PRISM: Privacy–friendly Routing in Suspicious MANETs (and VANETs)

Karim El Defrawy and Gene Tsudik
Outline

- Introduction
- Privacy and Security in MANETs
- Related Work
  - Overview of Group Signatures
- PRISM
  - Protocol and Operation
  - Security Analysis and Simulations
- Future Work and Conclusion
Mobile Ad-Hoc Networks (MANETs)

- Infrastructure-less
- Mobile
- Multitude of devices and capabilities
- May be deployed in **extreme settings** (e.g. military, search and rescue)
“Suspicious” MANETs

- Environment is “hostile” and “suspicious”
  - Military/battlefield: infantry, naval– and air–craft
  - Law enforcement: sting operations, attack/disaster aftermath
Vehicular Ad-Hoc Networks (VANETs)

- Special type of MANETs
- Restricted mobility (highways and roads)
- High speeds
- Privacy is a must
Privacy in MANETs

Goal:
- Tracking resistance ➔ no exposure of long-term IDs
- Escrowed Anonymity ➔ only certain authorized entities (e.g. law enforcement) can learn long-term ID

Challenges:
- How to authenticate if no long-term ID?
- How to achieve integrity, accountability in case of misbehavior?
- Malicious insiders become harder to combat
Security in MANETs

Typical security requirements:

- Confidentiality
- Integrity
- Authentication
- Accountability and non-repudiation

Main difficulty when coupled with privacy requirements
Related Work

- Secure on-demand routing protocols: Ariadne, SRDP, SEAD, EndairA, SRP... (no privacy)

- Privacy preserving on demand protocols: ANODR, MASK, D-ANODR, ARM, ODAR...
  - All use identity-centric communication
  - All require either:
    - Long Term ID or pseudonyms
    - Source shares information/keys with destination (ASR, ARM, ASRP, ANODR)
    - Source knows public key of destination (SDAR)
    - Online location/certificate servers (SPAAR, AO2P, ODAR)
  - Not location based
Related Work (Other)

- ALARM (ICNP’07) – privacy-preserving link state-based (proactive) routing protocol
  - Optimized Link State Routing (OLSR) is closest to ALARM but without privacy and security

- Location-aided forwarding scheme (e.g., LAR, GeoGrid … etc)
Our Contributions

- Location-centric communication instead of identity-centric more suitable in certain MANETs (VANETs) settings.

- Location-centric communication more privacy-friendly

- Group signatures used to construct privacy-preserving and secure on-demand MANETs routing protocol (PRISM)

- PRISM is based on AODV
Any member of a potentially large and dynamic group can sign a message (produce a GSIG)

GSIG can be verified by anyone who has a constant-length group public key

Valid signature $\implies$ signer is a group member

Given two GSIGs, it is *computationally infeasible* to determine if produced by same member

In the event of a dispute, a GSIG can be opened by off-line authority to reveal actual signer
GSIG Scheme Components (1)

- **SETUP**: an algorithm run by GM:
  - *input*: security parameter $k$
  - *output*: cryptographic specification of group, GM public key ($pk_{GM}$) and private keys ($sk_{GM}$)

- **JOIN**: a protocol between GM and user resulting in user becoming a member ($U$) and having a public/private key ($pk_{U}, sk_{U}$).

- **SIGN**: an algorithm executed by a group member:
  - *input*: message ($m$), group public key ($pk_{GM}$), member public/private key ($pk_{U}, sk_{U}$)
  - *output*: GSIG = $\delta$ of $m$
GSIG Scheme Components (2)

- **VERIFY**: an algorithm run by anyone:
  - *input*: message ($m$), GSIG ($\delta$), group public key ($pk_{GM}$)
  - *output*: binary flag indicating validity of GSIG

- **OPEN**: an algorithm run by the GM:
  - *input*: message ($m$), GSIG ($\delta$), group public key ($pk_{GM}$), GM secret key ($sk_{GM}$)
  - *output*: validity of signature, identity of signer ($pk_U$), a proof that allows anyone to verify identity of signer

- **REVOKE**: an algorithm run by GM to remove (revoke a user from the group)
GSIG Participants

- **Group Manager (GM):** entity responsible for administering the group. Has private key and group public key.

- **Group Members:** users/entities that represent the current set of authorized signers. Each has a public/private key and the group public key.

- **Outsiders:** any other user/entity external to group. Has group public key.
Assumptions

- **[LOCATION]** nodes can obtain location info (e.g., GPS)

- **[PRIVACY]** no long-term public node ID or address

- **[MOBILITY]** network is mobile but nodes are loosely synchronized (e.g., using GPS)

- **[SECURITY]**
  - Outside attackers
  - Passive (honest—but—curious) insiders
PRISM Operation

1. GM sets up the GSIG scheme

2. Nodes join the group with GM and generate keys and get the group public key

3. MANET deployment
PRISM Operation

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

SRC sends a route request (RREQ):

\[ <\text{DST-AREA}, \text{PK}_{\text{TMP}}, \text{TS}_{\text{SRC}}, \text{GSIG}_{\text{SRC}} > \]

- DST-AREA=Destination Area
- \( \text{PK}_{\text{TMP}} \)= temporary public key generated by source
- \( \text{TS}_{\text{SRC}} \)= current time stamp
- \( \text{GSIG}_{\text{SRC}} \)= Group signature over previous fields
PRISM Operation

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

SRC sends a route request (RREQ):

\(<\text{DST-AREA}, \text{PK}_{\text{TMP}}, \text{TS}_{\text{SRC}}, \text{GSIG}_{\text{SRC}}>\)

- DST-AREA = Destination Area
- \(\text{PK}_{\text{TMP}}\) = temporary public key generated by source
- \(\text{TS}_{\text{SRC}}\) = current time stamp
- \(\text{GSIG}_{\text{SRC}}\) = Group signature over previous fields
PRISM Operation

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

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

- DST-AREA = Destination Area
- \(\text{PK}_{\text{TMP}}\) = temporary public key generated by source
- \(\text{TS}_{\text{SRC}}\) = current time stamp
- \(\text{GSIG}_{\text{SRC}}\) = Group signature over previous fields
PRISM Operation

DST sends a route reply (RREP): 
<h(RREQ), Enc_{PK_{tmp}}(K_s, DST_{Loc}), GSIG_{DST}>

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):
\(<h(RREQ), Enc_{PK_{tmp}}(K_s, DST_{Loc}), GSIG_{DST}>\)

- \(h(RREQ)\) = 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
DST sends a route reply (RREP):

\[ <h(RREQ), Enc_{PK_{tmp}}(K_s, DST_{Loc}), GSIG_{DST}> \]

- \( h(RREQ) = \) 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
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.
PRISM Security Analysis (1)

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

- Eavesdrops to track peer nodes
  - Can't link multiple messages to same node (computationally infeasible to link GSIGs)
  - Can track node movement by monitoring likely trajectories (but need lots of topology knowledge)
  - Sees less topology than in link-state protocols (simulation)
PRISM Security Analysis (3)

- Active Insiders:
  - PRISM is 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
PRISM Topology Exposure

- Two mobility models:
  - RWM (Random Waypoint)
  - RPGM (Reference Point Group Mobility)
- DST–AREA radius = 20m
- Area = 1000m²
- Tx–Range=150m
- Num Nodes = 1000
- 50 sending sources
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
Total Number of Routing Messages

![Graph showing the total number of routing messages for different protocols (ALARM, PRISM) as a function of the number of destination locations. The graph displays lines for ALARM (Random Waypoint), PRISM (Random Waypoint), ALARM (RPGM), and PRISM (RPGM).]
Conclusion

- Location-centric communication is more privacy friendly

- Group signatures are a promising building block for privacy-preserving secure protocols

- Several research problems remain
Thank you!

http://www.ics.uci.edu/~keldefra