

## **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.

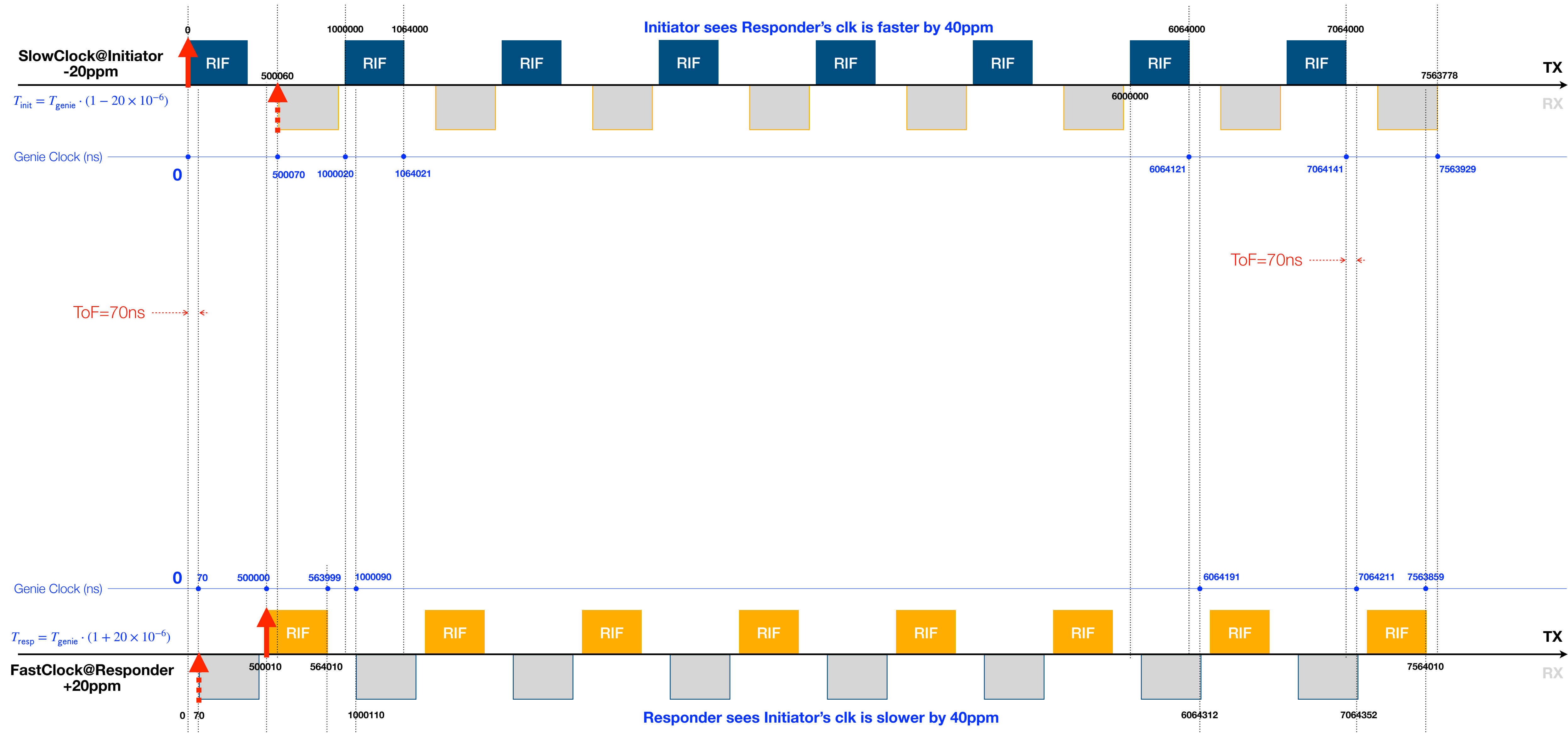
**Notice:** This document has been prepared to assist the IEEE P802.15. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.

**Release:** The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15.

# No-Attack Case

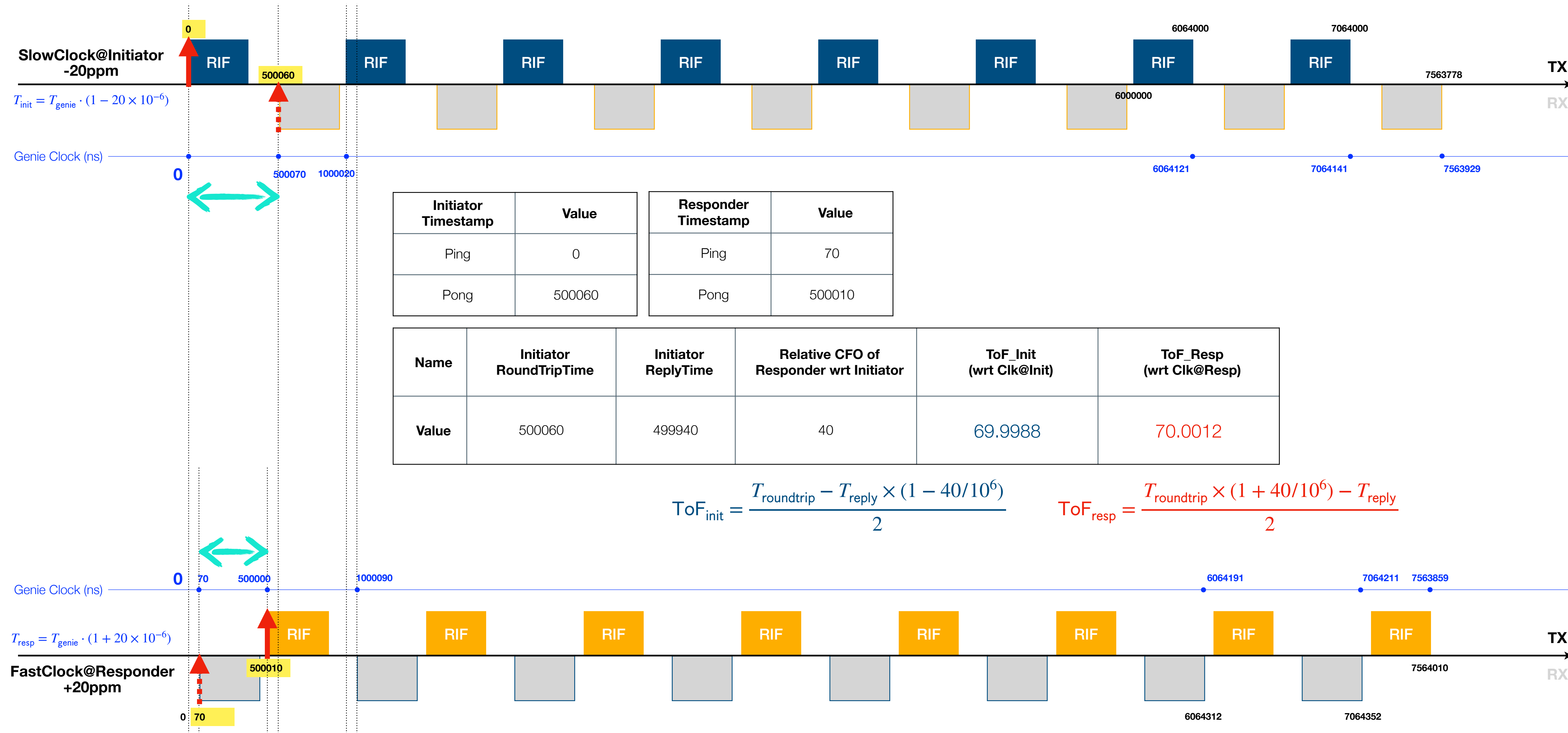
# SS-TWR with 2 MMS Packets

Time unit: nano-second



# SS-TWR with 2 MMS Packets

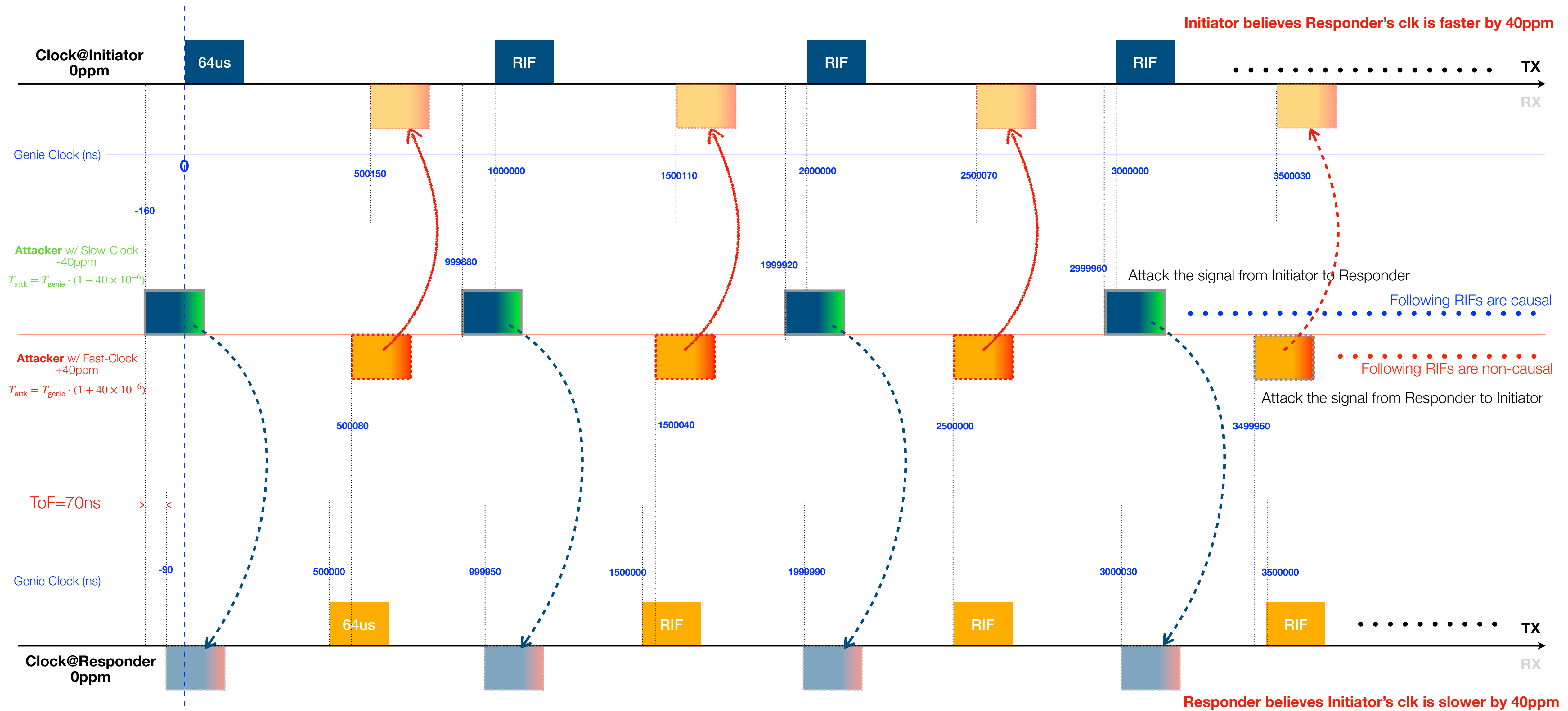
Time unit: nano-second



# Attack Case

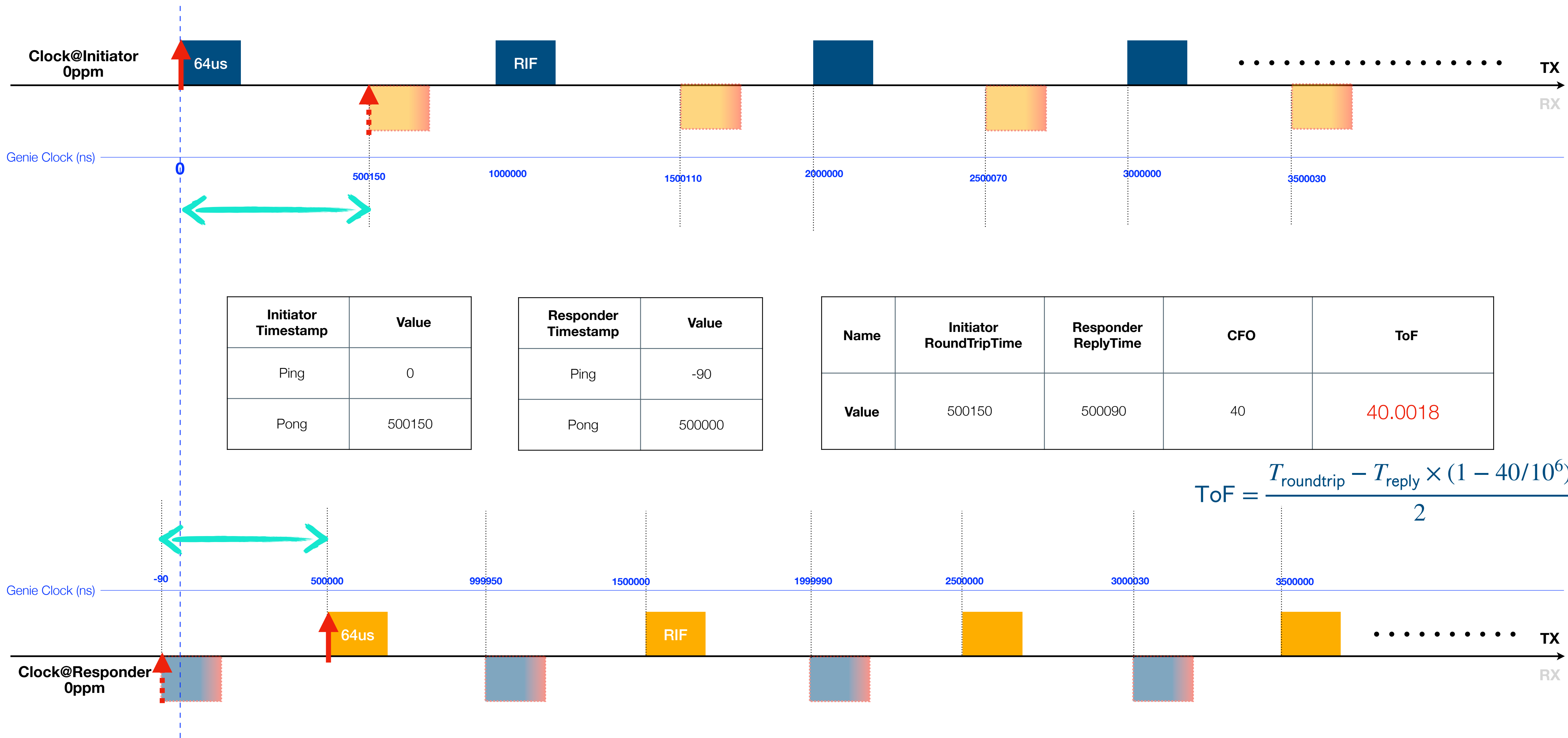
# SS-TWR with 2 MMS Packets

Attack example, time unit: nano-second



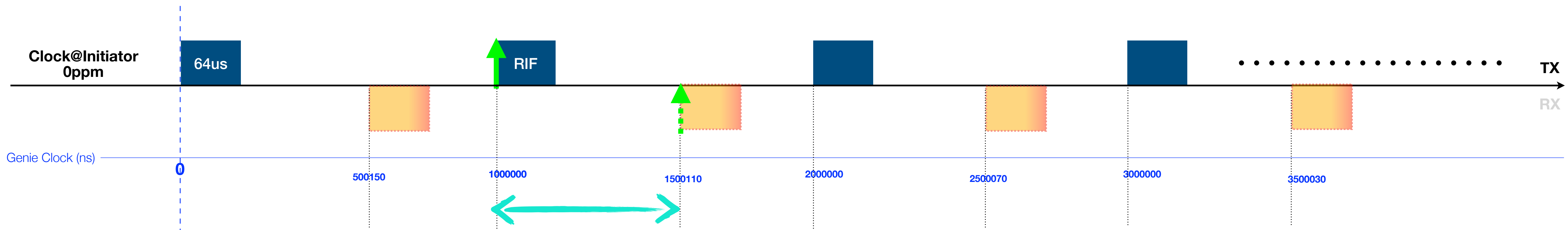
# SS-TWR with 2 MMS Packets

Attack example, time unit: nano-second



# SS-TWR with 2 MMS Packets

Attack example, time unit: nano-second

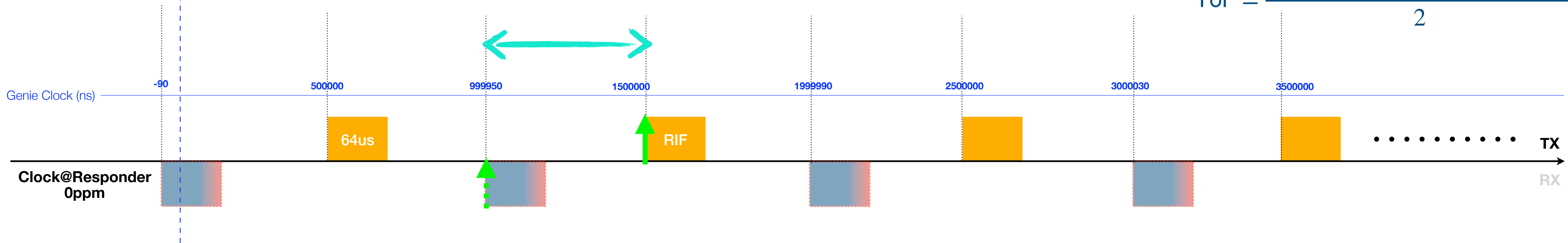


Initiator Timestamp	Value
Ping	1000000
Pong	1500110

Responder Timestamp	Value
Ping	999950
Pong	1500000

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

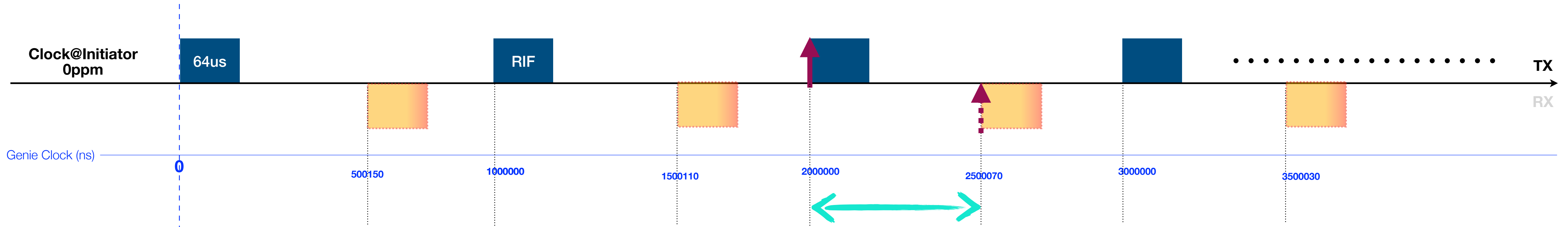
$$ToF = \frac{T_{roundtrip} - T_{reply} \times (1 - 40/10^6)}{2}$$





# SS-TWR with 2 MMS Packets

Attack example, time unit: nano-second

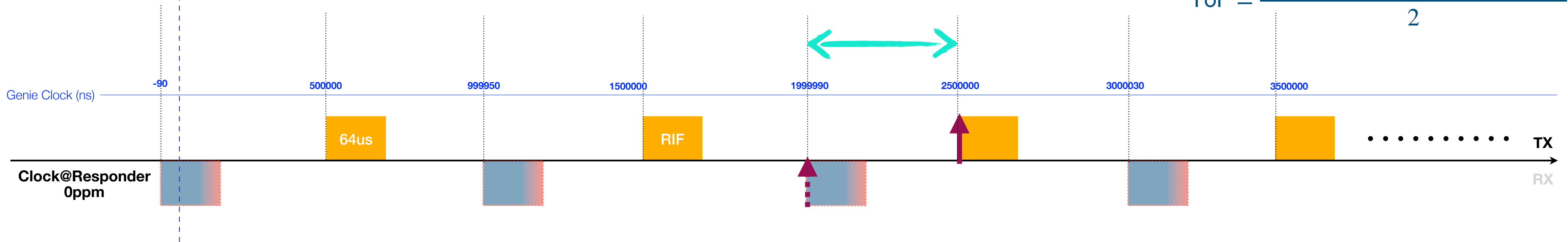


Initiator Timestamp	Value
Ping	2000000
Pong	2500070

Responder Timestamp	Value
Ping	1999990
Pong	2500000

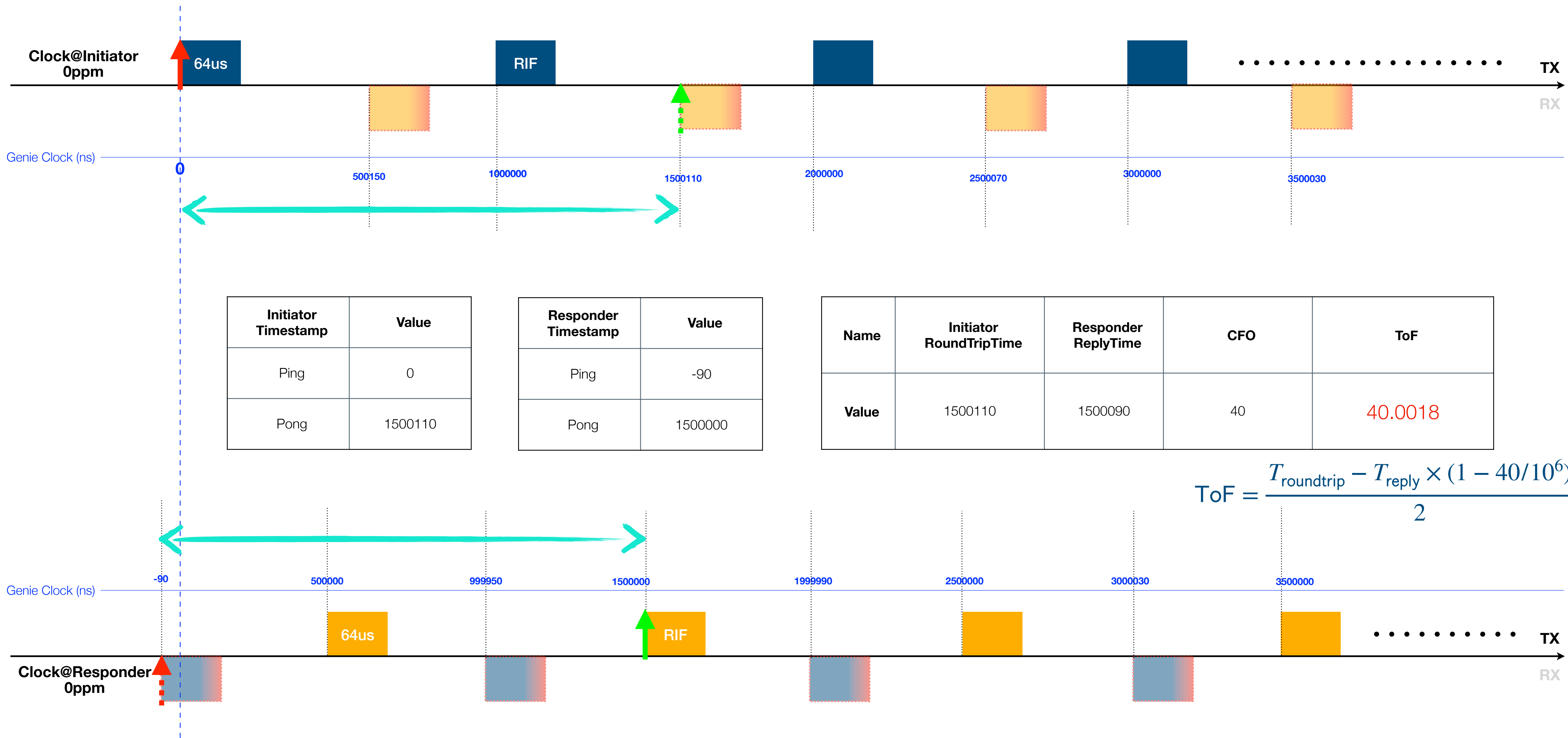
Name	Initiator RoundTripTime	Responder ReplyTime	CFO	ToF
<b>Value</b>	500070	500010	40	40.0002

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



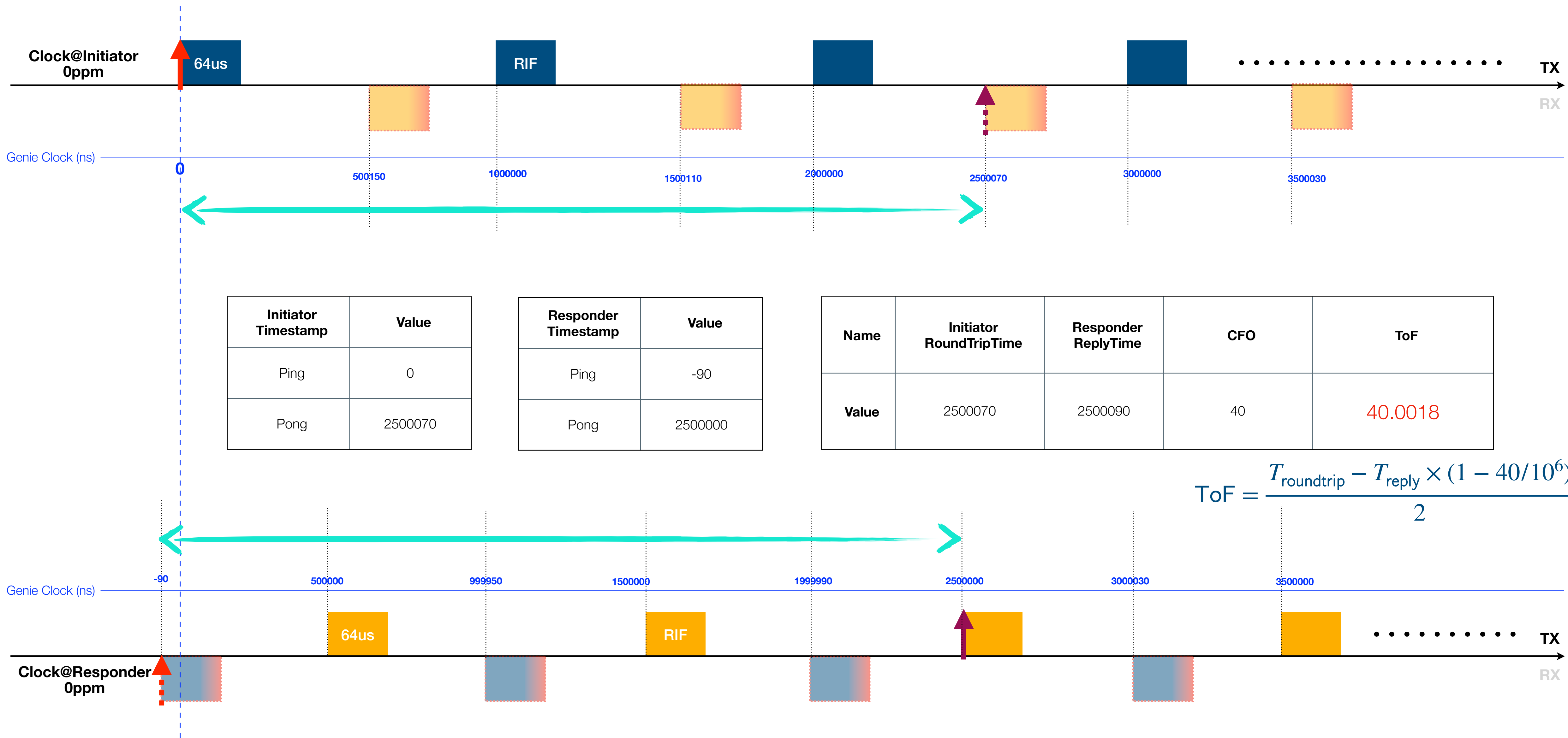
# SS-TWR with 2 MMS Packets

Attack example, time unit: nano-second



# SS-TWR with 2 MMS Packets

Attack example, time unit: nano-second



# 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.