Dipartimento di Informatica

Rilevazione di disservizi nella connettività di rete

Candidato:
Daniel Casenove

Relatore:
Luca Deri

Motivazione

- Numero di dispositivi wireless connessi in aumento
- 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 rilevare disservizi

Analisi Wi-Fi: Stato dell'Arte

- Algoritmi per l'analisi del segnale Wi-Fi:
  - Qualità del segnale: SNR
  - Topologia: non presenti in letteratura
- Cattura del traffico di rete mediante standard monitor mode e radiotap
- Strumenti «simili»:
  - Netspot: heatmap di qualità del segnale Wi-Fi
  - UniFi by Ubiquiti: soluzione proprietaria per il monitoraggio di reti
  - Kismet: limitato al numero di client per AP e potenza del segnale

Analisi Wi-Fi: Limiti delle attuali soluzioni

1. Focus principale sullo stato dell'access point
   - Valori di bontà del segnale
   - Suggerimenti non real-time per un'ottimizzazione della connessione
2. Soluzione professionali e proprietarie non interoperabili: non utilizzabili in ambito domestico e SMB
3. Mancanza di una visione totale della rete e dei dispositivi ad essa connessi

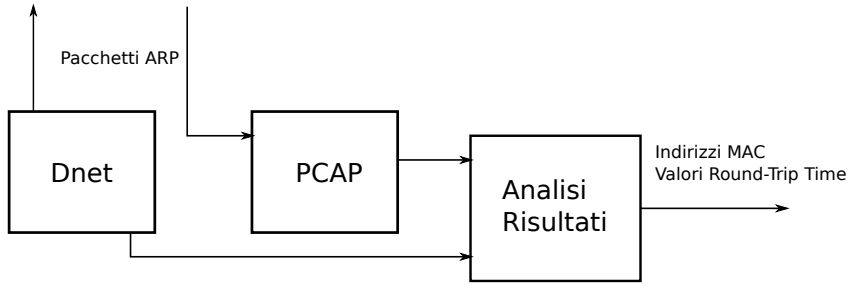
- Obiettivo del lavoro: fornire una soluzione per la rilevazione di disservizi in reti di tipo domestico e SMB

ArpScanner & Wi-Fi Topology
Risultati del Tirocinio

- Sviluppo di uno strumento per:
  - Analisi real-time del traffico della rete
    - Ricostruzione della topologia di rete a livello II
    - Misure della qualità del segnale
  - Monitoraggio dei dispositivi connessi alla rete
  - Identificazione dei nodi affetti da disservizi di connessione
  - Facile utilizzo e contenuto uso di risorse
  - Codice sorgente disponibile su GitHub
- Risultato originale:
  - Definizione di un algoritmo per la rilevazione della topologia di reti Wi-Fi totalmente passivo ed indipendente da un costruttore

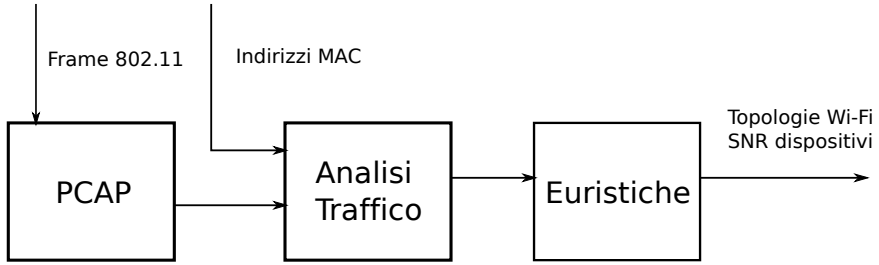
ArpScanner: Caratteristiche Principali

- 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: Caratteristiche Principali

- 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



WiFi-Topology: 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 ed euristiche: un nuovo algoritmo

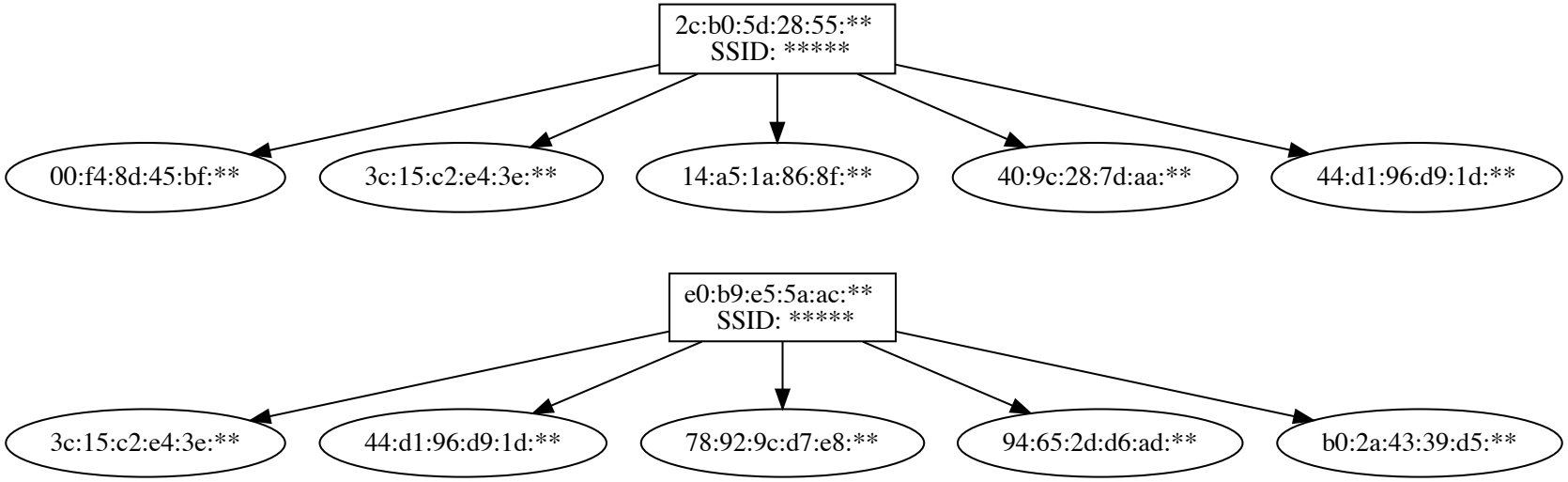
- Cattura di frame 802.11
  - Management frames
  - Control frames
  - Data frames
- Analisi di correttezza del frame ricevuto
- Aggiunta di relazioni tra indirizzi MAC che interagiscono:
  - Talker
  - Entry point
  - Exit point
- Identificazione di access point e repeater tramite euristiche su indirizzi MAC

Esempio di utilizzo WiFi-Topology

```
MAC Address: 70:4f:57:2e:2d:66 SSID: ntop Repeater Channel : 6 Signal : -46  Noise : -95
Device connessi:
00:80:8f:9a:ae:bd
28:57:be:e3:d7:cf
98:01:a7:a5:0c:93 *
MAC Address: d4:6e:0e:5d:4c:66 SSID: TP-LINK_5D4C66 Channel : 6 Signal : -96  Noise : -95
Device connessi:
MAC Address: b4:18:d1:e0:0e:ec SSID: ntop Home Channel : 6 Signal : -69  Noise : -95
Device connessi:
98:01:a7:a5:0c:93
70:4f:57:2e:2d:66
04:69:f8:58:09:51 *
10:13:31:f1:39:76 *
00:80:8f:9a:ae:bd *
28:57:be:e3:d7:cf *
MAC Address: 84:38:38:b4:3e:dd connesso a device MAC Address:  Signal : -94  Noise : -95
MAC Address: 04:71:4b:00:3d:8a connesso a device MAC Address:  Signal : -87  Noise : -95
MAC Address: 28:57:be:e3:d7:cf connesso a device MAC Address: b4:18:d1:e0:0e:ec Signal : -52  Noise : -95
MAC Address: 04:69:f8:58:09:51 connesso a device MAC Address: b4:18:d1:e0:0e:ec Signal : -26  Noise : -95
MAC Address: 98:01:a7:a5:0c:93 connesso a device MAC Address: 70:4f:57:2e:2d:66 Signal : -42  Noise : -95
MAC Address: 00:80:8f:9a:ae:bd connesso a device MAC Address: b4:18:d1:e0:0e:ec Signal : -51  Noise : -95
MAC Address: 10:13:31:f1:39:76 connesso a device MAC Address: b4:18:d1:e0:0e:ec tramite ethernet
```

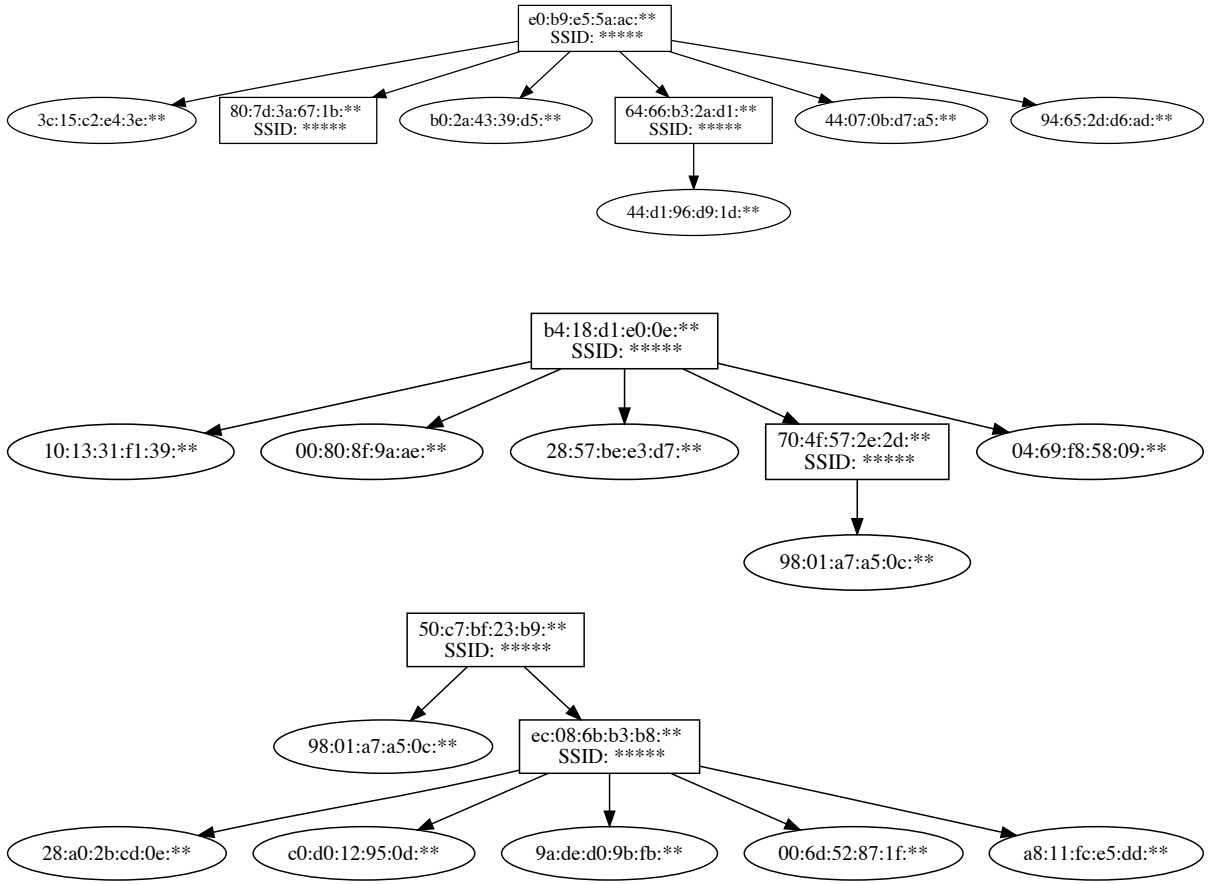
Validazione su reti con topologia semplice

- Rete casalinga o SMB
- Dispositivi direttamente collegati ad un access point
- Analisi validata dalla conoscenza della rete



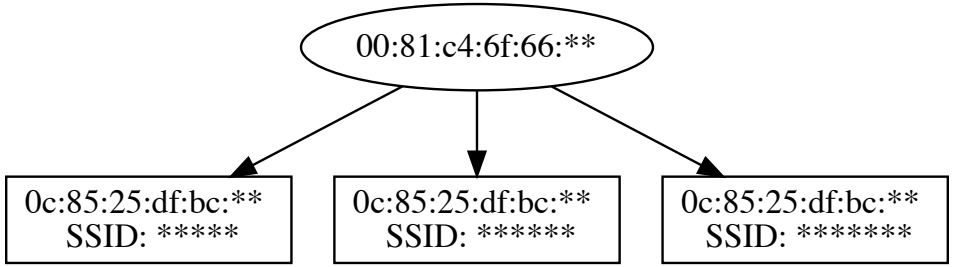
Validazione su reti con repeater

- 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 (Unipi, Area CNR di Pisa)
- Difficile da validare:
  - Alto numero di dispositivi
  - Topologia non conosciuta a priori



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
  - Cattura a line rate anche su reti con molti dispositivi
- Tempo di calcolo principalmente dovuto alla cattura
  - Cattura costante
  - Cattura programmata per una durata a scelta
- Soluzione implementabile su:
  - Router
  - Smartphone
  - SBC

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

- Definizione di un nuovo algoritmo per la rilevazione di topologie di reti Wi-Fi.
- 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

Grazie per l’attenzione

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

Octects : 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