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

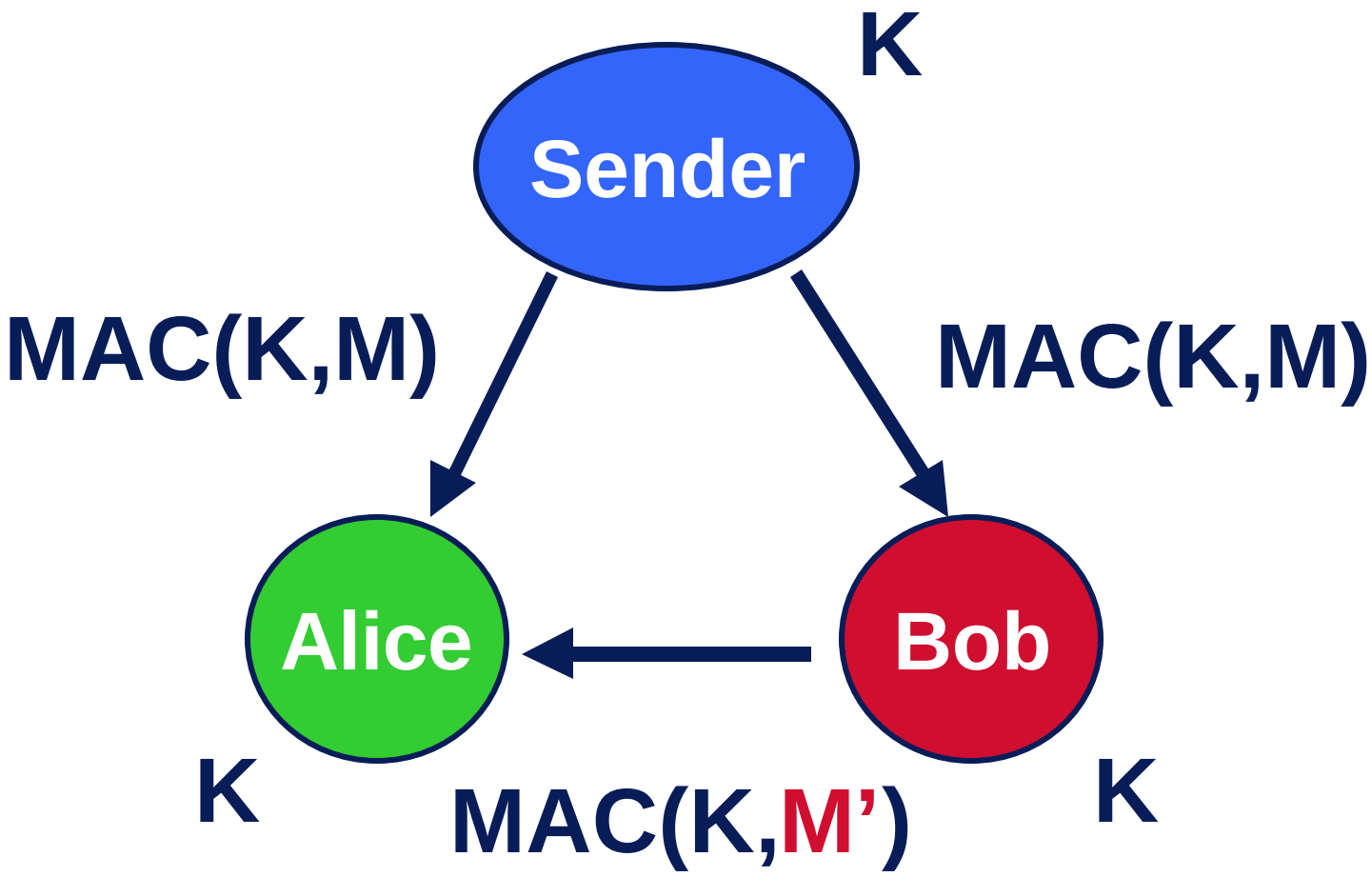
- One sender, many receivers
- Lossy channel (lost packets not retransmitted)
- Receiver authenticates individual packets
- Real-time data

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



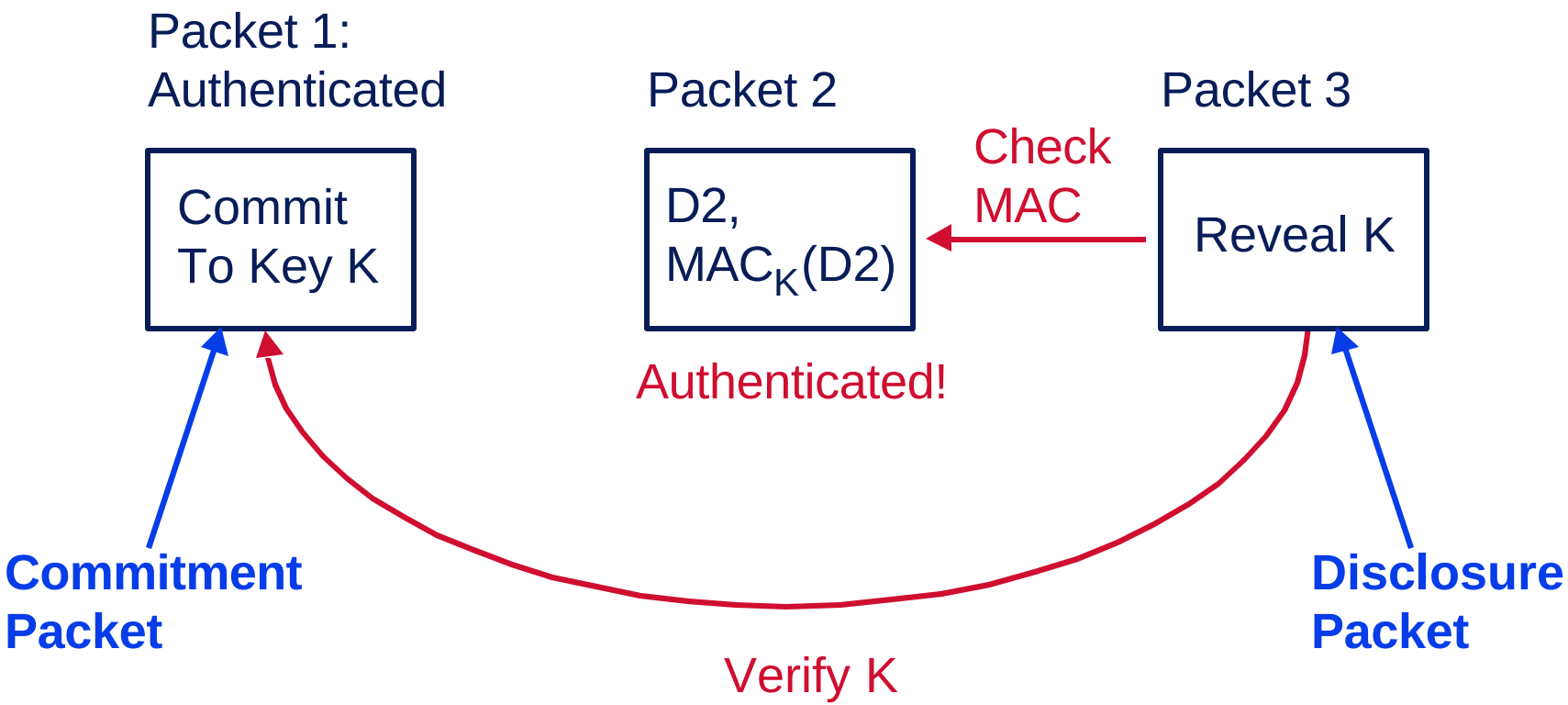
What About Digital Signatures?

- **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:**
  - **Can verify only if all packets arrive intact**
  - **Signature might get lost**
  - **Some partial solutions exist, but not completely satisfactory [GR,WGL,R]**
- **Other solutions exit, none are satisfactory.**

TESLA

- Provides multicast source authentication
- Efficient:
  - 2-3 MAC function computations (~1,000,000/s)
  - Low bandwidth overhead (10-20 bytes)
- Perfect resilience to packet loss
- Scalable: After initial receiver bootstrap, unidirectional data flow
- Drawbacks:
  - Relies on loose time synchronization w/ source.
  - Delayed authentication
  - Keeps state across packets

TESLA: The basic idea



Security Condition

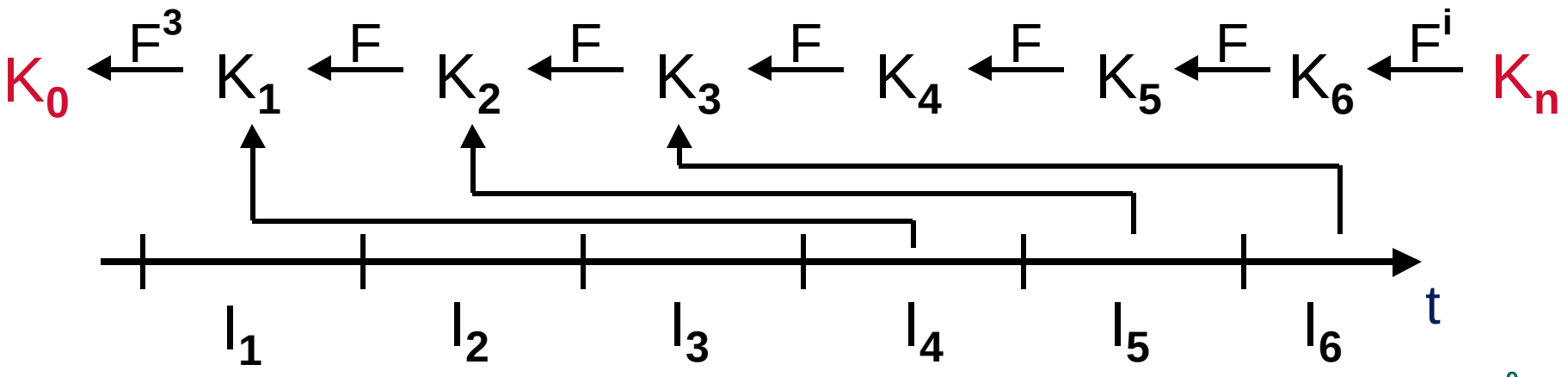
- Sender, receiver weakly time synchronize ($\pm \mathbf{d}_t$) (can be done in the registration protocol)

- **Security Condition** (for Packet P):
  Receiver verifies 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

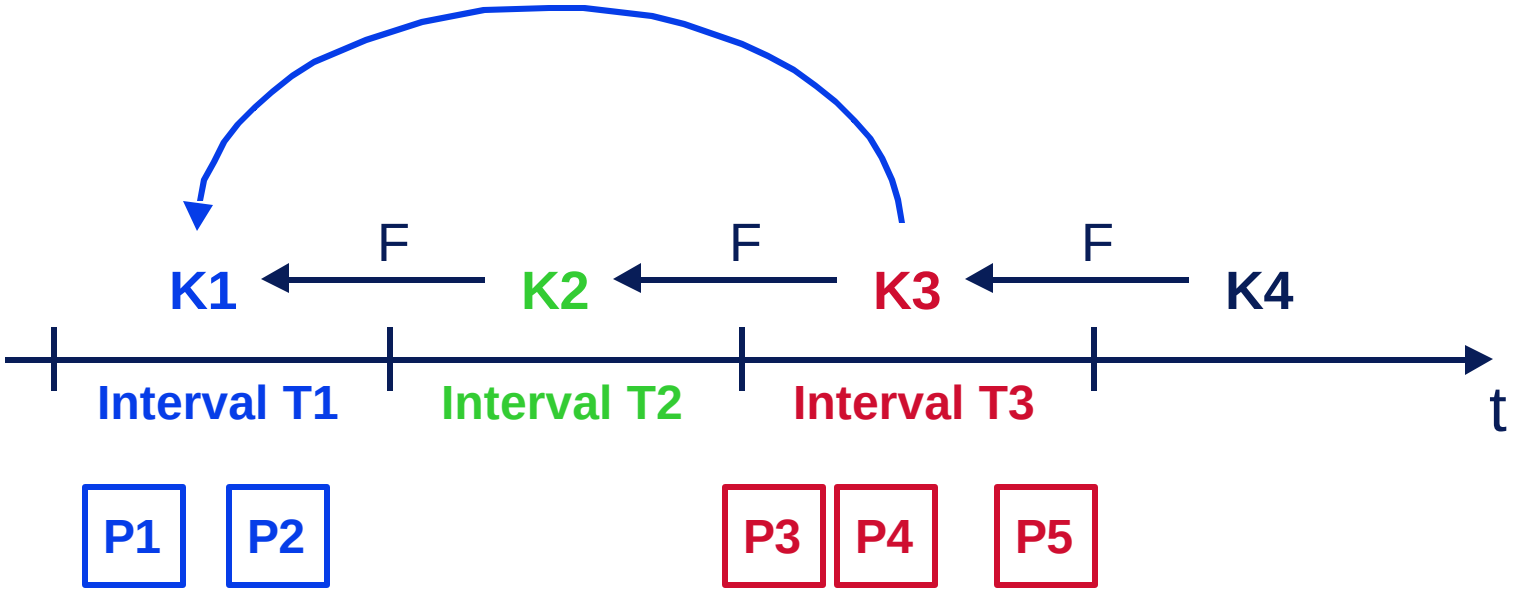
Sender Setup

- **Interval definition**
  - **Beginning time of one specific interval**
  - **Interval duration, disclosure delay**
- **Key chain**
  - **Compute using a pseudo-random function F**
  - **Digitally sign K_0, give to receivers at registration.**



Sending Authenticated Packets

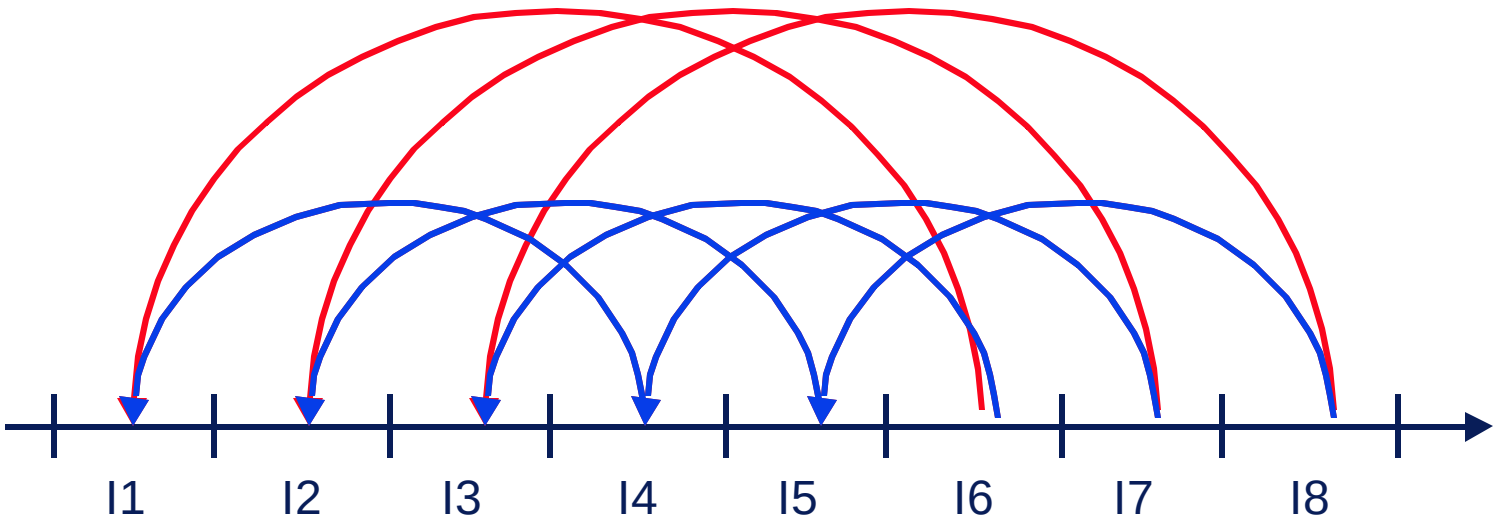
- **Authentication information for P2: MAC(K1, D2)**



Dealing with heterogenous delays

- Minimal disclosure time delay depends on RTT
- Different receivers prefer different disclosure time delay

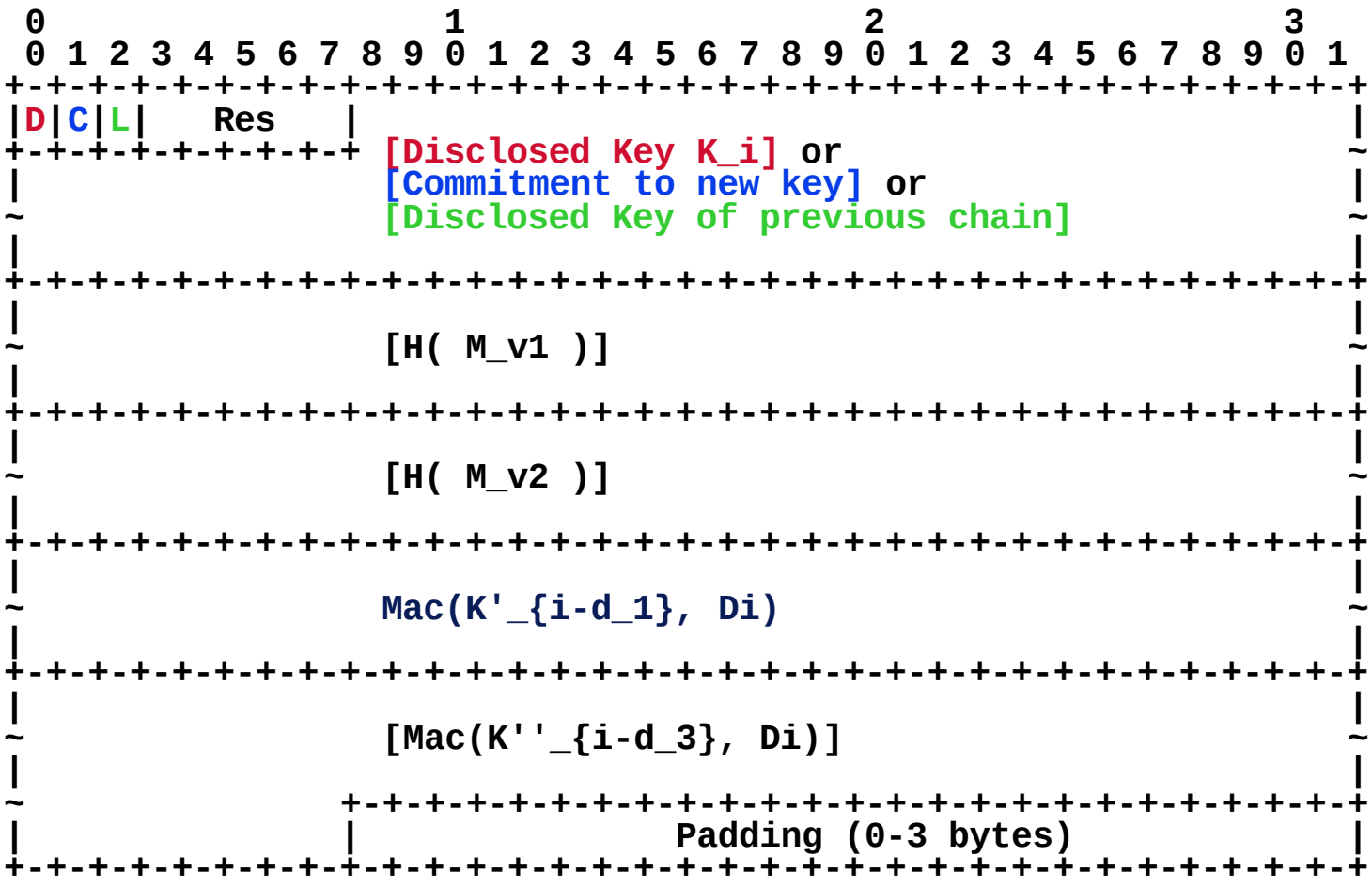
- Solution: Include multiple instances of basic scheme



TESLA within MESP/AMESP

- **TESLA can be used as the external authentication mechanism in MESP or AMESP.**
- **What needs to be specified is:**
  - **Format of external authentication field.**
  - **Structure of the corresponding SA. (This will be part of SA3.)**

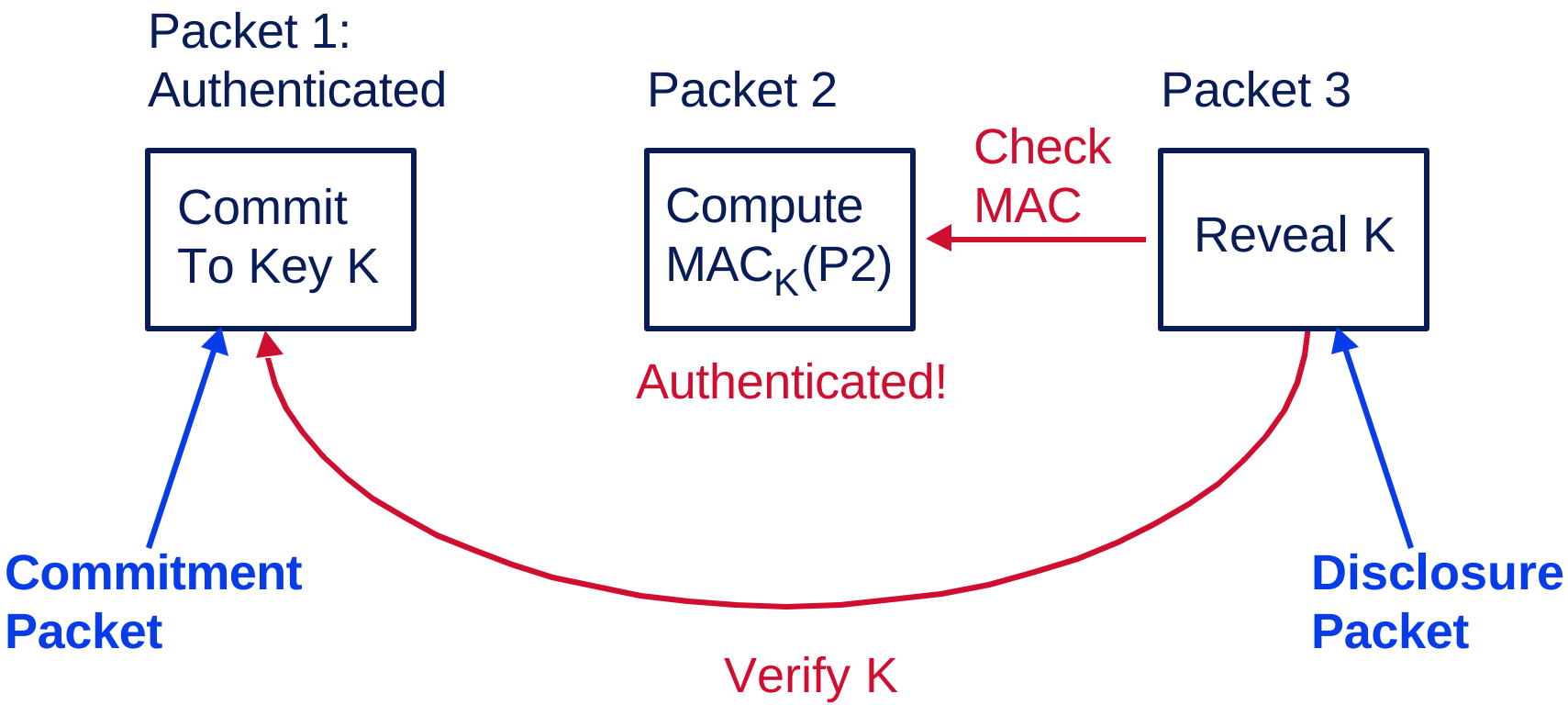
Authentication Field Format



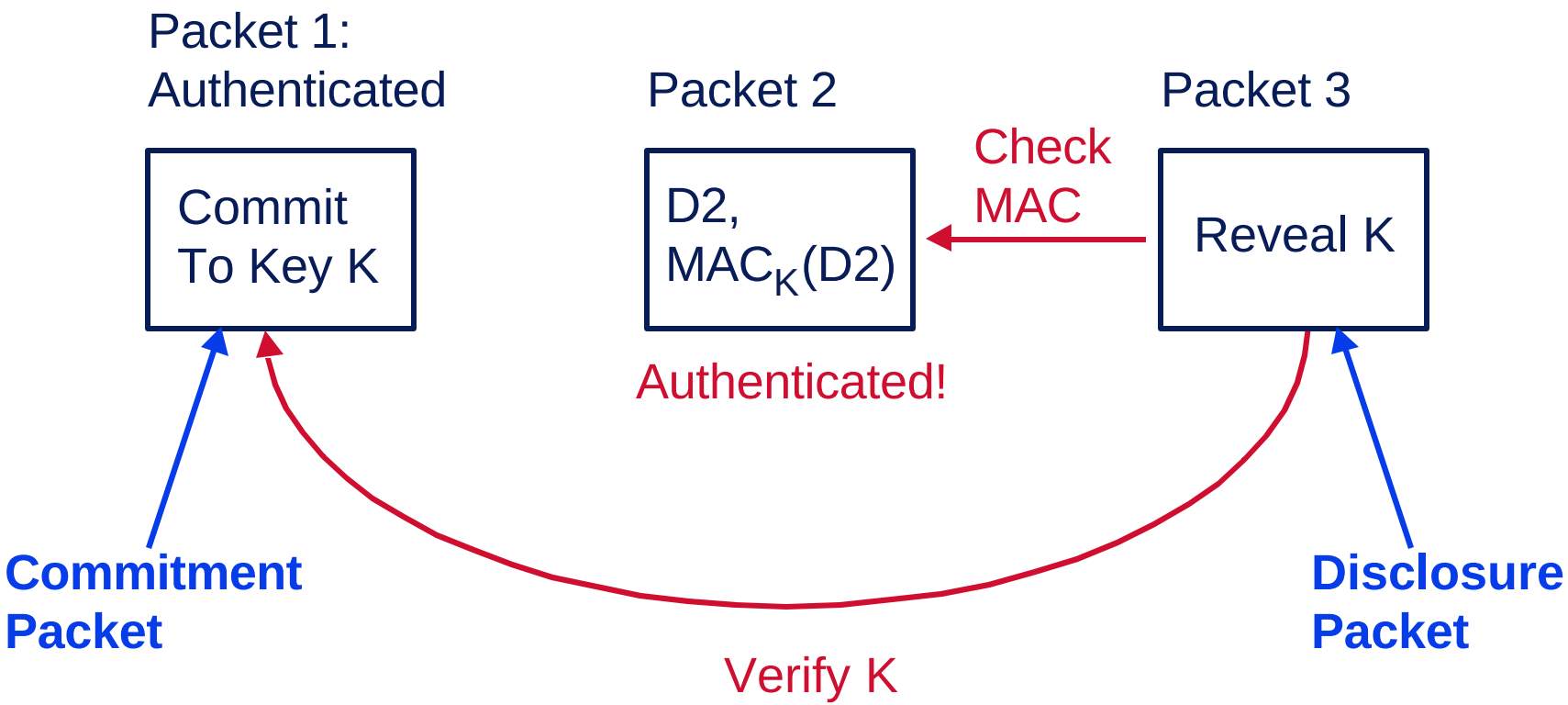
TESLA Status

- **Conference papers:**
  - **IEEE Security & Privacy 2000, NDSS 2001**
  - **See relevant references/credits there**
- **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



Step 1: Basic Scheme



Receiver Tasks