Attacks on neighbor discovery

Cryptographic Protocols (EIT ICT MSc)

Dr. Levente Buttyán
associate professor
BME Hálózati Rendszerek és Szolgáltatások Tanszék
Lab of Cryptography and System Security (CrySyS)
butteryan@hit.bme.hu, butteryan@crys.hu
Neighbor discovery

- many wireless networking mechanisms require that the nodes be aware of their neighborhood

- a simple neighbor discovery protocol:
  - every node broadcasts a neighbor discovery request
  - each node that hear the request responds with a neighbor discovery reply
  - messages carry node identifiers → neighboring nodes discover each other’s ID

- an adversary may try to thwart the execution of the protocol
  - prevent two neighbors to discover each other by jamming
  - create a neighbor relationship between far-away nodes
    - by spoofing neighbor discovery messages (can be prevented by message authentication techniques)
    - by installing a *wormhole* (cannot be prevented by cryptographic techniques alone)
What is a wormhole?

- a wormhole is an out-of-band connection, controlled by the adversary, between two physical locations in the network
  - the adversary installs radio transceivers at both ends of the wormhole
  - it transfers packets (possibly selectively) received from the network at one end of the wormhole to the other end via the out-of-band connection, and re-injects the packets there into the network

- notes:
  - the adversary’s transceivers are not regular nodes (no node is compromised by the adversary)
  - adversary doesn’t need to understand what it tunnels (e.g., encrypted packets can also be tunneled through the wormhole)
  - it is easy to mount a wormhole, but it may have devastating effects on routing
Effects of a wormhole

- at the data link layer: distorted network topology

- at the network layer:
  - routing protocols may choose routes that contain wormhole links
    - typically those routes appear to be shorter
    - flooding based routing protocols (e.g., DSR, Ariadne) may not be able to discover other routes but only through the wormhole
  - adversary can then monitor traffic or drop packets (DoS)
Wormholes in another context

- Access control system: gate equipped with contactless smart card reader
- Contactless smart card
- Contactless smart card emulator
- Fast connection
- Smart card reader emulator
- Wormhole
- User may be far away from the building

© Buttyán Levente, BME HIT
Budapesti Műszaki és Gazdaságtudományi Egyetem
Classification of detection methods

- centralized mechanisms
  - data collected from the local neighborhood of every node are sent to a central entity
  - based on the received data, a model of the entire network is constructed
  - the central entity tries to detect inconsistencies (potential indicators of wormholes) in this model
  - can be used in sensor networks, where the base station can play the role of the central entity

- decentralized mechanisms
  - each node constructs a model of its own neighborhood using locally collected data
  - each node tries to detect inconsistencies on its own
  - advantage: no need for a central entity (fits well some applications)
  - disadvantage: nodes need to be more complex
Statistical wormhole detection

- each node reports its list of believed neighbors to the base station
- the base station reconstructs the connectivity graph (model)
- *a wormhole always increases the number of edges* in the connectivity graph
- this increase may change the properties of the connectivity graph in a detectable way (anomaly)
- detection can be based on statistical hypothesis testing methods (e.g. the $\chi^2$-test)
Examples

- a wormhole that creates many new edges may increase the *number of neighbors* of the affected nodes
  - distribution of node degrees will be distorted

- a wormhole is usually a shortcut that decreases the length of the shortest paths in the network
  - distribution of the length of the shortest paths will be distorted
Multi-dimensional scaling

- the nodes not only report their lists of neighbors, but they also estimate (inaccurately) their distances to their neighbors

- connectivity information and estimated distances are input to a multi-dimensional scaling (MDS) algorithm

- the MDS algorithm tries to determine the possible position of each node in such a way that the constraints induced by the connectivity and the distance estimation data are respected
  - the algorithm has a certain level of freedom in “stretching” the nodes within the error bounds of the distance estimation

- let us suppose that an adversary installed a wormhole in the network
  - if the estimated distances between the affected nodes are much larger than the nodes’ communication range, then the wormhole is detected
  - hence, the adversary must also falsify the distance estimation \( \rightarrow \) distances between far-away nodes become smaller
  - this will result in a distortion in the virtual layout constructed by the MDS algorithm
Examples

- in 1D:
  
  ![Connectivity Graph and Reconstructed Virtual Layout](image1)

- in 2D:
  
  ![Wormhole in 2D](image2)
Packet leashes

- packet leashes ensure that packets are not accepted “too far” from their source

- geographical leashes
  - each node is equipped with a GPS receiver
  - when sending a packet, the node puts its GPS position into the header
  - the receiving node verifies if the sender is really within communication range

- temporal leashes
  - nodes’ clocks are very tightly synchronized
  - when sending a packet, the node puts a timestamp in the header
  - the receiving node estimates the distance of the sender based on the elapsed time and the speed of light
    \[ d_{est} < v_{light}(t_{rcv} - t_{snd} + \Delta_t) \]
  - note: \( v_{light} \Delta_t \) must be much smaller than the communication range
idea: authentication delay of TESLA can be removed in an environment where the nodes’ clocks are tightly synchronized

- by the time the sender reveals the key, the receiver has already received the MAC
- security condition: $t_r < t_s - \Delta t + \tau_{pkt}$
- note: $\Delta t$ must be very small or otherwise packets must be very long
Mutual Auth with Distance-bounding

--- initialization phase ---

$u$  
\[
\begin{align*}
generate \text{ random numbers } r \in \{0, 1\}^\ell, r' \in \{0, 1\}^\ell' \\
compute \text{ commitment } c_u &= H(r|r') \\
\end{align*}
\]

$v$
\[
\begin{align*}
generate \text{ random numbers } s \in \{0, 1\}^\ell, s' \in \{0, 1\}^\ell' \\
compute \text{ commitment } c_v &= H(s|s') \\
\end{align*}
\]

\[
\begin{align*}
c_u &\rightarrow c_v \\
c_v &\rightarrow c_u \\
\end{align*}
\]

--- distance-bounding phase ---

the bits of $r$ are $r_1, r_2, \ldots, r_\ell$
\[
\alpha_1 = r_1 \\
\alpha_1 \rightarrow \eta_1 \\
\beta_1 = s_1 \oplus \alpha_1 \\
\beta_1 \rightarrow \eta_1 \\
\]

measure delay between $\alpha_i$ and $\beta_i$
\[
\begin{align*}
\alpha_i &= r_i \oplus \beta_{i-1} \\
\alpha_i \leftarrow \eta_i \\
\beta_i &= s_i \oplus \alpha_i \\
\beta_i \leftarrow \eta_i \\
\end{align*}
\]

measure delay between $\alpha_\ell$ and $\beta_\ell$
\[
\begin{align*}
\alpha_\ell &= r_\ell \oplus \beta_{\ell-1} \\
\alpha_\ell \leftarrow \eta_\ell \\
\beta_\ell &= s_\ell \oplus \alpha_\ell \\
\beta_\ell \leftarrow \eta_\ell \\
\end{align*}
\]

--- authentication phase ---

\[
\begin{align*}
\mu_u &= mac_{k_{uv}}(u|v|r_1|s_1|\ldots|r_\ell|s_\ell) \\
\mu_v &= mac_{k_{uv}}(v|u|s_1|r_1|\ldots|s_\ell|r_\ell) \\
\end{align*}
\]

\[
\begin{align*}
\eta' | \mu_u &\rightarrow s' | \mu_v \\
\eta | \mu_v &\rightarrow s' | \mu_u \\
\end{align*}
\]

verify $c_v$ and $\mu_v$ verify $c_u$ and $\mu_u$

- MAD allows precise distance estimation without synchronized clocks
Using anchors

- anchors are special nodes that know their own positions (GPS)
- there are only a few anchors randomly distributed among regular nodes
- two nodes consider each other neighbors only if
  - they hear each other and
  - they hear more than $T$ common anchors
- anchors put their location data in their messages
- transmission range of anchors ($R$) is larger than that of regular nodes ($r$)
- wormholes are detected based on the following two principles:
  1. a node should not hear two anchors that are $2R$ apart from each other
  2. a node should not receive the same message twice from the same anchor
Principle 1

- $x$ hears anchors in $A_x$ and in $A_O$
- $P_1$ is the probability that it hears two anchors that are farther away from each other than $2R$
- The probability that there is at least one anchor in an area of size $S$ is $(1-e^{-\lambda^*S})$, where $\lambda^*$ is the density of anchors
- $P_1 \geq (1-e^{-\lambda^*S'_x})(1-e^{-\lambda^*S'_O})$, where $S'_x$ is the size of $A'_x$ and $S'_O$ is the size of $A'_O$
- This lower bound is maximum when $S'_x = S'_O$
Principle 2

- when x and O are closer than \(2R\), the discs \(A_x\) and \(A_O\) overlap
- if there is an anchor in the intersection \(A_{xO}\), then the messages of that anchor is heard twice by \(x\)
  - first directly and then from transceiver D who receives it from O through the wormhole
- the probability \(P_2\) of detection is equal to the probability that there is at least one anchor in \(A_{xO}\)
- \(P_2 = 1 - e^{-\lambda S_{xO}}\)
Summary on wormhole detection

- A wormhole is an out-of-band connection, controlled by the adversary, between two physical locations in the network.
- A wormhole distorts the network topology and may have a profound effect on routing.
- Wormhole detection is a complicated problem.
  - Centralized and decentralized approaches
  - Statistical wormhole detection
  - Wormhole detection by multi-dimensional scaling and visualization
  - Packet leashes
  - Distance bounding techniques
  - Anchor assisted wormhole detection
  - Many approaches are based on strong assumptions
    - Tight clock synchronization
    - GPS equipped nodes
    - ...
- Wormhole detection is still an active research area.