

Secure Tactical, Ad hoc, Networks (STAN)

Michael Burmester
Alec Yasinsac

1

Quote of the Day

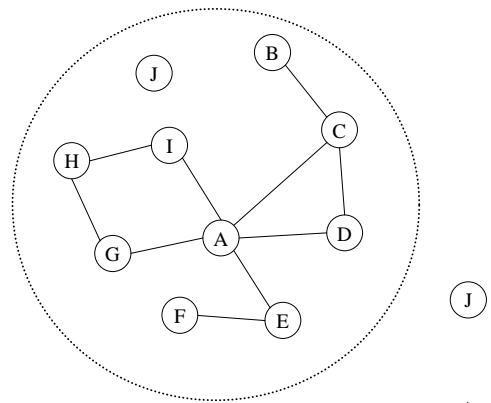
- "Winston, you are drunk!" -
- Lady Astor
- "Yes my dear, but you are ugly,
and in the morning I shall be
sober."
- Winston Churchill

2

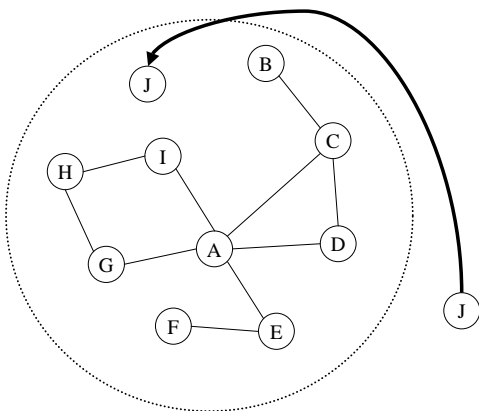
The Essence of:

- Ad hoc
 - Dynamic
 - Unpredictable
 - No controlling authority
- Tactical
 - Action with a purpose
 - Driven by events
 - Governed by a plan
 - Centrally controlled

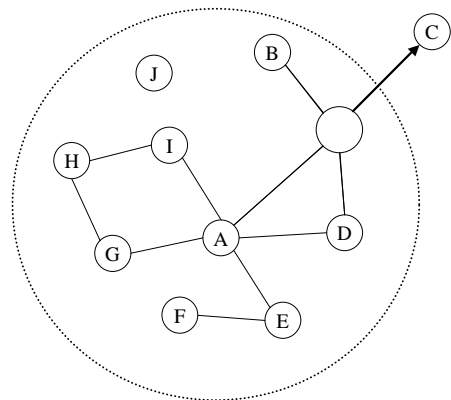
3



4

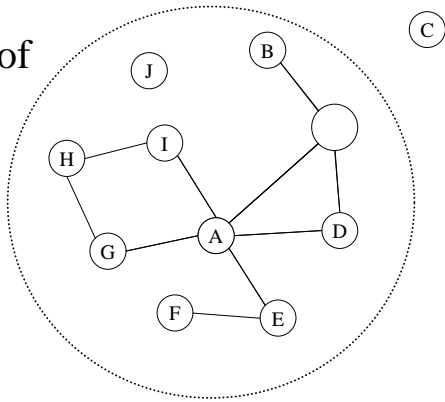


5



6

The Results of Three Events



7

Essentially, in STANs

- Group membership is:
 - Dynamic
 - In General, unpredictable
 - Occasionally, predictable
- Connectivity is the same

8

Group Communication Administration in STANs

- Create a group
- Add a member to a group
- Remove a member from a group
- Delete a group
- Merge two groups
- Split a group in two

9

Communication Issues

- Broadcast paradigm
- Bandwidth is limited
- Distance limited
- Line of sight matters
- Power consumption
- Etc.

10

Security Issues

- Members must be authenticated
 - Only members in the group can talk
 - Only members of the group can listen
- Message integrity must be protected
- Member locations not divulged
- Silent partners

11

Tactical Issues

- Timing is crucial
 - Delays can be disastrous
- Mutual understanding is essential
- Actions & capabilities are dictated by:
 - Tactical plan
 - Adjustments to the plan from above
 - Local adjustments to the plan
 - Reaction to events

12

Keys in Group Communication

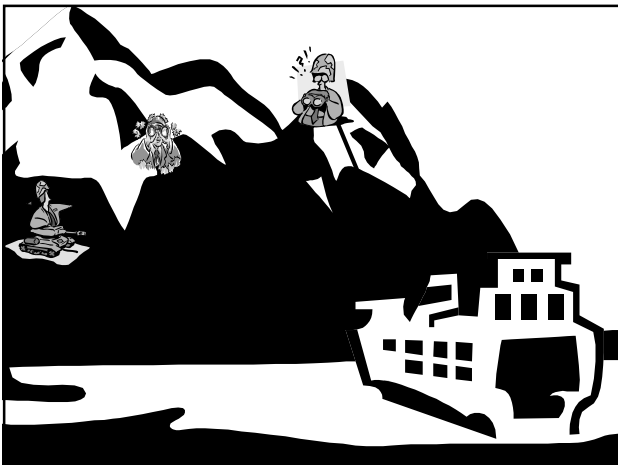
- Generate New Keys
- Distribute New Keys
- Distribute Old Keys
- Change Keys
- Revoke Keys

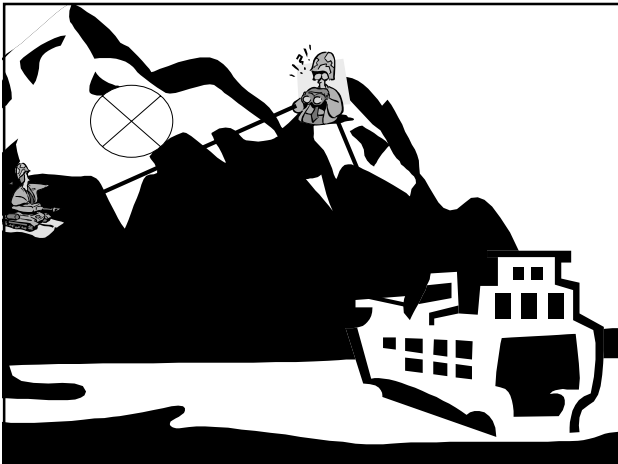
13

Key Operations for Group Communication in STANs

- Create a group
 - Generate New Key
 - Distribute New Key
- Add member
 - Distribute Old Keys
- Remove a member
 - Revoke Key or Change Keys
- Delete a group
 - Revoke Keys
- Merge two groups
 - Change Keys
- Split a group in two
 - Change Keys

14





Cryptography Paradigms

- Shared key
 - Everyone has the same key
- Fully connected
 - Connectivity is logically point to point
 - Each node acts as a translator to the next node
- Conference key
 - Encryption key K
 - Decryption keys k_i for $i = 1..nn$

22

Cryptography Paradigms

- Shared key
 - Everyone has the same key
- Fully connected
 - Connectivity is logically point to point
 - Each node acts as a translator to the next node
- Conference key
 - Encryption key K
 - Decryption keys k_i for $i = 1..nn$

23

More From
Dr. Mike Burmester

24