Tecnica di oscuramento del segnale radio con chiave crittografica basata su coordinate spaziali

- Stealth radio communication system with position cipher key -

Mario Marcovecchio

Università degli Studi di Firenze

March 12, 2012

Il presente lavoro indaga alcuni aspetti di un'attività di ricerca condotta dal prof. Del Re, dal prof. Mucchi e dall'Ing. Ronga presso l'UdR CNIT dell'Università degli Studi di Firenze

Crittografia

- Guerra continua tra crittografi e crittoanalisti

  $\Rightarrow$ in continua evoluzione

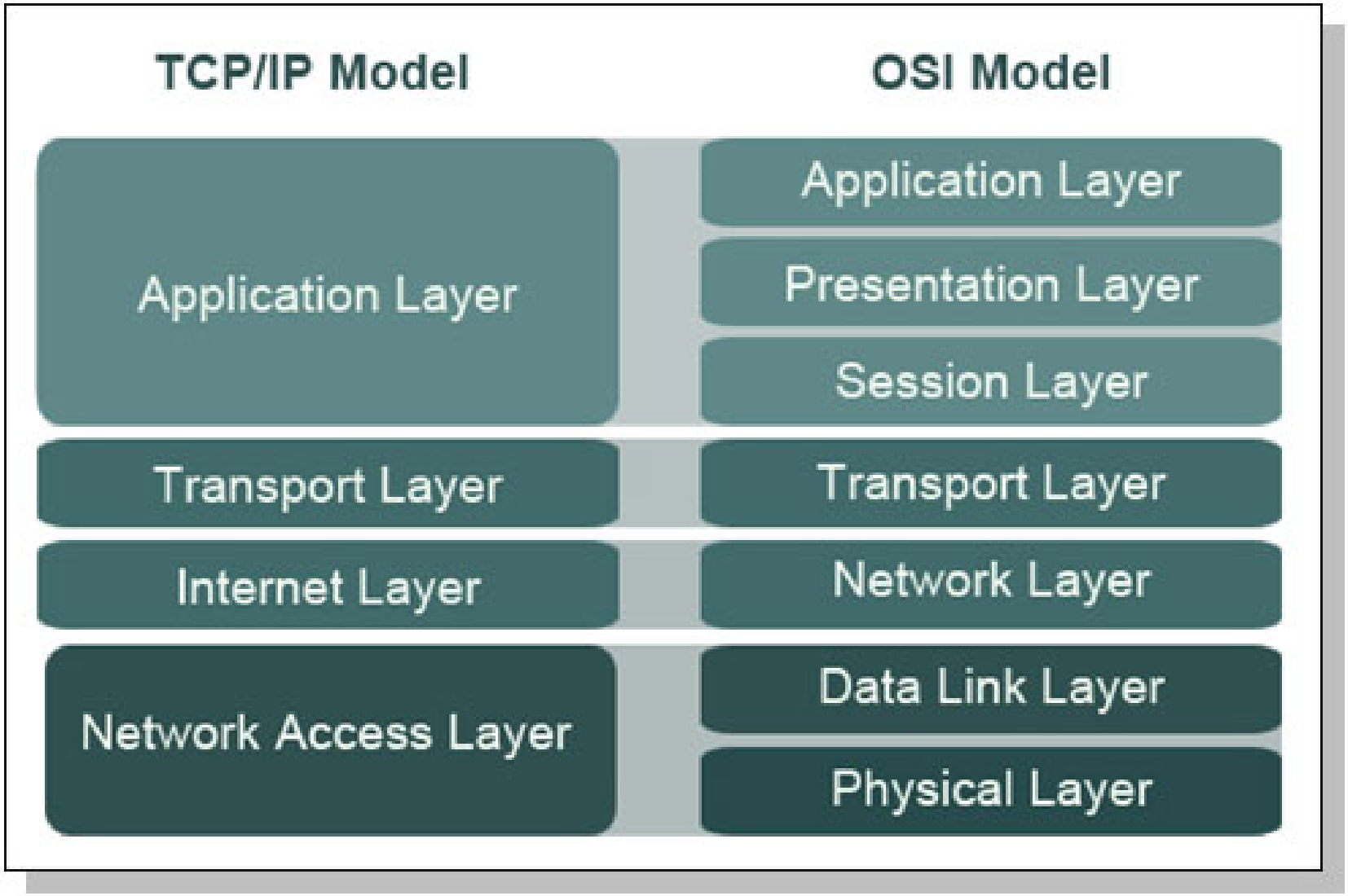
- Mancanza di un *canale sicuro*

  $\Rightarrow$ attacchi alla fase di scambio della chiave

- Non è un meccanismo intrinseco nel sistema

  $\Rightarrow$ rende un sistema potenzialmente **vulnerabile**

Sono necessarie nuove proposte per la sicurezza intrinseca


TCP/IP Model
OSI Model
Application Layer
Application Layer
Presentation Layer
Session Layer
Transport Layer
Transport Layer
Internet Layer
Network Layer
Network Access Layer
Data Link Layer
Physical Layer

Noise Loop Modulation

- L'informazione è legata al *rumore termico*
  - *Strettamente legato a quel preciso dispositivo*
  - *Modellabile come un processo stocastico*
- Struttura ad anello
- La corretta ricezione dipende dalla posizione dei terminali

Strumenti per l'analisi:

1. Proprietà stocastiche del rumore:

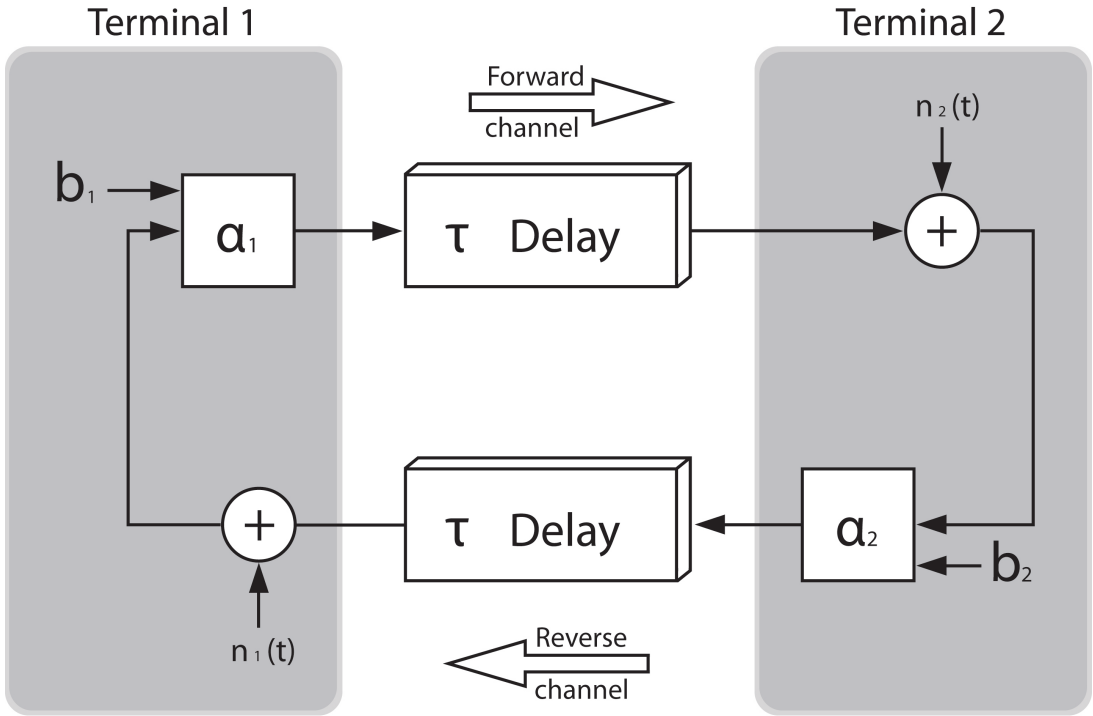
$$\mathbb{E}\left[e_i(t)e_j(t-m)\right] = \begin{cases} \sigma_n^2 & \text{se } i = j \quad , \quad m = 0 \\ 0 & \textit{altrimenti} \end{cases}$$

2. Modelli autoregressivi:

$$Y(t) = c + \sum_{i=1}^{p} \alpha_i Y(t-i) + e(t)$$

3. Equazioni di Yule-Walker:

$$R_{yy}(m) = \sum_{i=1}^{p} \alpha_i R_{yy}(m-i) + \delta_m \sigma_e^2$$



- $n_i(t)$ Rumore termico del terminale i; $n_i(t) \sim N(0, \sigma_n^2)$
- α_i Guadagno complessivo del link; $\alpha_i \in (0, 1)$
- b_i Bit trasmesso dal terminale i. $b_i \in [-1; +1]$
- $\tau_{12} = hT_c$ Ritardo di propagazione del link tra i terminali 1 e 2
- $y_i(t)$ Segnale ricevuto dal terminale i al tempo t

Analisi della catena di trasmissione:

1. Espressione dei segnali come modelli autoregressivi:

$$\begin{cases} y_1(n) &= n_1(n) + b_2\alpha_2 y_2(n-h) \\ y_2(n) &= n_2(n) + b_1\alpha_1 y_1(n-h) \end{cases}$$

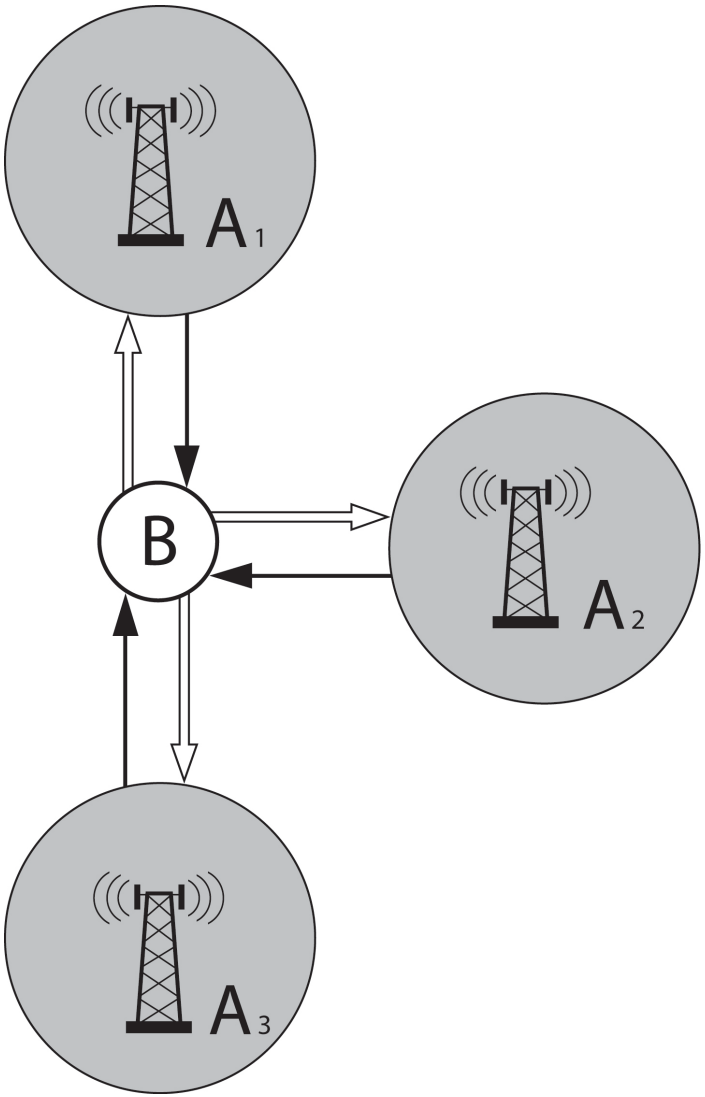
2. Espressione di $y_i(n)$ in termini di componenti di se stesso ritardate:

$$y_1(n) - b_1 b_2 \alpha_1 \alpha_2 y_1(n-2h) = n_1(n) + b_2\alpha_2 n_2(n-h)$$

3. Ottenimento dell'autocorrelazione di $y_i(n)$ attraverso le equazioni di Yule-Walker:

$$R_{y_1 y_1}(2h) = b_1 b_2 \frac{\alpha_1\alpha_2(1+\alpha_2^2)}{1-\alpha_1^2\alpha_2^2}\sigma_n^2$$

Advanced Noise Loop



- Sistema di stazioni $Alice$ centralizzato
- Può prevedere sincronizzazione tra le stazioni ($Synchronized$ A.N.L.)
- La chiave risiede nella posizione di B, determinata dai ritardi di propagazione
- Solo B demodula i segnali di $Alice$
- $R_{y_B y_B}(2h_i) = 0$ per h_i non multiplo dei ritardi τ_1, τ_2 o τ_3

- Demodulazione su B:

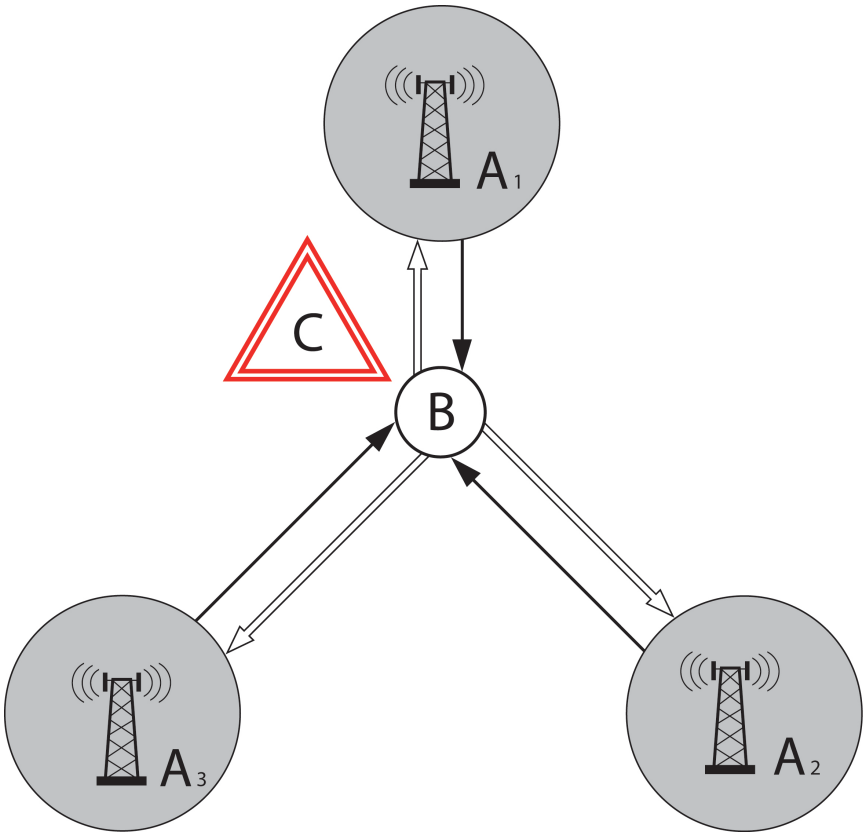
$$R_{y_B y_B}(2h_i) = \quad b_i b_B \quad \left(\frac{(\alpha_i \alpha_B)(1 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2)}{(1 - \alpha_1^2 \alpha_B^2 - \alpha_2^2 \alpha_B^2 - \alpha_3^2 \alpha_B^2)} \right) \sigma_n^2$$

- Demodulazione sulle stazioni $Alice$:

$$R_{y_i y_i}(2h_i) = \quad b_i b_B \quad \left(\frac{\alpha_i \alpha_B + \alpha_i \alpha_B^3}{1 - \alpha_i^2 \alpha_B^2} \right) \sigma_n^2$$

- Partendo dal segno di $b_1 R_{y_1 y_1}(2h)$, Bob ricava il segno di b_1 post-moltiplicando per il proprio bit b_B

Attacco all'Advanced Noise Loop



1. Intercettazione
   - uplink sincronizzato
   - uplink non sincronizzato
   - downlink sincronizzato
   - downlink non sincronizzato
   - up/down-link sincronizzato
   - up/down-link non sincronizzato
2. Denial of Service
   - attacco attivo uplink
   - attacco attivo downlink

- Ipotesi di attacco passivo in Up/Down-Link:

$$\begin{cases} y_i(n) &= n_i(n) + K_B y_B(n - h_i) \\ y_B(n) &= n_B(n) + \sum_{i=1}^{3} K_i y_i(n - h_i) \\ y_c(n) &= n_c(n) + \sum_{i=1}^{3} K_i y_i(n - h_{ci}) + K_B y_B(n - h_{Bc}) \end{cases}$$

- Autocorrelazione:

$$R_{y_c y_c}(2h_{Bc}) = \left(b_i b_B\right)^j \left(\frac{\left(\alpha_i^j \alpha_B^{j+4}\right)\left(1 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2\right)^2}{\alpha_B^2\left(\alpha_1^2 + \alpha_2^2 + \alpha_3^2\right)} \right) \sigma_n^2$$

- Risultato: l'attaccante non dispone di nessuno dei due bit per poter post-moltiplicare

$$\Rightarrow \quad \textbf{Il sistema è immune all'intercettazione}$$

Segnali sperimentati da terminale mobile e stazioni

- Ipotesi di attacco attivo in Uplink

$$\begin{cases} y_i(t) &= n_i(n) + K_B y_B(n - h_i) + K_c y_c(n - h_{ci}) \\ y_B(t) &= n_B(n) + \sum_{i=1}^{3} K_i y_i(n - h_i) \\ y_c(t) &= n_c(n) + \sum_{i=1}^{3} K_i y_i(n - h_{ci}) \end{cases}$$

- Ipotesi di attacco attivo in Downlink

$$\begin{cases} y_i(t) &= n_i(n) + K_B y_B(n - h_i) \\ y_B(t) &= n_B(n) + \sum_{i=1}^{3} K_i y_i(n - h_i) + K_c y_c(n - h_{Bc}) \\ y_c(t) &= n_c(n) + \sum_{i=1}^{3} K_i y_i(n - h_{ci}) + K_B y_B(n - h_{Bc}) \end{cases}$$

Bob e Alice, in presenza dell'attaccante, sperimentano:

- in uplink, se $h_{ci} \neq m h_i$

$$R_{y_i y_i}(2h_i) = b_i b_B \left(\frac{\alpha_i \alpha_B \sigma_e^2}{1 - K_{B1}^2 - K_{B2}^2 - K_{B3}^2 - K_{c1}^2 - K_{c2}^2 - K_{c3}^2} \right)$$

- in downlink, se $h_{Bc} \neq m h_i$

$$R_{y_B y_B}(2h_i) = b_i b_B \left(\frac{\alpha_i \alpha_B \sigma_e^2}{1 - \alpha_B^2 \alpha_1^2 - \alpha_B^2 \alpha_2^2 - \alpha_B^2 \alpha_3^2 - \alpha_B^2 \alpha_c^2} \right)$$

Conclusioni alla luce di quanto osservato:

1. la componente di sicurezza è un aspetto intrinseco nel funzionamento dell'*Advanced Noise Loop*
2. il sistema risulta completamente immune all'intercettazione
3. in pochi casi risulta possibile effettuare un disturbo sul solo terminale mobile, ma l'attaccante non riuscirebbe ad essere a conoscenza di averlo effettuato
4. può essere un buon candidato per lo scambio della chiave riuscendo a bypassare il problema del canale sicuro