

Security Vulnerabilities in Channel Assignment of Multi-radio Multi-channel Wireless Mesh Networks

Salil S. Kanhere

joint work with Anjum Naveed

Network Research Laboratory (NRL)

<http://www.nrl.cse.unsw.edu.au>

School of Computer Science and Engineering

The University of New South Wales

Sydney, Australia

UNSW } ENGINEERING
THE UNIVERSITY OF NEW SOUTH WALES





Outline

- Introduction
- Channel Assignment in Multi-radio Multi-Channel Wireless Mesh Networks
- Proposed Attacks
- Simulation Results
- Attack Prevention and On-going Work
- Conclusion



Project SWIMNET

- Smart Internet CRC
- Focus on multi-radio multi-channel mesh networks
- Two work packages
 - WP1- QoS, Capacity enhancement
 - WP2- Security
- Test-bed
 - 20-25 node mesh network



Introduction

- Wireless Mesh Networks (WMN) are emerging as a key last-mile access technology
 - Fast, easy and inexpensive network deployment
- Rapid deployments planned in major metropolitan cities, e.g.: Taipei, Moscow, Philadelphia,
- Security has largely been an afterthought
- The 802.11s standard proposes to use 802.11i for providing security
 - per-hop data confidentiality, data integrity, authentication
 - Problems associated with end-to-end security (identified in our other work)
 - Primary focus on intrusion prevention services
- Misbehaving/selfish node can seriously undermine the performance of the WMN



Security Issues in WMN – Network Layer



- Malicious nodes
 - Injecting bad packets, dropping good packets
- Selfish nodes
 - Why should I forward someone else's traffic when I can use those transmission opportunities for myself?
- Routing protocols assume that participating nodes are well behaved
- In WMN all nodes may not owned by same owner
 - My WMN router connected to my neighbour's router for Internet access.
 - Need to provide for end-to-end confidentiality and integrity within WMN
 - Verification/monitoring of nodes to ensure they confirm to the expected behaviour



Network Layer Security - Attacks

- Control Plane Attacks
 - Rushing attacks
 - Wormhole attacks
 - Black hole attacks (sinkhole in WSN)
 - Routing and channel assignment attacks
- Data Plain Attacks
 - Sleep deprivation attack in ad hoc/sensor networks
 - Malicious packet injection
 - Selective packet drop
 - Selfish behavior



Multi-radio Multi-channel WMN

- Wireless spectrum provides for multiple channels some of which are orthogonal
 - 3 orthogonal channels in 802.11b spectrum and 11 in 802.11a
- Mesh nodes can be equipped with multiple radios to increase the network capacity
- Several joint channel assignment and routing schemes have been proposed
 - Hyacinth (Rainawala, et al.)
 - SSCH (Bahl, et al.)
 - many more

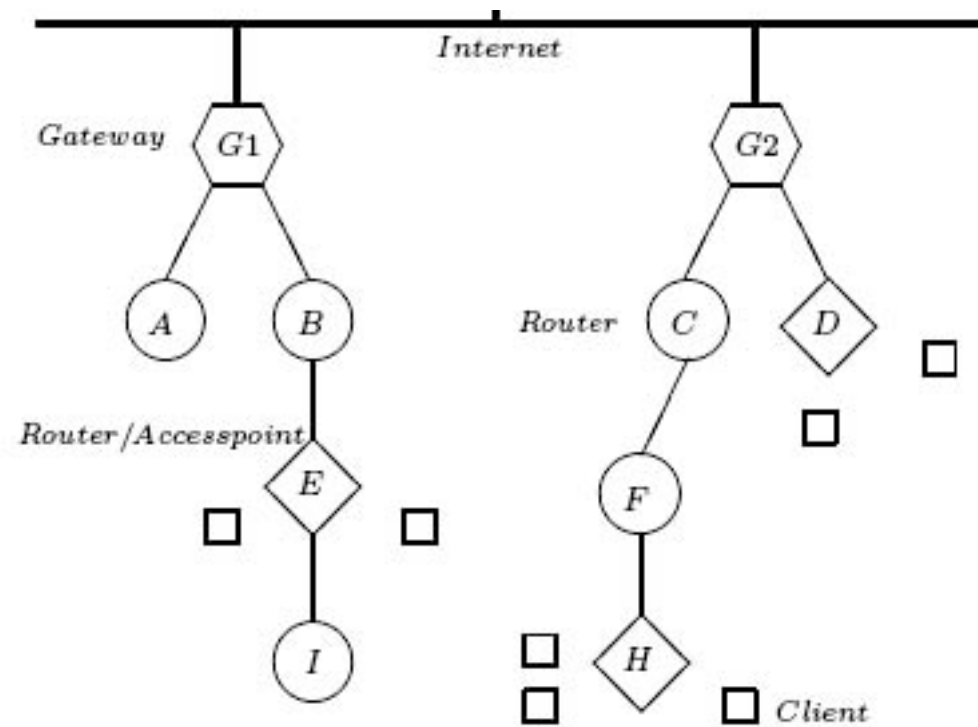


Hyacinth

- Interfaces of each node are divided in UP and DOWN interfaces
- Channel assignment for UP-NICs is responsibility of the parent node whereas each node looks after the assignment of DOWN-NICs
- Channels used by links closer to the gateway have higher priority
- Decision on channel assignment is based on
 - bandwidth usage
 - hop-count distance from the gateway and
 - channel assignment of interference domain neighbours
- Nodes periodically exchange channel assignment and bandwidth usage information



WMN Architecture



July 19, 2006



Why are these attacks possible?

- Channel assignment algorithms require WMN nodes to exchange channel assignment and usage information (CHNL_USAGE message in Hyacinth)
- Nodes are assumed to be well-behaved
- Complete trust in transmitted control information



Assumptions

- Attacks assume the existence of a misbehaving/selfish node
- Attacks are presented within the context of the Hyacinth framework
 - Extensible to other schemes
- Channel used on a particular link is associated with its parent node
- Links closer to gateway are heavily loaded
 - High priority heavily loaded channel



Proposed Attacks



- Parasite Attacks
 - Network Endo-Parasite Attack (NEPA)
 - Channel Ecto-Parasite Attack (CEPA)
- Low-cost Ripple Effect Attack (LORA)



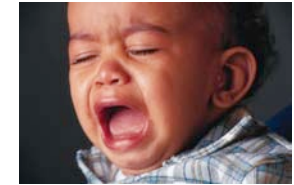
Parasite Attacks



- Objective - Increase interference on heavily loaded high priority channels
- A malicious/selfish node assigns one or more of its DOWN-NICs to the heavily loaded channel(s) in its interference domain
- This change is NOT conveyed to neighbouring nodes
- Hidden usage of heavily loaded channels
- Affects upstream channels which carry traffic from downstream child nodes



Parasite Attacks



- NEPA (Network Endo-Parasite Attack)
 - Multiple links are switched to different channels
 - Create interference with multiple channels
 - Affects a larger region of the network
 - Usually hard to detect (hidden hence *endo*)
 - Node may launch attack while still using other link(s) for regular forwarding

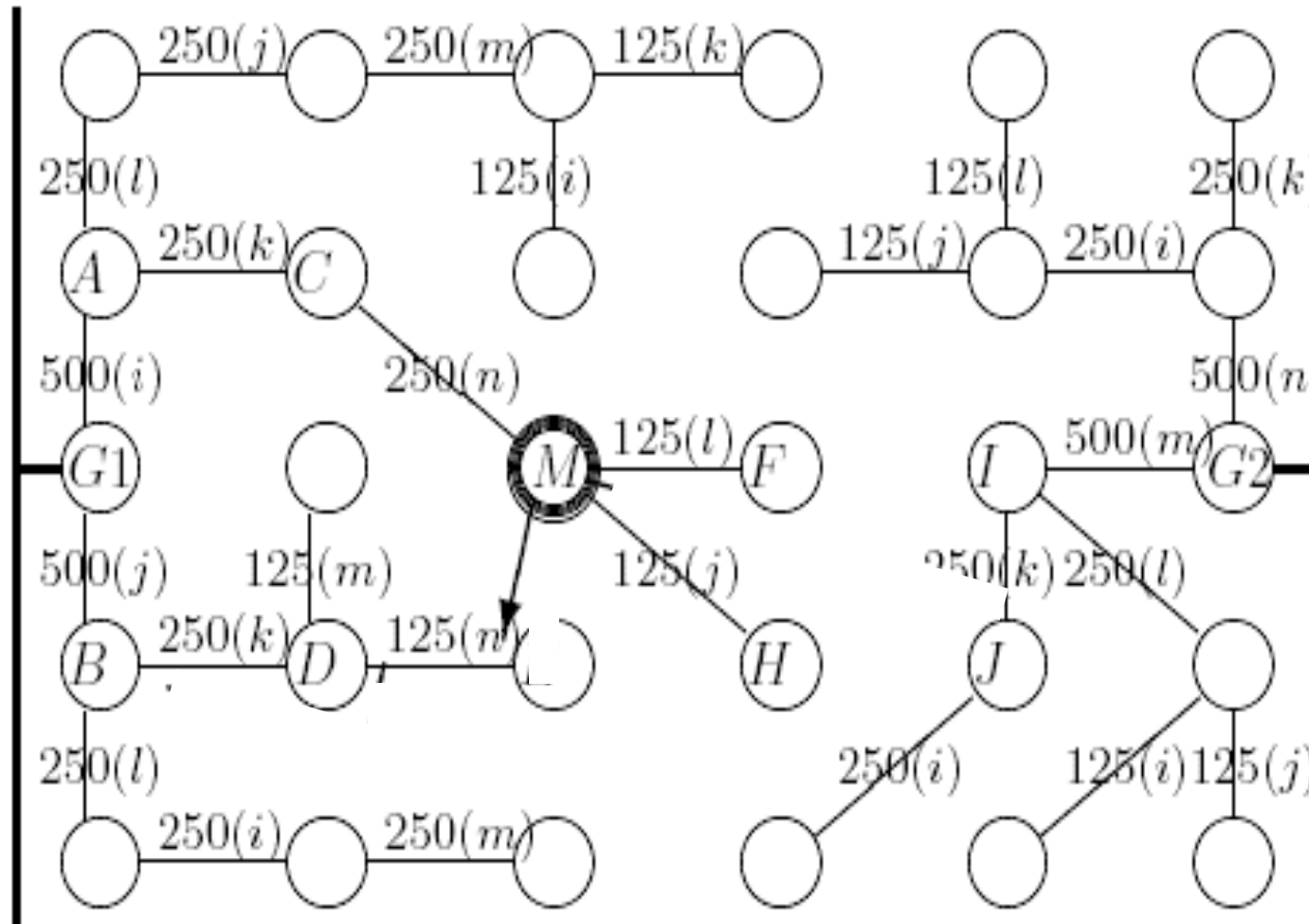


Parasite Attacks

- CEPA (Channel Ecto-Parasite Attack)
 - Multiple links switched to one highly loaded channel
 - Creates significant interference on the one channel
 - Damage restricted to nodes using that channel
 - Detection is easier due to severity (hence *ecto*)
 - Purely malicious behaviour



Example Parasite Attacks





Example Parasite Attacks

- M is misbehaving node
- Channel k and n are heavily loaded (500k and 375k)
- NEPA
 - Switch MF to k and MH to n
 - AC, BD, DE and CM will be affected. Note that AC is in M's routing path
- CEPA
 - Switch both MF and MH to k
 - Only AC and BD are affected but damage is greater

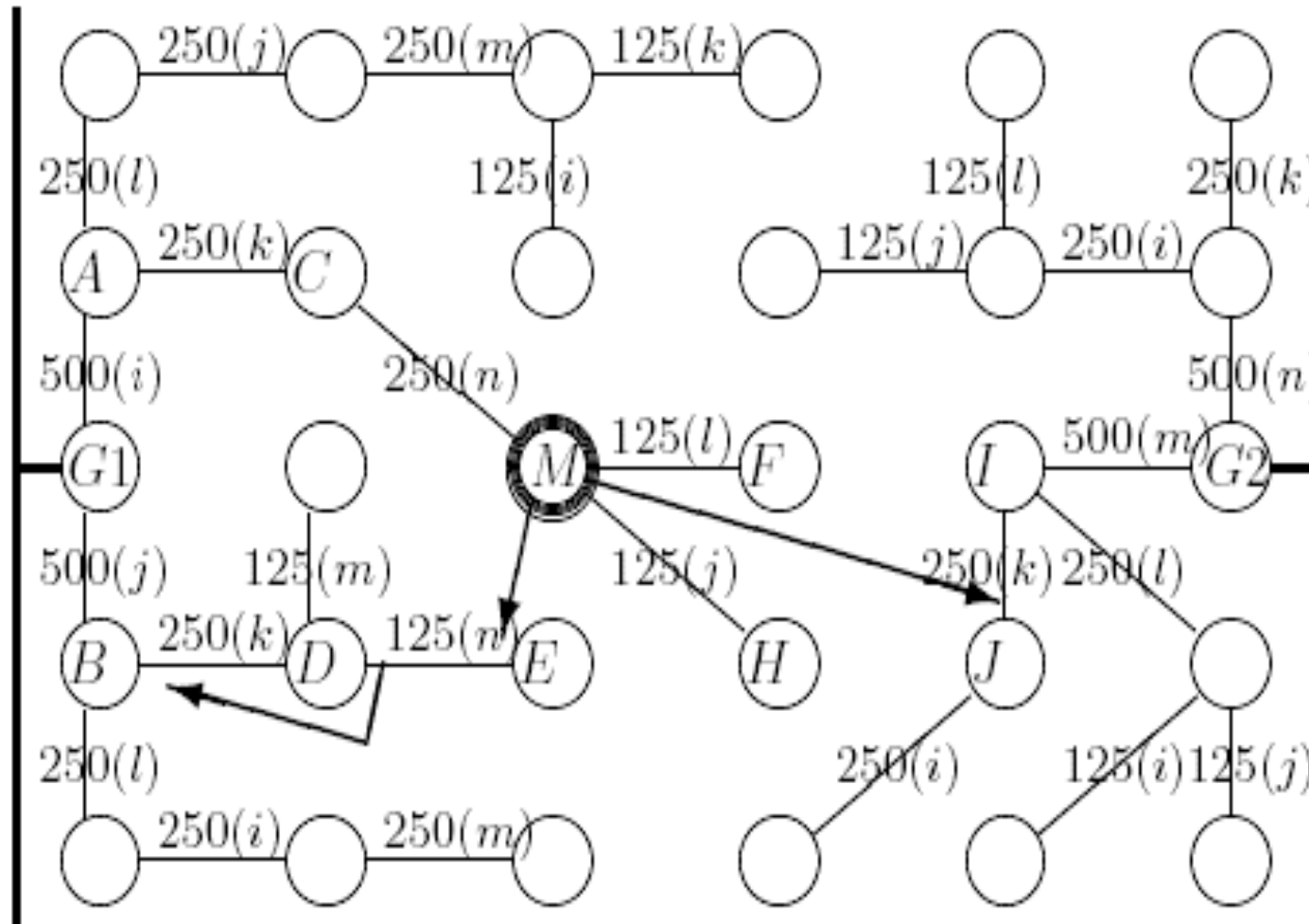


Low-cost Ripple Effect Attacks (LORA)

- Objective - force network into quasi-stable state
- Perpetrator does not actually change the channel assignments
- False channel assignment information is propagated into the network (illusion of heavy load)
- Causes other nodes to change their channel assignments
 - Could possibly create a ripple effect in the network
 - All channel assignment schemes prevent ripples downstream
 - LORA can create ripples upstream (towards more heavily loaded channels)
- Attacks can be easily tuned to create desired effect



Example of LORA





Example Parasite Attacks

- M is misbehaving node
- M informs its neighbours that link MF is switched to k and MH is switched to n
- Link IJ finds j to be more suitable so it switches its assignment
- Link DE is also switched to j
 - As a consequence BD is switched to k
- Even nodes C and A are affected



Simulations



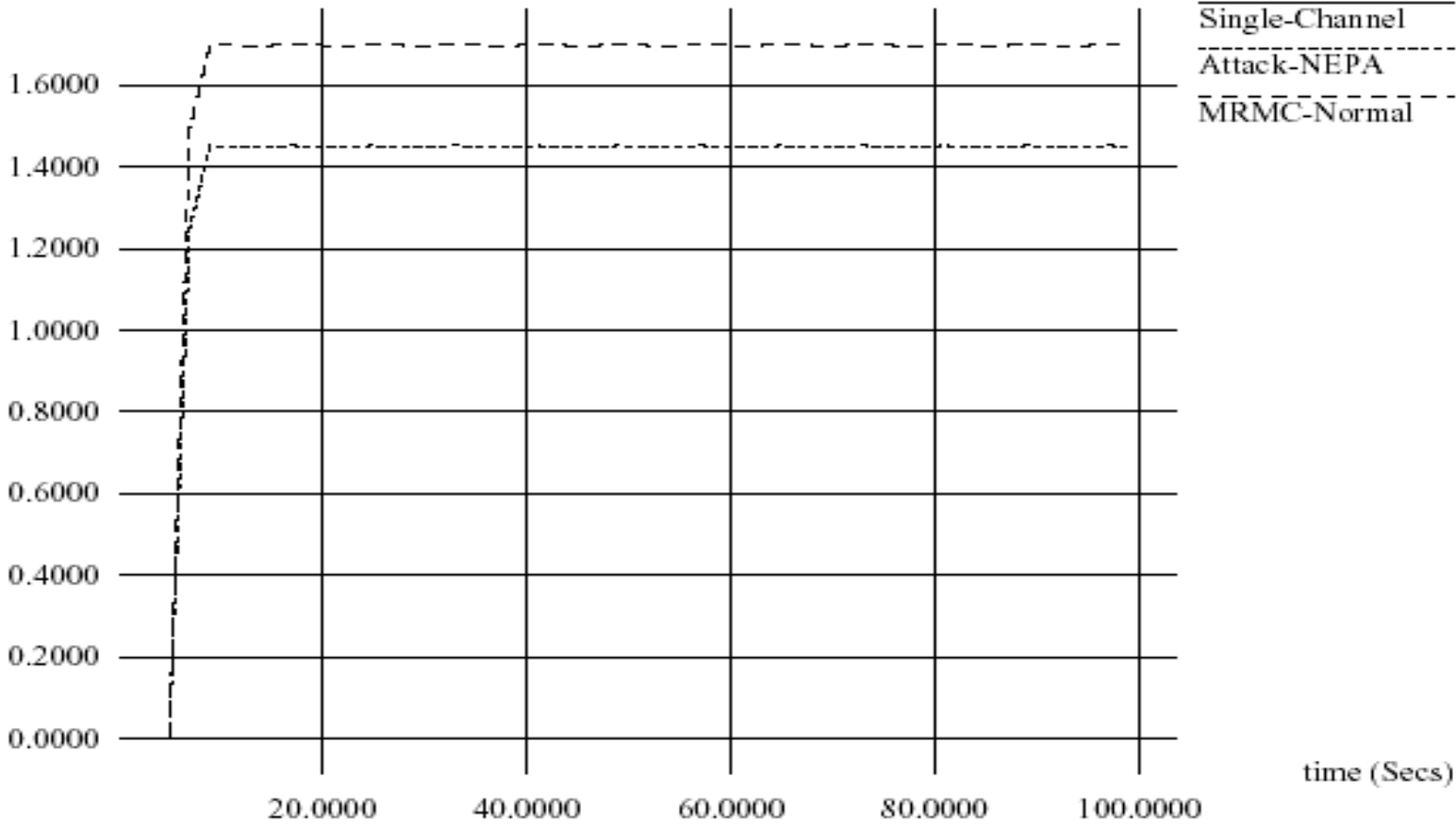
- Ns-2 based simulations
- Simulation Parameters
 - Grid topology of 25 mesh nodes
 - Each node equipped with 2 NICs
 - Several runs with different traffic characteristics and different choice of misbehaving nodes
 - A node 3 hop away from the gateway was a good choice for launching the attacks



Results NEPA

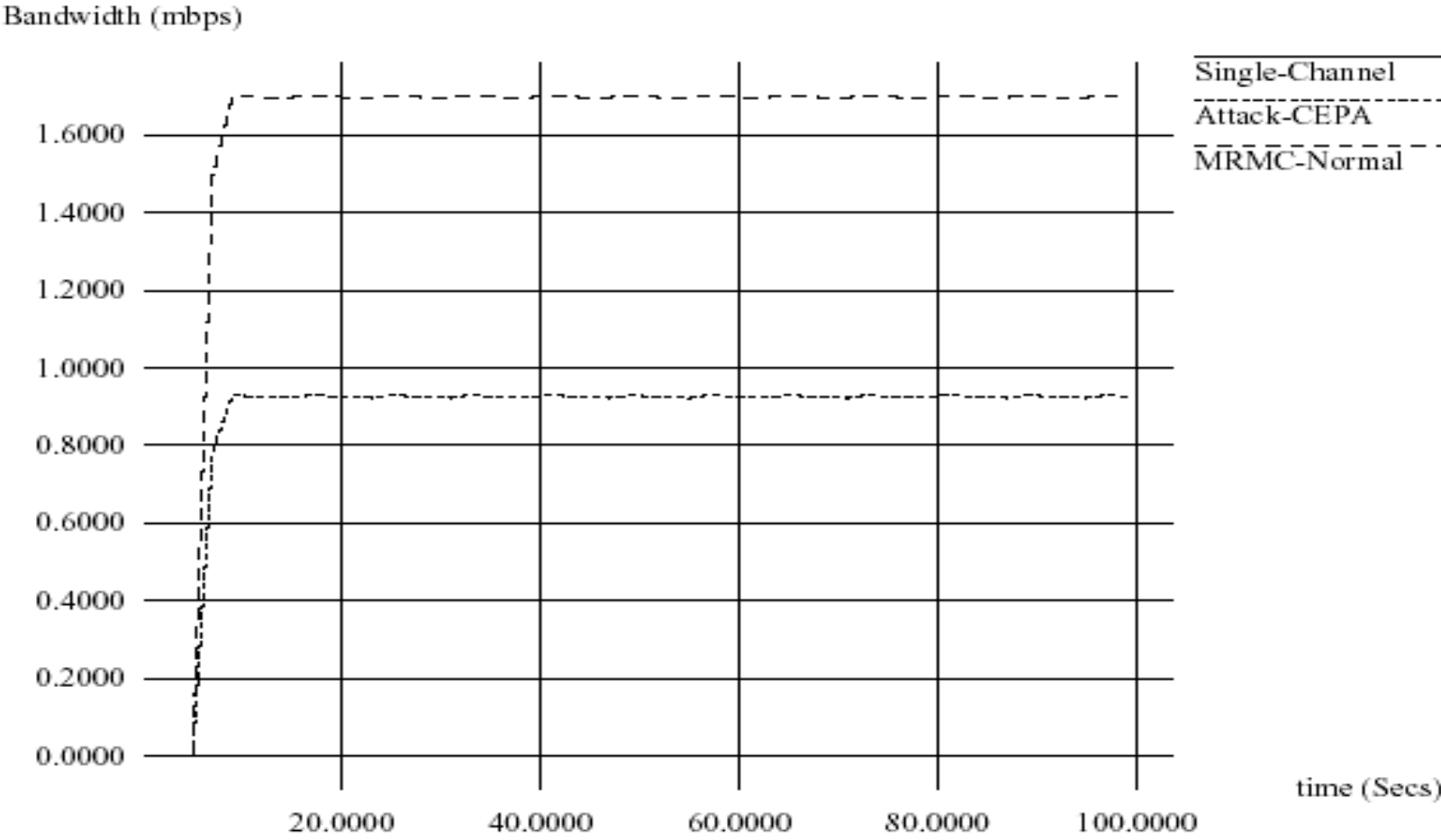


Bandwidth (mbps)



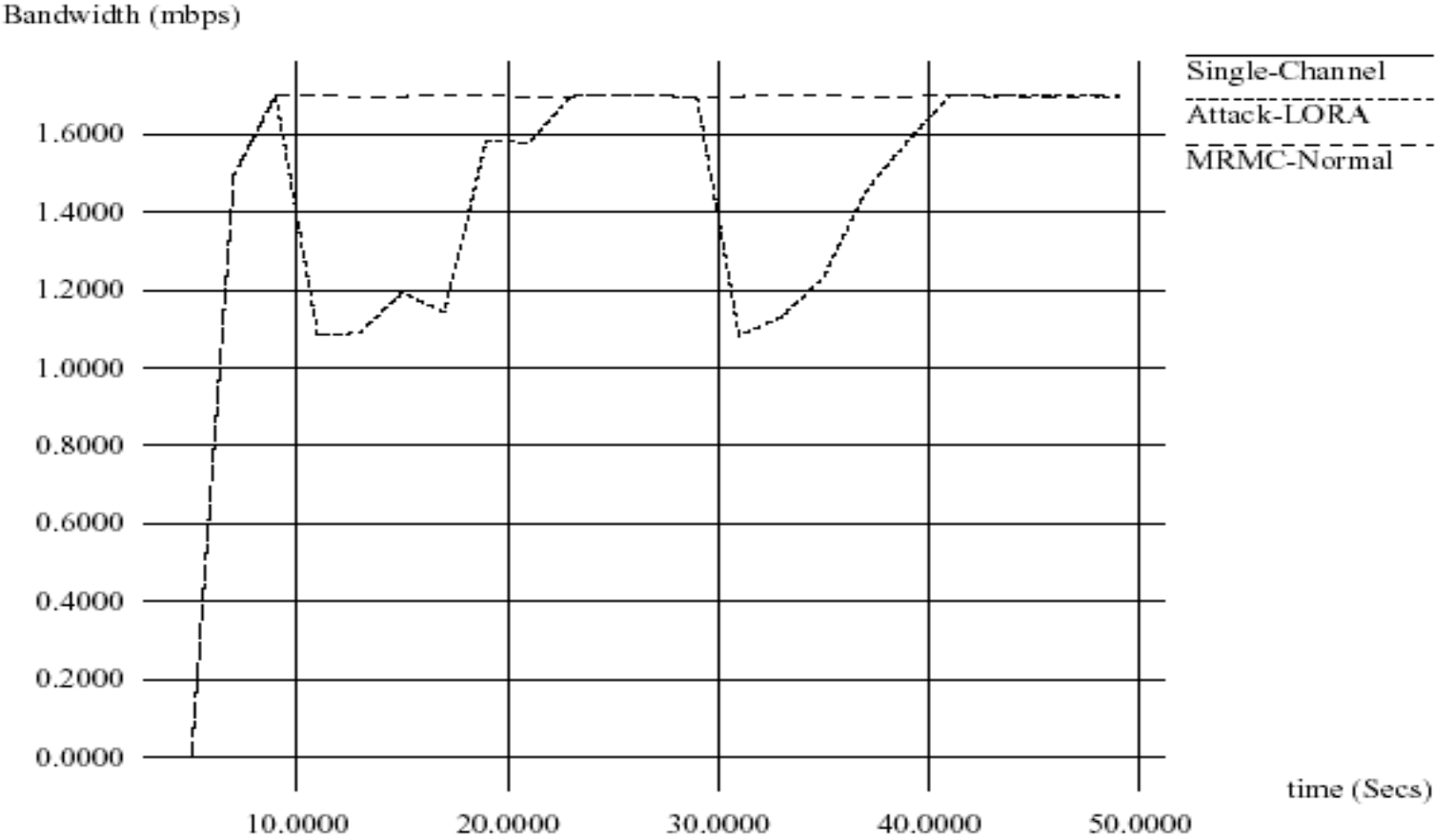


Results CEPA





Results LORA





Prevention



- Verification of channel assignment is essential
- *Verifier* nodes should scan the spectrum to determine channel usage
- Some sort of cooperative schemes
 - Voting
 - Threshold cryptography
- Security *inherent* in routing/channel assignment protocols

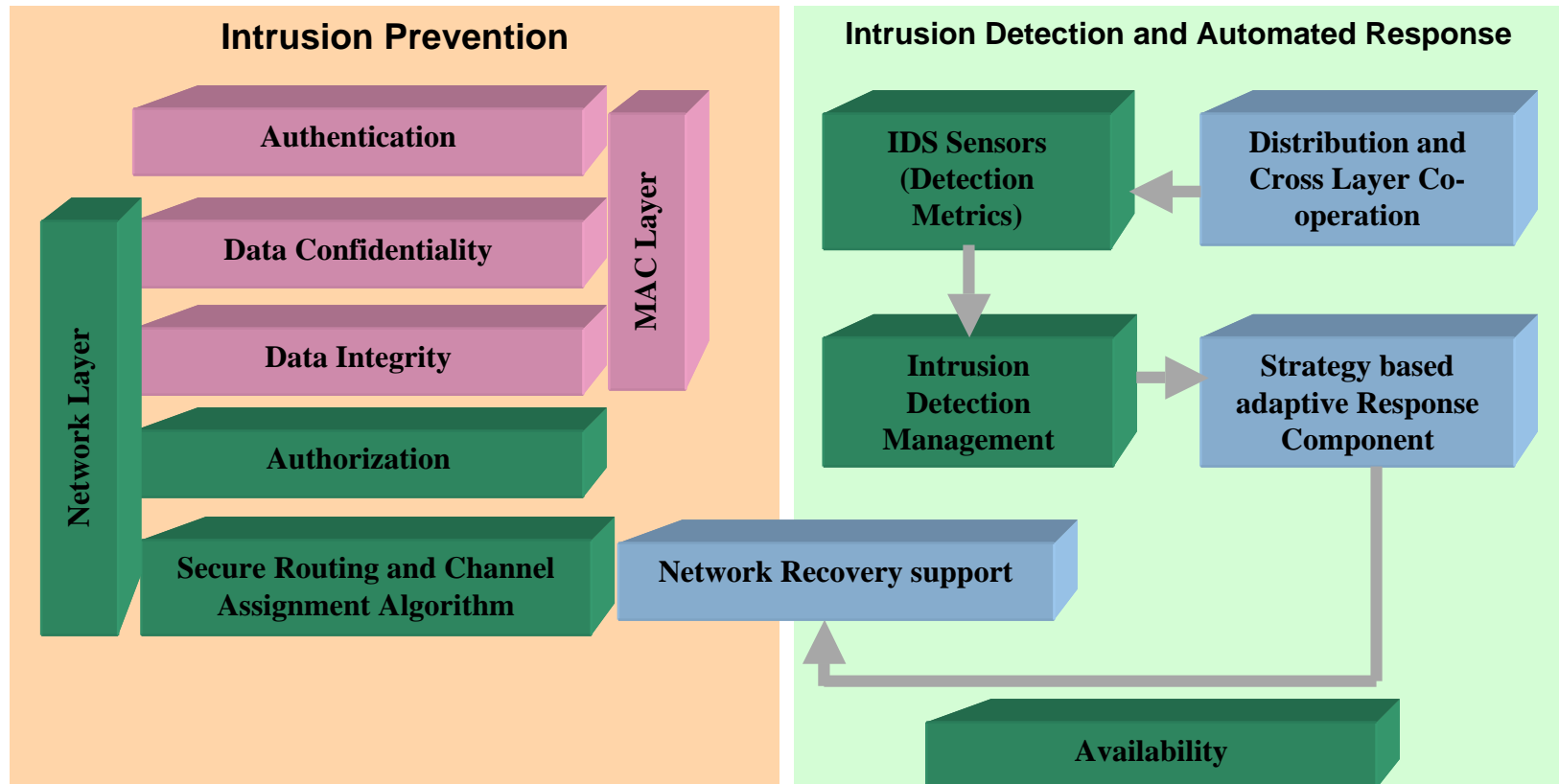


Current work – Secure Routing and Channel Assignment Algorithm

- Zone based secure routing and channel assignment algorithm with inherent security rather than an appurtenance service
- Network decomposition algorithms modified to incorporate the constraints of number of interfaces per node, number of available orthogonal channels and the number of interference domain neighbours of the nodes.
- Minimizing the interference for performance optimization and the robustness against node failures are key design goals in conjunction with security provisioning in our work.
- The controller node within each zone and the border nodes with neighbouring zones implement various levels of checks



Security in Wireless Mesh Networks





Future Work - Intrusion Detection with Automated Response

- Towards Self healing self administered wireless mesh networks
- Use of multiple intrusion detection techniques to increase the accuracy and decrease the false positives and false negatives
 - cross-feature analysis from data mining
 - non-zero sum non-cooperative two player games (game theory)
 - immune systems based approaches
 - further improvement in accuracy using multi-variable high degree polynomials
- Distributed Intrusion Detection
 - Zones of routing and channel assignment to be used for distribution



Intrusion Detection with Automated Response

- High accuracy of detection can lead to active automated response. We intend to propose adaptive response based on severity of intrusion level
 - If the intrusion has severe adverse effects, misbehaving node(s) will be dissociated
 - If the attack is minor then a simple alert for neighbouring nodes may suffice
 - Further responses will lie between two extremes based on severity level of attack
 - The effort is directed towards self administered WMN.
- Each response will be coupled with the appropriate recovery mechanism to ensure self healing network.
- This requires means to quantify attacks



Publications

- To appear
 - Book Chapter: Anjum Naveed, Salil Kanhere and Sanjay Jha, “Attacks and Security Mechanisms”, in *Security in Wireless Mesh Networks*, Auerbach Publication, CRC Press
 - Anjum Naveed and Salil Kanhere, “Security Vulnerabilities in Channel Assignment of Multi-Radio Multi-Channel Wireless Mesh Networks”, to appear in *IEEE Globecom*, November 2006
- Under review
 - Junaid Hussain, Anjum Naveed and Salil Kanhere, “Security Framework for Wireless Mesh Networks”, in review with *IEEE LCN 2006*



Questions ?