Software-Defined Networking Based Capacity Sharing in Hybrid Networks

Mateus A. S. Santos, Bruno T. de Oliveira, Cíntia B. Margi

Bruno A. A. Nunes, Thierry Turletti

University of Sao Paulo, INRIA Sophia Antipolis, UC Santa Cruz

Workshop on Capacity Sharing (CSWS'13) - Göttingen
• Introduction
• Network Model
• Software Defined Networks
• Requirements
• Background
  – ID-Based Cryptography
• Secure Capacity Sharing Framework
• Implementation
• Final Considerations
Introduction

- Mobile and Heterogeneous Network
- Connection Anywhere/anytime

- Extend the scope of existing infrastructure via infrastructure-less network
- Focus on security
- Leverage SDN to enable sharing of network resources in hybrid networks
Software Defined Networks (SDN)

- Separation between Control and Data
- Communication between Control- and Data-plane (E.g. via OpenFlow protocol)

Figure: Xuan-Nam Nguyen
Network Model

• A user “Alice” wishes to connect to the Internet
  – lacks network infrastructure (e.g. out of AP's range)
• Another user, “Bob” advertises his gateway services

Traditional Scenario

• ISP is NOT aware of Alice
• Bob's device used as a NAT

SDN-Enabled Scenario

• SDN controller is aware of Alice
• ISP controls the resources
Requirements

- GW act as SDN switches (e.g., Openflow)
- Gateway device incentive
- Access Control
  - GW performs \textit{challenge/response} with user
  - Controller authorizes user
Requirements

- Confidentiality and Data Authenticity
  - GW does not decrypt user traffic
  - Secure channels: User-AP, User-Controller

- QoS Policies (e.g., WFQ)

- Changing Gateways
ID-Based Cryptography (IBC)

• Users’ identity as a public key
  – no need to verify the public key using CA
  – protocols made simple and efficient
  – efficient pairwise key-agreement

• Synergy between SDN controllers and IBC
  – Controllers are trusted (manage the network)
  – Controllers can generate private keys to users
Secure Capacity Sharing Framework

Gateway discovery
  - GW sends periodic HELLO messages

Handshaking
  - GW authenticates user

Authentication Key Agreement
  - User agree on keys with GW, AP and Controller

User check-in
  - Controller authorization

End-to-end security
  - Encryption and authentication (symmetric cryptography)
Secure Capacity Sharing Framework

- **Alice**
  - Bcast-Find_GW
  - Handshaking
  - Handshaking
  - Wait_CheckIn
  - Alice_CheckIn
  - Alice’s Assignment

- **Bob (GW)**
  - Announce service
  - Alice_Check-In_Request
  - Alice_Check-In

- **AP OpenFlow**
  - Alice_Check-In_Request
  - Alice_Check-In

- **Controller**
  - Alice’s Registration
• OVSwitch at the GW node (Bob)
• Authentication Module – AM (Client-Server-Control): C/C++
Final Considerations

• Extend the scope of existing infrastructure via infrastructure-less network
• Focus on security
• Leverage SDN to enable sharing of network resources in hybrid networks

• Ongoing Work:
  – Secure Handover Support
  – Distribution of Control
  – Fault Tolerance in the Control Plane
Software-Defined Networking Based Capacity Sharing in Hybrid Networks

Bruno A. A. Nunes
INRIA Sophia Antipolis
bruno.astuto-arouche-nunes@inria.fr

Workshop on Capacity Sharing (CSWS'13) - Göttingen