Security and Privacy in Wireless Networks

Mohammad Hossein Manshaei
manshaei@gmail.com

Chapter 6: (secowinet.epfl.ch)

the wormhole attack, centralized and decentralized wormhole detection mechanisms.

SECURING NEIGHBOR DISCOVERY

Introduction

- 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)

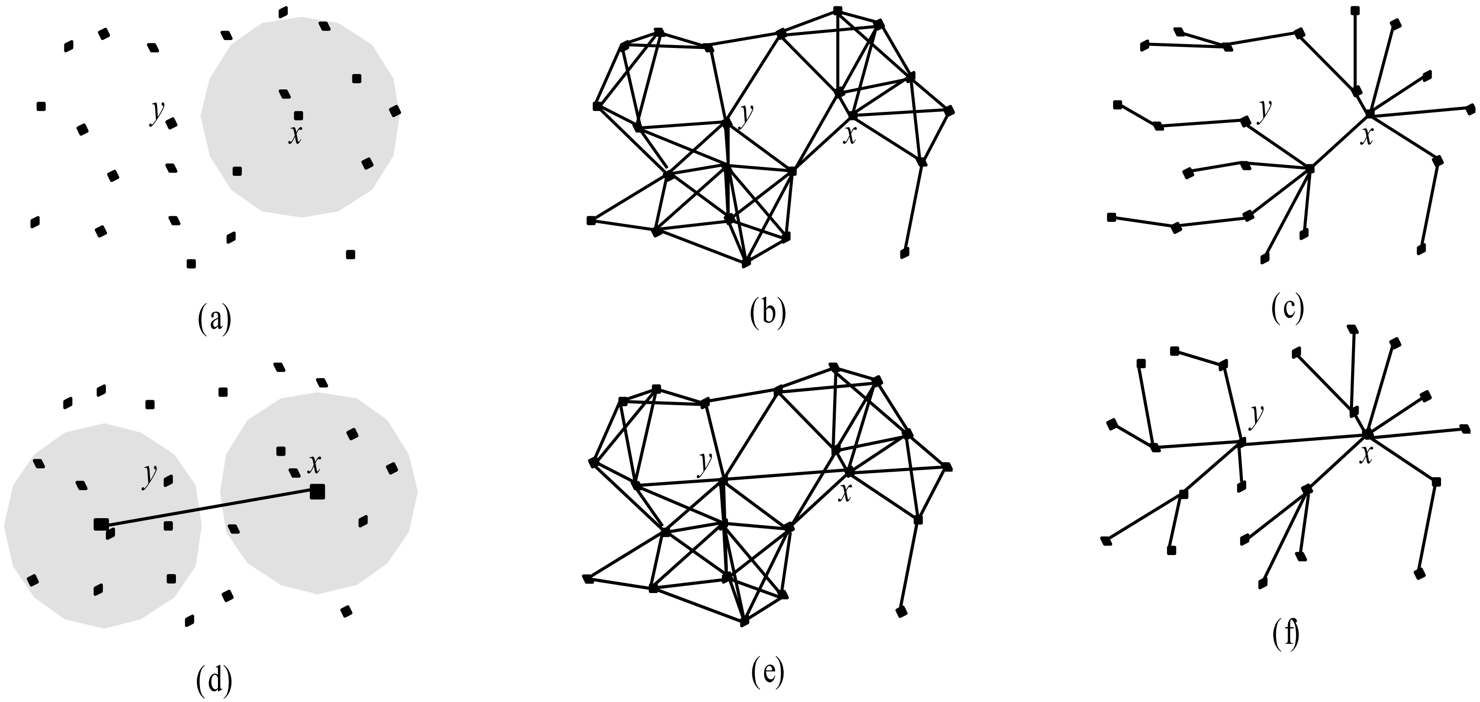
What is a wormhole?

- 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:
  - 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 and it may have devastating effects on routing

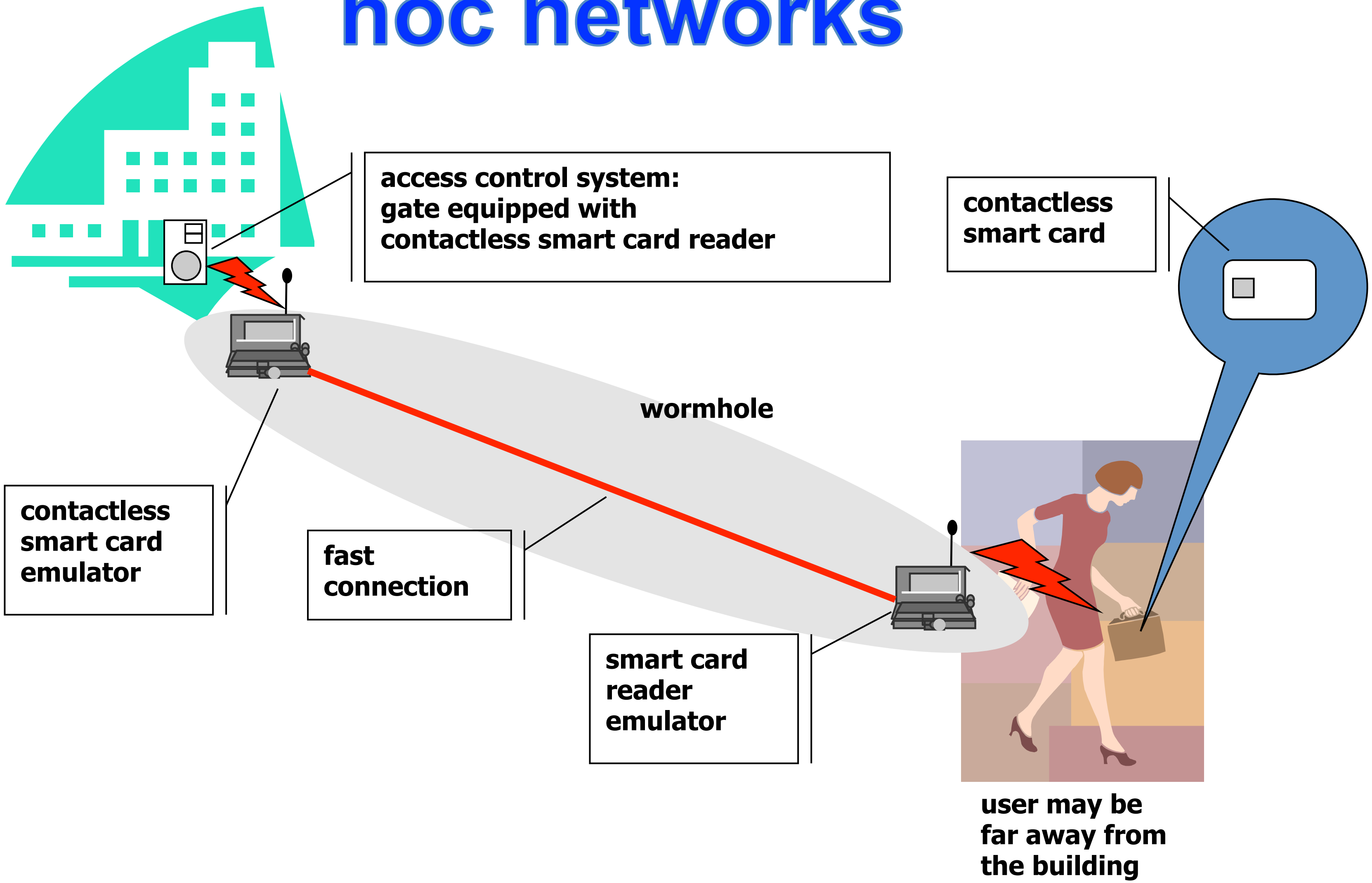
Effects of a wormhole

- 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 are not specific to ad hoc networks



Classification of Wormhole 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

Centralized Approaches to Detect Wormhole

1. Statistical Wormhole Detection
2. Multi-dimensional Scaling

Statistical Wormhole Detection in Sensor Networks

- 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 χ^2-test)

Statistical Wormhole Detection in Sensor Networks

- The probability that a node has exactly *k* neighbors

$$p(k) = \binom{n-1}{k} \cdot q^k \cdot (1-q)^{n-1-k}$$

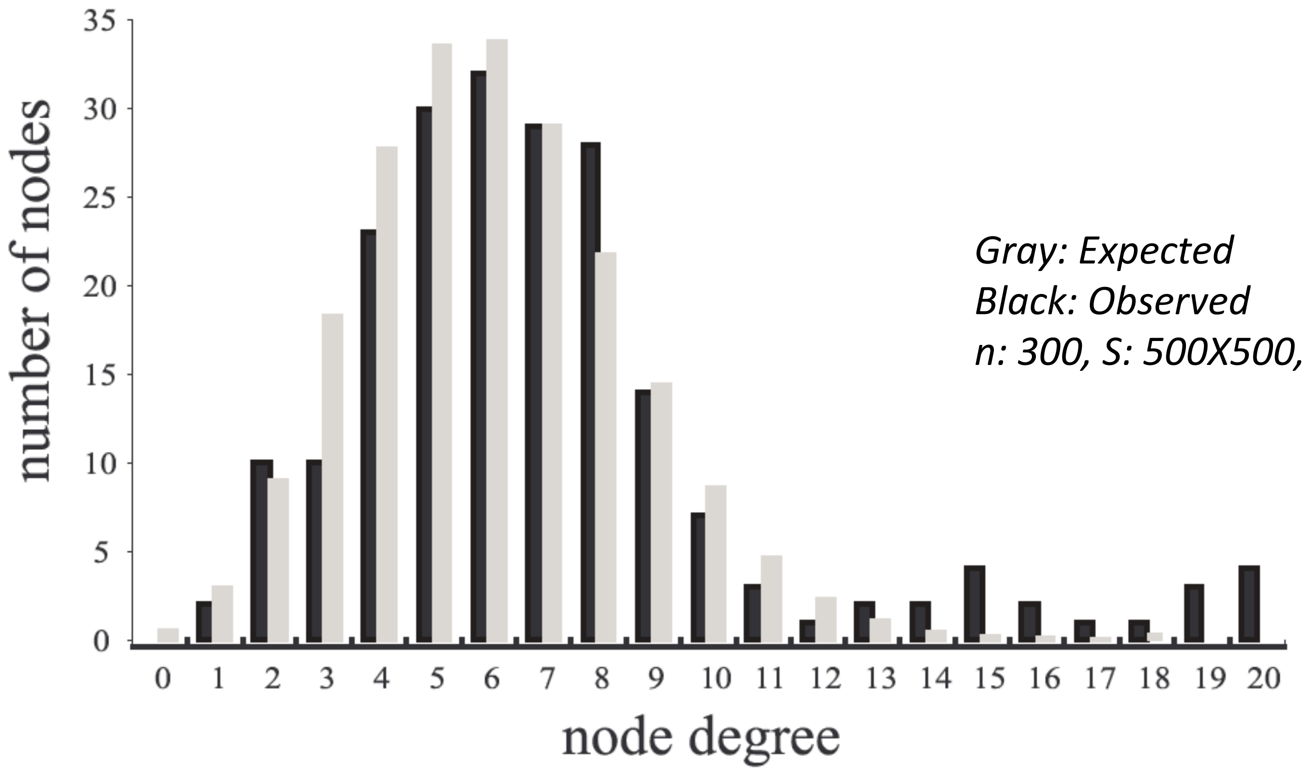
$$q = \frac{r^2\pi}{S}$$

- n: number of nodes in flat area of size S
- r: Communication Range

Example: Node Degree Expectation

- A wormhole that creates many new edges may increase the *number of neighbors* of the affected nodes

→ Distribution of node degrees will be distorted

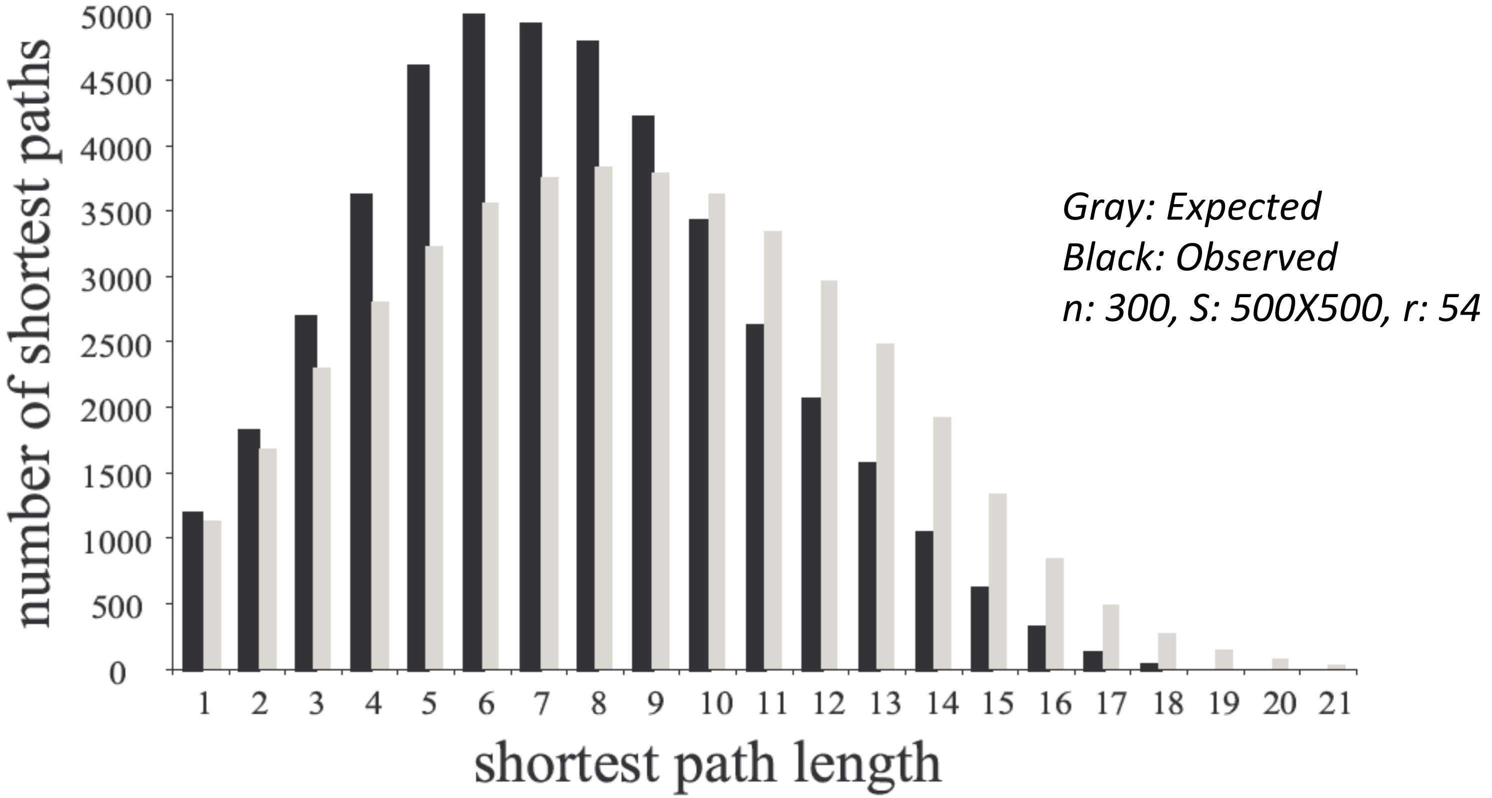


Gray: Expected
Black: Observed
n: 300, S: 500X500, r: 54

Example: Shortest Path

- 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



Centralized Approaches to Detect Wormhole

1. Statistical Wormhole Detection
2. Multi-dimensional Scaling

Multi-dimensional Scaling

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

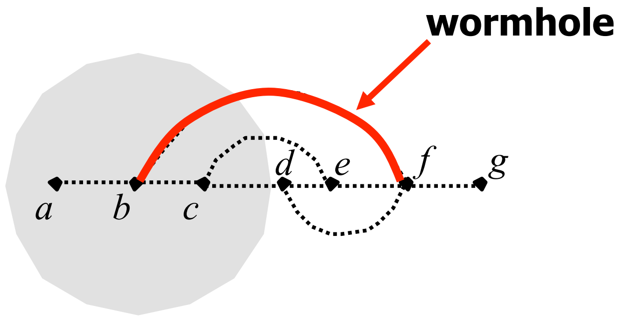
- Connectivity information and estimated distances are input to a multi-dimensional scaling (MDS) algorithm

- 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

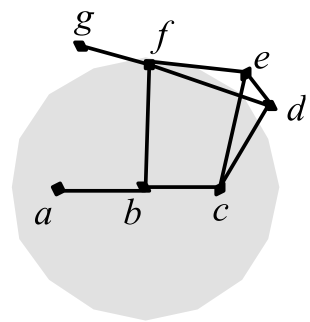
- Let us suppose that an adversary installed a wormhole in the network
  – if the estimated distances between the affected nodes are much larger than the nodes' communication range, then the wormhole is detected
  – hence, the adversary must also falsify the distance estimation → distances between far-away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

Examples

- in 1D:

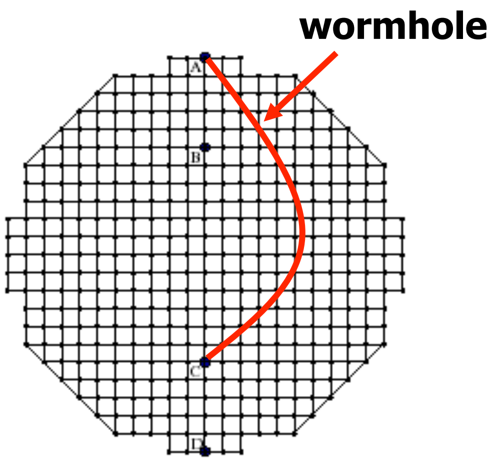


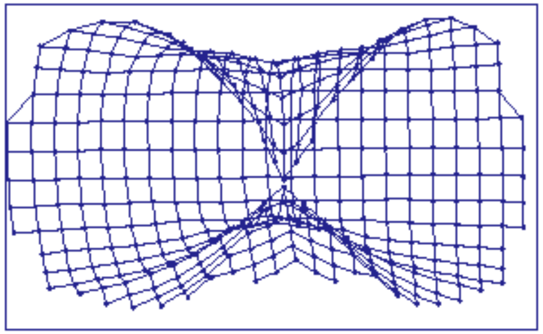
connectivity graph

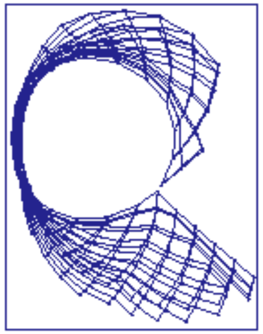


reconstructed virtual layout

- in 2D:







Decentralized Approaches to Detect Wormhole

1. Wormhole detection based on distance estimation
2. Wormhole detection using position information of anchors
3. Wormhole detection with directional antennas

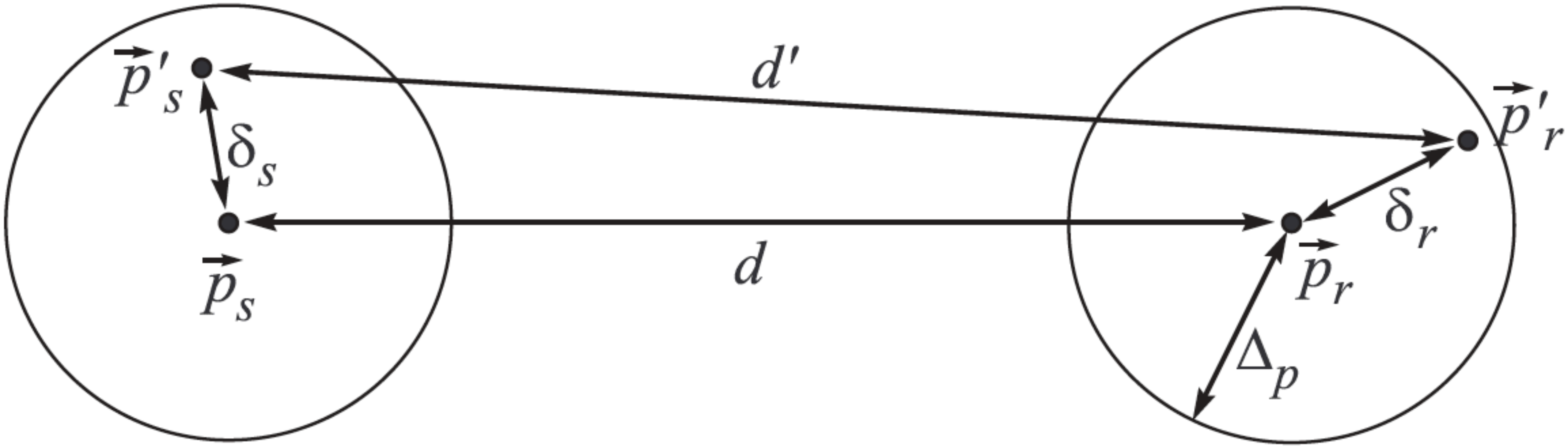
Packet leashes

- Packet leashes ensure that **packets are not accepted "too far"** from their source
  1. **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
  2. **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

Geographical Leashes



$$d' \leq d + 2\Delta_p + 2v_{max}(t_r - t_s + \Delta_t)$$

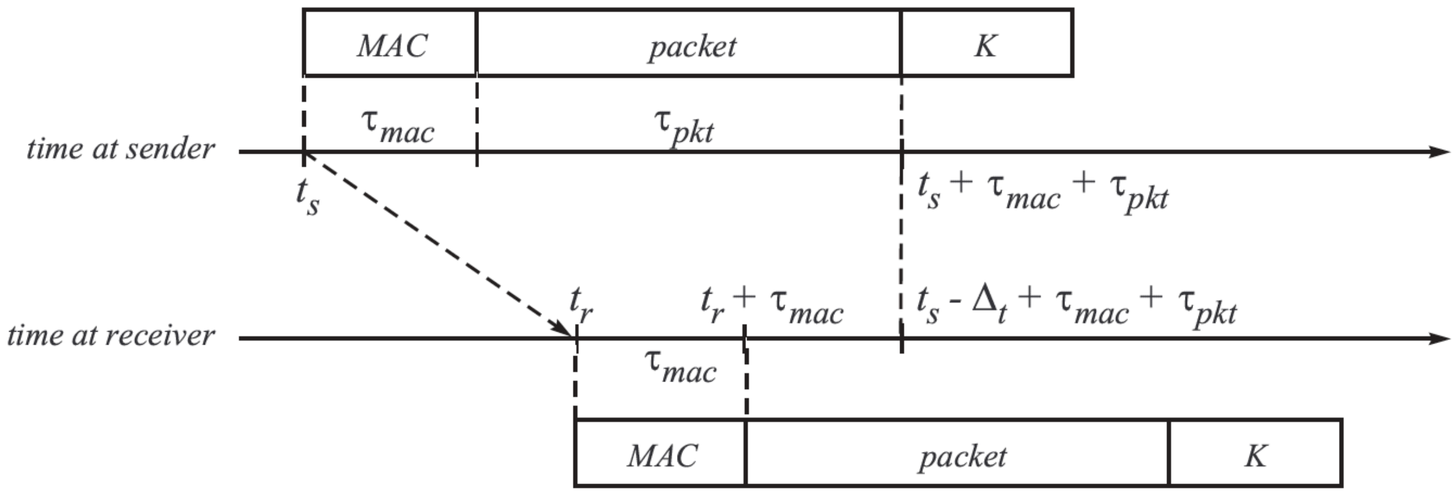
Security Issues

- the packets carrying the leashes **must be authenticated** and their **integrity should be protected**: *Digital Signature or MAC*

- **Digital signatures**
  - Provide broadcast authentication
  - But several orders of magnitude slower than symmetric key MAC computations, and speed is critical, especially in the case of temporal leashes.
- **MAC**
  - can be computed faster
  - they cannot be used efficiently to protect broadcast messages

TESLA with Instant Key-disclosure (TIK)

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: $t_r < t_s - \Delta_t + t_{pkt}$
- note: the clock synchronization error Δ_t must be very small

Distance Bounding

- Based on distance estimation between the nodes, but
  - does not require any clock synchronization
  - or localization mechanisms
- Main Idea:
  - The electro-magnetic waves propagate nearly with the speed of light and with current technology it is easy to measure local timings with nanosecond precision.

Mutual Authentication with Distance-bounding (MAD)

x		y
generate random numbers		generate random numbers
$r \in \{0,1\}^{\ell}$, $r' \in \{0,1\}^{\ell'}$		$s \in \{0,1\}^{\ell}$, $s' \in \{0,1\}^{\ell'}$
compute commitment $c_x = H(r\|\|r')$		compute commitment $c_y = H(s\|\|s')$
	$\xrightarrow{c_x}$	
	$\xleftarrow{c_y}$	
	— start of distance-bounding phase —	
the bits of r are $r_1, r_2, \ldots, r_\ell$		the bits of s are $s_1, s_2, \ldots, s_\ell$
$\alpha_1 = r_1$	$\xrightarrow{\alpha_1}$	
	$\xleftarrow{\beta_1}$	$\beta_1 = s_1 \oplus \alpha_1$
	$\ldots$	
$\alpha_i = r_i \oplus \beta_{i-1}$	$\xrightarrow{\alpha_i}$	measure delay between β_{i-1} and α_i
measure delay between α_i and β_i	$\xleftarrow{\beta_i}$	$\beta_i = s_i \oplus \alpha_i$
	$\ldots$	
$\alpha_\ell = r_\ell \oplus \beta_{\ell-1}$	$\xrightarrow{\alpha_\ell}$	measure delay between $\beta_{\ell-1}$ and α_ℓ
measure delay between α_ℓ and β_ℓ	$\xleftarrow{\beta_\ell}$	$\beta_\ell = s_\ell \oplus \alpha_\ell$
	— end of distance-bounding phase —	
compute MAC		compute MAC
$s_i = \alpha_i \oplus \beta_i$ $(i = 1, \ldots, \ell)$		$r_1 = \alpha_1$ and $r_i = \alpha_i \oplus \beta_{i-1}$ $(i = 2, \ldots, \ell)$
$\mu_x = mac_{k_{xy}}(x\|\|y\|\|r_1\|\|s_1\|\|\ldots\|\|r_\ell\|\|s_\ell)$		$\mu_y = mac_{k_{xy}}(y\|\|x\|\|s_1\|\|r_1\|\|\ldots\|\|s_\ell\|\|r_\ell)$
	$\xrightarrow{r'\|\|\mu_x}$	
	$\xleftarrow{s'\|\|\mu_y}$	
verify c_y and μ_y		verify c_x and μ_x

- MAD allows distance bounding without synchronized clocks

MAD: Summary

- As *r* and *s* are random, an adversary cannot try to cheat *x* by predicting the bits of *s* and responding earlier than *y*, and similarly it cannot cheat *y* either.
- MAD does not require the localization of the nodes or the synchronization of their clocks.
- MAD still requires, however, special hardware in the nodes in order to quickly switch the radio from receive mode into send mode.
- It needs a special medium access control protocol that allows for the transmission of bits without any delay

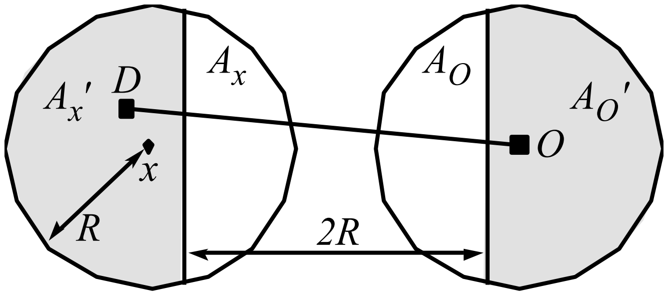
Decentralized Approaches to Detect Wormhole

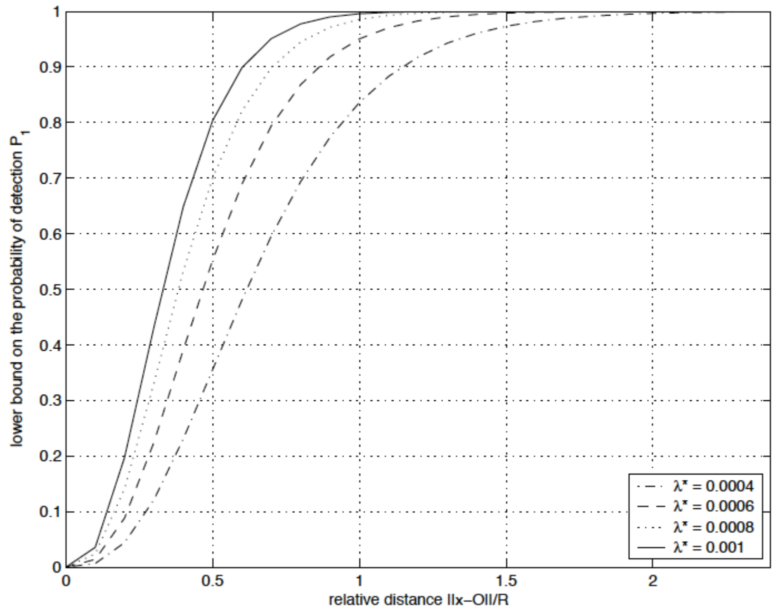
1. Wormhole detection based on distance estimation
2. Wormhole detection using position information of anchors
3. Wormhole detection with directional antennas

Using Position Information of 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 as 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, because the messages sent by the anchors are encrypted, and each anchor includes a one-time password in every message that it sends

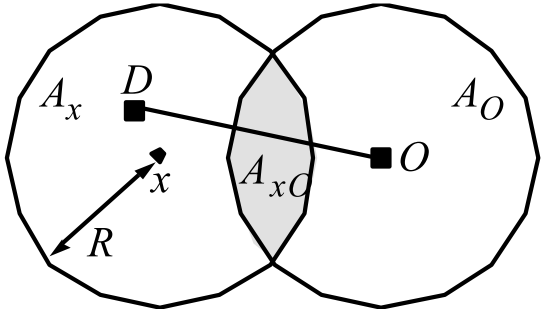
Principle 1

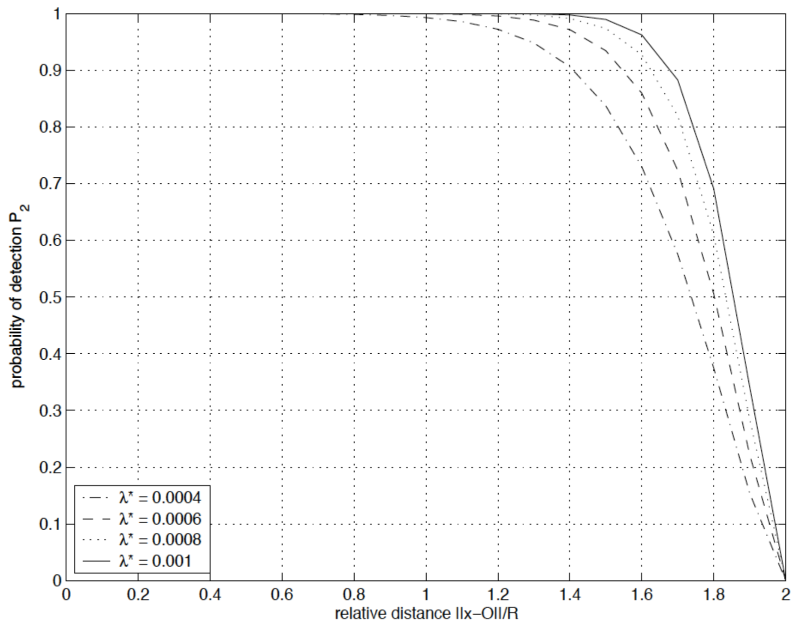




- x hears anchors in A_x and in A_O
- P_1 is the probability that it hears two anchors that are further away from each other than 2R
- The probability that there is at least one anchor in an area of size S is $(1-e^{-\lambda^*S})$, where λ^* is the density of anchors
- $P_1 \geq (1-e^{-\lambda^*S'_x})(1-e^{-\lambda^*S'_O})$,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





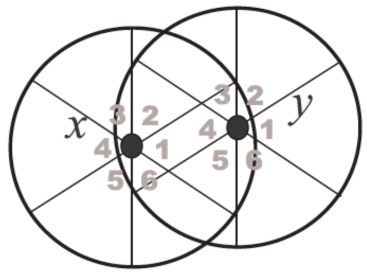
- When x and O are closer than 2*R*, the discs A_x and A_O overlap
- If there is an anchor in the intersection A_{xO}, then the messages of that anchor is heard twice by *x*
  - first directly and then from transceiver D who receives it from O through the wormhole
- The probability P_2 of detection is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

Decentralized Approaches to Detect Wormhole

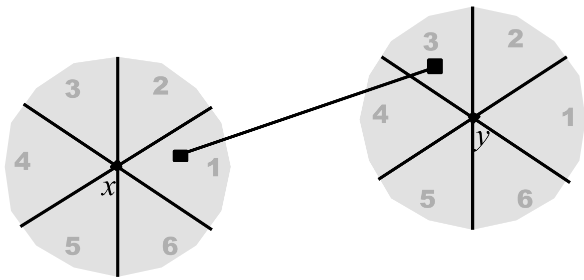
1. Wormhole detection based on distance estimation
2. Wormhole detection using position information of anchors
3. Wormhole detection with directional antennas

Wormhole Detection with Directional Antennas

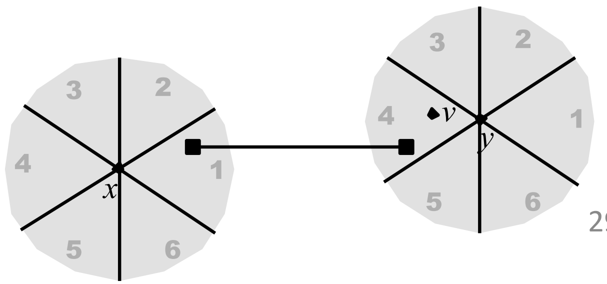
- When two nodes are within each other's communication range, they must hear each other's transmission from opposite directions (all antennas have the same orientation)



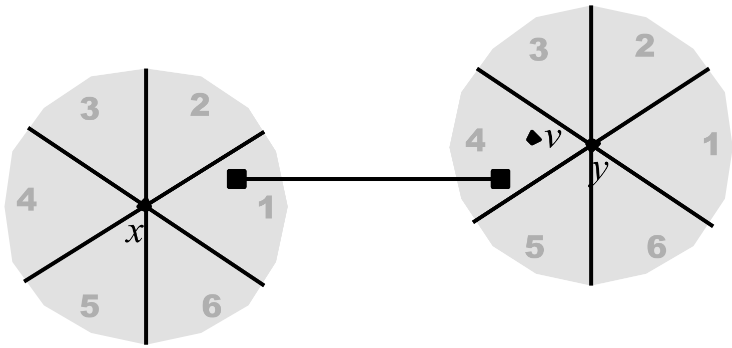
- If nodes x and y communicate through a wormhole, then this condition is not always satisfied:



- But this doesn't always work:

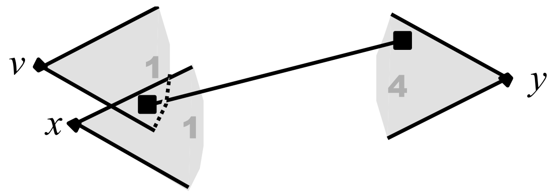


Idea: Using Verifiers



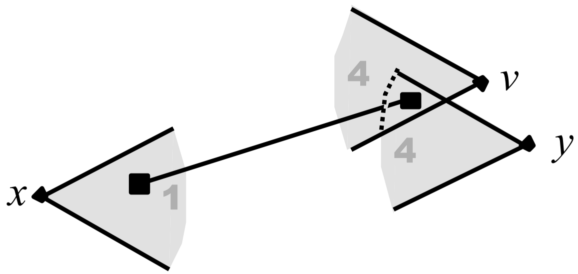
- If y and x were real neighbors and y heard x in zone 4, then every node in y's zone 4 would be a neighbor of x
- If they are not real neighbors, then there may be a node v in y's zone 4 that is not a neighbor of x (v and x don't hear each other from opposite directions)
- Such a v can be used by y as a verifier

Conditions for being a Verifier



- If node y hears v in the same zone in which it hears x, then y may hear both x and v through the wormhole

→ For a valid verifier v, y must hear v and x from different zones (i.e., $Z_{yv} \neq Z_{yx}$ must hold)



- If v hears x in the same zone in which y hears x (i.e., $Z_{vx} = Z_{yx}$), then they may both hear x through the wormhole's transceiver
- If, in addition, x happens to hear the other transceiver of the wormhole in zone $\underline{Z}_{yx}$, then x can establish neighbor relationships with both y and v

→ For a valid verifier v, v must hear x from a zone different from the one in which y hears x (i.e., $Z_{vx} \neq Z_{yx}$ must hold too).

Using Verifiers – the Mechanism

- **y accepts x as a neighbor if**
  - they hear each other from opposite zones
  - There’s at least one valid verifier v such that x and v hear each other from opposite zones

- **How does this detect wormholes ?**
  - let us assume that y hears x through the wormhole
  - → one end of the wormhole is near to x, the other end is in zone Z_{yx}
  - let us further assume that v is a valid verifier
  - → **first condition ($Z_{yv} \neq Z_{yx}$) is satisfied**
    - → y hears v directly (since y hears v from a zone different from Z_{yx})
    - → x hears both y and v through the wormhole
  - → **second condition ($Z_{vx} \neq Z_{yx}$) is satisfied**
    - → x and v cannot hear each other from opposite zones
      - let’s assume that $Z_{xv} = \underline{Z}_{vx}$
      - we know that x hears both y and v through the wormhole → $Z_{xy} = Z_{xv}$
      - in addition, we know that $Z_{xy} = \underline{Z}_{yx}$ (otherwise y would not consider x as a potential neighbor)
      - $\underline{Z}_{vx} = Z_{xv} = Z_{xy} = \underline{Z}_{yx}$ → $Z_{vx} = Z_{yx}$ (contradicts the second condition)

  - → No valid verifier v exists such that x and v hear each other from opposite zones
  - → **y will not accept x as a neighbor**

Summary

- 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
    - using directional antennas
  - many approaches are based on strong assumptions
    - tight clock synchronization
    - rapid bit exchange
    - GPS equipped nodes
    - directional antennas
    - …
- Wormhole detection is still an active research area