UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO DI INFORMATICA (CREMA)

CORSO DI LAUREA IN SICUREZZA DEI SISTEMI E DELLE RETI INFORMATICHE

ANNO ACCADEMICO 2016/2017

Utilizzo di Software Defined Radio per effettuare analisi di sicurezza su protocolli di comunicazione wireless

Maurizio Agazzini (matricola 875237)

RELATORE **Prof. Claudio A. Ardagna**

CORRELATORE **Dott. Marco Anisetti**

Le comunicazioni wireless nel mondo odierno

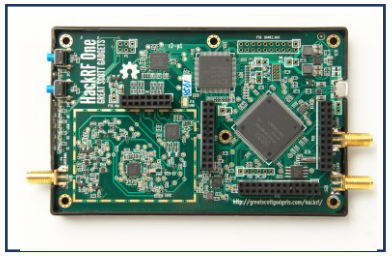
- Sempre più dispositivi utilizzano comunicazioni radio
- Le informazioni su come avvengono queste comunicazioni non sono pubbliche
- Come è possibile valutare la sicurezza di queste comunicazioni?

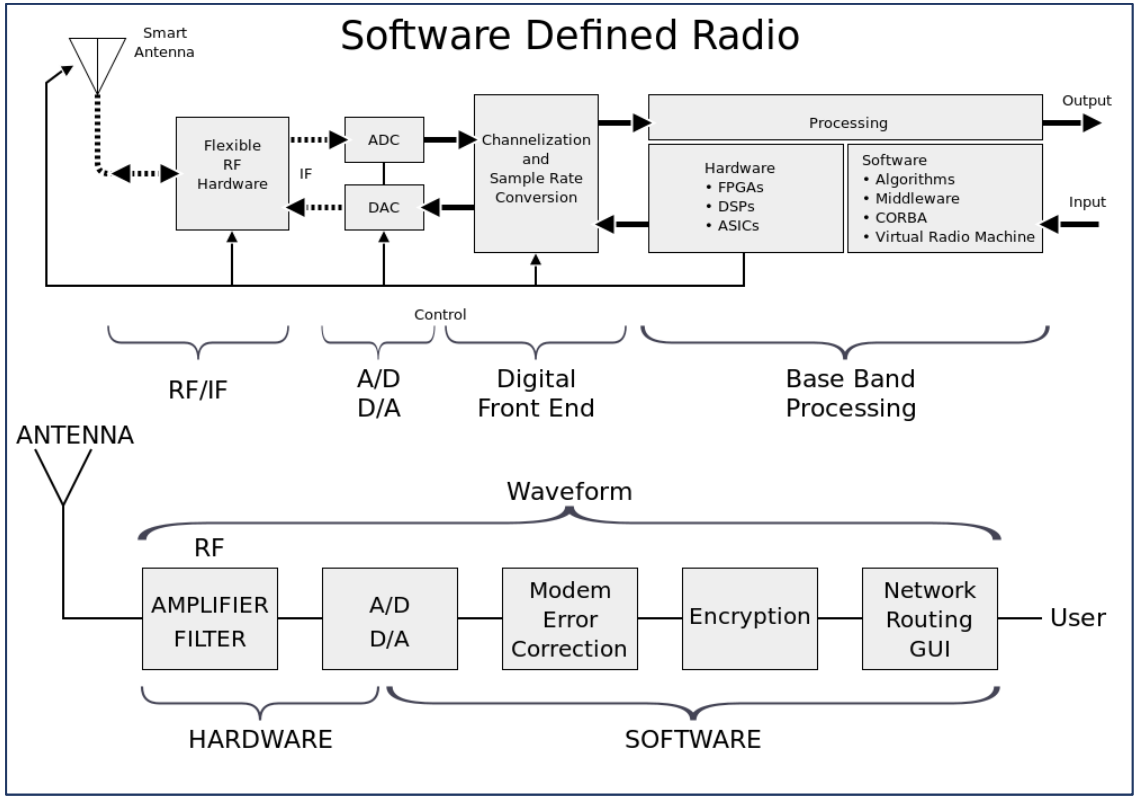
Problemi nell’analisi delle comunicazioni radio

- Necessario progettare hardware specifico
- Per poter progettare l’hardware è però necessario avere le specifiche di come avviene la comunicazione

Software Defined Radio (SDR)

- E’ possibile utilizzare le Software Defined Radio per effettuare analisi di sicurezza? Se sì, come?
- SDR - Hardware generico in cui il segnale “grezzo” viene passato a un processore programmabile o a un computer



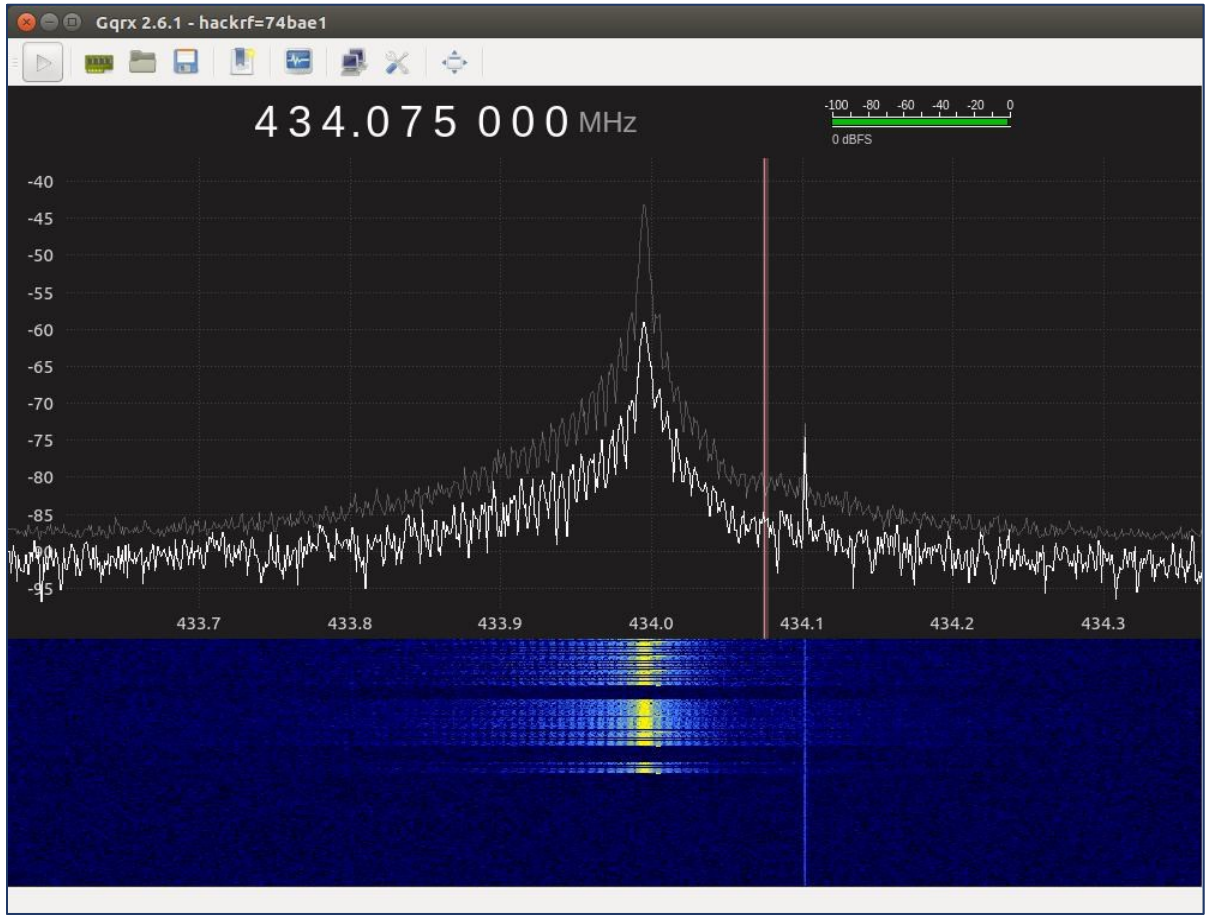


Quali problemi è necessario risolvere?

- Quale frequenza è utilizzata?
- Quale modulazione è utilizzata?
- Quali sono i timing della trasmissione?
- Quale encoding viene utilizzato?
- Come avviene la comunicazione a livello applicativo?

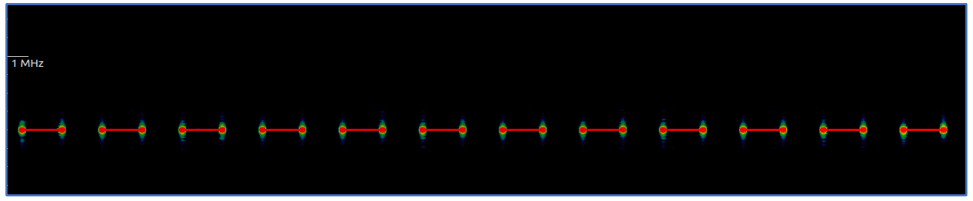
Identificazione delle frequenze utilizzate

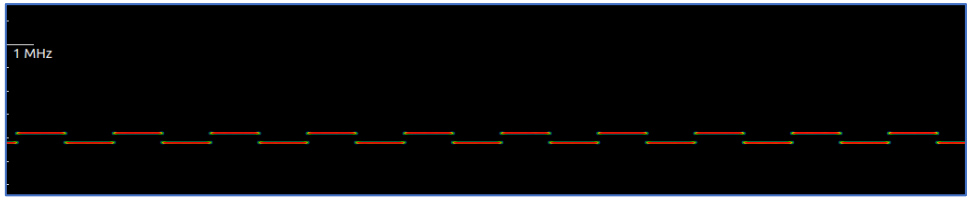
- Le SDR possono essere utilizzate come analizzatore di spettro per identificare in quali frequenze avvengono le trasmissioni



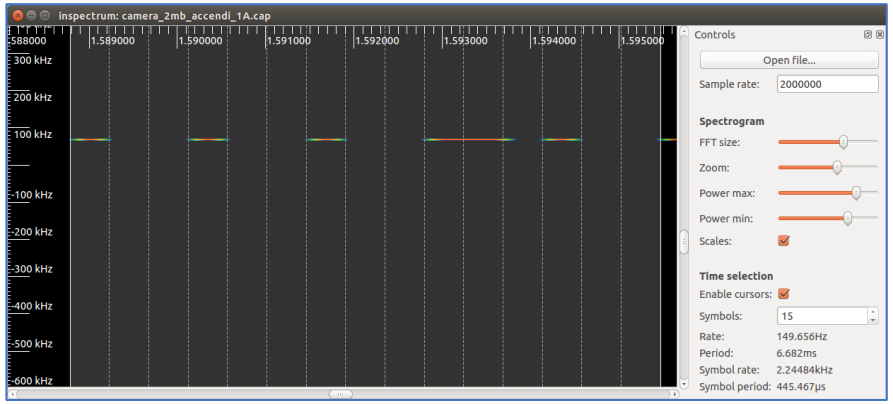
Modulazione e timing

- Effettuando un’analisi visuale del segnale è possibile identificare la modulazione utilizzata



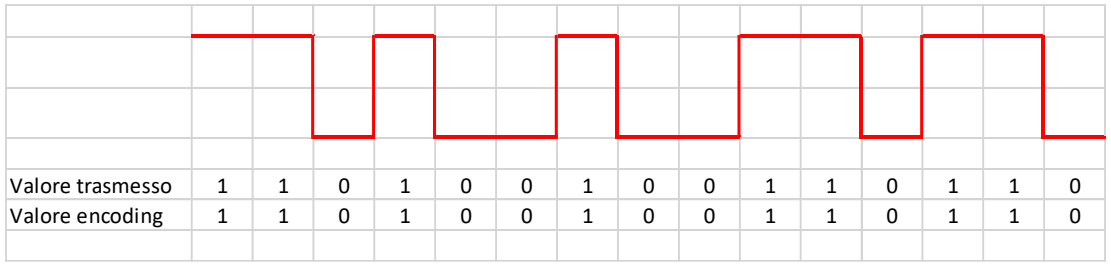


- E’ possibile utilizzare le SDR per analizzare i tempi di trasmissione

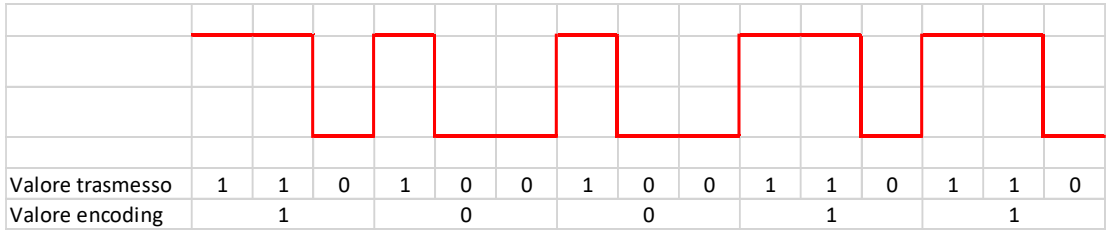


Encoding e decoding

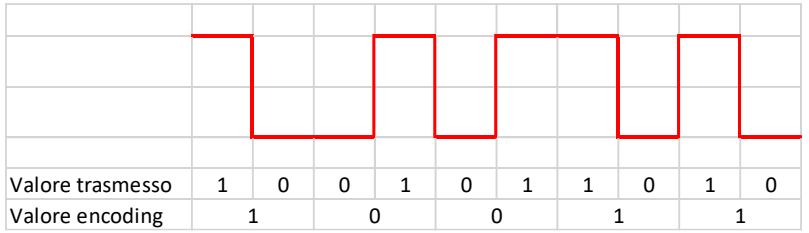
- Effettuando varie prove e analizzando le sequenze di dati estratti è possibile identificare quale encoding viene utilizzato



Valore trasmesso	1	1	0	1	0	0	1	0	0	1	1	0	1	1	0
Valore encoding	1	1	0	1	0	0	1	0	0	1	1	0	1	1	0



Valore trasmesso	1	1	0	1	0	0	1	0	0	1	1	0	1	1	0
Valore encoding		1			0			0			1			1	



Valore trasmesso	1	0	0	1	0	1	1	0	1	0
Valore encoding	1		0		0		1		1	

Possibili attacchi su protocolli radio

- Intercettazione
- Spoofing
- Replay attack
- Jamming
- Brute Force
- OpenSesame
- Rolljam
- Man In The Middle

Casi di studio

- Telecomando e presa elettrica
- Antifurto con telecomando
- Telecomando per apertura auto
- Sistema antifurto di ultima generazione

Sicurezza delle comunicazioni analizzate

Nel corso dello svolgimento del progetto sono stati sviluppati vari tool per effettuare comunicazioni e gli attacchi sui dispositivi selezionati come target.

	Presa 220v	Antifurto X10	Telecomando Fiat	Antifurto nuova generazione
Intercettazione	**Sì**	**Sì**	No	**Sì**
Spoofing	**Sì**	**Sì**	No	**Sì**
Replay attack	**Sì**	**Sì**	No	**Sì**
Jamming	**Sì**	**Sì**	Sì	Sì*
Brute force	**Sì**	**Sì**	Sì**	**Sì**
OpenSesame	N/A	N/A	N/A	N/A
RollJam	N/A	N/A	Sì	N/A
MITM	Sì	Sì	Sì	Sì

Conclusioni e lavori futuri

- Le SDR si sono rilevate un ottimo strumento per effettuare analisi di sicurezza su protocolli wireless
- I dispositivi analizzati per contro hanno dimostrato una scarsa attenzione alla sicurezza delle comunicazioni
- E’ possibile ipotizzare ulteriori lavori per analizzare comunicazioni differenti e più complesse concentrandosi in particolare sul layer applicativo