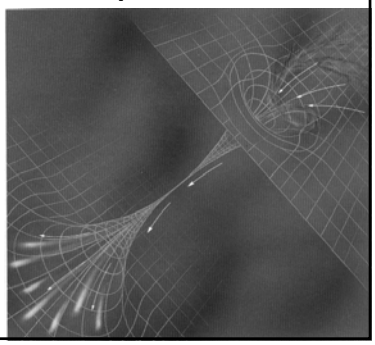
A Graph Theoretic Framework for Preventing the Wormhole Attack in Wireless Sensor Networks

Radha Poovendran
Network Security Lab
University of Washington

Wormholes – Hope for time travel

Wormhole: A space-time distortion that links two points in the Universe via a shorter path in distance/duration than the direct path.

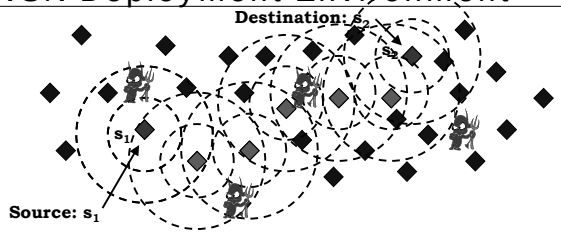
Can be a problem in wrong hands!



Outline

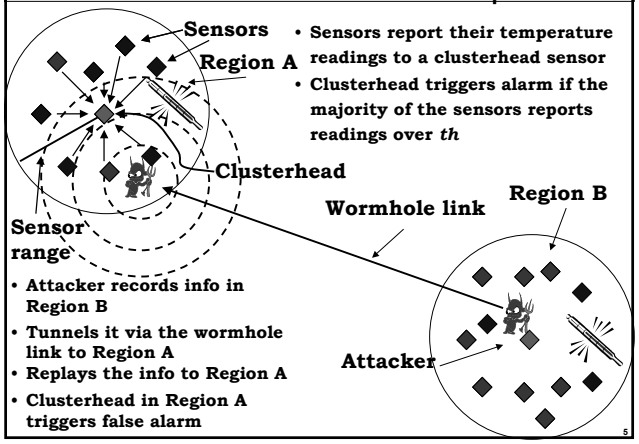
- **The Wormhole threat in Wireless Sensor Networks (WSN)**
- **Graph Theoretic Formulation**
- **Related Work**
- **Our Approach: Local broadcast Keys**
- **Security Analysis**
- **Conclusions**

WSN Deployment Environment



- **Ad hoc mode of communication - Distributed algorithms based on a cooperative principle**
- **Exchange of information locally**
- **Deployment region may be hostile**

Wormhole Attack – Example 1

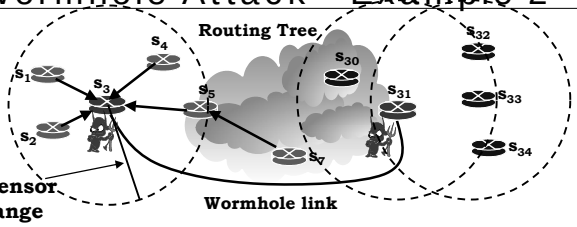


- Sensors report their temperature readings to a clusterhead sensor
- Clusterhead triggers alarm if the majority of the sensors reports readings over *th*

- Attacker records info in Region B
- Tunnels it via the wormhole link to Region A
- Replays the info to Region A
- Clusterhead in Region A triggers false alarm

5

Wormhole Attack – Example 2



- Attacker establishes a wormhole link between s_{31} and s_3.
- s_{31} and s_3 become neighbors in routing tree
- Sensors $\{s_1, s_2, s_3, s_4, s_5, s_7\}$ route through the wormhole link to reach any of $\{s_{30}, s_{31}, s_{32}, s_{33}, s_{34}\}$, and vice versa.
- The attacker controls/observes large amount of data.
- It can selectively drop packets, affect throughput, cause route oscillation.
- Sensor s_3 becomes a sinkhole for the local traffic to $\{s_{30}, s_{31}, s_{32}, s_{33}, s_{34}\}$

6

Impact of the Wormhole Threat

- **WSN Applications**
  - **Monitoring**
  - **Access Control**
  - **Localization**
- **Network Protocols**
  - **Routing**
  - **Neighbor discovery**

7

Wormhole Attack Properties

- **Type: Replay attack**
  - **The integrity and authenticity of the communication is not compromised**
  - **The success of the attack is independent of the strength of cryptographic primitives.**
  - **Freshness can be guaranteed by a speedy direct link.**

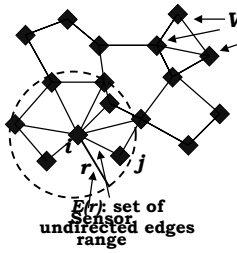
8

Outline

- **The Wormhole threat in Wireless Sensor Networks (WSN)**
- **Graph Theoretic Formulation**
- **Related Work**
- **Our Approach: Local broadcast Keys**
- **Security Analysis**
- **Conclusions**

9

Graph Representation of WSN



WSN represented by a Geometric Graph $G(V, E(r))$

$$e(i,j) = \begin{cases} 1, & if \ \|i-j\| \le r \\ 0, & if \ \|i-j\| > r \end{cases}$$

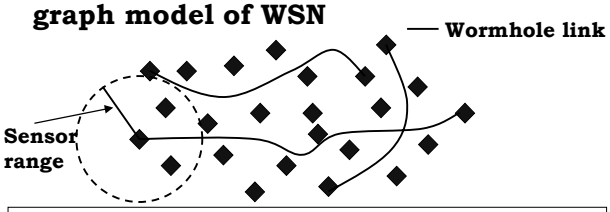
The Communication Graph $G(V, E_G)$ need not be identical to $G(V, E(r))$, but,

$$E_G \subseteq E(r)$$

10

Graph Interpretation of Wormholes

- **Wormholes violate the geometric graph model of WSN**



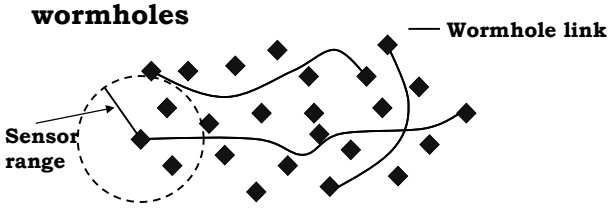
For a Communication Graph $G'(V, E_{G'})$ with wormholes $E_{G'} \not\subset E(r)$

Wormholes transform $G(V, E_G)$ to a Logical Graph $G'(V, E_{G'})$

11

The Wormhole Problem

Given a logical graph $G'(V, E_{G'})$ with wormholes



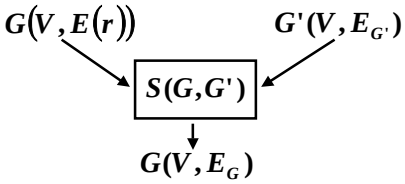
Extract from G' the communication graph $G(V, E_G)$ with

$$E_G \subseteq E(r)$$

12

Solving the Wormhole Problem

If $G(V, E(r))$ can be constructed (e.g. known locations of sensors) then:



$S : GxG' \rightarrow G$ a transformation such as XOR operation between the connectivity matrices of G, G'

What if $G(V, E(r))$ is UNKNOWN?

13

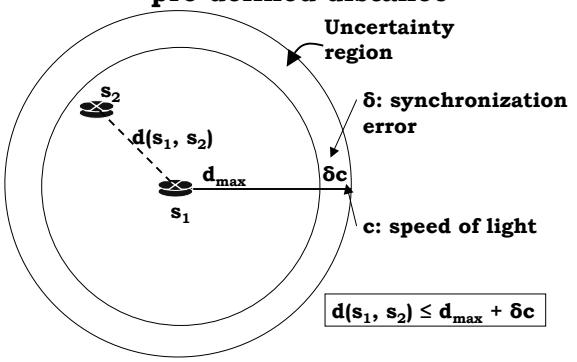
Outline

- **The Wormhole threat in Wireless Sensor Networks (WSN)**
- **Graph Theoretic Formulation**
- **Related Work**
- **Our Approach: Local broadcast Keys**
- **Security Analysis**
- **Conclusions**

14

Packet Leashes – Hu et al.

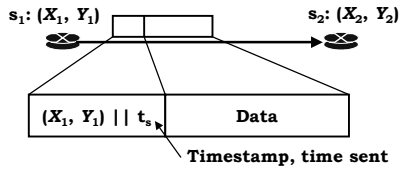
A packet cannot travel further than a pre-defined distance



15

Packet Leashes – Hu et al.

- **Locations of the nodes are known**
  - **Geographical Leashes**



- **s_2: Accept packet if:**

$$d(s_1, s_2) \leq (t_r - t_s + \delta)c$$

Speed of light

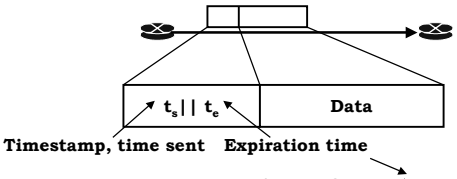
Time received

Synchronization error

16

Packet Leashes – Hu et al.

Temporal Leashes: Locations not known



- **s_2: Accept packet if:** $t_r \le t_e$

Time received

$$t_e - t_s = \frac{d_{\max} - \delta c}{c}$$

- **For $t_e > t_s$: $d_{max} > \delta c$**

17

Packet Leashes – Hu et al.

- **Packets Leashes can detect (and remove) wormholes if:**
  - **Geographical leashes:** $r \le (t_r - t_s + \delta)c$

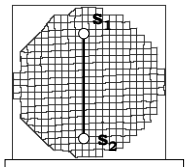
    Sensor communication range
  - **Temporal leashes:** $t_e - t_s = +\, r/c - \delta$
- **Requires tight synchronization**

  Eg: For $t_e > t_s$, if δ = 0.5msec → r > 150m

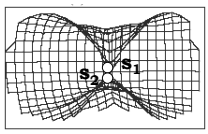
18

Visualization of Wormholes – Wang

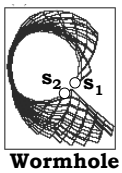
- **Construct a visual representation of the WSN**



Wormhole link



Wormhole between s_1, s_2 (front view)



Wormhole between two nodes (side view)

- **Idea: Wormholes shrink the distance between two points causing wraparound in the visual representation**

19

Visualization of Wormholes – Wang

- **Central Authority (CA) collects distance measurements of each sensor to its neighbors.**
- **Using Multi Dimensional Scaling (MDS), CA computes the relative position of each sensor.**

20

Outline

- **The Wormhole threat in Wireless Sensor Networks (WSN)**
- **Graph Theoretic Formulation**
- **Related Work**
- **Our Approach: Local broadcast Keys**
- **Security Analysis**
- **Conclusions**

21

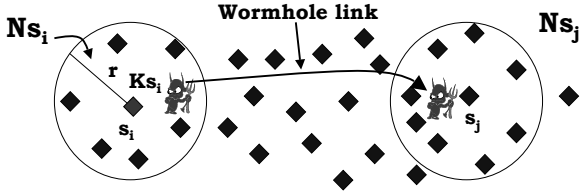
Our Approach : LBK

- **LBK: Local Broadcast Keys**

You need to be in the neighborhood to speak the same language and understand the message

22

Local Broadcast Keys (LBKs)



- **Each sensor uses a key Ks_i ONLY KNOWN to its neighborhood Ns_i.**
- **Broadcast information encoded with Ks_i, cannot be decrypted outside Ns_i.**

23

Correctness of the LBK Solution

- **Imposing LBKs to the "wormhole infected" logical graph $G'(V,E_{G'})$,**

$$e(i,j)=\begin{cases}1, & if \quad j \text{ holds } Ks_i\\ 0, & \text{otherwise}\end{cases}$$

- **Since j holds Ks_i iff j in in the neighborhood of i,**

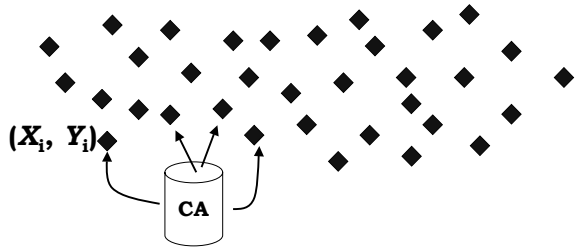
$$e(i,j)=\begin{cases}1, & if \quad \|i-j\|\le r\\ 0, & if \quad \|i-j\|>r\end{cases}$$

Geometric graph model is satisfied

24

Establishment of LBKs (1)

A) Static Network: Locations of the sensors are known.

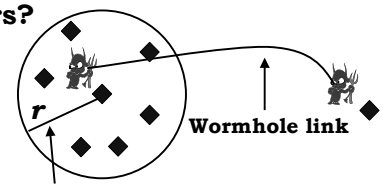


A Central Authority (CA) distributes the LBKs to sensors.

25

Establishment of LBKs (2)

B) Locations of the sensors are unknown, how do sensors discover their neighbors?



Sensor range

Neighbor discovery schemes are vulnerable to wormholes

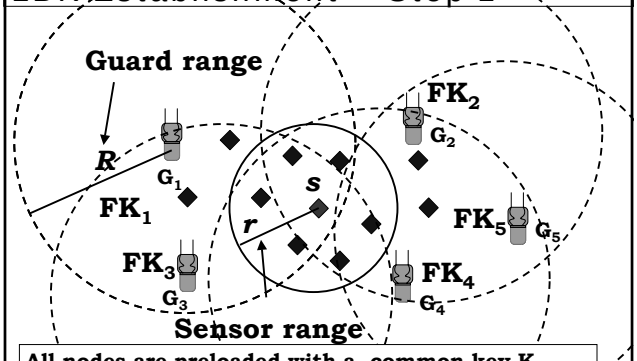
26

Secure Neighbor Discovery

1. **Perform distance bounding with neighbors – Requires:**
   - **time measurements with nanosecond accuracy**
   - **Nanosecond processing capable hardware**
2. **Perform Secure Localization (SeRLoc)**
3. **Use Power Proximity to infer distance**
4. **Proposed Approach: Use special nodes we call GUARDS.**

27

LBK Establishment – Step 1

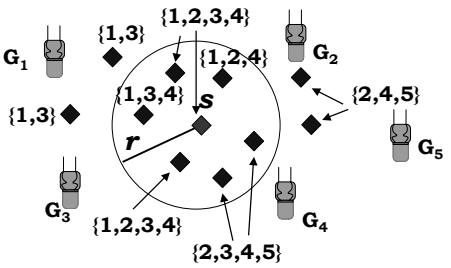


All nodes are preloaded with a common key K_0
Each Guard G_i broadcasts an encrypted fractional key $E_{K0}\{FK_i\}$

28

LBK Establishment – Step 1

{i,j,k,…}: indexes of the Guards heard

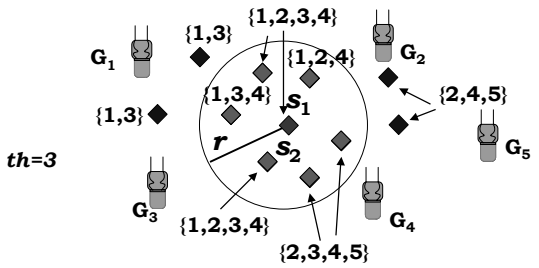


Sensors collect all the fractional keys they hear.

29

LBK Establishment – Step 2

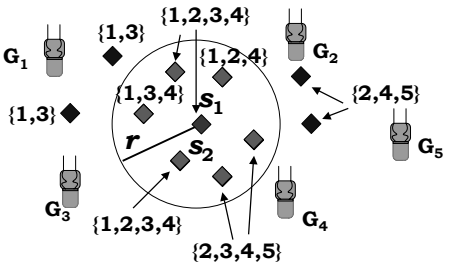
Every sensor announces the indexes of the fractional keys it hears and a threshold *th*



If a sensor s_i shares more than *th* fractional keys with s_1 → establish pairwise key $K_{s1,si}$

30

LBK Establishment – Step 2

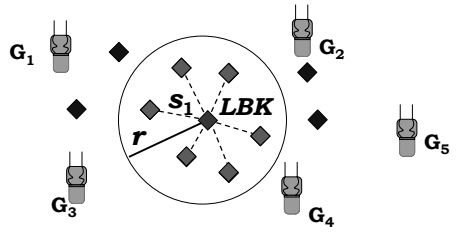


$K_{s1,s2}$=H(FK_1 || FK_2 ||FK_3|| FK_4}
H: Collision Resistant Hash function

31

LBK Establishment – Step 3

Sensor s_1 distributes its LBK via unicast to each neighbor s_i, using $K_{s1,si}$.

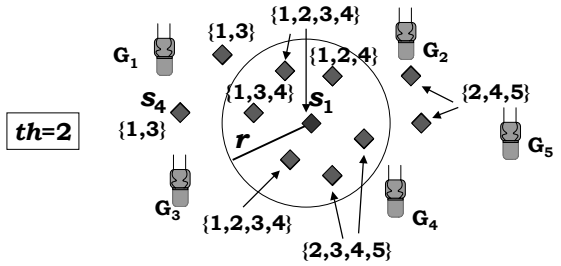


Each sensor holds its own LBK and the LBks of its neighbors.

32

LBK Establishment – non-neighbors

What if a node outside the sensor range shares sufficient keys with s_1?

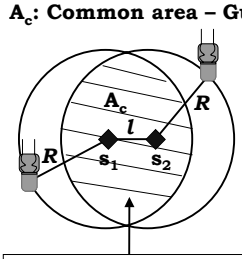


Threshold must be chosen carefully!
What do we mean by this?

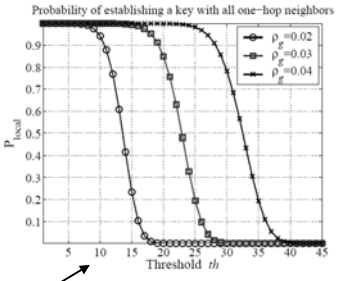
33

Deciding the Threshold value (1)

R: Guard range, *l*: distance between sensors (l≤r)
A_c: Common area – Guards heard to both s_1,s_2



At least *th* guards need to lay within A_c, $l \le r$

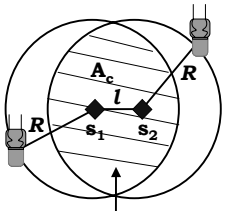


Computed as if all neighbors are at *l=r*

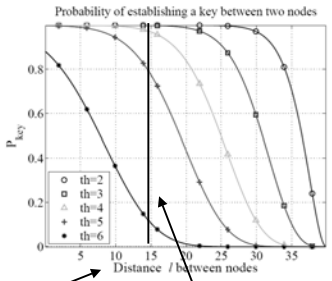
34

Deciding the Threshold value (2)

Probability of establishing a LBK with non-immediate neighbors



At least *th* guards need to lye within A_c, $l > r$



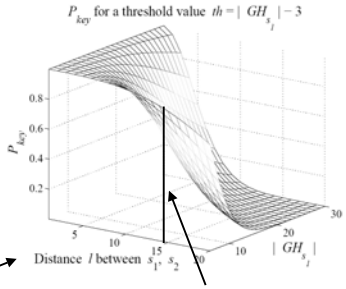
ρ_g=0.03 **Sensor range**

35

Locally computed Threshold

- **Locally decide for the threshold value *th* based on # of guards heard GH_s.**

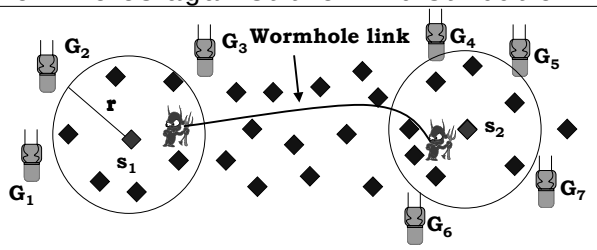
- **The threshold is some function of GH_s**
  ***th* = f(GH_s)**



ρ_g=0.03 **Sensor range**

36

Wormholes against the FK distribution

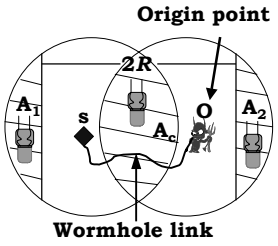


- **Attacker tunnels the transmissions of the FK via the wormhole link and replays at both ends.**
- **Sensors s_1, s_2 hear set of guards GH_s={G_1...G_7}**
- **s_1, s_2 establish a pairwise key and hence, a LBK**
- **If th >3, s_1 cannot establish an LBK with any of its neighbors**

37

Detecting wormholes during the FK distribution

Guards include their coordinates with every transmission of Fractional Keys (FK).



- **If sensor s hears a FK multiple times it is under a wormhole attack**
- **If sensor s hears two guards more than 2R apart, it is under a wormhole attack**

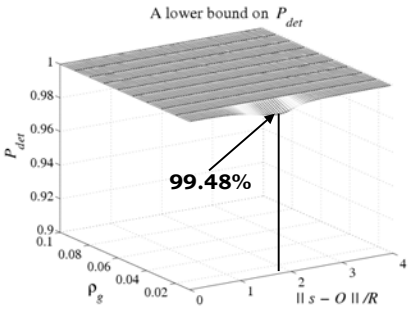
$$P_{\det} \geq \left(1-e^{-\rho_g A_c}\right)+e^{-\rho_g A_c}\left(1-e^{-\rho_g A_1}\right)^2$$

38

Wormhole Attack Detection

- **P_{det} during the distribution of fractional keys**

Once attack is detected execute challenge-response scheme to identify the closest guard



39

Conclusions

- **We showed: Any candidate solution eliminates wormholes if the communication graph produced satisfies the geometric graph constraints**
- **We proposed: A scheme for eliminating wormholes when sensors have unknown location and are not time synchronized**

Main idea behind the solution: If broadcasted information is encrypted at each neighborhood with a different Local Broadcast Key, it cannot be decrypted at some other neighborhood

40