ROBUST & RELIABLE DELIVERY OF SYNCHRONIZATION

A SURVEY OF METHODS & TECHNIQUES

NOVEMBER 2014

Anurag Gupta
agupta4u@gmail.com

Apologies

Sorry I could not present in person….

……**So reaching you remotely**.

Introduction

Typical Uses of Time/ Frequency

Communications

Applicable Sectors: Telecom, IT, Emergency Services

- Synchronization of Networks- TOD, Phase, frequency
- Handing over of calls between adjacent communicating entities

SCADA- Supervisory, Control & Data Acquisition

Applicable Sectors: Chemical, Critical Manufacturing, Dams ,Defense Industrial Base, Energy, Nuclear Reactors.

- Providing common time base for supervisory, control & alarm events
- Support for event logging

PMU synchronization

Applicable Sectors: Energy, Nuclear (power generation)

Regulatory Compliance, Transactional Forensics

Applicable Sectors: Finance, Banking

- Transaction logging
- Fraud detection & prevention

Targeted Accuracy By Application

This table proposes targets for time/ frequency accuracy by applications

CIS/ Application	End application accuracy target	Internal Clock accuracy (lines in the sand ☺)
Telecom (aggregation)	500ns to 1.5uS	~50 nS
Telecom (leaf nodes)	> 1 uS	~50 nS
Energy / Power PMU	1uS to 10uS	50nS
Multiple / fault logging	10uS to 5mS	100 -500 nS
Multiple / SCADA	<1ms to 100mS	100 -500 nS
HTF/ Latency Measurements	500uS to 10mS	100 -500 nS
Finance/ Transactional TS	10 to 100mS	100 -500 nS

Making the GNSS reception systems robust.

1. Anti jamming techniques/ Making systems resistant to jamming.
2. Anti spoofing – detect and isolate spoofed system.

Backing up GNSS with Alternate synchronization methods

1. Microwave links (physical layer methods)
2. Physical layer Frequency & time transfer (e.g. White Rabbit; DTI)
3. Assisted holdover methods.

Mitigation-Using Ensemble of / multiple clock sources

1. Inputs from multiple clocks are “averaged” and stable output delivered.
2. Majority voting techniques

Techniques

Making the GNSS reception systems robust.

1. Anti jamming techniques/ Making systems resistant to jamming

2. Anti spoofing – detect and isolate spoofed system.

(I will not talk about these here- A summary of these techniques is included in the backup slides as a reference)

Techniques (Cont.)

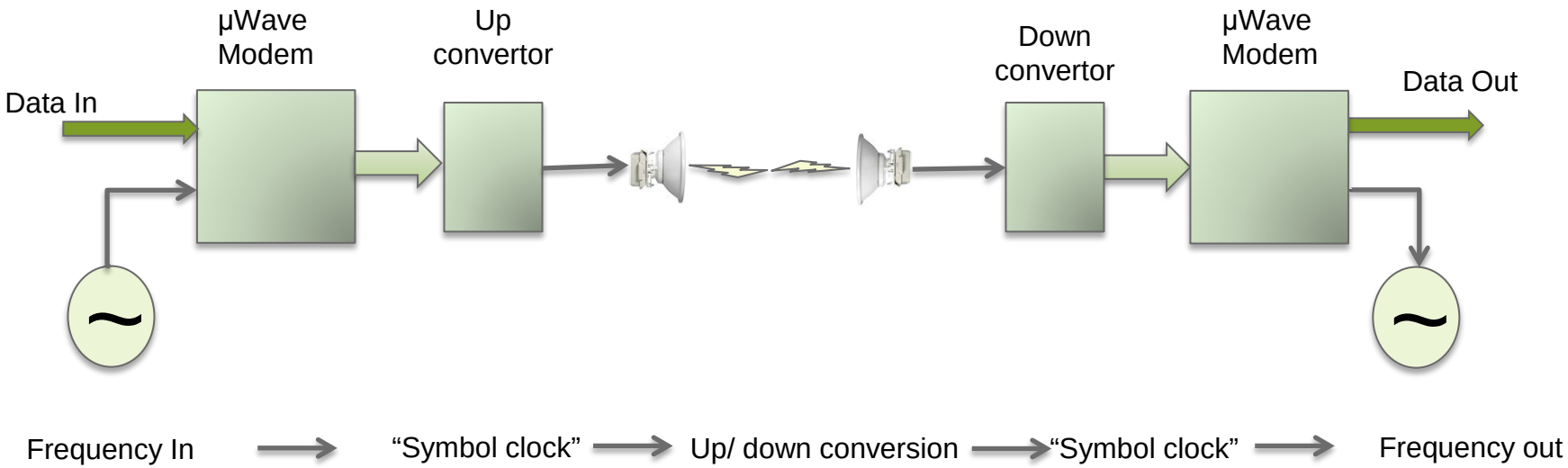
Backing up GPS with Alternate synchronization methods

1. Microwave links (physical layer methods)
2. Physical layer Frequency & time transfer (e.g. White Rabbit; DTI)
3. Assisted holdover methods.

Generally speaking the accuracy of the GNSS based systems is between 30 to 100nS. The underlying premise in using the backup techniques is- if we are able to transfer the time signal, while limiting the introduced error to a comparable value-

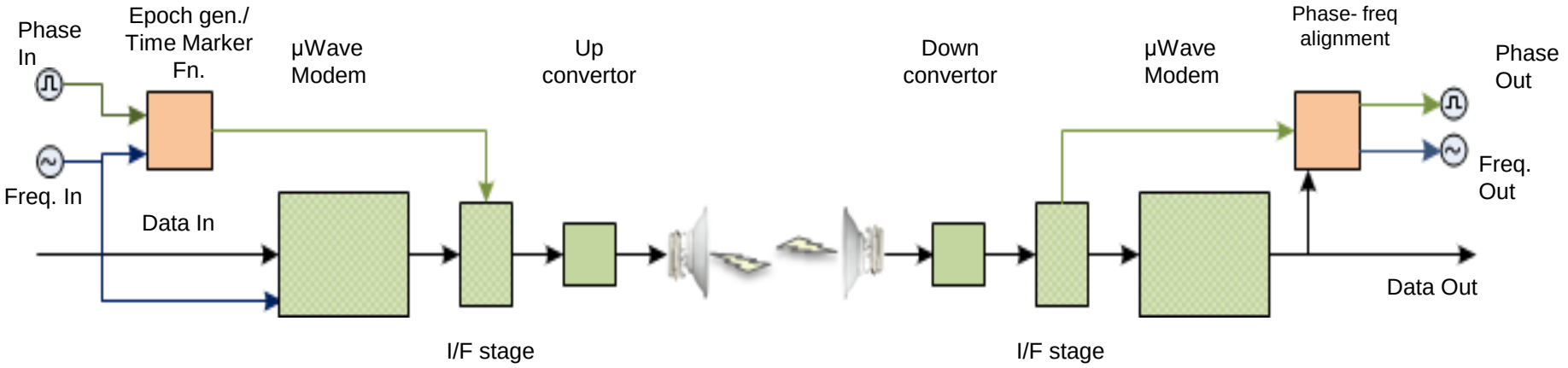
Then it is possible to backup the “local time signal” with a “remote” signal.

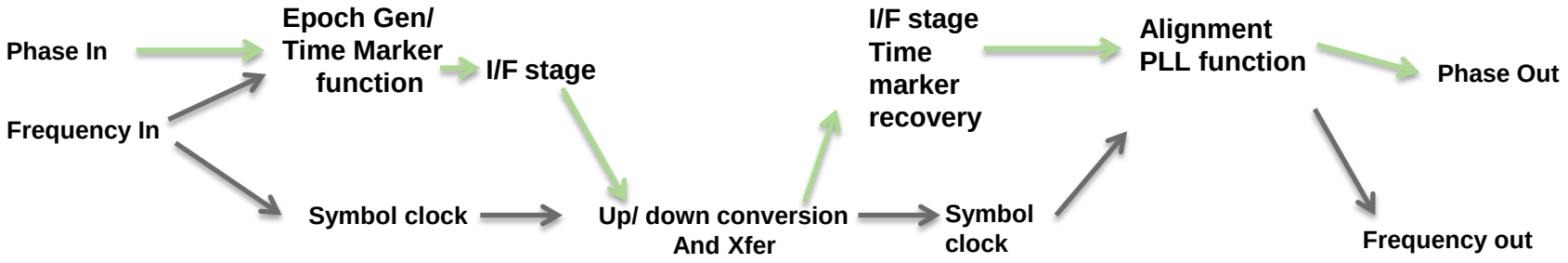
Step 1- Transferring frequency



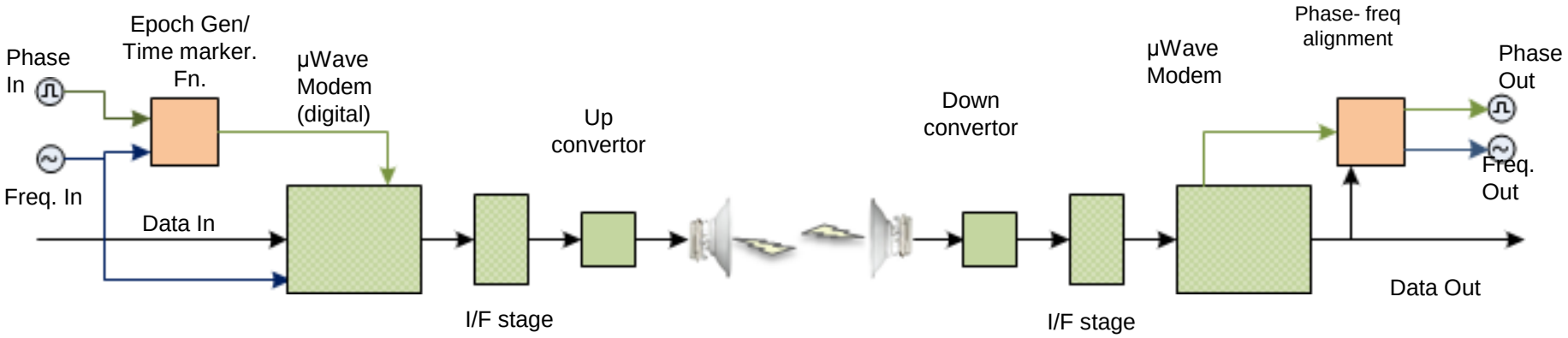
- The Frequency Out is physically traceable to Frequency In
  - F_{in} is used to generate the “symbol clock” at the transmit end.
  - Symbol clock is recovered by the modem at the receive end
  - F_{out} is regenerated from the symbol clock
- This scenario is reminiscent of the Sync-E operation

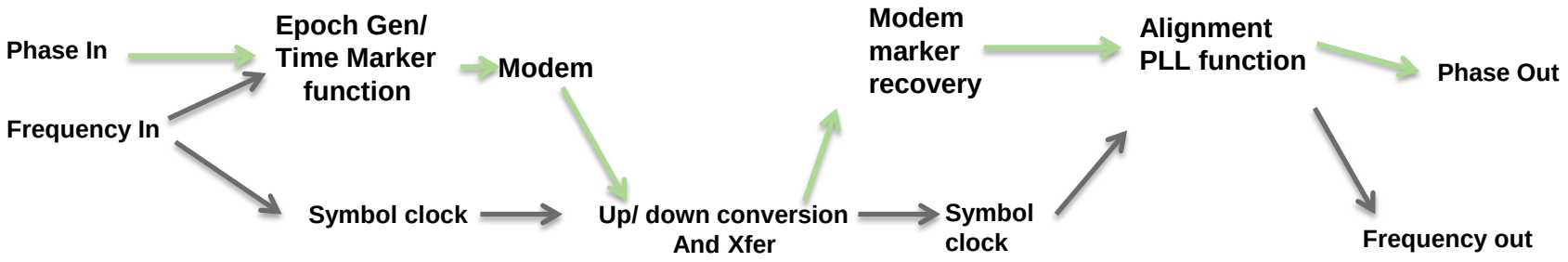
Step 2 option 1- Transferring Phase- I/F stage support





Step 2 option 2- Transferring Phase- modem support





Backing up GPS with Alternate synchronization methods

1. Microwave links (physical layer methods)
2. Physical layer Frequency & time transfer (e.g. White Rabbit; DTI)
3. Assisted holdover methods.

IEEE 1588 V3 (?)- High Accuracy Subcommittee

- Is working on techniques to deliver synchronization at sub nS accuracy

Sub nSec accuracies is not needed today. [slide 3]

- Techniques developed could extended to ~10nS accuracies
- This would enable the transport of time signal as a backup.

High Accuracy SC's work (current focus) is

inspired by White Rabbit….

IEEE 1588/ WR

A (over) simplified version of WR would be

Step 1- Syntonization phase- getting the two end points referenced to the common frequency [using sync-e]

Step 2- Calibration phase- (link characterization)

a. The frequency signal is looped back and the phase difference between outgoing and looped back signal measured.

b. The “invariant” and “variant” components of delay/ asymmetry are communicated between the end points and compensated.

- Invariant delays- propagation delays of optical components, PCB traces etc.
- Variant delays (same between power cycles) – delays through phys/ serdes

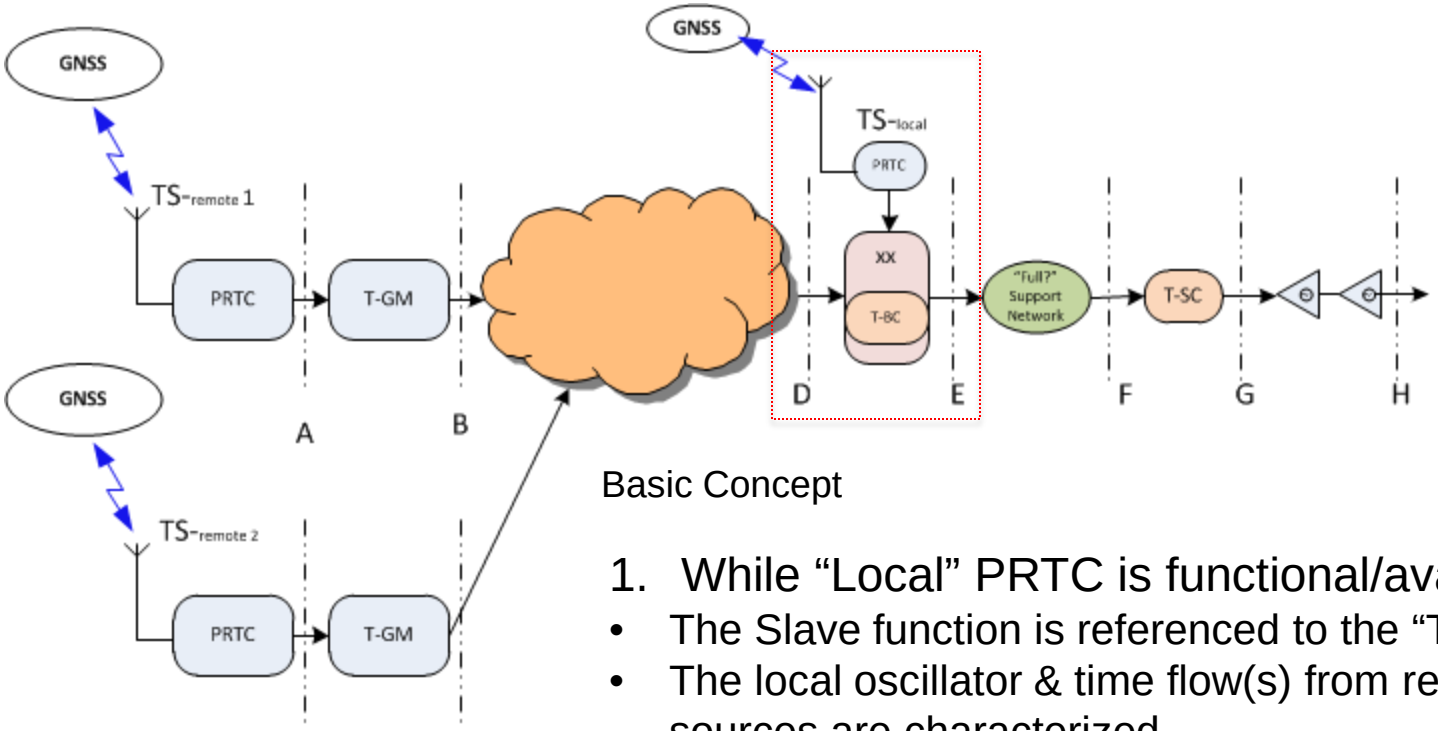
Step 3- exchange of “enhanced” time stamps, compensation and recovery of precise time signals

Take away- For (non-metrology) applications if sources of uncertainty could be bounded by design &/ or configuration then these methods are candidates for transport of time.

Techniques

Backing up GPS with Alternate synchronization methods

1. Microwave links (physical layer methods)
2. Physical layer Frequency & time transfer (e.g. White Rabbit; DTI)
3. Assisted holdover methods.



Basic Concept

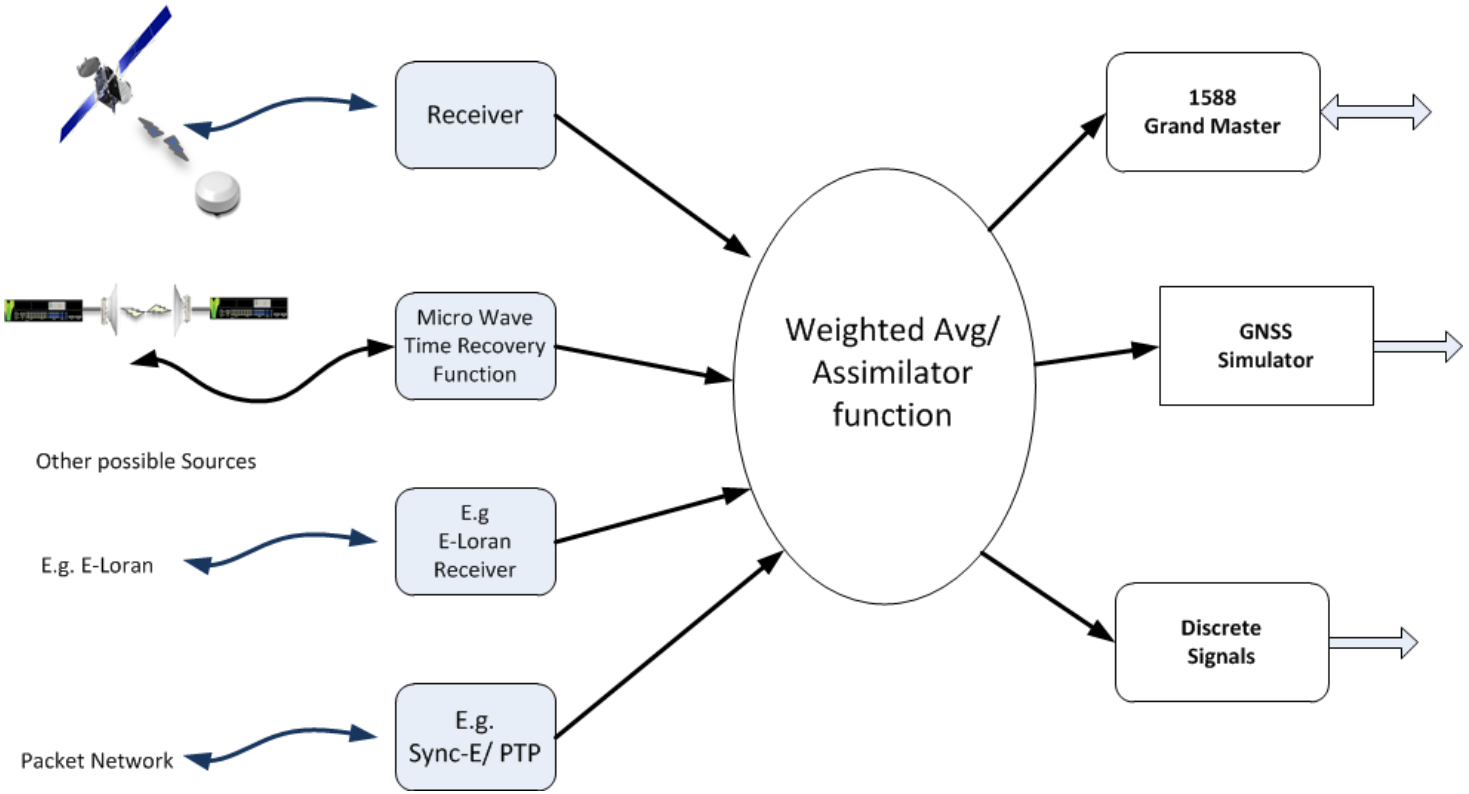
1. While “Local” PRTC is functional/available
   - The Slave function is referenced to the “TS-local
   - The local oscillator & time flow(s) from remote Time sources are characterized

2. When “Local” PRTC is not available

The time flows from remote sources are used to steer the local oscillator and maintain the “holdover” within expected limits

Using Ensemble of / multiple clock sources

1. Inputs from multiple clocks are “averaged” and stable output delivered.
2. Geographic diversity and redundancy.
3. Majority voting techniques

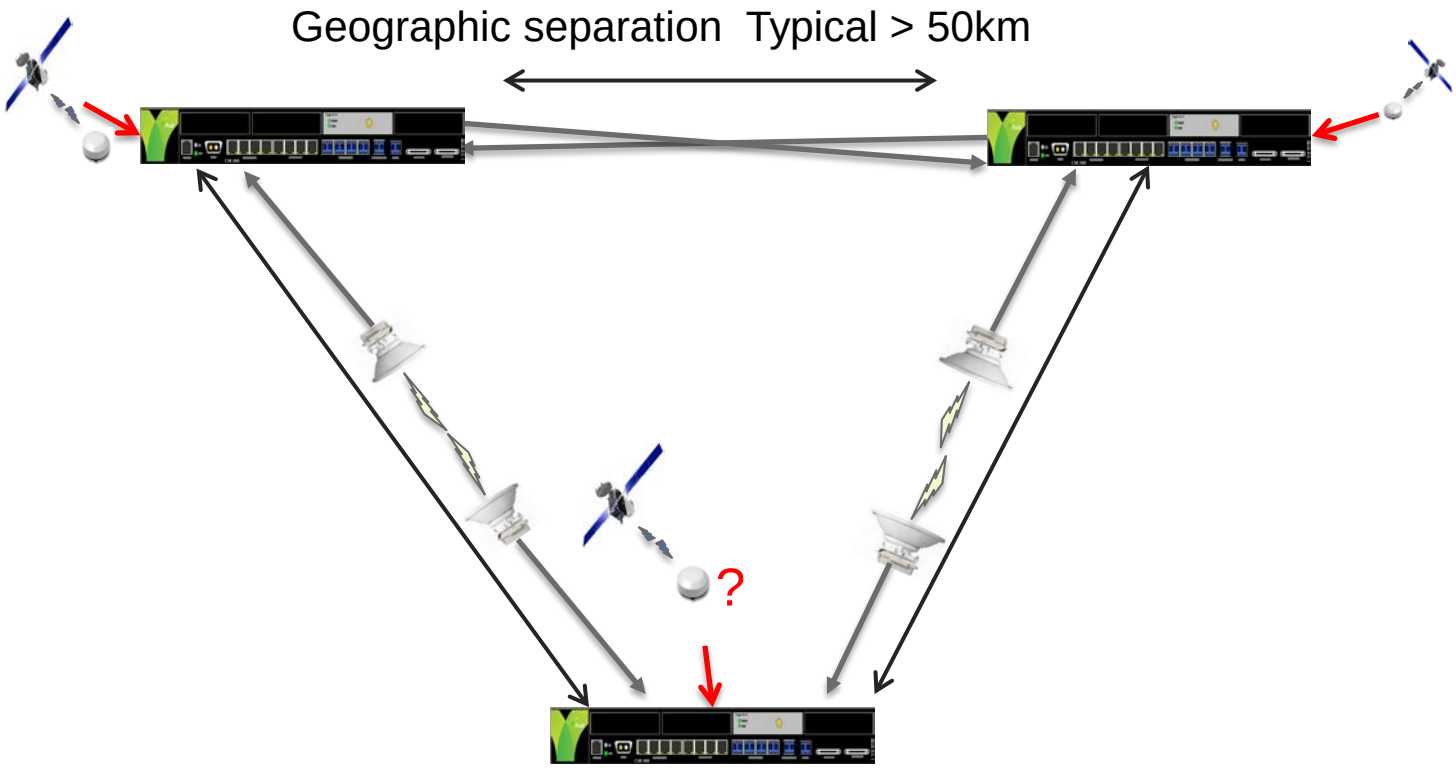


- Weighted Averaging of inputs- to generate stable outputs

Using an ensemble of clocks to generate a stable clock : NTP

Mitigation

Geographic Diversity & Redundancy



- Geographically diverse locations linked over Terrestial links- wired or wireless
- Exchange Time & frequency information
- Characterize links and determine Error bounds
- Majority voting

If GPS is compromised, the system could switch over to the physical layer backup

Closing thoughts …

- We enumerated a few methods for building reliable timing networks
- Each one of the techniques could play an important role

- Depending on the Application : Telecom, Power & utilities, Financial

one or more of the techniques could be applied

……. Enjoy rest of the conference

THANK YOU FOR YOUR ATTENTION……

QUESTIONS?- PLEASE EMAIL THEM

Anurag Gupta
Email: agupta4u@gmail.com

BACKUP SLIDES

GPS Spoofing

Detection Techniques (summary)

Test Statistic	Function	Limitation
Absolute signal power	Limit the spoof signal power	Antenna Attitude and Environment related
Signal power changing rate	Detect stationary spoof station	Antenna Attitude and Environment related
Relative signal strengths on all carriers	Detect spoofing on single carrier	Affected by ionosphere refraction
Range rate	Bound the phase and code range rate	Relate to GPS receiver's moving direction
Doppler shift	Detect spoof that uses one transmitter to spoof all satellites	
Correlation Peaks	Correlate L1/L2 binary message	

Anurag Gupta

GPS Spoofing

Detection Techniques (summary)

Test Statistic	Function	Limitation
GPS signal after removing all navigation data	Recover authentic data	Requires low spoof/authentic signal power ratio
Range differences: phase/code, L1/L2	Identify signal source	Needs to be L1/L2 receiver
Ephemeris data	Verify ephemeris data including satellite position	
Signal power and data	Jump detection	

Countermeasures for GPS signal spoofing: Wen, Huang, Dyer et alia