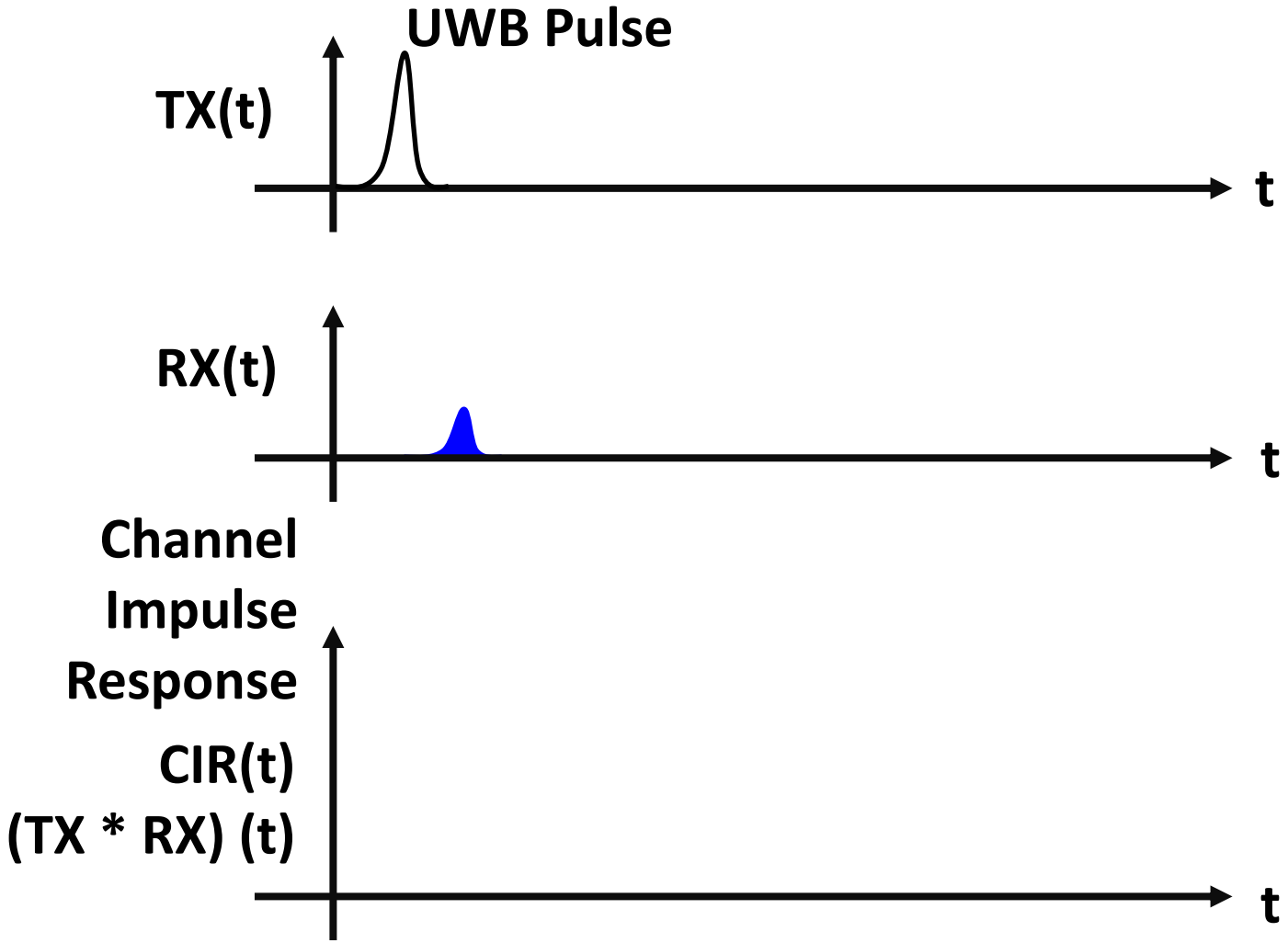
Unpredictable
=> An attacker cannot anticipate transmission to shorten the distance

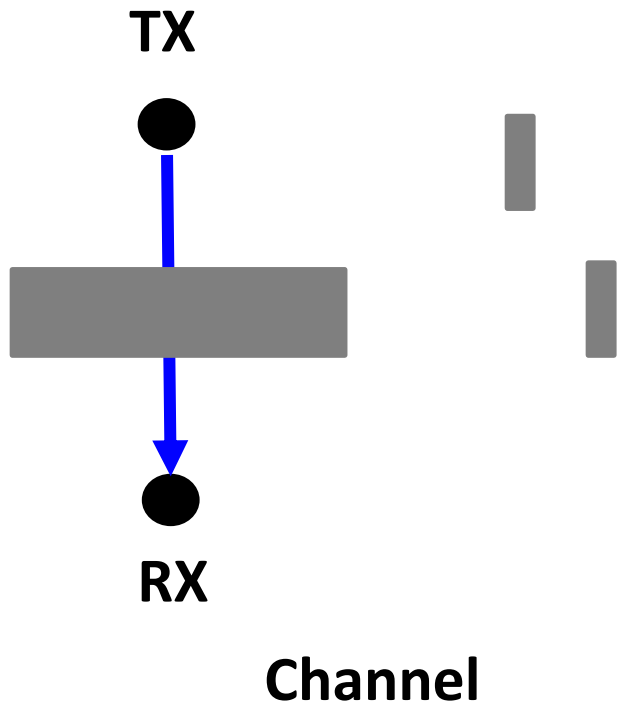
Background: IEEE802.15z HRP UWB physical layer (simplified)



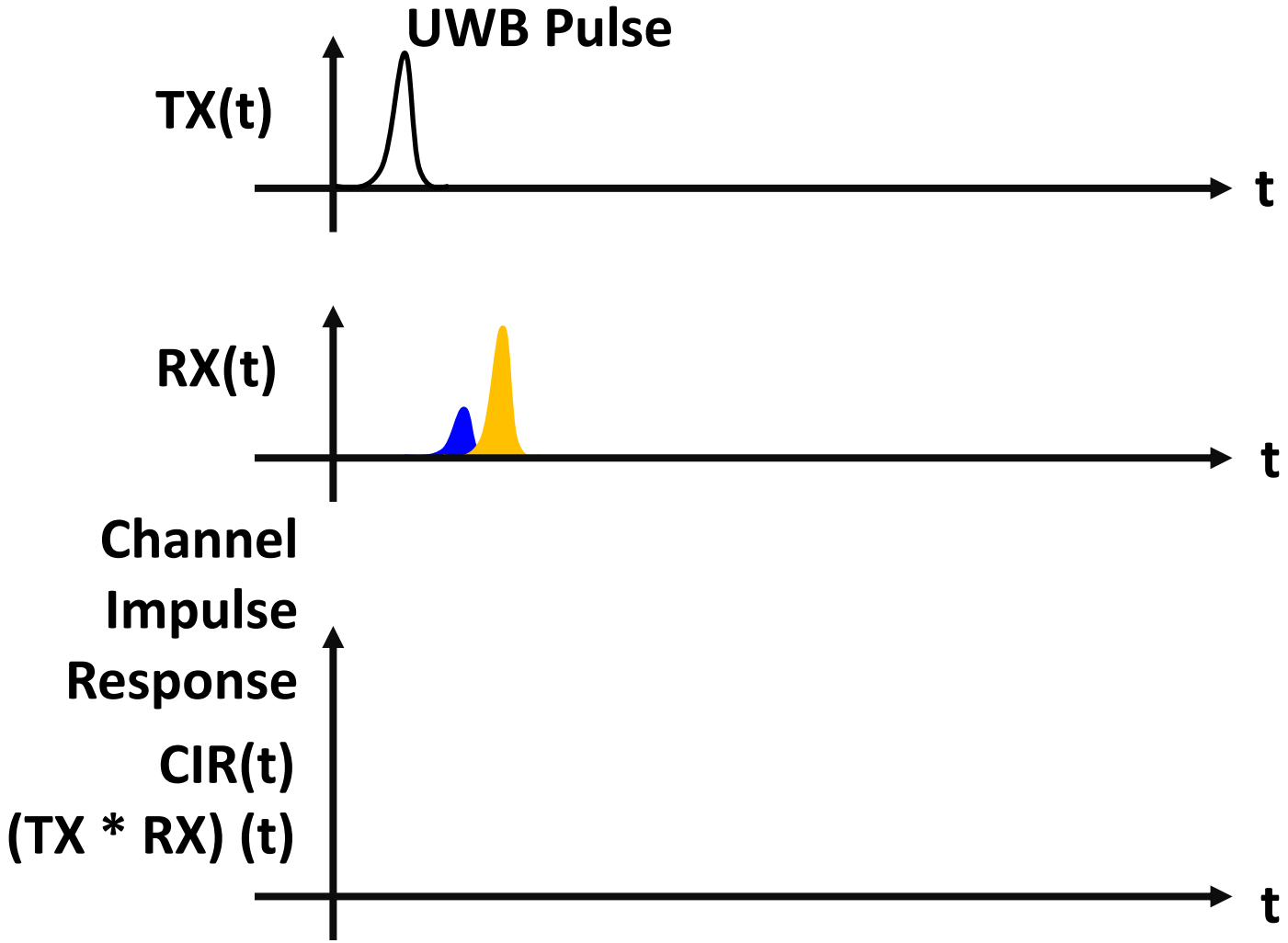


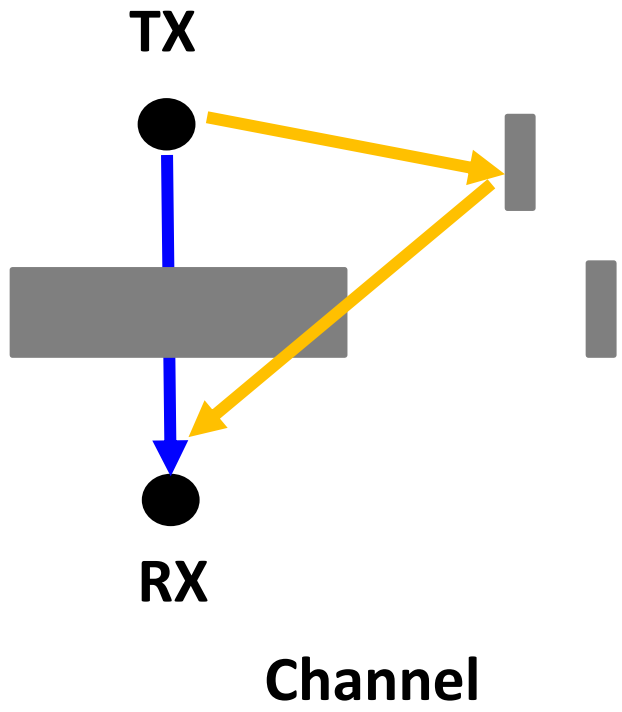
Background: IEEE802.15z HRP UWB physical layer (simplified)



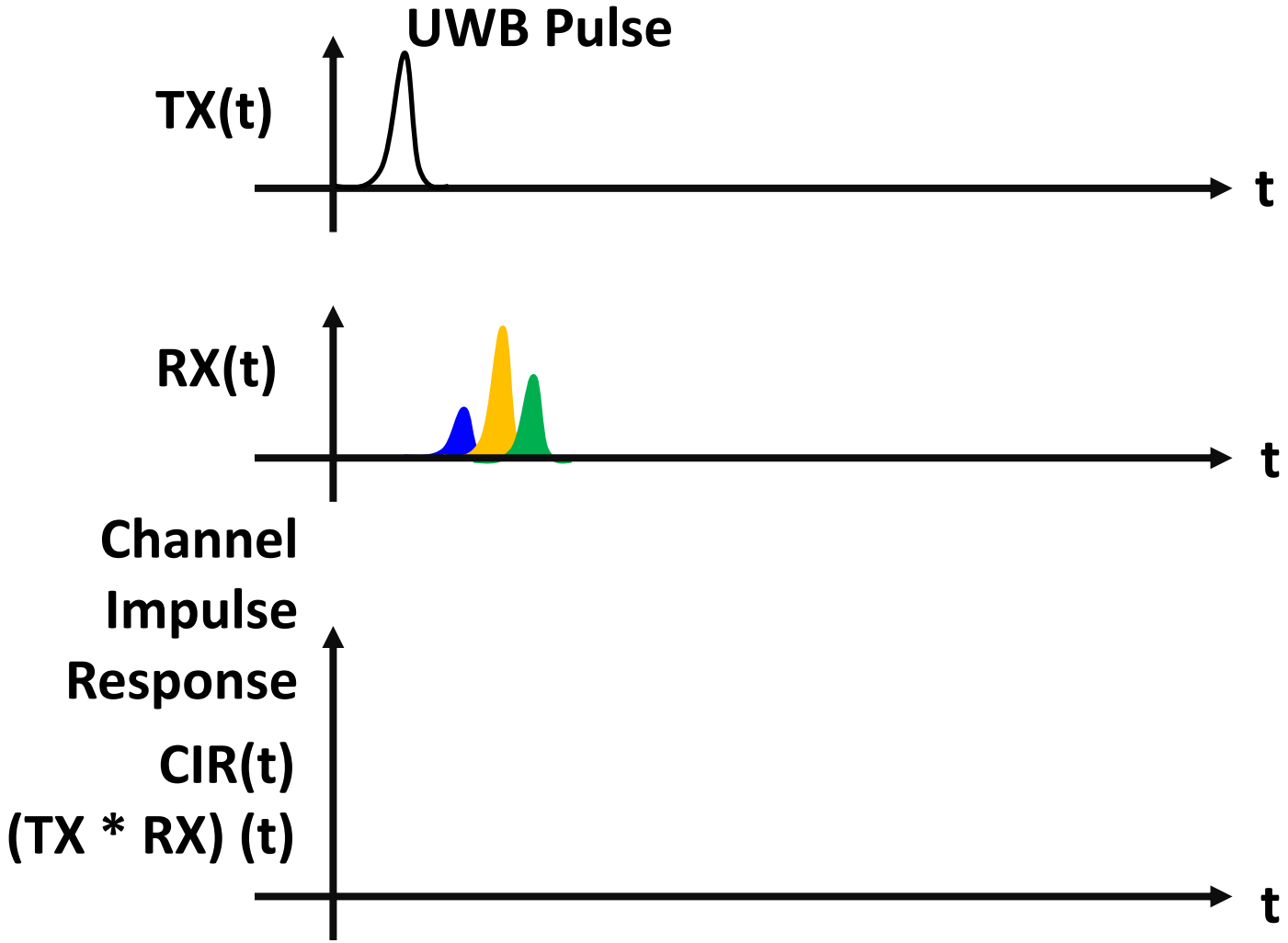


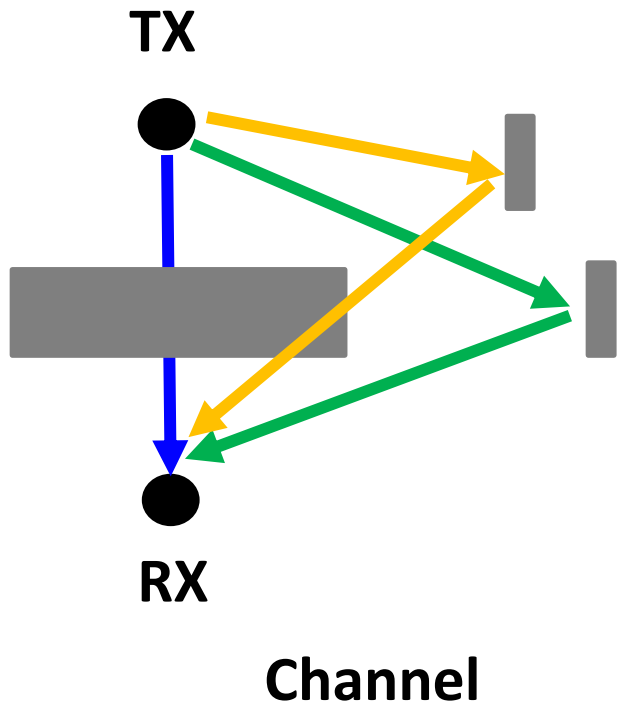
Background: IEEE802.15z HRP UWB physical layer (simplified)



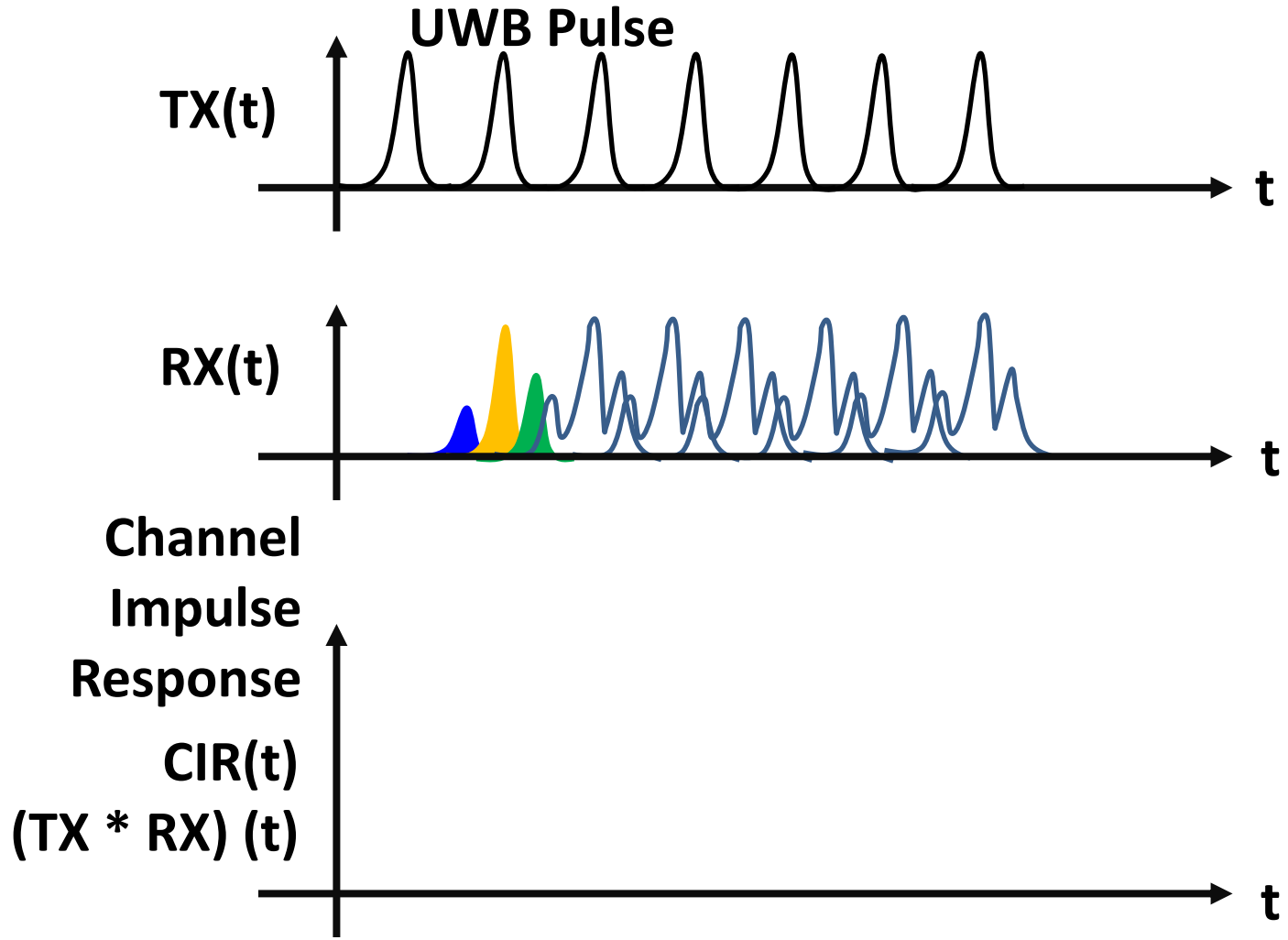


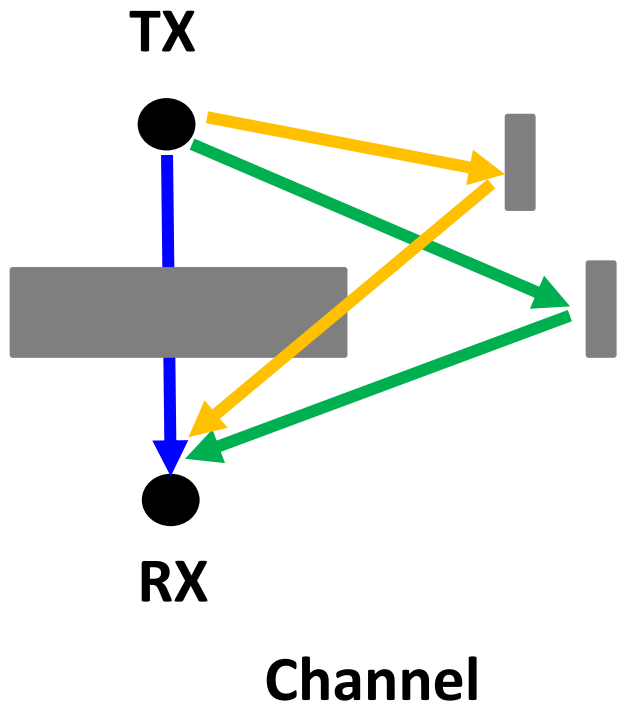
Background: IEEE802.15z HRP UWB physical layer (simplified)



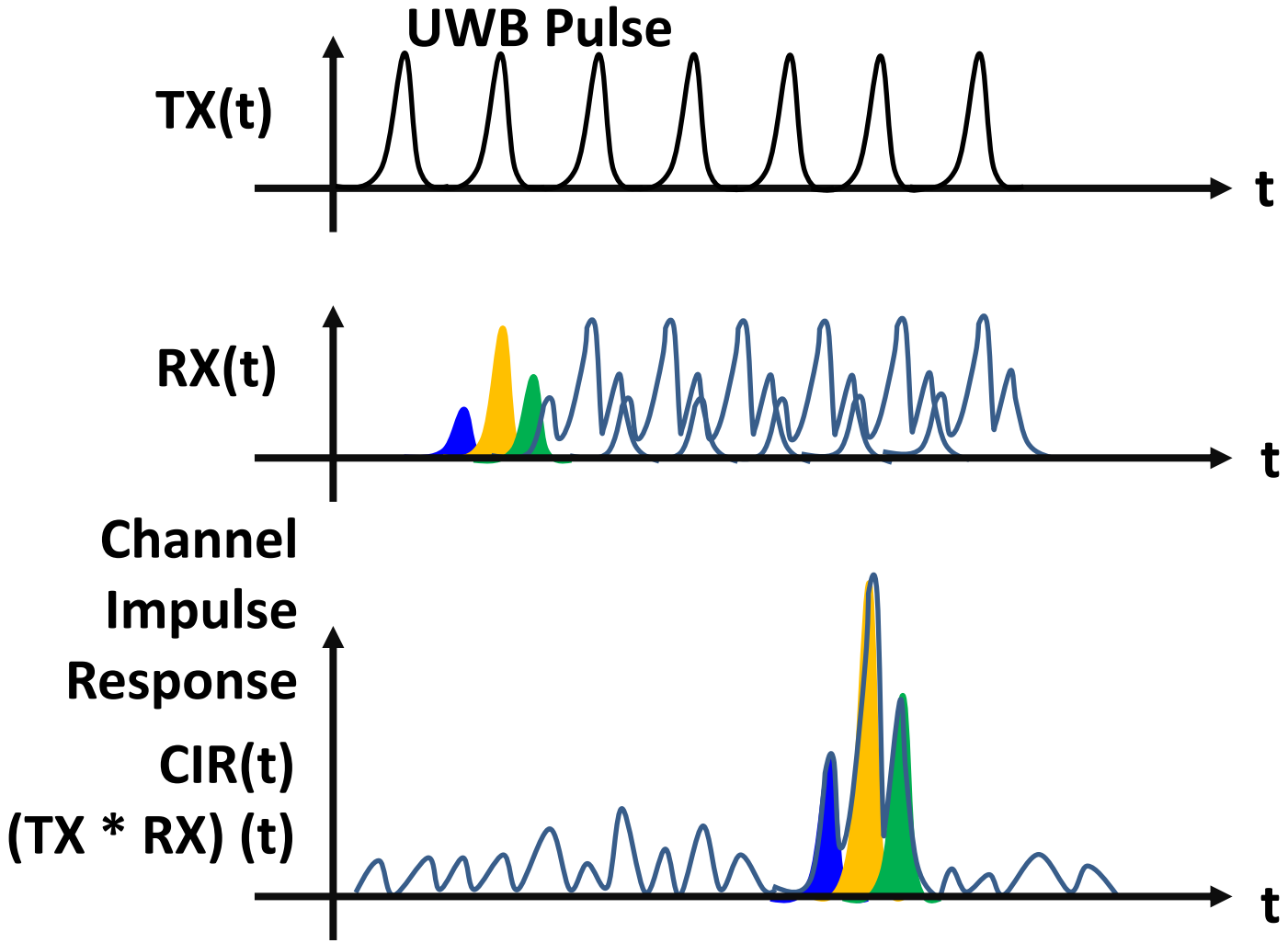


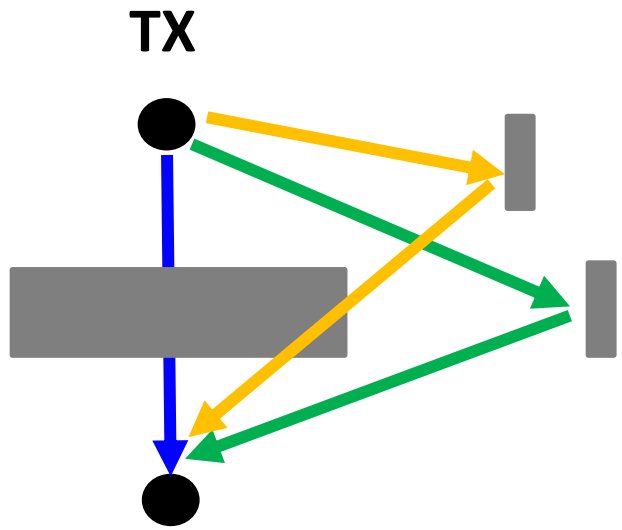
Background: IEEE802.15z HRP UWB physical layer (simplified)



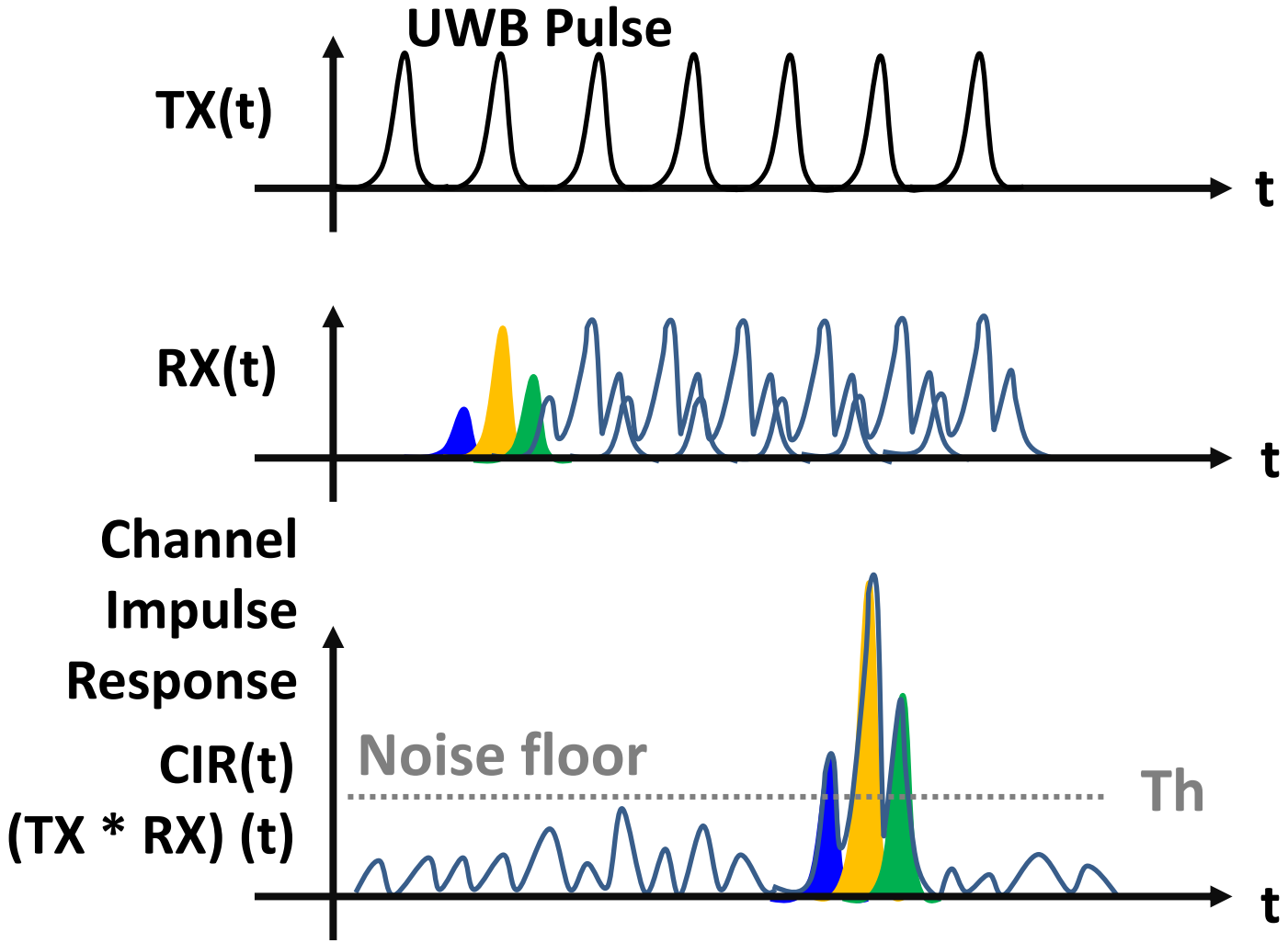


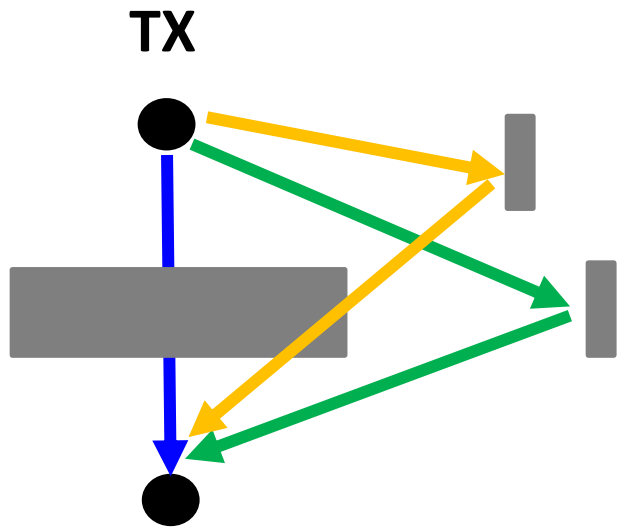
Background: IEEE802.15z HRP UWB physical layer (simplified)





Background: IEEE802.15z HRP UWB physical layer (simplified)

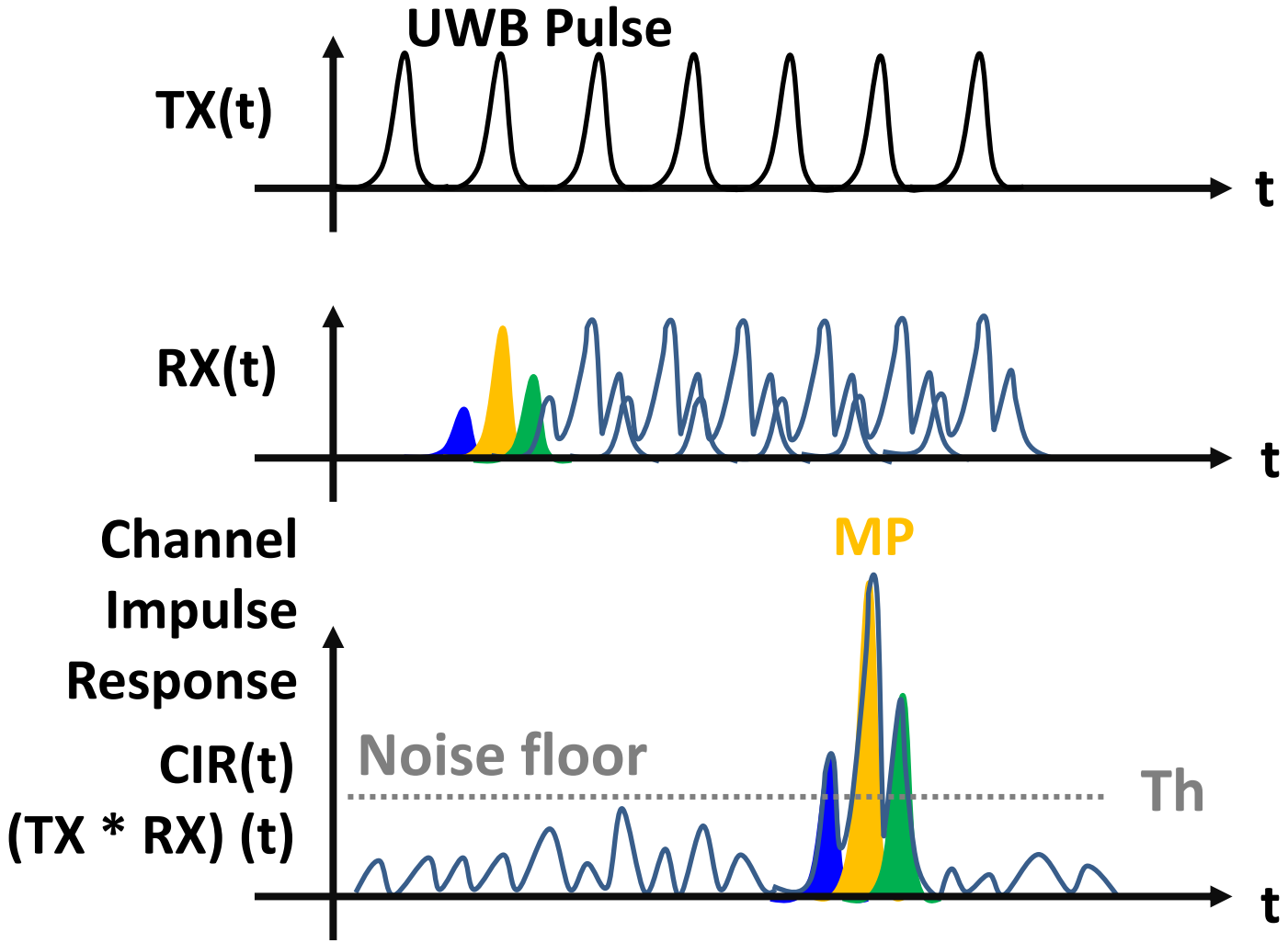


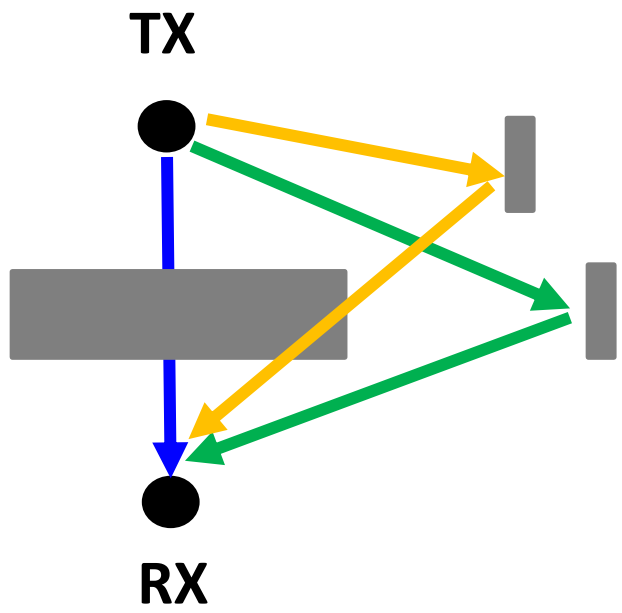


Channel

ETH zürich
TECHNISCHE UNIVERSITÄT DARMSTADT

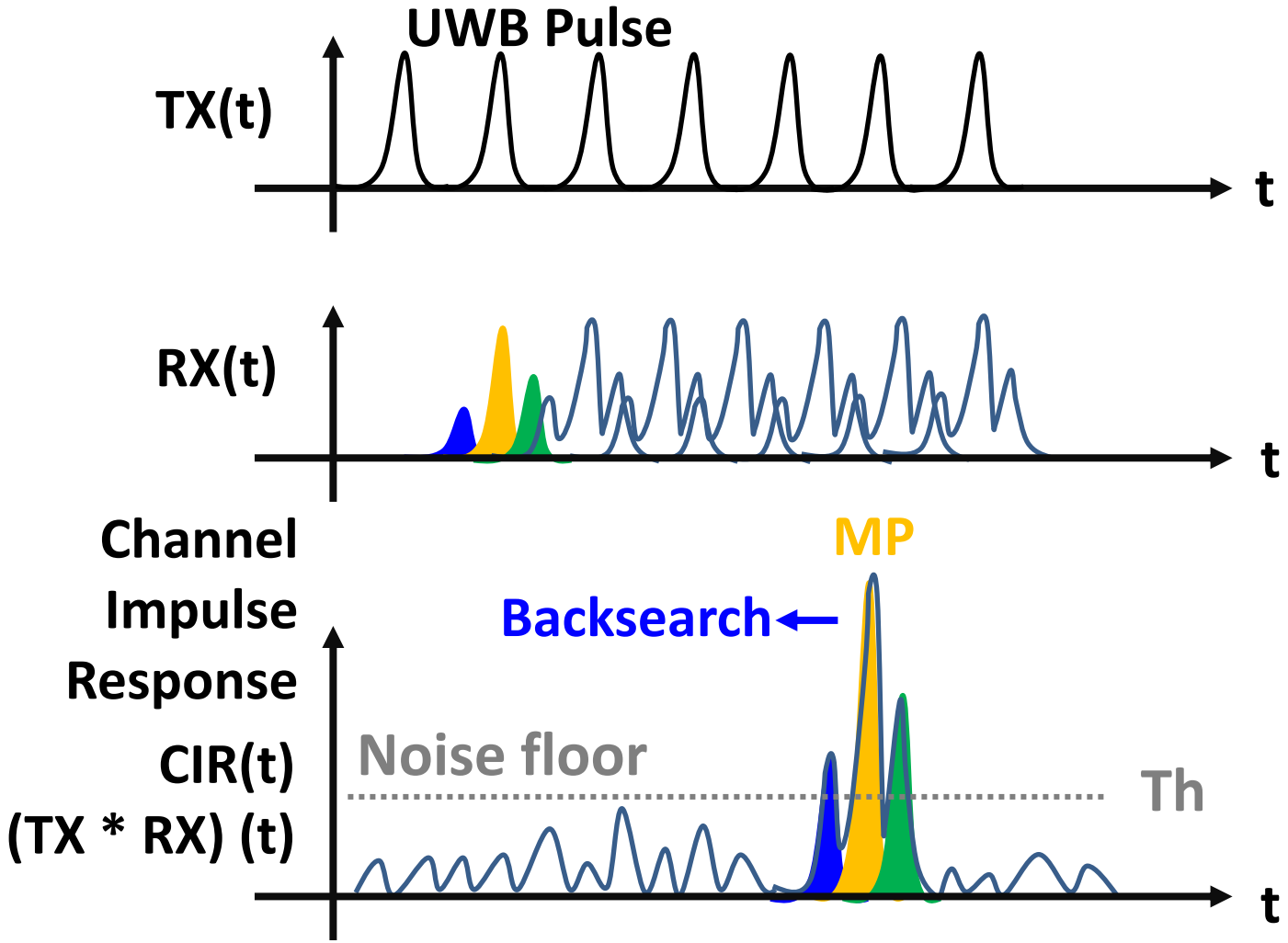
Background: IEEE802.15z HRP UWB physical layer (simplified)

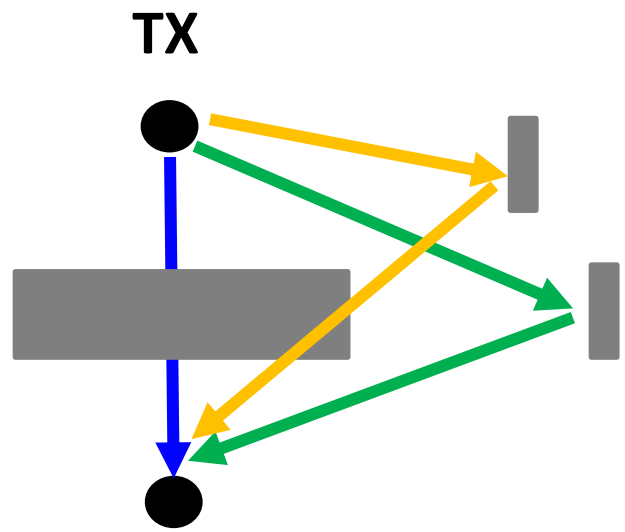




ETH zürich
TECHNISCHE UNIVERSITÄT DARMSTADT

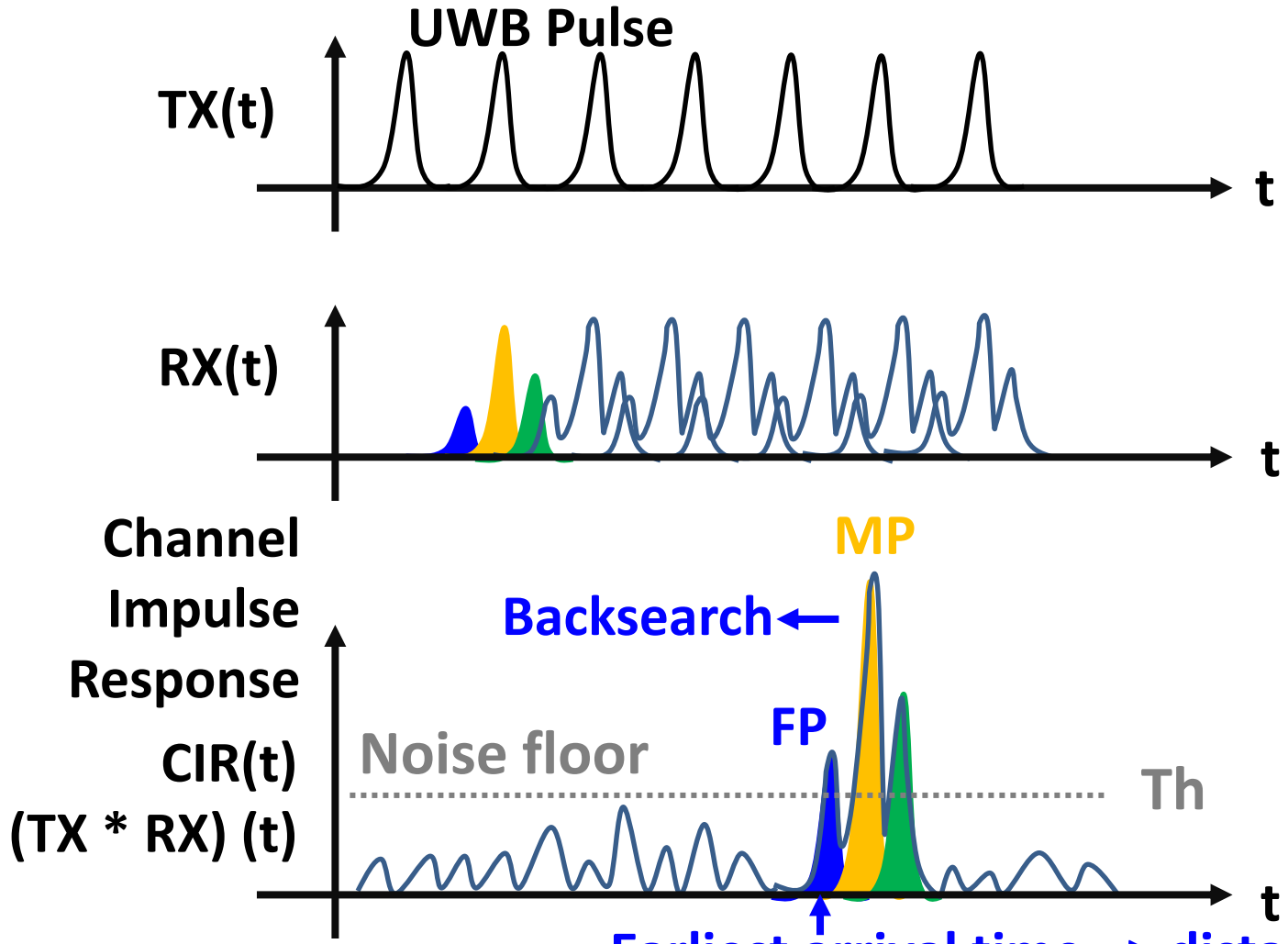
Background: IEEE802.15z HRP UWB physical layer (simplified)

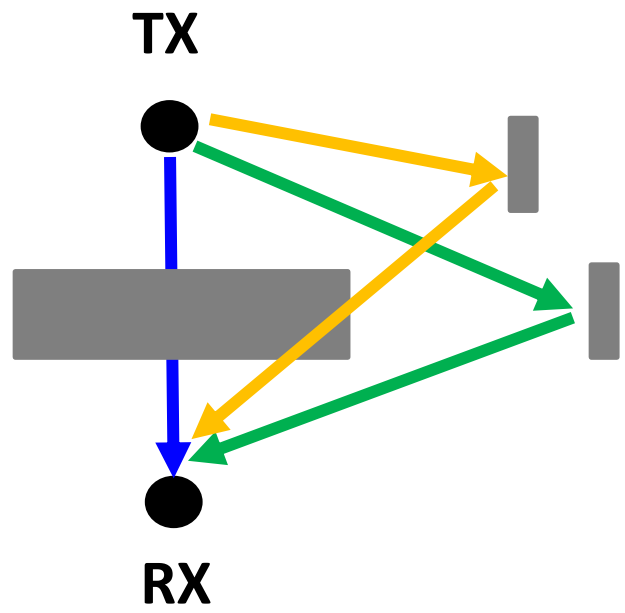




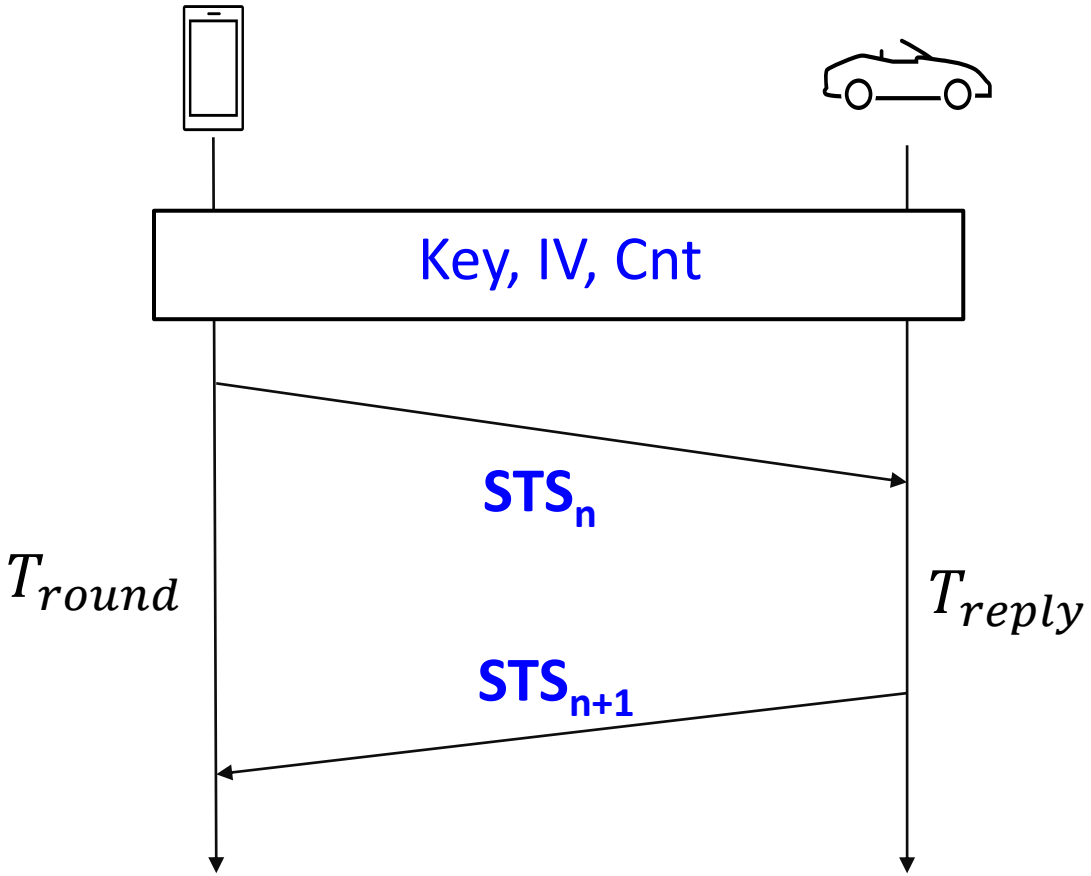
Channel

Background: IEEE802.15z HRP UWB physical layer (simplified)



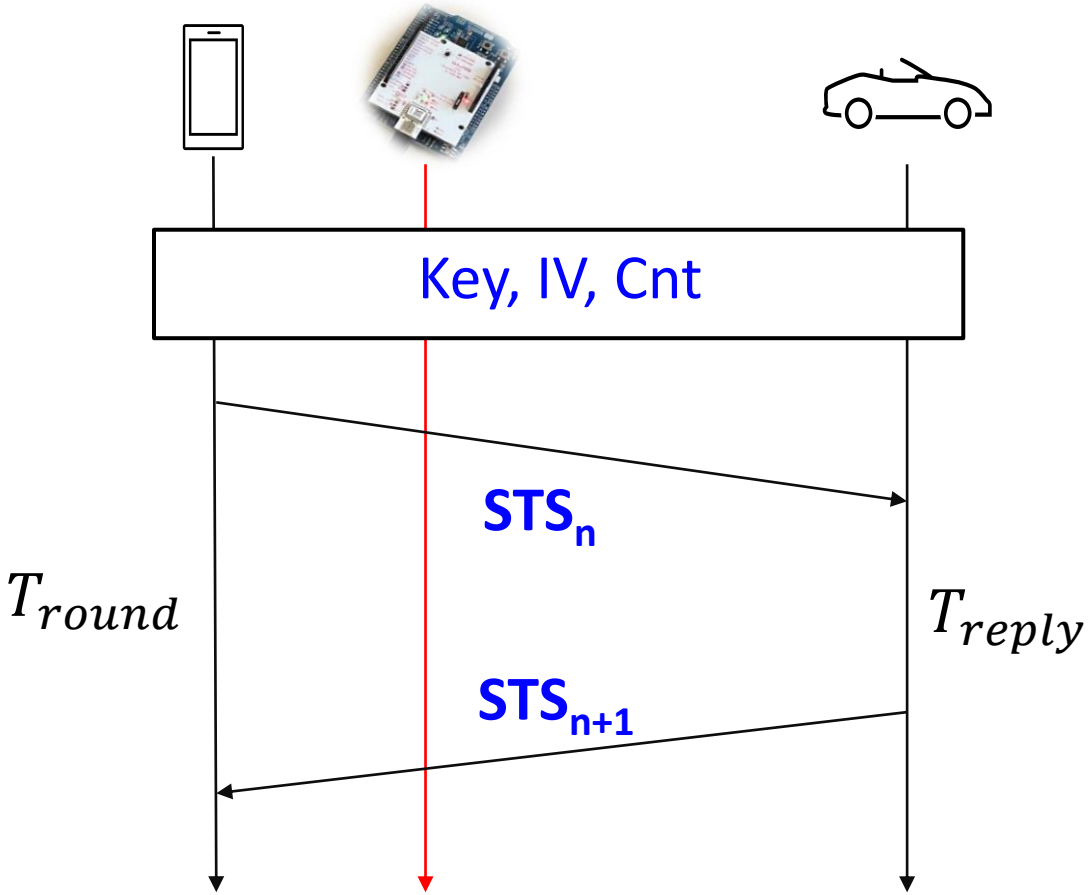


Ghost Peak: reactively inject a fake early path (simplified)



Threat model

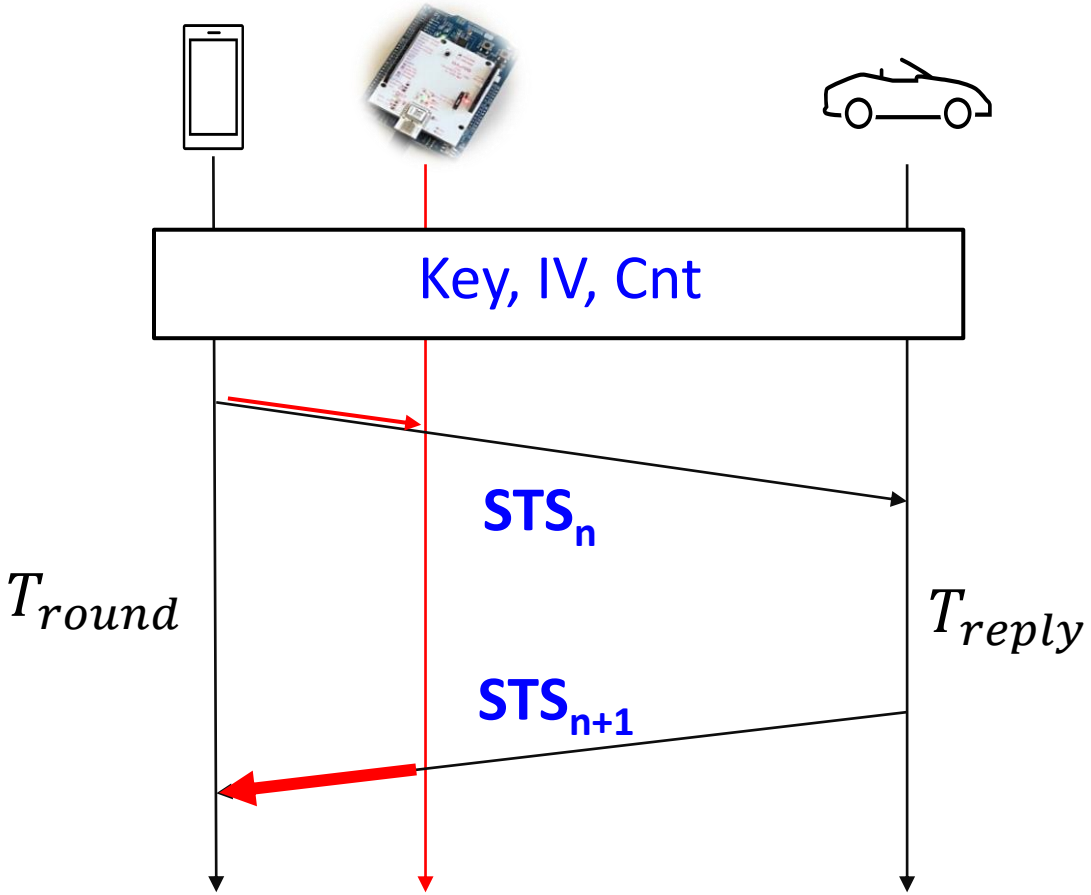
Ghost Peak: reactively inject a fake early path (simplified)



Threat model

- In range of one victim (standard 65USD transceiver)

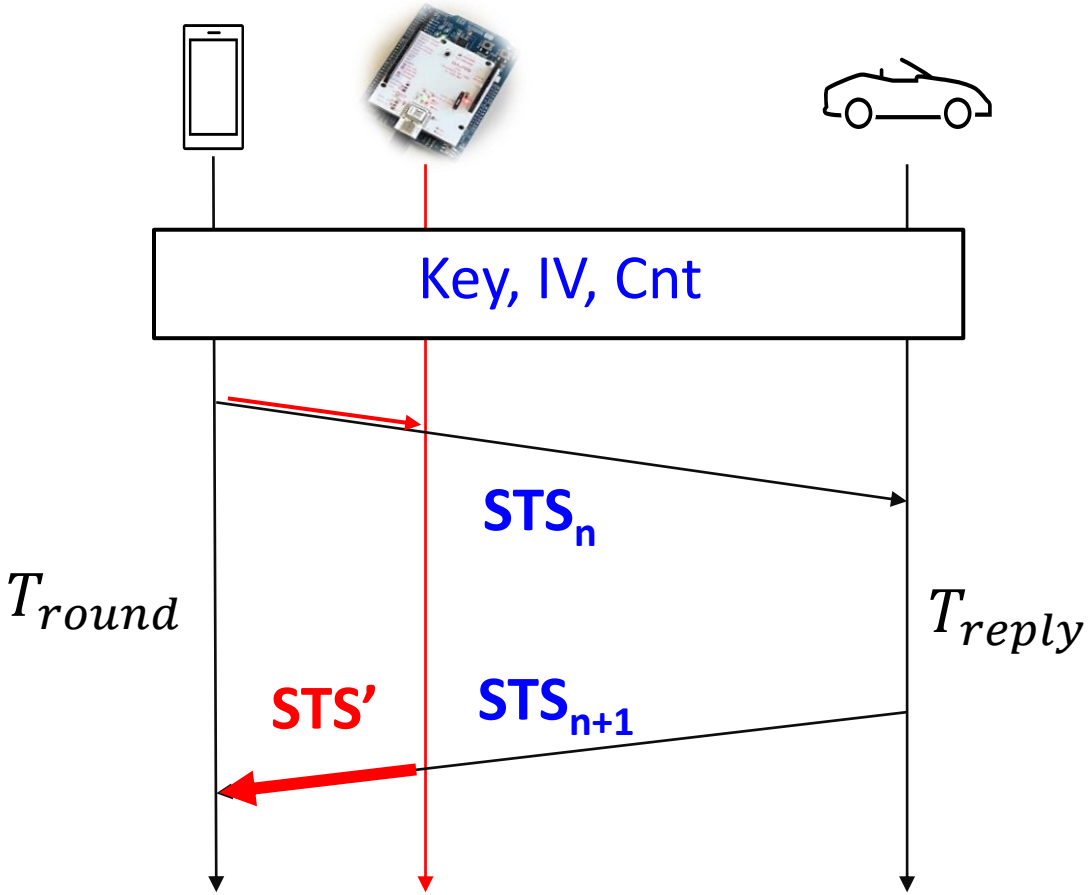
Ghost Peak: reactively inject a fake early path (simplified)



Threat model

- In range of one victim (standard 65USD transceiver)
- Reactive injection (us accuracy)

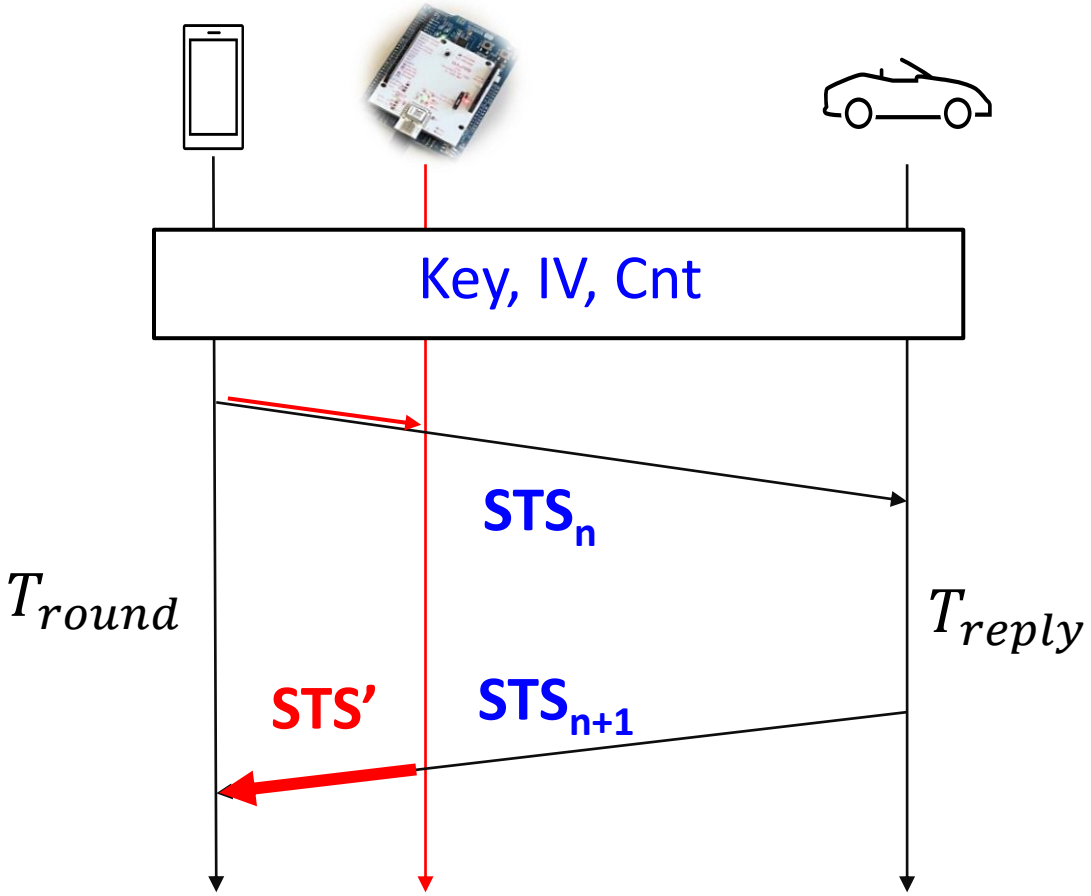
Ghost Peak: reactively inject a fake early path (simplified)



Threat model

- In range of one victim (standard 65USD transceiver)
- Reactive injection (us accuracy)
- No secret known

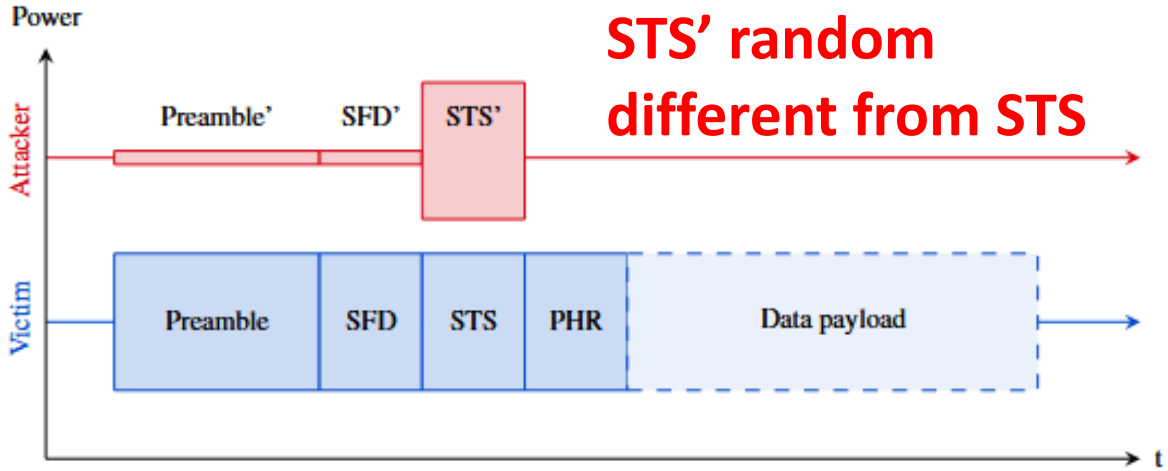
Ghost Peak: reactively inject a fake early path (simplified)



$$d = c\,(T_{round} - T_{reply})/2$$

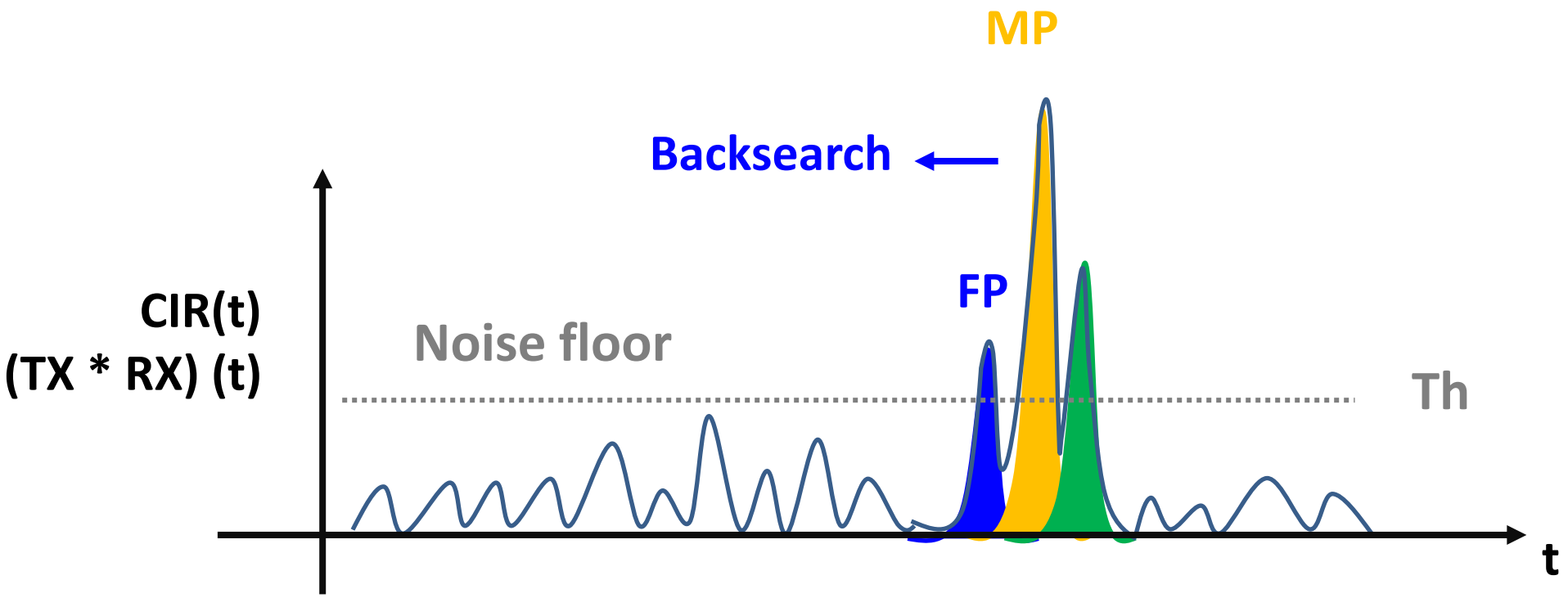
Threat model

- In range of one victim (standard 65USD transceiver)
- Reactive injection (us accuracy)
- No secret known

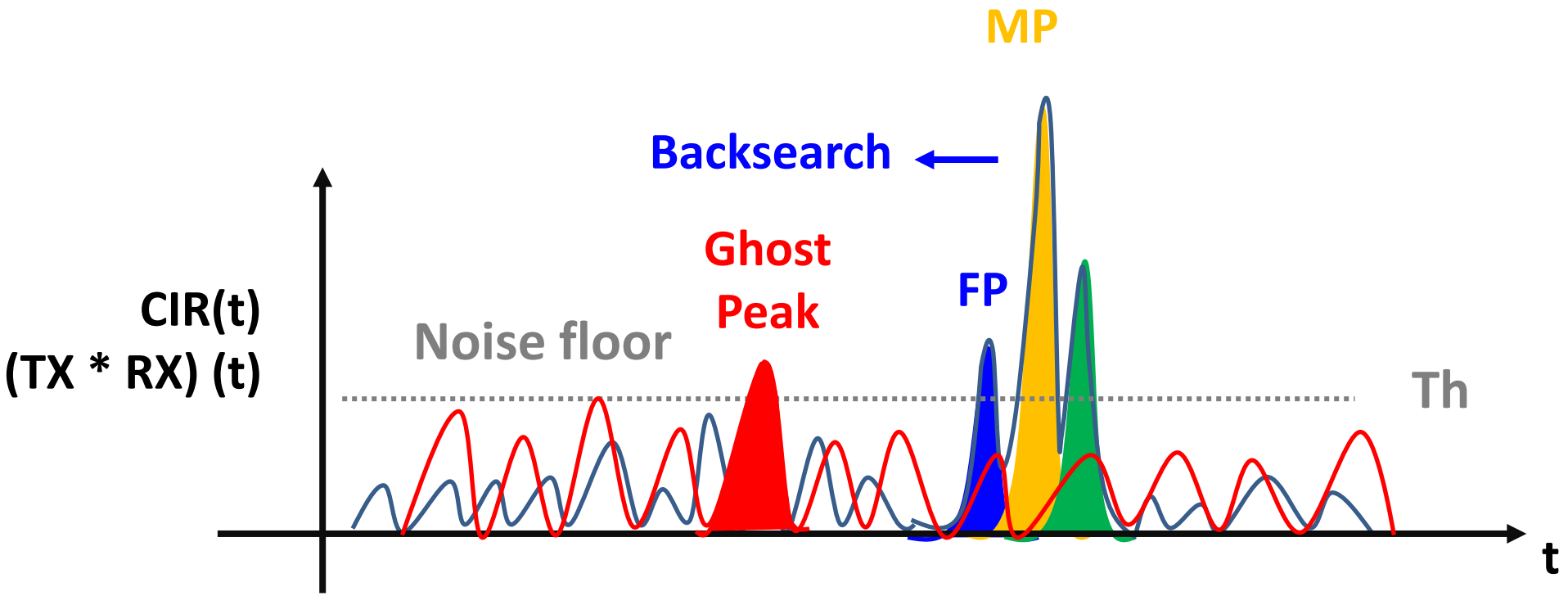


ETH zürich TECHNISCHE UNIVERSITÄT DARMSTADT

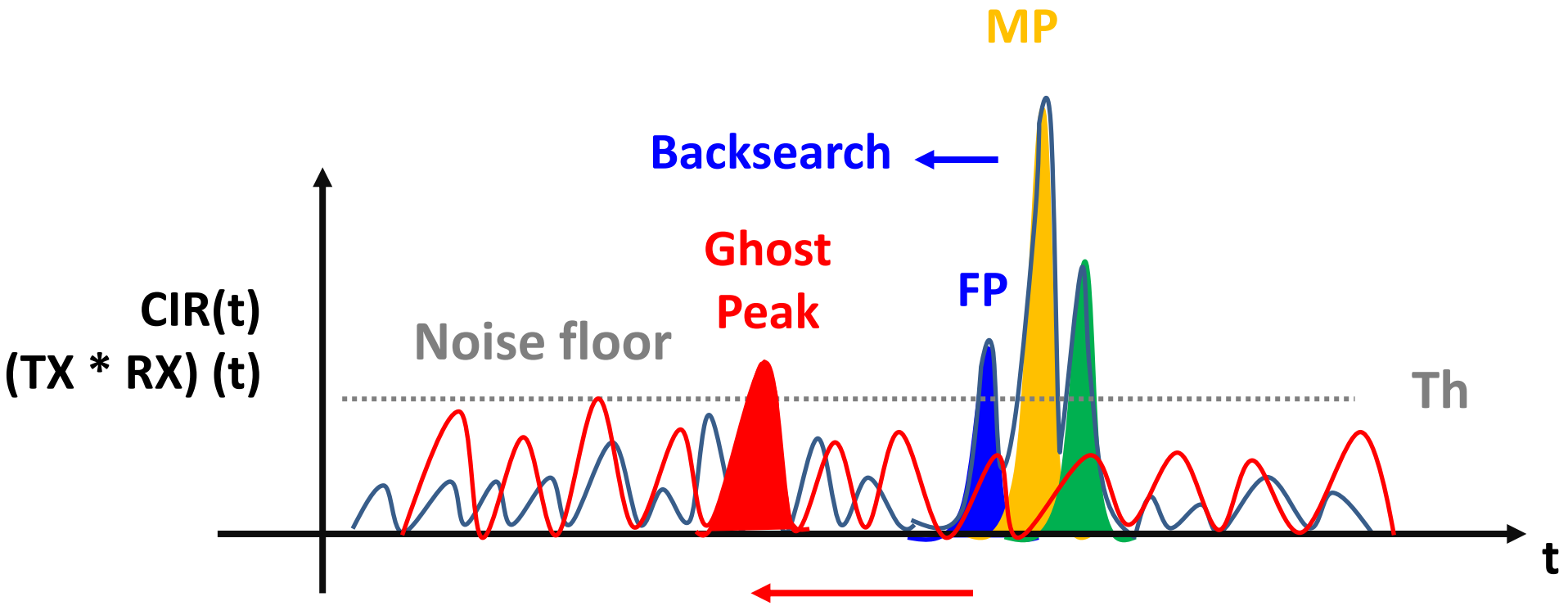
Ghost Peak: inject a fake early path (simplified model)



Ghost Peak: inject a fake early path (simplified model)



Ghost Peak: inject a fake early path (simplified model)



Earlier arrival time => distance reduction

Ghost Peak: summary of main results

Main Victim: Apple U1

Secondary victim: Apple, NXP, Qorvo

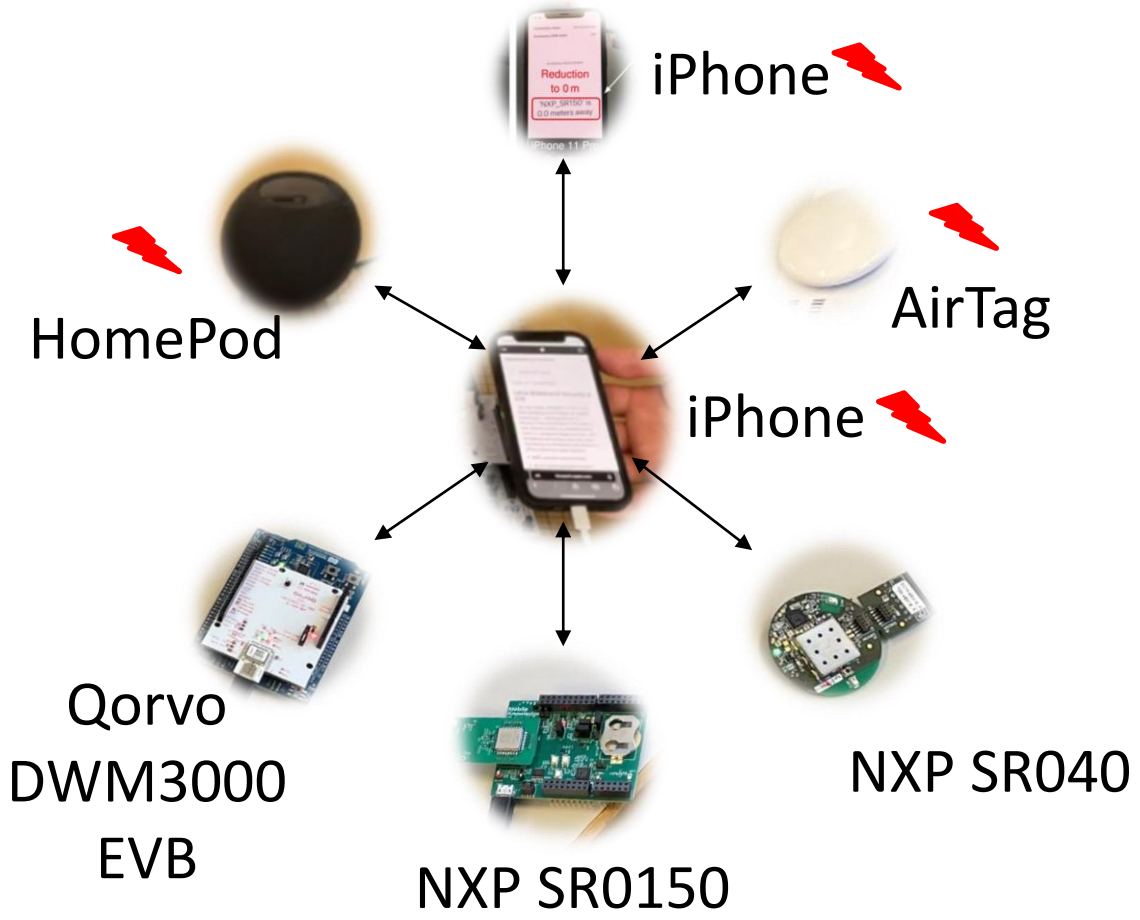
Attacker: Qorvo DWM3000EVB

Environment: real-world corridor

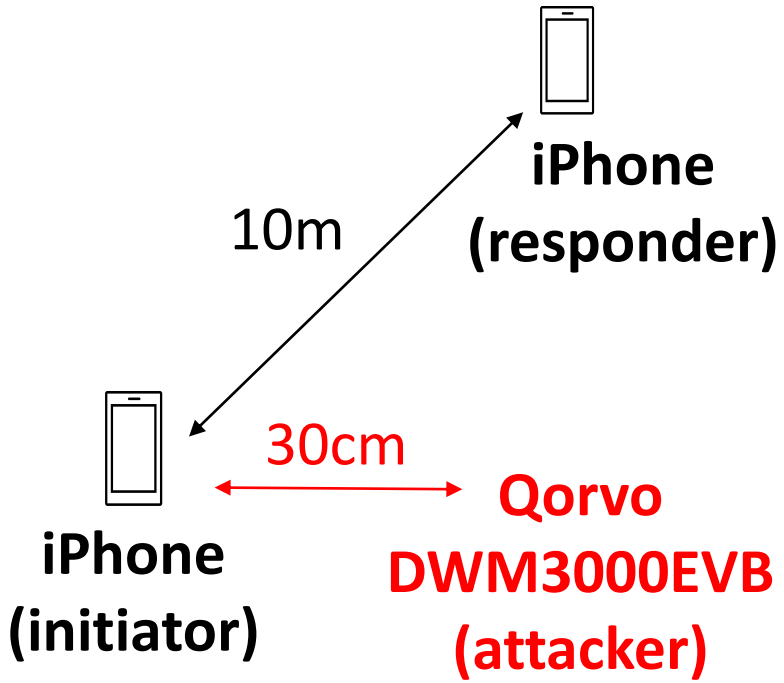
Max reduction: up to 12m reductions

Success rate : up to 4%

Check the paper for details

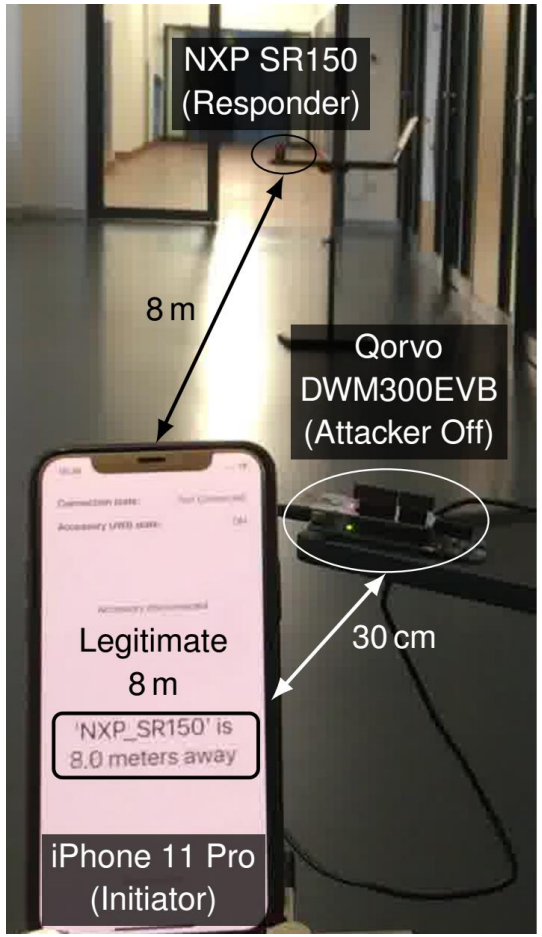


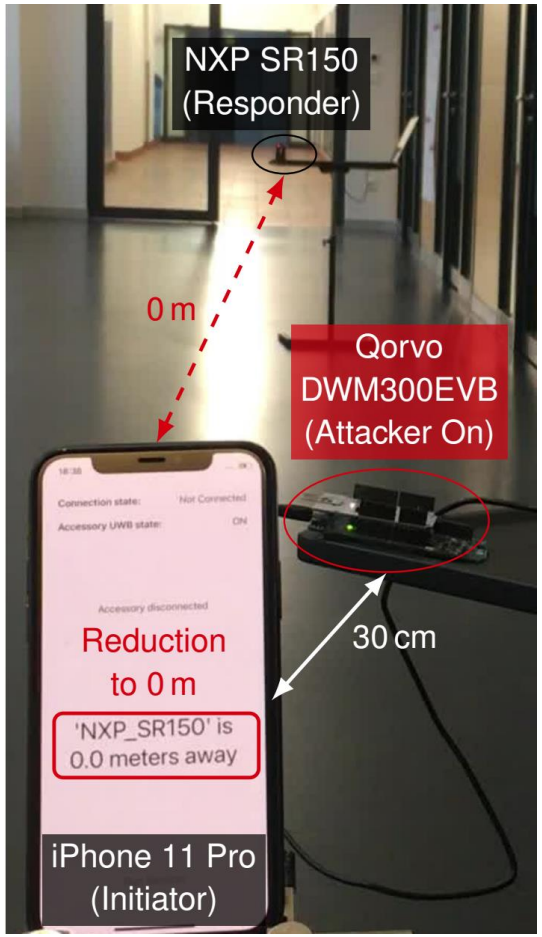
Ghost Peak: example of reduction

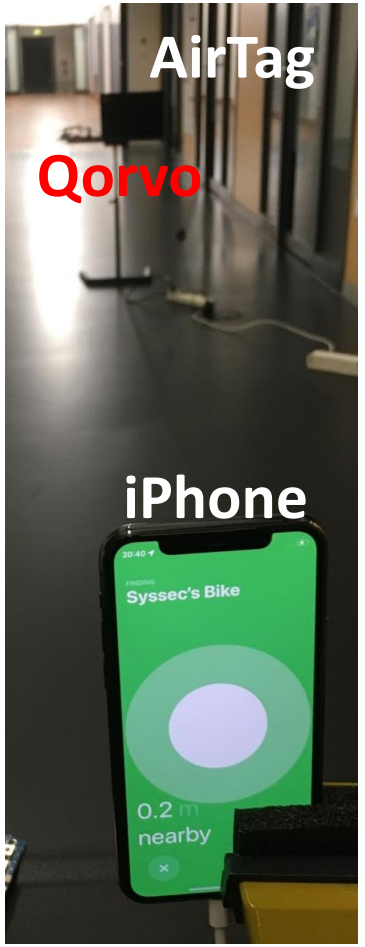


ETH zürich
TECHNISCHE UNIVERSITÄT DARMSTADT

Ghost Peak: examples of reductions







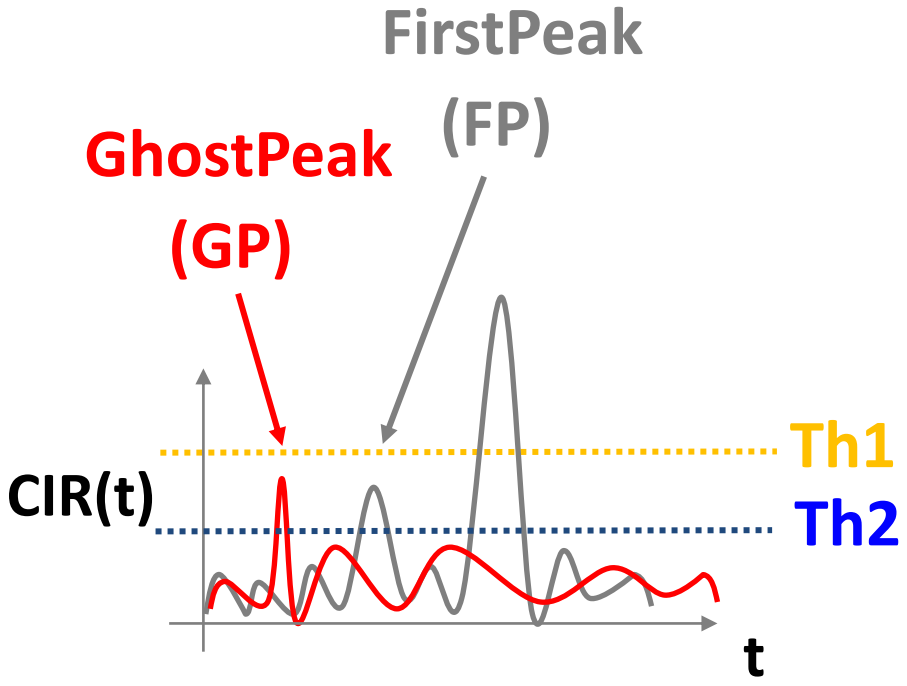
ETH zürich
TECHNISCHE UNIVERSITÄT DARMSTADT

Root problems

1. Challenging problem

GP (random STS) vs. FP (right STS, low power)

Worsened by inter-pulse interference of HRP



*Possible designs and security/performance tradeoffs:
Singh et. Al, "Security analysis of IEEE 802.15.4z/HRP UWB time-of-flight distance measurement", ACM WiSec 2021

Root problems

1. Challenging problem

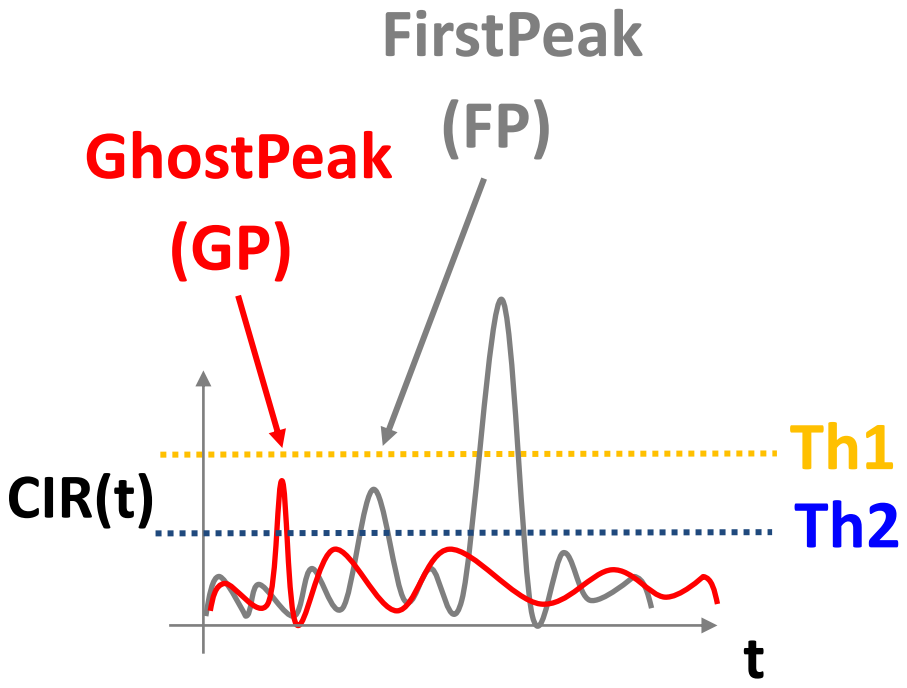
GP (random STS) vs. FP (right STS, low power)

Worsened by inter-pulse interference of HRP

2. Mix search and validation of EP

⇒ Security (Th1) vs. Performance (Th2)

⇒ Obscure implem. not defined in the standard*



*Possible designs and security/performance tradeoffs:
Singh et. Al, "Security analysis of IEEE 802.15.4z/HRP UWB time-of-flight distance measurement", ACM WiSec 2021

Root problems

1. Challenging problem

GP (random STS) vs. FP (right STS, low power)

Worsened by inter-pulse interference of HRP

2. Mix search and validation of EP

⇒ Security (Th1) vs. Performance (Th2)

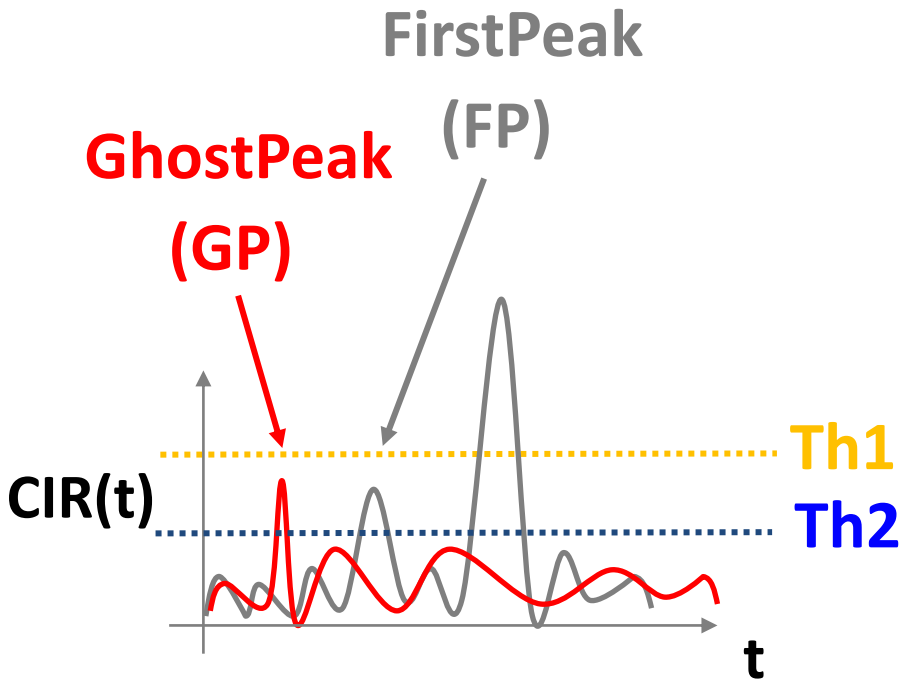
⇒ Obscure implem. not defined in the standard*

3. Lack of provable security

⇒ Correlation peak to STS similarity?

⇒ STS length to security level / success rate? Vice-versa?

⇒ Effect of obscure implem. mitigations?



*Possible designs and security/performance tradeoffs:
Singh et. Al, "Security analysis of IEEE 802.15.4z/HRP UWB time-of-flight distance measurement", ACM WiSec 2021

Mitigations & Future Work

Tuning some "Knobs" here and there + Testing

- Check preamble and STS consistency, Increase the threshold, …
- Test some configurations, …

Root problems not really solved
Attacking is "harder", by how much?

Mitigations & Future Work

Tuning some "Knobs" here and there + Testing

- Check preamble and STS consistency, Increase the threshold, …
- Test some configurations, …

Root problems not really solved
Attacking is "harder", by how much?

New IEEE standard (work in progress)

Tries to solve the problem at its root

- Decouple functionality/performance from security validation
- Provable security level in number of bits, open security design
- Best of HRP (perf.) and LRP (security)

Takeaway

Ghost Peak: Practical Distance Reduction Attacks Against HRP UWB Ranging

P. Leu[1*], G. Camurati[1*], A. Heinrich[2], M. Roeschlin[1], C. Anliker[1], M. Hollick[2], S. Capkun[1], J. Classen[2]

[1] ETH zürich [2] SEEMOO SECURE MOBILE NETWORKING TECHNISCHE UNIVERSITÄT DARMSTADT *Equal contribution

https://securepositioning.com/ghost-peak/
https://github.com/seemoo-la/uwb-sniffer

Takeaway

Ghost Peak: Practical Distance Reduction Attacks Against HRP UWB Ranging

P. Leu[1*], G. Camurati[1*], A. Heinrich[2], M. Roeschlin[1], C. Anliker[1], M. Hollick[2], S. Capkun[1], J. Classen[2]

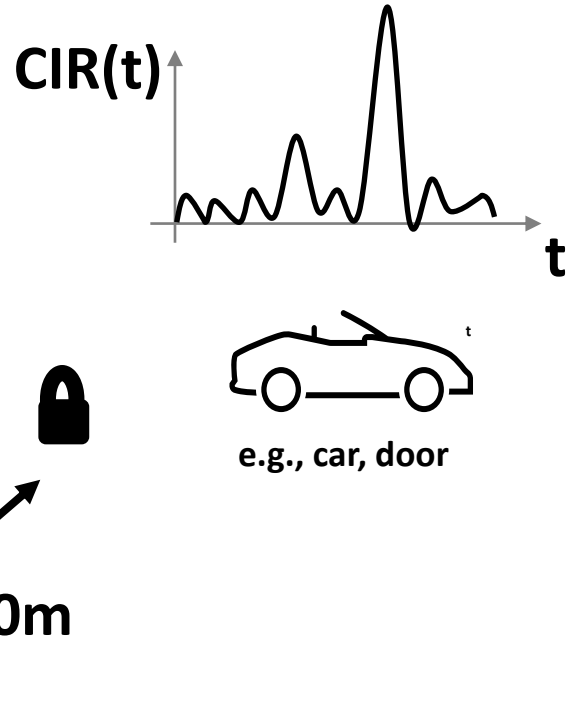
[1] ETH zürich [2] SEEMOO SECURE MOBILE NETWORKING TECHNISCHE UNIVERSITÄT DARMSTADT *Equal contribution

ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

https://securepositioning.com/ghost-peak/

https://github.com/seemoo-la/uwb-sniffer



Takeaway

Ghost Peak: Practical Distance Reduction Attacks Against HRP UWB Ranging

P. Leu[1*], G. Camurati[1*], A. Heinrich[2], M. Roeschlin[1], C. Anliker[1], M. Hollick[2], S. Capkun[1], J. Classen[2]

[1] ETH zürich [2] SEEMOO SECURE MOBILE NETWORKING TECHNISCHE UNIVERSITÄT DARMSTADT *Equal contribution

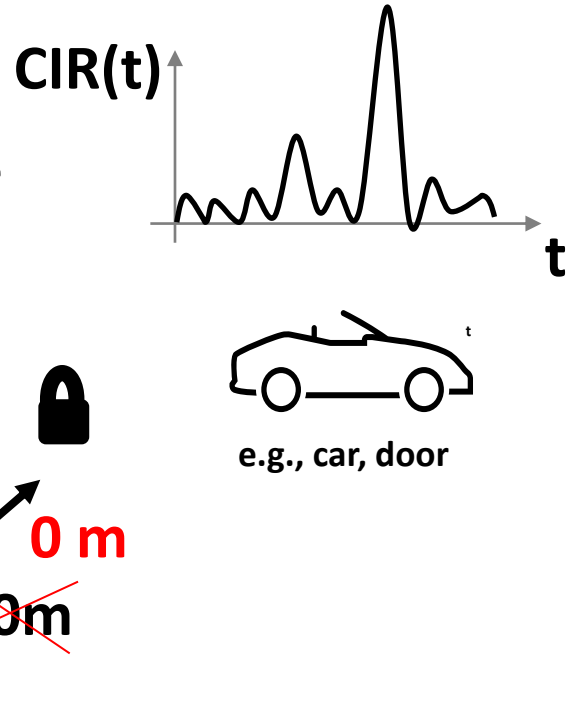
ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

https://securepositioning.com/ghost-peak/

https://github.com/seemoo-la/uwb-sniffer

First practical attack: trick two HRP UWB devices to think they are close



Takeaway

Ghost Peak: Practical Distance Reduction Attacks Against HRP UWB Ranging

P. Leu[1*], G. Camurati[1*], A. Heinrich[2], M. Roeschlin[1], C. Anliker[1], M. Hollick[2], S. Capkun[1], J. Classen[2]

[1] ETH zürich [2] SEEMOO SECURE MOBILE NETWORKING TECHNISCHE UNIVERSITÄT DARMSTADT *Equal contribution

ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

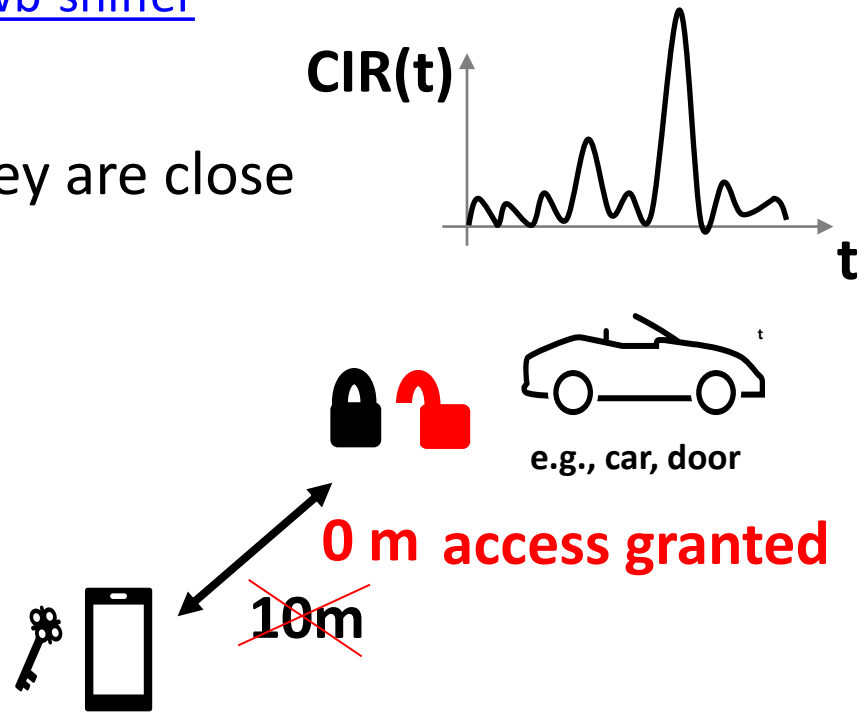
ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

https://securepositioning.com/ghost-peak/

https://github.com/seemoo-la/uwb-sniffer

First practical attack: trick two HRP UWB devices to think they are close

Impact: access control, payments, asset tracking, …



Takeaway

Ghost Peak: Practical Distance Reduction Attacks Against HRP UWB Ranging

P. Leu[1*], G. Camurati[1*], A. Heinrich[2], M. Roeschlin[1], C. Anliker[1], M. Hollick[2], S. Capkun[1], J. Classen[2]

[1] ETH zürich [2] SEEMOO SECURE MOBILE NETWORKING TECHNISCHE UNIVERSITÄT DARMSTADT *Equal contribution

ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

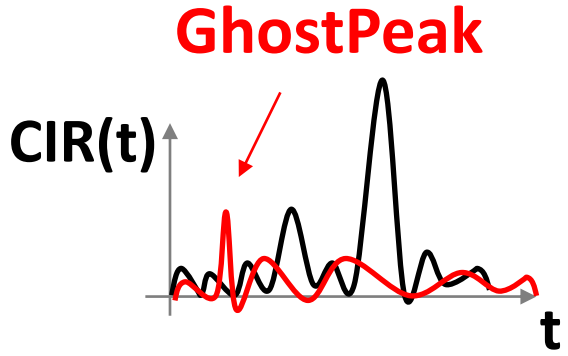
https://securepositioning.com/ghost-peak/

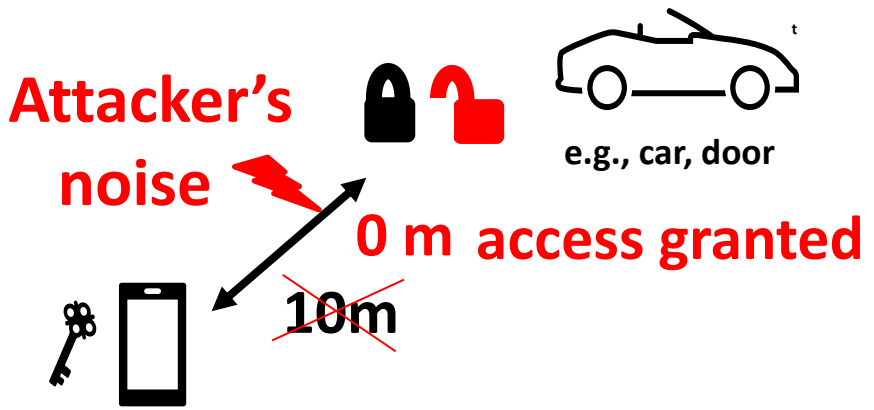
https://github.com/seemoo-la/uwb-sniffer

First practical attack: trick two HRP UWB devices to think they are close

Impact: access control, payments, asset tracking, …

How: injected noise causes fake early path (65USD device)





Takeaway

Ghost Peak: Practical Distance Reduction Attacks Against HRP UWB Ranging

P. Leu[1*], G. Camurati[1*], A. Heinrich[2], M. Roeschlin[1], C. Anliker[1], M. Hollick[2], S. Capkun[1], J. Classen[2]

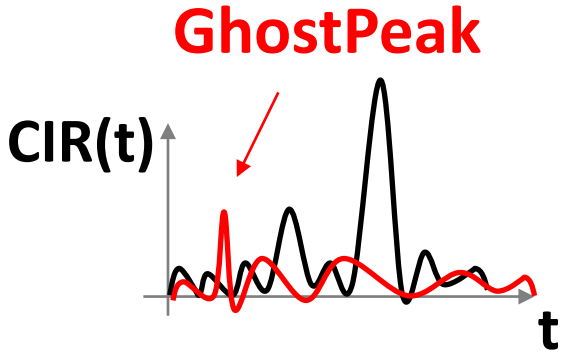
[1] ETH zürich [2] SEEMOO SECURE MOBILE NETWORKING TECHNISCHE UNIVERSITÄT DARMSTADT *Equal contribution

ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

https://securepositioning.com/ghost-peak/

https://github.com/seemoo-la/uwb-sniffer

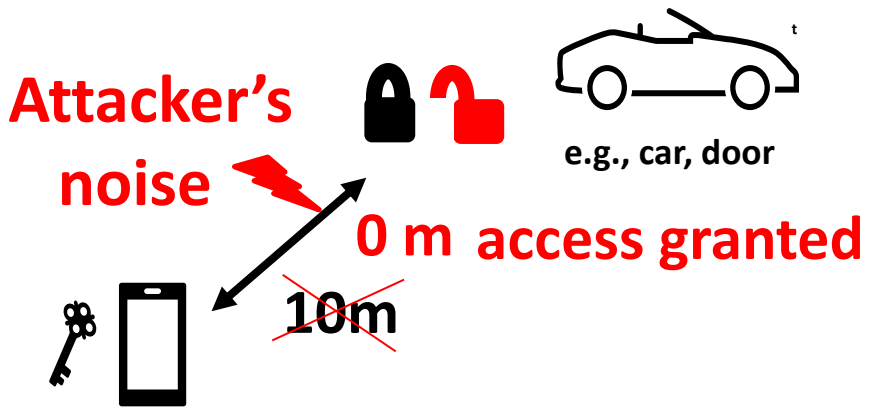


First practical attack: trick two HRP UWB devices to think they are close

Impact: access control, payments, asset tracking, …

How: injected noise causes fake early path (65USD device)

Threat model: in range, no knowledge of any secret



Takeaway

Ghost Peak: Practical Distance Reduction Attacks Against HRP UWB Ranging

P. Leu[1*], G. Camurati[1*], A. Heinrich[2], M. Roeschlin[1], C. Anliker[1], M. Hollick[2], S. Capkun[1], J. Classen[2]

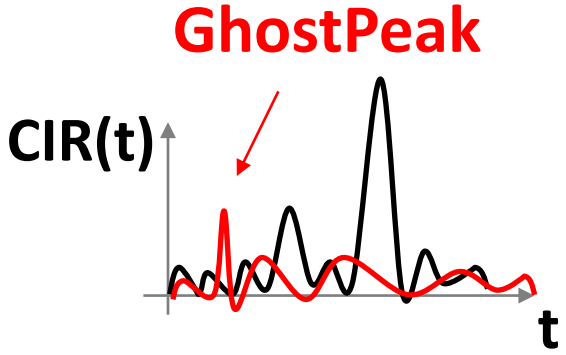
[1] ETH zürich [2] SEEMOO SECURE MOBILE NETWORKING TECHNISCHE UNIVERSITÄT DARMSTADT *Equal contribution

ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

https://securepositioning.com/ghost-peak/

https://github.com/seemoo-la/uwb-sniffer



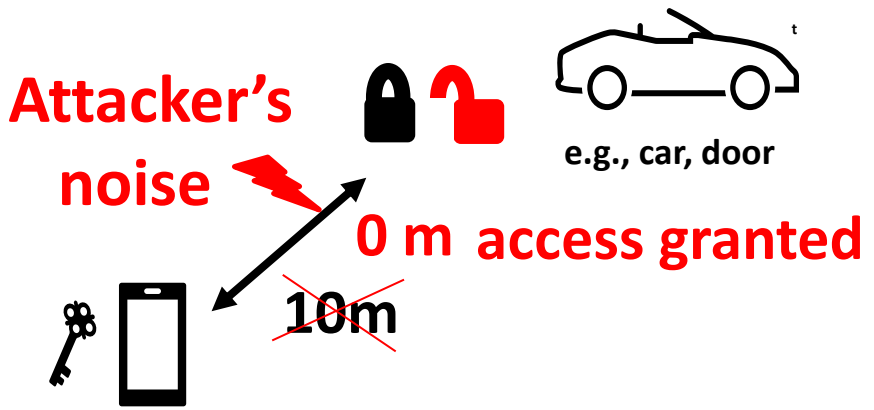
First practical attack: trick two HRP UWB devices to think they are close

Impact: access control, payments, asset tracking, …

How: injected noise causes fake early path (65USD device)

Threat model: in range, no knowledge of any secret

Root: no formal security level, obscure implementation



Takeaway

Ghost Peak: Practical Distance Reduction Attacks Against HRP UWB Ranging

P. Leu[1*], G. Camurati[1*], A. Heinrich[2], M. Roeschlin[1], C. Anliker[1], M. Hollick[2], S. Capkun[1], J. Classen[2]

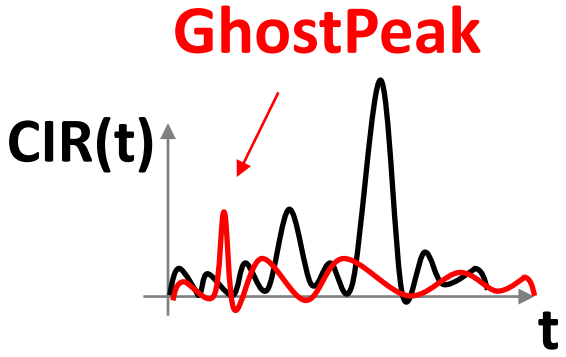
[1] ETH zürich [2] SEEMOO SECURE MOBILE NETWORKING TECHNISCHE UNIVERSITÄT DARMSTADT *Equal contribution

ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

https://securepositioning.com/ghost-peak/

https://github.com/seemoo-la/uwb-sniffer



First practical attack: trick two HRP UWB devices to think they are close

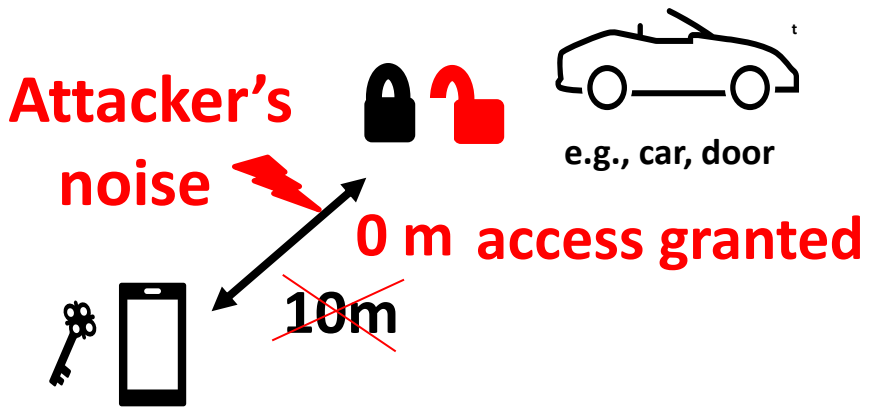
Impact: access control, payments, asset tracking, …

How: injected noise causes fake early path (65USD device)

Threat model: in range, no knowledge of any secret

Root: no formal security level, obscure implementation

Vulnerable: Apple U1, …?



Takeaway

Ghost Peak: Practical Distance Reduction Attacks Against HRP UWB Ranging

P. Leu[1*], G. Camurati[1*], A. Heinrich[2], M. Roeschlin[1], C. Anliker[1], M. Hollick[2], S. Capkun[1], J. Classen[2]

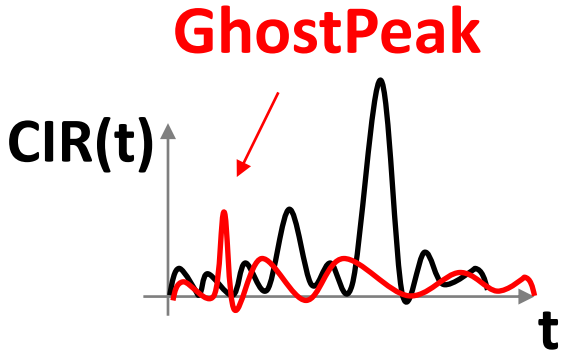
[1] ETH zürich [2] SEEMOO SECURE MOBILE NETWORKING TECHNISCHE UNIVERSITÄT DARMSTADT *Equal contribution

ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

https://securepositioning.com/ghost-peak/

https://github.com/seemoo-la/uwb-sniffer



First practical attack: trick two HRP UWB devices to think they are close

Impact: access control, payments, asset tracking, …

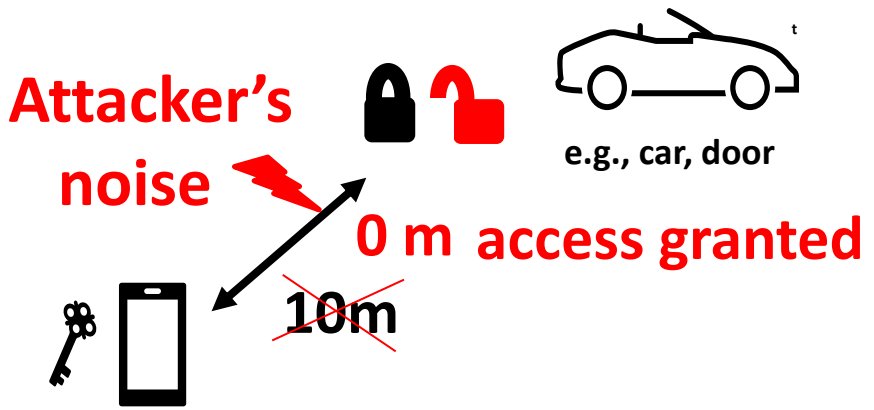
How: injected noise causes fake early path (65USD device)

Threat model: in range, no knowledge of any secret

Root: no formal security level, obscure implementation

Vulnerable: Apple U1, …?

One enough: Apple U1 + NXP/Qorvo



Takeaway

Ghost Peak: Practical Distance Reduction Attacks Against HRP UWB Ranging

P. Leu[1*], G. Camurati[1*], A. Heinrich[2], M. Roeschlin[1], C. Anliker[1], M. Hollick[2], S. Capkun[1], J. Classen[2]

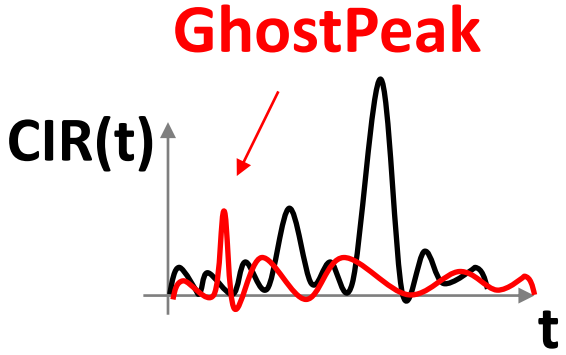
[1] ETH zürich [2] SEEMOO SECURE MOBILE NETWORKING TECHNISCHE UNIVERSITÄT DARMSTADT *Equal contribution

ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

https://securepositioning.com/ghost-peak/

https://github.com/seemoo-la/uwb-sniffer



First practical attack: trick two HRP UWB devices to think they are close

Impact: access control, payments, asset tracking, …

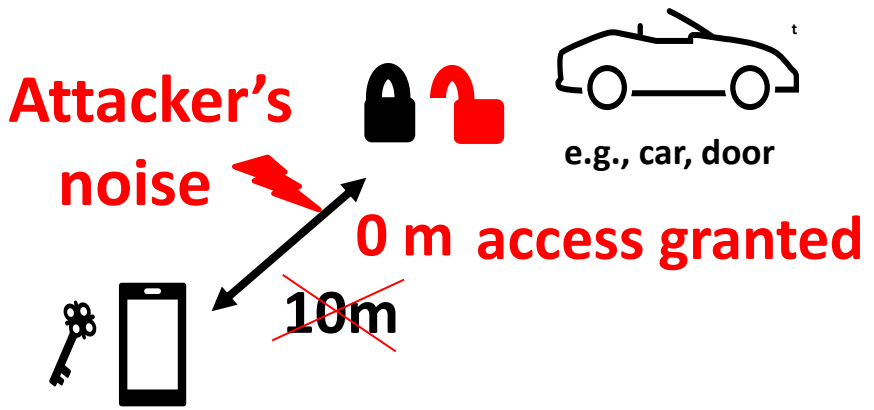
How: injected noise causes fake early path (65USD device)

Threat model: in range, no knowledge of any secret

Root: no formal security level, obscure implementation

Vulnerable: Apple U1, …?

One enough: Apple U1 + NXP/Qorvo



Thank you! Questions?

Backup Slides

Ghost Peak: main results

Primary Victim	Secondary Victim	Roles	Initiation	Max. Reduction	Success Rate
HomePod mini (Apple U1)	iPhone (Apple U1)	Init./Resp.	Proximity*	9.01 m	2.10 %
iPhone (Apple U1)	iPhone (Apple U1)	Init./Resp.	Developer choice**	12.45 m	4.08 %
AirTag (Apple U1)	iPhone (Apple U1)	Init./Resp.	User interaction	9.09 m	4.25 %
iPhone (Apple U1)	Tag (NXP SR040)	Resp./Init.	Developer choice**	4.80 m	1.87 %
iPhone (Apple U1)	Tag (NXP SR150)	Init./Resp.	Developer choice**	9.68 m	2.15 %
iPhone (Apple U1)	Tag (Qorvo DWM3000)	Init./Resp.	Developer choice**	8.13 m	3.09 %

Acknowledgements

This research has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program under grant agreement No 726227. This research has received funding from the Swiss National Science Foundation under NCCR Automation, grant agreement 51NF40_180545. This project has been partially funded by Fondation Botnar. This work has been co-funded by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.