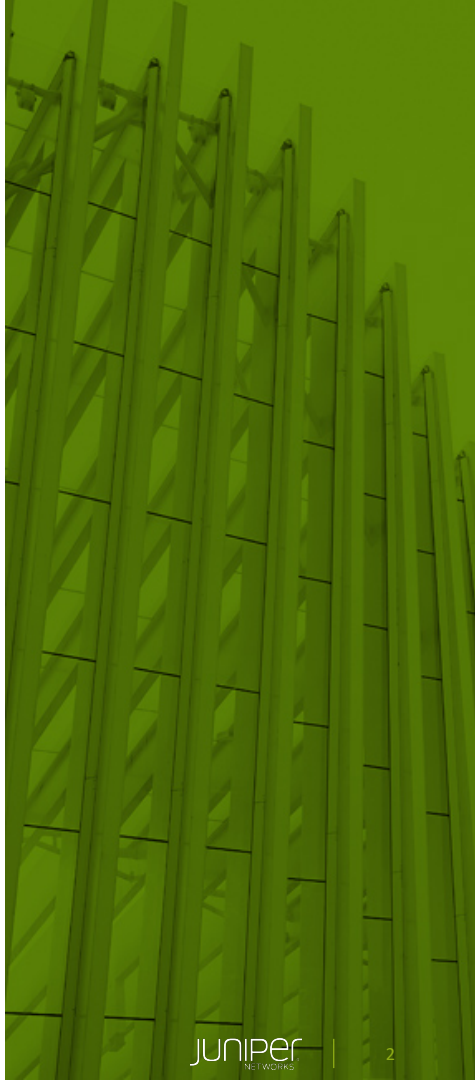
VETTING THE OPTION TO SECURE TIME INFORMATION

IEEE 1588

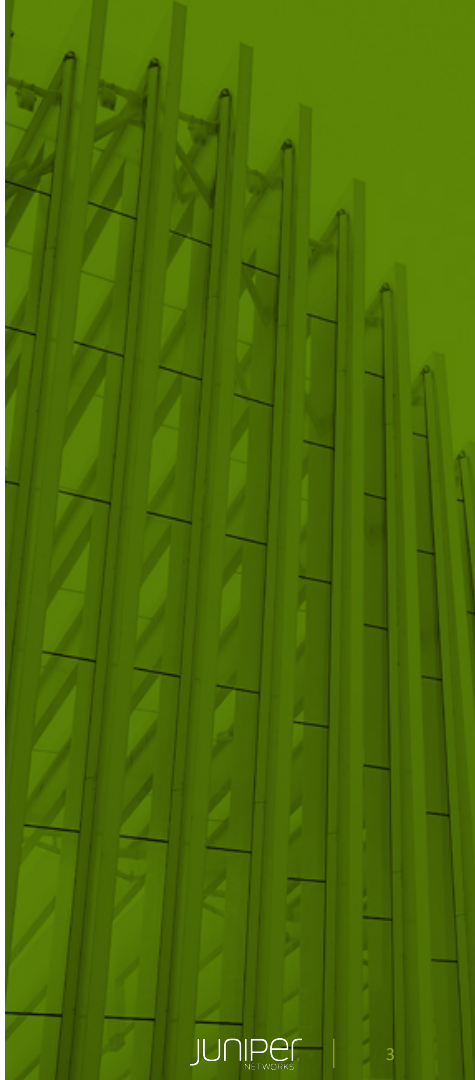
ggrammel@juniper.net

AGENDA

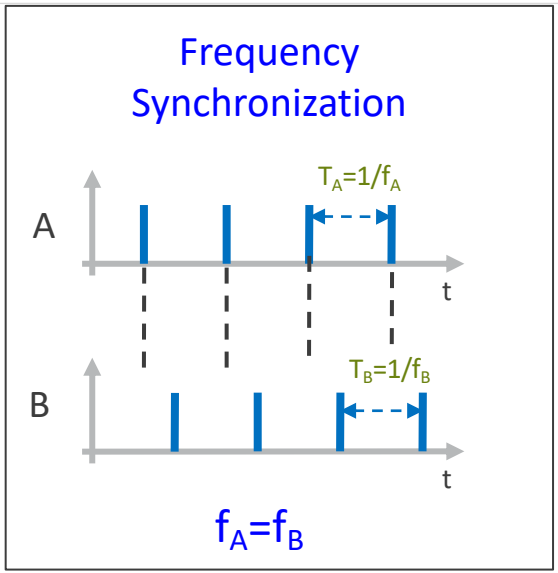
- Introduction in Precision Time Protocol
- Attacking PTP
- Implementing PTP
- Summary



INTRODUCTION

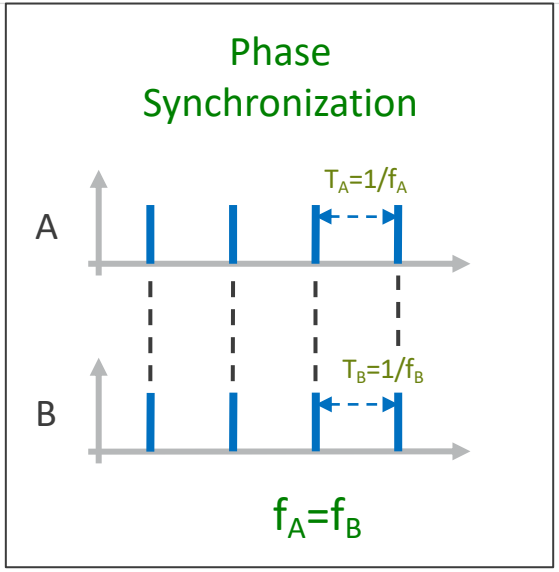


SYNCHRONIZATION OVERVIEW



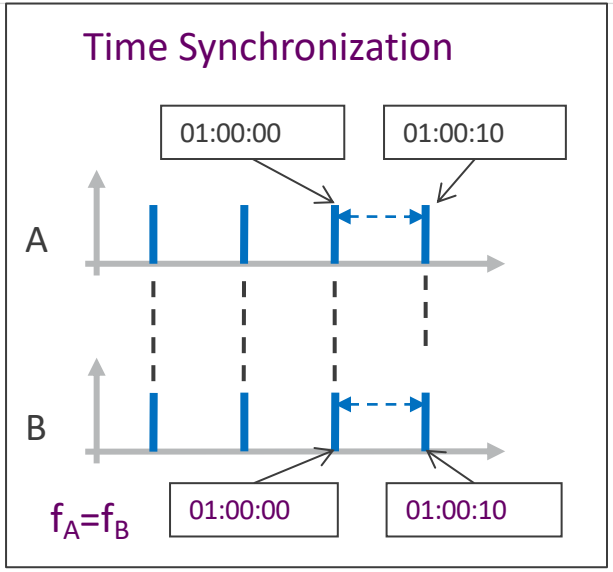
Aligning clocks with respect to *frequency*

FDD application



Aligning clocks with respect to *phase*

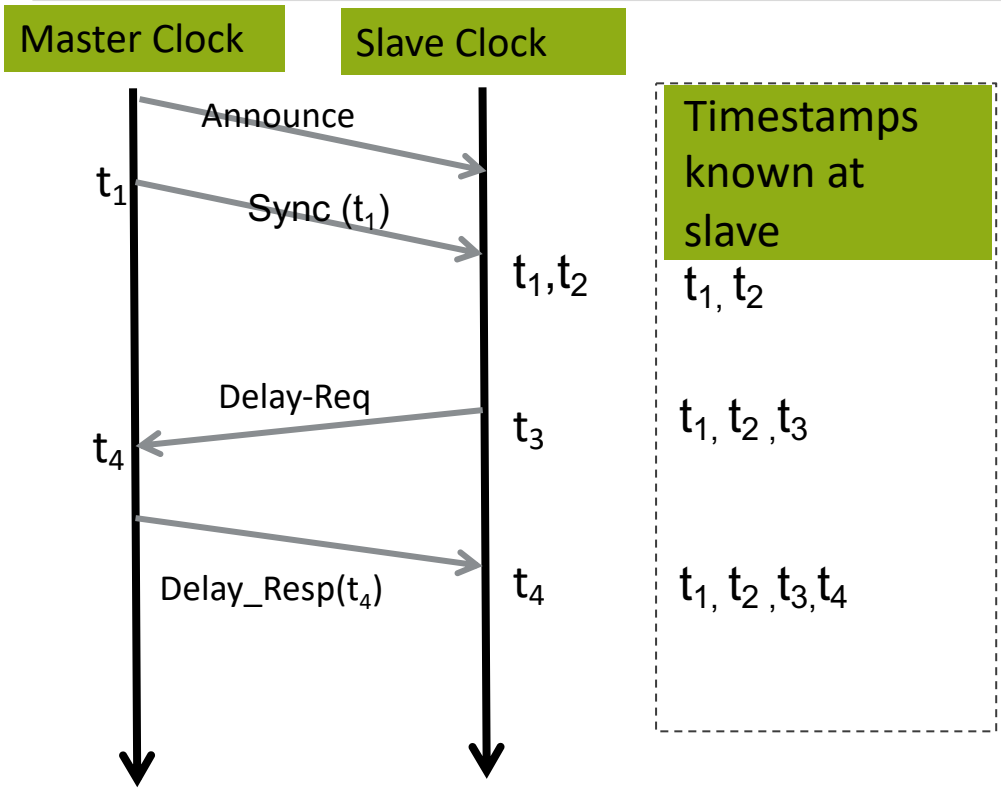
TDD application



Aligning clocks with respect to *time.*

FSI application

IEEE 1588
PTP PROTOCOL AND TIME SYNCHRONIZATION



Timestamps known at slave

t_1, t_2

t_1, t_2, t_3

t_1, t_2, t_3, t_4

$$\text{Offset} = [(t2 - t1) - (t4 - t3)] \div 2$$

PTP Accuracy depends:

- Packet Delay Variation
- Data path asymmetry
- Time-stamping accuracy
- Oscillator stability

PHASE (TDD) AND FREQUENCY (FDD) SYNC

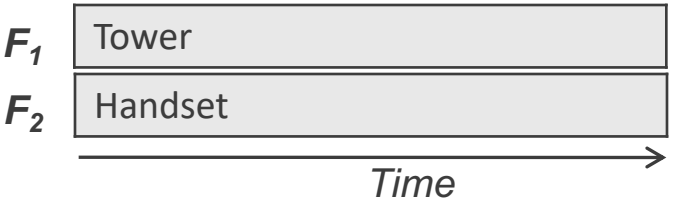
Frequency Division Duplex

Cell tower

Send to handset at frequency F_1

Handset

Send to tower at frequency F_2



Requires: accurate frequency

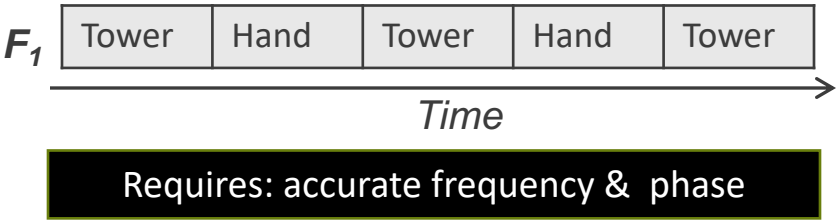
Time Division Duplex

Cell tower

Time: 12:00.01
Send to handset at frequency F_1

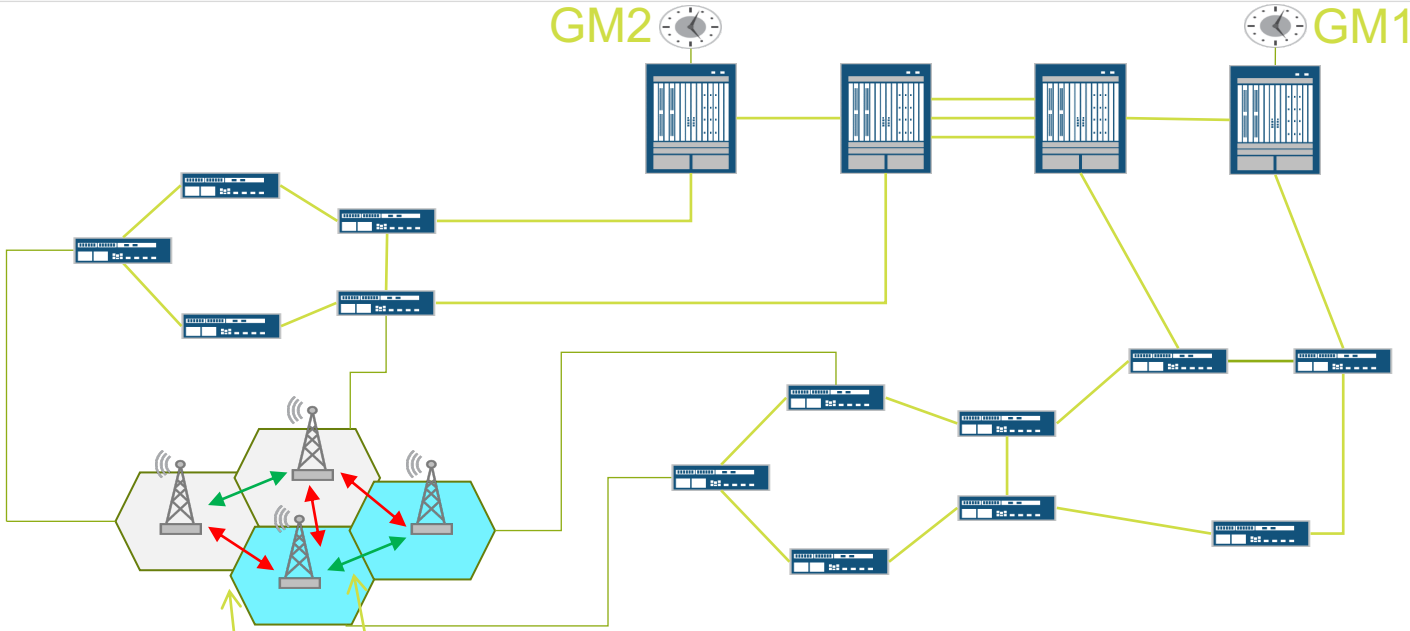
Handset

Time: 12:00.05
Send to tower at frequency F_1

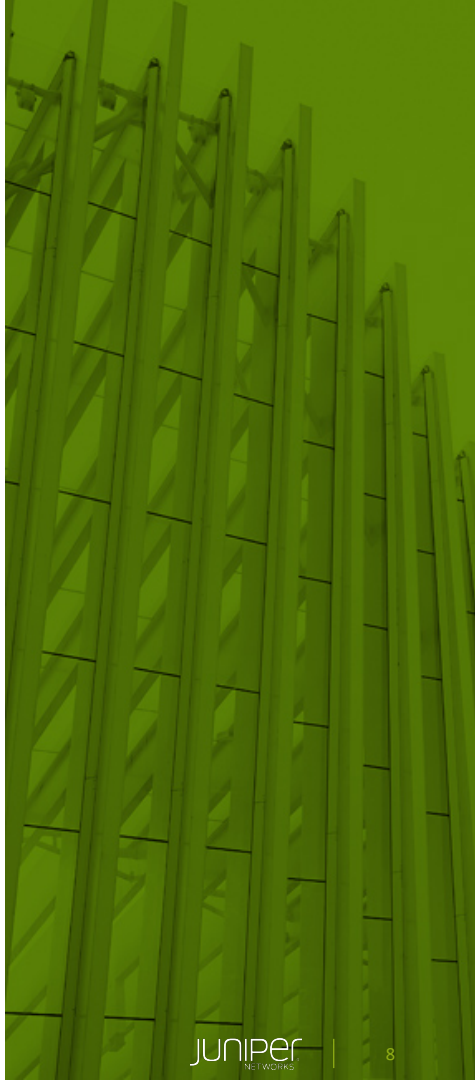


Requires: accurate frequency & phase

5G NETWORK EXAMPLE



IMPLEMENTING PTP



ATTACKING PTP

Source:

A Security Analysis and Revised Security Extension for the Precision Time Protocol

Eyal Itkin and Avishai Wool:
eyalitki@post.tau.ac.il, yash@eng.tau.ac.il

Tel Aviv University, Israel, May 28, 2016

- **Attackers:**
  - Out-of-Band Applicative adversary
  - Out-of-Band Network adversary
  - In-Band adversary
  - Hostile PTP Insider clock
  - Hostile PTP Management node
  - Hostile PTP Grandmaster node
- **Attack vector samples**
  - Forge DELAY_RESPONSE messages on behalf of the grandmaster, thus damaging the delay measurements of the target node.
  - Send spoofed SYNC messages with hostile timestamps on behalf of the grandmaster, to a chosen target node. The targeted node will recalibrate itself according to the specified attacker's time values.
  - The blind window snatching attack makes use of the PTP window behavior. At some point the attacker's packet will hit the legitimate window - so all subsequent legitimate packets fall outside the new window and are discarded.
  - An OOB applicative adversary, can propose himself as a grandmaster candidate by sending fake ANNOUNCE messages declaring him to be the best clock in the network. This can easily be done by faking to be a truly magnificent clock.
  - OOB Applicative adversary, can send fake management messages to upgrade a specified PTP node's dataset. As a result of its dataset improvement, the targeted node will win the BMC leader election and will be declared the network's grandmaster. After being elected, the adversary will send SET_TIME messages to directly control the target's time, thus taking full control of the time and structure of the whole PTP network.

GOOFED TIME: WHAT ARE THE SYMPTOMS?

- Automated events simply don’t occur or else they break. This happens because a trigger set to go off at a certain time can not be executed in the proper sequence.
- Loss of data because system software saves an out-of-date version of a data-item instead of the latest version.
- Security Holes occur because administrators cannot retrace activities since log files are inaccurate and effects (usally later in time) can no more traced back to a root cause (usually earlier in time).

ATTACK VECTORS

Attack	Attacker Type											
	Internal MITM			internal Injector			External MITM			External Injector		
	MACsec	Ipsec	1588 Annex K	MACsec	Ipsec	1588 Annex K	MACsec	Ipsec	1588 Annex K	MACsec	Ipsec	1588 Annex K
Interception and modification	✓	✓	✓									
Spoofing	✓	✓	✓		✓							
Replay	✓	✓	✓	✓	✓	✓						
Rogue master	✓	✓	✓	✓	✓	✓	✓	✓	✓			
Interception and removal	✓	✓	✓				✓	✓	✓			
Delay manipulation	✓	✓	✓					✓	✓		✓	✓
L2/L3 DoS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cryptographic performance	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Time source spoofing	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

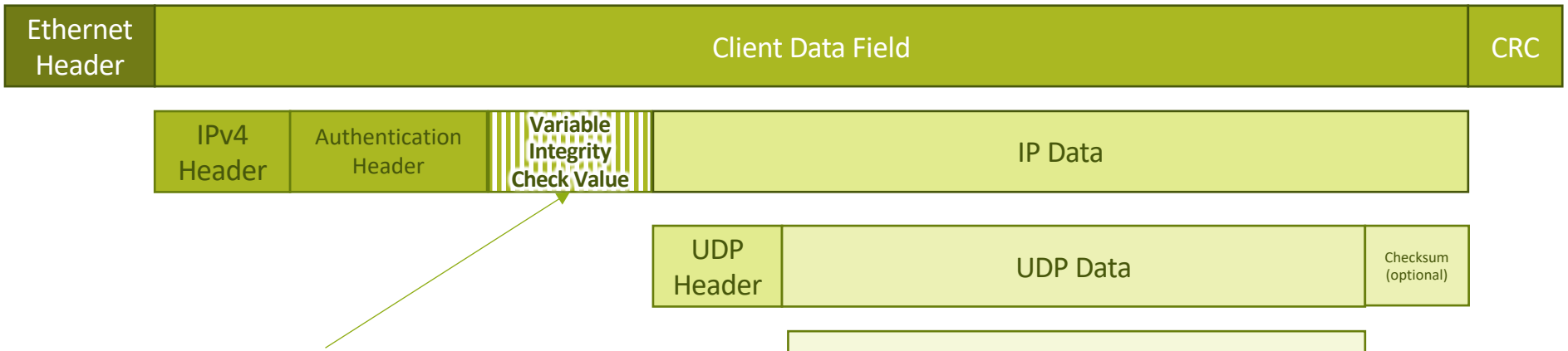
Source: **Time synchronization security using IPsec and MACsec**
Tal Mizrahi, Huawei Network.IO Innovation Lab

IPV4 OVER ETHERNET MESSAGE FORMAT

Sync Message Format									
Bits								Octets	Offset
7	6	5	4	3	2	1	0		
Header								34	0
origin Timestamp								10	34

CRC protects against packet corruption but does not authenticate.

AUTHENTICATED IPV4 OVER ETHERNET MESSAGE FORMAT



RFC4302: IP Authentication Header

1. Header is in front of PTP message but authenticates all IP Data
2. Variable length integrity check value shifts time stamp affecting accuracy

Sync Message Format									
Bits								Octets	Offset
7	6	5	4	3	2	1	0		
Header								34	0
origin Timestamp								10	34

KEY ISSUE

- To be precise, HW based PTP time stamping is a process excluding queuing.
- HW time stamping attaches the time stamp to the end of a packet and can only perform simple tasks maintaining the precision.
- Using existing Authentication mechanisms for IPv4/IPv6 is too complex to keep the necessary precision

Time Error per node	+/-ns
Class A	50
Class B	20
Class C	10
Class D (under definition)	2-3

Speed of light in fiber: 5ns/m

Source:

Rec. ITU-T G.8273.2/Y.1368.2 (01/2017):

- **T-BC permissible range of constant time error**

SOLUTION OPTIONS

1. Modify **RFC4302** for authentication to accept fixed length integrity check at the end of the packet.
   - Takes time to agree
2. Make Time stamping compatible with encryption (MACsec). Although encrypting time information is not a requirement, the side effect is that encryption protects against spoofing.
   - Works but has to be actively provisioned
3. Modify the PTP to self-authenticate by implementing the experimental Annex K of the IEEE 1588-2008
   - Requires security state machine in PTP handling
   - PTP Implementation needs to be hardened against DOS, malformed packets, …

SUMMARY

1. PTP is hard to protect against attacks
2. Best available option is to use 1588 in combination with MACsec
3. Operators are well advised to enable MACSEC on their devices