CERIAS

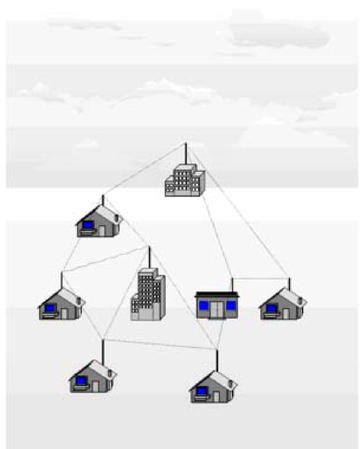
the center for education and research in information assurance and security

Enabling Confidentiality for Group Communication on Wireless Mesh Networks

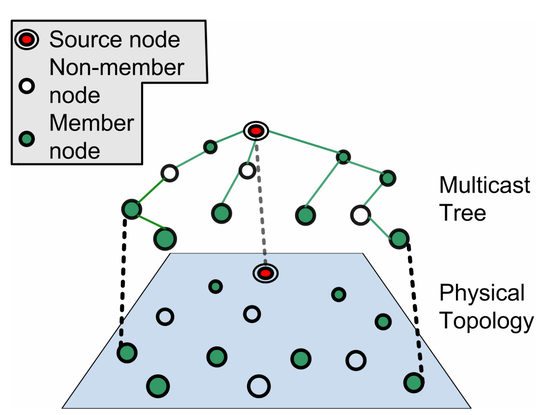
Jing Dong and Cristina Nita-Rotaru, Purdue University

Wireless mesh networks (WMNs) are a promising technology for enabling low cost community wireless access.
Group communication is an important class of application: multimedia conferencing, media broadcast, etc

Our target: Enabling data confidentiality for group communications on WMNs.



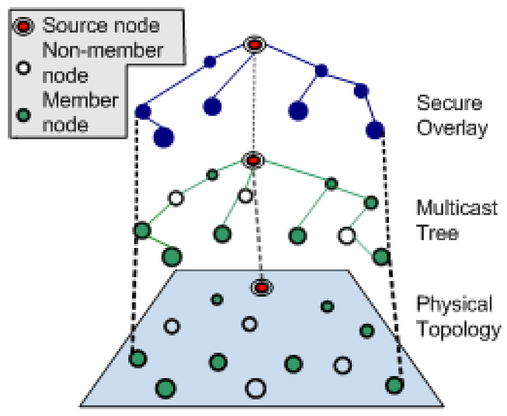
A Wireless Mesh Network

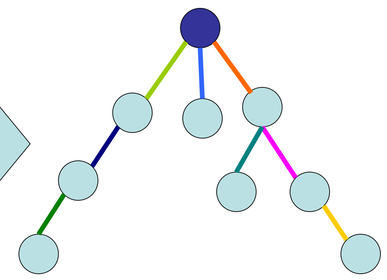


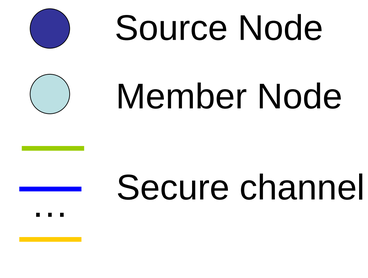
A typical multicast structure

Secure Overlay Based Approach

Build a secure overlay structure
Every node builds a secure channel with all neighboring group members

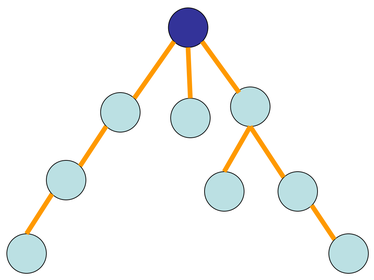






Group key based

1. Maintain a common group key on the secure overlay
2. Data packet is distributed with the group key

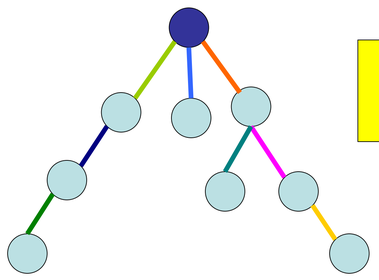


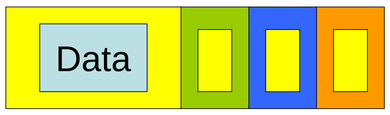
Packet structure

Data dissemination structure

Link key based

1. The data packet is encrypted with a data encryption key.
2. The data encryption key is distributed with the link key hop by hop



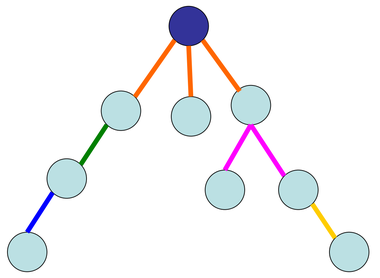


Packet structure

Data dissemination structure

Hop key based

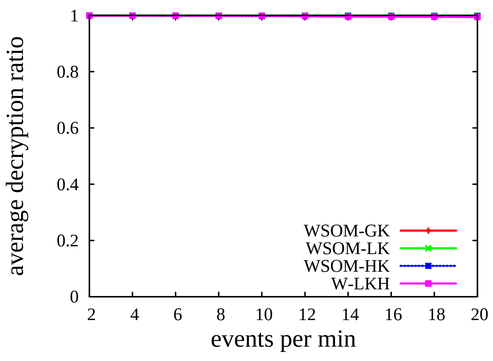
1. The data packet is encrypted with a data encryption key.
2. The data encryption key is distributed with the hop key.

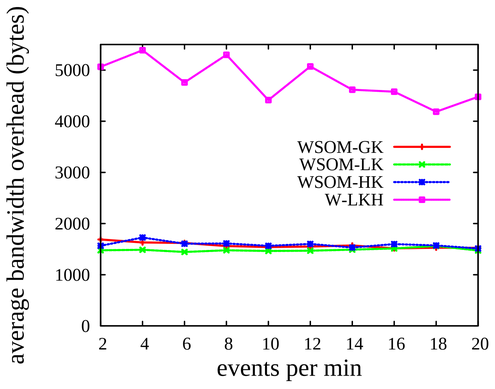


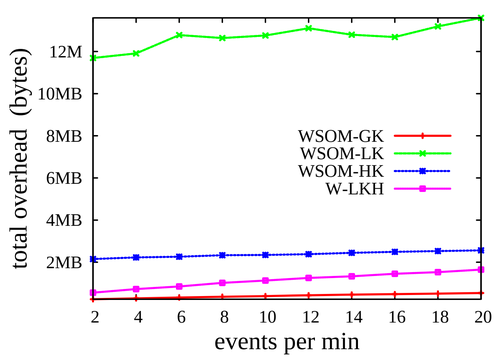
Packet structure

Data dissemination structure

Experimental Results







Conclusion

1. Adding confidentiality does not affect application performance
2. Secure overlay based protocols have lower overhead than protocol adapted from the wired environment
3. The link key based protocol incurs higher overhead than the group key based and hop key protocols

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center