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

MPTCP WG - IETF 106
Singapore, 2019.11.19

Motivation

- **Trust in Internet 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) adds the capability of using multiple paths to a regular TCP session.
- **Extend MPTCP to work with SAV** and thus improve the accountability of MPTCP connections.

Extension

- **WHY?**
  - **to enable MPTCP to work with SAV, thus improve the accountability of MPTCP connections.**
  - **With the accountability of connections, security is also improved.**
    - The main threats of MPTCP are described in [RFC6181], [RFC7430] and they are mainly caused by **forged control packets sent by malicious hosts with forged IP addresses.**
    - **Send ALL control packets via the trusted path** in a MPTCP connection and other security-oriented operations are OPTIONAL.

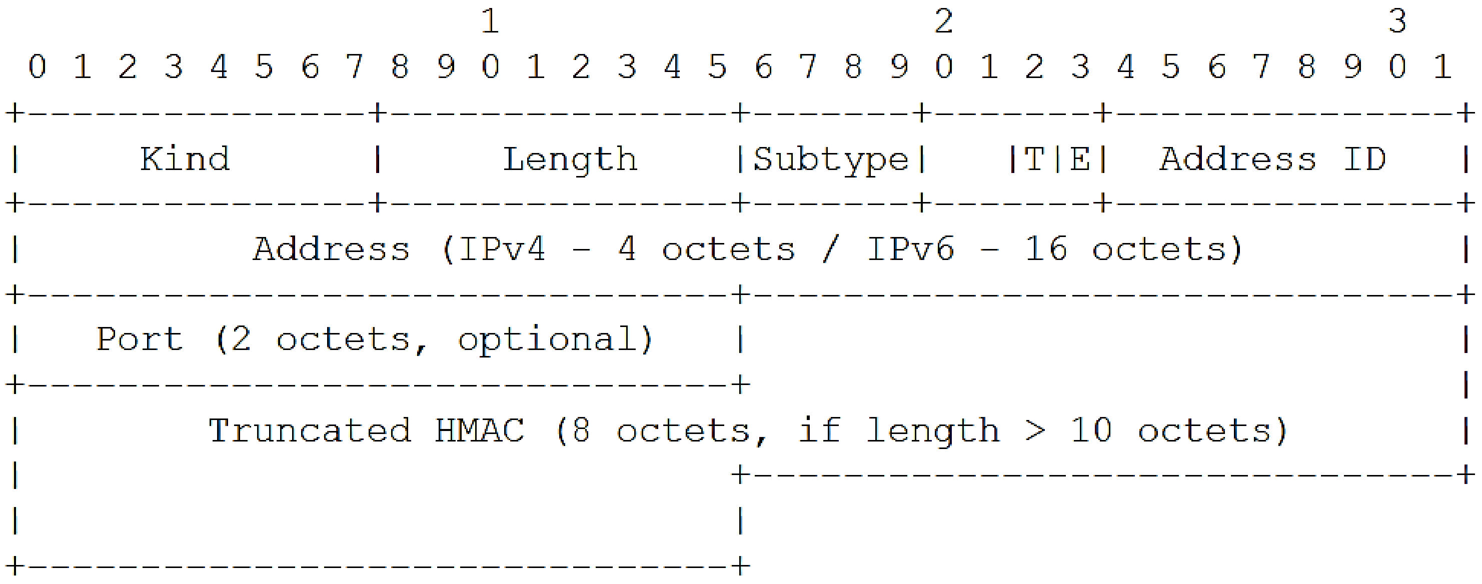
Extension

- **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

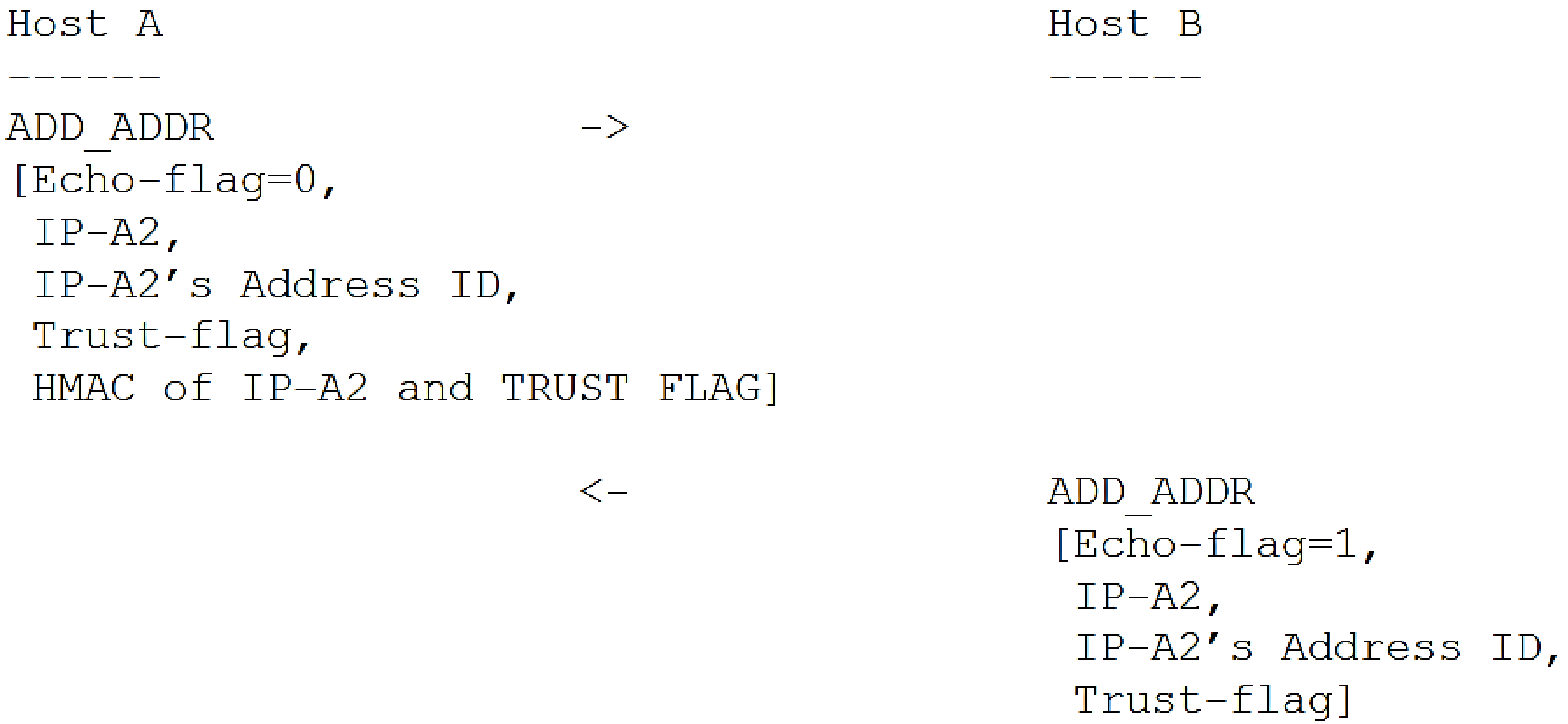


```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---------------+---------------+-------+-------+---------------+
|     Kind      |     Length    |Subtype|   |T|E|  Address ID   |
+---------------+---------------+-------+-------+---------------+
|          Address (IPv4 - 4 octets / IPv6 - 16 octets)         |
+-------------------------------+-------------------------------+
|   Port (2 octets, optional)   |                               |
+-------------------------------+                               |
|        Truncated HMAC (8 octets, if length > 10 octets)       |
|                               +-------------------------------+
|                               |
+-------------------------------+
```

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

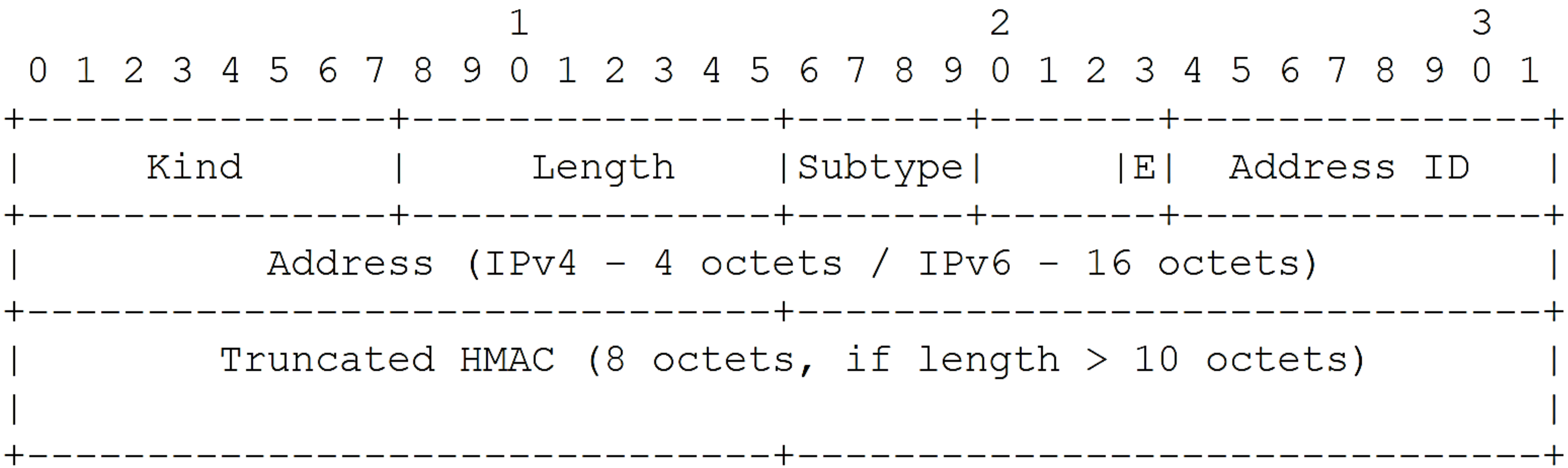


```
Host A                                     Host B
------                                     ------
ADD_ADDR               ->
[Echo-flag=0,
 IP-A2,
 IP-A2's Address ID,
 Trust-flag,
 HMAC of IP-A2 and TRUST FLAG]

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

ADD_ADDR option Interaction

Trusted Connection notification

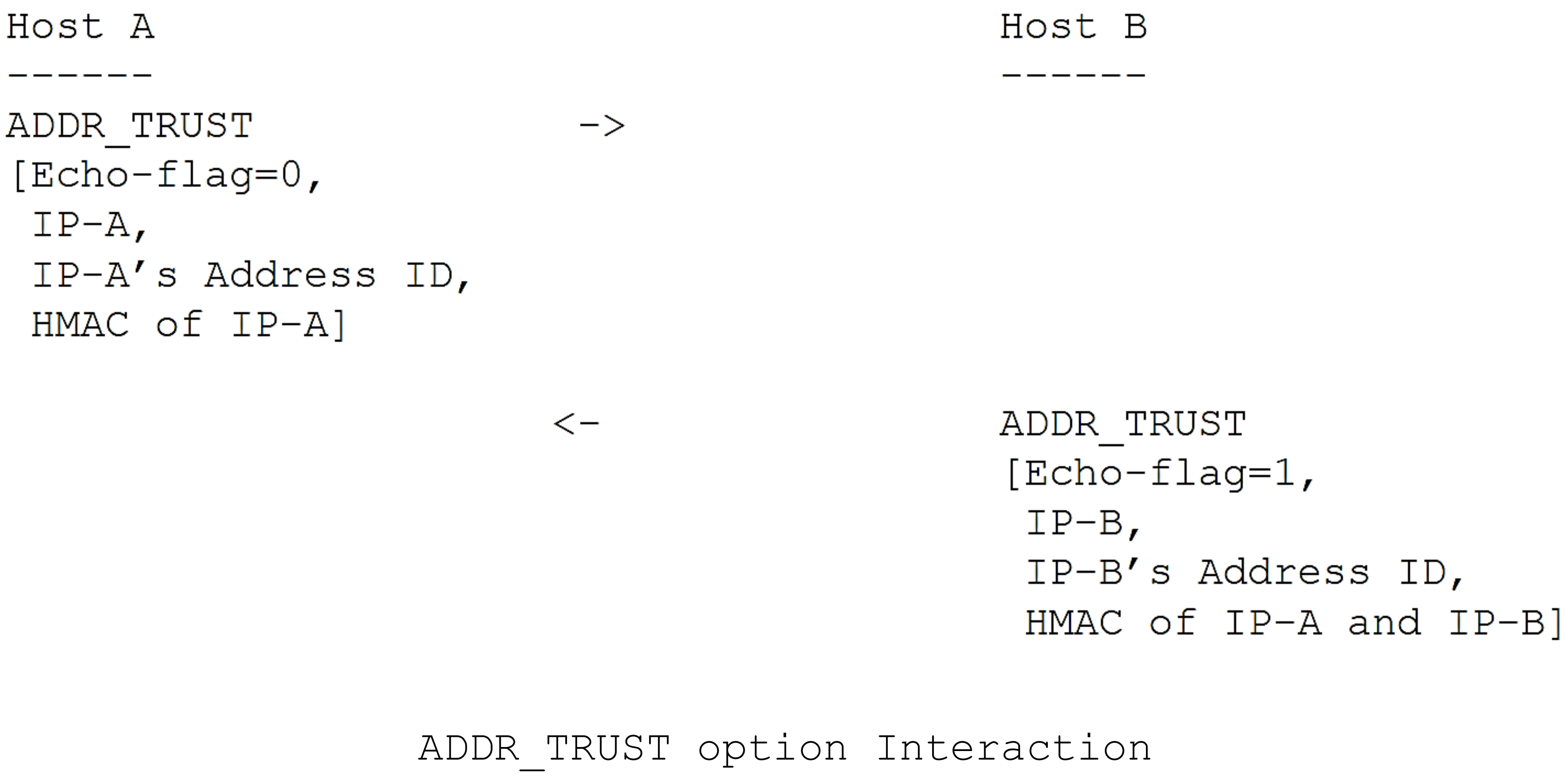


```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---------------+---------------+-------+-------+---------------+
|     Kind      |     Length    |Subtype|     |E|  Address ID   |
+---------------+---------------+-------+-------+---------------+
|          Address (IPv4 - 4 octets / IPv6 - 16 octets)         |
+-------------------------------+-------------------------------+
|        Truncated HMAC (8 octets, if length > 10 octets)       |
|                                                               |
+-------------------------------+-------------------------------+
```

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

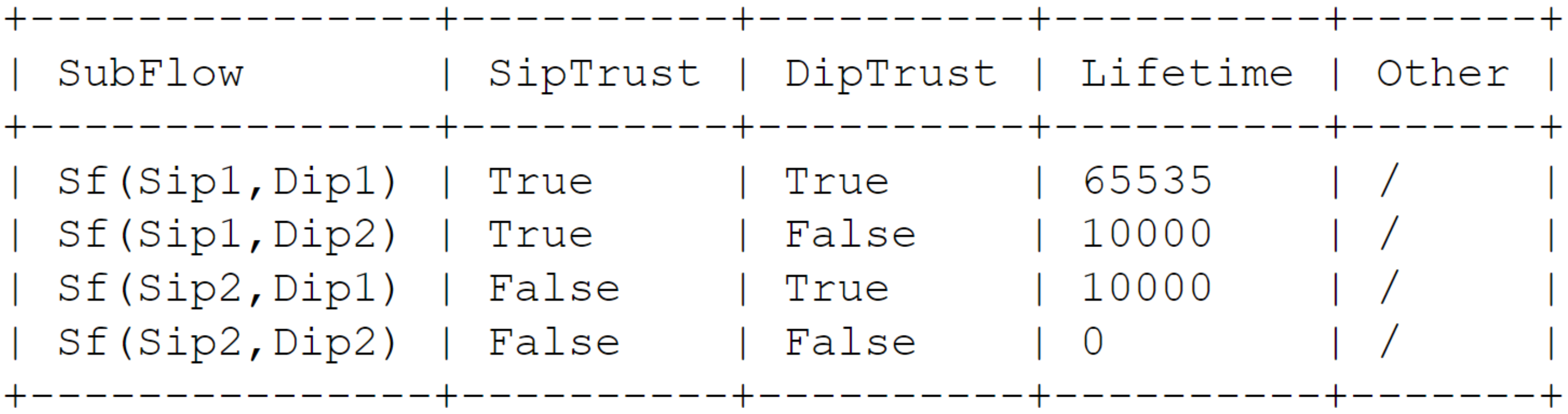


```
Host A                                  Host B
------                                  ------
ADDR_TRUST             ->
[Echo-flag=0,
 IP-A,
 IP-A’s Address ID,
 HMAC of IP-A]

                      <-                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