

Time and Timing in Defence Applications



Mark O'Dare
November 2006

Introduction

A high level introduction to the following topics are presented for consideration.

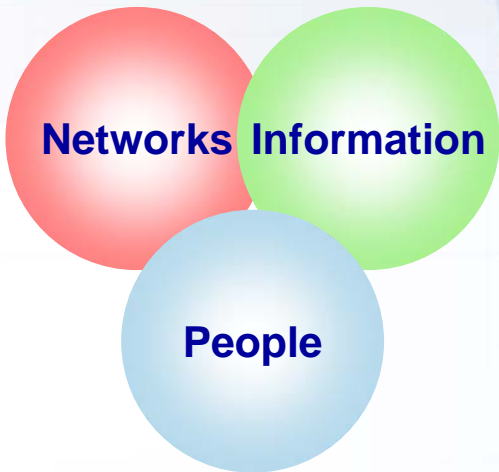
- Current Status of Defence Networks
 - NEC and NCW
 - Example Networks and Associated Technologies
- Radio Considerations
- Cryptographic Considerations
- Networks and Synchronisation

Network Enabled Capability (NEC)

NEC (UK MOD JSP 777)

NEC offers a new way of not just “*doing things better*” but of “*doing better things*”.

How?



Progressive development of defence equipment, software processes and structures. Integration of Sensors, Decision Makers, weapons platforms etc.



Timely Information and intelligence drawn from a broad range of sources to support political and military decision making etc.



Enhanced force protection and reduction of fratricide. Individual and collective training etc.

Network Centric Warfare (NCW)

- NCW is often considered to be the US equivalent to NEC, though there are significant differences.
- Some try to define NCW and others refuse to define NCW.
- NCW may be described (not defined!) as a concept. NCW points to a course to steer to assist the military in transitioning to the information age. (Vice Admiral Arthur K. Cebrowski President, Naval War College).
- NCW considers the network to be the primary driver, while NEC views the network as an enabler only.
- NCW is a planned and structured development of technology roll-out, while NEC is expected to evolve through networking battlefield entities .

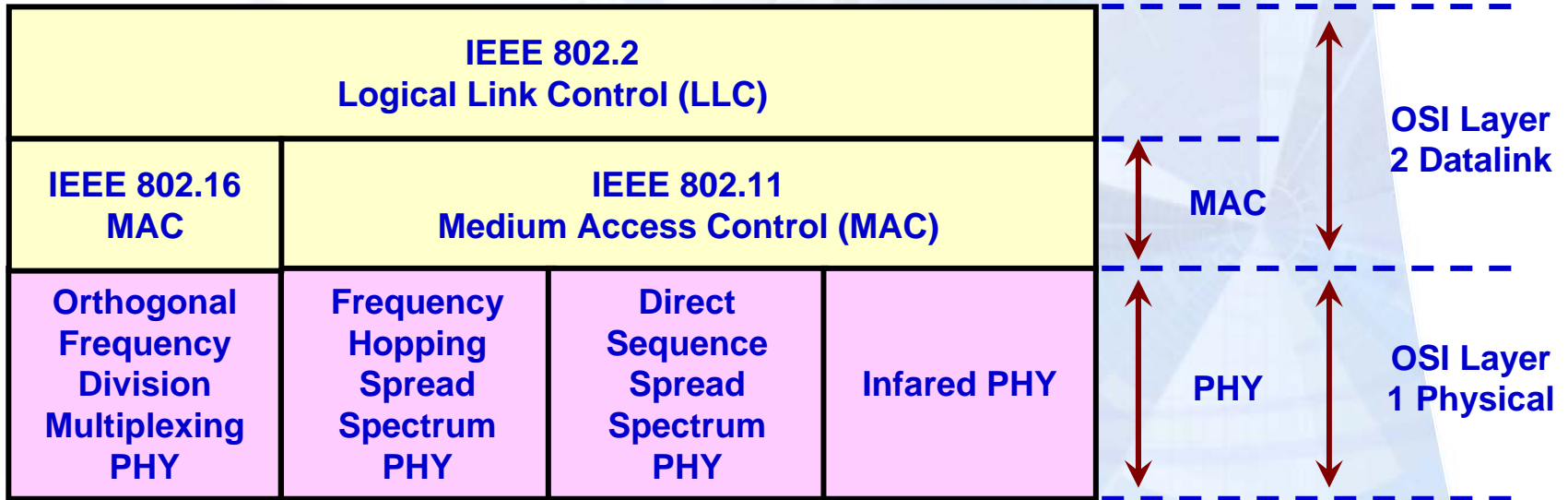
The bottom Line: NEC or NCW, the network is an important factor in defence, warfighting and tactical operations.

Example Defence Networks

- **Cormorant** – UK Tactical Wide Area Network based on ATM technology with COTS products.
 - **SKYNET 5** – Next Generation UK secure military Satellite Programme with ATM core. Has the ability to interwork with legacy technologies.
 - **TITAAN** (Theatre Independent Tactical Army and Air Force Network) – The Royal Netherlands Army network is IP-based and uses OSPF as the routing protocol.
 - **WINT-T** – (The Warfighter Information Network-Tactical) Tactical Communications network of the US army which has migrated from ATM to IP.
- With just a few examples, it is clear that a range of technologies are being used in defence networks. A move has been made to IP networking, but interworking with legacy technologies will still be an issue for years to come.

Wireless LAN/MAN Physical Layer

WIFI and WIMAX are finding their way into military networks.

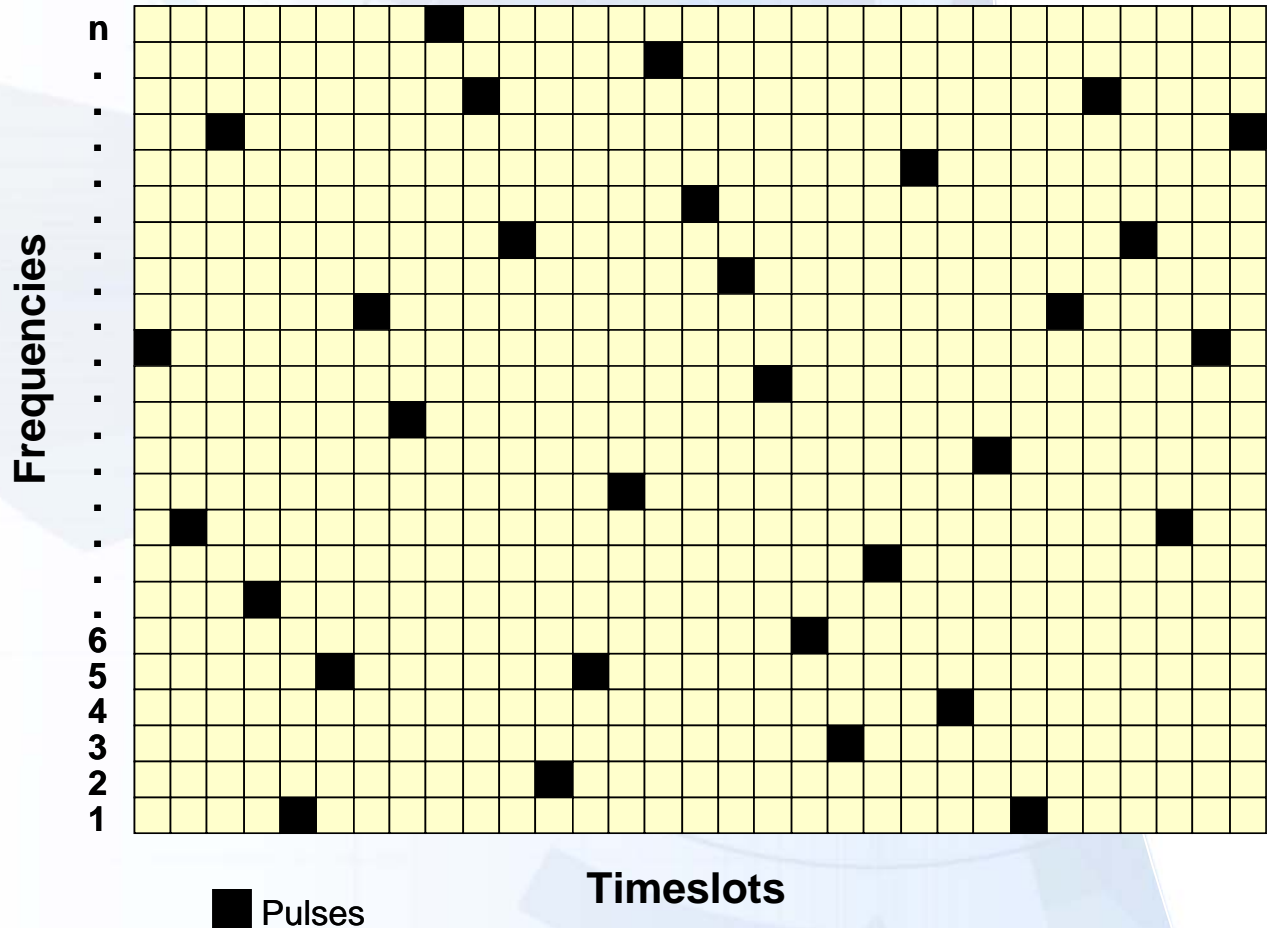


NOTE: The physical layer is not restricted for WIMAX. IEEE 802.16 defines a MAC layer that supports multiple physical layer (PHY) specifications.

The Physical layer technologies are not new, spread spectrum technologies have been used since World War II in tactical networks. They were developed to reduce the likelihood of snooping, jamming and position detection.

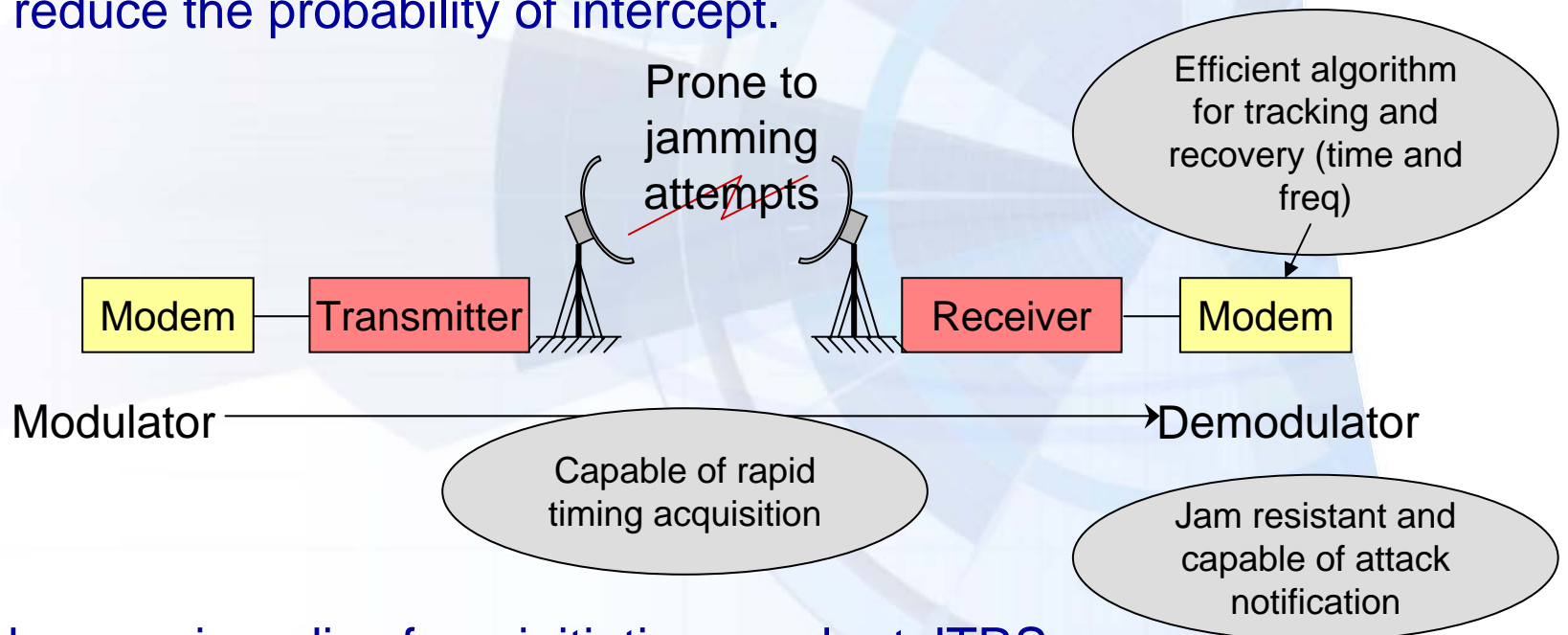
Frequency Hopping

- One of the most commonly used spread spectrum techniques is frequency hopping.
- It is essential that the frequency hopping transmitter and receiver are synchronised so that the frequency hopping is carried out at the right time.



Radio Considerations

As we have seen, spread spectrum techniques are commonly used in the tactical environment to mitigate interference due to jamming, and to reduce the probability of intercept.

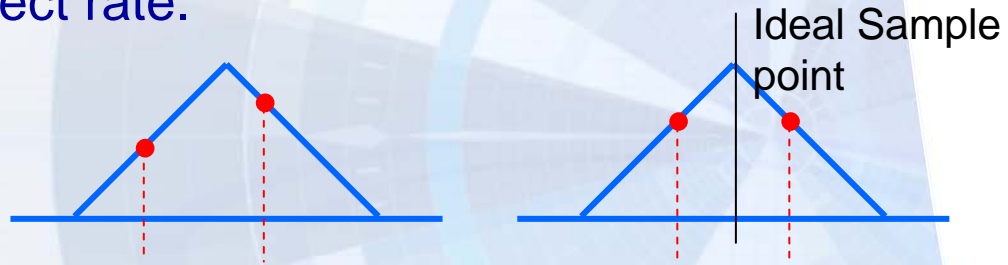


Advances in radios from initiatives such as JTRS (Joint Tactical Radio Systems) have resulted in an increased popularity in Software Defined Radios (SDRs) for military applications.

Symbolic Timing

Symbol synchronisation is required for successful recovery of the signal. There are a number of methods that may be used to overcome intersymbol interference (ISI). We must also ensure that we sample at the correct rate.

Early-Late gate algorithm (3 samples per bit)



Mueller and Muller Algorithm (1 sample per bit)

$$e_n = (y_n * y_{n-1}') - (y_{n-1} * y_n')$$


Gardner Algorithm (2 samples per bit)

$$e_n = (y_n - y_{n-2}) y_{n-1}$$

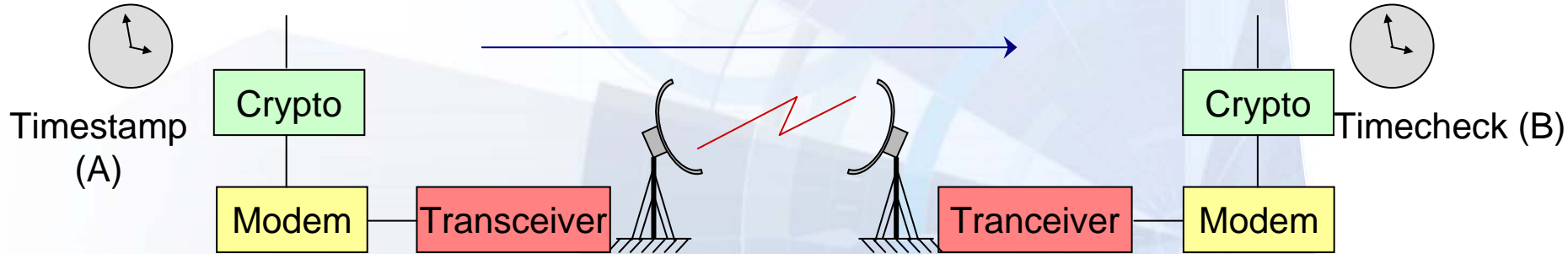
y_n = Sample from current symbol

Y_{n-1}' = decision based on current symbol

Y_{n-1} = Sample from previous symbol

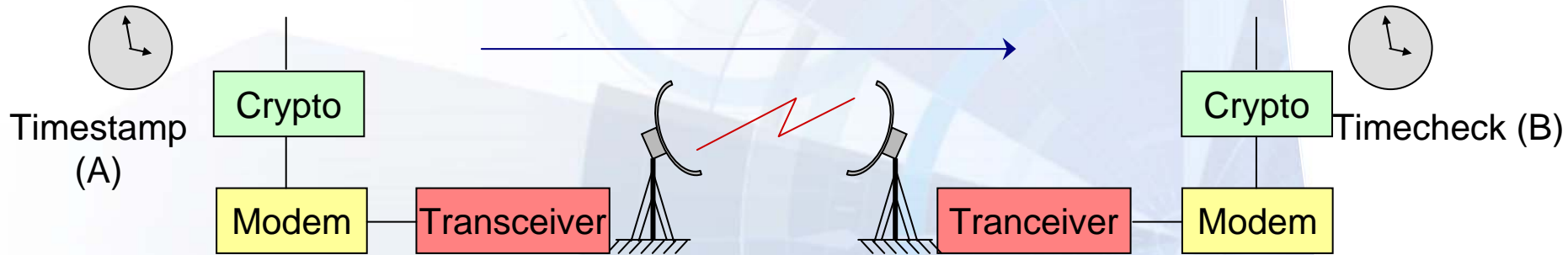
Y_{n-1}' = Decision based on previous symbol

Timestamps



- Message is cryptographically bound to a timestamp. On receipt of the message a validity check is performed, B is subtracted from A and the result is scrutinised. The message is valid if it is within a pre-defined window.
- Only one message is received with each timestamp.
- Requires common reference clock – fully synchronised link. Not effective in a distributed system.
- Clock used to timestamp must be protected from attack or reset.

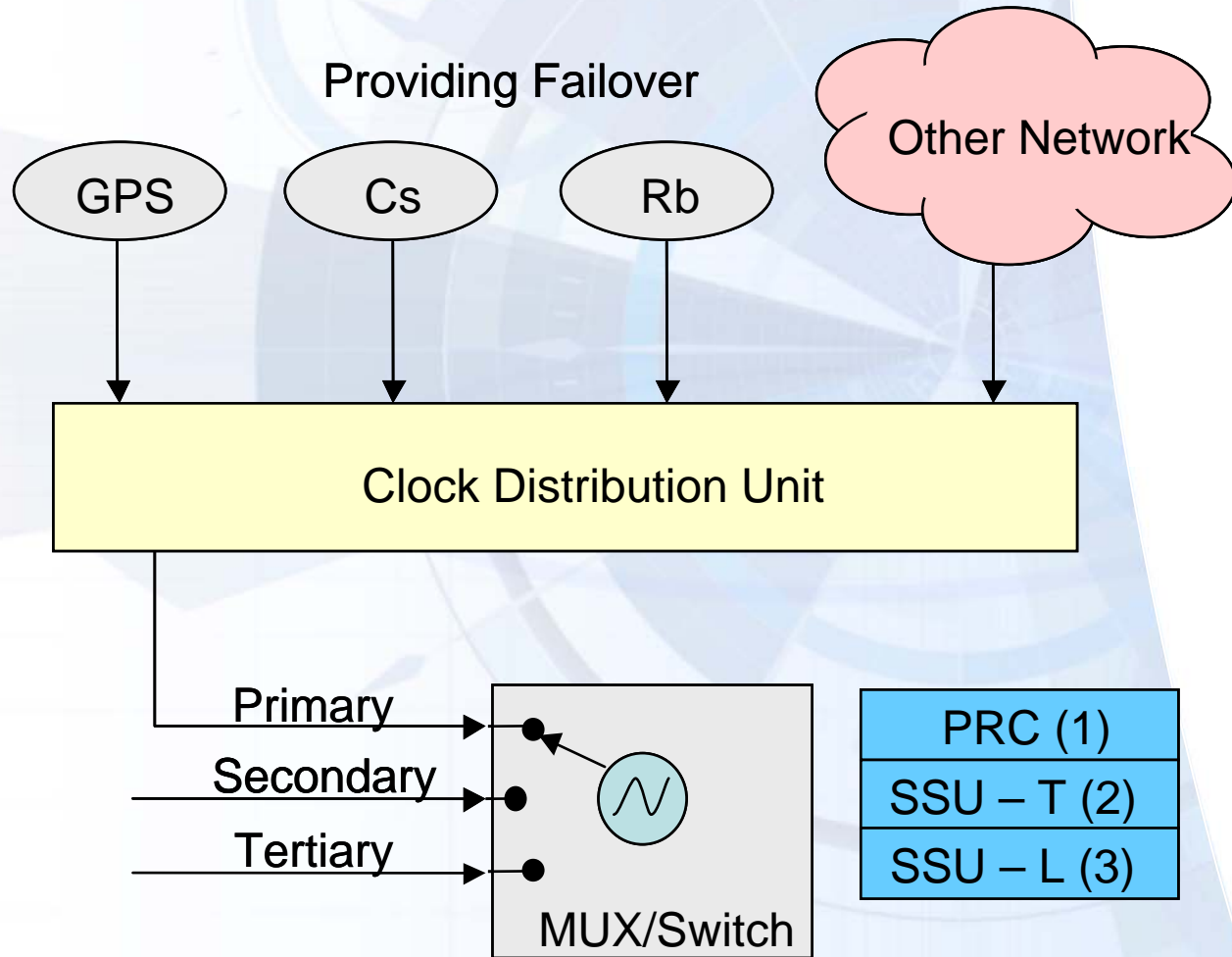
Cryptographic Synchronisation



- For synchronous stream cipher, the transmit station and receive station are cryptographically synchronised.
- Both stations will operate with respect to the same point within the same cryptographic key.
- Although cryptographic synchronisation is fundamentally different from network synchronisation, accurate timing is important to ensure that the devices rapidly acquire a synchronous state.

Failover

- Consider availability, accuracy and stability of a number of potential timing candidates.

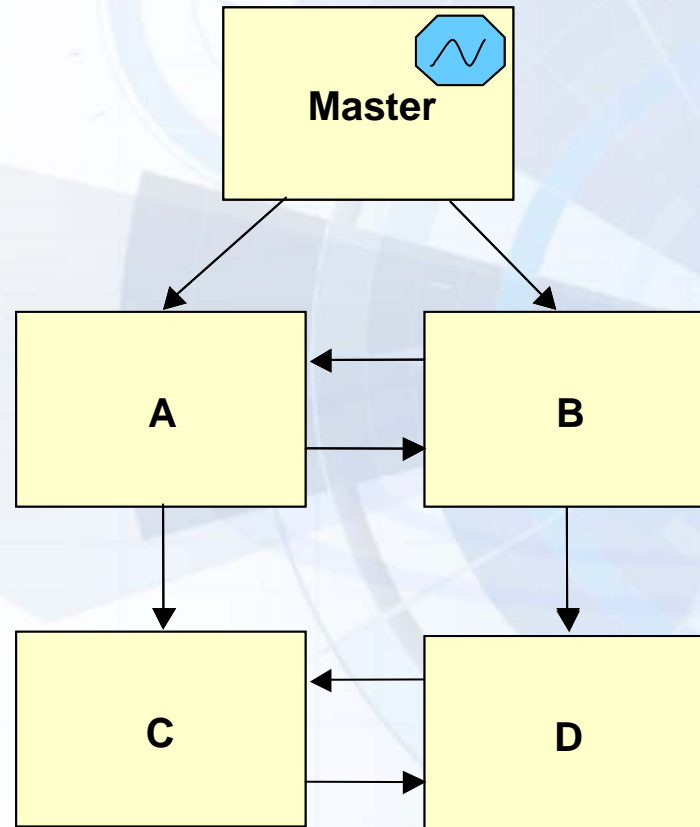


Dynamic Topology – Master/Slave

- Change in topology due to an intentional change (design or tactical requirement).

OR

- Change in topology Unintentional (e.g. attack).

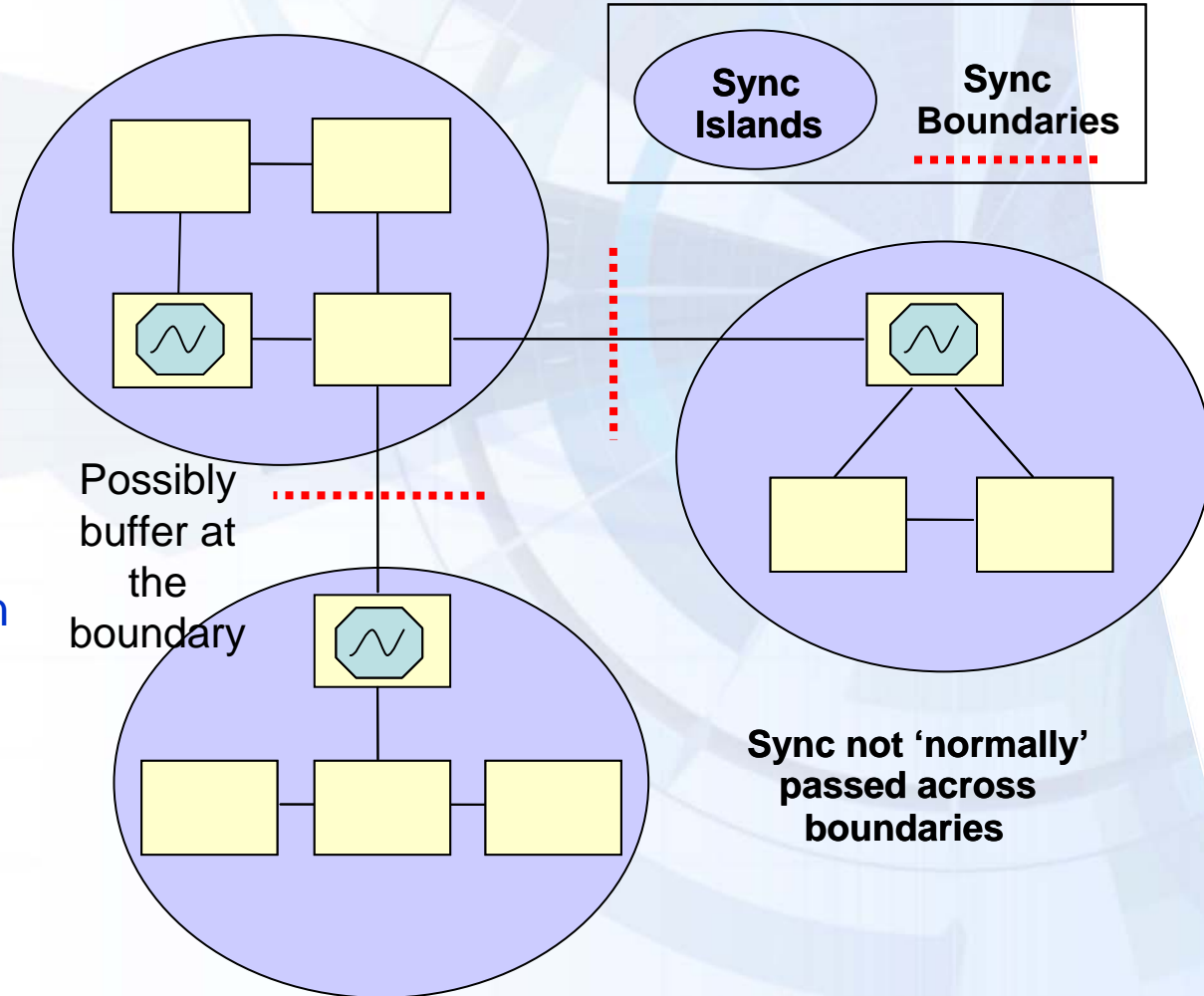


If B has to move or fails, then D can derive timing from the master via A - C

- Consider alternate routes to maintain traceability of synchronisation to the master clock source.
- Beware of Sync loops.

Islands and Boundaries – Independent Clocks

- Adjacent nodes may have different clock sources.
- Where Islands and Boundaries exist, slips will occur; the goal in this case is to minimise the slip rate.



Conclusions

- **Defence systems are prone to attack and jamming, resistance to attack should be a major consideration.**
- **As a contingency to loss of synchronisation path, high quality clocks should be considered for distributed timing.**
- **Accurate and Stable Synchronisation systems are imperative to ensuring that a network is robust, reliable, secure and effective.**
- **Network Enabled Capability is a prime consideration for successful operations; stringent planning is essential.**
- **Consideration must be given to synchronisation products, standards and schemes currently being developed. E.g Small form factor atomic clocks.**