Architecting Information Security Services for Federate Satellite Systems

Marc Sanchez Net, Iñigo del Portillo, Bruce Cameron, Ed Crawley

3nd International Federated Satellite Systems Workshop

August 28th 2015

Outline

- Introduction
- Security Threats Identification
- The Interaction State Model
  - Hop-to-hop interactions
  - The Interaction State Machine
  - QoS for FSS Security Services
- Conclusions & Future Work

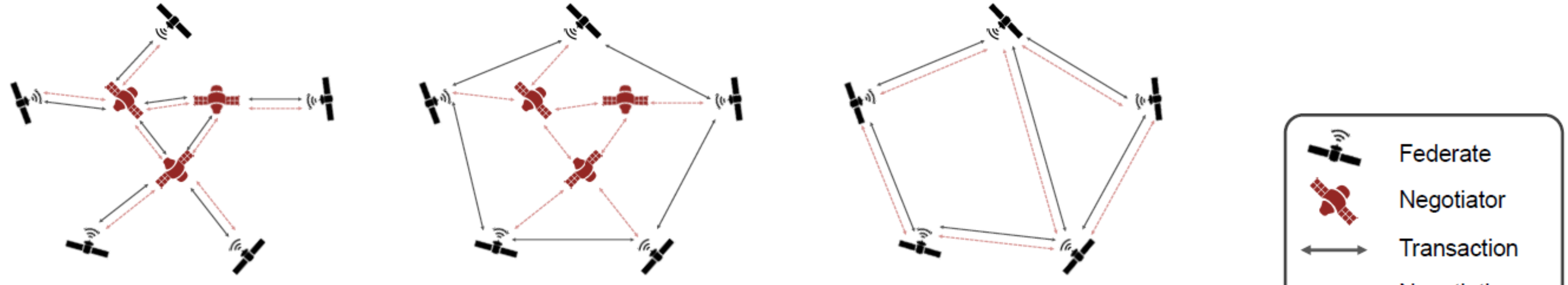
Introduction

Federate Satellite Systems leverage under-utilized capabilities from spacecraft that are in orbit, by sharing resources among them.

Two types of interactions are envisioned in a FSS during resource exchange [1]:

- **Transactions**: Exchange of resources among satellites
- **Negotiations** : Ability to efficiently allocate resources from suppliers to customers

The functionality of these interactions can be assigned to different federates yielding three canonical FSS architectures.



(a) Centralized FSS (b) Negotiated FSS (c) Distributed FSS

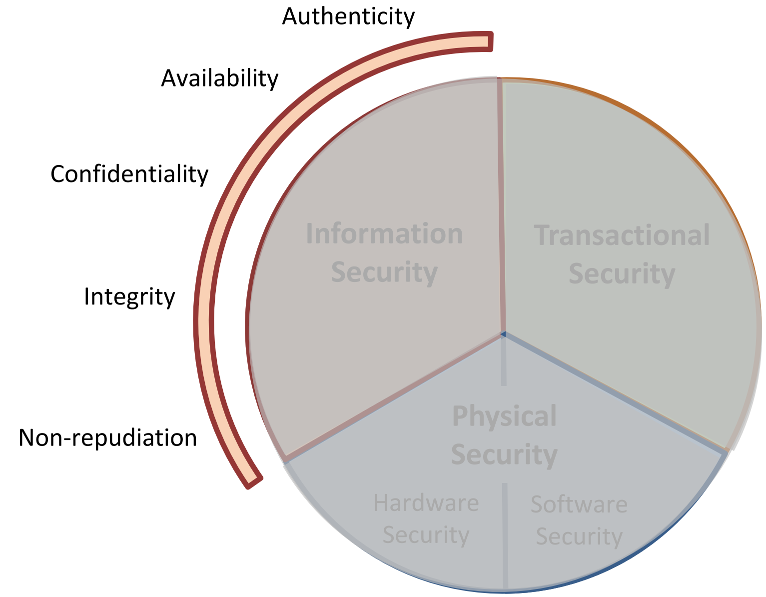
[1] Golkar A., *Design margin utilization in commercial satellite cloud computing systems*, 65th International Astronautical Congress, no. IAC-14-D3, 2014

Marc Sanchez Net <msnet@mit.edu>
Iñigo del Portillo <portillo@mitedu>

Introduction

The FSS literature recognizes the presence of malicious federates, therefore a security analysis is needed.

Risks inherent to a FSS can be perceived from a triple complimentary standpoint.



In this paper we focus on **Information Security** Threats and Mitigation.

The outcome of this work is a **conceptual framework** to understand the **architectural implications** of providing information security services in the FSS environment.

[illegible]

We **do not** propose any specific recommendation on security ciphersuites to implement [Internet Research Task Force, CCSDS]

Security Threats Identification

	Attack			
Threat	Name	Type	InfoSec Service	Comments
Identity theft	Eavesdropping	Passive	Authentication Integrity	A federate steals the identify of another federate user by listening to the information stream he is relaying
Identity theft	Impersonation	Active	Authentication Non-repudiation	A federate sends messages through the FSS network under a false identity
Link disruption	Jamming	Active	Availability	A malicious entity incapacitates a communication media in the FSS network
Supplier disruption	Denial of service	Active	Availability Non-repudiation	A federate wastes supplier resources by submitting useless or malicious jobs
Data theft	Eavesdropping	Passive	Authentication Confidentiality	A federate copies information content from another federate while relaying it
Data theft	Phishing	Passive	Confidentiality Non-repudiation	A federate sends malicious jobs to a supplier in order to obtain sensitive information of the federate
Data corruption	Eavesdropping	Active	Authentication Integrity Non-repudiation	A federate modifies the information stream that he is relaying
Data destruction	Denial of service	Active	Authentication Integrity Non-repudiation	A federate does not relay an information stream, thus destroying the information
Data replay	Replaying	Active	Authentication Integrity Non-repudiation	A federate records and then re-sends the same information multiple times

Marc Sanchez Net <msnet@mit.edu>
Iñigo del Portillo <portillo@mitedu>

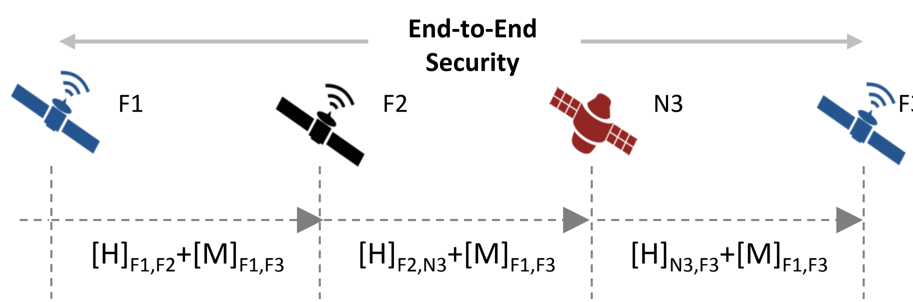
The Interaction State Model (I)

- The Interaction State Model describes the information security for different types of interactions between two FSS nodes.

- To simplify the problem, each federate is assumed to *only* evaluate the trustworthiness of his immediate peer (one-hop) and the channel between them. Therefore, 4 canonical configurations are possible:

Node 1	*Channel*	*Node 2*	*Acronym*	*Symbol*
Trusted	Not Trusted	Not Trusted	*TNN*	N1 → Channel → N2
Trusted	Trusted	Not Trusted	*TTN*	N1 → Channel → N2
Trusted	Not Trusted	Trusted	*TNT*	N1 → Channel → N2
Trusted	Trusted	Trusted	*TTT*	N1 → Channel → N2

- For encryption purposes, the Interaction State Model is only concerned with the securing the header information (H). The payload or message (M) is assumed to be end-to-end protected by an FSS-external mechanism



Marc Sanchez Net <msnet@mit.edu>
Iñigo del Portillo <portillo@mitedu>

The Interaction State Model (II)

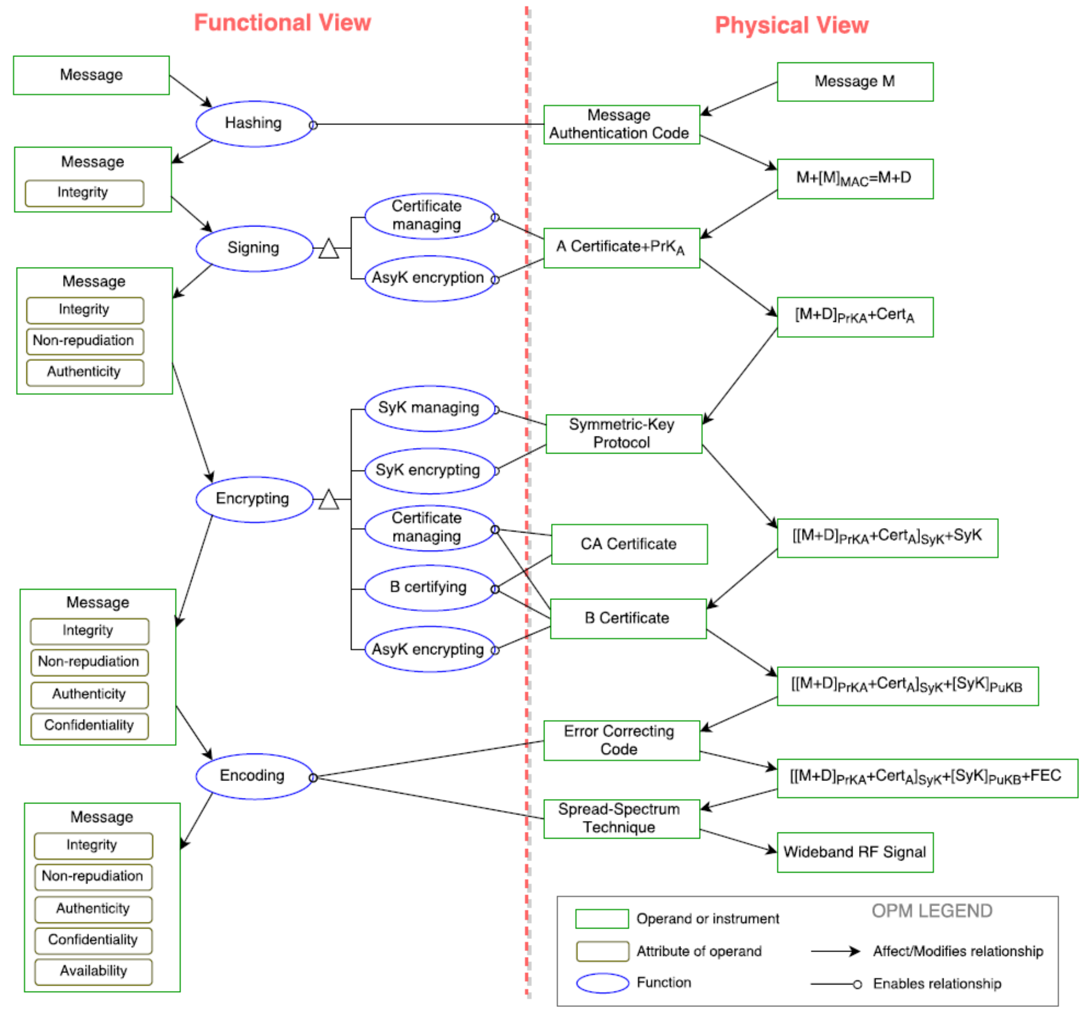
The model assumes a reference security architecture similar to the one used in most Internet services.

Hop-to-hop security services are provided by implementing 5 primary functions:

- Hashing
- Signing
- Encrypting
- Certifying
- Encoding

Functions incrementally provide InfoSec services to the messages transmitted through the FSS network.

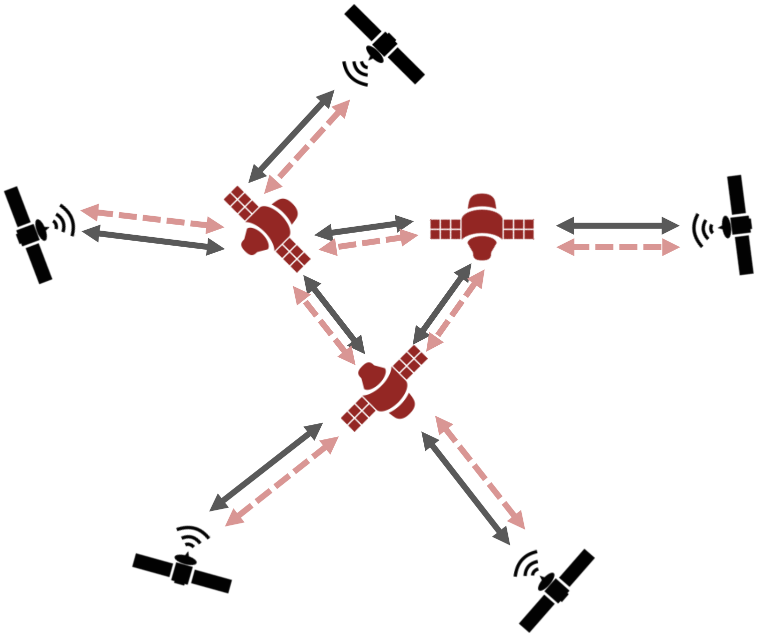
Certifying is assumed to encompass all functionality to maintain the chain of trust in a PKI infrastructure.



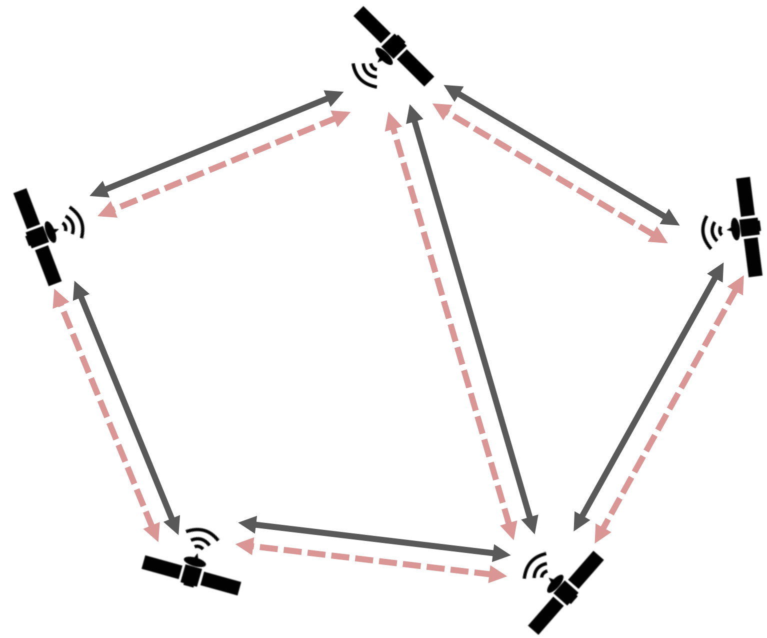
Marc Sanchez Net <msnet@mit.edu>
Iñigo del Portillo <portillo@mitedu>

The Interaction State Model (III)

Centralized Architecture

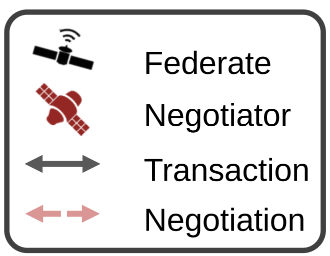


Distributed Architecture



N_1-C-N_2	H	S	C	Ec	En
TNT	✓	✗	✗	✗	✓
TTT	✗	✗	✗	✗	✗

NEGOTIATION PHASE

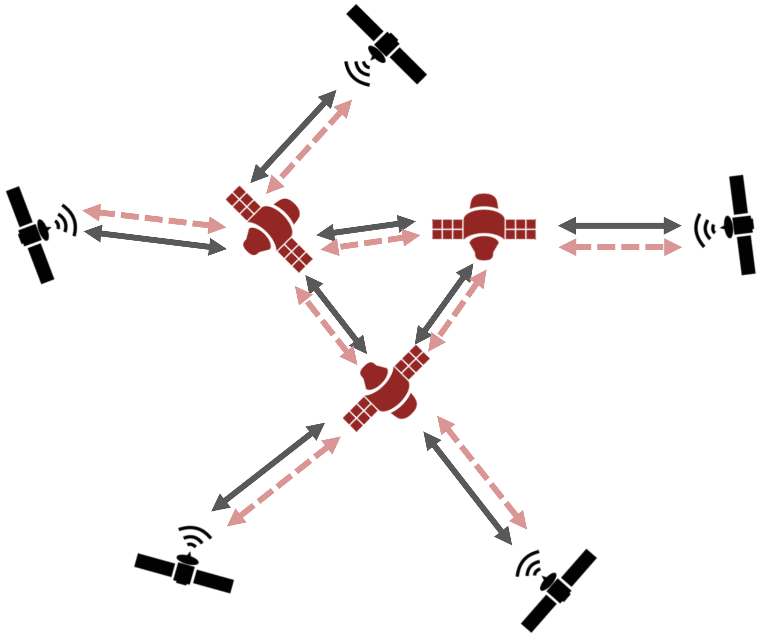


N_1-C-N_2	H	S	C	Ec	En
TNN	✓	✓	✓	✗	✓
TTN	✓	✓	✓	✗	✗

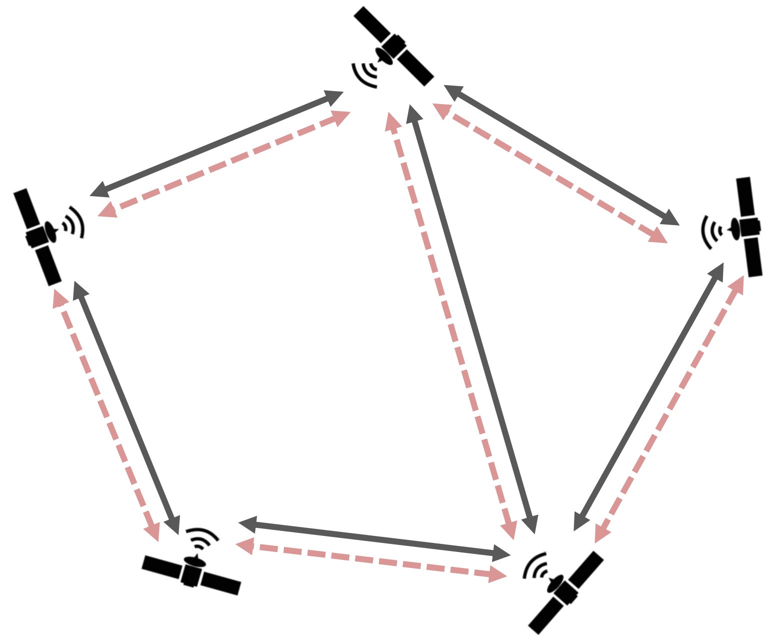
Marc Sanchez Net <msnet@mit.edu>
Iñigo del Portillo <portillo@mitedu>

The Interaction State Model (III)

Centralized Architecture



Distributed Architecture



N_1-C-N_2	H	S	C	Ec	En
TNT	✓	✗	✗	✓	✓
TTT	✗	✗	✗	✗	✗

TRANSACTION PHASE

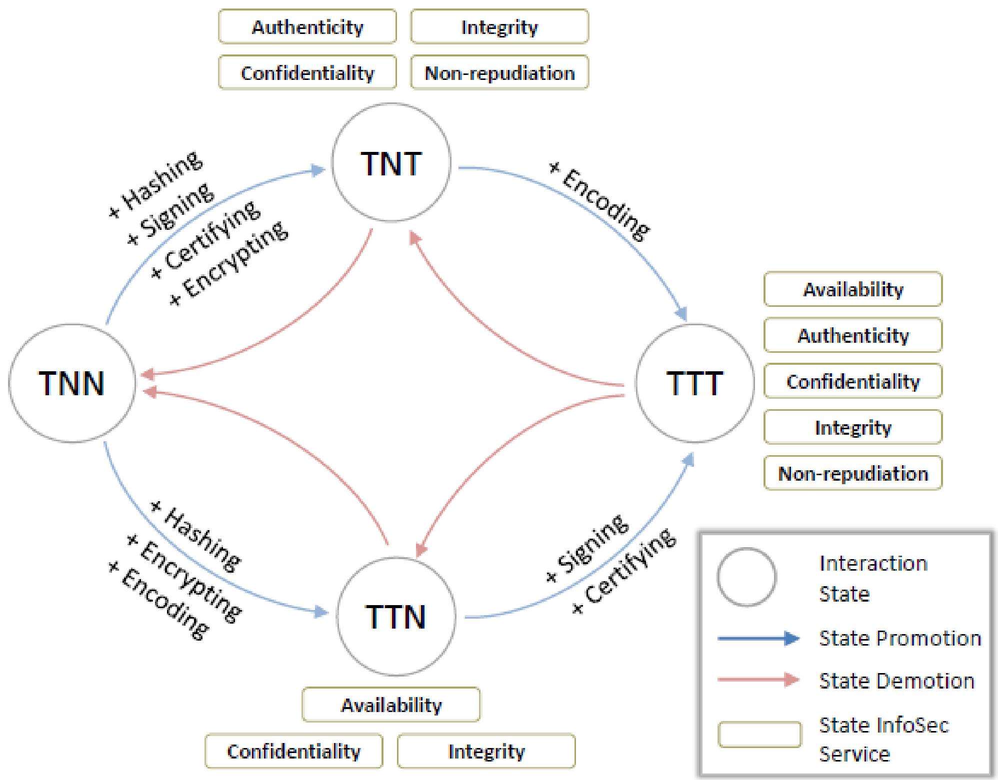
- Federate
- Negotiator
- Transaction
- Negotiation

N_1-C-N_2	H	S	C	Ec	En
TNN	✓	✓	✓	✓	✓
TTN	✓	✓	✓	✓	✗

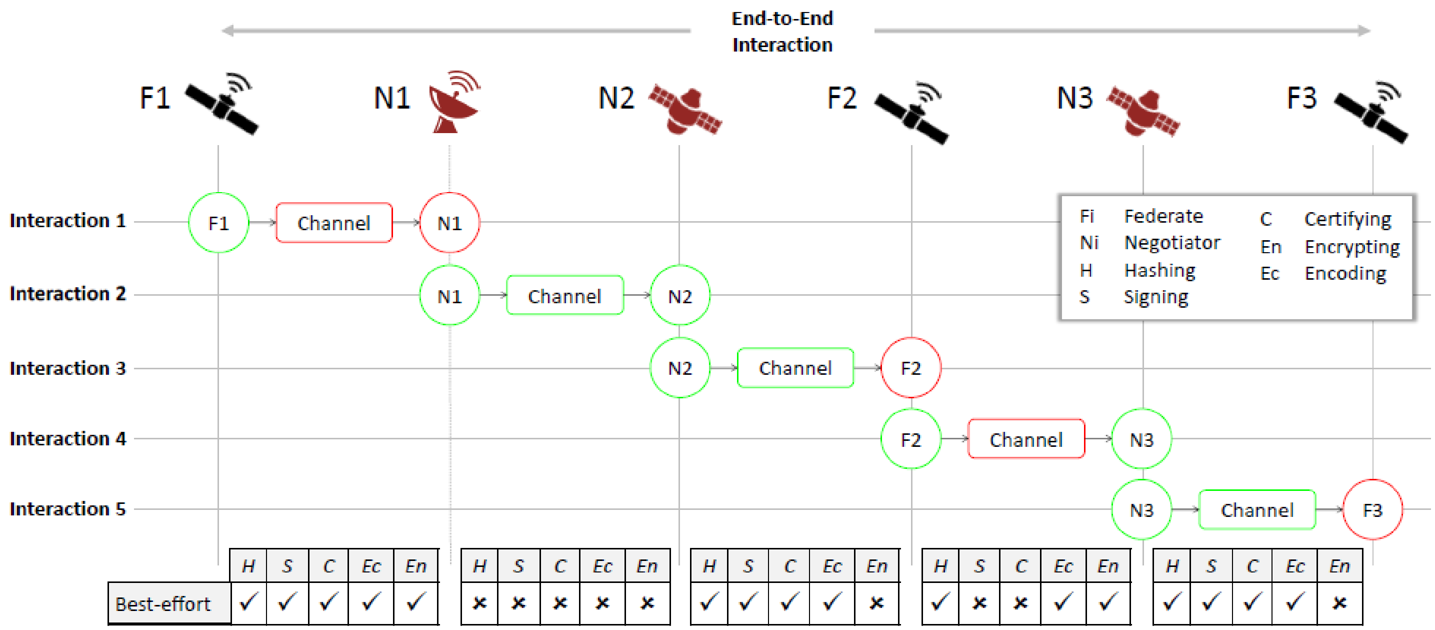
Marc Sanchez Net <msnet@mit.edu>
Iñigo del Portillo <portillo@mitedu>

The Interaction State Machine

- The Interaction State Machine is a transition diagram that specifies the InfoSec services that an FSS node can provision given the implemented functionality by him and his peer.
- An interaction between two FSS participants can be state-promoted (blue) and state-demoted (red)
- State promotion enhances the “level of security” for both the header and the information payload.
- However, it also requires increased computation and bandwidth resources. Therefore, what is the optimal policy?



QoS for FSS Security Services



- In a **Best-effort** mode, each hop is provided with the InfoSec mechanisms requested based on the state perceived by the transmitting node.
- However, the source of the information might not trust the state perception of other nodes, or might want that some InfoSec services are applied in the transaction
- In a **Guaranteed** mode, all the nodes must enforce a subset of the InfoSec services. This allows to define different Quality of Services (QoS) for FSS Security Services
- Guaranteed and best-effort security services can be used to (1) enrich the FSS marketplace and (2) design routing policies that maximize system efficiency in provisioning secured interactions.

Marc Sanchez Net <msnet@mit.edu>
Iñigo del Portillo <portillo@mitedu>

Conclusions & Future Work

CONCLUSIONS

- The architecture of information security services is assed based on a threat analysis.
- Mitigation of the treats is achieved by provisioning 5 types of security services.
  - Due to the transaction-based nature of the system, **non-repudiation** is a security service that the system must provide.
- The Interaction State Model is a fundamental tool to understand which services must be provided in order to ensure information security in a FSS.

FUTURE WORK

- Both the physical and the transactional view of the FSS security architecture should be analyzed and threats identified
- Performance analyses on different security mechanisms for implementing the security services functions and key-management process should be performed
- The system implications of providing different levels of security-QoS must be further studied

Marc Sanchez Net <msnet@mit.edu>
Iñigo del Portillo <portillo@mitedu>

Thank you for your attention!

Q&A

Backup Slides