Project: IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)

Submission Title: Clock Attack to SS-TWR in the Case of UWB MMS

Date Submitted: November 2024

Source: Xiliang Luo, Vinod Kristem, Moche Cohen (Apple)

Address: One Apple Park Way, Cupertino, CA 95104, USA

E-Mails: xiliang_luo@apple.com

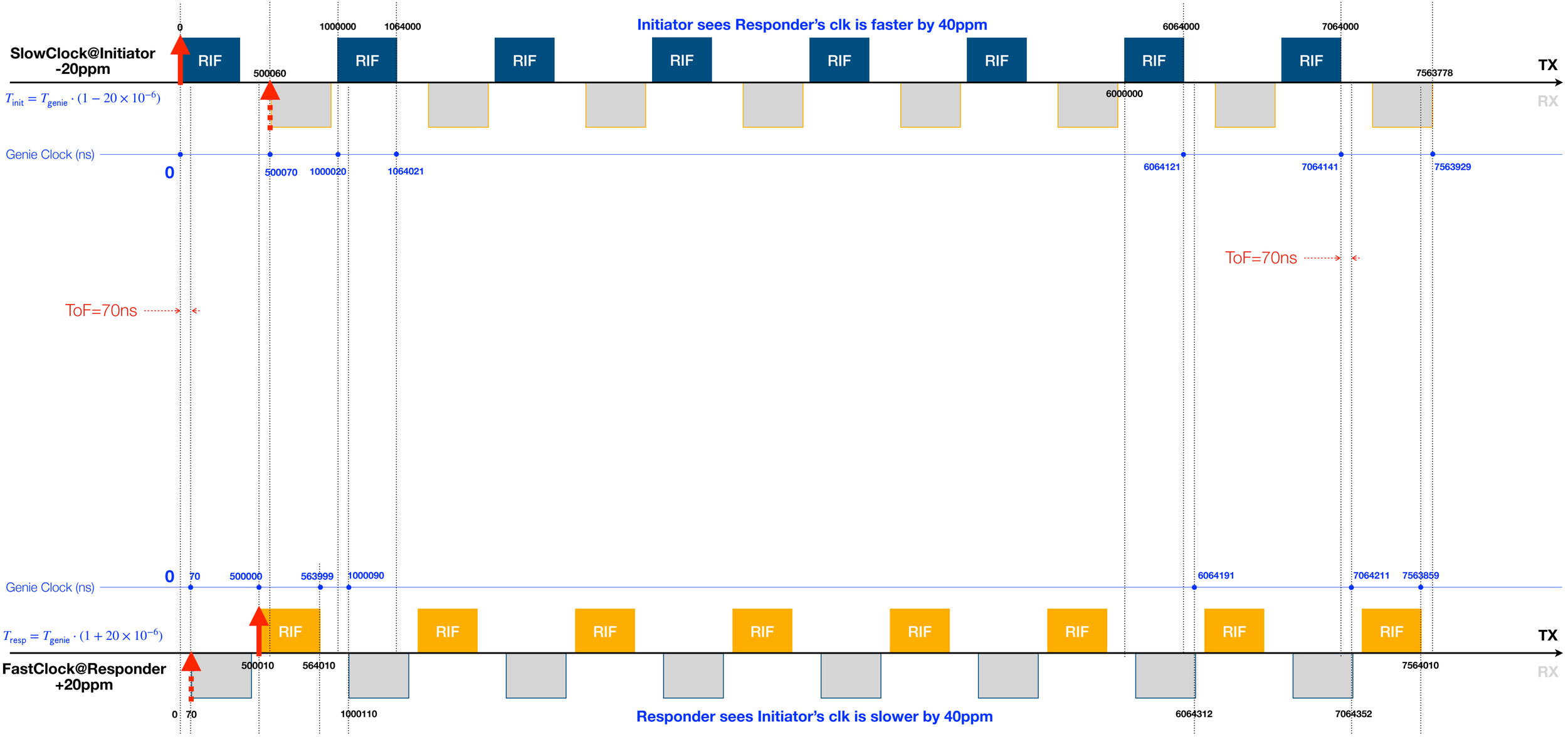
Abstract: Show an example of clock attack to SS-TWR in the case of UWB MMS with RIFs.

Purpose: Motivate more discussions and studies on ranging integrity with mixed MMS.

No-Attack Case

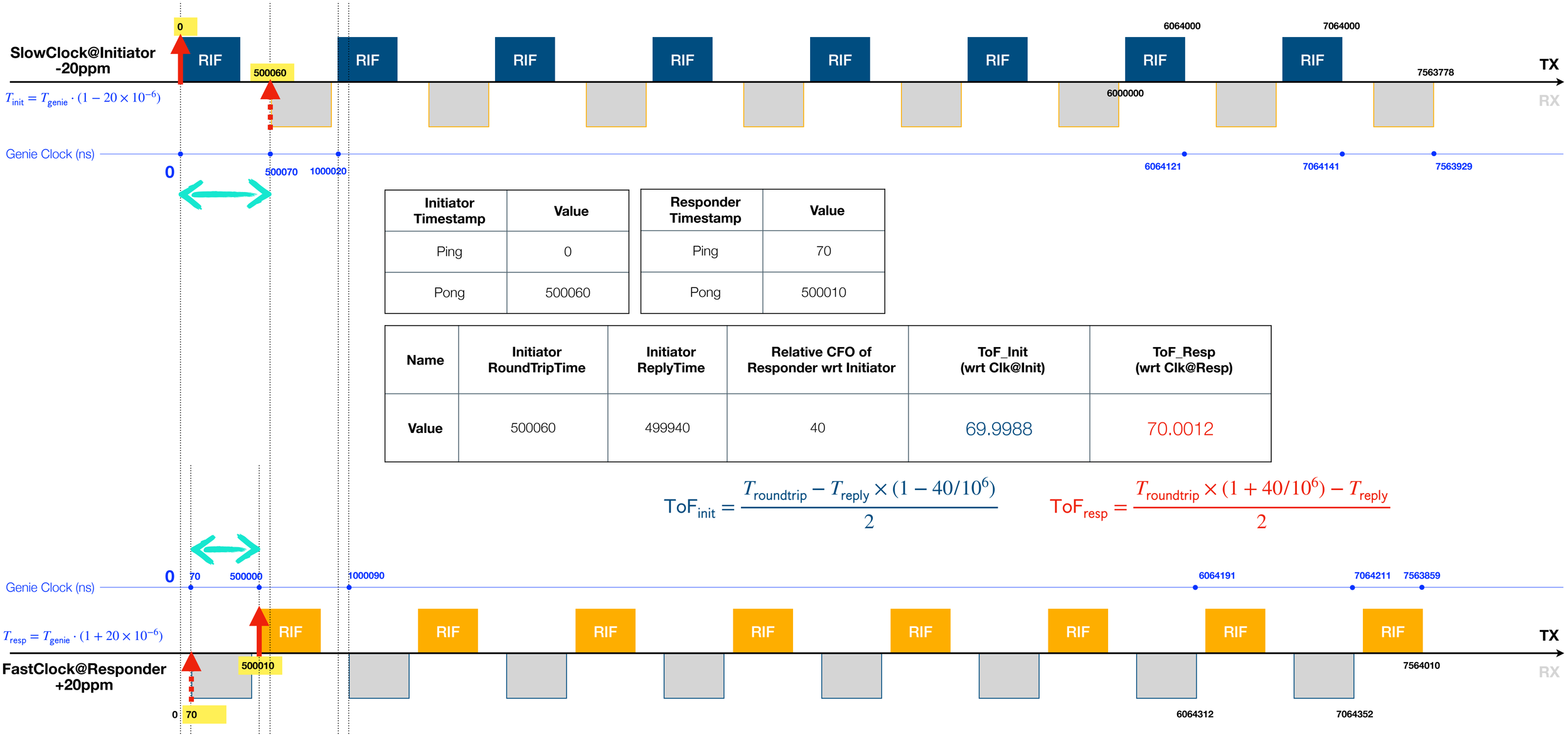
SS-TWR with 2 MMS Packets

Time unit: nano-second



SS-TWR with 2 MMS Packets

Time unit: nano-second



Initiator Timestamp	Value
Ping	0
Pong	500060

Responder Timestamp	Value
Ping	70
Pong	500010

Name	Initiator RoundTripTime	Initiator ReplyTime	Relative CFO of Responder wrt Initiator	ToF_Init (wrt Clk@Init)	ToF_Resp (wrt Clk@Resp)
Value	500060	499940	40	69.9988	70.0012

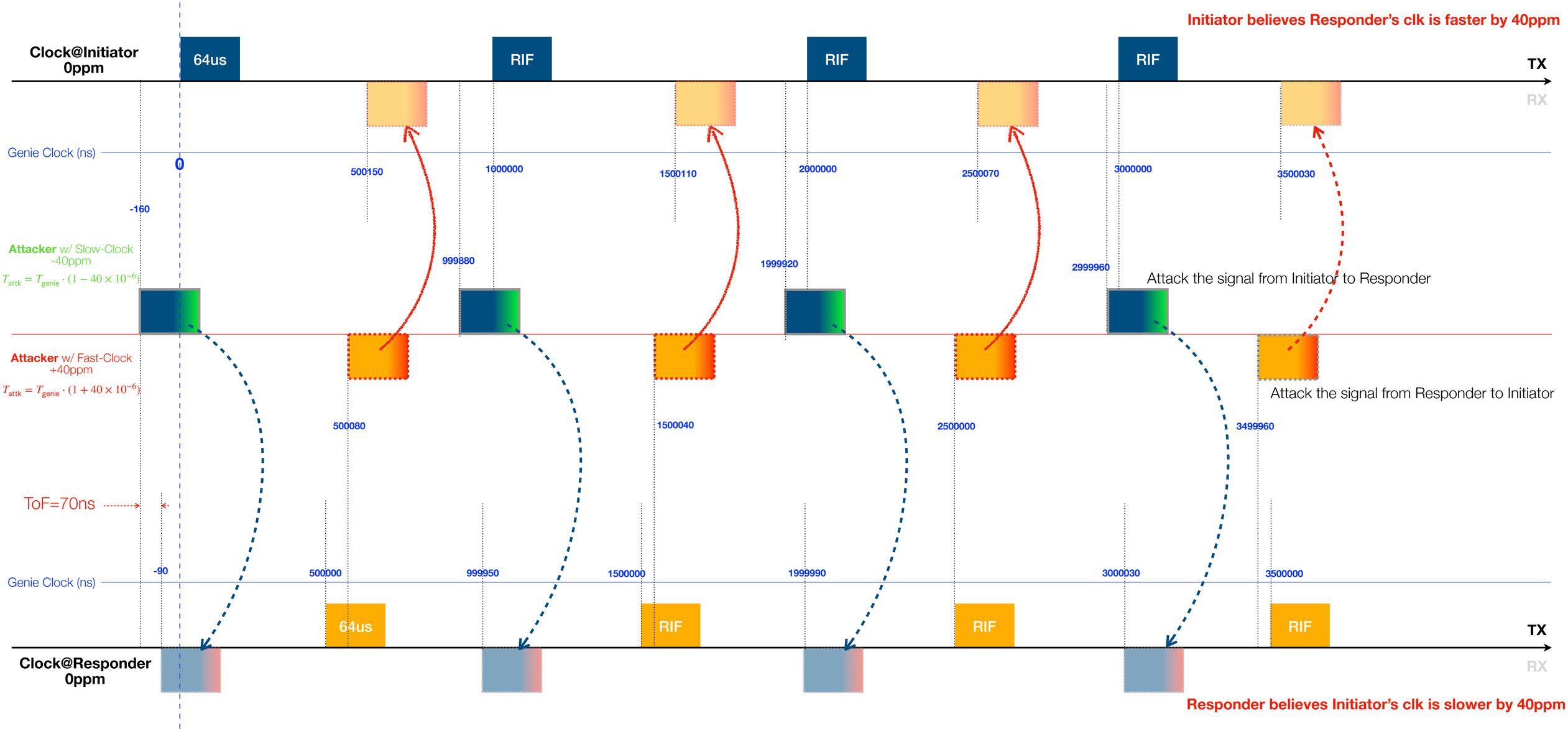
$$\text{ToF}_{\text{init}} = \frac{T_{\text{roundtrip}} - T_{\text{reply}} \times (1 - 40/10^6)}{2}$$

$$\text{ToF}_{\text{resp}} = \frac{T_{\text{roundtrip}} \times (1 + 40/10^6) - T_{\text{reply}}}{2}$$

Attack Case

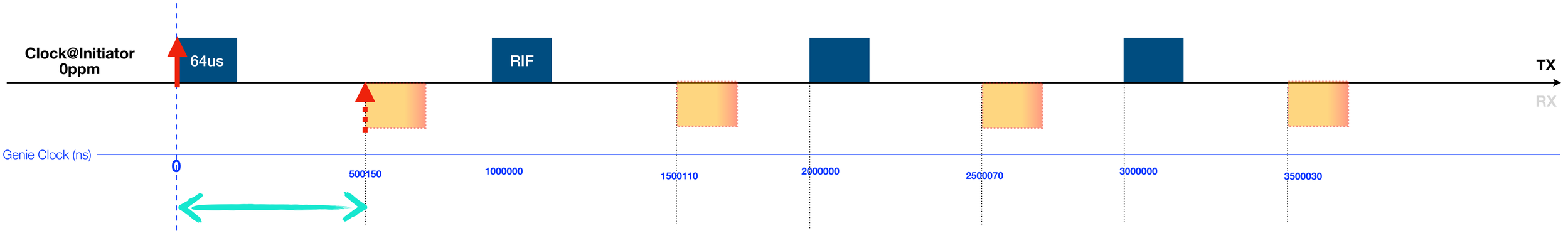
SS-TWR with 2 MMS Packets

Attack example, time unit: nano-second



SS-TWR with 2 MMS Packets

Attack example, time unit: nano-second

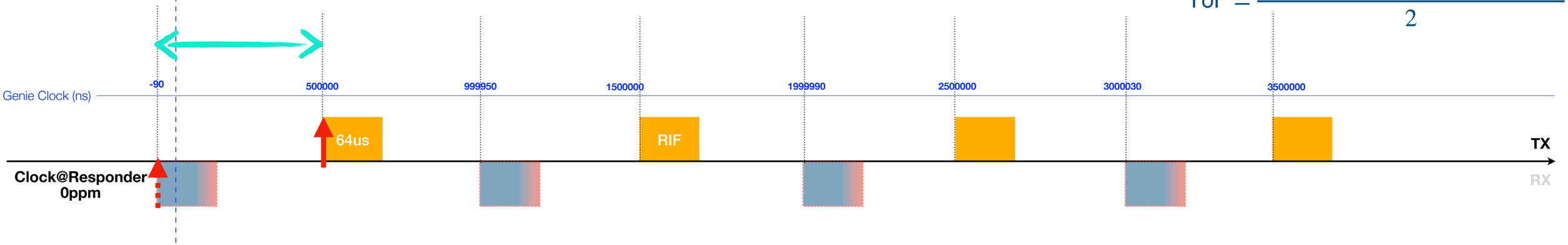


Initiator Timestamp	Value
Ping	0
Pong	500150

Responder Timestamp	Value
Ping	-90
Pong	500000

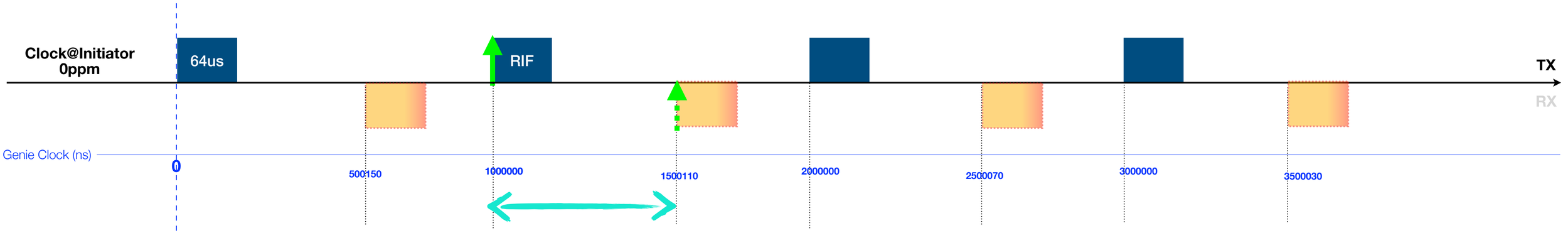
Name	Initiator RoundTripTime	Responder ReplyTime	CFO	ToF
Value	500150	500090	40	40.0018

$$\text{ToF} = \frac{T_{\text{roundtrip}} - T_{\text{reply}} \times (1 - 40/10^6)}{2}$$



SS-TWR with 2 MMS Packets

Attack example, time unit: nano-second

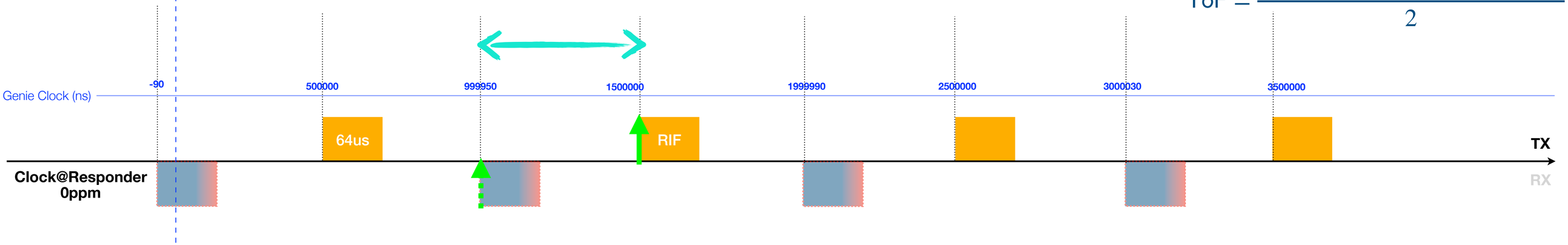


Initiator Timestamp	Value
Ping	1000000
Pong	1500110

Responder Timestamp	Value
Ping	999950
Pong	1500000

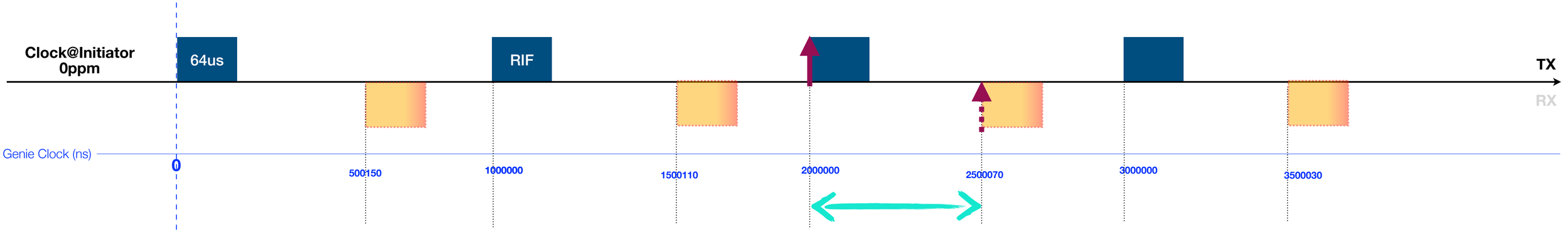
Name	Initiator RoundTripTime	Responder ReplyTime	CFO	ToF
Value	500110	500050	40	40.001

$$\text{ToF} = \frac{T_{\text{roundtrip}} - T_{\text{reply}} \times (1 - 40/10^6)}{2}$$



SS-TWR with 2 MMS Packets

Attack example, time unit: nano-second

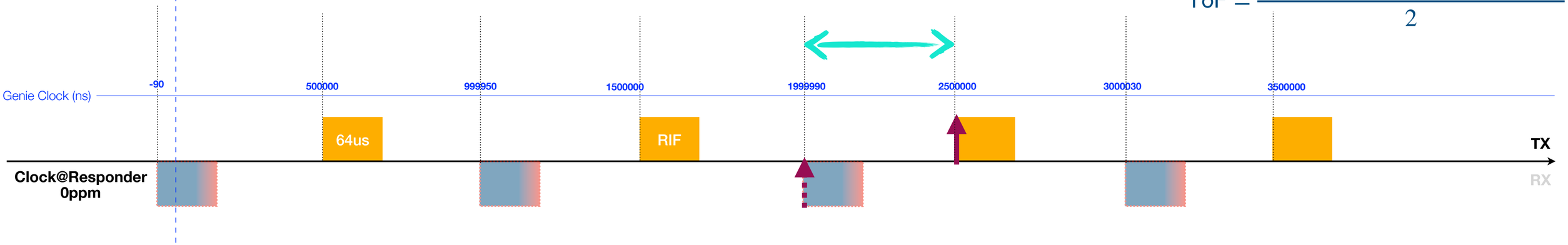


Initiator Timestamp	Value
Ping	2000000
Pong	2500070

Responder Timestamp	Value
Ping	1999990
Pong	2500000

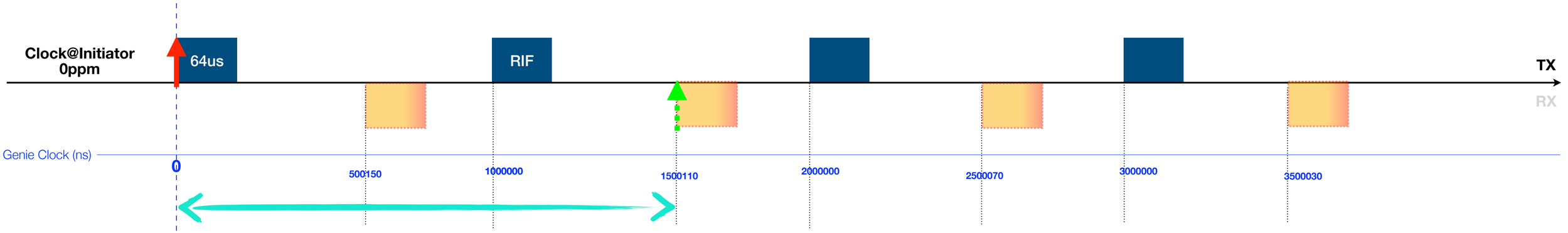
Name	Initiator RoundTripTime	Responder ReplyTime	CFO	ToF
Value	500070	500010	40	40.0002

$$\text{ToF} = \frac{T_{\text{roundtrip}} - T_{\text{reply}} \times (1 - 40/10^6)}{2}$$



SS-TWR with 2 MMS Packets

Attack example, time unit: nano-second

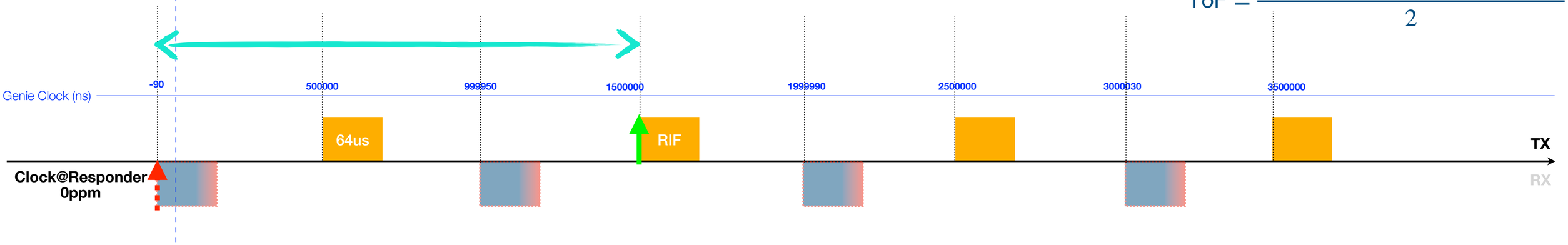


Initiator Timestamp	Value
Ping	0
Pong	1500110

Responder Timestamp	Value
Ping	-90
Pong	1500000

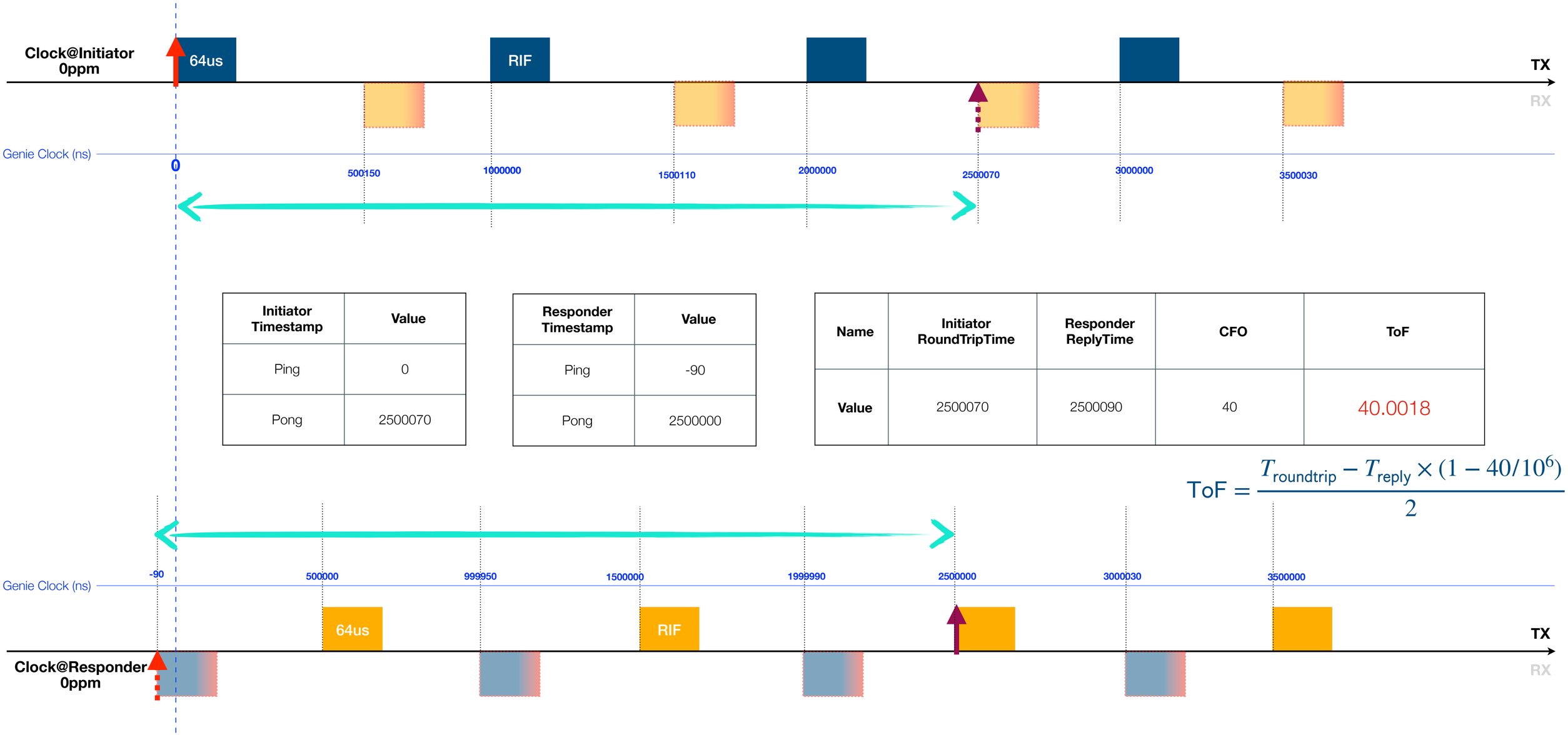
Name	Initiator RoundTripTime	Responder ReplyTime	CFO	ToF
Value	1500110	1500090	40	40.0018

$$\text{ToF} = \frac{T_{\text{roundtrip}} - T_{\text{reply}} \times (1 - 40/10^6)}{2}$$



SS-TWR with 2 MMS Packets

Attack example, time unit: nano-second



Initiator Timestamp	Value
Ping	0
Pong	2500070

Responder Timestamp	Value
Ping	-90
Pong	2500000

Name	Initiator RoundTripTime	Responder ReplyTime	CFO	ToF
Value	2500070	2500090	40	40.0018

$$\text{ToF} = \frac{T_{\text{roundtrip}} - T_{\text{reply}} \times (1 - 40/10^6)}{2}$$

Summary

- We have shown one possible attack to UWB MMS when SS-TWR is utilized to derive the ToF value
  - Prove one system is secure is hard
  - Prove one system is insecure could be simple and one counterexample is sufficient

- What we should do to achieve ranging integrity with UWB MMS
  - DS-TWR is necessary
  - More discussions and studies are still needed to ensure distance-bounding under DS-TWR
    - How to take advantage of the multiple RIF-RMARKERs defined in 4ab ?
    - How to report in an efficient manner?
    - Etc.