



**Anonymous Location-Aided Routing
Protocols for Suspicious MANETs**

Gene Tsudik

SPROUT:
**Security & Privacy Research Outfit
UC Irvine**

<http://sprout.ics.uci.edu>

joint work with Karim El Defrawy



2

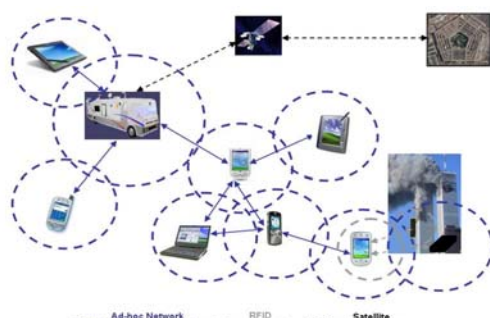
Outline

- Suspicious MANETS
- Goals
- ALARM
 - Security
 - Future Work
- PRISM
 - Security
 - Comparison
- Summary, Future Work, etc.

3

“Normal” MANETS

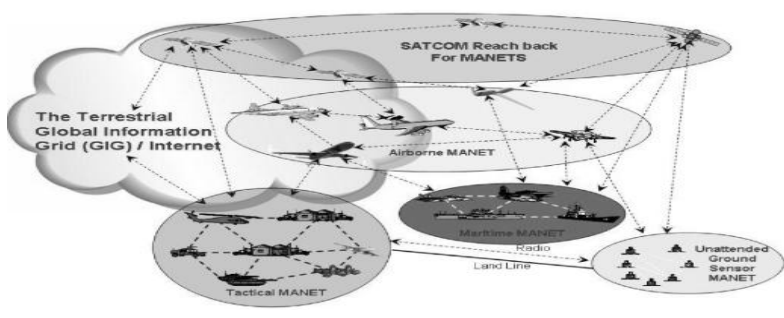
- No infrastructure
- Multi-hop
- Set of peer nodes
- Nodes move (but not too much)
- Nodes have unique names/addresses/IDs
- Routing protocols communication



9/20/10 4

“Suspicious” MANETs

- Environment is “hostile” and “suspicious”
 - Military/battlefield
 - Law enforcement
 - Mobile WSN (with self-locomotion)

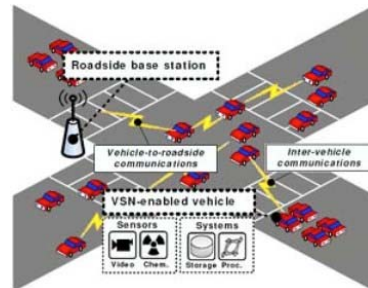


9/20/10

5

Vehicular Ad-Hoc Networks (VANETs)

- › Special type of MANETs
- › Restricted mobility (highways and roads) and high speeds
- › Privacy often required
- › Operation might be critical (e.g., ambulance)



9/20/10

6

WSNs with self-locomotion

- › Unattended WSNs, e.g., operating in remote locations
- › Covering certain fixed geographical area, e.g., for surveillance purposes
- › Adversary may compromise some nodes
- › Tracking should be prevented
- › How can nodes arrange themselves to inhibit tracking?

9/20/10

7

Privacy in MANETs

- Goal:
 - Tracking resistance → no long-term IDs for nodes
 - Escrowed Anonymity → only special authorized entities (e.g., court) can learn long-term IDs
- Challenges:
 - How to authenticate without long-term IDs?
 - How to achieve accountability in case of misbehavior?
 - Malicious insiders become harder to combat

9/20/10

8

Security in MANETs

- Typical security requirements:
 - Confidentiality
 - Integrity
 - Authentication
 - Accountability and non-repudiation

Difficult when coupled with privacy requirements...

9/20/10

9

Related Work

- Secure routing protocols: Ariadne, SRDP, SEAD, EndairA, SRP... (no privacy)
- Privacy-preserving routing protocols: ANODR, MASK, D-ANODR, ARM, ODAR...
 - All use identity-centric communication
 - All require one or more of:
 - Long-term IDs, pseudonyms, public keys, shared secrets, or on-line servers/TTPs
 - Not location-based
 - More later...

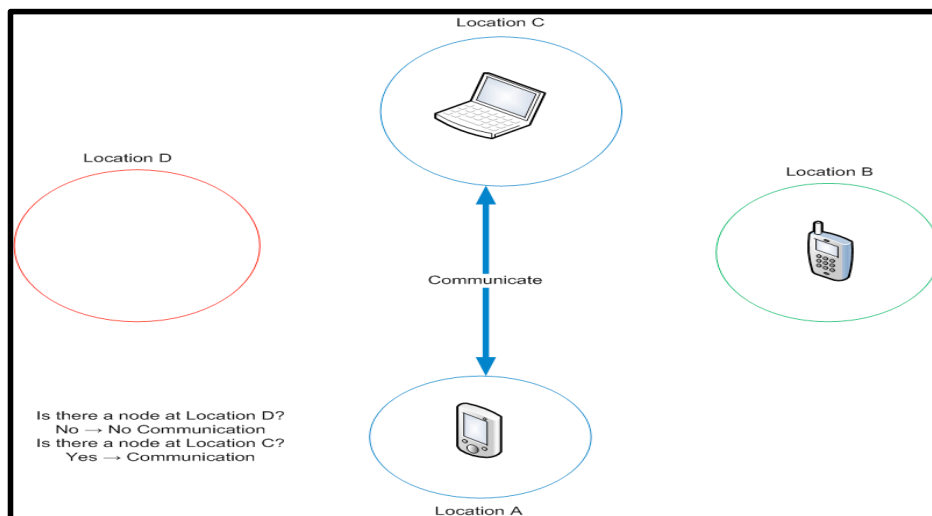
9/20/10

10

Our Results

- Location-centric communication instead of identity-centric
 - Well-suited for suspicious MANET/VANET settings.
- Location-centric communication is more privacy friendly
- Use of group signatures to construct privacy-preserving and secure MANETs routing protocols
- ALARM based on Link-State (OLSR)
- PRISM based on Flooding (AODV)

Location-based Communication Decisions 11



Assumptions 12

- **[LOCATION]** each node is equipped with a GPS or similar device
- **[PRIVACY]** no public node identities / addresses
- **[MOBILITY]** some min. number (k) of nodes move periodically
 - tracking a node require discerning it among a subset of nodes that moved in the interim
- **[SYNCHRONY]:** common (leap-frog) mobility followed by common rest
- **[SECURITY]**
 - all outsider attacks
 - passive (honest-but-curious) insiders

13

Auxiliary Assumptions

- [TIME] nodes maintain loosely synchronized clocks
- [RANGE] nodes have uniform transmission range*

14

Reactive vs Distance Vector vs Link State

- **Reactive:** route discovery requires ID (if based on location need to determine location first)
- **Distance Vector:** weak security, slow convergence
- **Link State:** no discovery phase, fast convergence, strong security, scalability not a pressing matter (e.g., with 100s of nodes)

15

ALARM

- Nodes communicate based on current location
- Anonymity, Authentication and Integrity
- Works with any location-aided forwarding scheme
- Group Signatures provide escrowed anonymous authentication
 - One-time pseudonyms
 - Anonymous authentication of origin and data integrity
 - Revocable/escrowed anonymity
- Can use any group signature scheme
 - unless protection against Sybil attacks is needed

16

Group Signatures (GSIG)

- Any member in a potentially large and dynamic group can sign a message (produce a signature)
- Signature can be verified by anyone who has a constant-length group public key
- Valid signature implies that the signer is a genuine group member
- Given two signatures, it is computationally infeasible to determine if they were signed by the same group member
- In the event of a dispute, a group signature can be opened to reveal actual signer

17

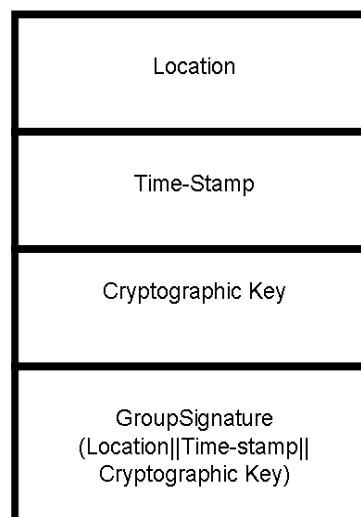
Group Signatures in ALARM

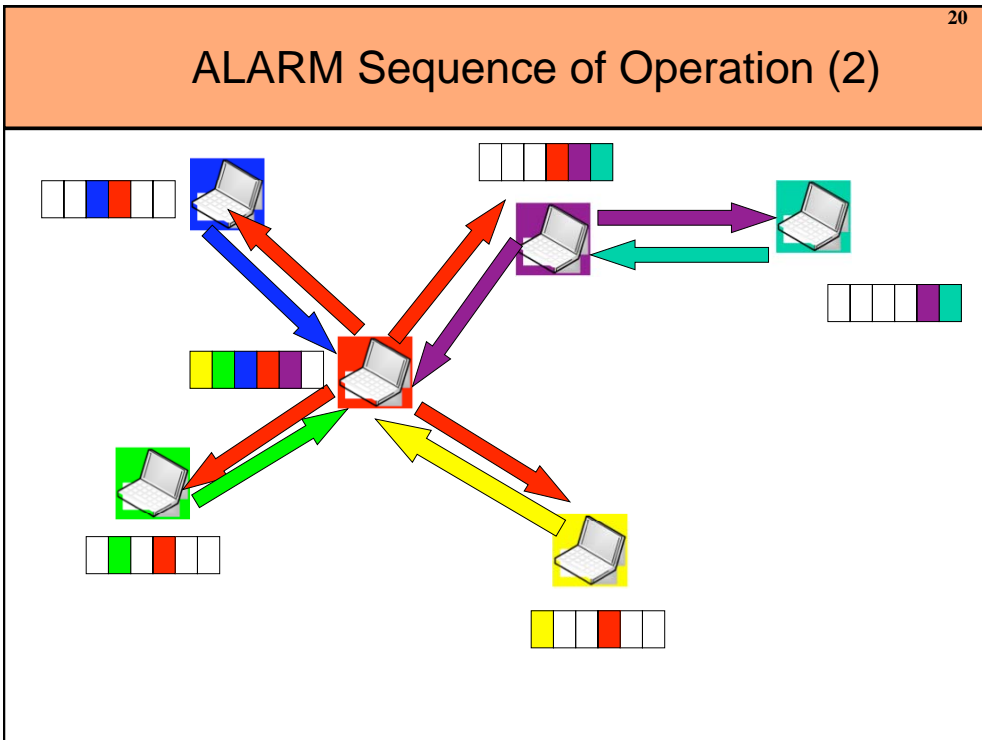
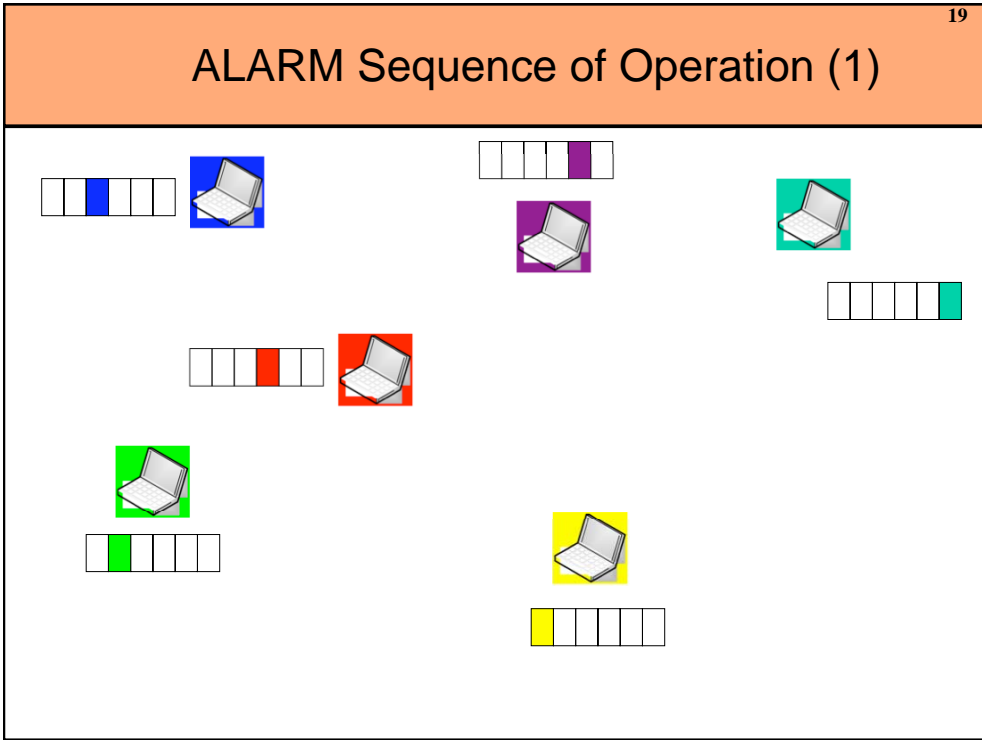
- A node generates a GSIG over its Location Announcement Message (LAM)
- Two LAMs by same node can not be linked
- Anyone can verify that LAM was produced by an authorized group member (node)
- Assume an off-line (trusted) group manager who sets up the GSIG scheme

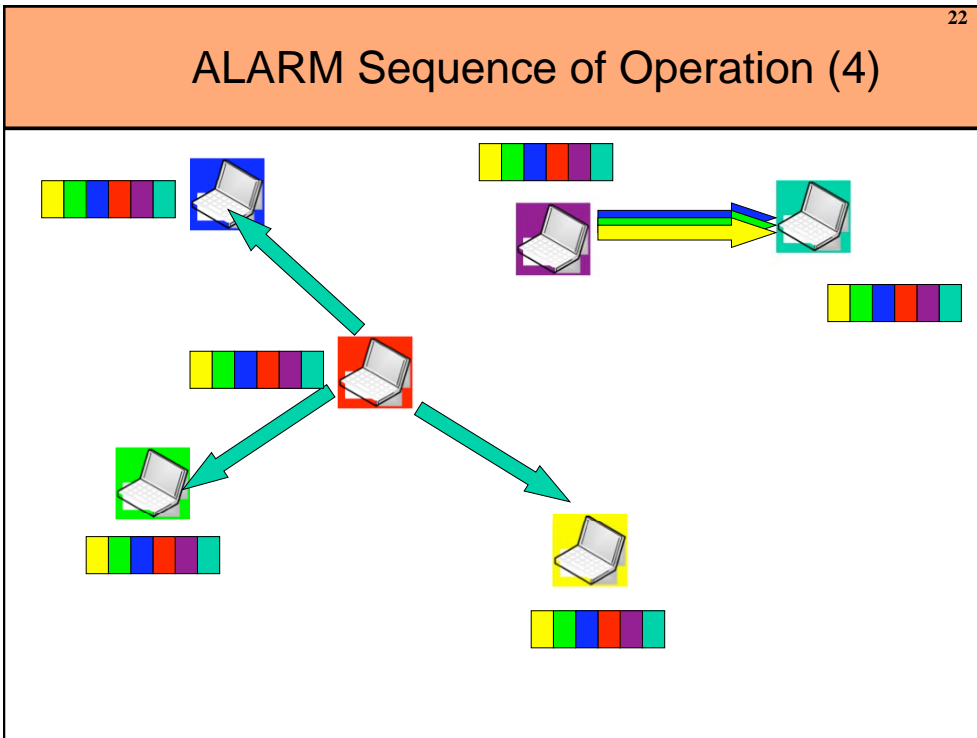
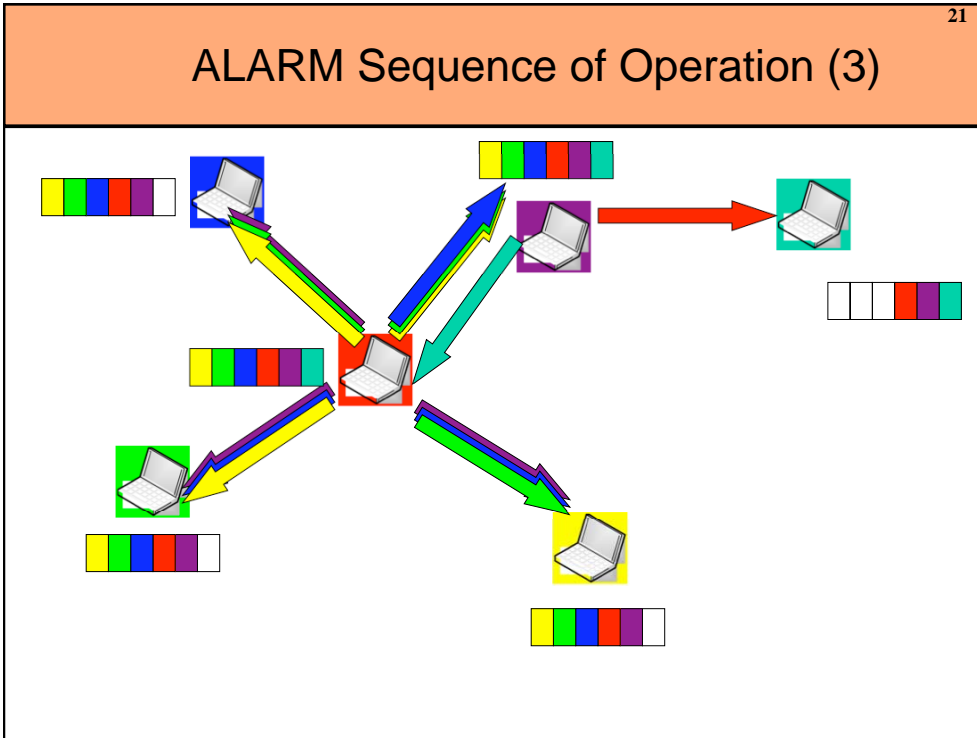
18

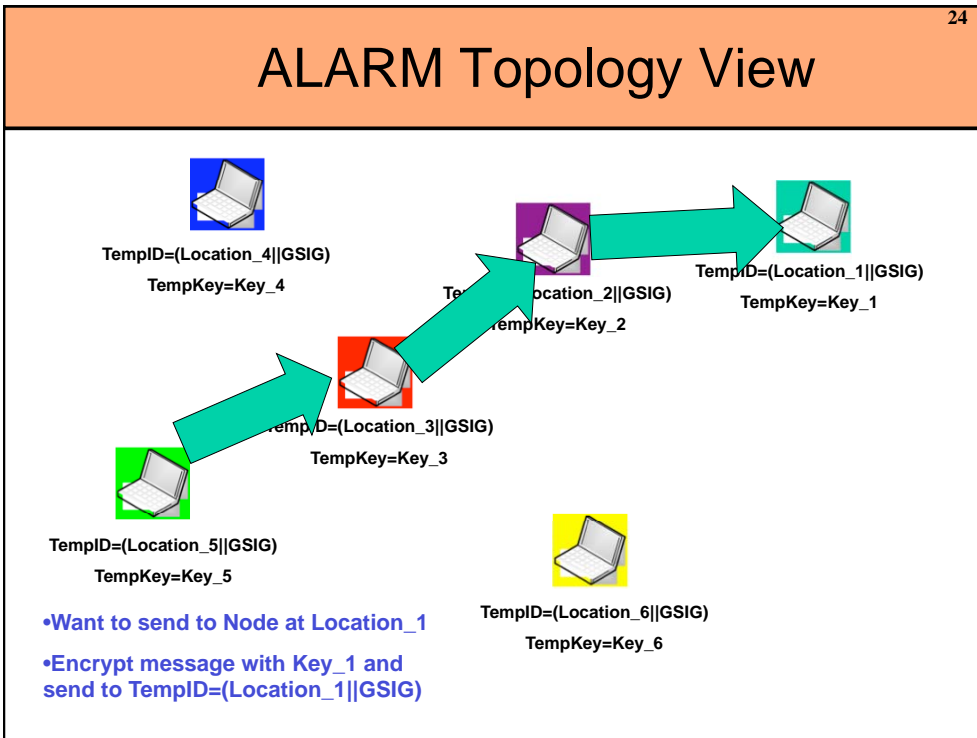
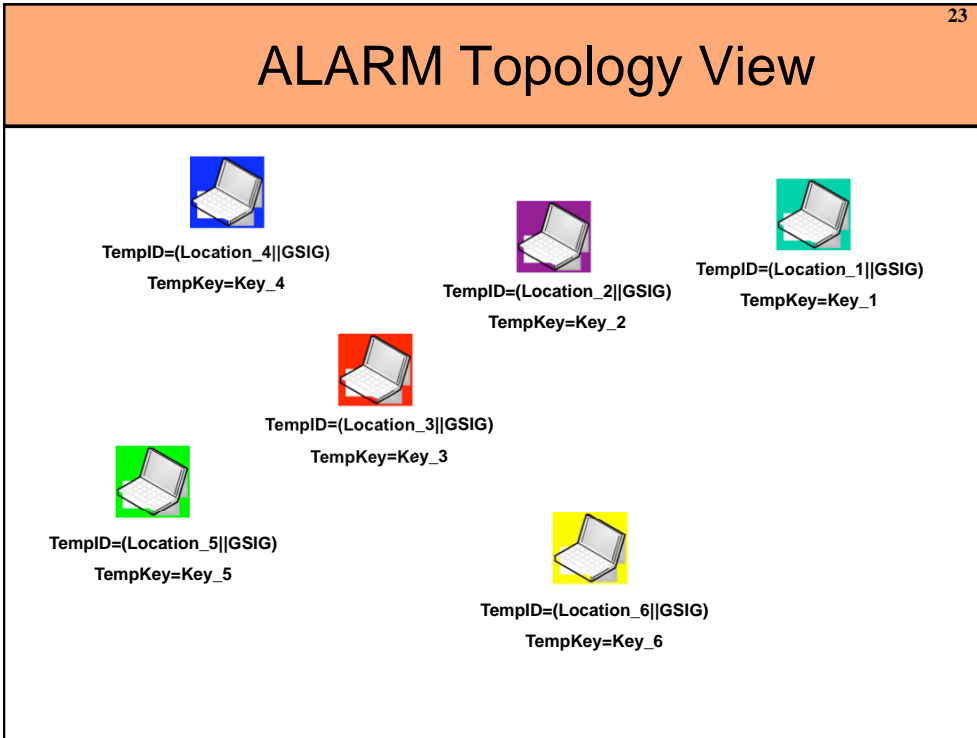
Location Announcement Message (LAM)

- **Location**: current location of node
- **Time-Stamp**: current time-period number (to prevent replays)
- **Ephemeral Key**: for encrypting data exchanged later (e.g., Diffie-Hellman half-key)
- **Group Signature**: provides authentication & integrity. Used as one-time pseudonym for node at that location.









Security Analysis (1)

Active/Passive Outsider:

- Records, replay messages or inject new messages
 - Replay attacks prevented by LAM time-stamps
 - Injecting / modifying LAMs requires producing genuine GSIGs

Security Analysis (2)

Passive Insider (Honest-but-Curious):

- Eavesdrops on messages, attempts to track peers nodes
 - Can't link two messages to same node (computationally infeasible to link two GSIGs)
 - Can track movement of node by monitoring likely trajectories
 - if node movement is random and K nodes move within same period, attack not effective (simulation)

Average Node Privacy (ANP)

- One possible metric capturing node privacy
- Determines fraction of all nodes to which a node can be mapped between two successive topology snapshots

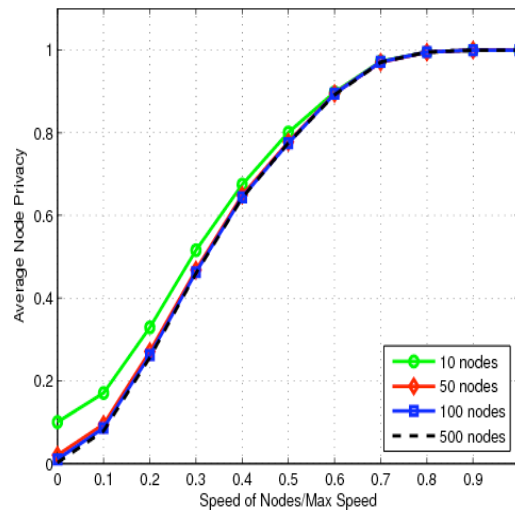
$$ANP = \sum_{i=0}^{i=K} (K - K'_i) / K^2$$

- K = total number of nodes
- K'_i = number of nodes to which i can't be mapped

Simulation Results (Random Walk)

Random Walk Mobility Model:

- All nodes move
- 1km*1km area
- Max speed = 1.4km/period between 2 LAMs

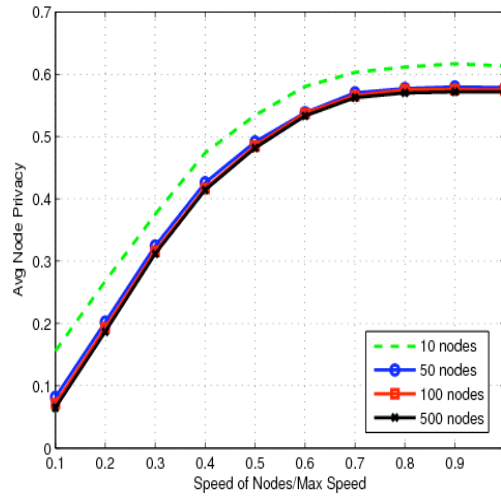


29

Simulation Results (Random Waypoint)

Random Waypoint Mobility Model:

- All nodes move
- Nodes stop with probability (0.5) for duration of 2 LAMs
- 1km*1km area
- Max speed = 1.4 km/ period between 2 LAMs

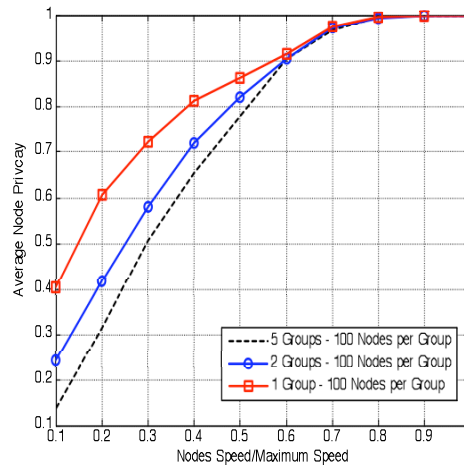


30

Simulation Results: RPGM

Reference Point Group Mobility (RPGM):

- All nodes move
- 1km*1km area
- Max speed = 1.4 km/ period between 2 LAMs
- ANP is better at lower speeds since RPGM ensures nodes are in each other's vicinity



31

Security (3)

Active Insider:

- Lies about other locations = creates phantom nodes with signed LAMs (Sybil attack)
 - Need to modify GSIG scheme to allow self-distinction
 - Has been done (FC'98, PET'06)
- Lies about own location
 - Need secure hardware...
 - Must contain GSIG Sign and GPS components

32

Future Work

To Do:

- Better (more precise) analytical privacy model
- Better evaluation with “real” MANET traces
 - Unsurprisingly, military traces are hard to come by...
 - But, VANET traces are easier to obtain

33

PRISM: Motivation

Issues with ALARM:

- LS exposes topology
- LS requires many closely-spaced messages
- Leap-frog mobility model uncommon
- Sybil attack detection is awkward

34

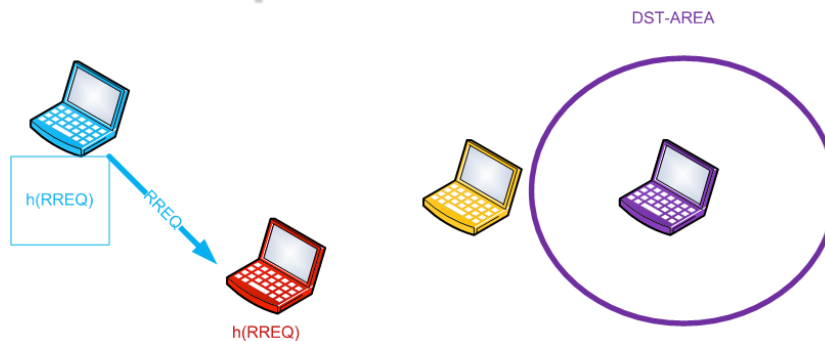
PRISM: Motivation

- No permanent identities (location-centric comm.)
- No explicit topology exposure
- Destination is a geographical area
- Hit-and-miss on-demand protocol
- **Goals:**
 - **Privacy:** against insiders and outsiders
 - **Security:** against passive insiders and outsiders
 - (active insiders detected off-line)
 - **Efficiency:** low overhead

PRISM Operation

- Works on top of AODV (using RREQ and RREP)
 - AODV is on-demand (reactive) → does not *propagate topology information*, in contrast with reactive protocols
 - AODV is distance-vector → no routes are exposed
 - AODV is robust: uses flooding for route discovery → no need for synchronized mobility (leapfrog)
- RREQ flooded using target geographical area
- RREP forwarded only by nodes in RREQ
- Use hash of RREQ, RREP as a route identifier
- Group signatures used for authentication
 - un-linkable and un-forgeable

PRISM Operation



SRC wants to talk to a node in DST-AREA!

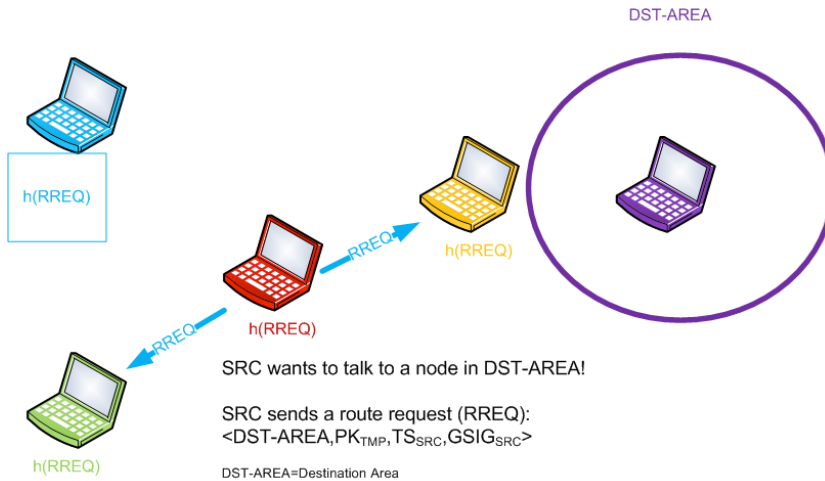
SRC sends a route request (RREQ):
 $\langle \text{DST-AREA}, \text{PK}_{\text{TMP}}, \text{TS}_{\text{SRC}}, \text{GSIG}_{\text{SRC}} \rangle$

DST-AREA=Destination Area
 PK_{TMP}= temporary public key generated by source
 TS_{SRC}= current time stamp
 GSIG_{SRC}= Group signature over previous fields

9/20/10

37

PRISM Operation



SRC wants to talk to a node in DST-AREA!

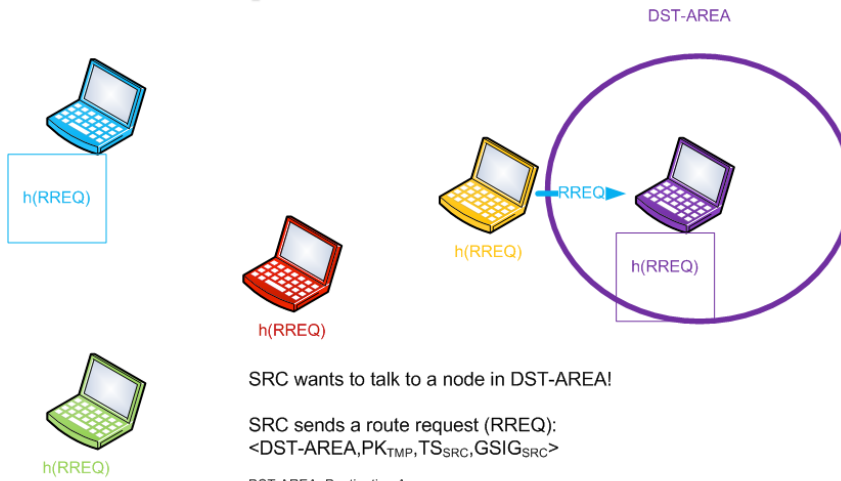
SRC sends a route request (RREQ):
<DST-AREA, PK_{TMP}, TS_{SRC}, GSIG_{SRC}>

DST-AREA=Destination Area
PK_{TMP}= temporary public key generated by source
TS_{SRC}= current time stamp
GSIG_{SRC}= Group signature over previous fields

9/20/10

38

PRISM Operation

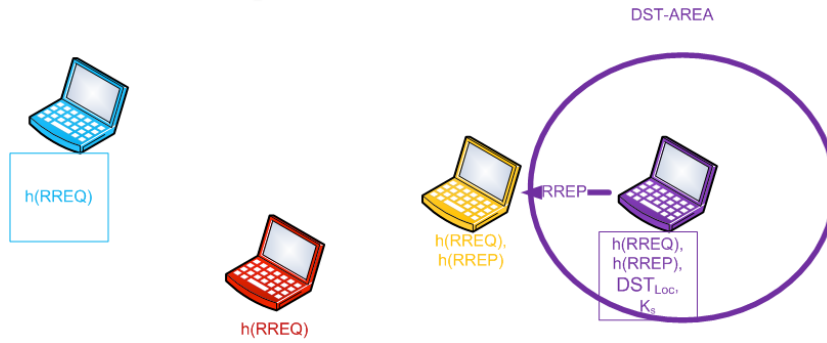


SRC wants to talk to a node in DST-AREA!

SRC sends a route request (RREQ):
<DST-AREA, PK_{TMP}, TS_{SRC}, GSIG_{SRC}>

DST-AREA=Destination Area
PK_{TMP}= temporary public key generated by source
TS_{SRC}= current time stamp
GSIG_{SRC}= Group signature over previous fields

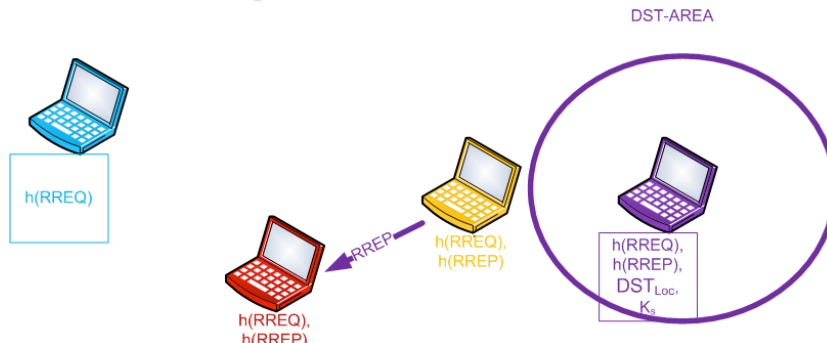
PRISM Operation



DST sends a route reply (RREP):
 $\langle h(RREQ), Enc_{PK_{tmp}}(K_s, DST_{Loc}), GSIG_{DST} \rangle$

$h(RREQ)$ = hash of RREQ message
 $Enc_{PK_{tmp}}()$ = encryption under key PK_{tmp}
 K_s = session secret key
 DST_{Loc} = exact location of destination
 $GSIG_{DST}$ = destination GSIG of previous fields

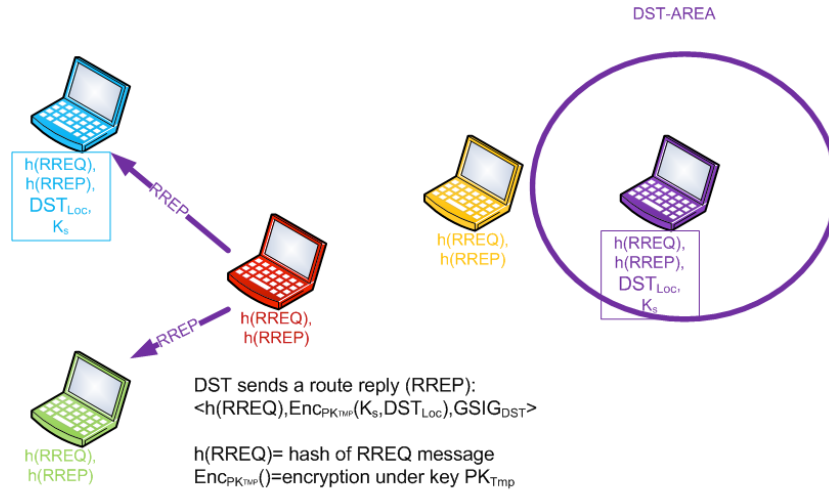
PRISM Operation



DST sends a route reply (RREP):
 $\langle h(RREQ), Enc_{PK_{tmp}}(K_s, DST_{Loc}), GSIG_{DST} \rangle$

$h(RREQ)$ = hash of RREQ message
 $Enc_{PK_{tmp}}()$ = encryption under key PK_{tmp}
 K_s = session secret key
 DST_{Loc} = exact location of destination
 $GSIG_{DST}$ = destination GSIG of previous fields

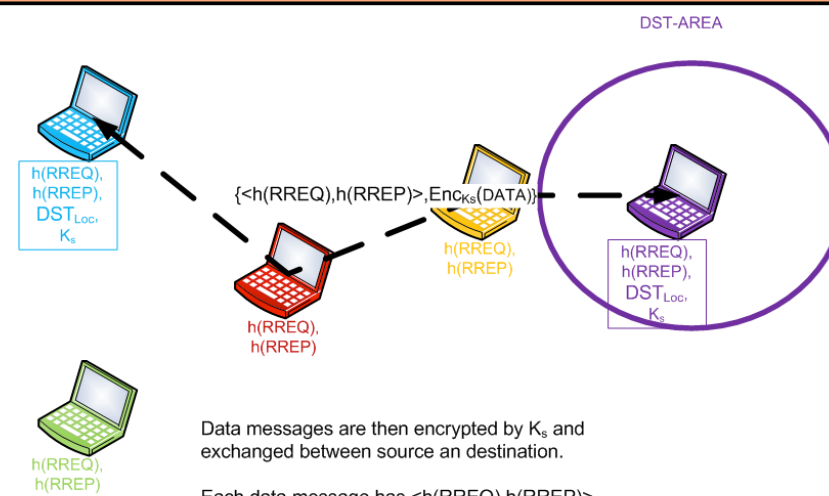
PRISM Operation



DST sends a route reply (RREP):
 $\langle h(RREQ), Enc_{PK_{tmp}}(K_s, DST_{Loc}), GSIG_{DST} \rangle$

$h(RREQ)$ = hash of RREQ message
 $Enc_{PK_{tmp}}()$ = encryption under key PK_{tmp}
 K_s = session secret key
 DST_{Loc} = exact location of destination
 $GSIG_{DST}$ = destination GSIG of previous fields

PRISM Operation



Data messages are then encrypted by K_s and exchanged between source and destination.

Each data message has $\langle h(RREQ), h(RREP) \rangle$ as a route identifier.

43

ALARM vs PRISM

- ◆ALARM: communication decision depends on current topology (link state)
- ◆PRISM: communication decision determined independent of current topology (AODV)
- ◆PRISM exposes less topology (more privacy)
- ◆PRISM has less routing overhead (fewer messages)
- ◆PRISM is *hit-and-miss* → wasted route discovery

CLAIM: no way to “fix” hit-and-miss problem without either:
 (1)ALARM-like approach, or
 (2) long-term identities

9/20/10
44

ALARM vs. PRISM

ALARM	PRISM
Link State based	AODV based
Proactive	Reactive
Restricted mobility model (leap frog)	Any mobility model
Exposes entire topology snapshot	Exposes partial topology
Precise knowledge of node location	Hit-and-miss approach
Send to specific node @ location	Sends to area, not specific location

9/20/10

45

PRISM Security Analysis (1)

- Active/Passive Outsiders:
 - Records, replays and injects new routing messages
 - Replay attacks prevented due to RREQ/RREP time-stamps
 - Injecting or modifying messages requires producing genuine GSIGs (computationally infeasible)

9/20/10

46

PRISM Security Analysis (2)

- Passive (honest-but-curious) Insiders:
 - Eavesdrop in order to track peer nodes
 - Can't link two messages to same node (computationally infeasible to link two GSIGs)
 - Can track movements by monitoring likely trajectories (but need whole topology)
 - Less topology exposure than in link state

9/20/10

47

PRISM Security Analysis (3)

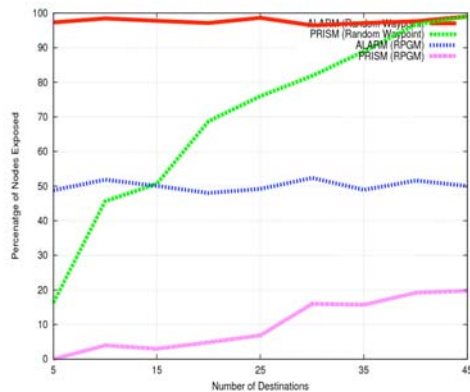
- ▶ Active Insiders:
 - Not secure against active insiders in real time
 - Active insiders can lie about their locations and create phantom nodes (does not hurt privacy)
 - Can be detected off-line by GM

9/20/10

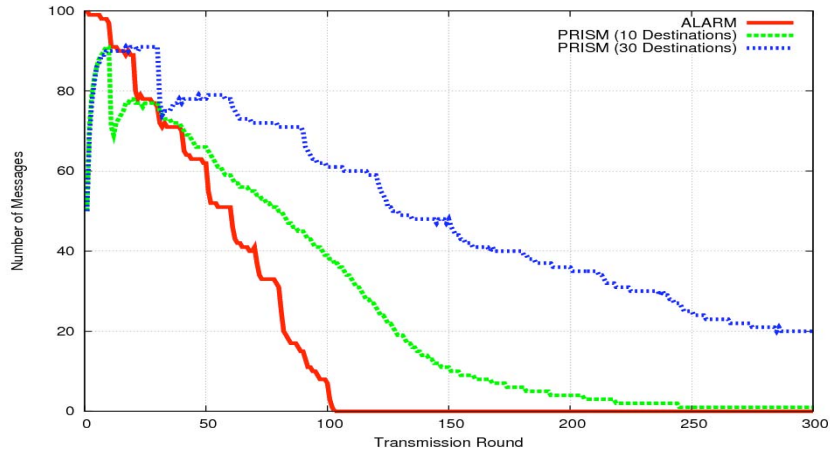
48

PRISM Topology Exposure

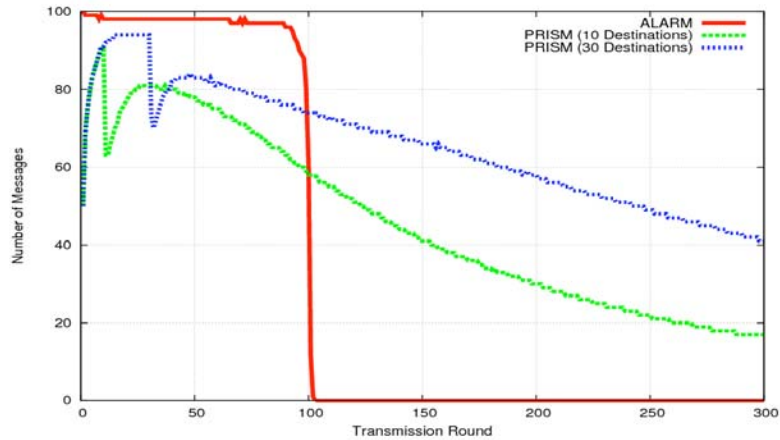
- Two mobility models
- DST-AREA radius = 20m
- Area = 1000m²
- Tx-Range=150m
- Num Nodes= 1000
- Parameters to ensure 90% connectivity in network in RWM (but only 50% in RPGM)
- 50 sending sources



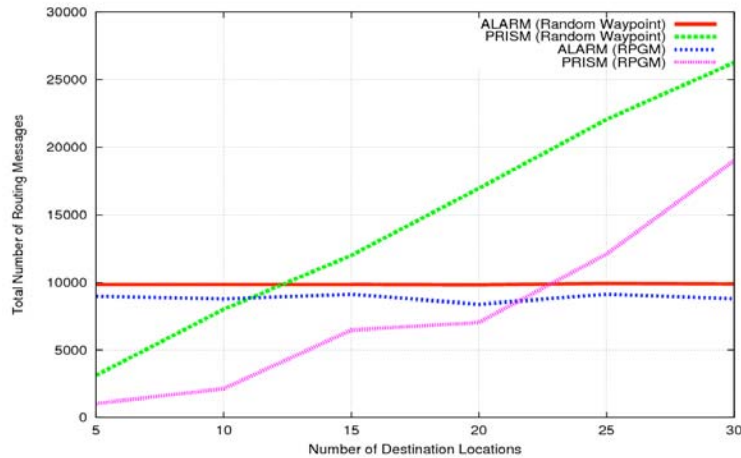
Details of Routing Messages vs Time (RPGM)



Routing Messages / Time (Random Waypoint)



Total Number of Routing Messages



52

Related Work

- ◆ SPAAR and AO2P require on-line location servers.
- ◆ ASR and ARM assume that each authorized source-destination pair pre-shares a unique symmetric key.
- ◆ ASRP assumes that each source-destination pair shares some secret information, e.g., the public key of the destination or a symmetric key.
- ◆ ANODR assumes that the source shares some secret with the destination for the construction of a trapdoor, e.g., the destination's TESLA key.
- ◆ SDAR assumes that the source knows the public key of the destination, obtained from a CA
- ◆ ODAR requires an on-line public key distribution server.
- ◆ MASK and D-ANODR contain the destination in the clear in each RREQ message.

9/20/10

53

Future Work

- One time certificates instead of GSIG (scalability issues)
- Prevent active insiders based on location information and directions of RREQ
- Accommodate heterogeneous MANET devices (i.e. no GPS and GSIG capability)
- Evaluation with real mobility traces

54

Conclusions

- Use of location-centric, instead of identity-centric, communication paradigm
 - No long-term node identifiers, shared or public keys
 - No on-line servers (TTPs) of any kind
- Example of advanced crypto tools at work... 😊
- Much more work needed

End

Questions?
Comments?
Complaints?