UWB-ED: Distance Enlargement Attack Detection in Ultra-Wideband

Mridula Singh, Patrick Leu, AbdelRahman Abdou, Srdjan Capkun
Dept. of Computer Science
ETH Zurich
USENIX, 2019

2021/10/26
Presenter: 20213310 Minkyoo Song

Ultra-Wideband (UWB)

Ultra-Wideband (UWB)

- Very wide spectrum ,500MHz (in case of WiFi, 20~80MHz)

$\Rightarrow$ Very quick

- Operate with relatively low frequency

$\Rightarrow$ Robust to obstacles

- Use ToF (Time of Flight) to measure the distance

=> Accurate, Fast, Secure

Challenge – External attacker can manipulate measured distance

Attack Scenario

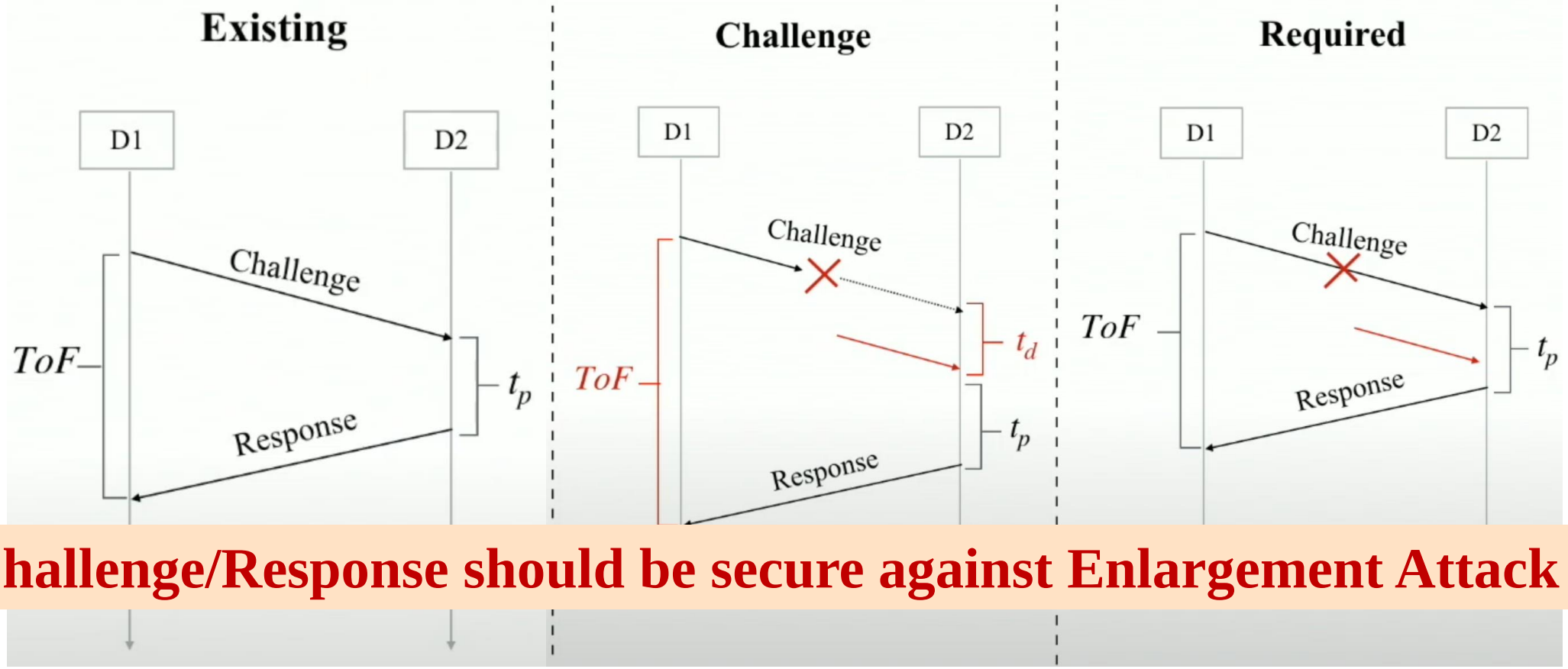
Distance Reduction Attack

Distance Enlargement Attack

Attack Scenario

- Until now, community worked on preventing Distance Reduction Attacks
- However, not enough works about Distance Enlargement Attacks
- **Paper's contribution** UWB-ED: The first scheme that prevents Distance Enlargement Attacks

ToF Distance Measurement



Challenge/Response should be secure against Enlargement Attack

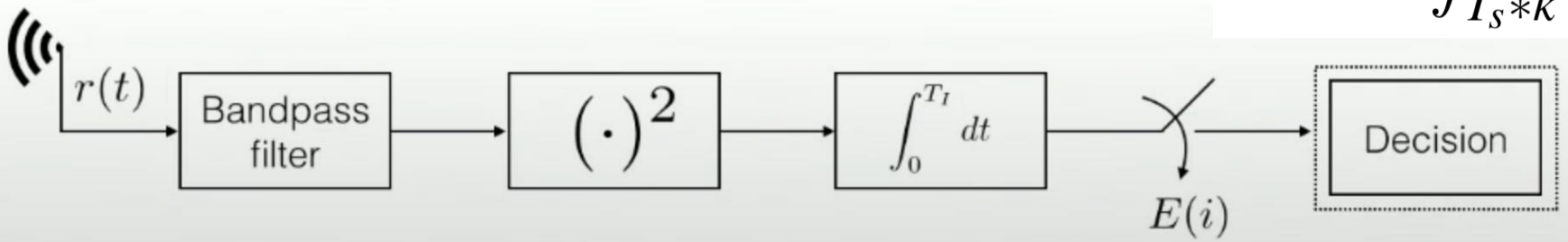
Physical Layer of UWB

OOK Modulation

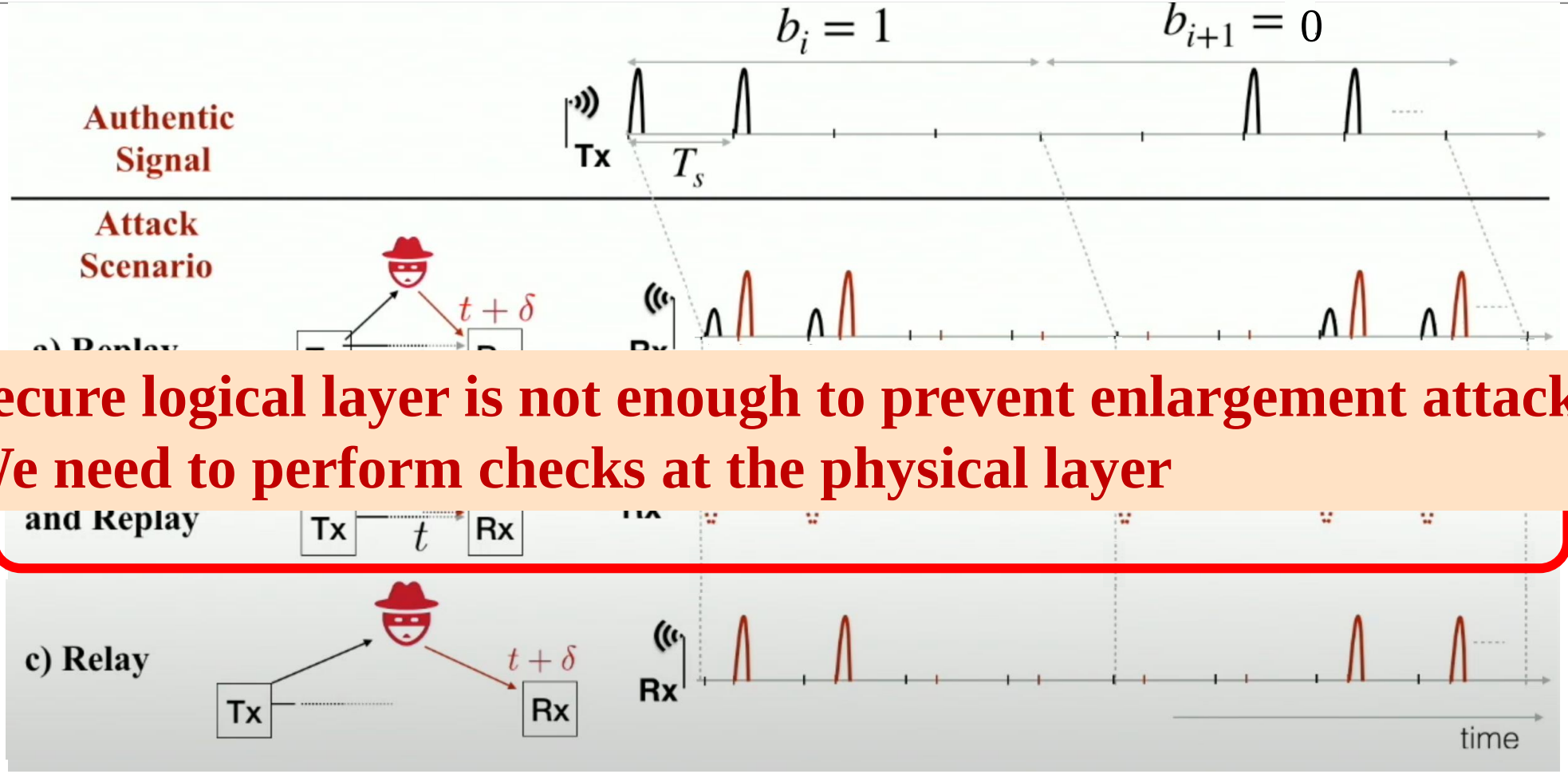
$$b = [0,1,1,...]$$

Energy Detector Receiver (non-coherent)

$$E(k) = \int_{T_s*k}^{T_s*k+T_I} [r(t)]^2 dt$$



Distance Enlargement Attacks

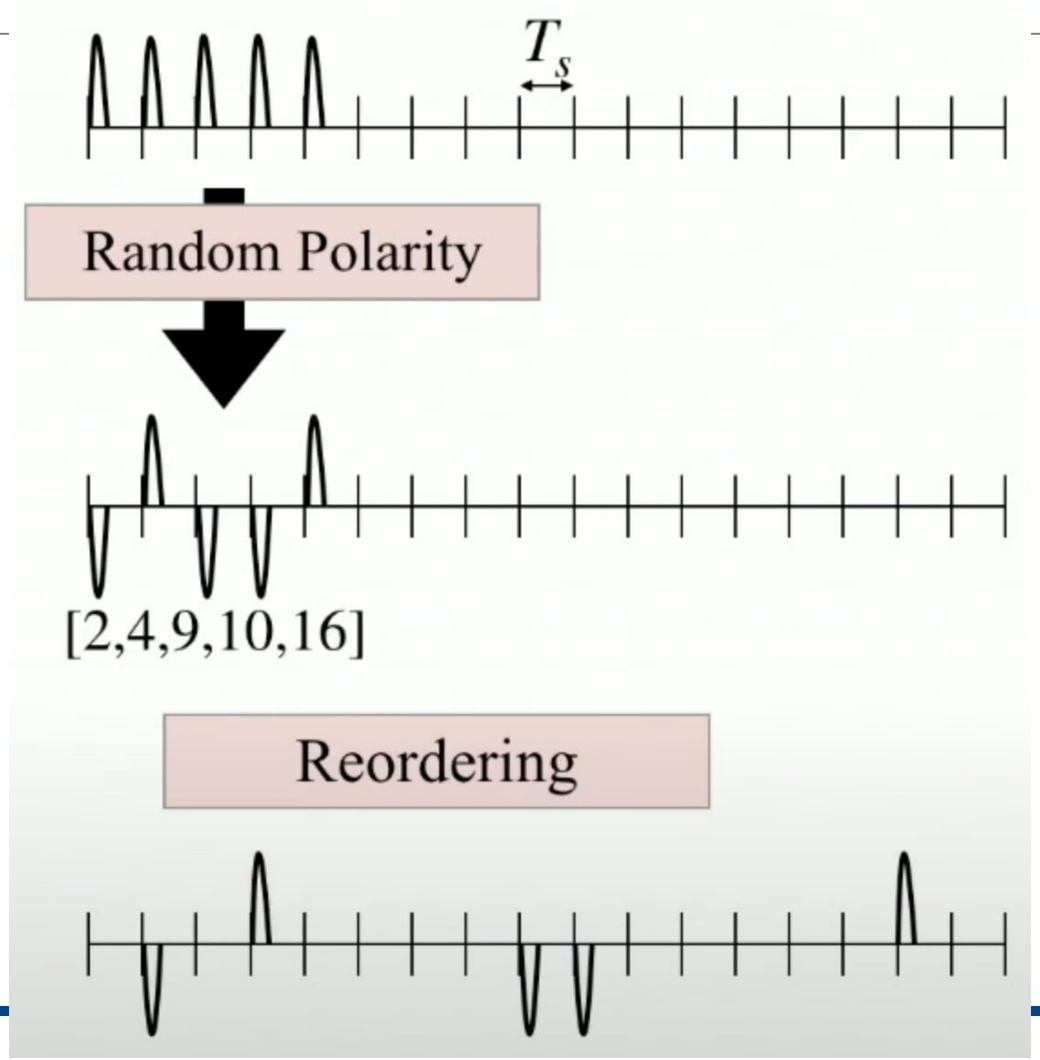


Secure logical layer is not enough to prevent enlargement attacks
We need to perform checks at the physical layer

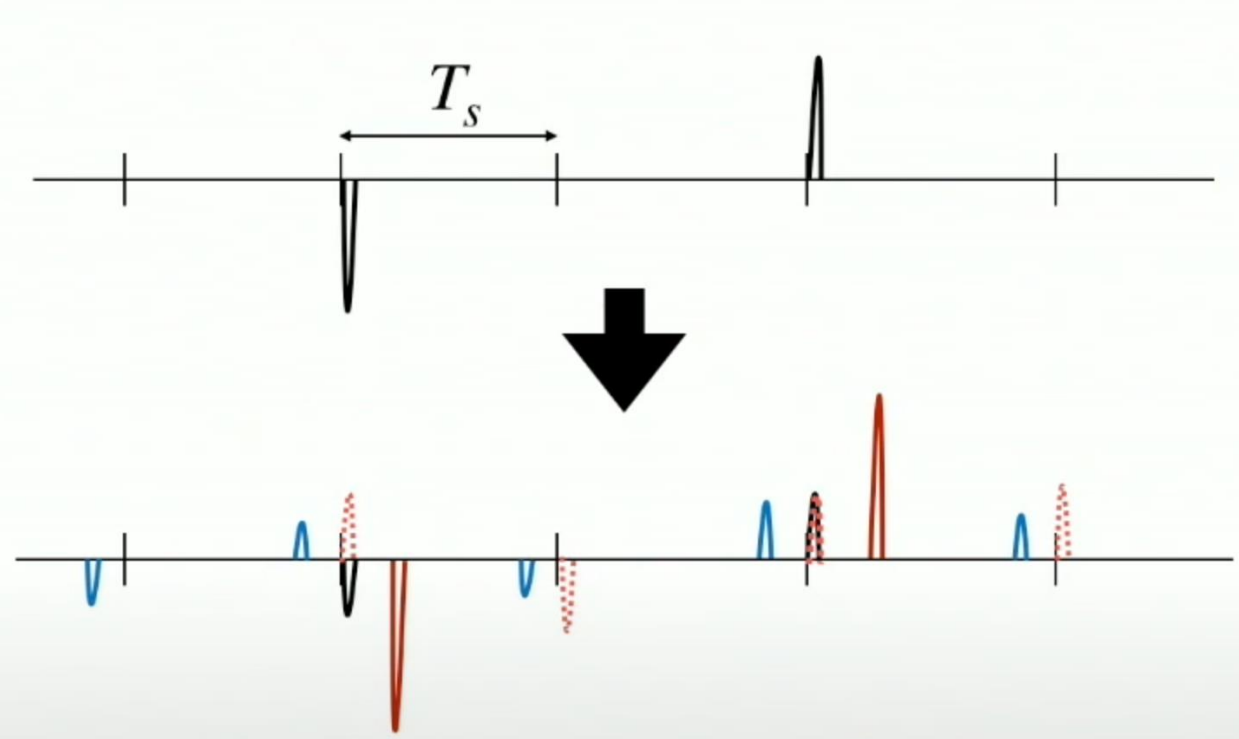
Verification Code Structure

- α pulses
- B positions does not have pulses
- Similar to OOK Modulation

- $T_s > ToF_{max}$: Adversary's replayed signal falls between two authentic pulse positions.



Code Sent and Received



Degraded Signal

Signal degrades due to channel effects

Noise

Transceiver noise cannot be eliminated

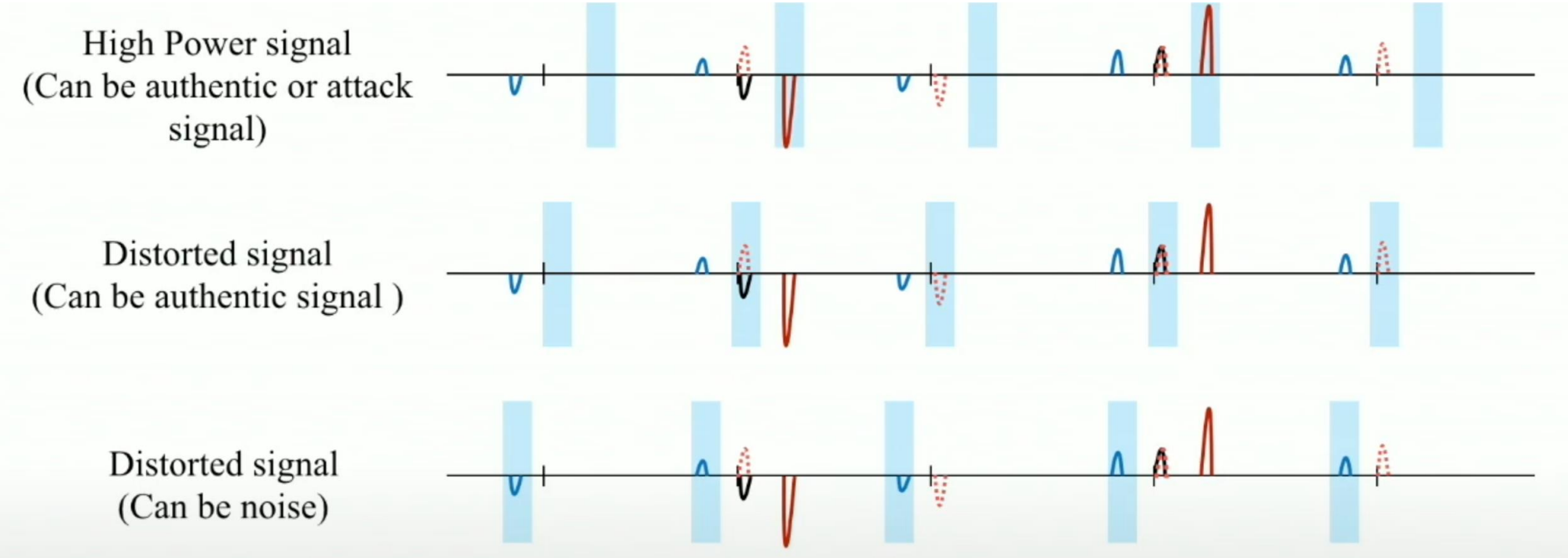
Adversary's distortion Signal

Adversary send cancellation signal to prevent authentic code detection

Adversary Replyed Signal

Adversary send replayed signal for the incorrect ToA estimation

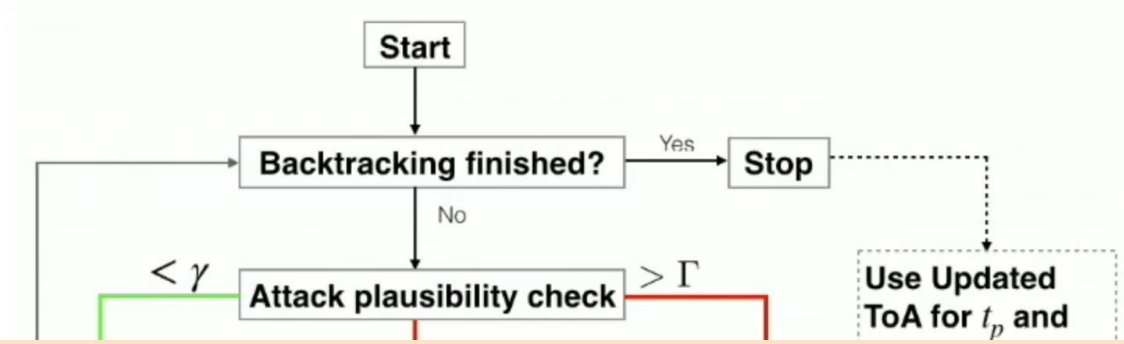
Back-search for Code Detection



Authentic signal should not be discarded as Noise

noise should not be detected as authentic signal

Verification Code Detection



Attack Plausibility check

Accumulated power of the received signal

$$\gamma < P_{total} < \Gamma$$

- γ — Threshold to distinguish signal and noise

- **Energy of the received signal should be less than threshold Γ**

$$\mathbf{P_{total} < \Gamma}$$

- **Received signal should not be similar to expected code**

$$\boldsymbol{P(Bin_{\alpha}^{r} > Bin_{\beta}^{r}) < Pnoise}$$

These tests check for the similarity of the received signal with the code and not the exact match

selected from present (α) and absent (β) positions

$$\mathbb{P}(Bin_{\alpha}^{r} > Bin_{\beta}^{r}) \geq \mathbb{P}_{noise}$$

- Multiple tests are needed as some tests can fail due to channel conditions

Security Properties of the Code Structure

Random Polarity If adversary guesses the pulse polarity incorrectly, it will increase energy at the pulse presence position

Random Position If adversary guesses position of the pulse incorrectly, it will add pulse at pulse absent position

Signal (After degradation)	0	-1	0	-1	0	0	1	0	0	0	-1	1	A_l
(Distortion signal) Adversary Signal	-1	0	0	1	0	1	1	-1	0	0	-1	0	A_a
Receiver Gets	-1	-1	0	0	0	1	2	-1	0	0	-2	1	$A = A_l + A_a$
Energy Received	1	1	0	0	0	1	4	1	0	0	4	1	$\sim A^2$

Authentic Signal

Bin_α	1	1	1	1	1		
Bin_β	0	0	0	0	0	0	0

Signal after Attack

Bin_α	1	0	4	4	1		
Bin_β	1	0	0	1	1	0	0

Evaluation

Probabilistic Model

Simulations

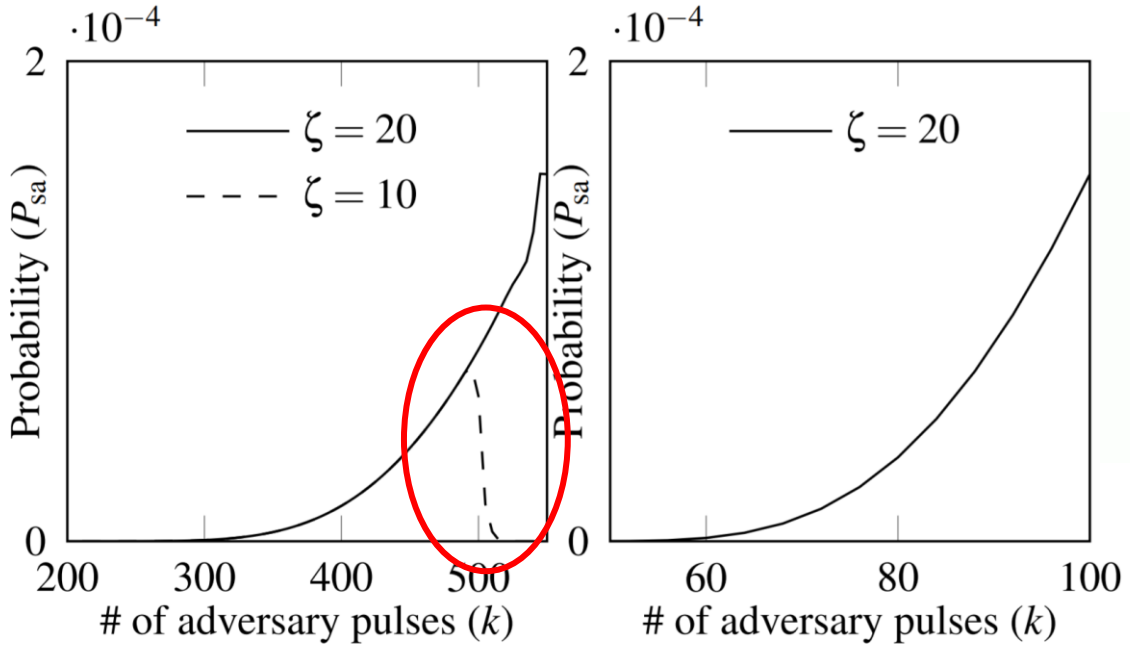
Probability of Attack Success (P_{sa})

Probability of attack success (P_{sa}) depends on following factors

- Code Structure – α,β
- Number of pulses aggregated - r
- Number of pulses transmitted by adversary – k
- Channel Condition - E

$$P_{total} < \Gamma$$

$$\mathbb{P}(Bin_{\alpha}^{r} > Bin_{\beta}^{r}) < \mathbb{P}_{noise}$$

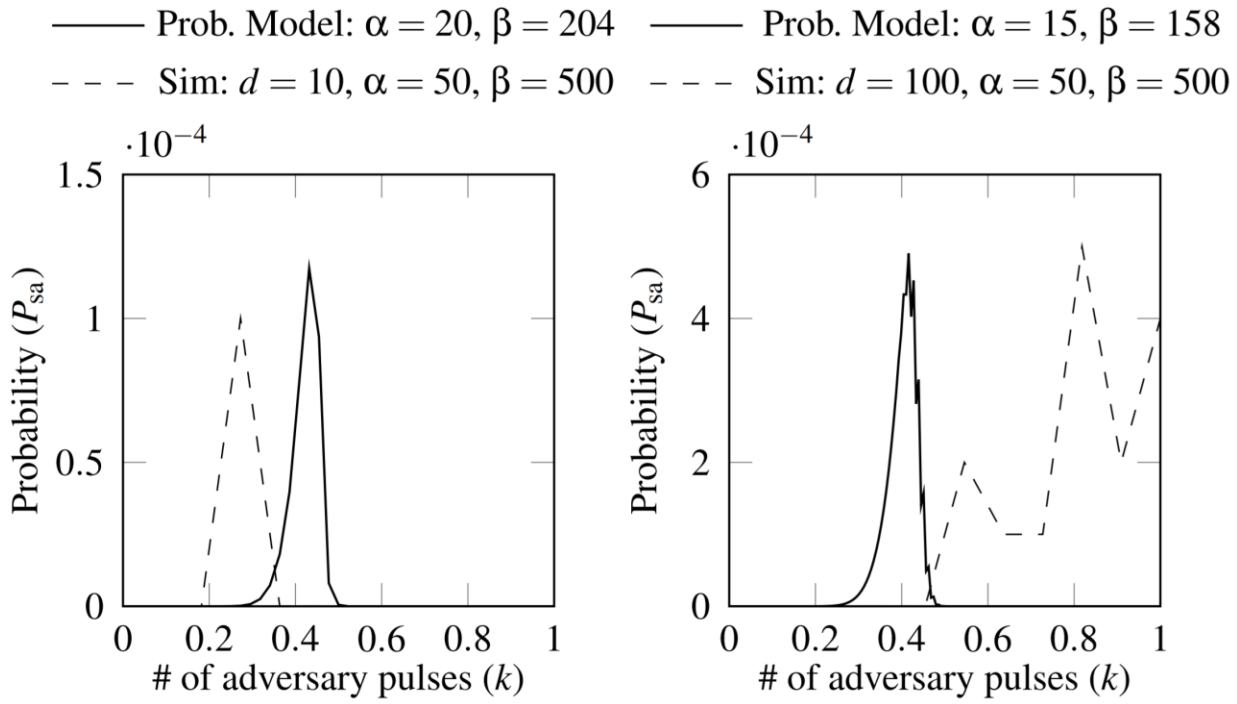


(a) $\beta = 500$; $r = \alpha = 50$. (b) $\beta = 50$; $r = \alpha = 50$.

Simulations

Probabilistic model is validated by using simulations

- Use IEEE 802.14.4a channel model to simulate channel conditions such as noise, multi-path effect, and path loss
- Bandwidth of each pulse is 500MHz, transmit power is -35dBm/MHz, T_s=1μs, and back-search is restricted to 660ns
- The figure show the result for two different operating distances d=10 and d=100
- The results are for r=α and P_{noise}=0.8
- The probability of noise mistaken as code is 10^{-6}



Conclusion

- Preventing Distance Enlargement attacks is important in a number of applications
- UWB-ED is the first scheme that prevents distance enlargement attacks
- UWB-ED prevents both logical and physical layer attacks

Related Works

- Taponecco, Lorenzo, et al. "On the feasibility of overshadow enlargement attack on IEEE 802.15. 4a distance bounding." *IEEE Communications Letters* 18.2 (2013): 257-260.

⇒ Show that the success of enlargement attacks using replay depends on the amount of delay the adversary introduces

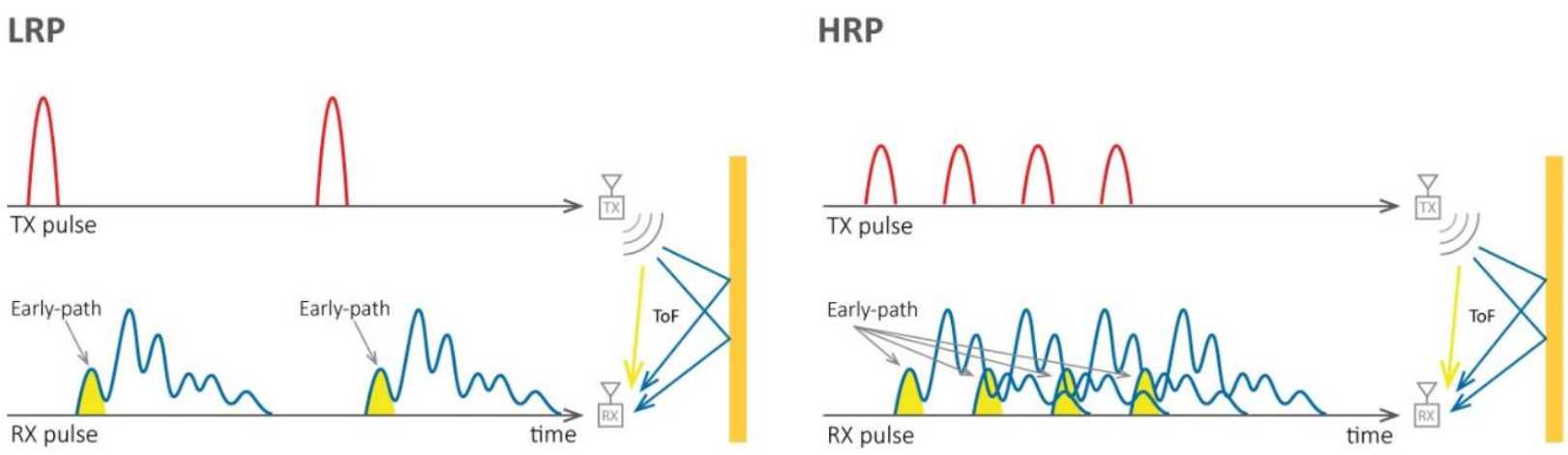
- Compagno, Alberto, et al. "Modeling enlargement attacks against UWB distance bounding protocols." IEEE Transactions on Information Forensics and Security 11.7 (2016): 1565-1577.

⇒ Provide a probabilistic model for the success of overshadowing attacks, which captures different channel conditions and leading edge detection techniques for ToA estimation

- Tippenhauer, Nils Ole, Kasper Bonne Rasmussen, and Srdjan Capkun. "Physical-layer integrity for wireless messages." Computer Networks 109 (2016): 31-38.

⇒ Explore a theoretical approach to detect adversarial signal annihilation for distance enlargement: using a single pulse-per-symbol

Follow-up Studies



- Singh, Mridula, et al. "Security analysis of IEEE 802.15. 4z/HRP UWB time-of-flight distance measurement." Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks. 2021.

⇒ Show HRP-based UWB technologies used in Samsung and Apple are all vulnerable **via simulation**

- On going work (**Srdjan**)

⇒ Prove the practical vulnerabilities of HRP **via real-world experiments**

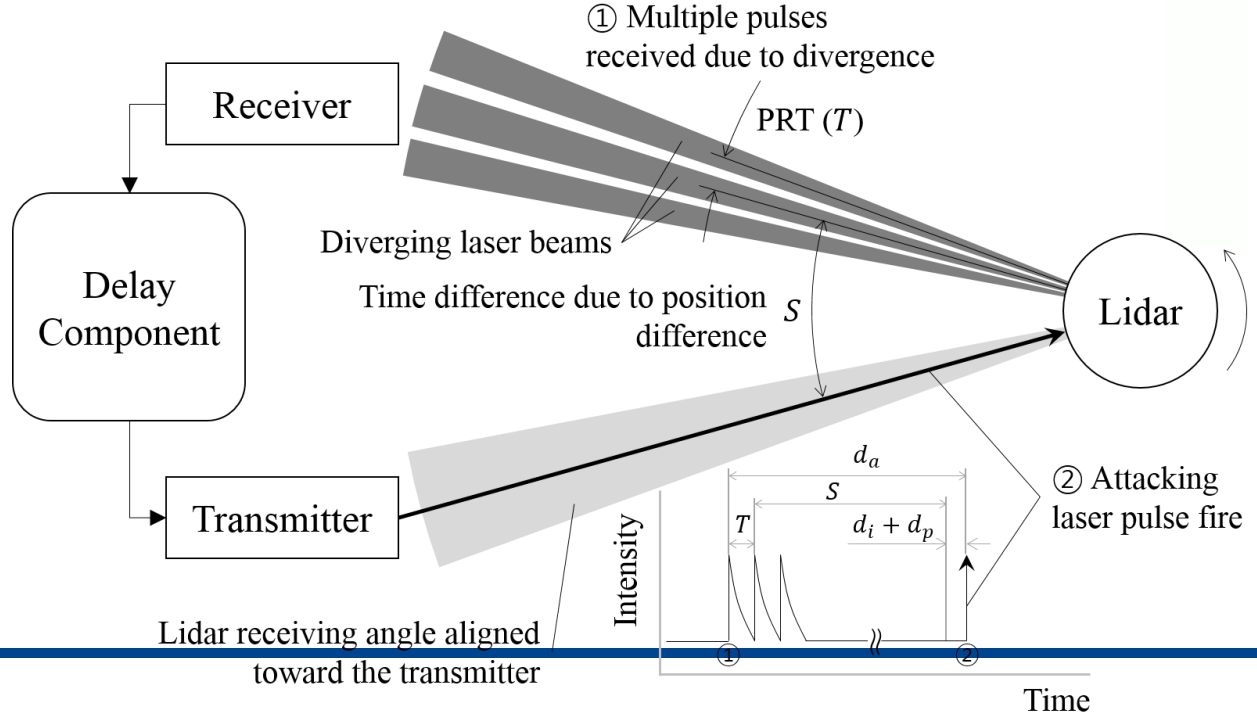
QnA

- **YongHwa Lee**, Is there any other impressive research dealing with attacks similar to distance enlargement or sensor spoofing targeting other important sensors like optical, ultrasonic, infrared, and LiDAR?

⇒ Shin, Hocheol, et al. "**Illusion and dazzle**: Adversarial optical channel exploits against lidars for automotive applications." Springer, 2017.

⇒ Capture Lidar's signal with receiver and transmit delayed signal

⇒ Could induce multiple moving fake dots



QnA

QnA

- **Kyeong Tae Kim**, In the result, why does not the channel condition, such as path loss, noise, and interference due to multipath components, affect the performance and security of the system?

⇒ Actually they considered channel condition in parameterization

$$f(d) = PL_0 + 10 \cdot n \cdot log\left(\frac{d}{d_0}\right)$$

Formula used for calculating Γ in **attack plausibility check**

constant representing the **path loss** at the reference distance d0

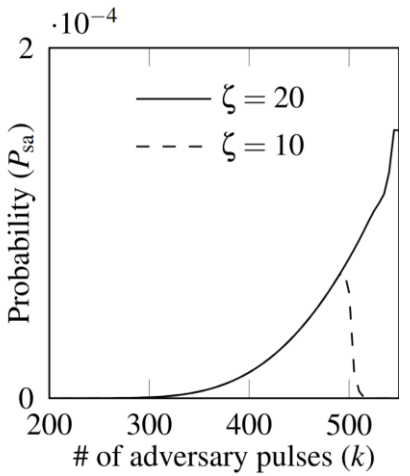
$$\gamma = (\alpha + \beta) \cdot \sigma_N^2$$

Receiver's **noise variance**

Power loss

$$R = f(D_1 + D_2) - (f(D_1) + E)$$

$$\zeta = 10^{R/10}$$



Thank you for listening!