# Trusted Multi-Path TCP extension

draft-hewu-mptcp-trust-00

**Hewu Li**, Qian Wu, Boyang Wu, **Qi Zhang**, Jiang Zhou,  Jun Liu

Tsinghua  University, China


清華大學
Tsinghua University

MPTCP WG - IETF 106
Singapore, 2019.11.19

# Motivation

- **Trust in Internet has been and is being supported by more and more infrastructures.**
  - **S**ource **A**ddress **V**alidation (SAV) mechanisms are developed to prevent IP spoofing, thus improving the accountability of Internet.
    - SAVI: Source Address Validation Improvements (IETF SAVI WG, RFC 7039)
    - SAVA: Source Address Validation Architecture (RFC 5210)
- Multipath TCP (MPTCP) is facing security challenges caused by forged control packets sent by malicious hosts with forged IP addresses. (RFC6181, RFC7430)
- **Extend MPTCP to work with SAV**
  - Improve the accountability of MPTCP connections.
  - Security can also be improved.

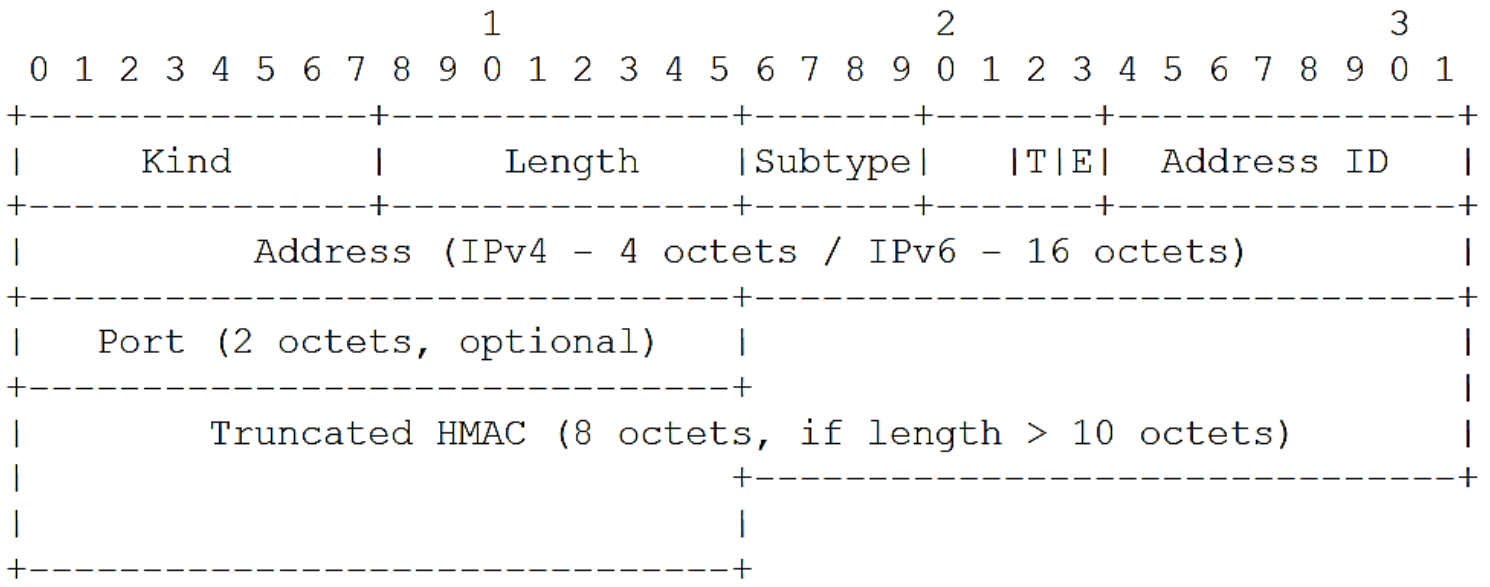
# Extension

- **WHAT?**
  1. We define that an IP address is trusted if it's protected by SAVI or SAVA.
  2. Only if source IP and destination IP are both trusted, the sublow is trusted.
  3. MPTCP control packets are sent preferentially through trusted subflows.
  4. If there is no trusted subflow, MPTCP performs as usual.

# Extension

- **HOW?**
  1. **Trusted Address notification**: Extend **ADD_ADDR option** to carry trusted address passively.
  2. **Trusted Connection notification**: To make sure that both parties of the communication know if the subflow is trusted, propose **ADDR_TRUST option** to notify the trusted address proactively.
  3. Propose **Trusted Path Binding Table (TPBT)** to maintain trusted subflow state.

# Trusted Address notification




Add Address (ADD_ADDR) Option with HMAC

- Flag T (Trust): the flag indicates whether the address is trusted.
- Flag E (Echo): set to 1 in the response.
- Truncated HMAC: 8 octets HMAC of <address, Trust Flag>.

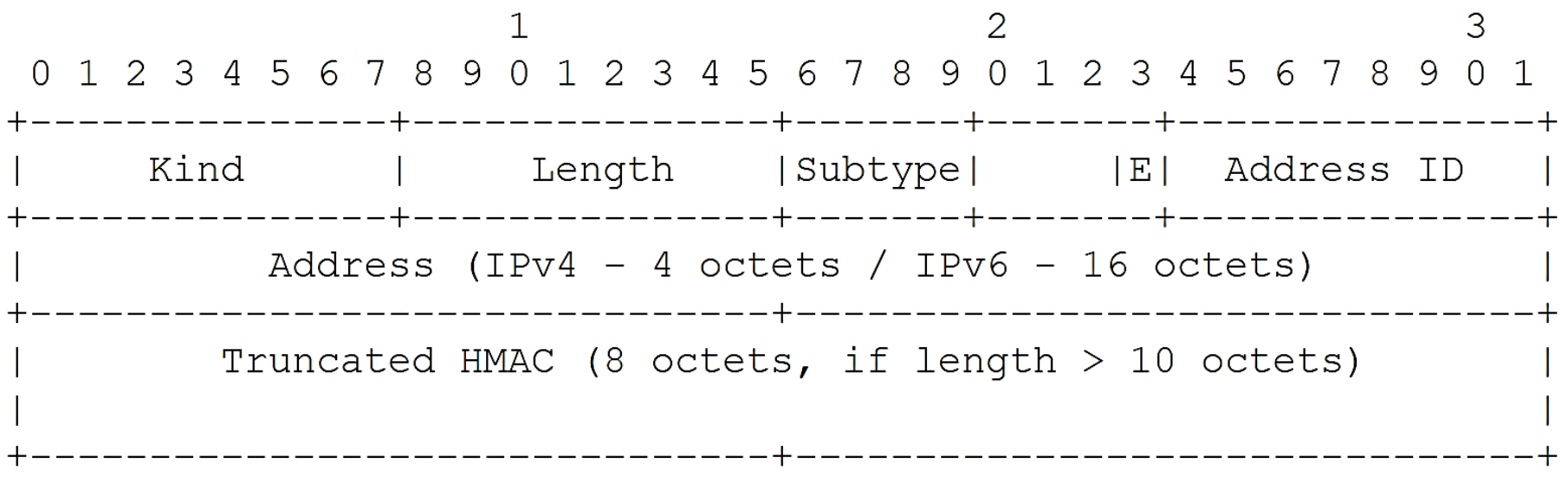
# Trusted Address notification

```
Host A                                          Host B
------                                          ------
ADD_ADDR                  ->
[Echo-flag=0,
 IP-A2,
 IP-A2's Address ID,
 Trust-flag,
 HMAC of IP-A2 and TRUST FLAG]

                          <-                    ADD_ADDR
                                                [Echo-flag=1,
                                                 IP-A2,
                                                 IP-A2's Address ID,
                                                 Trust-flag]
```

ADD_ADDR option Interaction

# Trusted Connection notification




Address Trust (ADDR_TRUST) Option with HMAC

- Flag E(Echo): set to 1 in the response.
- Address: the trusted address.
- Truncated HMAC:  8 octets HMAC of the trusted address.

# Trusted Connection notification

```
Host A                                          Host B
------                                          ------
ADDR_TRUST                  ->
[Echo-flag=0,
 IP-A,
 IP-A's Address ID,
 HMAC of IP-A]

                            <-                  ADDR_TRUST
                                                [Echo-flag=1,
                                                 IP-B,
                                                 IP-B's Address ID,
                                                 HMAC of IP-A and IP-B]
```

ADDR_TRUST option Interaction

# Trusted Path Binding Table (TPBT)

| SubFlow | SipTrust | DipTrust | Lifetime | Other |
|---|---|---|---|---|
| Sf(Sip1,Dip1) | True | True | 65535 | / |
| Sf(Sip1,Dip2) | True | False | 10000 | / |
| Sf(Sip2,Dip1) | False | True | 10000 | / |
| Sf(Sip2,Dip2) | False | False | 0 | / |

Table 1: An Example of TPBT

- SubFlow: a specific subflow consists of a source address, a destination address.
- SipTrust: whether the source address is trusted.
- DipTrust: whether the destination address is trusted.
- LifeTime: the lifetime of this entry in TPBT.
- Other: reserved field for future use.

# THANKS

# Comments & Questions

lihewu@cernet.edu.cn
qi-zhang19@mails.tsinghua.edu.cn

Trusted MPTCP extension
draft-hewu-mptcp-trust-00

Hewu Li, Qian Wu, Boyang Wu, Qi Zhang, Jiang Zhou, Jun Liu
Tsinghua University, China



MPTCP WG - IETF 106
Singapore, 2019.11.19

# BACKUP

# A framework of trusted MPTCP

- Trusted Address Notify (taNotify)
- Trusted Path Mark (tpMark)
- Trusted Path Choose (tpChoose).

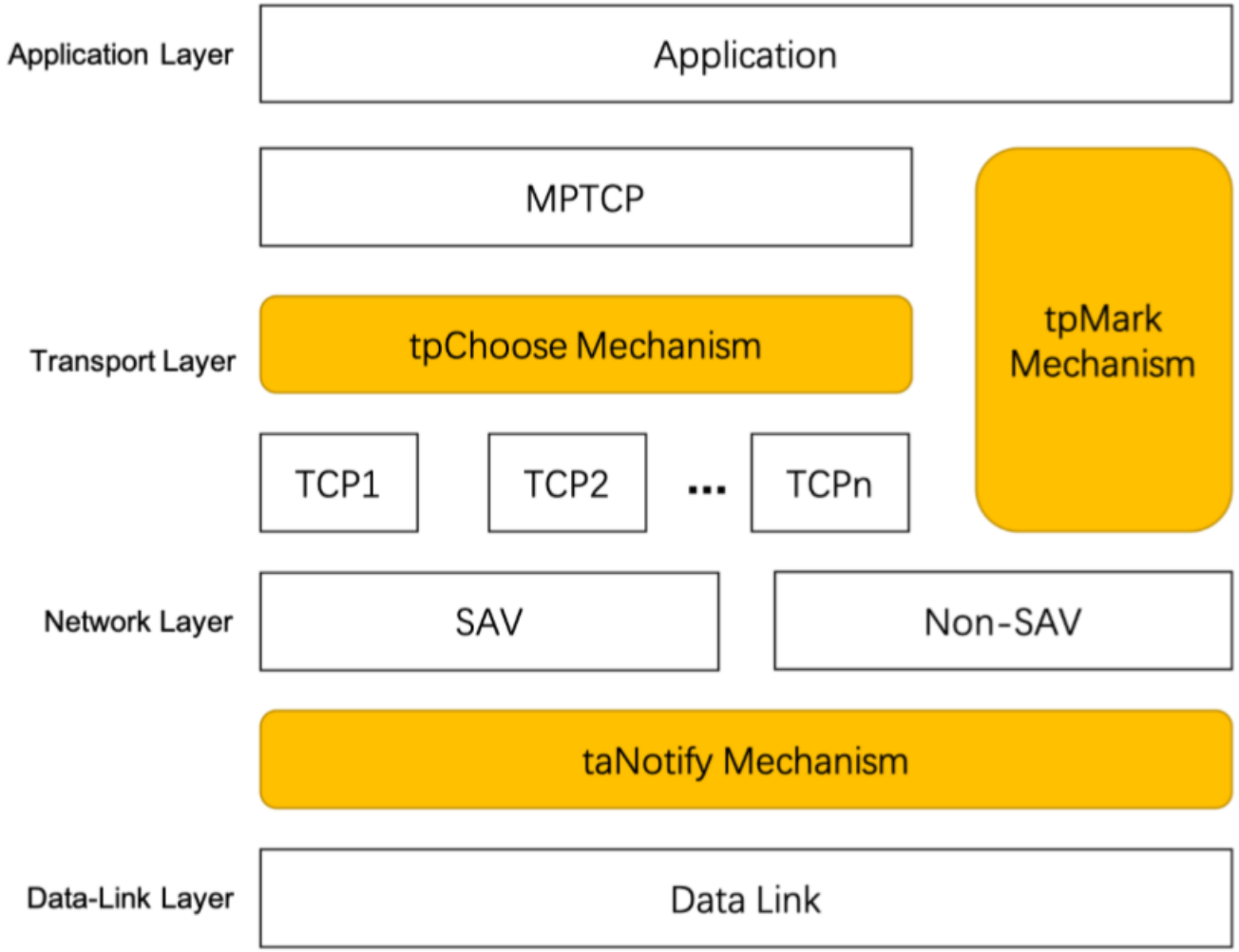



Fig. 1. TMPTCP Framework: three extended mechanisms on the network protocol stack

# A simple system to evaluate

This experiment simulates the scenario where a smart device (actually we use a linux computer to simulate it) is connected to multiple servers at the same time, and designs two paths of wired and wireless, one is trusted and the other is not.

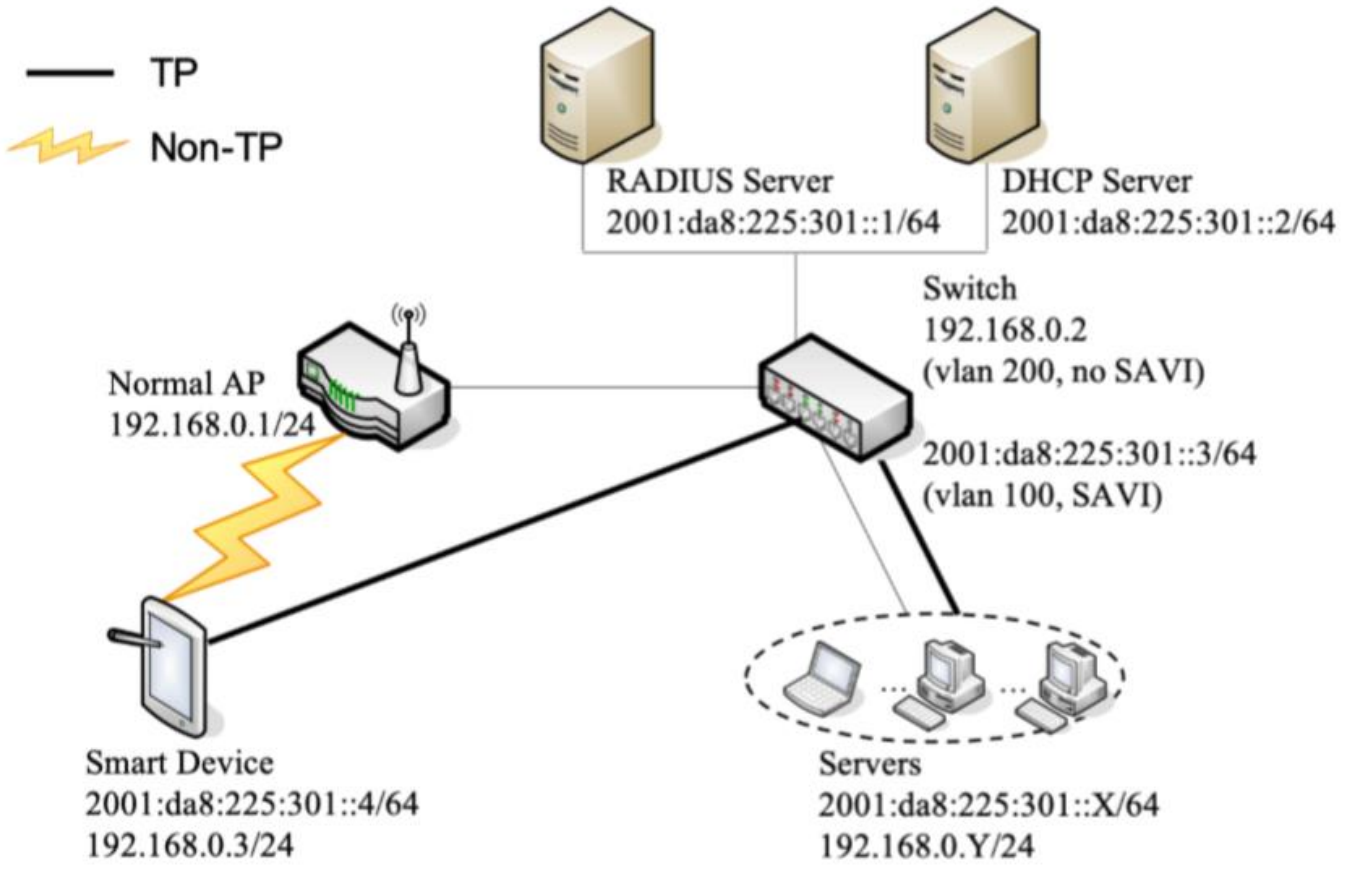



Fig. 5. Evaluation Experiment: A Simple System with Two Paths

# CPU Usage Comparison between Plain MPTCP and Trusted MPTCP

As the packet rate grows, the gap between plain MPTCP and Trusted MPTCP become larger and larger.

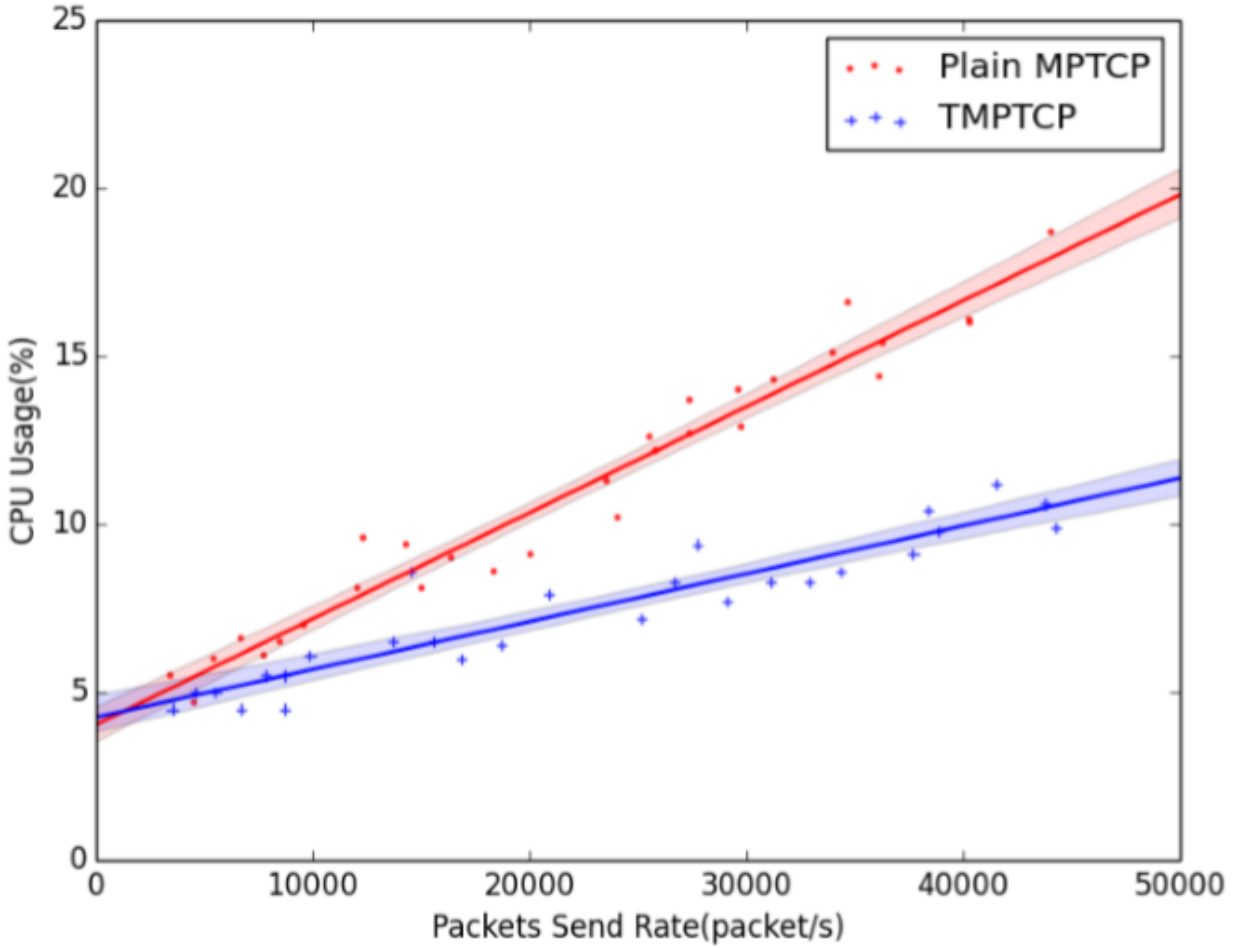



Fig. 6. CPU Usage Comparison between Plain MPTCP and TMPTCP