TESLA: Multicast Source Authentication Transform

Bob Briscoe (BT)
Ran Canetti (IBM Watson)
Adrian Perrig (UC Berkeley / Digital Fountain)
Dawn Song (UC Berkeley)
Doug Tygar (UC Berkeley)

Problem: Efficient Source Authentication

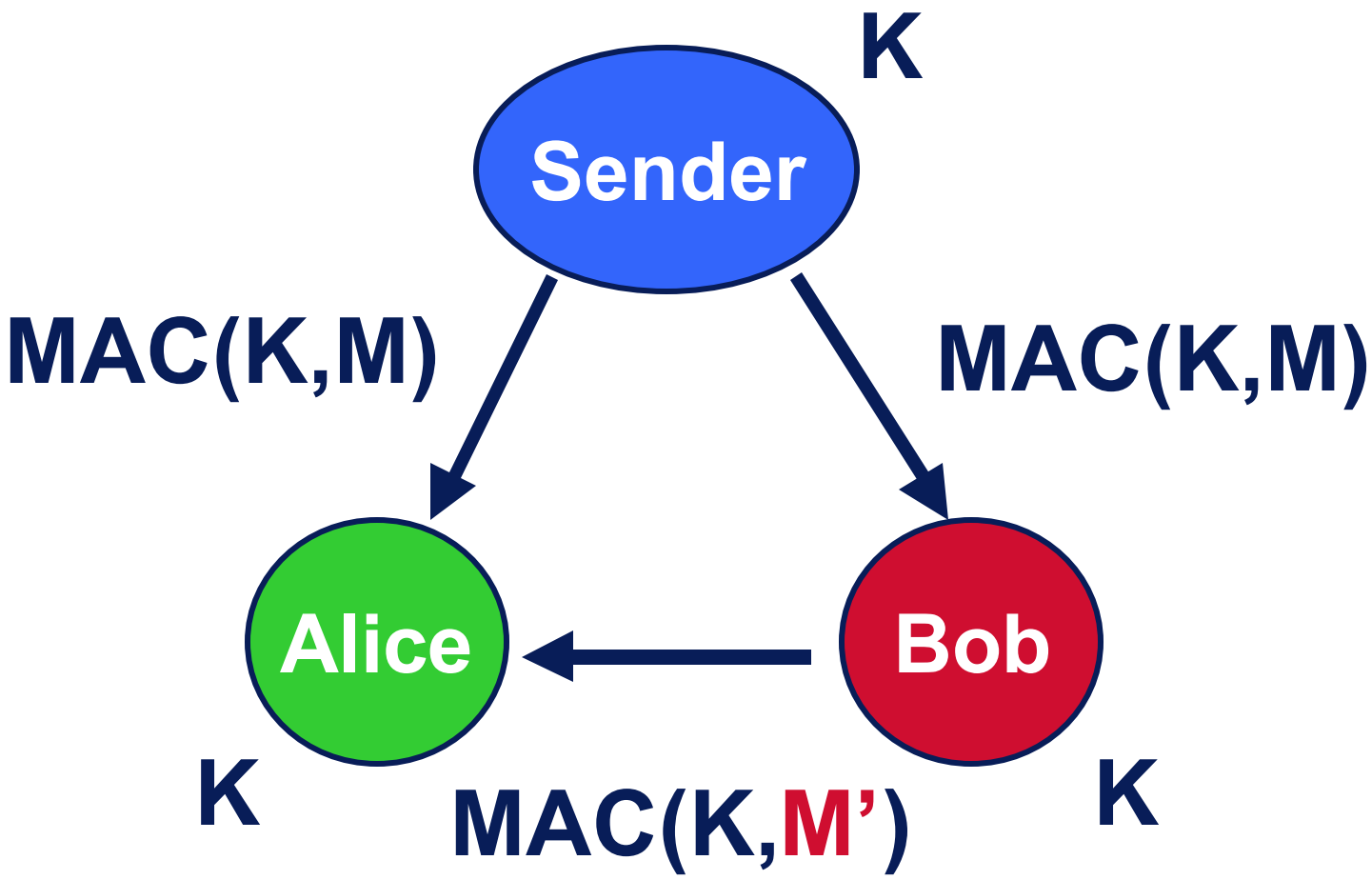
- One sender, many receivers
- Lossy channel (lost packets not retransmitted)
- Receiver authenticates individual packets
- Real-time data

How Do We Solve Source Authentication in Unicast?

- Sender and receiver share secret key
- Sender attaches MAC to every packet
- Receiver verifies each MAC

- Low overhead
  - ~10 bytes per packet
  - MAC computation is fast (~1,000,000/s)
- Secure in two-party case
- But: Insecure in multi-party case

Problem: Simple MAC is Insecure for Multiple Receivers



What About Digital Signatures?

- Sender attaches signature to each packet
- Signatures are too expensive
  - High computation cost (~100/s)
  - High verification cost (~1000/s)
  - High communication cost (128 bytes)
- Amortize signature over multiple packets
  - Signature might get lost
  - Opens doors to DoS attacks
- One-time signatures
  - High computation cost (~10,000/s)
  - High communication cost (~200 bytes)

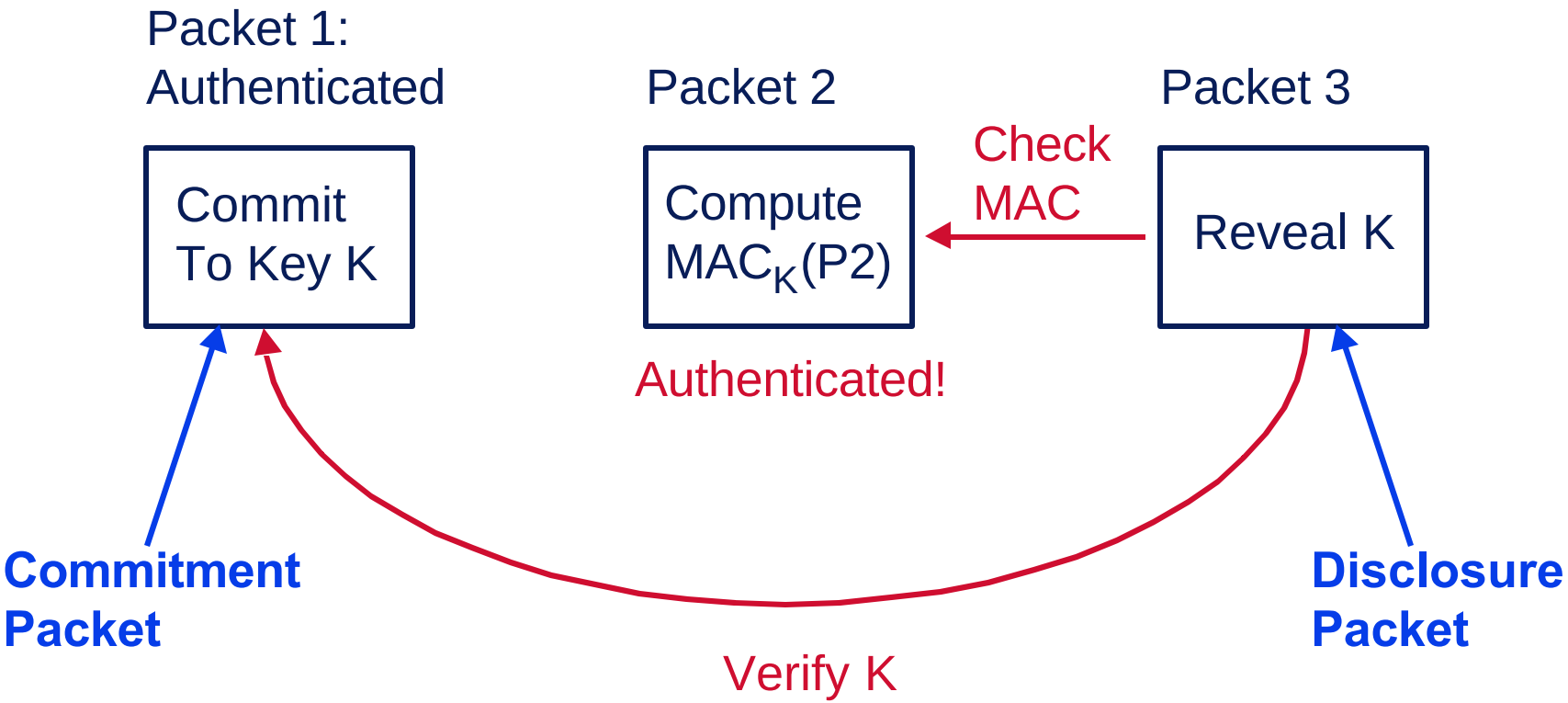
TESLA

- Provides multicast source authentication
- Efficient:
  - ~1 MAC function computation (~1,000,000/s)
  - Low overhead (10-20 bytes)
- Perfect loss robustness
- Scalable: After initial receiver bootstrap, unidirectional data flow
- Drawback: Delayed authentication

TESLA Status

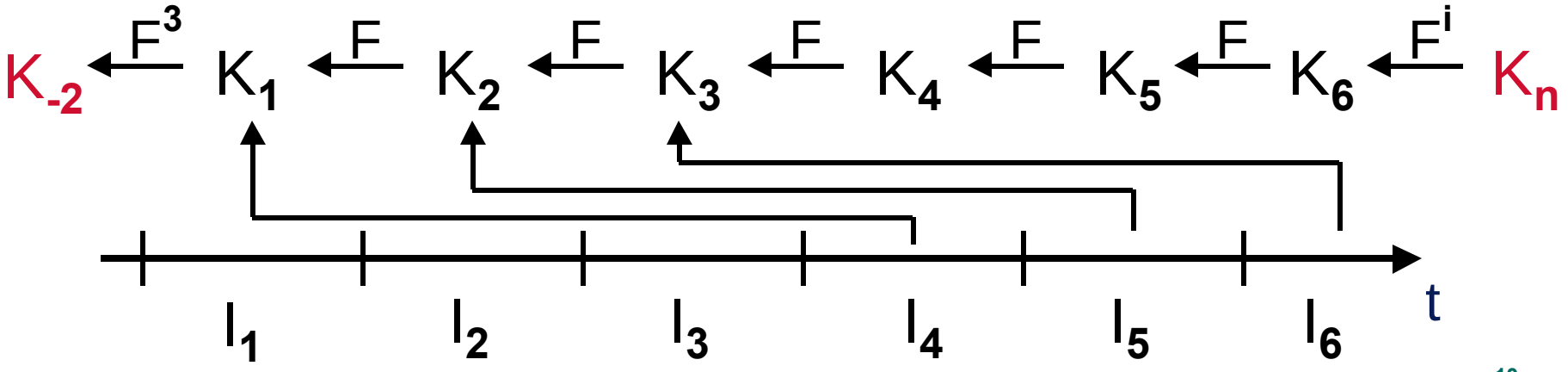
- **Conference papers:**
  - **IEEE Security & Privacy 2000**
  - **NDSS 2001**
- **Internet draft:**
  - **Source authentication transform in MESP/AMESP**
  - **Suits authentication needs for RMT**
  - **http://www.ietf.org/internet-drafts/ draft-irtf-smug-tesla-00.txt**
- **More information: www.securemulticast.org**

Basic TESLA Scheme



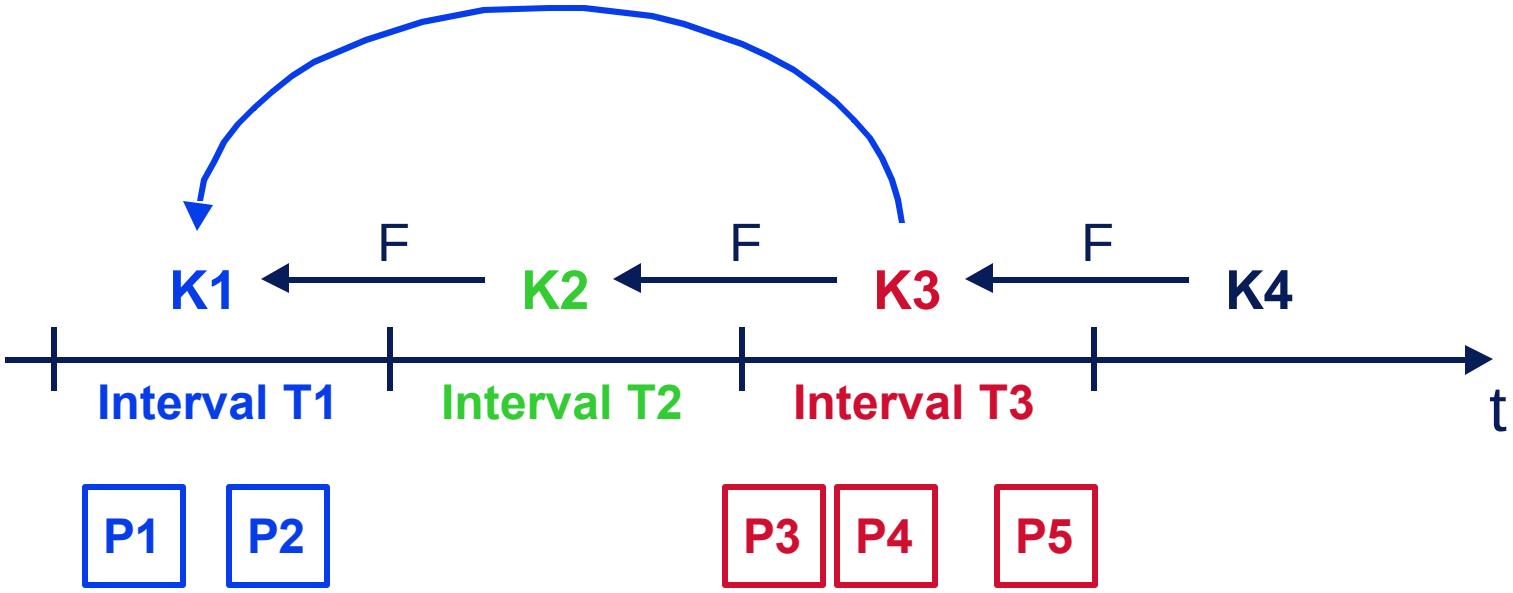
Sender Setup

- **Interval definition**
  - Beginning time of one specific interval
  - Interval duration
- **Key chain**
  - Pseudo-random function F
  - Key chain commitment
  - Disclosure delay

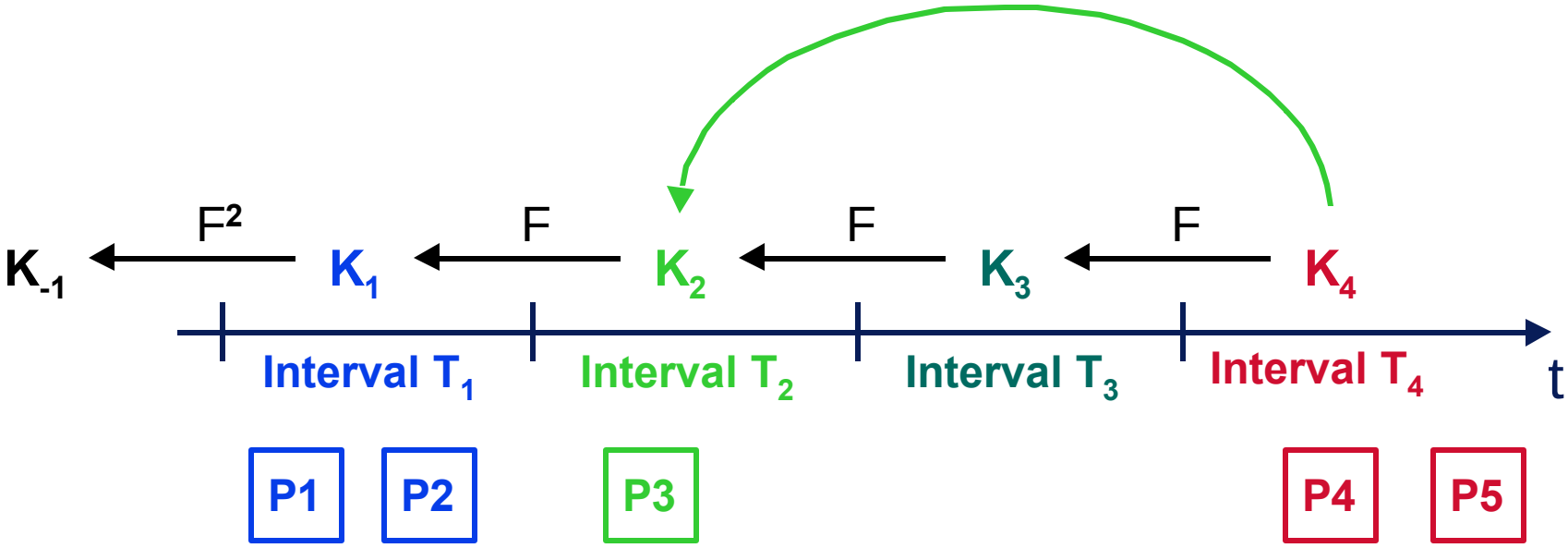


Sending Authenticated Packets

- **Authentication information for P2: MAC(K1, D2)**



Receiver Tasks



Security Condition

- Sender, receiver weakly time synchronized ($\pm d_t$)

- **Security Condition** (for Packet P):
  Receiver is certain that packet P arrives before sender discloses K_P

- If security condition not satisfied, drop packet
- Attacker can at most do denial-of-service attack
  - Speeding up / delaying packets does not help