Wireless: Can You Secure Me NOW ?

Prof. Bharat Bhargava
Department of Computer Sciences
Center for Education and Research in Information Assurance and Security (CERIAS)
Purdue University

www.cs.purdue.edu/people/bb

Supported in part by I3P, NSF grants
IIS 0209059, CNS 0242840, Cisco, Motorola

ANSWER

- Not Yet and may be Not for Some Time

Security is Needed

- Pervasive Access to Medical Records
- Securing Access to devices and sensors in homes/building
- Securing trusted communication for collaborations
- Mobile Multi-Media Applications

Why Security is not Possible ?

- Do not understand the Individual Attacks
- Possibility of Collaborative Attacks
- Can not control Environment beyond our Wireless Device
- Hard to Detect and Identify Intruders
- Hard to Specify Privacy Policies?
- Infrastructures for Experiments is not Available

Outline

- Characterizing collaborative/coordinated attacks
- Types of collaborative attacks
- Open issues
- Proposed solutions
- Conclusions and outlook

Informal definition:

"Collaborative attacks (CA) occur when more than one attacker or running process synchronize their actions to disturb a target network"

Collaborative Attacks (cont'd)

- Forms of collaborative attacks
  - Multiple attacks occur when a system is disturbed by more than one attacker
  - Attacks in quick sequences is another way to perpetrate CA by launching sequential disruptions in short intervals
  - Attacks may concentrate on a group of nodes or spread to different group of nodes just for confusing the detection/prevention system in place
  - Attacks may be long-lived or short-lived
  - Attacks on routing

Collaborative Attacks (cont'd)

- Open issues
  - Comprehensive understanding of the coordination among attacks and/or the collaboration among various attackers
  - Characterization and Modeling of CAs
  - Intrusion Detection Systems (IDS) capable of correlating CAs
  - Coordinated prevention/defense mechanisms

Collaborative Attacks (cont'd)

- From a low-level technical point of view, attacks can be categorized into:
  - Attacks that may overshadow (cover) each other
  - Attacks that may diminish the effects of others
  - Attacks that interfere with each other
  - Attacks that may expose other attacks
  - Attacks that may be launched in sequence
  - Attacks that may target different areas of the network
  - Attacks that are just below the threshold of detection but persist in large numbers

Examples of Attacks that can Collaborate

- Denial-of-Messages (DoM) attacks
- Blackhole attacks
- Wormhole attacks
- Replication attacks
- Sybil attacks
- Rushing attacks
- Malicious flooding

We are investigating the interactions among these forms of attacks

Example of probably **incompatible** attacks:

Wormhole attacks need fast connections, but **DoM** attacks reduce bandwidth!

Examples of Attacks that can Collaborate (cont'd)

- Denial-of-Messages (DoM) attacks
  - Malicious nodes may prevent other honest ones from receiving broadcast messages by interfering with their radio
- Blackhole attacks
  - A node transmits a malicious broadcast informing that it has the shortest and most current path to the destination aiming to intercept messages
- Wormhole attacks
  - An attacker records packets (or bits) at one location in the network, tunnels them to another location, and retransmits them into the network at that location

Examples of Attacks that can Collaborate (cont'd)

- Replication attacks
  - Adversaries can insert additional replicated hostile nodes into the network after obtaining some secret information from the captured nodes or by infiltration. Sybil attack is one form of replicated attacks
- Sybil attacks
  - A malicious user obtains multiple fake identities and pretends to be multiple, distinct nodes in the system. This way the malicious nodes can control the decisions of the system, especially if the decision process involves voting or any other type of collaboration

Examples of Attacks that can Collaborate (cont'd)

- Rushing attacks
  - An attacker disseminates a malicious control messages fast enough to block legitimate messages that arrive later (uses the fact that only the first message received by a node is used preventing loops)
- Malicious flooding
  - A bad node floods the network or a specific target node with data or control messages

Current Proposed Solutions

- Blackhole attack detection
  - Reverse Labeling Restriction (RLR)
- Wormhole Attacks: defense mechanism
  - E2E detector and Cell-based Open Tunnel Avoidance (COTA)
- Sybil Attack detection
  - Light-weight method based on hierarchical architecture [Yi06]
- Modeling Collaborative Attacks using Causal Model

Blackhole attack detection: Reverse Labeling Restriction (RLR)

- Every host maintains a blacklist to record suspicious hosts who gave wrong route related information
- Blacklists are updated after an attack is detected
- The destination host will broadcast an INVALID packet with its signature when it finds that the system is under attack on sequence. The packet carries the host's identification, current sequence, new sequence, and its own blacklist
- Every host receiving this packet will examine its route entry to the destination host. The previous host that provides the false route will be added into this host's blacklist

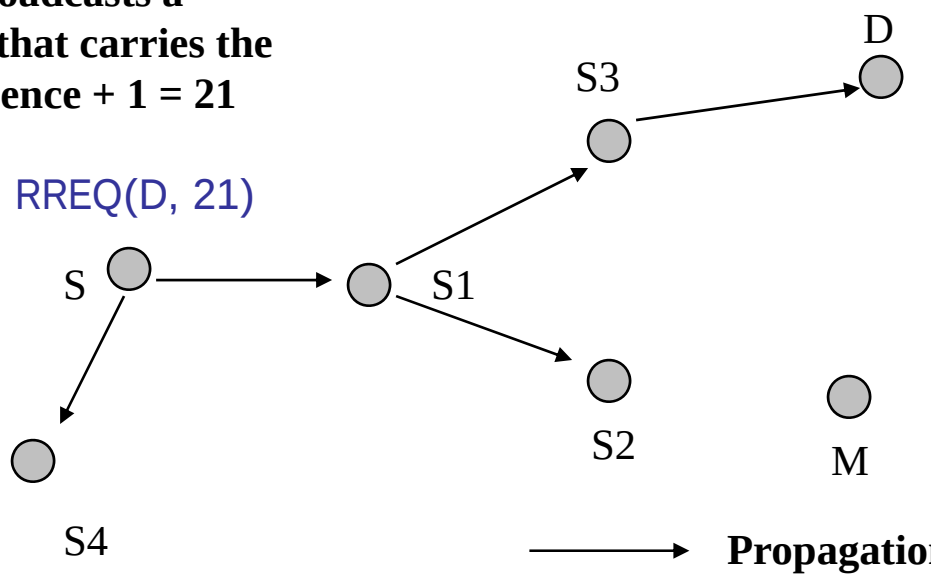
- W. Wang, Y. Lu and B. Bhargava, "On Security Study of Two Distance Vector Routing Prototols for Mobile Ad Hoc Networks." in the proceedings of IEEE International Conference on Pervasive Computing and Communications (PerCom'2003), Texas, March 2003.

RLR (cont'd)

Detecting false destination sequence attack by destination host during route rediscovery

- During Route Rediscovery, False Destination Sequence Number Attack is Detected, S needs to find D again
- Node movement breaks the path from S to M (trigger route rediscovery)

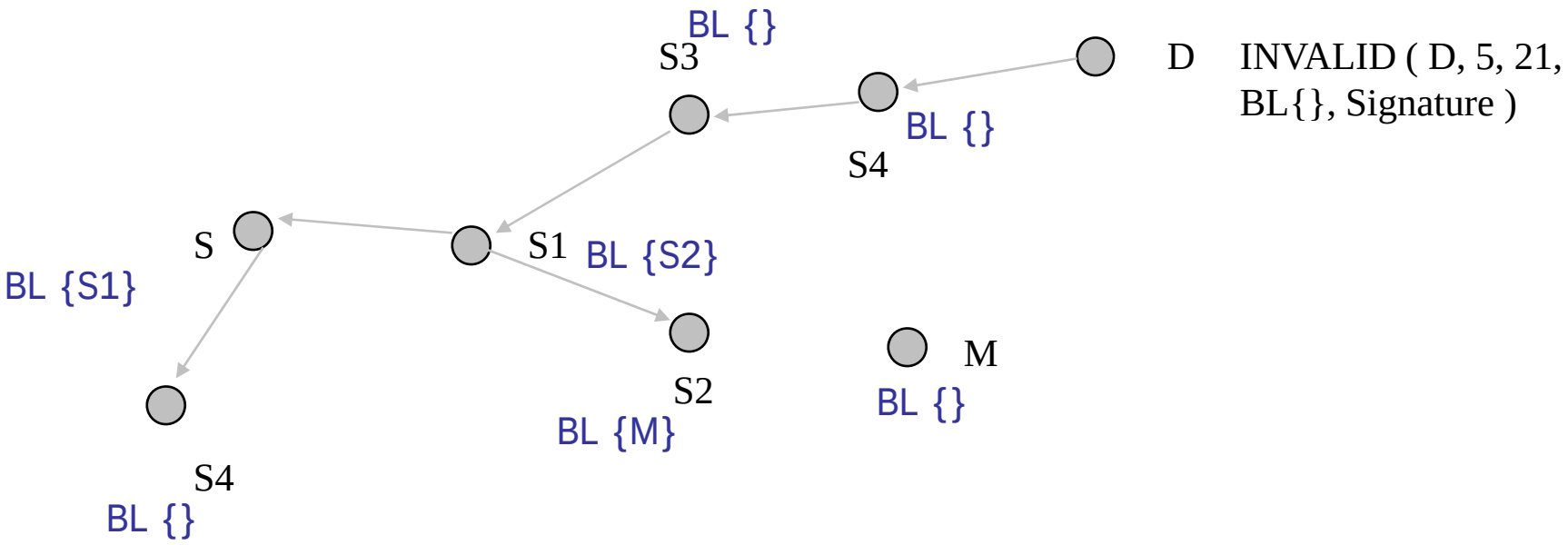
(1). S broadcasts a request that carries the old sequence + 1 = 21



(2) D receives the RREQ. Local sequence is 5, but the sequence in RREQ is 21. D detects the false destination sequence number attack.

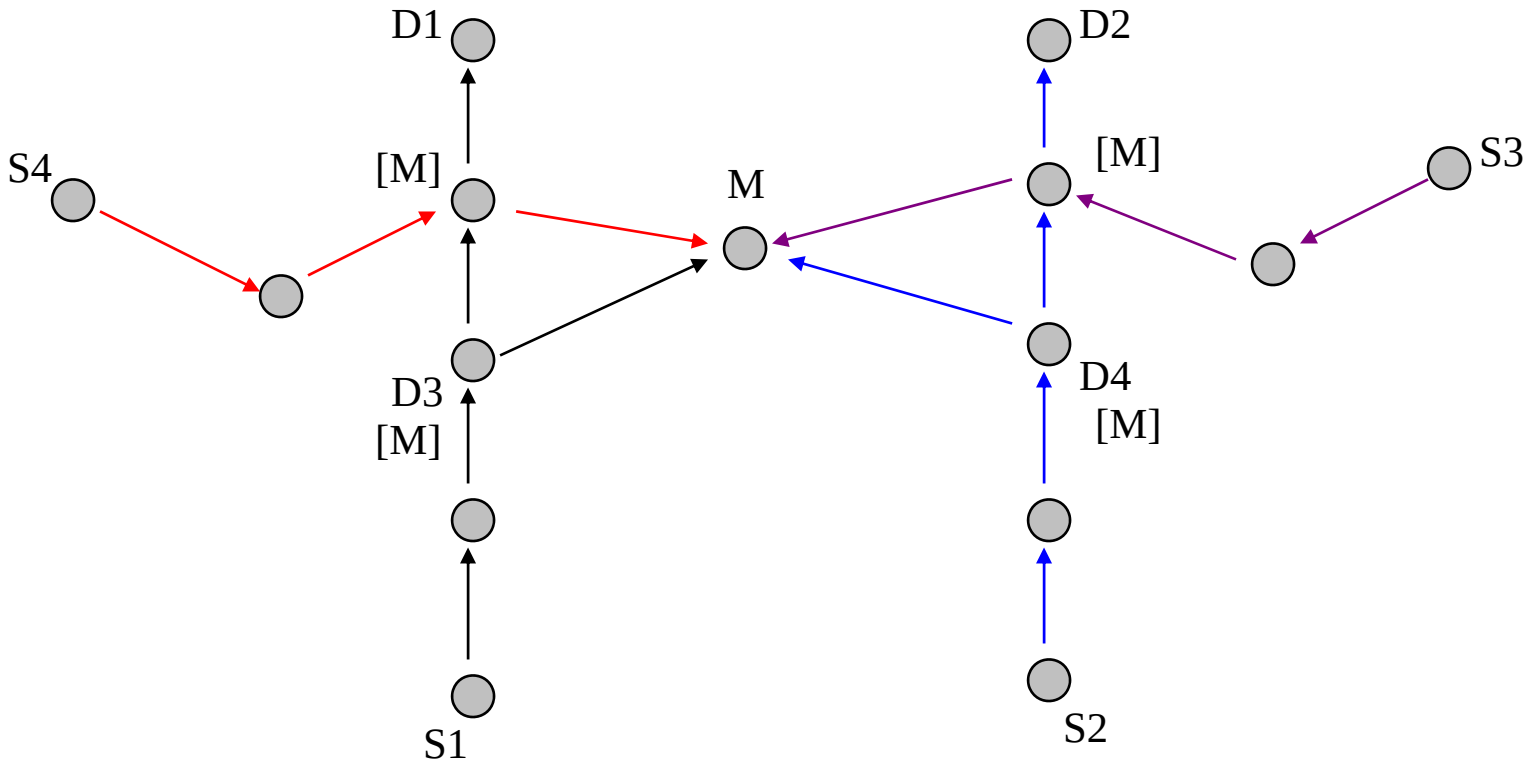
RLR (cont'd)

- Correct destination sequence number is broadcasted. Blacklist at each host in the path is determined



RLR (cont'd)

- Malicious site is in blacklists of multiple destination hosts

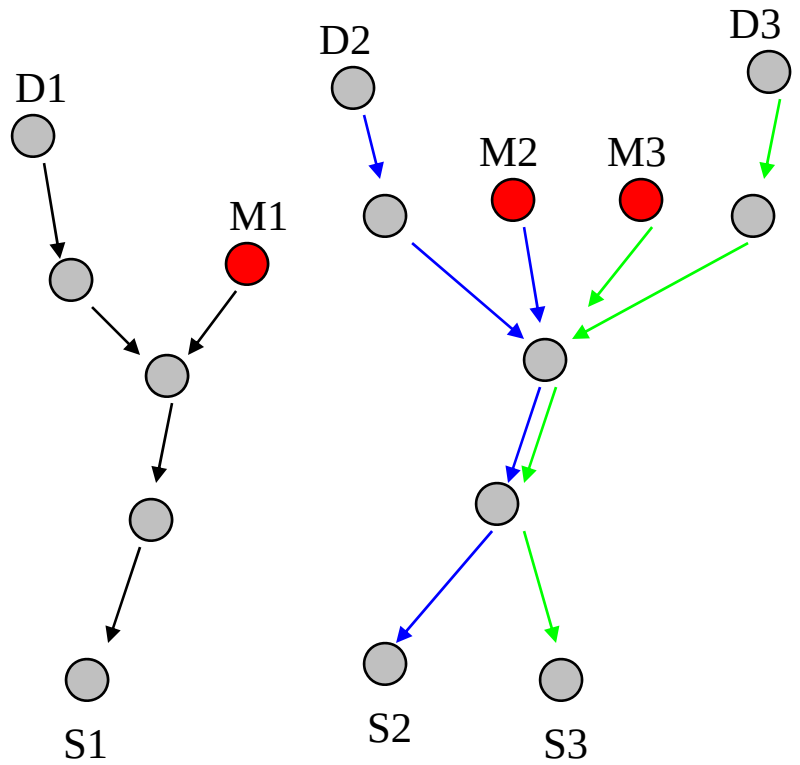


M attacks 4 routes (S1-D1, S2-D2, S3-D3, and S4-D4). When the first two false routes are detected, D3 and D4 add M into their blacklists. When later D3 and D4 become victim destinations, they will broadcast their blacklists, and every host will get two votes that M is malicious host

RLR (cont'd)

Acceleration in Intruder Identification

Multiple attackers trigger more blacklists to be broadcasted by D1, D2, D3



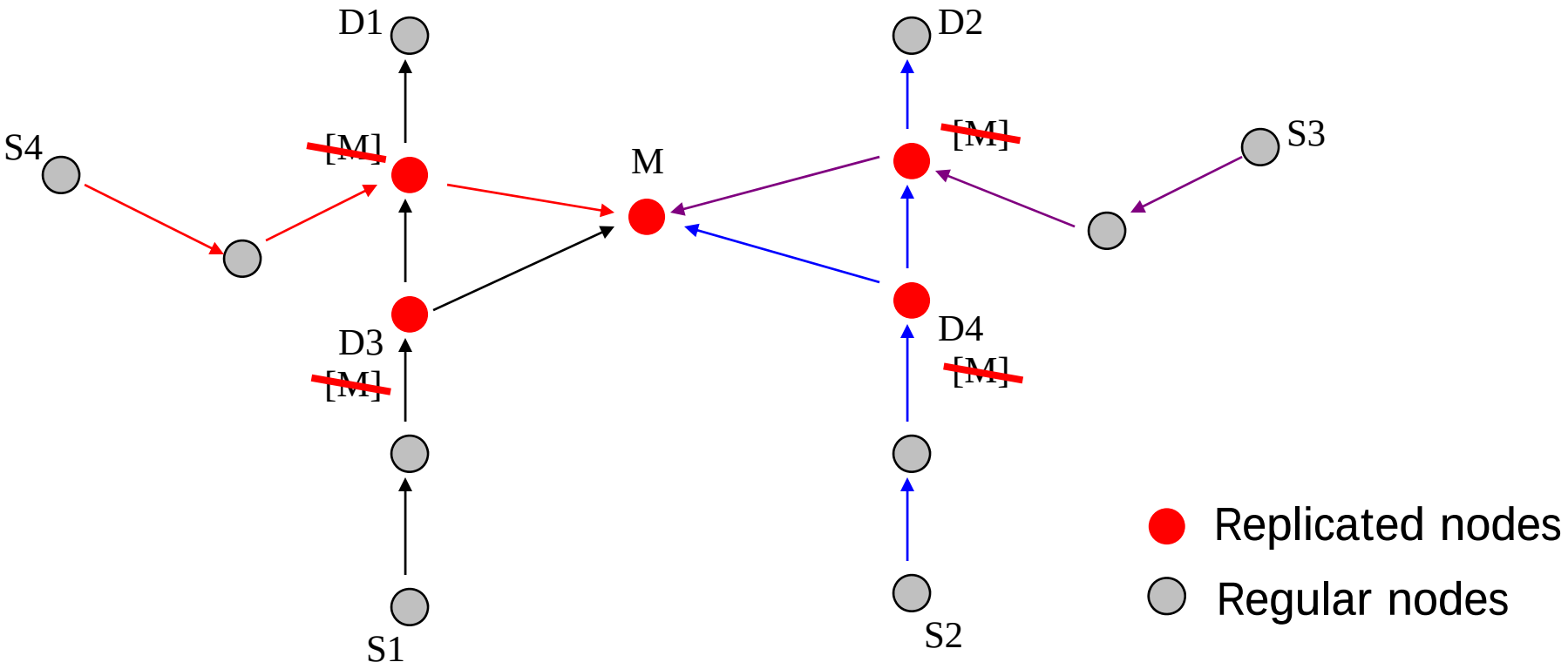
Coordinated attacks by M1, M2, and M3

RLR (cont'd)

- Update Blacklist by Broadcasted Packets from Destinations under Attack
  - Next hop on the false route will be put into local blacklist, and a counter increases. The time duration that the host stays in blacklist increases exponentially to the counter value
  - When timer expires, the suspicious host will be released from the blacklist and routing information from it will be accepted

Two Attacks in Collaboration: blackhole & replication

- The RLR scheme cannot detect the two attacks working simultaneously
- The malicious node M relies on the replicated neighboring nodes to avoid the blacklist



Wormhole Attacks defense

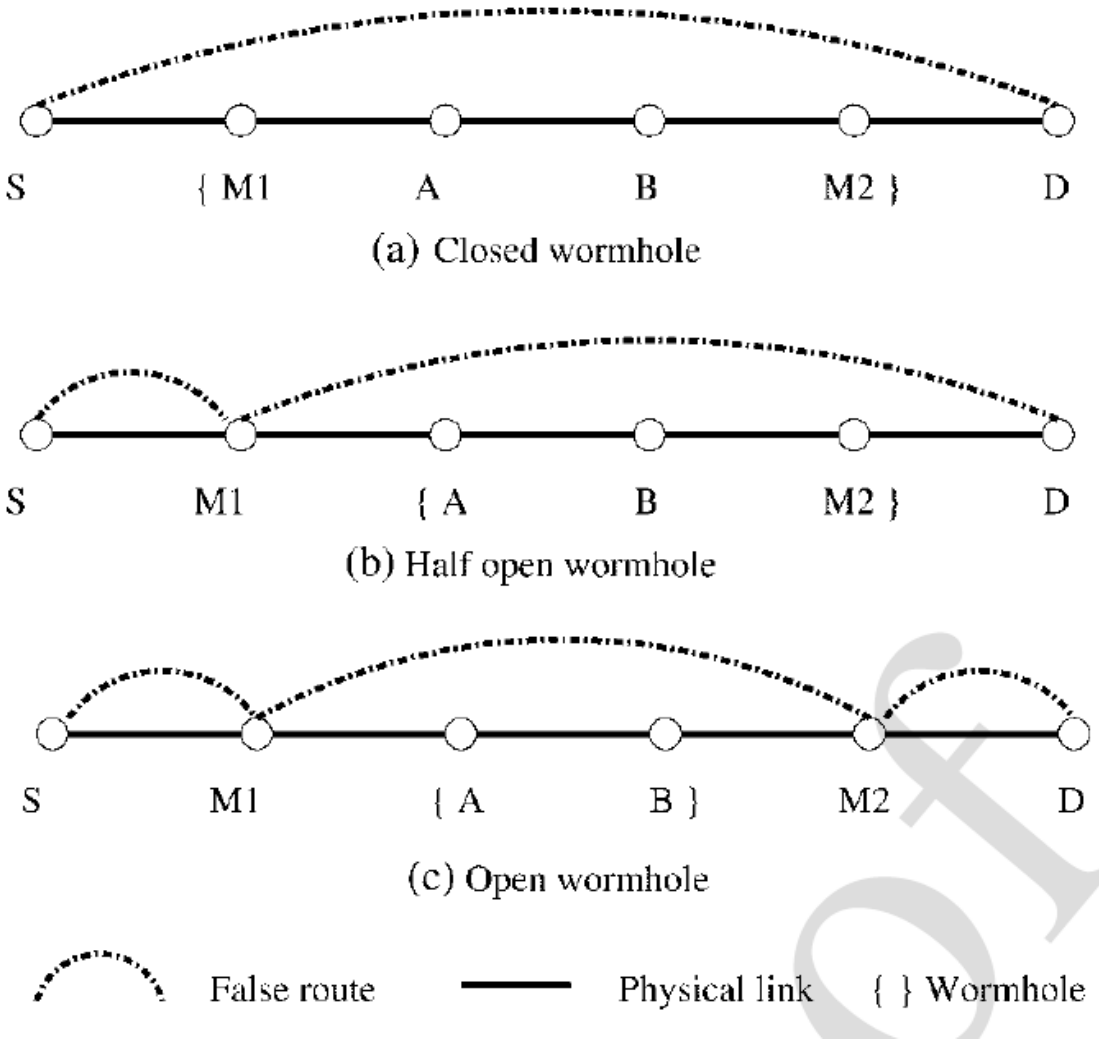
- A pair of attackers can form a tunnel, fabricating a false scenario that a short path between sender and receiver exists, and so packets go through a wormhole path being either compromised or dropped
- In many routing protocols, mobile nodes depend on the neighbor discovery procedure to construct the local network topology
- Wormhole attacks can harm some routing protocols by inducing a node to believe that a further away node is its neighbor

Wormhole Attacks: proposed defense mechanism

- This is a preliminary mechanism to classify wormhole attacks in its various forms
- It takes a more generic approach than previous work in the sense that it is end-to-end and does not rely on trust among neighbors
- It assumes trust between sender and receiver only to detect wormhole attacks on a multi-hop route
- Geographic information is used to detect anomalies in neighbor relation and node movements
- W. Wang, J. Kong, B. Bhargava, and M. Gerla, Visualisation of wormholes in underwater sensor networks: a distributed approach, Int. J. Security and Networks, Vol. 3, No. 1, 2008

Wormhole Attacks: proposed defense mechanism (cont'd)

- The e2e mechanism can detect:
  - Closed wormhole
  - Half open wormhole
  - Open wormhole



Wormhole Attacks: proposed defense mechanism (cont'd)

- The approach requires considerable computation and storage power as periodical wormhole detection packets are transmitted and the response are used to compute nodes position, velocity etc
- Because of that, an additional scheme called COTA is proposed to manage the detection information. It records and compares only a part of the <*time, position*> pairs
- Using a suitable relaxation, COTA has the same detection capability as the end-to-end mechanism

Wormhole Attacks: proposed defense mechanism (cont'd)

- Simulation evaluations: false positive with no attack

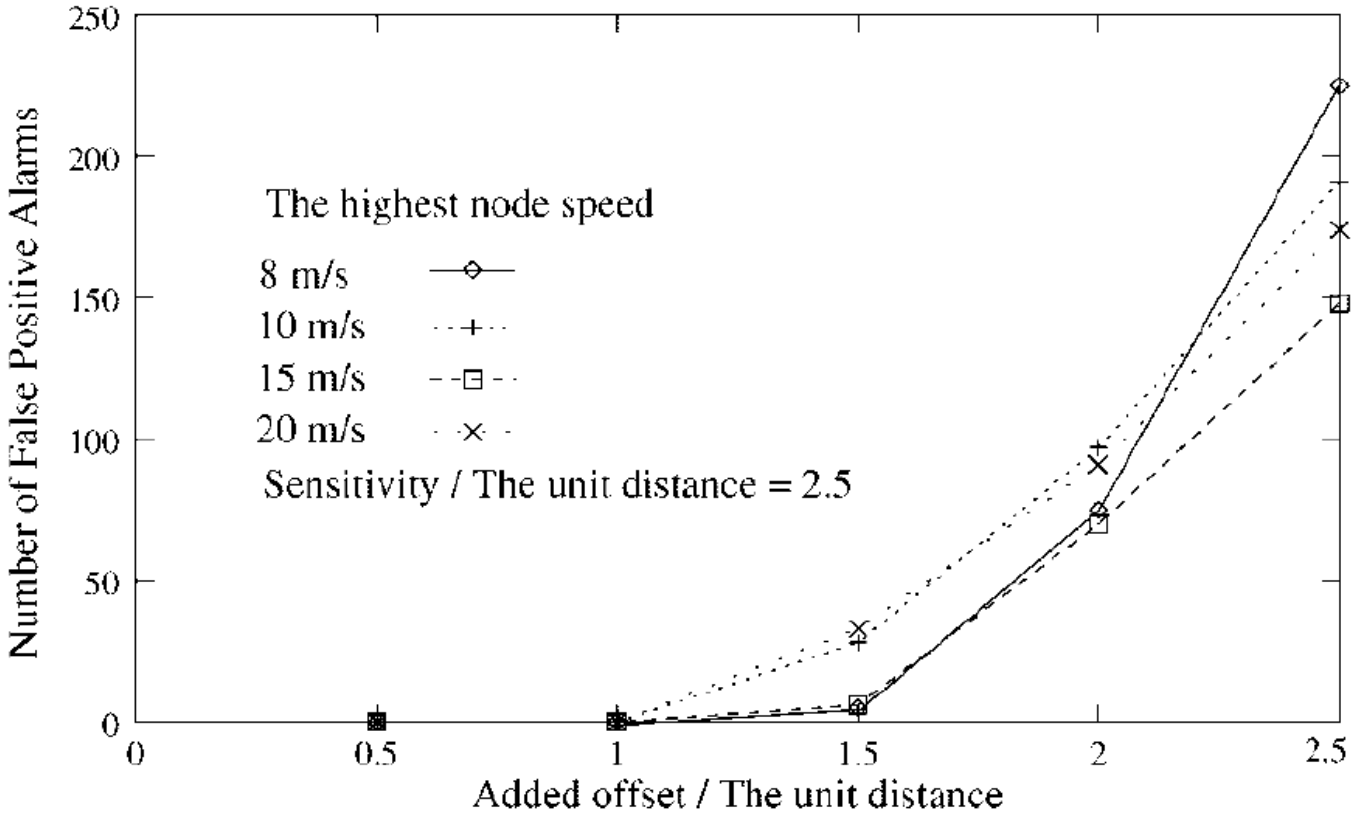


Fig. 6. False positive alarms: no wormholes, added offset/the unit distance changes.

Wormhole Attacks: proposed defense mechanism (cont'd)

- Simulation evaluations: false positive with attack

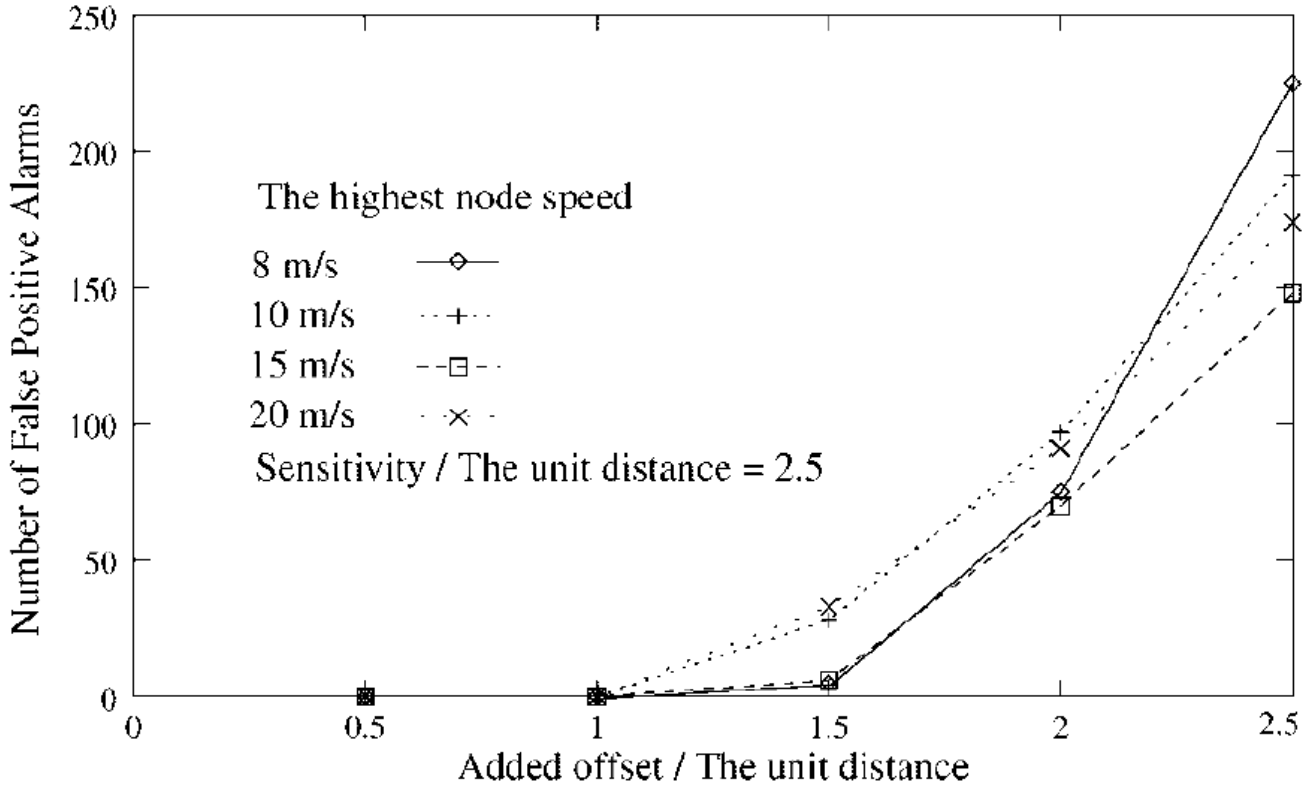


Fig. 7. False positive alarms: wormholes exist, added offset/ the unit distance changes.

Sybil Attack Detection

A Hierarchical Architecture for Sybil Attack Detection

- The Sybil attack is a harmful threat to sensor networks
  - Sybil attack can disrupt multi-path routing protocols by using a single node to present multiple identities for the multiple paths
  - Existing approaches are not oriented toward energy

Sybil Attack Detection: Proposed Method

- Use identity certificates to defend against Sybil attacks
- Each node is assigned some unique information by the setup server
- The server then creates an identity certificate for each level-0 node binding this node's identity to the assigned unique information
- The group leader creates an identity certificate for its group member (level-1 node)
- To securely demonstrate its identity, a node first presents its identity certificate, then it proves that it possesses the associated unique information

Modeling Collaborative Attacks

- Attack graph
  - A general model technique used in assessing security vulnerabilities of a system and all possible sequences of exploits an intruder can take to achieve a specific goal
  - We are currently working on a modeling for **collaborative graph attacks** to identify not only sequence of exploits but also concurrent and collaborative exploits. This leads to our **Causal Model**

Causal model

Purposes:

- Identify all attacks events that occur during the launch of individual and collaborative attacks
- Establish a partial order (or causal relationship) among all attack events and produce a “causal attack graph”
- Verify the security properties of the causal attack graph using model checking techniques.
  - Specifically, verify a sequence of events that lets the security checker proceeds from initial state to the goal state

Causal model (cont'd)

- Identify the set of events that are critical to perform the attacks.
  - Specifically, investigate how to find a minimum set of events that, once removed, would disable the attacks
- Determine whether the occurrences of some event/state transitions are based on message transmission or collaboration
  - Based on this, one can infer the degree of collaboration and temporal ordering in the system

Causal model (cont'd)

- A collaborative attack X can be modeled as a set of attacks {Xi} such that Xi is the local attack launched by attacker n
- Each local attack Xi is modeled by a FSM (finite state machine) and has independent state and event specifications, such as preconditions, postconditions, and state transition rules
- In simple distributed attacks such as Distributed Denial-of-Service Attacks, the FSMs of each local attack can be the same. However, in sophisticated collaborative attacks, FSMs of local attacks are not necessarily homogeneous
- Each local attack Xi can be formally defined as:
  <Sn, En, Mn, Ln>
  - **Sn** denotes a set of states in the local attack, **En** denotes a set of events in the local attack, **Mn** denotes a set of communication messages, and **Ln** denotes a set of local operations on Mn.

Causal model (cont'd)

- In collaborative attacks, events in attacks occur in certain sequences. A sequence of attack events may cause more damage to the system than others
- There are certain relationships among the events and we model the relationships by causal rules.

- Definition of causal rules
  - A causal rule U consists of
  - <P, Q, A>
  - P and Q are events
  - A is one of the causal relationships (->, →, - →>)

Conclusions

- Exciting area of research
- Modeling attacks in collaboration is a very topical issue
- Tradeoff between accuracy and computation inexpensiveness is critical

Future work

- A lightweight learning toll is to be applied to enhance our current approaches
- The remaining types of attacks will be addressed
- Models for detecting attacks in collaboration are underway and the causal model will be evaluated in depth
- General guidelines will be defined to protect ad hoc networks from potential attacks
- More simulations and real life experiments

References (1)

[BH83] B. Bhargava and C. Hua, "A Causal Model for Analyzing Distributed Concurrency Control Algorithms," IEEE Transactions on Software Engineering, 1983.

[DETER] DETER: A Laboratory for Security Research, http://www.isi.edu/deter/.

[Do02] J. Douceur, "The Sybil Attack," *Proc. IPTPS*, Feb. 2002.

[FQL06] H. Fu , S. Kawamura, and C. Li, " Bloom-based Q-composite: A Generalized Framework of Random Key Pre-distribution Schemes for Wireless Sensor Networks," *Proc. IEEE International Conference on Intelligent Robots and Systems*, Oct. 2006.

[HPJ03a] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," *ACM Workshop on Wireless Security (WiSe)*, Sep 2003.

References (2)

[La78] L. Lamport, Time clocks, and the ordering of events in a distributed, system, Communication of ACM, vol.21, pp.558-564, July 1978.

[MFMG05] K. Mandalas, D. Flitzanis, G. F. Marias, and P. Georgiadis, "A Survey of Several Cooperation Enforcement Schemes for MANETs," *Proc. IEEE ISSPIT2005*, Symposium on "Security and Privacy in Mobile and Wireless Computing, Dec. 2005,

[NM04] K. Nadkarni and A. Mishra, "A novel intrusion detection scheme for wireless ad hoc. networks," *Proc. IEEE WCNC'04*, Mar., 2004.

[PM03] A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks," *Proc. Radio and Wireless Conference RAWCON,* Aug. 2003.

[QSL05] L. Qian, N. Song and X. Li, "Detecting and locating wormhole attacks in wireless ad hoc networks through statistical analysis of multi-path," *IEEE Wireless Communications and Networking Conference (WCNC),* Mar. 2005.

References (3)

[RB07] R. Oliveira and T. Braun, "A Smart TCP Acknowledgment Approach for Multihop Wireless Networks," IEEE Transactions on Mobile Computing, Vol. 6, No. 2, pp. 192-205, Feb. 2007.

[RFKN05] S. Ramaswamy, H. Fu, and K. Nygard, “Effect of Cooperative Black Hole Attack on Mobile Ad Hoc Networks,” *Proc. ICWN*, Jun. 2005.

[Yi06] Yin, “Poblems and Solutions for Handling Attacks in Sensor Networks,” *Ph.D. thesis*, *University of Missouri-Rolla*, MO. 2006.

[WBLW06] W. Wang, B. Bhargava, Y. Lu, and X. Wu, “Defending against Wormhole Attacks in Mobile Ad Hoc Networks,” *WCMC*, vol. 6, issue 4, pp. 483-503, Jun. 2006.

[WKBG] W. Wang, J. Kong, B. Bhargava, and M. Gerla, Visualization of wormholes in underwater sensor networks: a distributed approach, Int. J. Security and Networks, Vol. 3, No. 1, 2008

[WBLW] W. Wang, B. Bhargava, Y. Lu, and X. Wu. "Defending Against Wormhole Attacks in Mobile Ad Hoc Networks." Wiley Journal on Wireless Communications and Mobile Computing, Vol 5, 1-21, 2005.

[WB] X. Wu and B. Bhargava. "A02P: Ad Hoc On-Demand Position-Based Private Routing Protocol." IEEE Transactions on Mobile Computing Vol. 4, No. 4, 335-348, July, 2005.

[LBWZW] Y. Lu, B. Bhargava, W. Wang, Y. Zhong, and X. Wu, "Secure Wireless Network with Movable Base Stations." in IEICE Transaction on Communications, IEICE/IEEE Joint Special Issue on Assurance Systems and Networks, Vol.E86-B, No. 10, pp. 2922 - 2930, 2003.