Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures

Chris Karlof, David Wagner
University of California at Berkeley
{ckarlof,daw}@cs.berkeley.edu

Presenter – Lening Li
lli4@wpi.edu

WORCESTER POLYTECHNIC INSTITUTE · 1865 · WPI

OUTLINE

- I. INTRODUCTION
- II. BACKGROUND
- III.SENSOR NETWORKS VS. AD-HOC WIRELESS NETWORKS
- IV. RELATED WORK
- V. PROBLEM STATEMENT
- VI. ATTACKS ON SENSOR NETWORK ROUTING
- VII. ATTACKS ON SPECIFIC SENSOR NETWORK PROTOCOLS
- VIII. COUNTERMEASURES
- IX. ULTIMATE LIMITATIONS OF SECURE MULTI-HOP ROUTING
- X. CONCLUSION

I. INTRODUCTION

- **Five main contributions:**
  - Propose threat model and security goals for secure routing in wireless sensor networks.
  - Introduce two novel classes of previously undocumented attacks against sensor networks – sinkhole attacks and HELLO floods.
  - Show, for the first time, how attacks against ad-hoc wireless networks and peer-to-peer networks, can be adapted into powerful attacks against sensor networks.
  - Present the first detailed security analysis of all the major routing protocols and energy conserving topology maintenance algorithms for sensor networks. The authors describe practical attacks against all of them that would defeat any reasonable security goals.
  - Discuss countermeasures and design considerations for secure routing protocols in sensor networks.

OUTLINE

- I. INTRODUCTION
- II. BACKGROUND
- III.SENSOR NETWORKS VS. AD-HOC WIRELESS NETWORKS
- IV. RELATED WORK
- V. PROBLEM STATEMENT
- VI. ATTACKS ON SENSOR NETWORK ROUTING
- VII. ATTACKS ON SPECIFIC SENSOR NETWORK PROTOCOLS
- VIII. COUNTERMEASURES
- IX. ULTIMATE LIMITATIONS OF SECURE MULTI-HOP ROUTING
- X. CONCLUSION

II. BACKGROUND

- They use term sensor network to refer to a heterogeneous system combing tiny sensors and actuators with general purpose computing elements. Sensor networks may consist of hundreds or thousands of low-power, low-cost nodes, possibly mobile but more likely at fixed locations, deployed en mass to monitor and affect the environment.

II. BACKGROUND

- Note that: for concreteness, they target the Berkeley TinyOS sensor platform in their work.
- Sensor networks often have one or more points of centralized control called base stations.
- Base stations are typically many orders of magnitude more powerful than sensor nodes.

II. BACKGROUND

- A base station might request a steady stream of data, which is referred as data flow.
- In order to reduce the total number of messages sent and thus save energy, sensor readings from multiple nodes may be processed at one of many possible aggregation points.
- Power management in sensor networks is critical.

II. BACKGROUND

- The resource-starved nature of sensor networks poses great challenges for security.
- And barriers will unlikely disappear. Because we expect that users will want to ride Moore's law curve down towards ever-cheaper systems at a fixed performance point, rather than holding price constant and improving performance over time.

II. BACKGROUND

Protocol	Relevant attacks
TinyOS beaconing	Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes, HELLO floods
Directed diffusion and its multipath variant	Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes, HELLO floods
Geographic routing (GPSR, GEAR)	Bogus routing information, selective forwarding, Sybil
Minimum cost forwarding	Bogus routing information, selective forwarding, sinkholes, wormholes, HELLO floods
Clustering based protocols (LEACH, TEEN, PEGASIS)	Selective forwarding, HELLO floods
Rumor routing	Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes
Energy conserving topology maintenance (SPAN, GAF, CEC, AFECA)	Bogus routing information, Sybil, HELLO floods

Fig. 1. Summary of attacks against proposed sensor networks routing protocols.

OUTLINE

- I. INTRODUCTION
- II. BACKGROUND
- III.SENSOR NETWORKS VS. AD-HOC WIRELESS NETWORKS
- IV. RELATED WORK
- V. PROBLEM STATEMENT
- VI. ATTACKS ON SENSOR NETWORK ROUTING
- VII. ATTACKS ON SPECIFIC SENSOR NETWORK PROTOCOLS
- VIII. COUNTERMEASURES
- IX. ULTIMATE LIMITATIONS OF SECURE MULTI-HOP ROUTING
- X. CONCLUSION

III. SENSOR NETWORKS VS. AD-HOC WIRELESS NETWORKS

- Wireless sensor networks share similarities with ad-hoc wireless network. But several important distinctions can be drawn between the two.
- Most traffic in sensor networks can be classified into one of three categories:
  - Many-to-one: Multiple sensor nodes send sensor reading to a base station or aggregation point in the network.
  - One-to-many: A single node(typically a base station) multicasts or floods a query or control information to several sensor nodes.
  - Local communication: Neighboring nodes send localized messages to discover and coordinate with each other. A node may broadcast messages intended to be received by all neighboring nodes or unicast messages intended for a only single neighbor.

III. SENSOR NETWORKS VS. AD-HOC WIRELESS NETWORKS

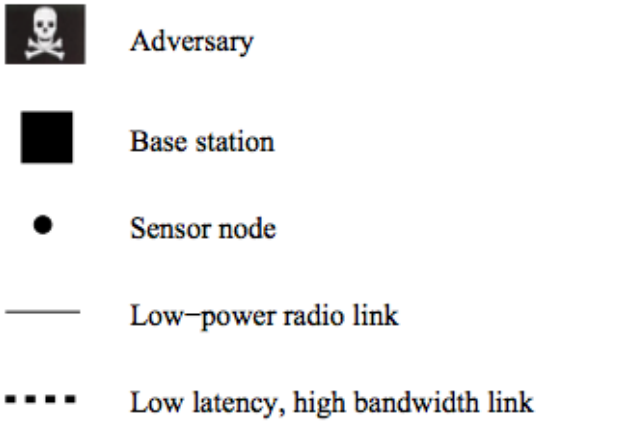

Fig. 2. **Sensor network legend.** All nodes may use low power radio links, but only laptop-class adversaries and base stations can use low latency, high bandwidth links.

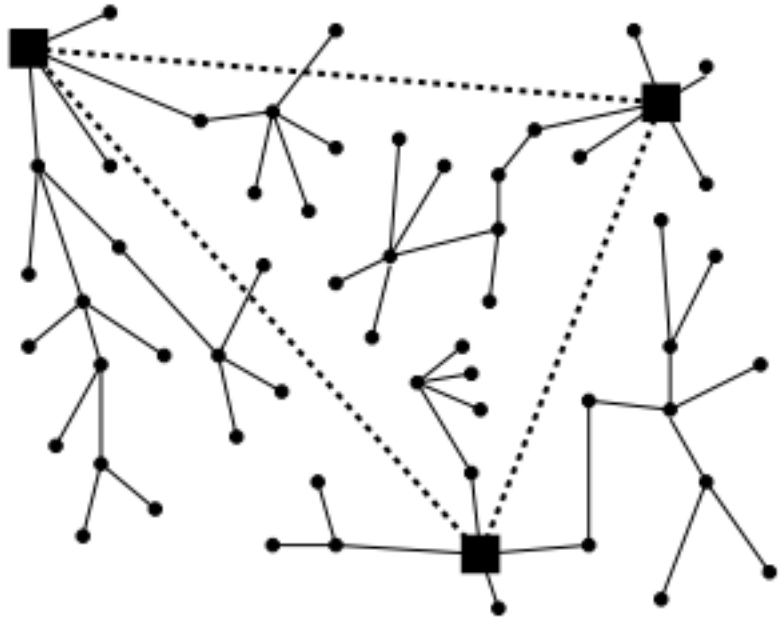

Fig. 3. A representative sensor network architecture.

Note that: node in sensor networks often exhibit trust relationships beyond those that are typically found in ad-hoc networks.

OUTLINE

- I. INTRODUCTION
- II. BACKGROUND
- III.SENSOR NETWORKS VS. AD-HOC WIRELESS NETWORKS
- IV. RELATED WORK
- V. PROBLEM STATEMENT
- VI. ATTACKS ON SENSOR NETWORK ROUTING
- VII. ATTACKS ON SPECIFIC SENSOR NETWORK PROTOCOLS
- VIII. COUNTERMEASURES
- IX. ULTIMATE LIMITATIONS OF SECURE MULTI-HOP ROUTING
- X. CONCLUSION

IV. RELATED WORK

- Security issues in ad-hoc networks are similar to those in sensors networks, but the defense mechanisms developed to sensor networks.
- Public key cryptography is too expensive for sensor nodes.
- Protocols based on symmetric key are based on source routing or distance vector protocols are too expensive.

IV. RELATED WORK

- Marti et al. and Buchegger and Boudec consider the problem of minimizing the effect of misbehaving or selfish nodes on routing, which is promising, but is vulnerable to blackmailers.
- Perrig et al. present two building block security protocols optimized.
  - SNEP provides confidentiality, authentication, and freshness.
  - *μ*TESLA provides authenticated broadcast.

OUTLINE

- I. INTRODUCTION
- II. BACKGROUND
- III.SENSOR NETWORKS VS. AD-HOC WIRELESS NETWORKS
- IV. RELATED WORK
- V. PROBLEM STATEMENT
- VI. ATTACKS ON SENSOR NETWORK ROUTING
- VII. ATTACKS ON SPECIFIC SENSOR NETWORK PROTOCOLS
- VIII. COUNTERMEASURES
- IX. ULTIMATE LIMITATIONS OF SECURE MULTI-HOP ROUTING
- X. CONCLUSION

V. PROBLEM STATEMENT

- A. Network assumptions
  - Because sensor network use wireless communication, we must assume that radio links are insecure.
  - We do not assume sensor nodes are tamper resistant.
- B. Trust Requirements
  - since base stations interface a sensor network to the outside world, the compromise of a significant number of them can render the entire network useless. So we assume that base stations are trustworthy.

V. PROBLEM STATEMENT

- **C. Threat Models**
  - Distinction between *mote-class attackers* and *laptop-class attackers*: a laptop-class attacker may have more powerful devices.
  - An attacker with laptop-class devices can do more than an attacker with only ordinary sensor nodes.
  - A second distinction between outsider attacks and insider attacks: Insider attacks may be mounted from either compromised sensor nodes.

V. PROBLEM STATEMENT

- **D. Security Goals**
  - In the ideal world, secure routing protocol should guarantee the integrity, authenticity, and availability of messages in the presence of adversaries of arbitrary power. Every eligible receiver should receive all messages intended for it and able to verify the integrity of every message as well as the identity of the sender.
  - Protection against eavesdropping is not an explicit security goal of a secure routing algorithm.
  - Protection against the replay of data packets should not be a security goal of a secure routing protocol.
  - In the presence of compromised or insider attackers, especially those with laptop-class capabilities, it is most likely that some if not all of these goals are not fully attainable.

OUTLINE

- I. INTRODUCTION
- II. BACKGROUND
- III.SENSOR NETWORKS VS. AD-HOC WIRELESS NETWORKS
- IV. RELATED WORK
- V. PROBLEM STATEMENT
- VI. ATTACKS ON SENSOR NETWORK ROUTING
- VII. ATTACKS ON SPECIFIC SENSOR NETWORK PROTOCOLS
- VIII. COUNTERMEASURES
- IX. ULTIMATE LIMITATIONS OF SECURE MULTI-HOP ROUTING
- X. CONCLUSION

VI. ATTACKS ON SENSOR NETWORK ROUTING

- Most network layer attacks against sensor networks fall into one of the following categories:
  - Spoofed, altered, or replayed routing information
  - Selective forwarding
  - Sinkhole attacks
  - Sybil attacks
  - Wormholes
  - HELLO flood attacks
  - Acknowledgement spoofing

VI. ATTACKS ON SENSOR NETWORK ROUING

- A. Spoofed, altered, or replayed routing information
  - The most direct attack against a routing protocol is to target the routing information exchanged between nodes.
- B. Selective forwarding
  - In a selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them.
  - Selective forwarding attack is conceivable and adversary overhearing a flow passing through neighboring nodes might be able to emulate selective forwarding by jamming or causing a collision on each forwarded packet of interest.

VI. ATTACKS ON SENSOR NETWORK ROUTING

- **C. Sinkhole attacks**
  - The goal is to lure nearly all the traffic from a metaphorical sinkhole with the adversary at the center.
  - Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm.
  - One motivation for mounting a sinkhole attack is that it makes selective forwarding trivial.
  - The reason sensor networks are particularly susceptible to sinkhole attack is due to their specialized communication pattern.

VI. ATTACKS ON SENSOR NETWORK ROUTING

- **D. The Sybil attack**
  - The Sybil attack can significantly reduce the effectiveness of fault-tolerant schemes.
  - Sybil attack also pose a significant threat to geographic routing protocols.

VI. ATTACKS ON SENSOR NETWORK ROUTING

- **E. Wormholes**
  - In the wormhole attack, and adversary tunnels messages received in one part on the network over a low latency link and replay them in a different part.
  - An adversary situated close to a base station may be able to completely disrupt routing by creating a well placed wormhole. An adversary could convince nodes who would only one or two hops away via the wormhole. This can create a sinkhole: since the adversary on the other side of the wormhole can arterially provide a high-quality route to the base station, potentially all traffic in the surrounding area will be drawn.
  - Detection is potentially difficult when used in conjunction with the Sybil attack.

VI. ATTACKS ON SENSOR NETWORK ROUTING

- F. HELLO flood attack
  - Many protocols require to their neighbors, and a node receiving such a packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within (normal) radio range of the sender, which may be false.
  - For example, an adversary advertising a very high quality route to the base station to every node in the network could cause a large number of nodes to attempt to use this route, but those nodes sufficiently far away from the adversary would be sending packets into oblivion.
  - An adversary does not necessarily need to be able to construct legitimate traffic in order to use the HELLO flood attack, just can simply re-broadcast overhead packets.

VI. ATTACKS ON SENSOR NETWORK ROUTING

- G. Acknowledgement spoofing
  - Several sensor network routing algorithms rely on implicit or explicit link layer acknowledgements. Due to the inherent broadcast medium, and adversary can spoof link layer acknowledgments for "overheard" packets addressed to neighboring nodes. Goals include convincing the sender that a weak link is strong or that a dead or disabled node is alive.

OUTLINE

- I. INTRODUCTION
- II. BACKGROUND
- III.SENSOR NETWORKS VS. AD-HOC WIRELESS NETWORKS
- IV. RELATED WORK
- V. PROBLEM STATEMENT
- VI. ATTACKS ON SENSOR NETWORK ROUTING
- VII. ATTACKS ON SPECIFIC SENSOR NETWORK PROTOCOLS
- VIII. COUNTERMEASURES
- IX. ULTIMATE LIMITATIONS OF SECURE MULTI-HOP ROUTING
- X. CONCLUSION

VII. ATTACKS ON SPECIFIC SENSOR NETWORK PROTOCLS

- A. TinyOS beaconing
- B. Directed diffusion
- C. Geographic routing
- D. additional routing protocols
  - Clustering protocols such LEACH, rumor routing, and energy conserving topology maintenance algorithms such as SPAN and GAF.

A. TinyOS beaconing

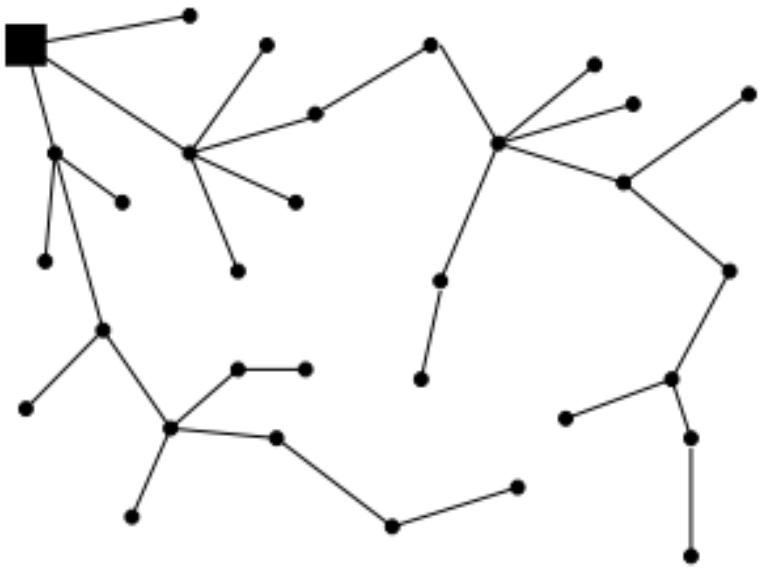

Fig. 4. A representative topology constructed using TinyOS beaconing with a single base station.

The TinyOS beaconing protocol constructs a breadth first spanning tree rooted at a base station. Periodically the base station broadcasts a route update. All nodes receiving the update mark the base station as its parent and rebroadcast the update.

A. TinyOS beaconing

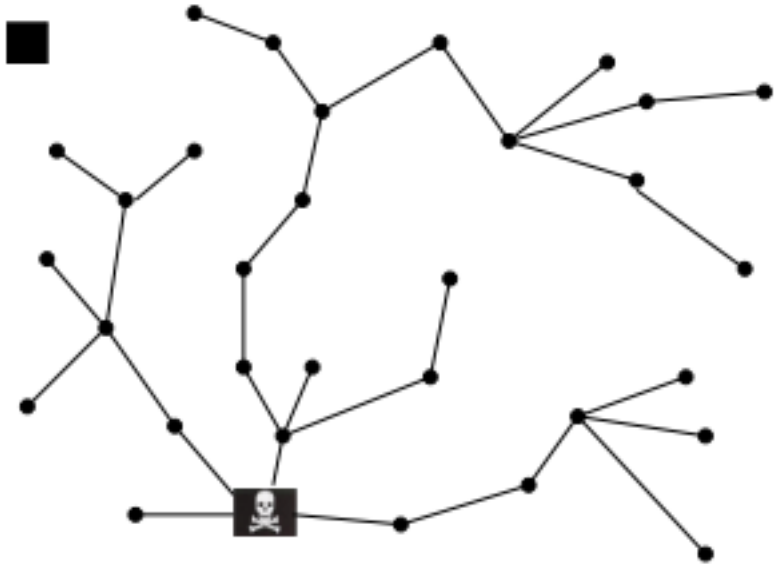

Fig. 5. An adversary spoofing a routing update from a base station in TinyOS beaconing.

- **Attack: the TinyOS beaconing protocol in highly susceptible to attack.**

• Since routing updates are not authenticated, it is possible for any node to claim to be a base station and become the destination of all traffic in the network (see Figure 5).

A. TinyOS beaconing

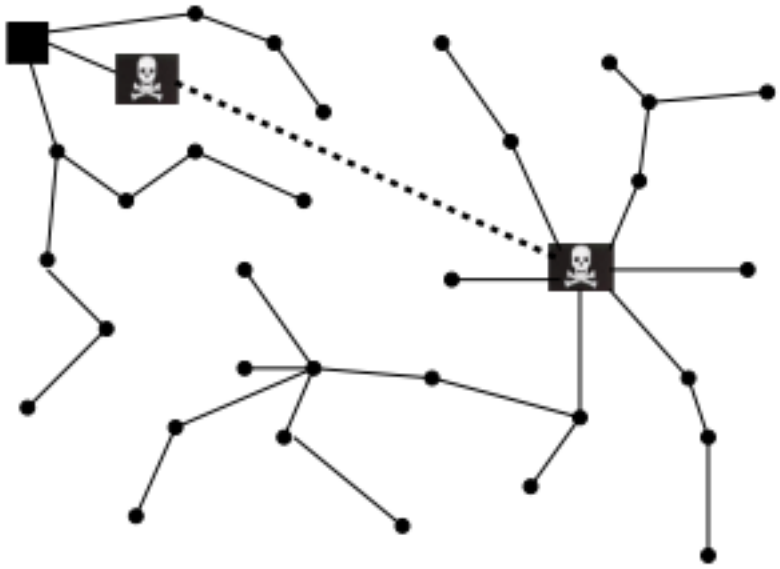

Fig. 6. A laptop-class adversary using a wormhole to create a sinkhole in TinyOS beaconing.

- As seen in Figure 6, all traffic in the targeted area will be channeled through the wormhole, enabling a potent selective forwarding attack.

Authenticated routing updates will prevent an adversary form claiming to be a base station, but a powerful laptop class adversary can still easily wreak havoc.

A. TinyOS beaconing

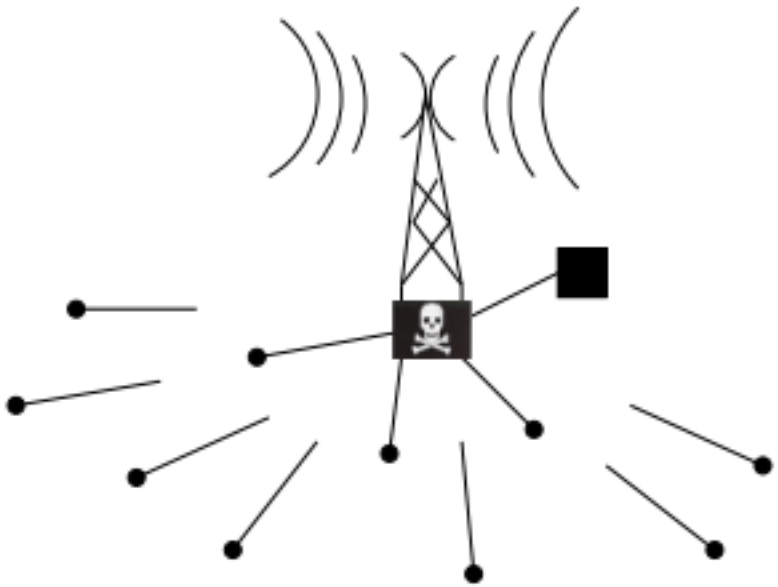

Fig. 7. HELLO **flood attack against TinyOS beaconing.** A laptop-class adversary that can retransmit a routing update with enough power to be received by the entire network leaves many nodes stranded. They are out of normal radio range from the adversary but have chosen her as their parent.

- As shown in Figure 7, the network is crippled: the majority of nodes are stranded, sending packets into oblivion.

- If a laptop-class adversary has a powerful transmitter, it can use HELLO flood attack to broadcast a routing update load enough to reach the entire network, causing every node to mark the adversary as its parent.
- Routing loop can easily be created by mote-class adversaries spoofing routing updates.

B. Directed diffusion

- Directed diffusion is a data-centric algorithm for drawing information out of a sensor network.
- There is a multipath variant of directed diffusion as well.
- Attacks: due to the robust nature of flooding, it may be difficult for an adversary to prevent interests from reaching targets able to satisfy then
- Suppression: Flow suppression is an instance of denial-of-service. The easiest way to suppress a flow is to spoof negative reinforcements.

B. Directed diffusion

- Cloning: Cloning a flowing enables eavesdropping.
- Path influence: an adversary can influence the path taken by a data flow by spoofing positive and negative reinforcements and bogus data events.
- Selective forwarding and data tampering: by using the above attack to insert herself onto taken by a flow of events, an adversary can gain full control of the flow.

B. Directed diffusion

- A laptop-class adversary can exert greater influence on the toplofty by creating a wormhole between node A located next a base station and node B located close to where events are likely to be generated.
- The multipath version may appear more robust against these attacks, but it is vulnerable.

C. Geographic routing

- Geographic and Energy Aware Routing and Greedy Perimeter Stateless Routing leverage node's positions and explicit geographic packet destinations to efficiently disseminate queries and route replies.
- Attacks: Location information can be misrepresented.

C. Geographic routing

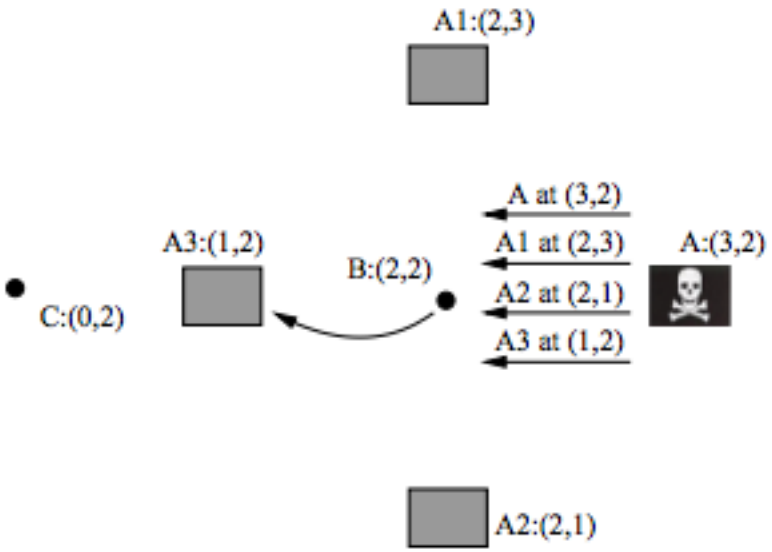

Fig. 8. **The Sybil attack against geographic routing.** Adversary A at actual location (3,2) forges location advertisements for non-existent nodes A1, A2, and A3 as well as advertising her own location. After hearing these advertisements, if B wants to send a message to destination (0,2), it will attempt to do so through A3. This transmission can be overheard and handled by the adversary A.

- As depicted in Figure 8, an adversary can advertise multiple bogus nodes surrounding each target in a circle (or sphere), each claiming to have maximum energy.

- *Without too much additional effort, an adversary can dramatically increase her chances of success by mounting a Sybil attack. As depicted in Figure 8, an adversary can advertise*
- *multiple bogus nodes surrounding each target in a circle*
- *(or sphere), each claiming to have maximum energy.*

C. Geographic routing

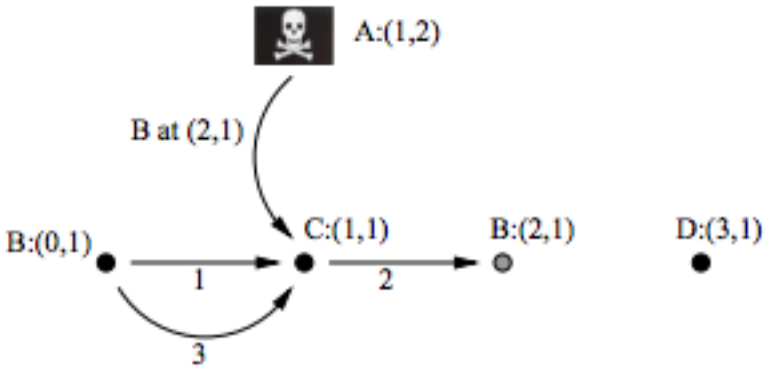

Fig. 9. **Creating routing loops in GPSR.** By forging a location advertisement claiming B is at (2,1), an adversary can create a routing loop as described in Section VII-C.

- Consider the hypothetical topology in Figure 9 and flow of packets from B to location (3,1). Assume the maximum radio range is one unit. If an adversary forges a location advertisement claiming B is at (2,1) and sends it to C, then after B forwards a packet destined for (3,1) to C, C will send it back to B because it believes B is close to the ultimate destination. B and C will forever forward the packet in a loop between each other.

- *In GPSR an adversary can forge location advertisements to create routing loops in data flows without having to actively participate in packet forwarding.*

D. Additional routing protocols

- Refer to the appendix for security analysis of minimum cost forwarding, clustering protocols such as LEACH, rumor routing, and energy conserving topology maintenance algorithms such as SPAN and GAF.

OUTLINE

- I. INTRODUCTION
- II. BACKGROUND
- III.SENSOR NETWORKS VS. AD-HOC WIRELESS NETWORKS
- IV. RELATED WORK
- V. PROBLEM STATEMENT
- VI. ATTACKS ON SENSOR NETWORK ROUTING
- VII. ATTACKS ON SPECIFIC SENSOR NETWORK PROTOCOLS
- VIII. COUNTERMEASURES
- IX. ULTIMATE LIMITATIONS OF SECURE MULTI-HOP ROUTING
- X. CONCLUSION

VIII. COUNTERMEASURES

- A. Oursider attacks and link layer security
- B. The Sybil attack
- C. HELLO flood attacks
- D. Wormhole and sinkhole attacks
- E. Leveraging global knowledge
- F. Selective forwarding
- G. Authenticated broadcast and flooding
- H Countermeasure summary

A. Outsider attacks and link layer security

- The majority of outsider attacks against sensor network routing protocols can be prevented by simple link layer encryption and authentication using a globally shared key. The majority of selective forwarding and sinkhole attacks are not possible because the adversary is prevented form joining the topology.
- Major class of attacks not countered by layer encryption and authentication mechanisms are wormhole attacks and HEELO flood attacks.

A. Outsider attacks and link layer security

- The attacks against TinyOS beaconing described in Section VII-A illustrate these techniques, and link layer security mechanisms can do nothing to prevent them.
- Link layer security mechanisms using a globally shared key are completely ineffective in presence of insider attacks or compromised nodes.

B. The Sybil attack

- An insider cannot be prevented from participating in the network, but she should only be able to do so using the identities of the nodes she has compromised.
- One solution is to have every node share a unique symmetric key with a trusted base station.
- Thus, when a node is compromised, it is restricted to communicating only with its verified neighbors.

C. HELLO flood attacks

- The simplest defense against HELLO flood attacks is to verify the bidirectionality of a link before taking meaningful action based on a message received over that link. The identity verification protocol described in Section VIII-B is sufficient to prevent HELLO flood attack.

D. Wormhole and sinkhole attacks

- Wormhole and sinkhole attacks are very difficult to defend against.
- A technique for detecting wormhole attacks which requires extremely tight time synchronize and it is thus infeasible for most sensor networks.

E. Leveraging global knowledge

- A significant challenge in securing large sensor networks is their inherent self-organizing, decentralized nature.
- To account for topology changes due to radio interference or node failure, nodes would periodically update a base station with the appropriate information. Drastic or suspicious changes to the topology might indicate a node compromise, and the appropriate action can be taken.

E. Leveraging global knowledge

- We have discusses why discussed why geographic routing can be relatively secure against wormhole, sinkhole, and Sybil attacks, but the main remaining problem is that location information advertised form neighboring nodes must be trusted.
- Sufficiently restricting the structure of the topology can eliminate the requirement for nodes to advertise their locations if all nodes' locations are well known.

F. Selective forwarding

- Even in protocols resistant to sinkholes, wormhole, and the Sybil attack, a compromised node has significant probability of including itself on a data flow to launch a selective forwarding attack if it is strategically located near the source or base station.
- Multipath routing can be used to counter these types of selective forwarding attacks.
- The use of multiple braided paths may provide probabilistic protection against selective forwarding and use only localized information.

OUTLINE

- I. INTRODUCTION
- II. BACKGROUND
- III.SENSOR NETWORKS VS. AD-HOC WIRELESS NETWORKS
- IV. RELATED WORK
- V. PROBLEM STATEMENT
- VI. ATTACKS ON SENSOR NETWORK ROUTING
- VII. ATTACKS ON SPECIFIC SENSOR NETWORK PROTOCOLS
- VIII. COUNTERMEASURES
- IX. ULTIMATE LIMITATIONS OF SECURE MULTI-HOP ROUTING
- X. CONCLUSION

G. Authenticated broadcast and flooding

- Since base stations are trustworthy, adversaries must not be able to spoof broadcast or flooded message form any base stations.
- Proposals for authenticated broadcast intended for use in more conventional setting either use digital signature and/or have packet overhead that well exceed the length of typical sensor network packet.

G. Authenticated broadcast and flooding

- Flooding can be a robust means for information dissemination in hostile environments because it requires the set of compromised nodes to form a vertex cut on the underlying topology to prevent a message form reaching every node in the network.

H. Countermeasure summary

- Link-layer encryption and authentication, multipath routing, identity verification, bidirectional link verification, and authenticated broadcast can protect sensor network routing protocols against outsiders, bogus routing information, Sybil attack, HELLO floods, and acknowledgement spoofing, and it is feasible to augment existing protocols with these mechanisms.
- Sinkhole attacks and wormholes pose significant challenges to secure routing protocol design, and it is unlikely there exists effective countermeasures against these attacks that can be crucial to design routing protocols in which these attacks are meaningless or ineffective. Geographic routing protocols are one class of protocols that hold promise.

IX. ULTIMATE LIMITAIONS OF SECURE MULTI-HOP ROUTING

- Clustering protocols like LEACH where cluster-heads communicate directly with a base station may ultimately yield the most secure solutions against node compromise and insider attacks.
- Another option may be to have a randomly randomly rotation set of "virtual" base stations to create an overlay network.

OUTLINE

- I. INTRODUCTION
- II. BACKGROUND
- III.SENSOR NETWORKS VS. AD-HOC WIRELESS NETWORKS
- IV. RELATED WORK
- V. PROBLEM STATEMENT
- VI. ATTACKS ON SENSOR NETWORK ROUTING
- VII. ATTACKS ON SPECIFIC SENSOR NETWORK PROTOCOLS
- VIII. COUNTERMEASURES
- IX. ULTIMATE LIMITATIONS OF SECURE MULTI-HOP ROUTING
- X. CONCLUSION

X. CONCLUSION

- The currently proposed routing protocols for these networks are insecure.
- Link layer encryption and authentication mechanisms may be a reasonable first approximation. Cryptography is not enough to defend against lap-class adversaries and insiders
- Careful protocol design is needed as well.

Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures

Thank You!

Questions ??

WORCESTER POLYTECHNIC INSTITUTE · 1865 · WPI