BatCave: Adding Security to the BATMAN Protocol

Anne G. Bowitz, Espen G. Graarud,
Lawrie Brown, Martin G. Jaatun

September 2011

ITEM, NTNU, Trondheim, Norway
UNSW@ADFA, Canberra, Australia

Research Problem

- need to implement a secure ad hoc network that might be used in emergency services, disaster assistance, and military applications
- that can be established quickly
- with controls to limit access to network

Who Are We?

- Anne G. Bowitz & Espen G. Graarud: 2010 Masters students at ITEM, NTNU, Norway
  - thesis work on simulation & prototype
- Lawrie Brown: UNSW@ADFA academic
  - original proposal from Erasmus Mundus visit
- Martin G. Jaatun: SINTEF research scientist
  - prior SINTEF project, thesis supervisor

Solution Overview

- extend BATMAN adhoc net routing protocol
  - so routing advertisements only accepted from authorised stations in the network
- use X.509 proxy certificates
  - to identify authorised client stations
  - generated by each network client
  - signed by a suitably authorised station
    - likely located with emergency services command unit

Related Work

- SINTEF project to develop a secure restricted ad-hoc network for emergency use
  - suggested extensions to OLSR routing protocol
  - using either pre-configured or short-lived certificates to identify clients
  - details mostly unspecified

Related Work cont.

- other work outlines issues with conventional PKI in such ad hoc networks
  - issues with certificate validation and revocation
  - proposal has some nodes intermittently connected
  - unlikely in such emergency or disaster scenarios
- short-lived X.509 certificates may be suitable for low power/resource limited devices
  - no revocation, less computationally intensive algs

Addressing Limitations

- in choice of ad hoc network routing protocol
  - OLSR standard, but see performance issues
  - BATMAN simpler, best overall performance
- in choice of certificate type to use
  - existing proposals involve using a mix of conventional and short-lived certificates
    - issuing stations need CA functionality & certificates
  - propose use of proxy certificates instead

X.509 Proxy Certificates

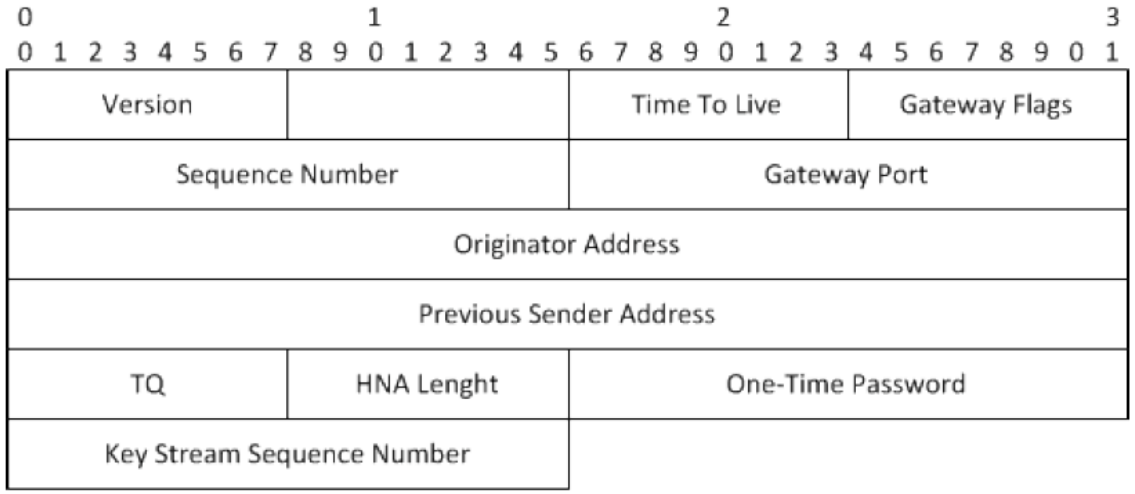
- X.509 certificates with proxy extensions
  - so can use in most existing PKI applications
- signed by conventional client or proxy cert
  - hence any client can issue proxy certificates
- can use shorter lifetimes & smaller key sizes
  - to better suit lower resourced mobile stations
- use as access token /capability for a service
  - opposite sense to current use in grid computing
    - where user delegates rights to a server

BATMAN

- Better Approach To Mobile Adhoc Networking
- replaces OLSR pro-active routing protocol
  - which requires every node in network to calculate whole routing path, link-state, complex
- BATMAN nodes only compute next hop
  - compares number of routing messages received from each node and who was the last sender
  - hence a simpler, distance-vector, routing protocol

BATMAN OGM

- exchanges OGM routing messages
  - are received and rebroadcasted by all nodes
  - so nodes learn existence of each and first hop

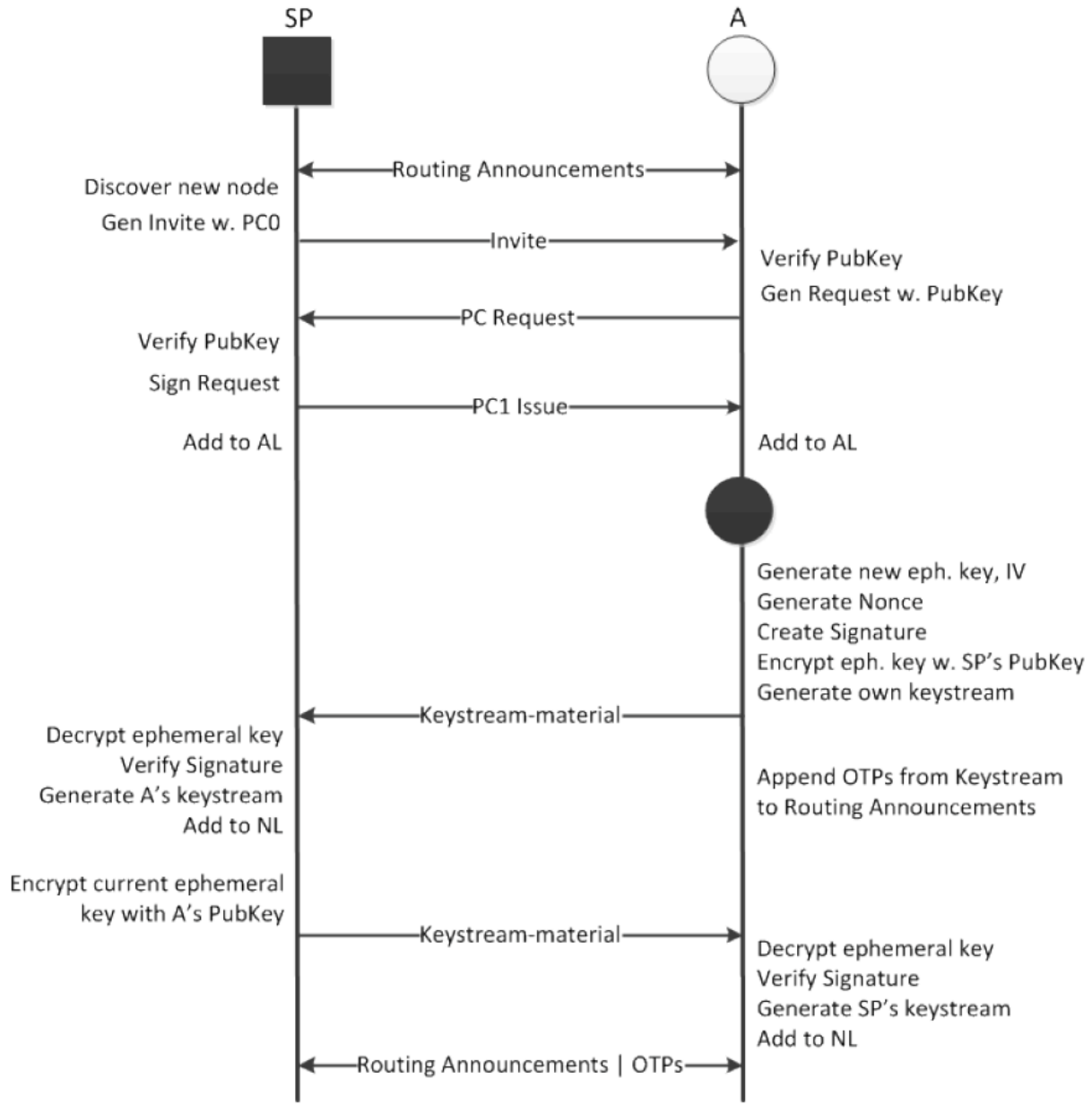


Requirements

- consider emergency situation scenario, with communication infrastructure unavailable
- Ad hoc networks have desired characteristics
  - quick and inexpensive setup
  - independent of communication infrastructure
- but also introduce security challenges
- we refine these needs further in the paper

Solution Outline

- system design requires nodes to authenticate and be trusted before using the network
- starts with out-of-band authentication
  - where master node verifies new nodes
- SP discovers new node via routing announcements and invites it to handshake
  - establish trust, verify fingerprints, issue proxy


SP
A
Routing Announcements
Discover new node
Gen Invite w. PC0
Invite
Verify PubKey
Gen Request w. PubKey
PC Request
Verify PubKey
Sign Request
PC1 Issue
Add to AL
Add to AL
Generate new eph. key, IV
Generate Nonce
Create Signature
Encrypt eph. key w. SP's PubKey
Generate own keystream
Keystream-material
Decrypt ephemeral key
Verify Signature
Generate A's keystream
Add to NL
Append OTPs from Keystream
to Routing Announcements
Encrypt current ephemeral
key with A's PubKey
Keystream-material
Decrypt ephemeral key
Verify Signature
Generate SP's keystream
Add to NL
Routing Announcements | OTPs

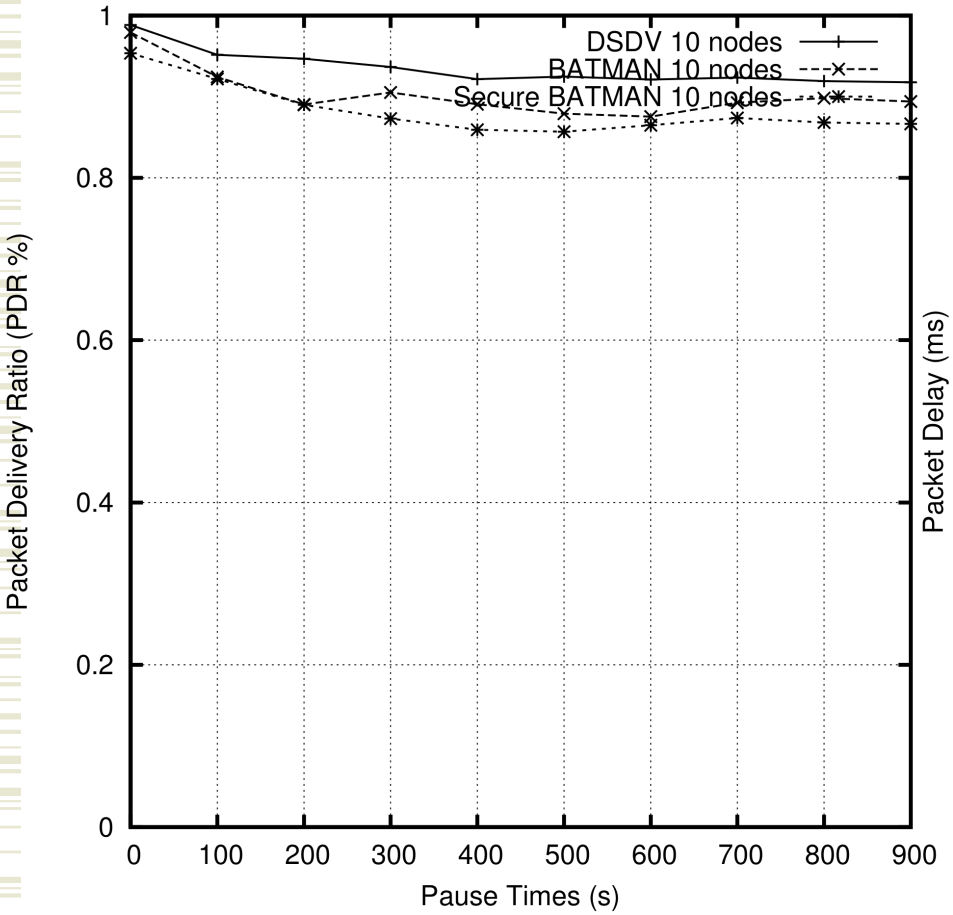
Solution Outline cont.

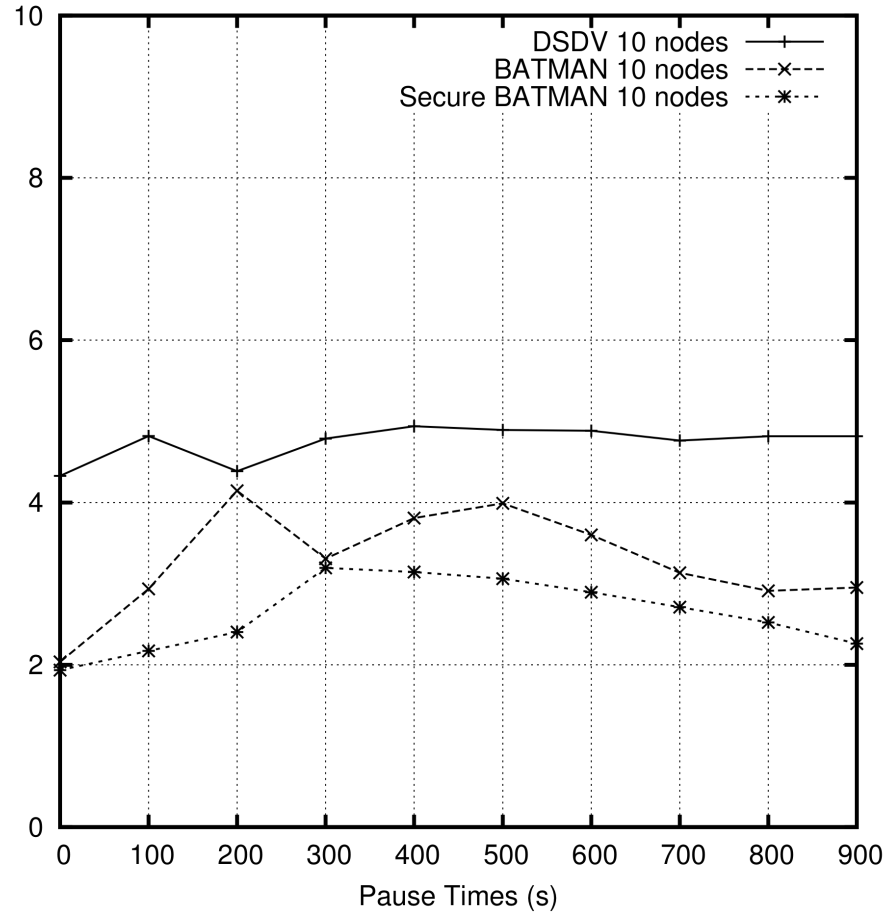
- once have proxy cert, each node periodically broadcasts (actually unicast) a message with
  - ephemeral key, IV, nonce, and digital signature
- used to generate a keystream (AES-CBC)
- then appends two new bytes from keystream
  - to each routing announcement
  - to re-broadcasts of neighbors' announcements
  - forms a one-time password on announcements

Solution Outline cont.

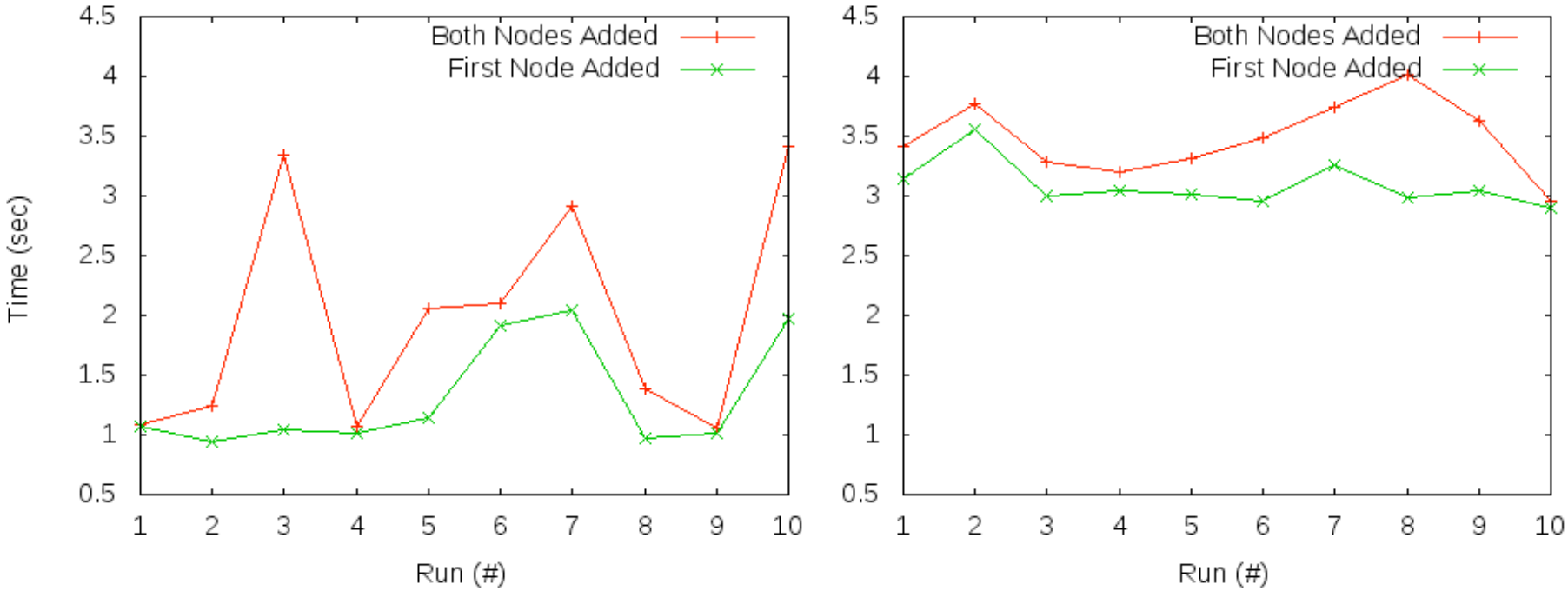
- SP regularly broadcasts lists of trusted nodes
  - with id, address and public key for each
  - list is signed by SP to guarantee integrity
- hence nodes only learn about new nodes from this list, not directly
- other nodes can rebroadcast list for SP if offline

NS3 Simulations

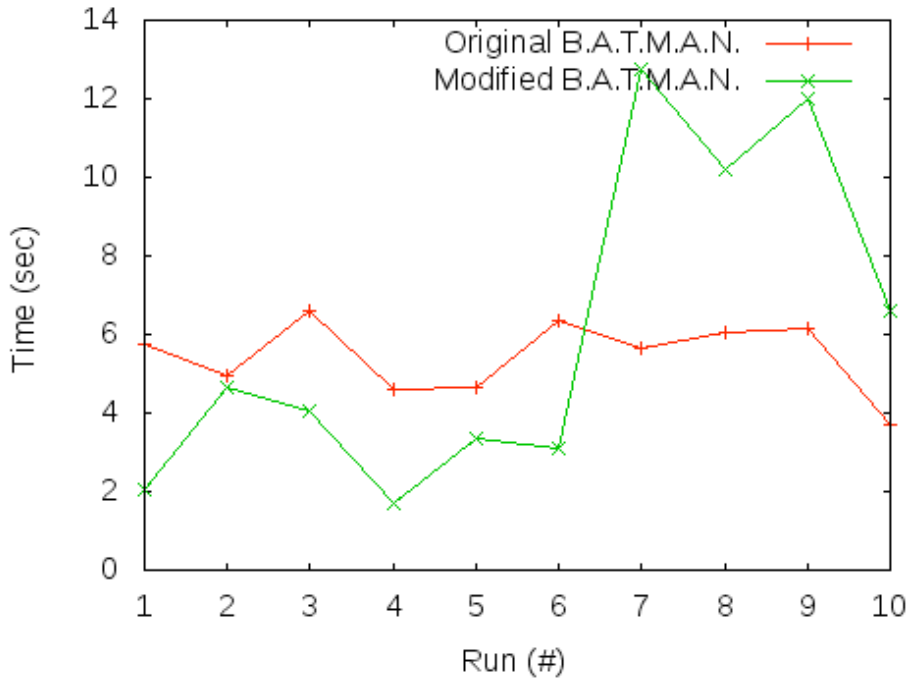




Prototype on Ubuntu Linux



Prototype on Ubuntu Linux



Discussion

- propose novel solution that continuously verifies routing announcements received from neighbors
  - not using digital signatures on each as too big
  - can't just sign a very few as leave open weaknesses
  - rather use keystream as one-time password to verify messages
- solution is based on trust
  - that each node correctly sends and rebroadcasts announcements
  - scheme does not protect against malicious but trusted nodes

Conclusion & Questions

- presented security extension to BATMAN ad hoc routing protocol
  - to handle controlled network admission
  - to prevent unauthorized nodes influencing routing
- NS3 simulations indicate these security mechanisms impose reasonable overheads
- prototype implementation confirms this
  - although further refinements are desirable
- hence BatCave is a viable security solution