Current Status of the TESLA Drafts:
Draft-ietf-msec-tesla-intro-01
Draft-ietf-msec-tesla-spec-00

Adrian Perrig, Bram Whillock (CMU)

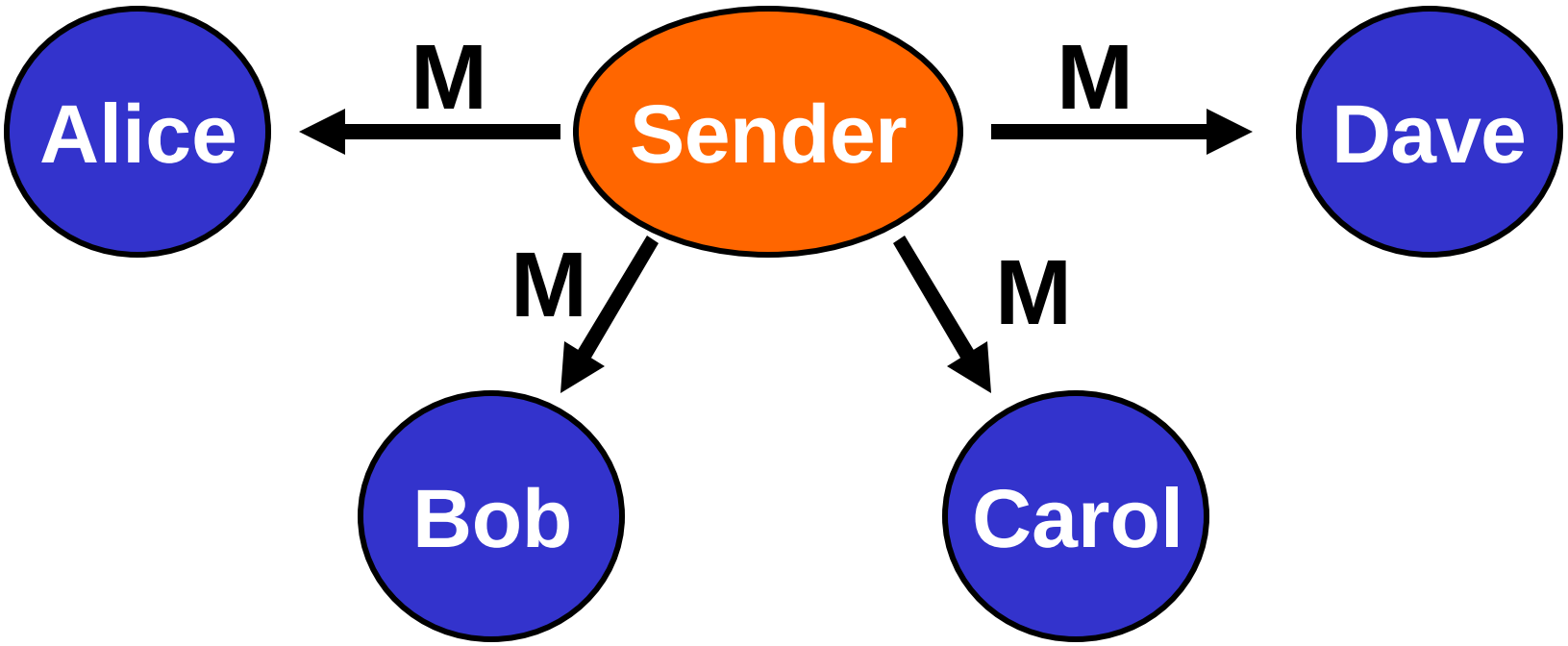
Ran Canetti (IBM)

Outline

- Review basic TESLA protocol
- Outline of the current drafts
- Recent updates
- Next steps

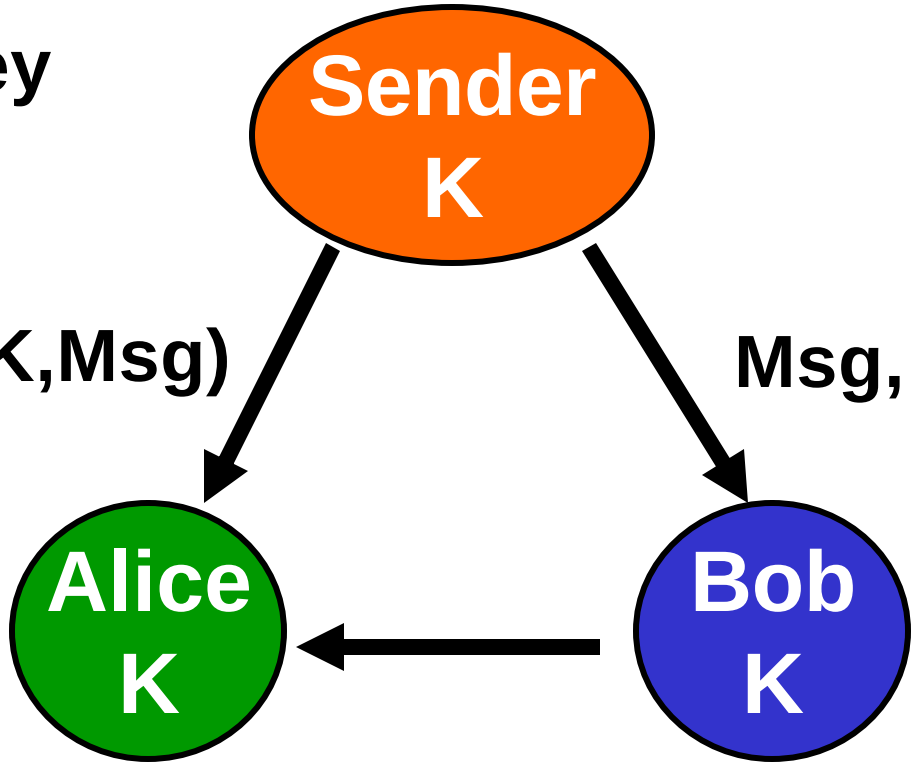
Broadcast Authentication

- Broadcasts data over wireless network
- Packet injection usually easy
- Receivers should be able to verify data origin



Authentication Needs Asymmetry

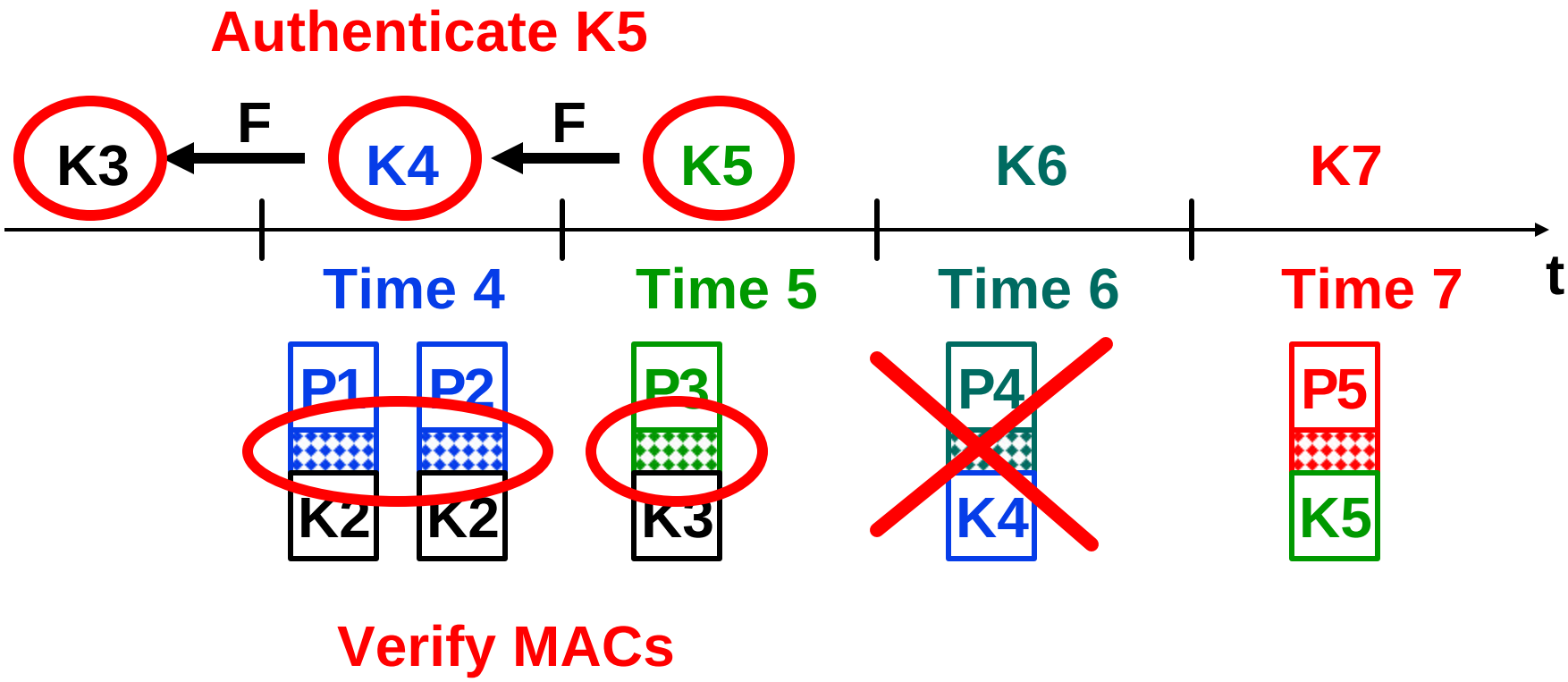
K = shared key



Forged Msg, MAC(K, Forged Msg)

MAC: Message Authentication Code
(authentication tag)

Basic TESLA Protocol

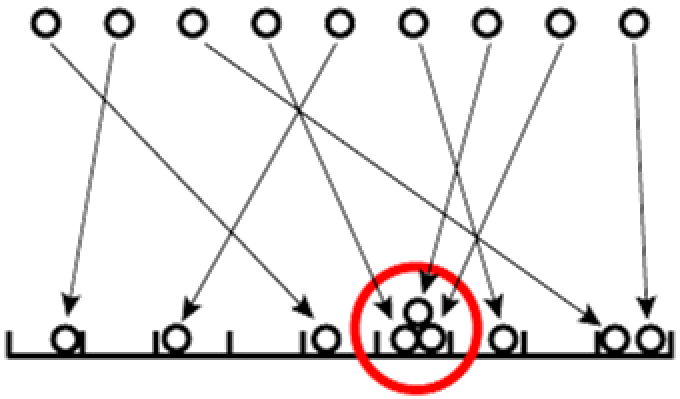


TESLA Features

- **Low overhead**
  - **Communication (~ 20 bytes)**
  - **Computation (~ 1 MAC computation / packet)**
- **Perfect robustness to packet loss**
- **Independent of number of receivers**
- **Delayed authentication (can be mitigated)**

Secure Broadcast Communication
in Wired and Wireless Networks

Adrian Perrig
J. D. Tygar



Kluwer

Outline of Current Drafts

- **Draft-ietf-msec-tesla-intro-01**
  - **Basic description/introduction to TESLA**
  - **For Informational RFC**
  - **http://www.securemulticast.org/draft-ietf-msec-tesla-intro-01.txt**
- **Draft-ietf-msec-tesla-spec-00**
  - **Plan: TESLA within ESP/MESP**
  - **For Standards Track RFC**
  - **http://www.securemulticast.org/draft-ietf-msec-tesla-spec-00.txt**

Draft-ietf-msec-tesla-intro-01

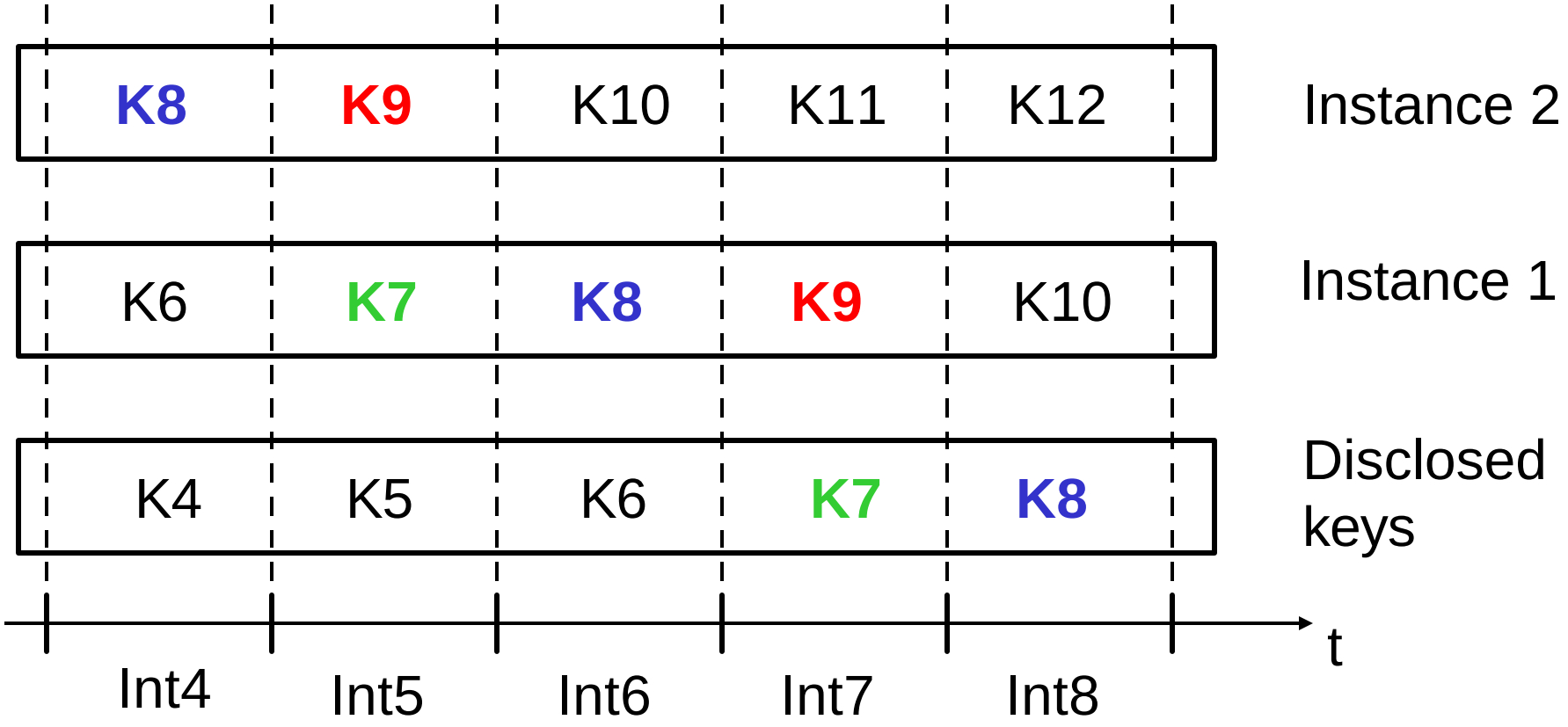
- General overview of the TESLA authentication protocol
- Add
  - Immediate authentication
  - Concurrent TESLA instances
- Last call before next IETF
- Comments welcome!

Immediate Authentication

- **Reasons for stand alone draft**
  - **Complex issues**
  - **Independent of TESLA, can be used with other authentication/signature schemes as well**
  - **Planned enhancements we're currently working on**

Concurrent TESLA Instances

- **Multiple TESLA instances share same key chain**
- **Only 10 bytes overhead for additional instance**



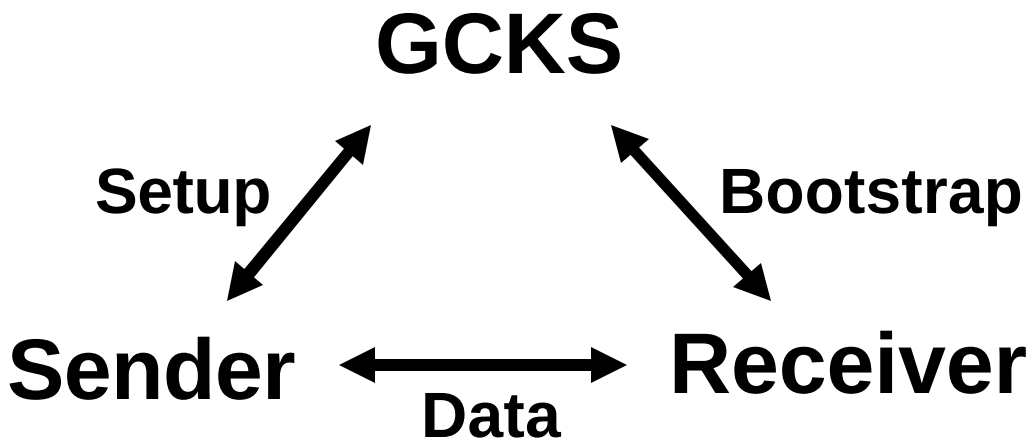
Draft-ietf-msec-tesla-spec-00

- **Current technical draft**
  - **Specifies TESLA field format**
  - **Format of bootstrap messages**
- **Future directions**
  - **TESLA within ESP/MESP**
  - **Changing key chains**
  - **Concurrent TESLA instances**
  - **Bootstrap TESLA parameters with GDOI / GSAKMP / MIKEY**
  - **For Standards Track RFC**

TESLA Bootstrapping

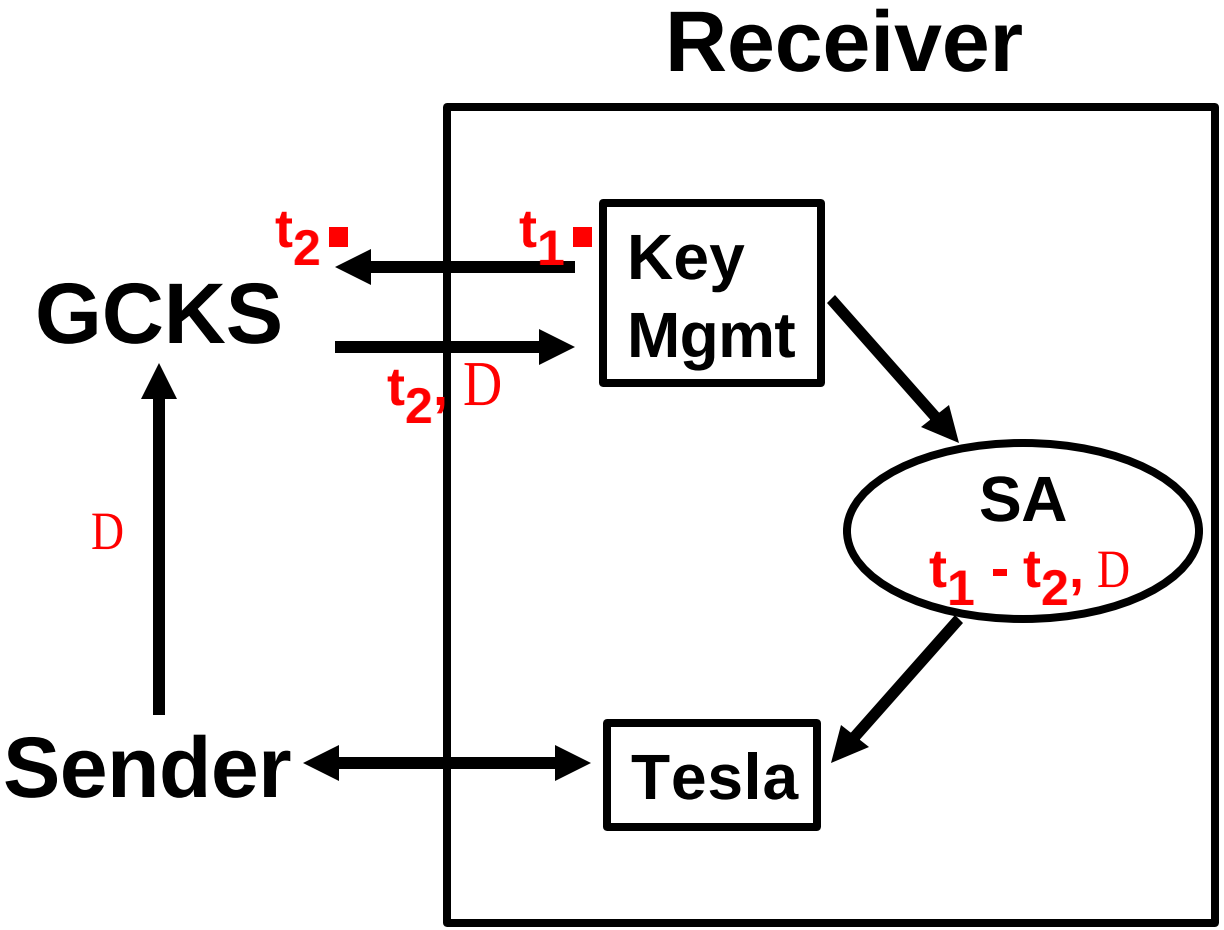
- **Required parameters**
  - **Loose time synchronization**
    i.e., upper bound on sender's clock
  - **Time interval information**
    - **Id of time interval (e.g., j)**
    - **Start time of time interval (T_j)**
    - **Time interval duration**
  - **Key disclosure interval**
  - **Authentic key chain value (K_j)**
- **Bootstrapped with key management protocol: GDOI / GSAKMP / MIKEY**

Indirect Time Synchronization via Key Management Protocol



- Time synchronization issues
  - Receiver needs upper bound on Sender time
  - Bootstrapping time through GCKS
  - GCKS has upper bound of time synchronization error
  - Receiver adds time synchronization errors

Receiver Diagram



Upper bound on sender's time: $t_S < t_R - t_1 + t_2 + D$

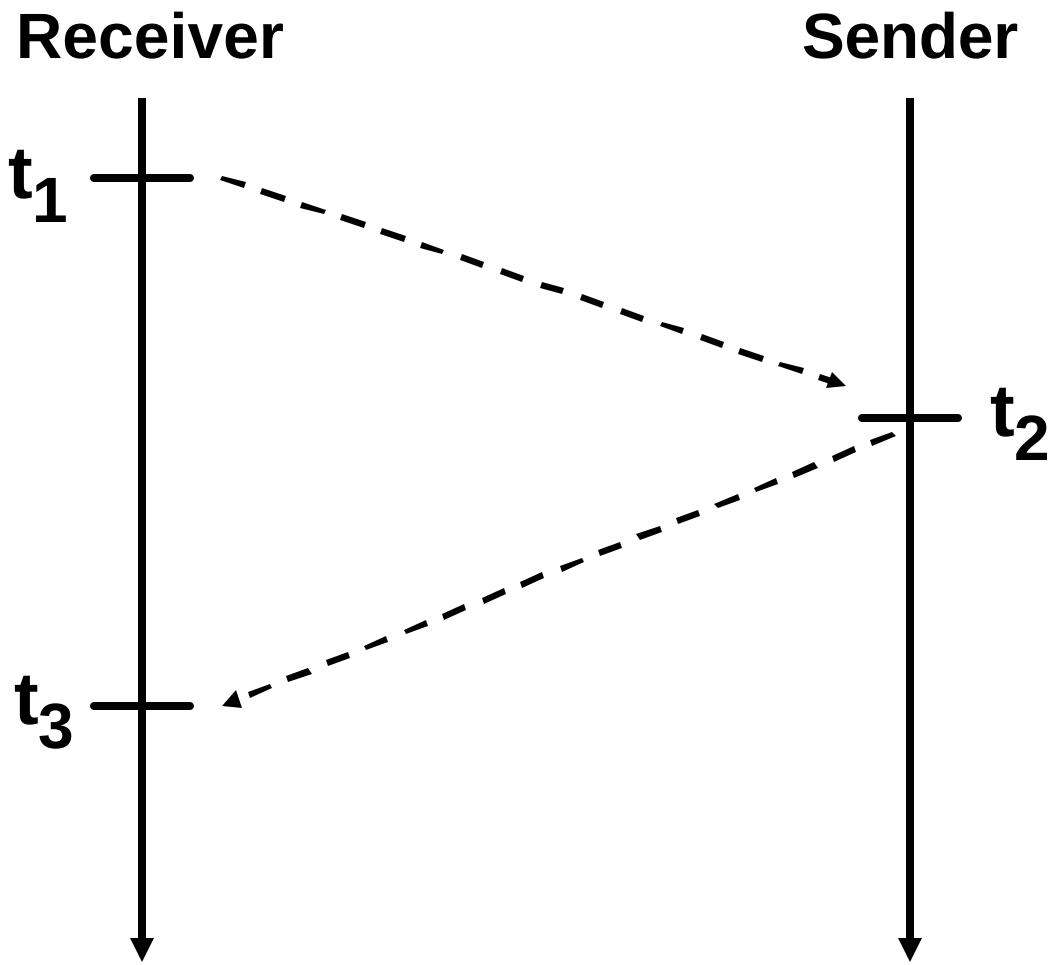
Recent Progress

- New additions to TESLA family
  - Mia Canetti
  - Bram Whillock
- Reference TESLA implementation by Bram Whillock
  - http://www.ece.cmu.edu/~adrian/tesla.html

Next Steps

- Need team for second implementation
- http://www.ece.cmu.edu/~adrian/tesla.html
- Integrate with ESP/MESP
- Bootstrap TESLA parameters with GDOI / GSAKMP / MIKEY

Upper Bound on Sender's Time



Upper bound on sender's time: $t_S < t_R - t_1 + t_2$