IP Address Handoff and Cluster-Based Security Architecture in (M)ANET

Fabian Meyer

Email: fmeyer@cs.uni-goettingen.de

Telematics Group
Institute for Informatics
University of Göttingen, Germany

Papers

A Cluster-Based Security Architecture for Ad Hoc Networks

M. Bechler, H.-J. Hof, D. Kraft, F. Pählke, L. Wolf

IP Address Handoff in the MANET

H. Zhou, M.W. Mutka, L.M. Ni

A Cluster-Based Security Architecture for Ad Hoc Networks

- 1: Basic Ideas
- 2: Cluster-Based Approach
- 3: Conceptual Building Blocks
- 4: Details

1: Basic Ideas

- Problems:
  - Central authority not possible in ad hoc network
    - Too risky because it would be a central attack-point
  - Pre-shared schemes not possible
  - Encryption is worthless without authentication
- Solution:
  - De-centralized Certification Authority (CA)
    - Decentralization through „threshold cryptography“
  - Clustering

Decentralized CA 1/2

- Threshold Cryptography
  - Security by spreading the secret over different entities
  - Trusted dealer divides a secret „D“ into „n“ parts
  - Knowledge of „k“ parts (k ≤ n) allows secret reconstruction
  - This is called a „(k,n) threshold scheme“

Decentralized CA 2/2

- Secret Sharing
  - Verifiable Secret sharing
    - Construction algorithm ensures that each node can verify secret and shares both
  - Proactive Secret Sharing (PSS)
    - Secret shares change periodically without changing the secret itself
      - Periodic change only needed if no other event has triggered a change in the meantime (e.g. new or leaving CH's)

2: Cluster-Based Approach

- Main goal:
  - Basis for secure communication and accescontrol
    - Without central entities
- Additional goals:
  - Support for open networks (no pre-shared secrets necessary)
  - Fine-grained access control
  - Quick adaption to changes in the network
  - Scalability to support large number of nodes

Clustering 1

- Partitioning of an ad hoc network into several clusters
- Each cluster has one Cluster Head (CH)
- Gateways (GW) manage communication with adjacent clusters
  - 2 schemes for choosing new GW's:
    - Each node that comes into contact with another cluster can become a GW
    - Permission to become GW has to be given by CA

Clustering 2

- Beacons
  - CH's send beacons (CHb) periodically, containing:
    - Public Keys of the CH-Network and the CH itself
    - List of nodes in the cluster and their status (guest, member, GW…)
    - Information about GW's and adjacent clusters
  - GW's send GW-beacons (GWb) periodically
    - Informs cluster of adjacent clusters

Clustering 3

- This approach is independet of the routing protocol
  - Cluster-based routing protocols can benefit from synergy effects:
    - Secure Routing (possibility to choose nodes that shall forward packets e.g. only authenticated cluster members)
      - 2 Routing tables in each cluster node
  - Clusters can be formed as needed if no clustering is provided by the routing protocol

3: Conceptual Building Blocks

- 1. Network-wide distributed certification infrastructure
- 2. Symmetric encryption for secure communication on intra-cluster links
- 3. Access control through Authorization Certificates (AuthCert)

3.1 Network-Wide CA

- The Certification Authority
  - Is distributed over the whole network
    - Enhanced availabilty
    - No singular target for attacker present
  - All CH's together form the CH-Network
    - CH-Network is used as distributed CA
    - Every CH holds a share of the secret key (also called „network key“)
    - More than 1 network can be present in the same area
      - They must use different network keys
      - They may or may not be merged later

3.1 Network-Wide CA

- Cluster Heads
  - CH's can choose a successor
    - All states and the network key share are transferred to the new CH
    - Old CH informs CH-Network as well as cluster of the change
    - Key-share updates will then be send to the new CH
  - Failing CH's trigger the building of a new cluster
    - Very complicated and costly if a network already exists

3.2 Intra-Cluster Security

- Symmetric key known to all cluster-nodes used for encrypting intra-cluster traffic
  - Hides source and destination address and data from eavesdroppers outside the cluster
  - Can be integrated or replace IEEE 802.11 or Bluetooth mechanisms

3.3 Authorization through Certificates

- New node join cluster as guests with no rights
  - Needs to get its public key signed by CH-Network to become full member
    - Must be authenticated first
- Full members can get access to certain services/ressources (GW's, Printer, FTP Server, ...) through „Authorization Certificates“ (AuthCert)

3.3 Authorization through Certificates

- New node Authentication
  - Node needs to gather „Warrant Certificates“
    - Issued by nodes of the cluster with the privilege to warrant
    - New node needs to authenticate itself to the nodes that will issue a warrant for it
      - Authentication can be done:
        - » On Technical Level (direct contact via cable or IRDA…)
        - » Outside Technical Level (users talk, number plate recognition)
    - The more warrants a new node has, the surer its authentication (with possible additional rights).

3.3 Authorization through Certificates

- Access control
  - Entities controlling a ressource/service can issue certificates for nodes to use the respective ressource/service
    - Can also grant nodes the privilege to grant access to the ressource/service
  - Simpler methods possible:

LEVELS OF CONTROL OVER ADMITTED USERS

User or provider group	*Credential*
all nodes	none
all full members	secret cluster key or certified public node key
specific nodes	authorization certificate
directly trusted nodes	any of the above, or a preshared key

4: Details

- 1. Log-on Procedure
- 2. Merging a Cluster into a Network
- 3. Merging 2 Networks
- 4. Adaptable Complexity

4.1 Log-on Procedure

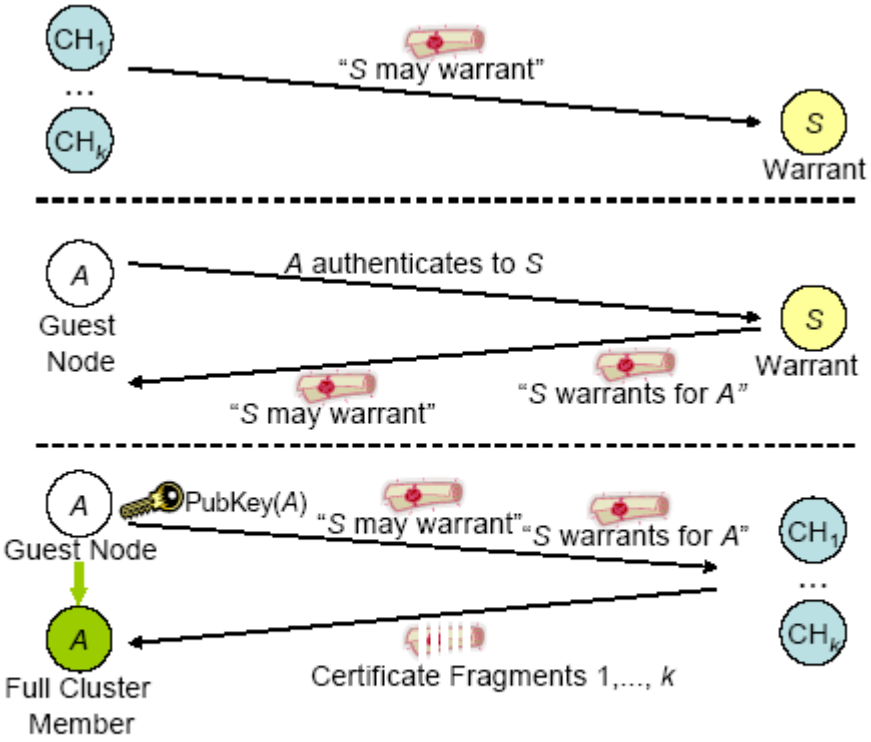


Fig. 1. Authentication process

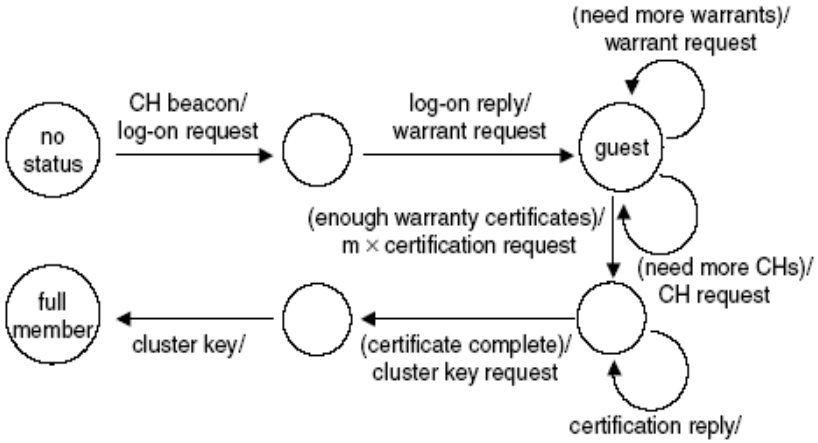


Fig. 2. States of a new node during log-on

4.2 Merging a Cluster into a Network

- CH of the cluster to merge needs to get warrants from nodes of the new network
  - If enough warrants are gathered, the CH becomes a member of the CH-Network and receives a share of the network-key
  - If not, CH-duties have to be passed to a node of the cluster that has acquired enough certificates
  - If no node acquires enough certificates, the cluster is dissolved and all nodes have to join existing clusters of the new network

4.3 Merging 2 Networks

- Difficult and Costly
- 2 network-keys can't be mixed: one has to be dropped
  - All certificates issued with the dropped key have to be re-issued
  - Possible adaption of the (k,n)-threshold scheme necessary
  - Before the merge it has to be decided which key to drop
    - Best way: Decision based on number of issued certificates

4.4 Adaptable Complexity

- The complexity introduced by encryption can be adated
  - Per-case decision, based on the power of the node
  - Levels:
    - 1. no encryption
    - 2. secret cluster-key (for intra-cluster traffic)
    - 3. Public keys for nodes (directly exchanged)
    - 4. Public keys for nodes (using CA)
  - If no consens about the level is reached, no communication is possible.

Papers

A Cluster-Based Security Architecture for Ad Hoc Networks

M. Bechler, H.-J. Hof, D. Kraft, F. Pählke, L. Wolf

IP Address Handoff in the MANET

H. Zhou, M.W. Mutka, L.M. Ni

IP Address Handoff in the MANET

- 1: MANET
- 2: Motivation
- 3: Related Works
- 4: Solutions to Broken Routing Fabrics
- 5: Solutions to Broken Communication

1: MANET

- Temporary, wireless network of mobile nodes
- No infrastructure
- IP-based
  - Nodes have to be configured with a free IP address to receive unicast messages
  - IP address may change during a session

IP Address Changes 1/4

- Merge of two network parts:

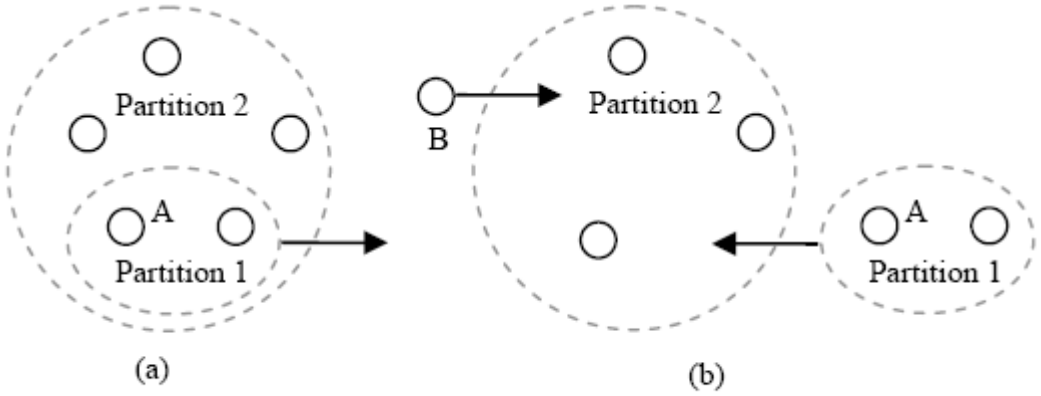


Figure 1. A network is partitioned and then merged later

IP Address Changes 2/4

- Merge of two independent MANETs:

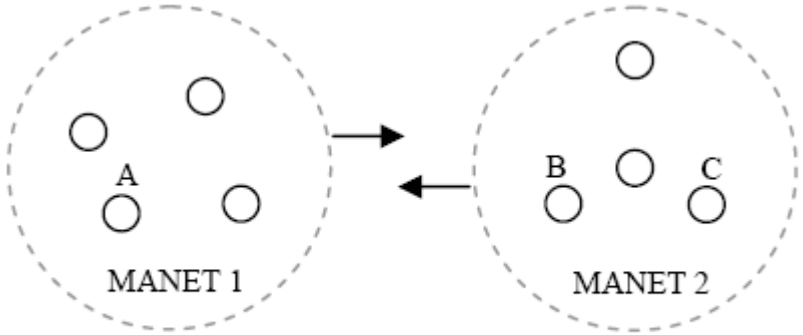


Figure 2. Merger of two independent MANETs

IP Address Changes 3/4

- Merge of MANET with a LAN:

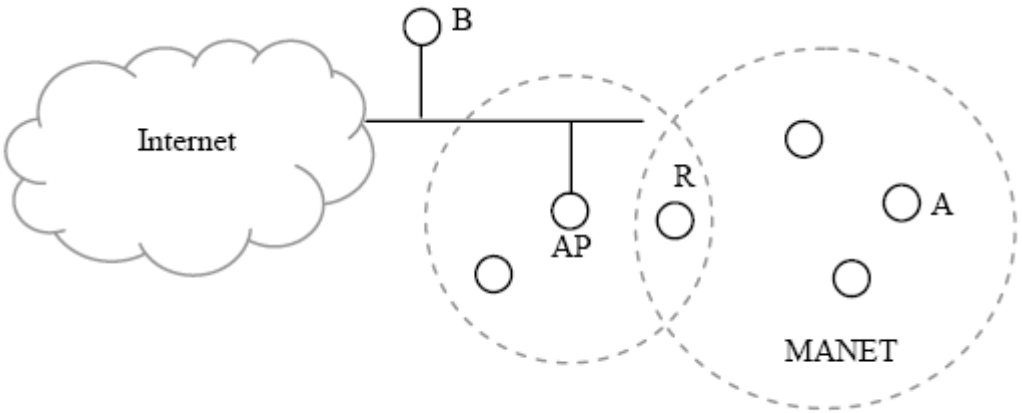


Figure 3. The merger of a MANET and a WLAN

IP Address Changes 4/4

- Hierarchical addressing scheme:

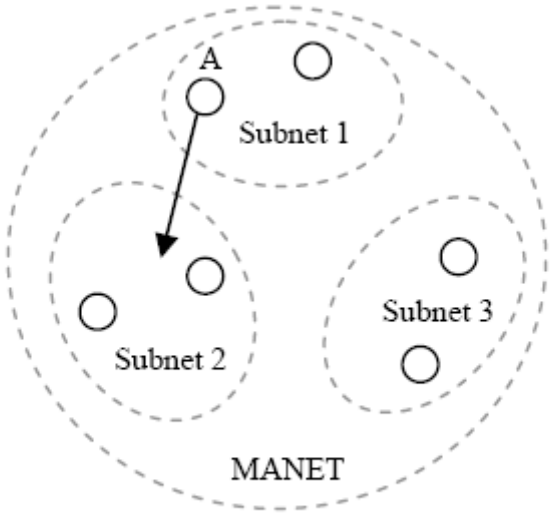


Figure 4. A MANET with hierarchical addressing scheme

2: Motivation for Handoff Scheme

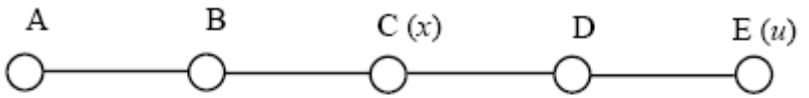
- Broken routing fabrics
  - Cause overhead on network load and time for fixing
- Broken on-going communications
  - Not practical when using real-time media
  - Active resuming may not be possible if the address of e.g. a FTP-server changes
  - Privacy issues
    - e.g. VoIP connections may end up being redirected to false node

3: Related Works

- MobileIP
  - Uses HomeAgent to forward packets for Home Address to new Temporary Address
    - HA not reachable in typical MANET
- Tunneling
  - Introduces „DoS“ problem
    - (as described in detail later on)

4: Solutions to Broken Routing Fabrics

- In this work AODV assumed as routing protocol
  - Ad hoc On demand Distance Vector routing
    - Reactive („lazy“)
    - Table-driven
- Node C informs neigbors of address change
  - Using „Route Shift“ Packet
    - Contains both Ips
    - Vulnerable to IP spoofing
      - Auth needed



Dest	Next
D	C (x)
E	C (x)

Dest	Next
B	C (x)
A	C (x)

Figure 5. A MANET of 5 nodes in a chain

Route Shift Packet Authentication

- Route Shift packet is broadcasted to neighbors (TTL=1)
- Authentication via CA causes too much overhead
  - A „cookie“ approach is used
    - Node generates a random number for its IP address
    - Node sends a hash of that number in RREQ, RREP and HELLO messages (receiving nodes store the hash)
    - Route Shift can be verified by sending the original random number (that all nodes can verify using the hash)

5: Solutions to Broken Communication

- 1. Assumptions
- 2. Route Rebuilding
- 3. Communication Preservation
- 4. Challenges to Key Management

5.1 Assumptions

- IP Layer supports more than 1 IP address per node
  - All links are bi-directional
  - New address is primary, old address secondary
  - Primary address is used on new outgoing packets
  - Secondary address ensures that packets to the old address still reach the node
  - HELLO messages are extended to contain both addresses
  - Node must not answer to Routing Request (RREQ) packets to the old address

5.2 Route Rebuilding

- Route rebuilding is achieved through „gratuitous Route Reply“ (gRREP)
  - Update along all paths that connect to old address
  - Sent for all active/recent communication to ensure all partners notice the change

5.3 Communication Preservation

- Problem: Checksums are calculated in the transport-layer in the end-hosts based on source and destination address
- Solution: adapted NAT mechanism

Adapted NAT Mechanism

- A
  - Incoming: new address „y“ changed to „x“ (for correct verification)
  - Outgoing: old source „x“ changed to „y“
- B
  - Incoming:new address „y“ changed to „x“ (for correct verification)
  - Outgoing:old destination „x“ changed to „y“

Address:
x -> y

Advantage over Tunneling

- Overhead of a second IP header is saved
- Only one address has to be changed in each NAT (faster)
- Tunneling brings „DoS“ Problem:
  - Limitation: A -> C not possible

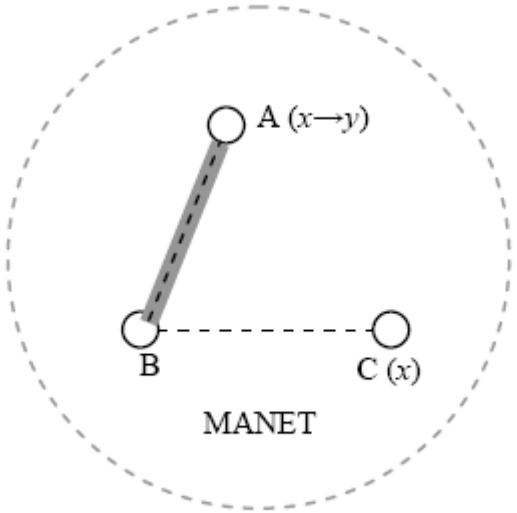


Figure 6. A “DoS” problem caused by IP tunneling

Further Enhancements to NAT 1

- NAT now uses sequence and port numbers to discern connections

TABLE I. NAT TABLE AT NODE B

1	2	3	4	5	6
Old remote address	New remote address	Local port	Remote port	Remote sequence number	Next remote sequence number
x	y	80	2030	228743	22884312
…	…	…	…	…	…

TABLE II. NAT TABLE AT NODE A

Old address	New address	Port number
x	y	2030
x	y	…

Address Change Messages

- Table in node B is built using „Address Change Messages“ (ACM)
- ACM:
  - Trigger the installation of a NAT entry
  - Can be combined with gRREP to save overhead
  - Has to be sent before data packets
    - Data can be buffered until ACM is sent
    - If no data is waiting, A may wait until B sends a packet before sending an ACM to B
  - Must be verifyable (e.g. signed with A's priv. key)

Deletion of NAT Entries

- NAT table entries must be deleted somewhen
  - TCP FIN flag on a data packet from A to B
  - Problematic with UDP, as UDP does not support flags
  - Timeout

5.4 Challenge to Key Management

- Problem: Node with changed IP address will be denied because its key is correctly bound to another address
- Solution: Use of the „cookie“-scheme with a random number and hash (same as with ACM)

The End

Thanks for your attention!