Evaluation of Delay/Disruptive Tolerant Network (DTN) Solutions in Networks under Intentional Attack

Speaker:

LT(N) Eng. Alessandro CIGNONI

Authors:

PhD Marco CELLO

LT(N) Eng. Alessandro CIGNONI

Prof. Mario MARCHESE

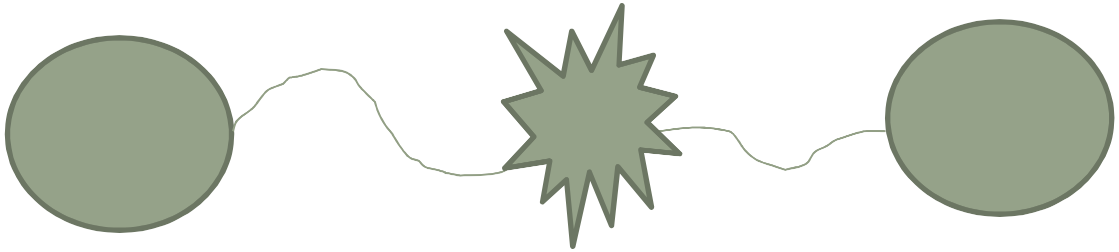
Outline

- Introduction to Delay/Disruptive Tolerant Network (DTN)
- *DTN as a Strategy for Information Assurance and Infrastructure Network Reliability*
- *Cyber Hyper-Domain*
- M&S for Cyber Battle Labs and CAX

DTN concept

- The DTN architecture embraces the concepts of occasionally-connected networks
- The basis for this architecture lies on **the Interplanetary Internet**
- Various operational environments, including those subject to **disruption and disconnection** and those with high-delay;
- Deep space is one specialized example
- **Other networks** to which DTN architecture applies

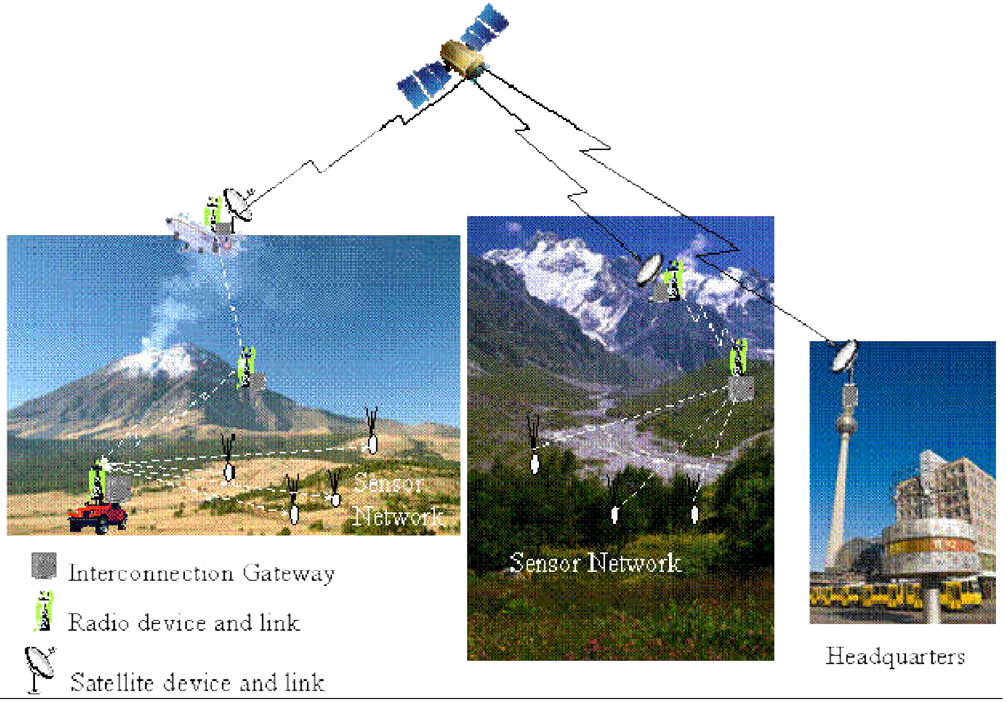
DTN concept



- DTN solution applies when End-to-end connection is : **not permanently guaranteed**; intentionally and not intentionally interrupted; operating with very large delays; operating intermittently

DTN application scenarios

- Emergency operations, interventions in hazardous areas,…

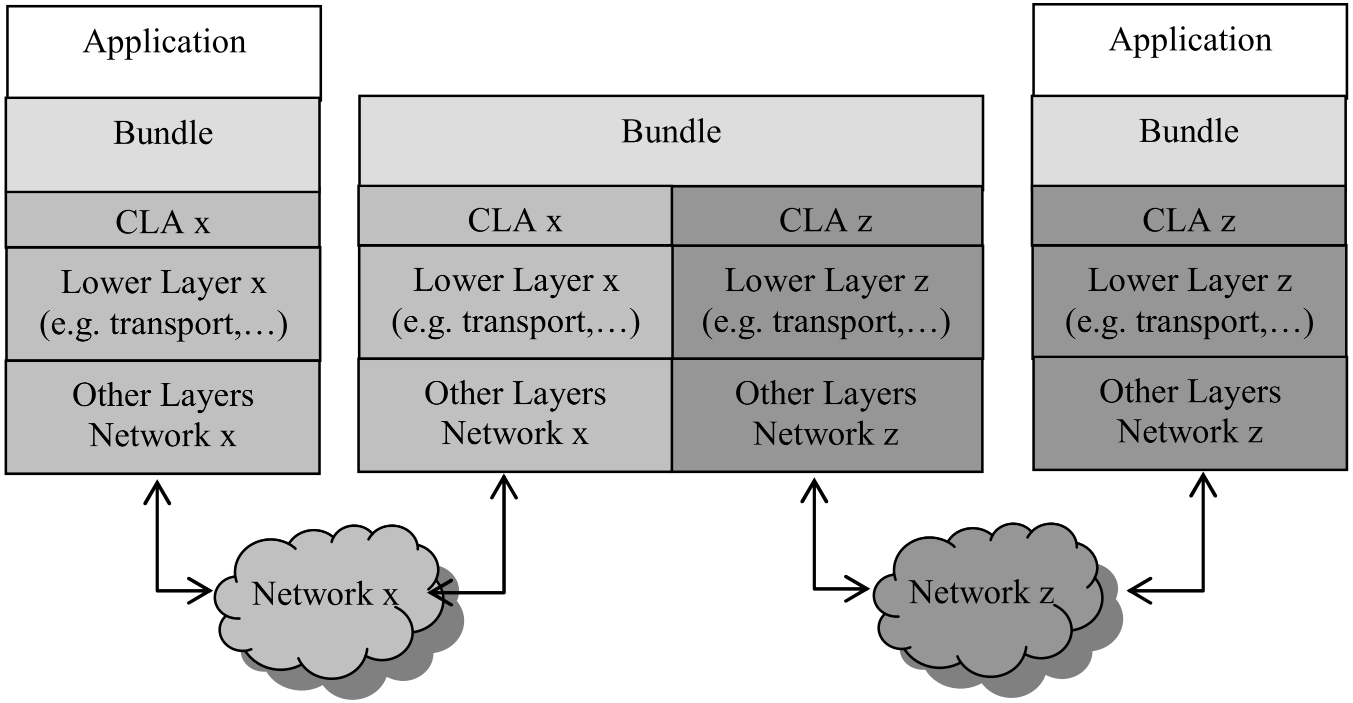


DTN Architecture Bundle Protocol

- *DTN architecture based on the **introduction of an overlay** above transport or other lower layer protocols*
- *The essential point is that in such an overlay, **delays and disruptions can be handled at each DTN 'hop'** in a path between sender and dest*
- *Nodes on the path can provide **storage***
- *The DTN architecture **does not require contemporaneous end-to-end connectivity***

DTN architecture Bundle protocol

- The basic unit of data in the Bundle Protocol is a “bundle” which is a message that carries application layer protocol data units
- The BP can interface with different lower layer (usually transport) protocols through “Convergence Layer Adapters”, (CLAs)



DTN as an overlay solution

- *DTN architecture is suited for acting as* ***overlay on top of a heterogeneous network***

- *By installing a Bundle Protocol Agent (BPA) on end-points and nodes at the border of homogeneous segments,* ***the end-to-end path can be divided into many DTN hops****.*

- *On* ***each DTN hop different CLAs can be used***

Information storage Int Nodes

- Another important difference between DTN and traditional **TCP/IP networking is related to information storage**

- In standard networks information is persistently stored only at end nodes

- This may not be the case in challenged networks. In DTN networks information is persistently (long-term) stored at intermediate DTN nodes

Information storage Int Nodes

- This feature differentiates the DTN architecture also from PEPs.
- In contrast, bundles can be stored at intermediate nodes for extended durations, and also be saved in persistent memory

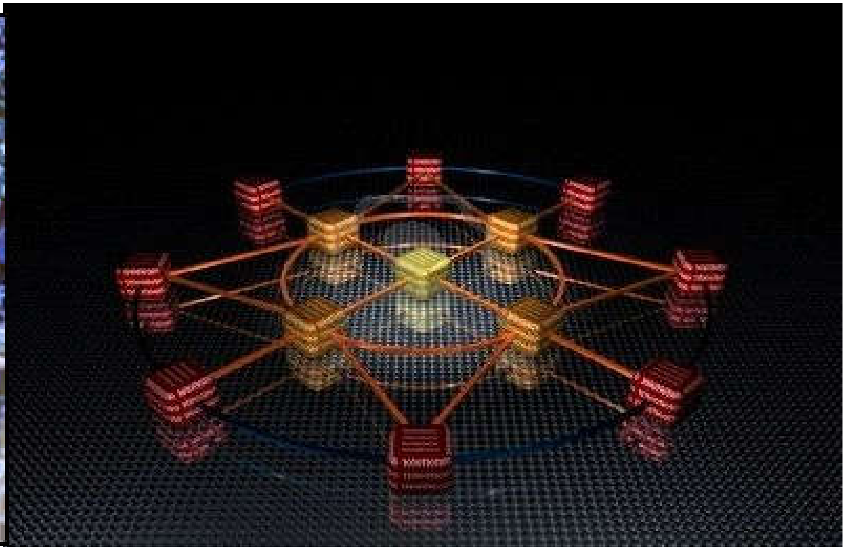
DTN as Network Defense Strategy

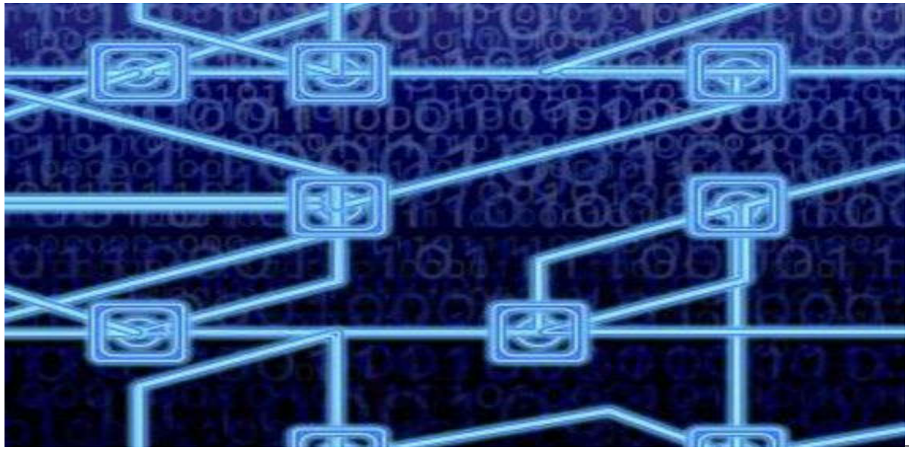
- The new idea is to use **DTN to increment Infrastructrure Network Resilience**, mitigating the effects of an intention attack to network links/nodes;
- The attack is considered as a bandwidth reduction up until no bandwidth availability

Network Resilience and Cyber Defence

urity rootkit phishing malware worm
rootkit phishing malware worm trojan viru
t phishing malware worm trojan virus spa
ishing malware worm trojan virus spam hack
malware worm trojan virus spam hackers sp
re worm trojan virus spam hackers spyware
m trojan virus spam hackers spyware secur
jan virus spam hackers spyware security ro
rus spam hackers spyware security rootkit
am hackers spyware security rootkit phis

Network Resilience and Cyber Defence





Network Resilience to:

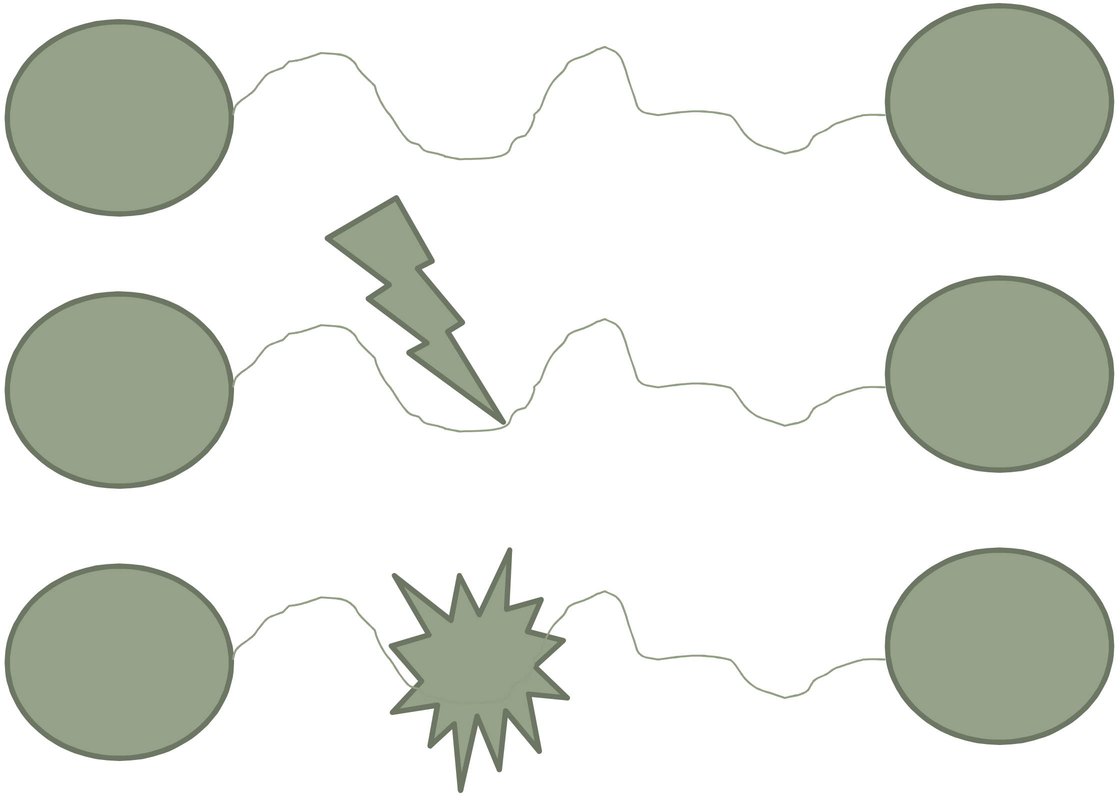
Protect Core Infrastructure

Assure Information Superiority in the Cyber Battle Field

- *Sithuation Awarness*
- *Common Operational Picture*

DTN as Network Defense Strategy

- Effect of the attack



Attack

Bandwidth

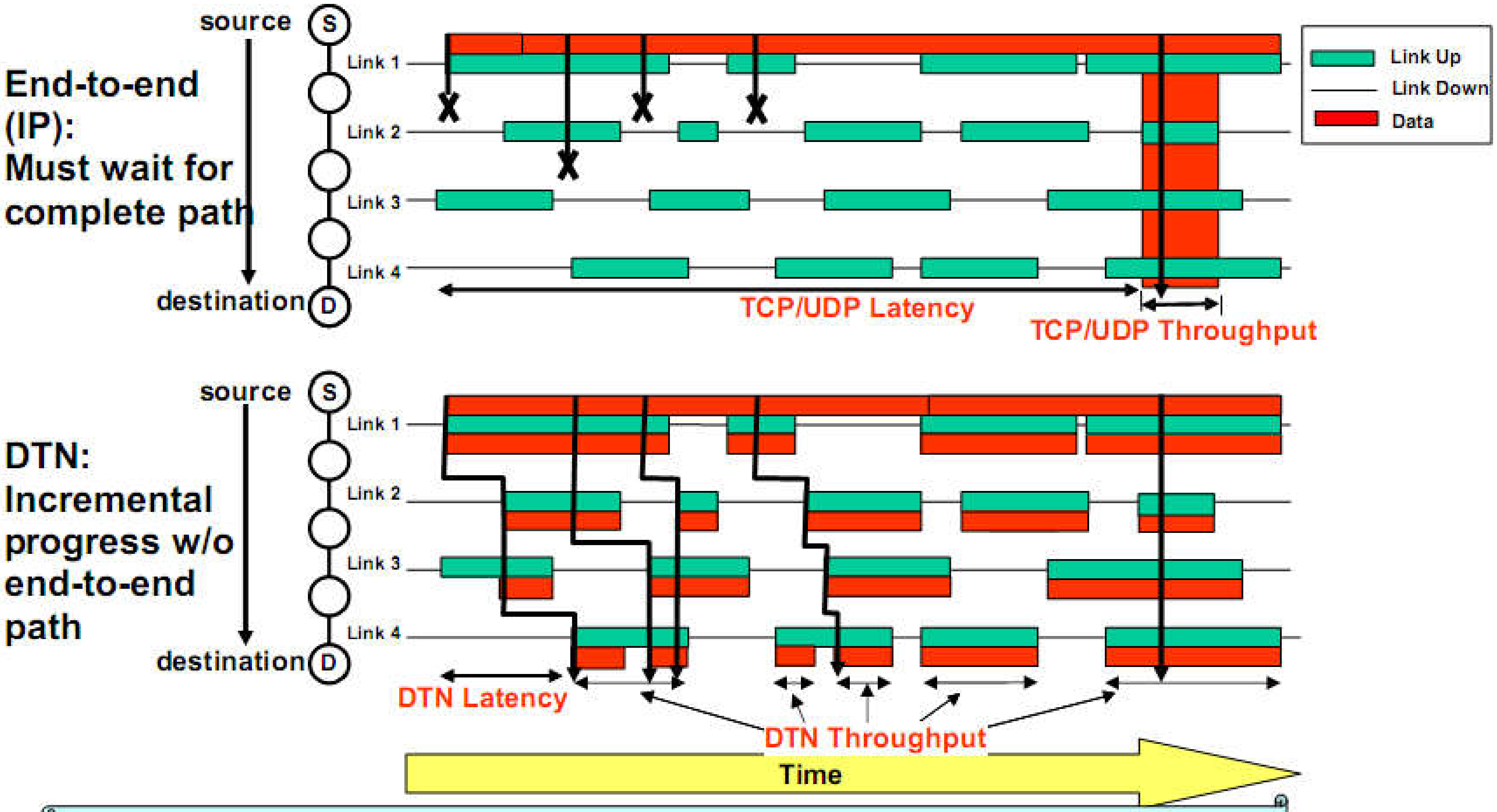
Cancellation

Link Disruption and
no service

DTN as Network Defense Strategy

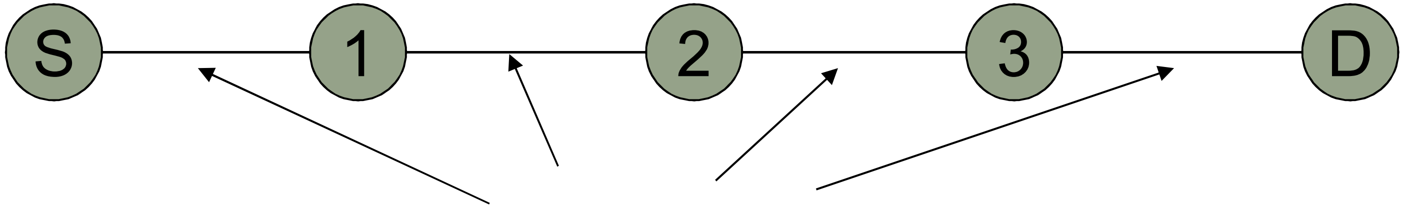
- If network nodes use the DTN architecture, can this help managing and mitigating the negative effect of the attack?
- Even if the hypothesis must be deeper verified, preliminary analysis support the idea

Preliminary results



DTN Can Reduce Delay and Increase Throughput

Very simple model



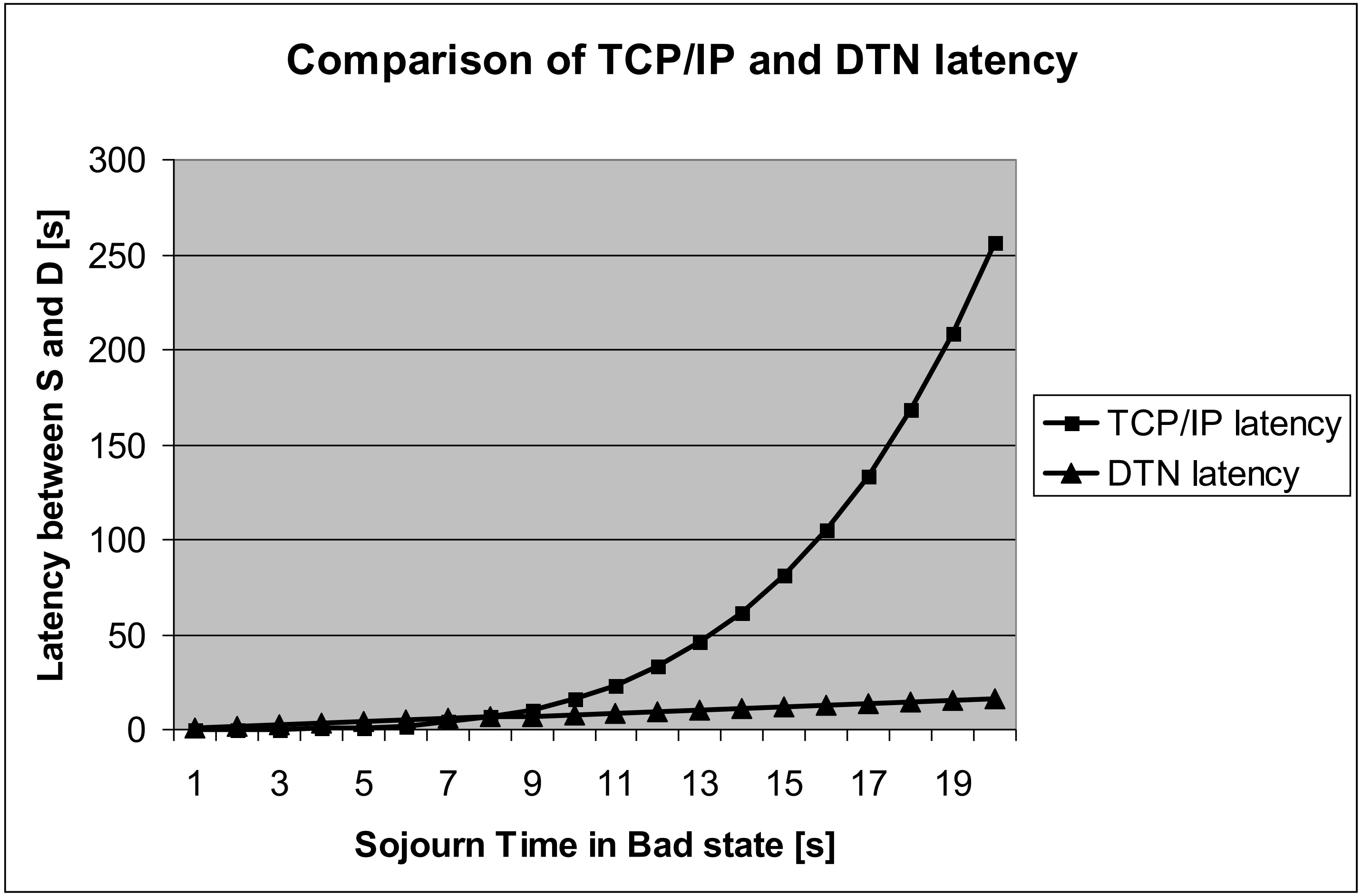
Links behavior modeled as 4 independent continuous Time Markov Chains

- π_G stationary probability of Good state (no interruption);
- π_B stationary probability of Bad state (interruption)
- T_B sojourn time in Bad state (exponentially distributed with parameter $\lambda_{B)}$
- $1/\lambda_B$ average sojourn time in Bad state
- T_x transmission time

Very simple model

- Single IP packet generated by S to D;
- TCP/UDP latency (must wait to complete a path)
  - $(\pi_B / \lambda_B)^4 + 4Tx$
- DTN latency
  - $4(\pi_B / \lambda_B) + 4Tx$

Very simple model



M&S Pillar

- More accurate Protocol Model;
- Protocol Behaviour Simulation - NS3 Based / OPNET Based
- Network Infrastracture Simulation – OPNET Based

Cyber Hyper-Domain

- DTN in Software Defined Networking Hypothesis: Cyber Hyper Dimensional or *Cyber Hyper-Domain*
  - *Free BSD Jials*
  - *Stanford Clean Slate Projects*

Cyber Hyper-Domain

- *Hyper-Dimentional* Cyber Domain (men-driven and/or autonomus cognitive processes to inter-dimension switch);
  - *Time*
  - *Space*
  - *Virtual Space*
  - *Autonomous Systems Domains /Topology / Routing Strategies and Protocols*
- Different NetworkTopology and Routing Strategy are separated in different Jails.

Cyber Defence CAX

- Cyber Hyper-Domain M&S
- Distributed Battle Labs Interconnection
- *Men and Autonomous Agents CAX in the simulated Cyber Hyper-Domain*

Cyber Defence CAX

- *Assure Information Superiority in the Cyber Hyper-Domain which directly translates into Power Superiority in the Battlefield*

Contact :

NATO M&S COE:

LT(N) Eng. Alessandro CIGNONI

sesto.natomes.areadottrina02@smd.difesa.it

DITEN – University of Genoa:

Prof. Mario Marchese

mario.marchese@unige.it

PhD Marco Cello

marco.cello@unige.it