Resist Malicious Packet Dropping in Wireless Ad Hoc Networks

Tao Wan
Digital Security Group
School of Computer Science
Carleton University

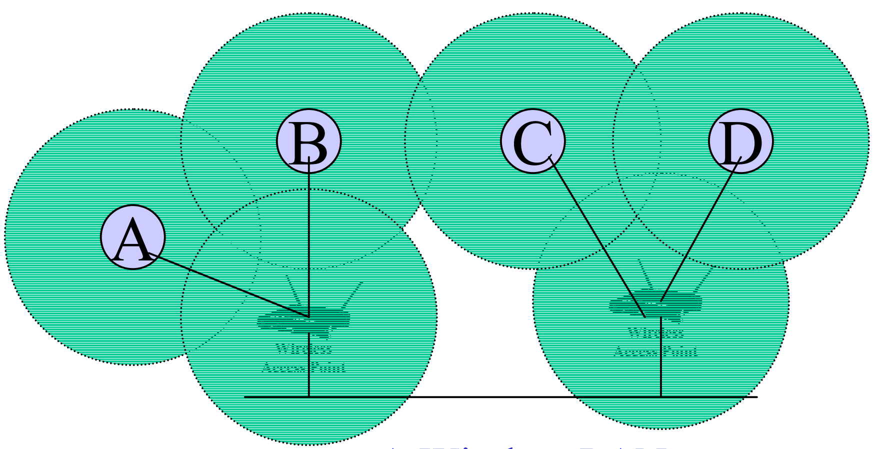
Oct 10, 2003

Outline

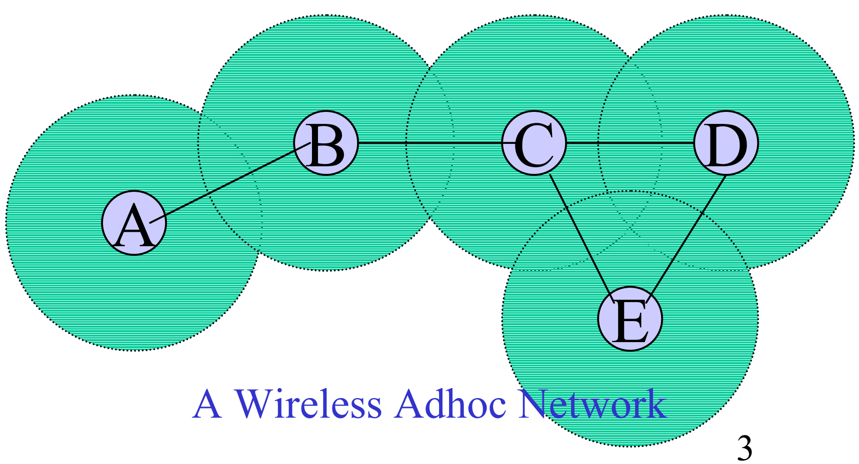
- Introduction
- Related Work
- Distributed Probing
- Simulation Results
- Concluding Remarks

Wireless Ad Hoc Networks

- A group of mobile wireless nodes
- No fixed infrastructures
- Dynamic network topology
- Cooperative routing protocols
- Mobile Ad hoc NETworks (MANET)



A Wireless LAN



A Wireless Adhoc Network

MANET Routing Protocols

- Dynamic Source Routing (DSR)
- Ad hoc On demand Distance Vector (AODV)
- Destination-Sequenced Distance Vector (DSDV)
- Optimized Link State Routing (OLSR)

MANET Routing Protocol Vulnerabilities

- No security protection mechanisms
  - No entity authentication
  - No message authentication
- Weak Assumptions
  - Nodes are trustworthy
  - Nodes are cooperative

Denial of Service (DoS) Attacks against MANET

- DoS by exploiting routing vulnerabilites
  - Blackhole, Congestion
  - Invalid routes (loop, network unreachable, etc)
- DoS by injecting/dropping data traffic
  - Clogging (injecting packets)
  - Malicious packet dropping

Malicious Packet Dropping

- Serious DoS attacks
  - many motivations
  - combined with other attack techniques
- Easy to launch
  - compromise nodes, join a network
- Difficult to detect
  - passive
  - No detection mechanism in protocol stacks
    - link layer, network layer, transport layer

Related Work

Secure Routing Protocols

- Asymmetric cryptographic primitives
  - Digital signatures
- Symmetric Cryptographic primitives
  - One-time digital signatures
  - One-way hash chains
  - Authentication trees
  - ...

Defeat Clogging

- Quality of Service (QoS)
- IP traceback / Pi (Path identification)
- Egress/Ingress filtering

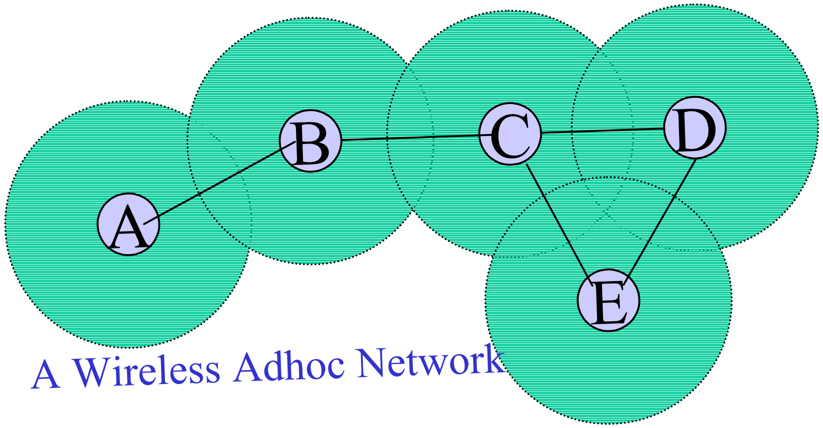
Detect and mitigate packet dropping

- Perlman proposed a hop-by-hop ACK in 1988 [PER88]
- Cheung proposed a neighborhood probing for wireline network in 1997 [CHE97]
- Bradley proposed a distributed monitoring approach for wireline network in 1998 [BRA98]
- Marti, et al proposed a neighborhood overhearing for MANETs in 2000 [MAR00]
- Padmanabhan and Simon proposed secure traceroute in 2002 [PAD02].

Distributed Probing

Distributed Probing Scheme

- Every node monitor the forwarding behavior of every other node by probing
- An Example
  - Suppose node A wants to know if B forwards A's packets to C
  - A sends a probe message to C through B
  - If A receives an ACK from C, it knows that B is good
  - Otherwise, it is possible that B is bad



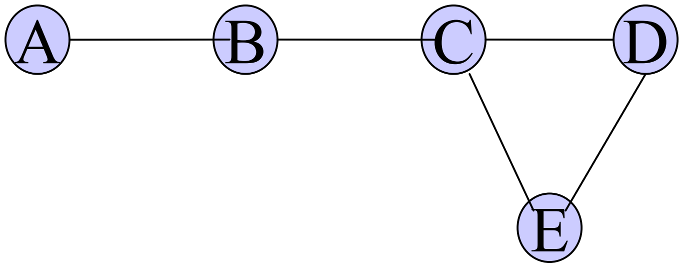
Assumptions

- Probe messages are indistinguishable from data packets
  - IP layer security (IPsec ESP)
  - adversaries have limited capability (e.g., dropping packets by manipulating routing tables)
- Multi-hop source routing protocols (e.g., DSR)
- Bi-directional communication links (e.g., IEEE 802.11)

Dynamic Source Routing (DSR)

- Route discovery & Route maintenance
- On-demand/source routing
- Routing cache (path/link)

B	A→B
C	A→B→C
D	A→B→C→D
D	A→B→C→E→D
E	A→B→C→E
E	A→B→C→D→E



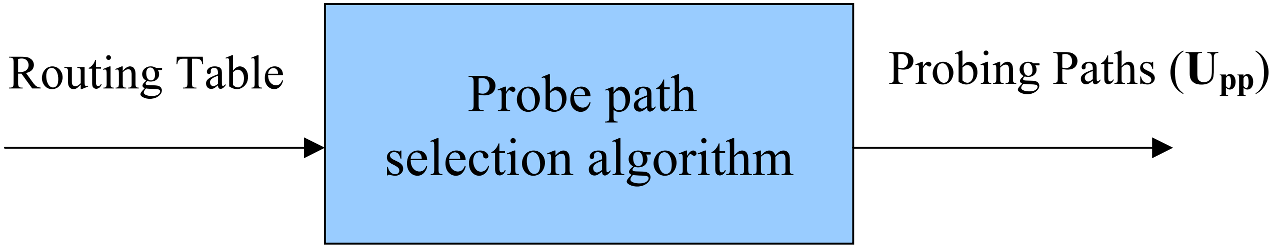
Distributed Probing

- Design Questions
- Probe path selection algorithm
- Distributed probing algorithm
- Node diagnosis algorithm
- Avoid detected BAD nodes in path selection

Design Questions

- Which nodes to probe
  – All nodes / a subset of nodes
- Which path to probe over
  – Shortest / longest / any path
- How to probe over a path
  – From nearest to furthest
  – From furthest to nearest
  – Binary search, etc
- When to probe
  – periodically / on demand

Probe Path Selection



Probe Path Selection

- Notations
  - $\mathbf{U_{pp}}$ is a set of paths
  - A path, p, is a set of nodes with order
  - The length of p is the number of hops, | p|
  - For $0 \le i \le |p|$, p[i] is the i^{th} node in the path
- Examples
  - p_1={A, B, C, D}, p_2 ={A, C, B, D}, then $p_1 \neq p_2$
  - $|p_1|=3$
  - $p_1[3]$ = D, $p_1[2]$ = C, $p_1[1]$ = B, $p_1[0]$ = A
  - $p_1[|p_1|]$ = D, $p_1[|p_1|-1]$ = C, ...

Probe Path Selection

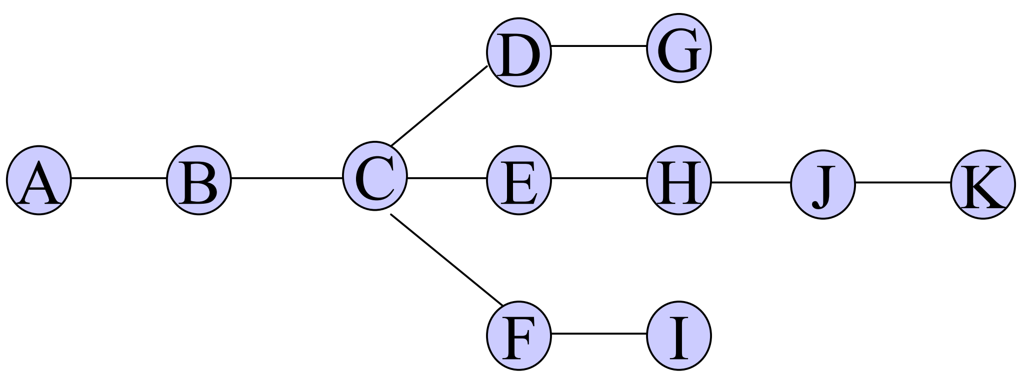
- Rule #1
  - $\forall\, p_i, p_j \in \mathbf{U_{pp}}, p_i \not\subset p_j$
  - p_1={A, B, C}, p_2 ={A, B, C, D}, remove p_1
- Rule #2
  - $\forall\, p_i, p_j \in \mathbf{U_{pp}}, p_i[|p_i|-1] \notin p_j - |p_j|$
  - p_1={A, B, C}, p_2 ={A, B, D, E}, remove C from p_1
- Rule #3
  - $\forall\, p_i \in \mathbf{U_{pp}}, |p_i| > 1$

Distributed Probing Algorithm

- Probe a path from the furthest node to the nearest
- $\forall$ $p \in$ $\mathbf{U_{pp}}$, probe $p[|p|]$
- If an ACK is received, $\forall$ $v \in p$ and $v \neq p[|p|]$, v is *Good*
- Otherwise, probe $p[|p|-1]$.
- If an ACK is not received from $p[i+1]$ ($0 \le i < |p|$) but received from $p[i]$, diagnose $p[i]$

Distributed Probing Algorithm

- Simple idea
- The implementation is little bit complex
  - ACK may be lost
  - Retransmission of probing messages (k out of n)



Node Diagnosis Algorithm

- If p[i] is responsive, but p[i+1] is not. Three possibilities:
  - p[i] is *Bad*
  - p[i+1] is *Down*
  - the link p[i] → p[i+1] is broken
- Search next shortest path, p_a, to p[i+1] without going through p[i]
- if p[i+1] is responsive, probe p[i] over p_a → p[i+1] → p[i]. If p[i] is responsive, p[i] is *Bad*. Otherwise, p[i] → p[i+1] is broken for other reasons.

Simulation Results

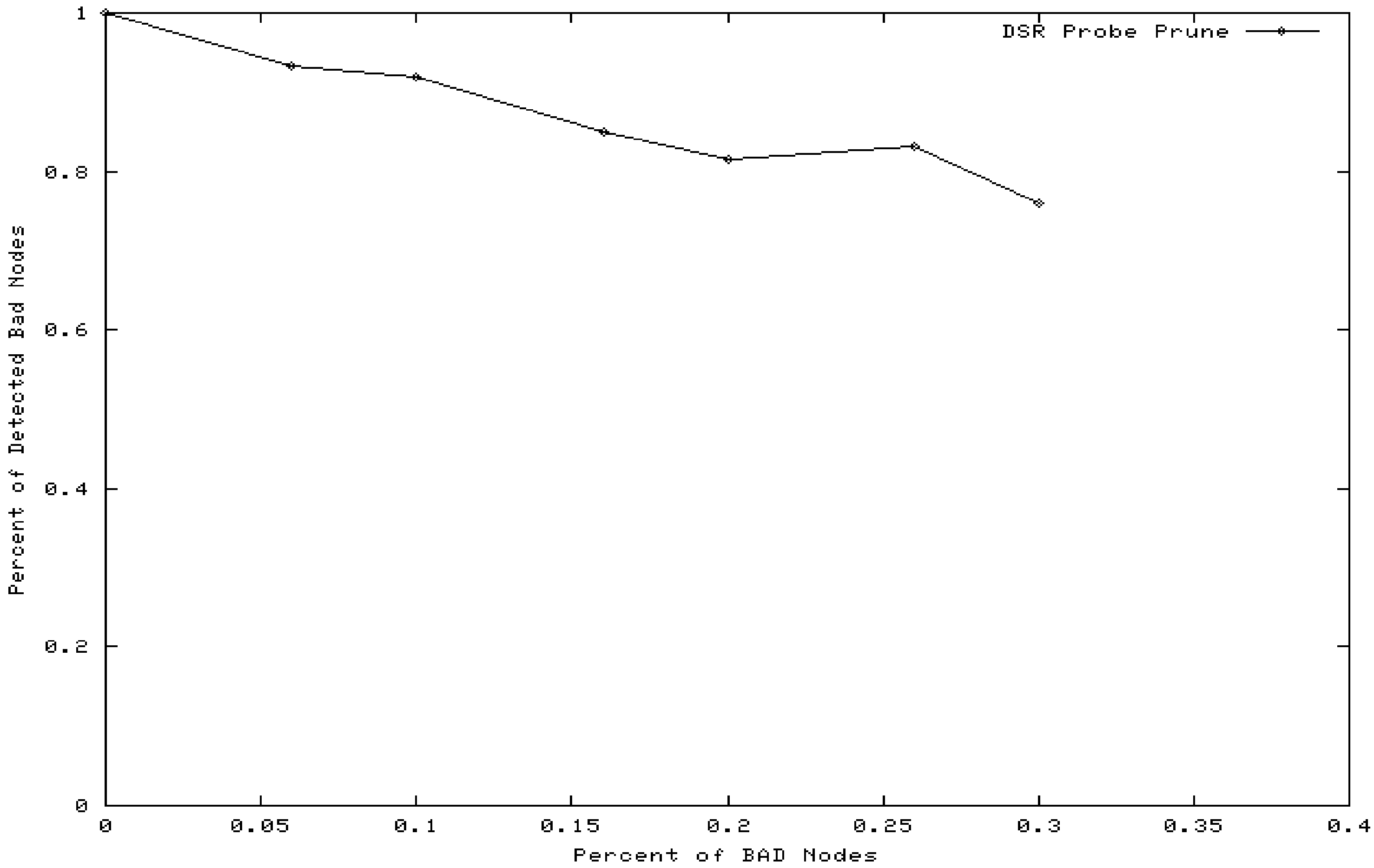
Simulation Environment

- NS-2 v2.1b9a with CMU wireless extensions
- DSR with path routing caches
- 670m x 670m, 50 mobile nodes
- random waypoint mobility model
- maximum speed 20m/s
- pause time: 0, 50, 100 seconds
- Comm pattern: 10 connects, 4 packets/s
- # of bad nodes: 0, 3, 5, 8, 10, 13, 15

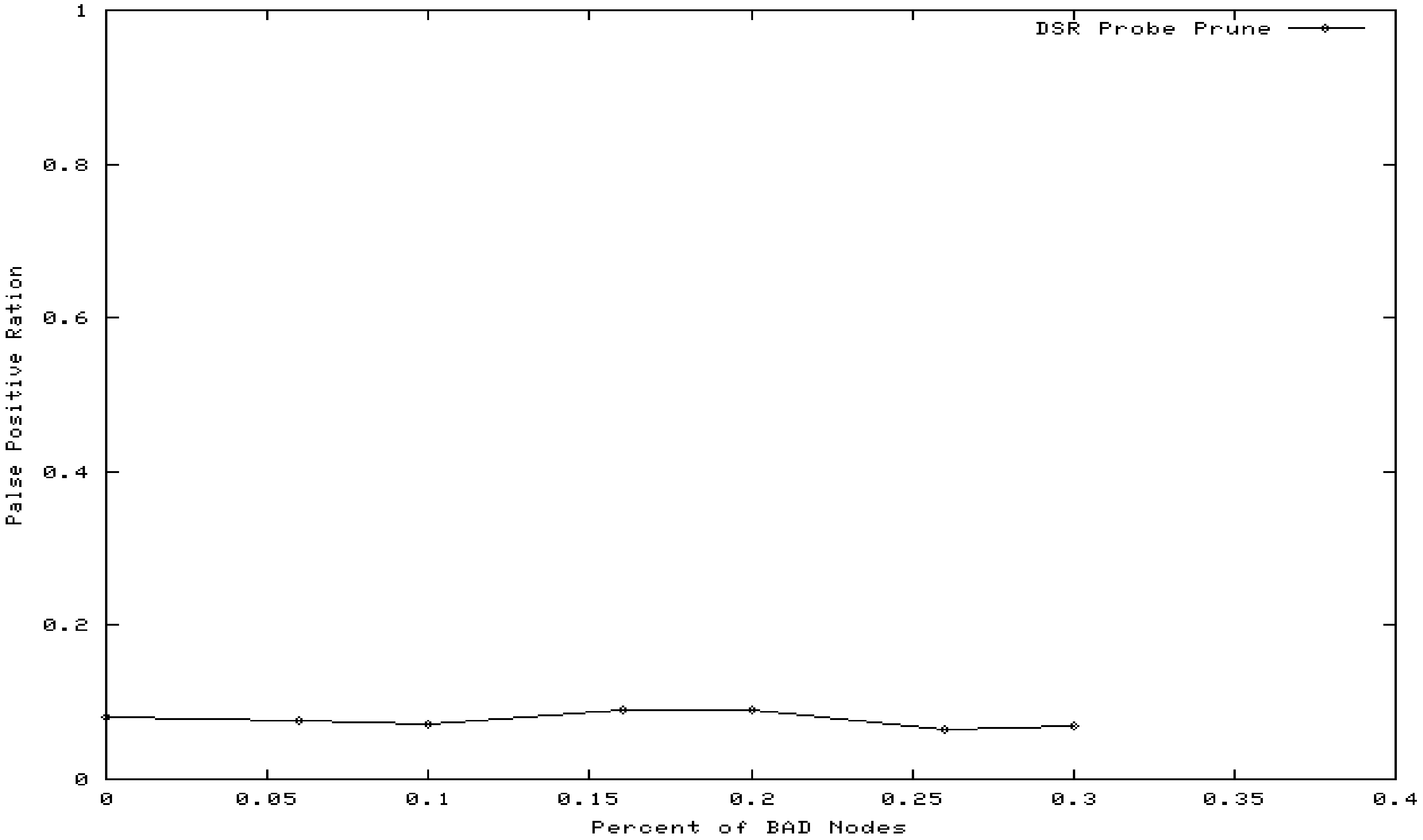
Metrics

- Detection rate
  - # of detected BAD nodes / # of actual BAD nodes
- False positive rate
  - # of GOOD nodes mistakenly detected as BAD / # of GOOD nodes
- Packet delivery rate
  - # of data packets received / # of data packets sent in application layer
- Network overhead
  - # of routing related packet transmissions (including probe messages) / # of packet transmissions

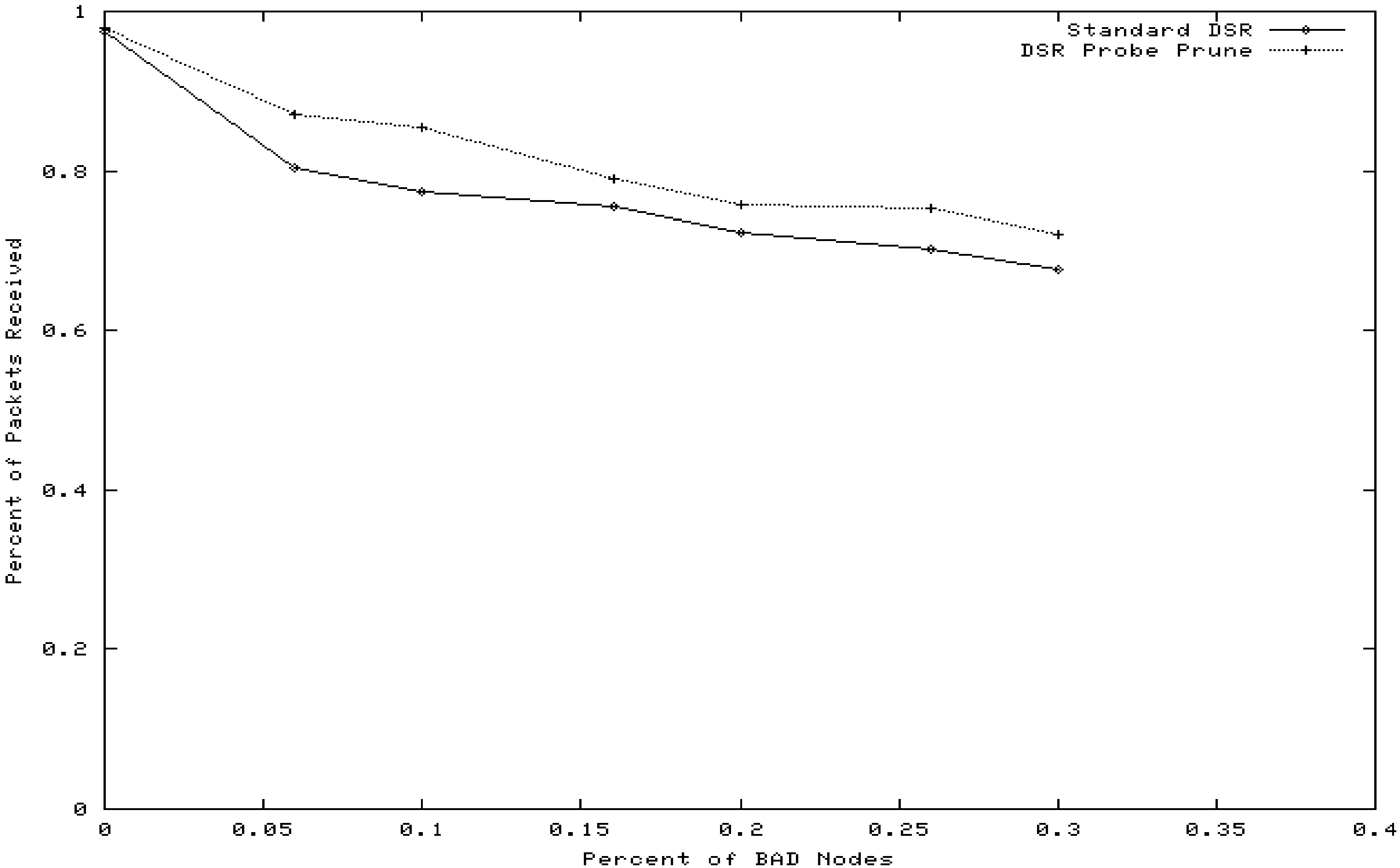
Detection Rate
(50-Second pause time)



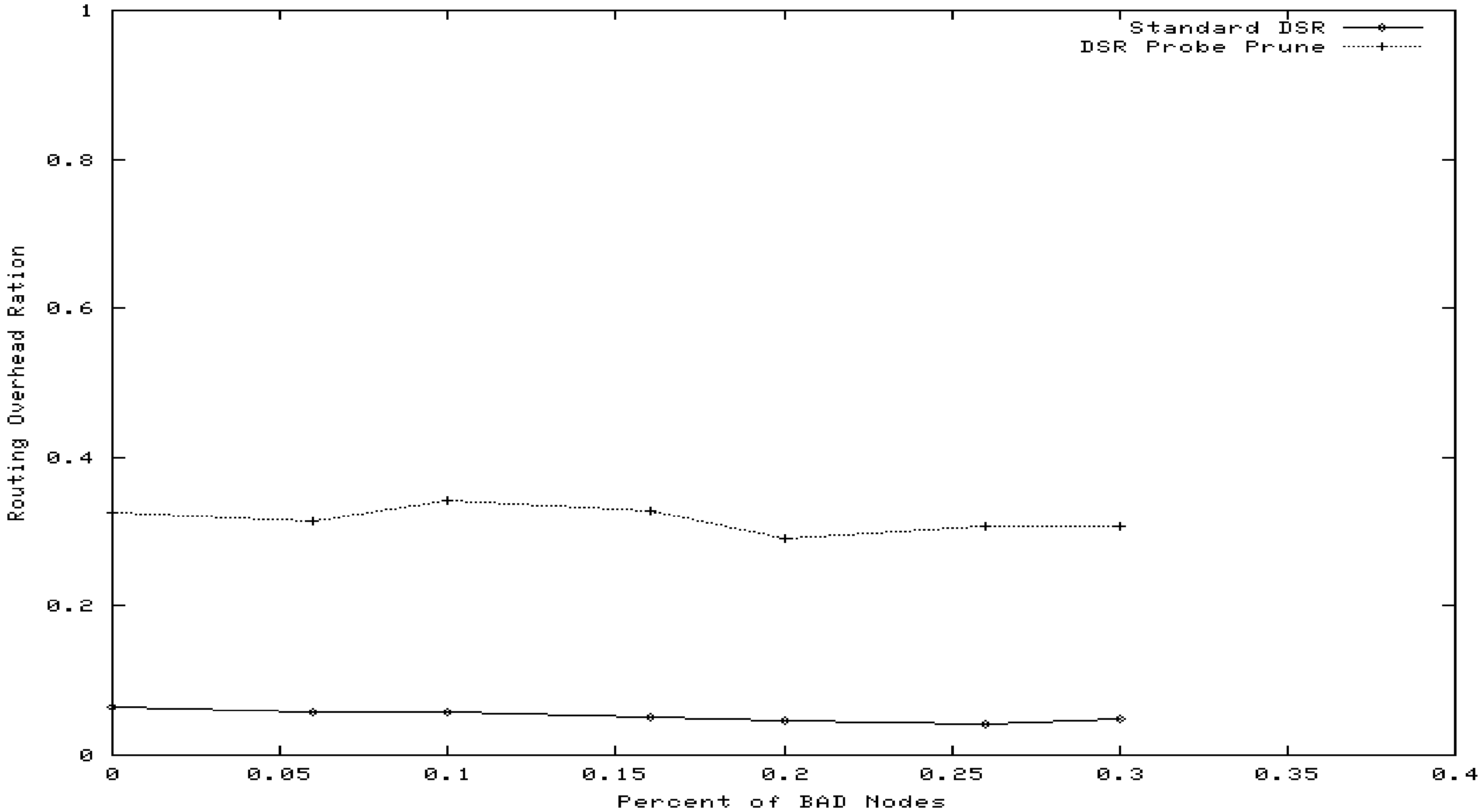
False Positive Rate
(50-Second pause time)



Network Throughput (50-Second pause time)



Overhead
(50-Second pause time)



Concluding Remarks

Concluding Remarks

- Incremental deployment
  - Independent from existing routing protocols
- Overhead Reduction
  - piggyback data packets
- Detection Rate Improvement
  - combined with overhearing

References

[BRA98] K.A. Bradley, S. Cheung, N. Puketza, B. Mukherjee, and R.A. Olsson. "Detecting Disruptive Routers: A Distributed Network Monitoring Approach". In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 115-124, May 1998.

[CHE97] S. Cheung and K. Levitt. "Protecting routing infrastructure from denial of service using cooperative intrusion detection". In *Proceedings of New Security Paradigms Workshop*, Cumbria, UK, September 1997.

[MAR00] S. Marti, T.J. Giuli, K. Lai, and M. Baker. "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks". In *Proceedings of the Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM 2000)*, August 2000.

[PER88] R. Perlman. "Network Layer Protocols with Byzantine Robustness". *PhD thesis*, Massachusetts Institute of Technology, August 1998.

Thanks!