Security and Cooperation in Wireless Networks

http://secowinet.epfl.ch/

Chapter 5: Establishment of security associations

key establishment in sensor networks;

key establishment in ad hoc networks exploiting

- physical contact
- vicinity
- node mobility;

revocation;

Chapter outline

5.1 Key establishment in sensor networks
5.2 Exploiting physical contact
5.3 Exploiting mobility
5.4 Exploiting the properties of vicinity and of the radio link
5.5 Revocation

Exploiting physical contact

- target scenarios
  - modern home with multiple remotely controlled devices
    - DVD, VHS, HiFi, doors, air condition, lights, alarm, …
  - modern hospital
    - mobile personal assistants and medical devices, such as thermometers, blood pressure meters, …
- common in these scenarios
  - transient associations between devices
  - physical contact is possible for initialization purposes
- the ***resurrecting duckling*** security policy
  - at the beginning, each device has an empty *soul*
  - each empty device accepts the first device to which it is physically connected as its master (imprinting)
  - during the physical contact, a device key is established
  - the master uses the device key to execute commands on the device, including the *suicide* command
  - after suicide, the device returns to its empty state and it is ready to be imprinted again

Chapter outline

5.1 Key establishment in sensor networks
5.2 Exploiting physical contact
5.3 Exploiting mobility
5.4 Exploiting the properties of vicinity and of the radio link
5.5 Revocation

Exploiting vicinity

- problem
  - how to establish a shared key between two PDAs?
- assumptions
  - no CA, no KDC
  - PDAs can use short range radio communications (e.g., Bluetooth)
  - PDAs have a display
  - PDAs are held by human users
- idea
  - use the Diffie-Hellman key agreement protocol
  - ensure key authentication by the human users

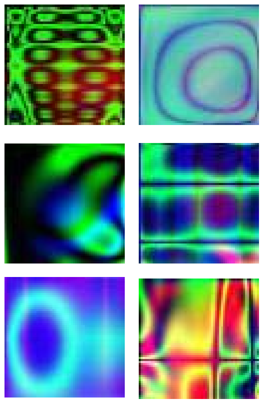
Diffie-Hellman with String Comparison

Alice		Bob
Given ID_A, g^{X_A}		Given ID_B, g^{X_B}
Pick $N_A \in_U \{0,1\}^k$		Pick $N_B \in_U \{0,1\}^k$
$m_A \leftarrow 0 \| ID_A \| g^{X_A} \| N_A$		$m_B \leftarrow 1 \| ID_B \| g^{X_B} \| N_B$
$(c_A, d_A) \leftarrow \text{commit}(m_A)$		$(c_B, d_B) \leftarrow \text{commit}(m_B)$
	$\xrightarrow{c_A}$	
	$\xleftarrow{c_B}$	
	$\xrightarrow{d_A}$	$\hat{m}_A \leftarrow \text{open}(\hat{c}_A, \hat{d}_A)$
$\hat{m}_B \leftarrow \text{open}(\hat{c}_B, \hat{d}_B)$	$\xleftarrow{d_B}$	Verify 0 in $\hat{m}_A$; $i_B \leftarrow N_B \oplus \hat{N}_A$
Verify 1 in $\hat{m}_B$; $i_A \leftarrow N_A \oplus \hat{N}_B$		

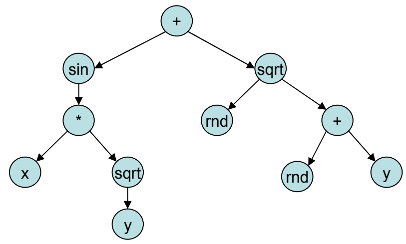
If $i_A = i_B$, Alice and Bob output "Accept" $\hat{m}_B$ and $\hat{m}_A$, respectively.

theorem: the probability that an attacker succeeds against the above protocol is bounded by $n\gamma 2^{-k}$, where n is the total number of users, γ is the maximum number of sessions that any party can participate in, and k is the security parameter

Application of Random Art images



- random value is converted into three two-variable functions
  - each can be represented as a tree



- these formulae define the color value of each pixel of the resulting image

Is it possible to rely on the radio channel only?

- a solution: Integrity Codes
- assumption
  - it is possible to implement a channel with the following property:
    - bit 0 can be turned into bit 1
    - bit 1 cannot be turned into bit 0
  - an example:
    - bit 1 = presence of random signal (~noise)
    - bit 0 = no signal at all
- i(ntegrity)-codes
  - each codeword has the same number of 0s and 1s
  - such a codeword cannot be modified in an unnoticeable way
  - encoding messages with i-codes ensures the integrity of the communications → Man-in-the-Middle is excluded

Shake them up!

- create common security context by shaking two devices together
  - needs accelerometers in the devices (modern phones and PDAs are equipped with lot of sensors)
  - it is possible to reliably distinguish the case when two devices move together from the case when they both move but not together

- protocol:
  - use Diffie-Hellman to set up a key K between A and B
  - shake them up → acceleration sequences a and b
  - A encrypts a with K, B encrypts b with K
  - they exchange the cryptograms using the Interlock protocol
    - first exchange first half of all ciphertext blocks
    - then exchange second half of all ciphertext blocks
  - MitM is thwarted because the first halves alone cannot be decrypted!

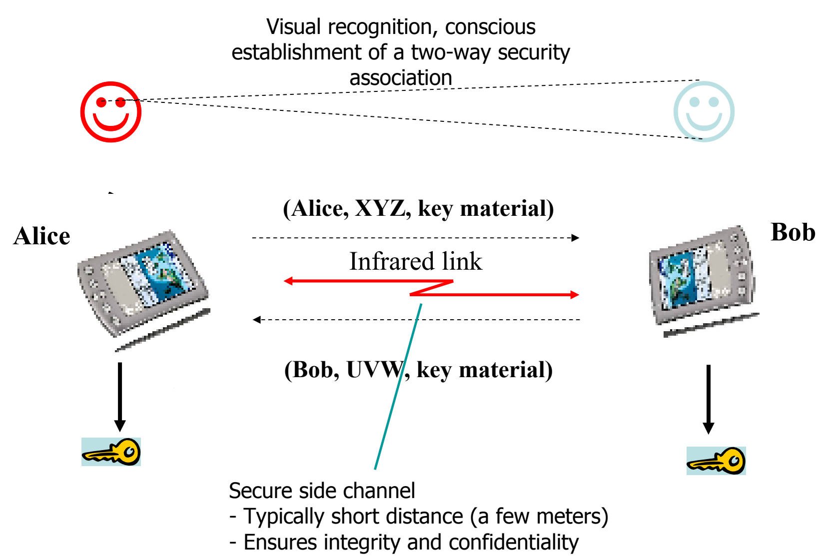
Chapter outline

5.1 Key establishment in sensor networks
5.2 Exploiting physical contact
5.3 Exploiting mobility
5.4 Exploiting the properties of vicinity and of the radio link
5.5 Revocation

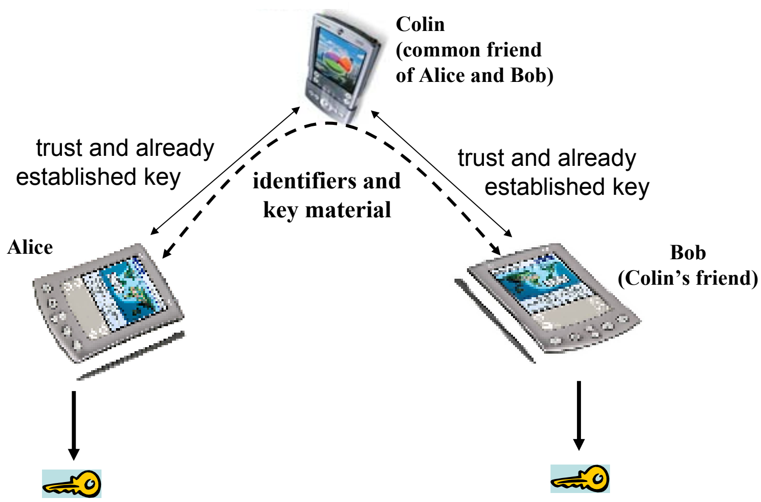
Does mobility increase or reduce security ?

- Mobility is usually perceived as a major security challenge in networking
  - Wireless communications
  - Sporadic availability of the user/node
  - Higher vulnerability of the device
  - Reduced computing capability of the devices
- However, in real life, people often move (and gather) to increase security
  - Face to face meetings
  - Transport of assets and documents
  - Authentication by physical presence
- Can we take advantage of mobility to increase security in networking?
- Yes, we can, assuming that
  - nodes are operated by humans
  - when in the vicinity of each other, nodes can use a ***secure side channel*** (e.g., infra red) to exchange a key
  - each node has some ***friends*** (peers that are trusted by the node), and there is already a key shared between each pair of friends

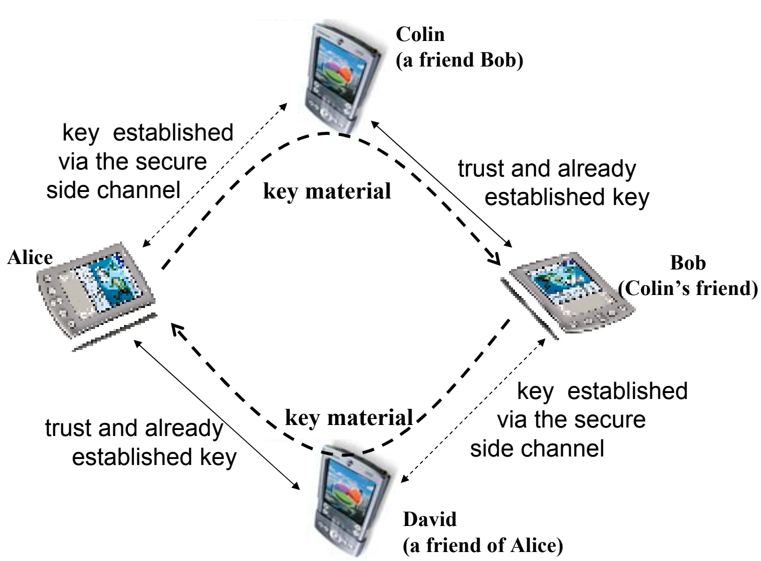
Exploiting vicinity and the secure side channel



Taking advantage of common friends



What if there's no common friend?



A possible implementation

$$
\begin{array}{l}
\text{msg1 } u \rightarrow v : f, r_u \\
\text{msg2 } v \rightarrow u : g, r_v \\
\text{msg3 } u \rightarrow g : u, \{d_{u\rightarrow g}, req, v, k_u, r_v\}k_{ug} \\
\text{msg4 } g \rightarrow v : g, \{d_{g\rightarrow v}, rep, u, k_u, r_v\}k_{vg} \\
\text{msg3}' \ v \rightarrow f : v, \{d_{v\rightarrow f}, req, u, k_v, r_u\}k_{vf} \\
\text{msg4}' \ f \rightarrow u : f, \{d_{f\rightarrow u}, rep, v, k_v, r_u\}k_{uf} \\
\qquad u, v \ : k_{uv} = h(k_u, k_v)
\end{array}
$$

- notes:
  - single trusted party is replaced with two parties trusted by one entity each
  - if f and g are not colluding, then they cannot compute kuv
  - both u and v trust at least one of f and g for not colluding

Pace of establishment of the security associations

- **Depends on several factors:**
  - Area size
  - Number of communication partners: *s*
  - Number of nodes: *n*
  - Number of friends
  - Mobility model and its parameters (speed, pause times, …)

Desired security associations :
p_{ij} = 1, if i and j wants to setup a shared key, and 0 otherwise

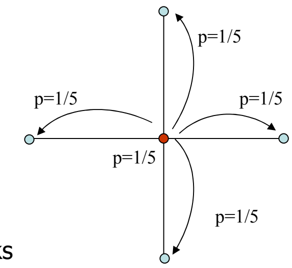
Established security associations :
$e_{ij}(t)$ = 1, if at time t nodes i and j already share a key, and 0 otherwise

Convergence : $$r(t) = \frac{\sum_{i,j} e_{ij}(t) \cdot p_{ij}}{\sum_{i,j} p_{ij}}$$

and the convergence time t_M is the earliest time at which $r(t) = 1$.

Mobility models

- Random walk
  - discrete time
  - simple, symmetric random walk
  - **area:** Bounded and toroid grids (33x33, 100x100, 333x333)
  - **number of nodes:** 100

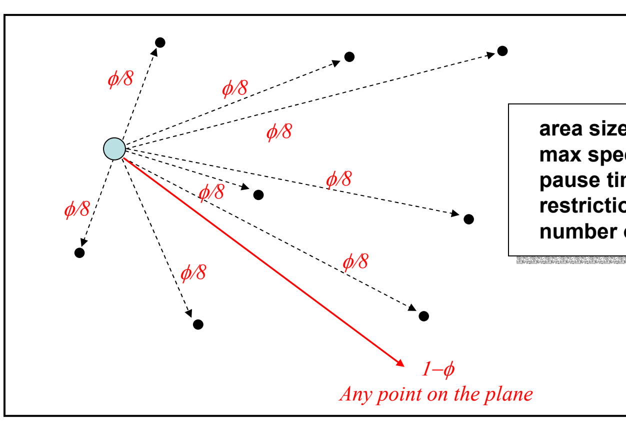


- Random waypoint
  - most commonly used in mobile ad hoc networks
  - continuous time
  - **area size:** 1000m x1000m
  - **max speed:** 5m/s, 20m/s
  - **pause time:** 5s, 100s, 200s
  - **security power range**: 5m (SSC), 50m 100m (radio)

- Common simulation settings
  - simulations are run 20 times
  - confidence interval: 95%

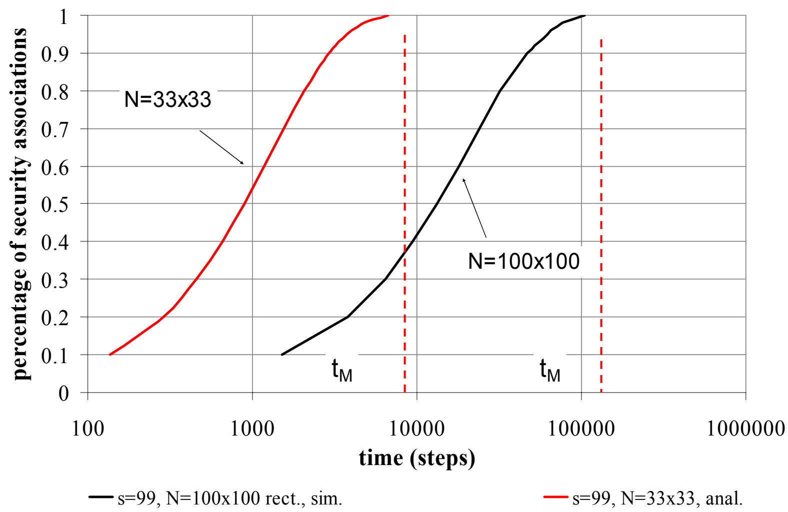
(Restricted) random waypoint

- Restricts the movement of nodes to a set of points with a predefined probability ϕ
- Regular random waypoint is a special case ($\phi = 0$)



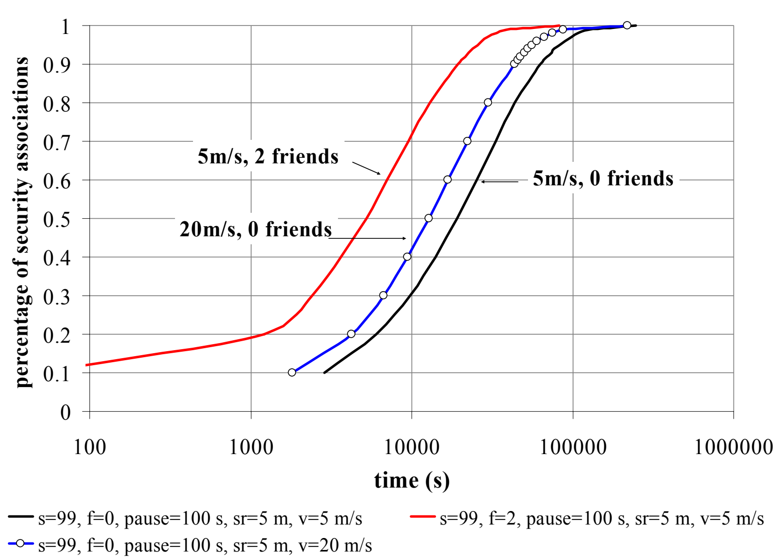
area size: 1000m x1000 m
max speed: 5m/s, 20m/s
pause time: 5s, 100s, 200s
restriction probability: 0.1, 0.5, 1
number of restriction points: 20

Size matters

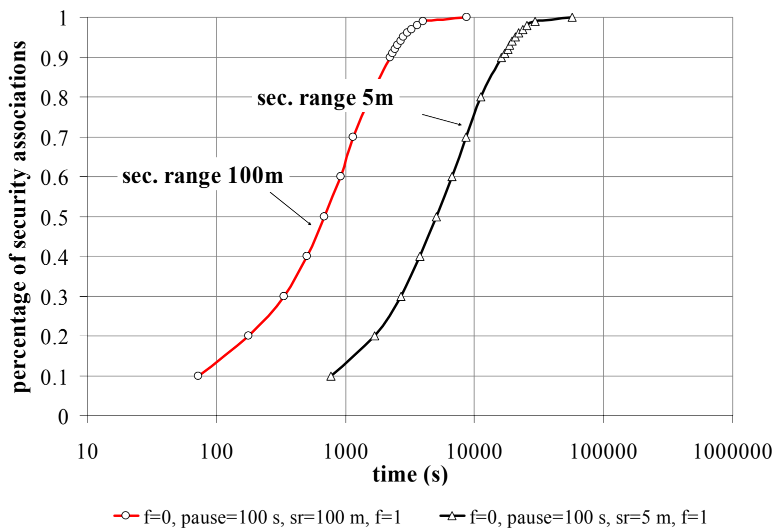


$t_M = O(N \log N)$

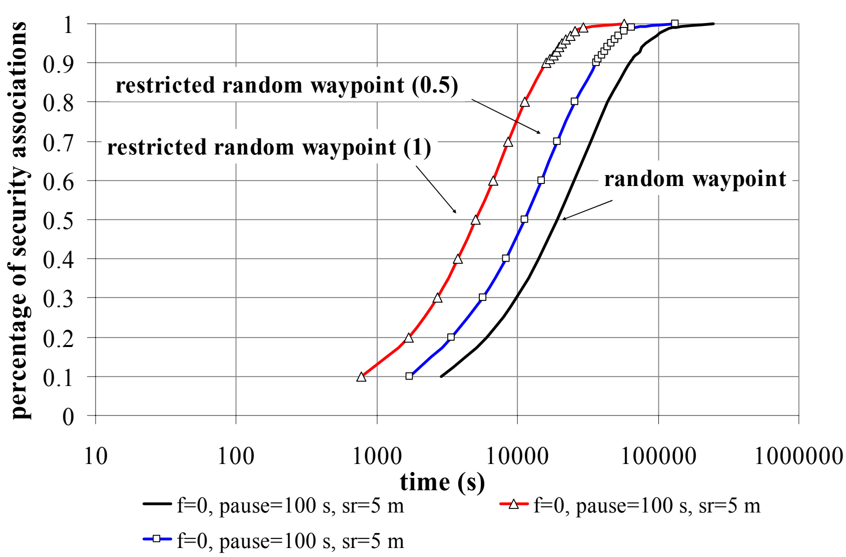
Friends help



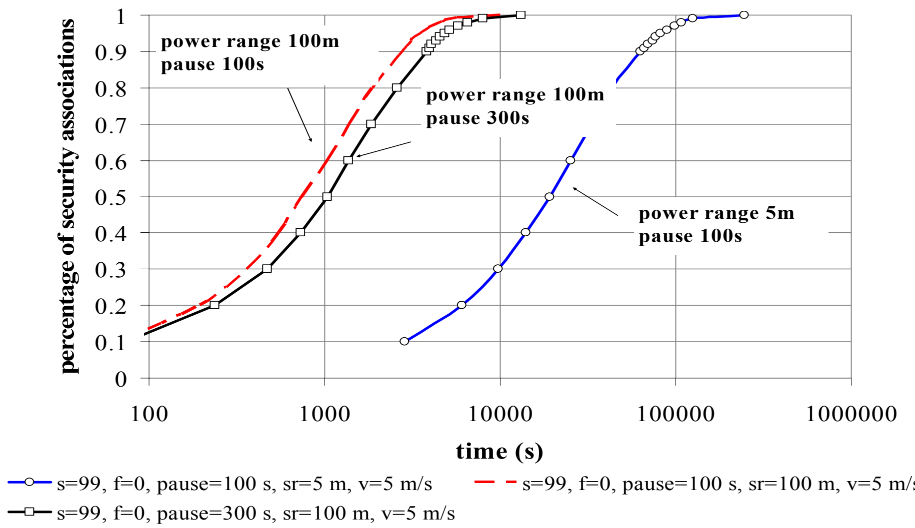
Security range matters



Meeting points help



Pause time



Summary

- it is possible to establish pairwise shared keys in ad hoc networks without a globally trusted third party
- mobility, secure side channels, and friends are helpful
- stuff useful in general
  - Random Art
  - Integrity Codes
  - DH with Interlock