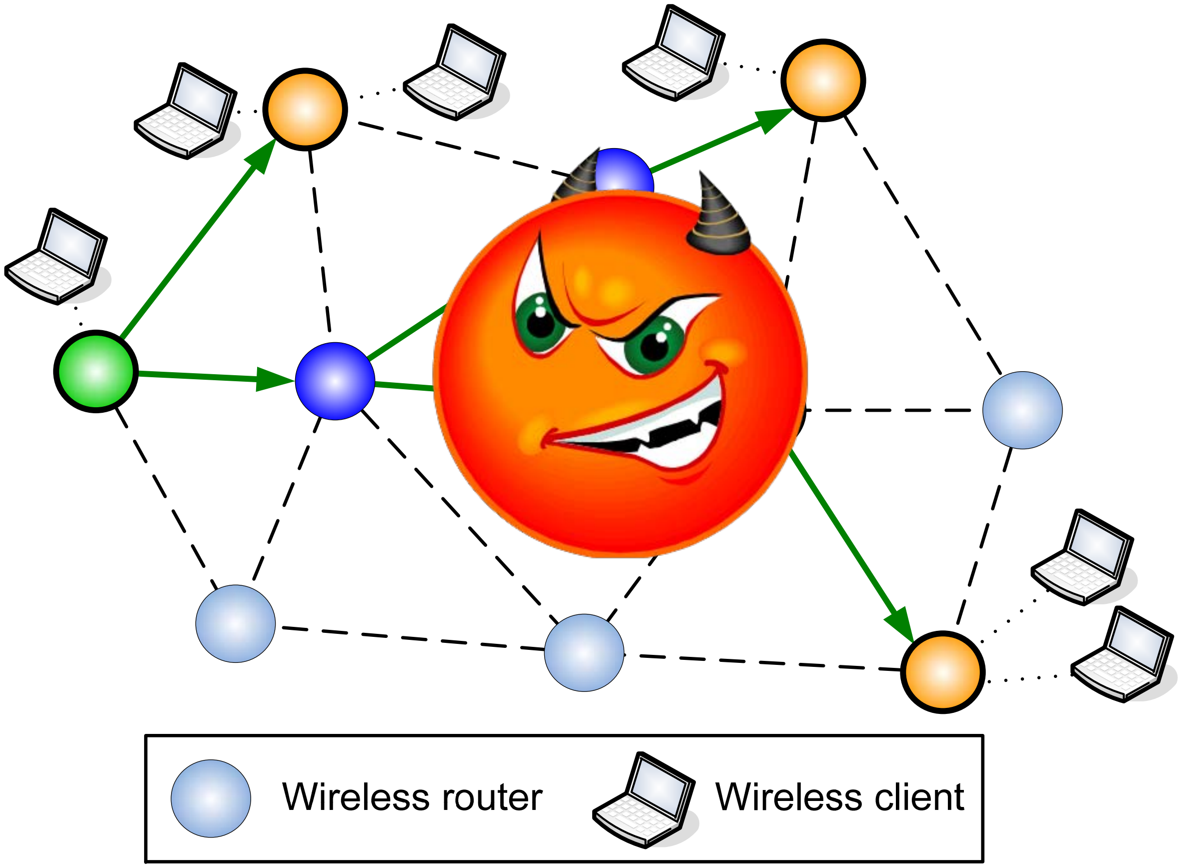
Secure Group Communication in Wireless Mesh Networks

Jing Dong, Kurt Ackermann, Cristina Nita-Rotaru

Department of Computer Science and CERIAS

Purdue University

Group Communication in Wireless Mesh Networks



Multimedia Conferencing

Video/audio broadcasting

Online gaming

Distance learning

Confidential Group Communication

- Ensure data confidentiality against outsiders

- Application
  - Paid video broadcasting
  - Sensitive multimedia conferencing

Related Work

- On wired networks
  - LKH [Wong ’00] and its variants [Li ’01, Zhang ’03, Zhang ’04]
  - Protocols for overlay networks [Yiu ’04, Abad ’05, Zhu ’05]
- Wireless networks
  - GKMPAN [Zhu ’04]
  - CRTDH [Balachandran ’05]
  - Secret key management [Chan ’03, Du ’06]

None of them address the unique features of WMNs

Our Approach: SeGrOM

- Decentralize membership management
  - To avoid communication and computation bottleneck
- Localize communication
  - To save limited bandwidth
  - To reduce communication latency
- Exploit wireless broadcast
  - To improve performance and save bandwidth
- Use symmetric cryptography
  - To reduce computation overhead

System and Security Model

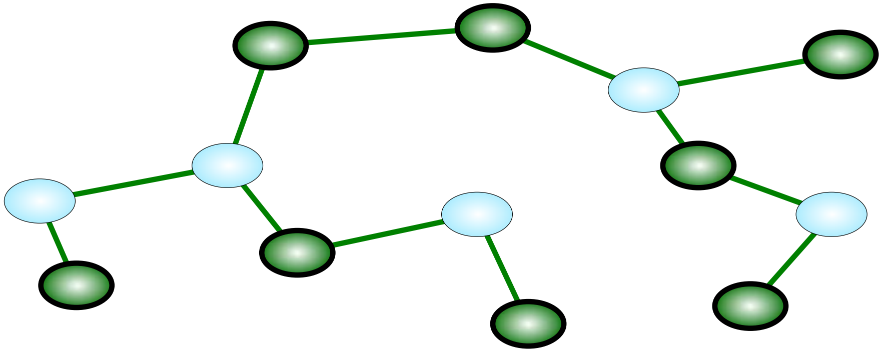
- Tree-based multicast protocol
- Public key infrastructure
  - Group membership authentication
- supports dynamic group membership
- Security Goal
  - Confidentiality against outsider attacks
    - Wireless routers,
    - Non-member clients, or
    - Other devices
  - Forward and backward secrecy
    - Protect future data from members who have left
    - Protect past data from newly joined members

SeGrOM Architecture

Two-level architecture

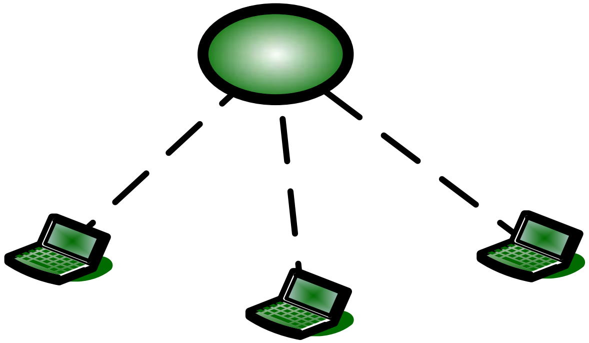
Global Data Delivery

Inter-router communication



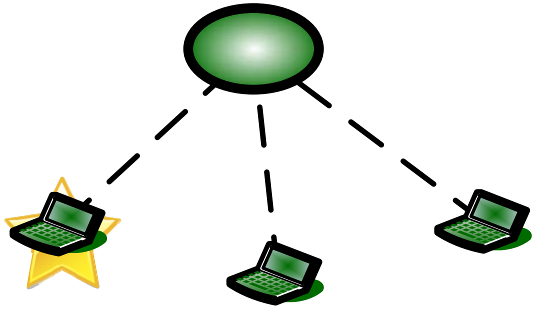
Local Data Delivery

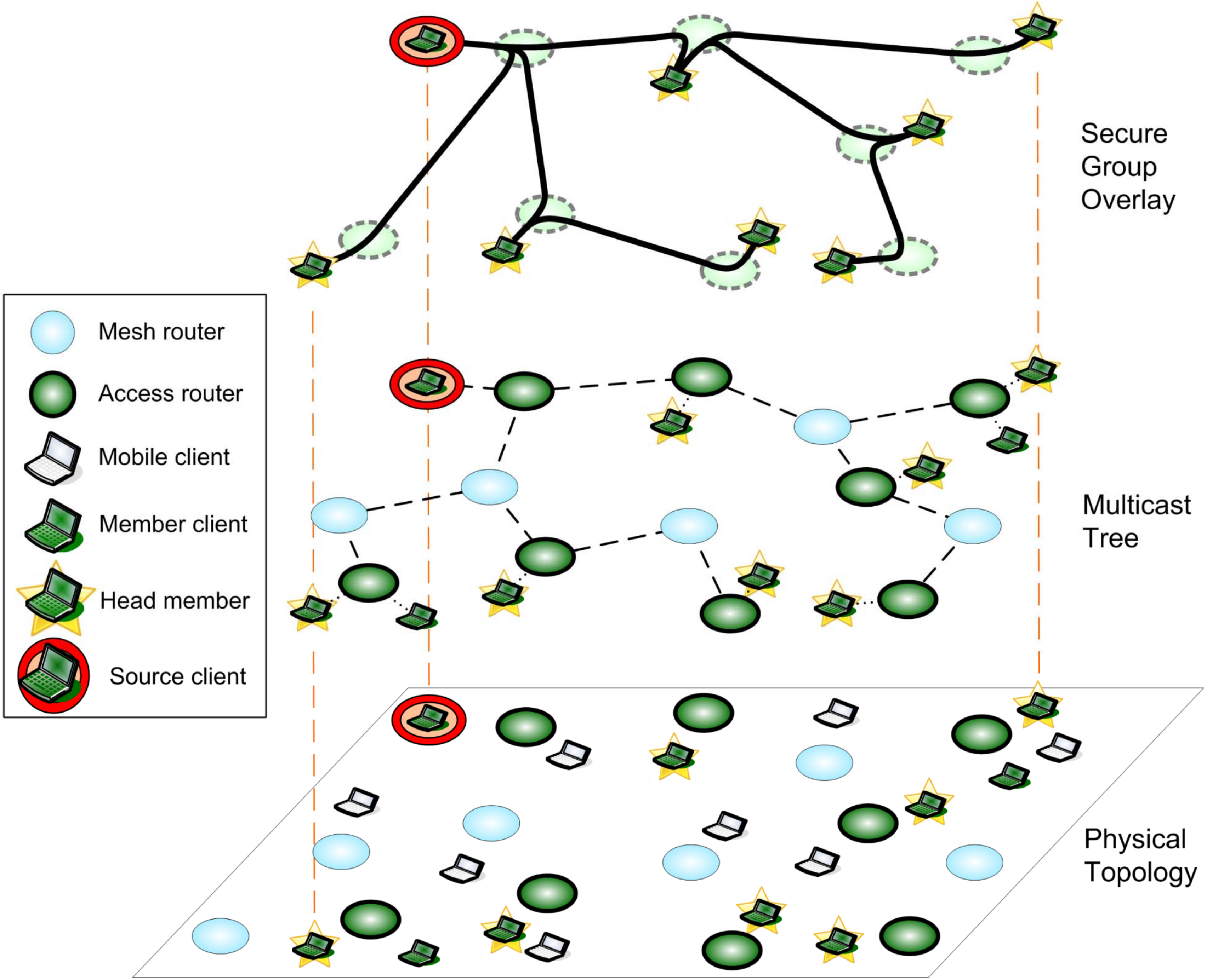
Intra-router communication



SeGrOM Head Member and Group Overlay

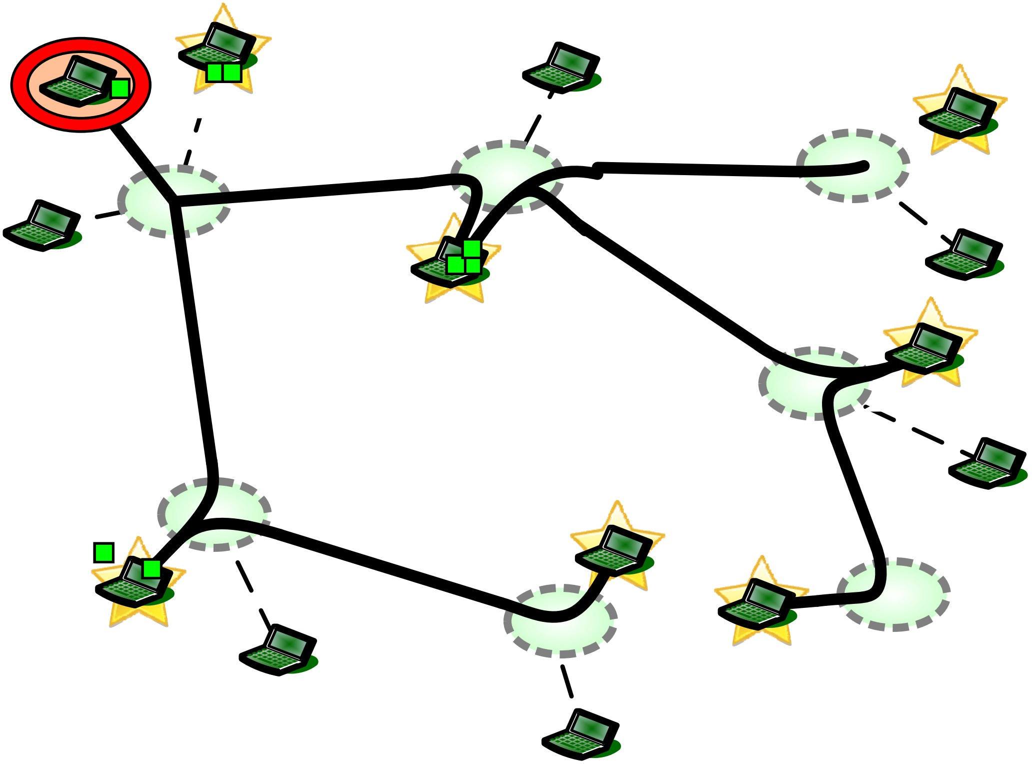
- Head member
  - One per access router
  - Elected among local member clients
  - Participate in global data delivery
  - Coordinate local data delivery
- Secure group overlay
  - Secret key between neighboring head members




Mesh router
Access router
Mobile client
Member client
Head member
Source client
Secure Group Overlay
Multicast Tree
Physical Topology

SeGrOM Data Flow

- Source forwards data to the local head member
- Local head member forwards data to
  - other local member clients
  - downstream head members
- Downstream head members forwards data to
  - their local member clients
  - downstream head members



Secure Local Data Delivery

- Relies on a common local data key
- Data delivery
  - Encrypt data using the local data key
  - Send it to the access router
  - Access router broadcast to other client nodes
- To preserve forward and backward secrecy
  - Join or leave of local group member refreshes the local data key

Global Data Delivery on Secure Group Overlay

- SeGrOM-Group
  - Use a common group key
  - The group key is refreshed to provide forward/backward secrecy
- SeGrOM-Link
  - Use the symmetric keys on the secure group overlay directly
  - Encrypt and deliver data for each of the downstream head members separately
- SeGrOM-Hop
  - Maintain a hop key on each hop
  - Exploit broadcast for group data delivery
  - Optimized communication and computation cost compared to SeGrOM-Link

Global Data Delivery on Secure Group Overlay

- SeGrOM-Group
- SeGrOM-Link
- SeGrOM-Hop

SeGrOM-Group

- All head members share a common group key
- Data is encrypted using the common group key for delivery across the backbone routers
- Pro:
  - Simplicity
  - Broadcast advantage and computation efficiency
- Cons:
  - Group key needs to refreshed for every head member change – global communication

SeGrOM-Link

- Use symmetric keys on the secure group overlay for data delivery
- Pros:
  - Avoids global communication
- Cons:
  - Expensive in computation
  - Does not exploit broadcast advantage

SeGrOM-Hop

- Maintain a hop key at each hop
- Data is encrypted using the hop key hop by hop
- Pros:
  - Localized communication
  - Exploit broadcast for group data delivery
  - Optimized communication and computation cost compared to SeGrOM-Link
- Cons:
  - The need to maintain hop keys – but it involves only local communication

Handling Group Dynamics

- Join/leave of non-head members
  - Only involves communication with the local head member
  - Refreshes local data key
- Join/leave of head members
  - Involves communication with neighboring head members
  - Updates the group overlay

Localized communication → Application responsiveness

Member Revocation: SeGrOM-Revoke

- CRL is inefficient in WMNs
- Exploit client movement locality
- Each client selects a set of ***home routers***
  - Maintains the revocation status
- Revocation
  - CA sends a revocation notice to the members on the home routers
- Check revocation status
  - Sends a query to any member on any of the home routers – **Localized communication**
  - If no member exists, send query to the CA

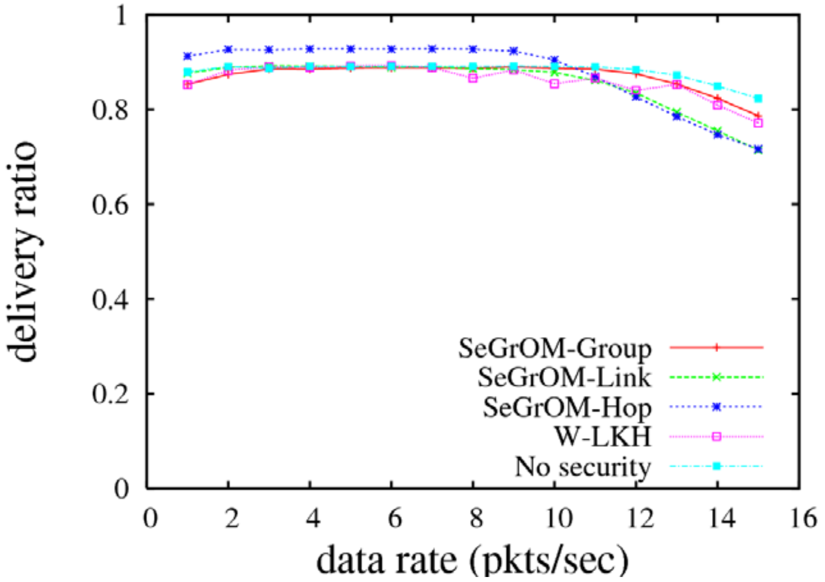
Experimental Evaluation

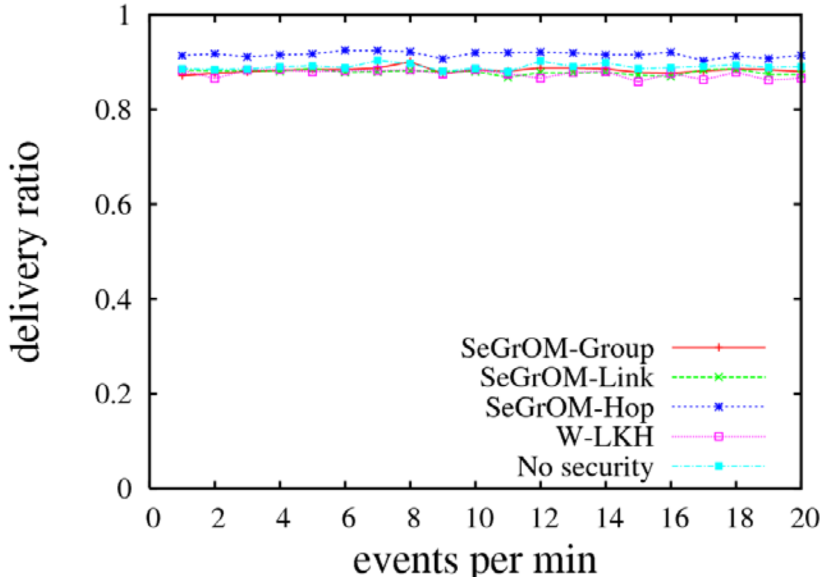
- ns2 with MAODV
- 802.11 radio, bandwidth 2Mbps, range 250m, 1500m x1500m area
- Network structure
  - 100 wireless routers
  - 100 member clients
  - Member clients join with the nearest router
- One client as source
- Poisson group dynamics
  - join rate = leave rate for stabilized group size

Protocols Compared

- W-LKH
  - Centralized protocol
- SeGrOM Protocols
  - SeGrOM-Group
  - SeGrOM-Link
  - SeGrOM-Hop

Application Performance

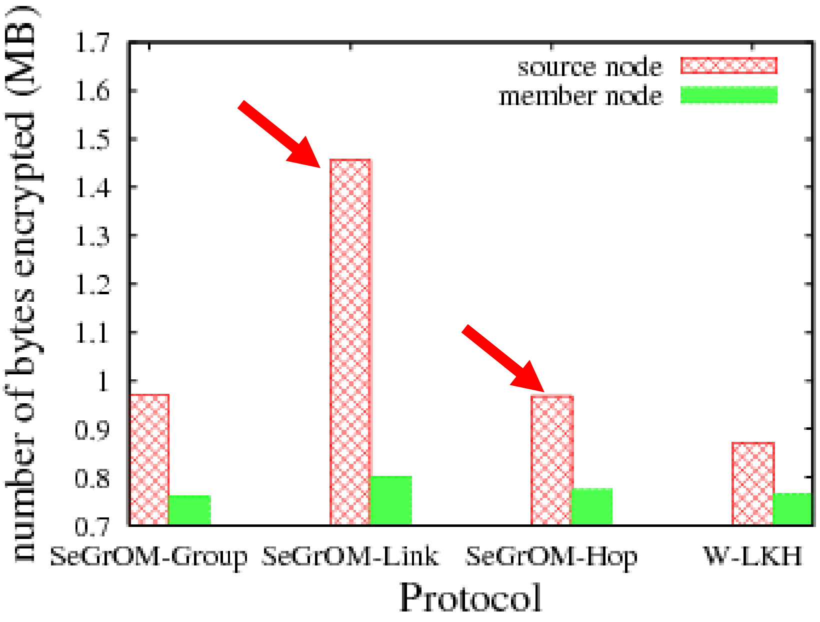

Delivery ratio vs. data rates


Delivery ratio vs. group dynamics

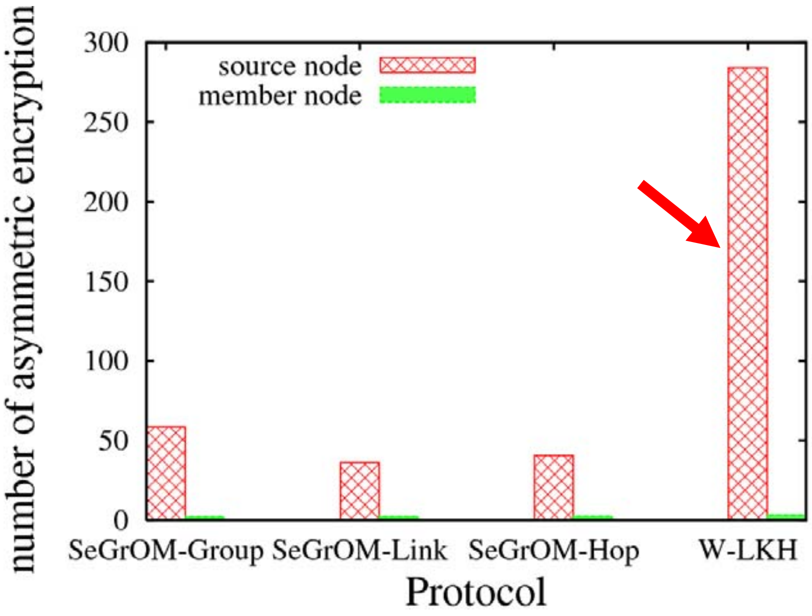
Adding confidentiality does not degrade performance

Computation Overhead

Symmetric encryptions



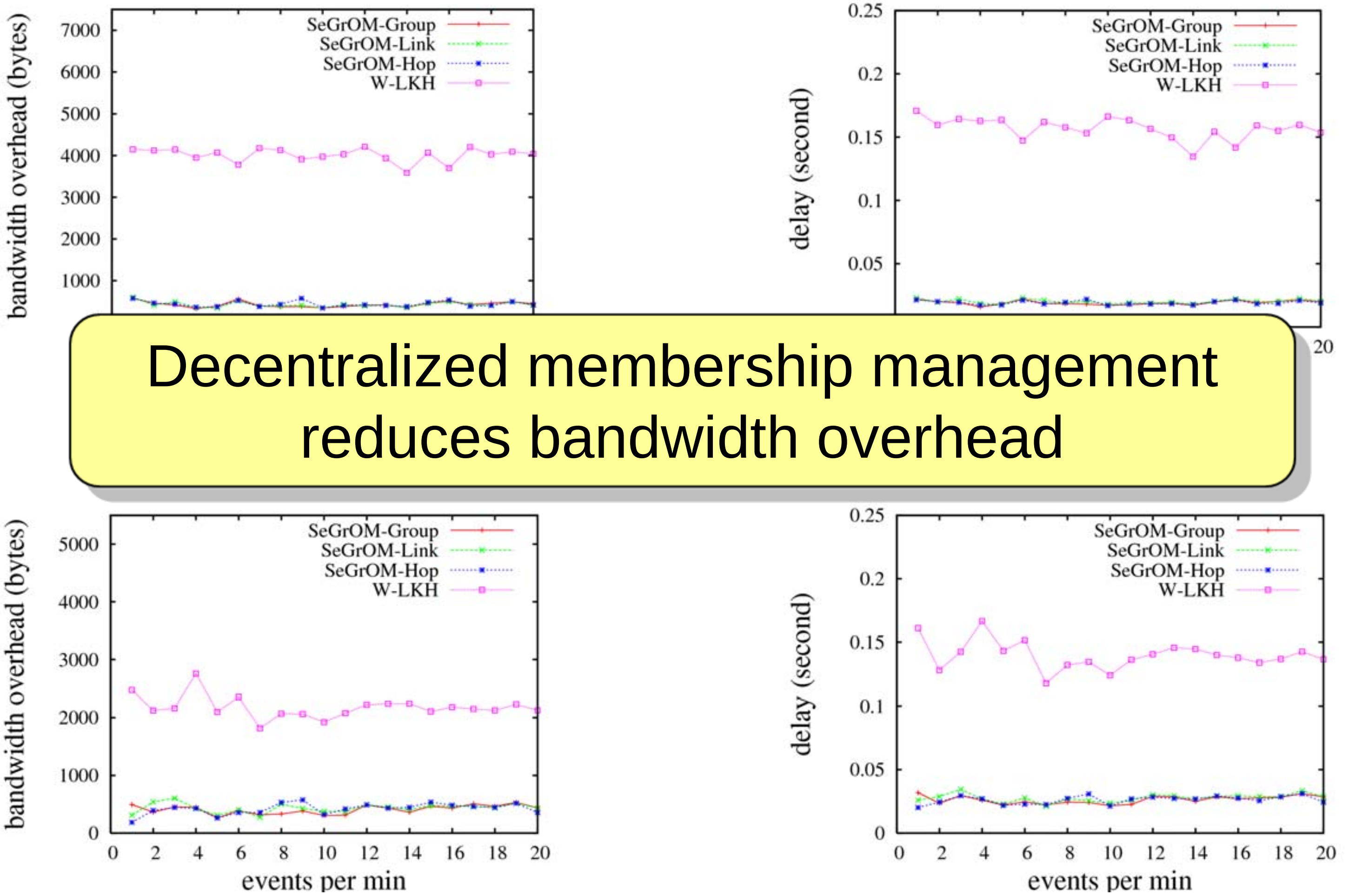
Asymmetric encryptions



Decentralized protocol avoids computation bottleneck

Join and Leave Bandwidth Overhead and Latency

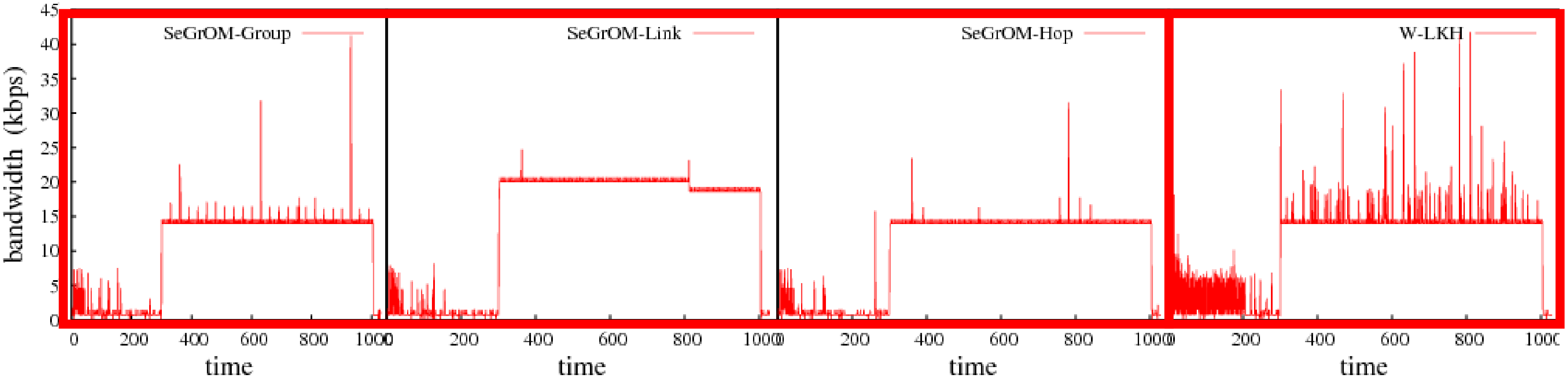
Join bandwidth overhead and latency



Decentralized membership management reduces bandwidth overhead

Peak Bandwidth Comparisons

SeGrOM-Group SeGrOM-Link SeGrOM-Hop W-LKH



Decentralized schemes reduces bandwidth variability

Conclusion

- We proposed a framework for achieving data confidentiality for group communications in WMNs
- We proposed several variants that tradeoff complexity and performance
- We show that
  - Adding confidentiality does not degrade performance
  - Decentralized protocols are more efficient

Thank You!

Questions?

Contact: dongj@cs.purdue.edu