



# Rilevazione di disservizi nella connettività di rete

Candidato:

Daniel Casenove

Relatore:

Luca Deri

# Sviluppo delle reti e del traffico

---

- Numero di dispositivi connessi in aumento:
  - Smartphone
  - Tablet
  - Dispositivi IoT
- Cambio del mezzo trasmissivo in favore del Wi-Fi
- Nuovi paradigmi per la fruizione dei servizi:
  - Streaming
  - Cloud storage
- Necessità di monitorare reti locali per disservizi

# Software in utilizzo

---

- UniFi Ubiquity
  - Monitoraggio di dispositivi del produttore Ubiquity
- Netspot
  - Fornisce soluzioni per il deploy di reti Wi-Fi
- inSSIDer
  - Analizzatore di reti Wi-Fi, suggerisce canali su cui instaurare Wi-Fi
- Kismet
  - Rilevamento di dispositivi wireless, sniffer e WIDS framework

# Limiti delle attuali soluzioni

---

- Focus principale sullo stato dell'access point
  - Valori di bontà del segnale
  - Suggerimenti non real-time per un'ottimizzazione della connessione
- Mancanza di una visione totale della rete e dei dispositivi ad essa connessi
- Ristrette a dispositivi di rete professionali

# Una soluzione per reti domestiche

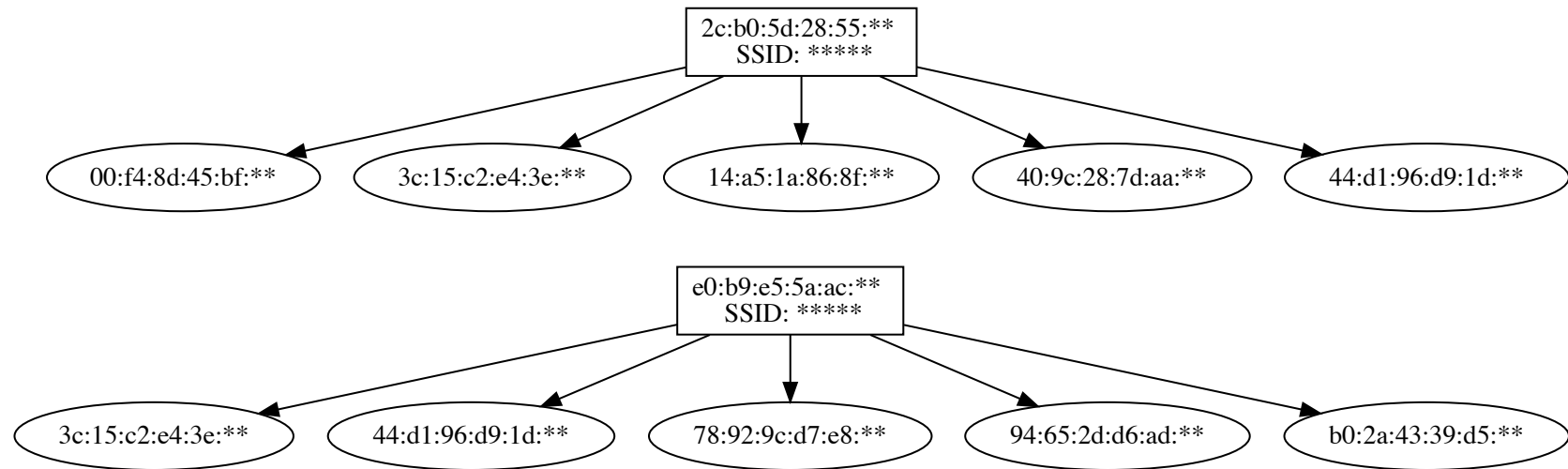
---

- Analisi real-time del traffico della rete
  - Ricostruzione della topologia di rete
  - Misure di bontà del segnale
- Monitoraggio dei dispositivi connessi alla rete
- Identificazione dei nodi affetti da disservizi di connessione
- Facile utilizzo e contenuto uso di risorse

# Validazione su reti semplici

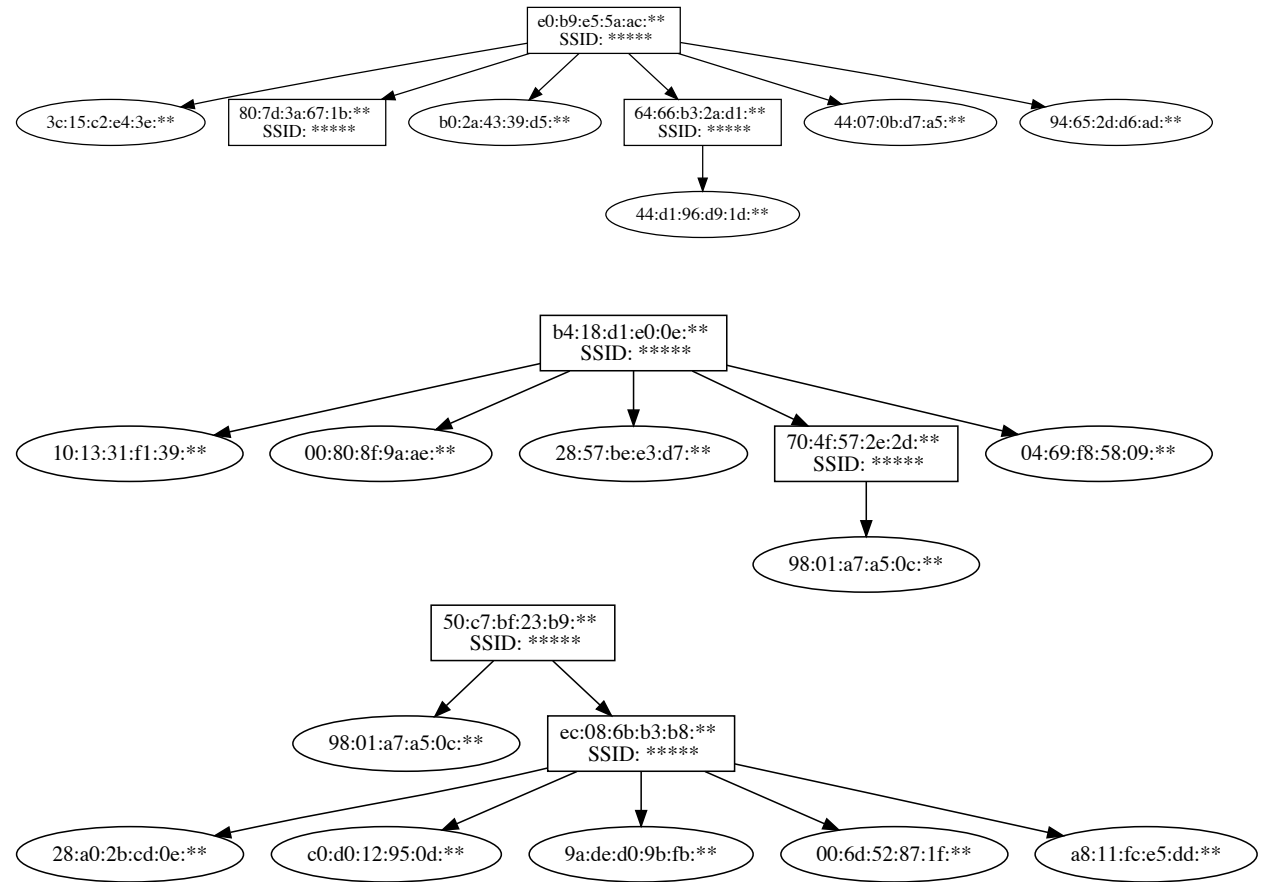
---

- Dispositivi direttamente collegati ad un access point
- Analisi validata dalla conoscenza della rete



# Validazione su reti con repeater

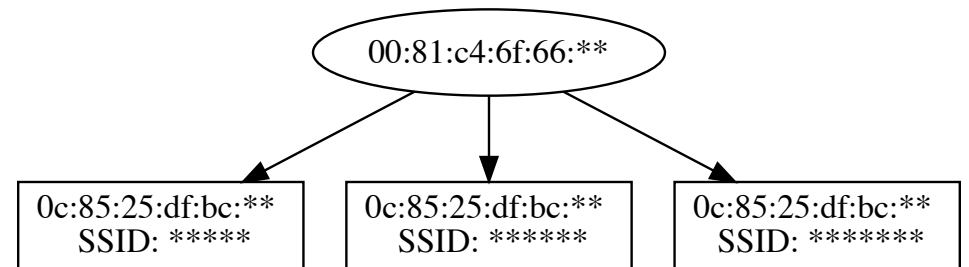
- Presenza di repeater ed altri dispositivi che annunciano reti wireless
- Ricostruzione attraverso euristiche e validazione data dalla conoscenza della topologia della rete



# Validazione su reti professionali

---

- Corretta identificazione di più reti Wi-Fi per access point
- Difficile da validare:
  - Alto numero di dispositivi
  - Topologia non conosciuta a priori





# Rilevazione di disservizi

---

- Round Trip Time (RTT)
  - < 1ms all'interno della rete
- Signal to Noise Ratio (SNR)
  - Differenza tra potenza segnale e rumore di fondo
- Rilevazione del nodo specifico affetto da disservizio
  - Topologia rilevata più misure di bontà del segnale

SNR (dB)A	Segnale	Velocità
>40	Eccellente	Massima
25-40	Molto buono	Ottima
15-25	Basso	Buona
10-15	Molto basso	Bassa
<10	Assente	Assente

# Analisi della performance

---

- Uso di memoria dipendente dal traffico
  - ~20MB per 30,000 pacchetti catturati ed analizzati
  - Generalmente ~5MB per catture live di 15 secondi
- Tempo di calcolo principalmente dovuto alla cattura
  - Cattura costante
  - Cattura programmata per una durata a scelta
- Soluzione implementabile su:
  - Router
  - Smartphone
  - SBC

# ArpScanner

---

- Monitoraggio attivo
- Effettua Arp Scan sulla rete in analisi
  - Assegna indirizzi MAC ad indirizzi IPv4
- Arp Ping
  - Calcolo del RTT dei pacchetti inviati
  - Metrica utile per dispositivi cablati e Wi-Fi
- Fornisce dati utili alla libreria WiFi-Topology

# WiFi-Topology

---

- Monitoraggio passivo
- Cattura del traffico 802.11
  - Ricostruzione della topologia della rete
  - Calcolo della potenza del segnale Wi-Fi
- Utilizzo di euristiche per determinare:
  - Access point
  - Repeater

# 802.11 Frames

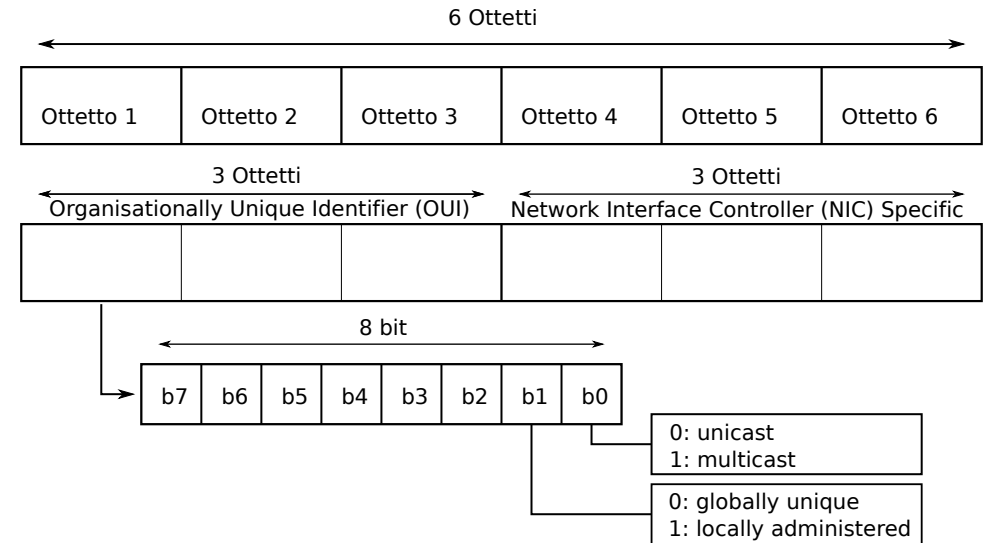
- FC:
  - Tipi di frame
    - Management frame
    - Control frame
    - Data frame
  - Sottotipi di frame
  - To DS
  - From DS
- Indirizzi MAC
- Frame body
- FCS

Octets : 2	2	6	6	6	2	6	2	2	Variable	4
Frame Control	Duration \ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	QoS Control	HT Control	Frame Body	FCS

Bits : 2	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Power Mgmt	More Data	Prot. Frame	Order

# Indirizzi MAC

- Identificano unicamente una scheda di rete
- Suddivisi in due gruppi di ottetti:
  - OUI: Assegnato dall' IEEE
  - NIC: Scelto dal produttore
- Il primo ottetto determina:
  - Globally Assigned
  - Locally Assigned
  - Unicast
  - Multicast



# Analisi ed euristiche

---

- Gestione di indirizzi:
  - Globalmente assegnati / Localmente assegnati
  - Unicast / Multicast
- Euristiche:
  - Access Point
  - Repeater

# Lavori futuri

---

- Estendere il supporto di WiFi-Topology a reti professionali
  - Analisi dei frame destinati a Wireless Distribution Systems (WDS)
- Aggiunta di euristiche riguardanti canali Wi-Fi
- Calcolo di statistiche TCP
  - Perdita pacchetti
  - Pacchetti out of order
  - Ritrasmissioni
- Implementazione di tecniche per il service discovery
- Database di indirizzi MAC



# Conclusioni

---

- Sviluppo ed implementazione di una soluzione open-source
  - ArpScanner
  - WiFi-Topology
- Validata correttamente su diversi tipi di reti:
  - Semplici
  - Complesse
- Rilevamento specifico di nodi affetti da disservizi
- Contenuto utilizzo di risorse
- Estendibile a reti di tipo professionale

Grazie per l'attenzione