

Group Key Establishment in Ad Hoc Networks Using Mobility Prediction

Kristin Burke

Overview

- Ad Hoc Networks
- Group Key Establishment
- Problems: Group Key in Ad Hoc
- Mobility Prediction
- Thesis Question
- References

Ad Hoc Networks

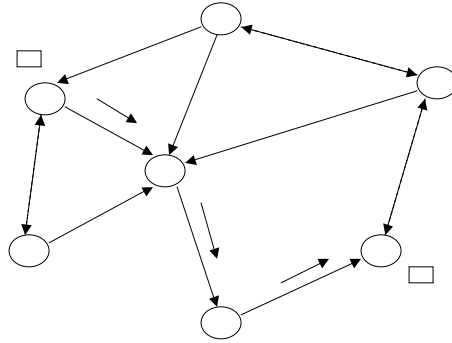
- Dynamic, peer-to-peer networks with no pre-existing infrastructure
 - No central entities, fixed routers, name servers, etc.
- Parties involved may not have a common history
- Often temporary, can be mobile

Ad Hoc Networks

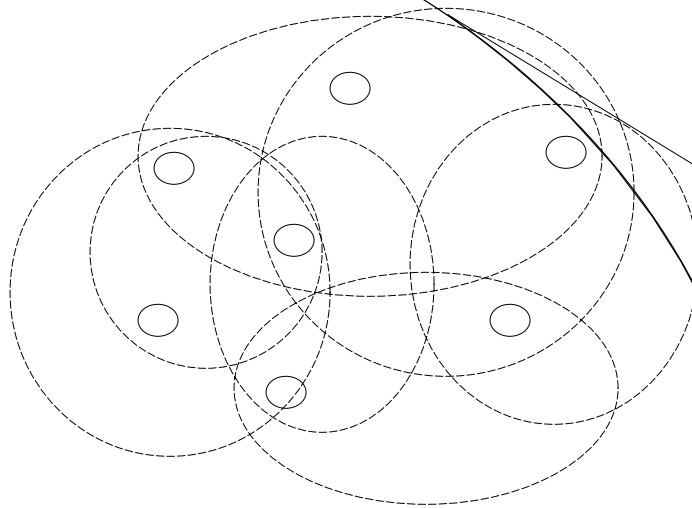
- Devices are small and portable
 - Don't have much memory or computational power
- Nodes can lose connection easily
 - Move out of range
 - Run out of batteries
 - Be compromised

Network

Packet from ○ to ○



Ad hoc network



Group Key Establishment

- Groups of nodes in ad hoc networks want to share a key
 - Have not previously agreed on any common secret
 - Eavesdropper can listen to their communications
- Most group key protocols were not made with ad hoc networks in mind

Group Key Protocols (for Ad Hoc)

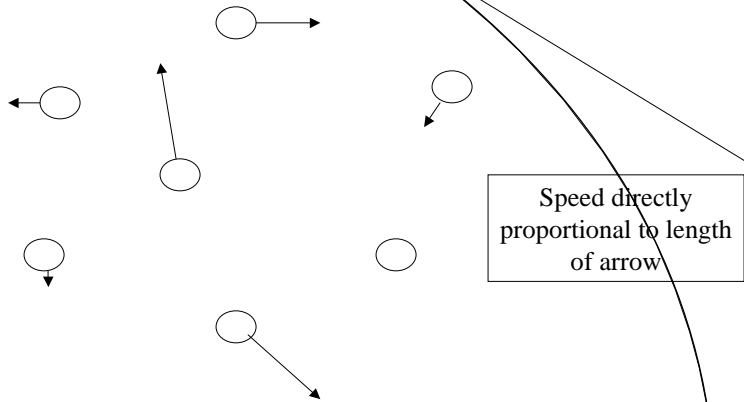
- CLIQUES
- GDH.2
- Hypercube
- Octopus
- Tree-based BD
- YTCC

Problems: Group Key in Ad Hoc

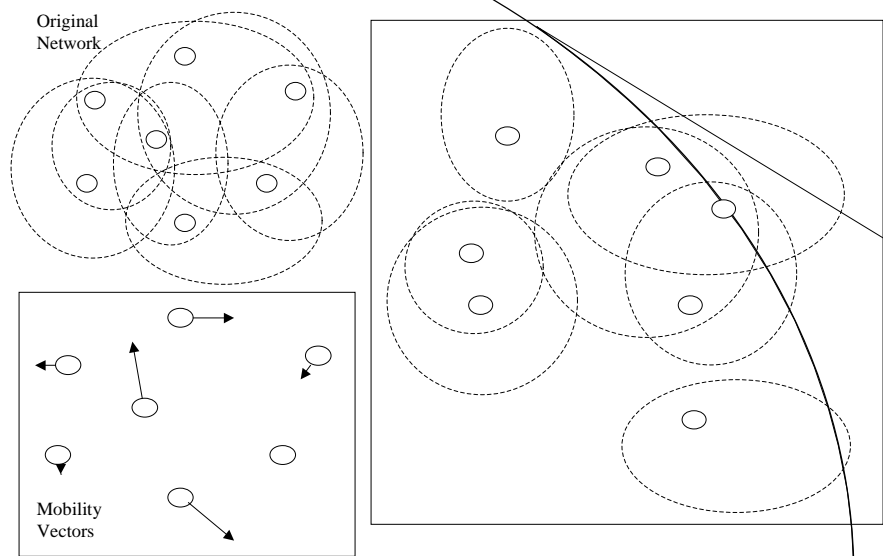
- Global Broadcast may be out of the question
 - Many group key protocols use broadcast
- Changing topology
 - Exchanges must be fast
- No infrastructure
 - No trusted third parties to calculate key & distribute

Mobility Vectors

Network with mobility vectors



Nwk w/ mobility vectors at time t



How MVs help

- Improve efficiency of group re-keying, adding and deleting group members, and group partitions

References

- *Key Establishment in Ad-hoc Networks*, Maarit Hietalahti, Tik-110.501 Seminar on Network Security