Secure Communication Protocols: State of the art

Zhendong Ma
zhendong.ma@uni-ulm.de

Outline

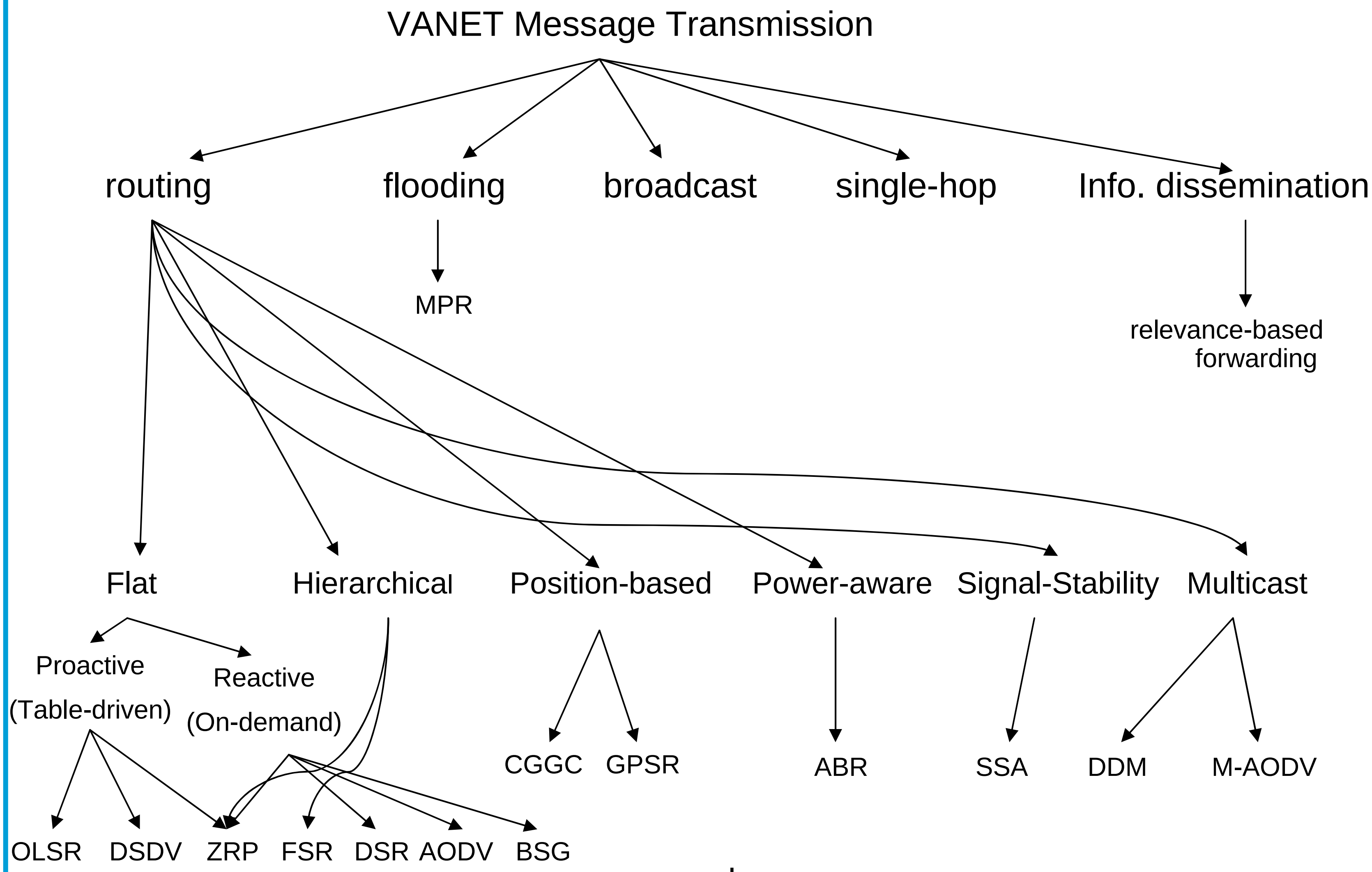
- Communications in VANET
- Unsecure routing protocols
- Dangers to VANET communications
- Secure routing protocols in ad hoc networks
- Secure routing using position information
- Problems, open questions

Secure Communication?

- Message Transmission Protocols
  - Routing
  - Flooding
  - Broadcast
  - Single-Hop Unicast
  - Information Dissemination
- Authentication Protocols
- Integrity Protection
- Key Exchange Protocols
- …

Focus for this talk

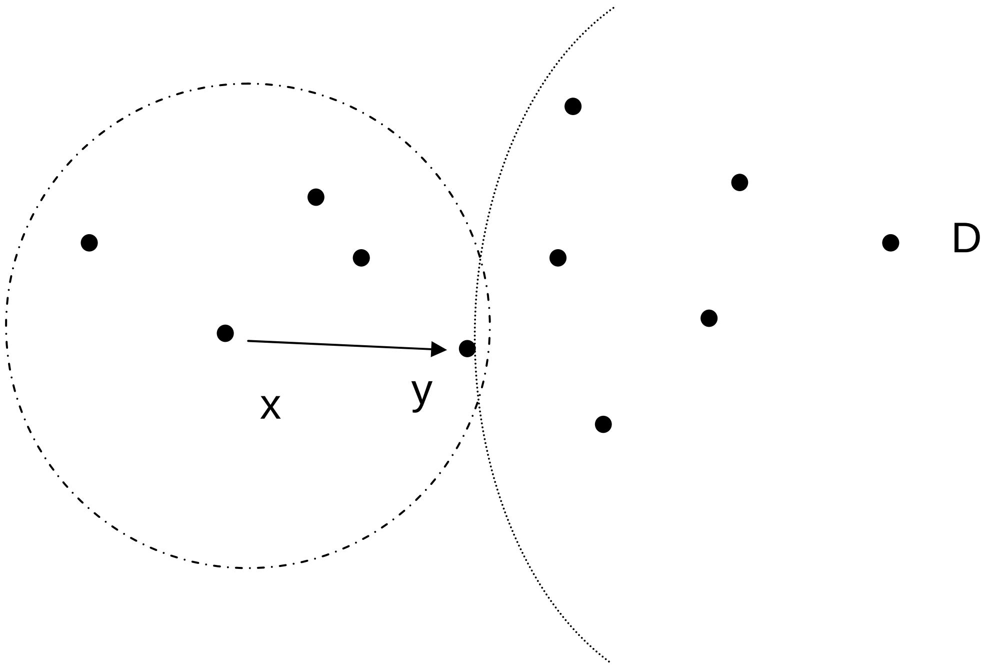
Communications in VANET



and many more…

Greedy forwarding

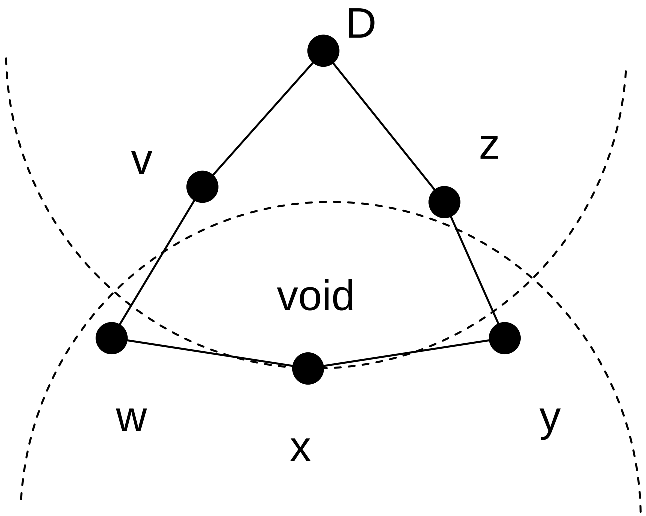
Node forward message to the neighbor, whose position is closer to the destination than itself



Greedy forwarding

(x->y->z->D) or (x->w->v->D)

Greedy forwarding fail



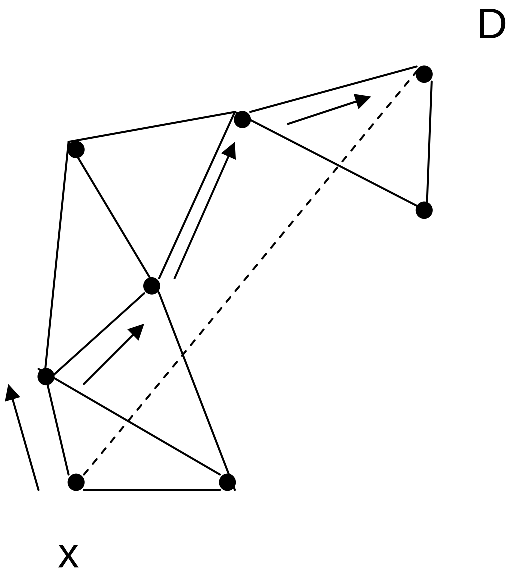
Greedy Perimeter Stateless Routing

- Position-based unicast routing protocol
- Greedy forwarding if node knows its one-hop neighbors’ position is closer to destination
- Perimeter forwarding if there is no one-hop neighbor closer to destination

Greedy Perimeter Stateless Routing

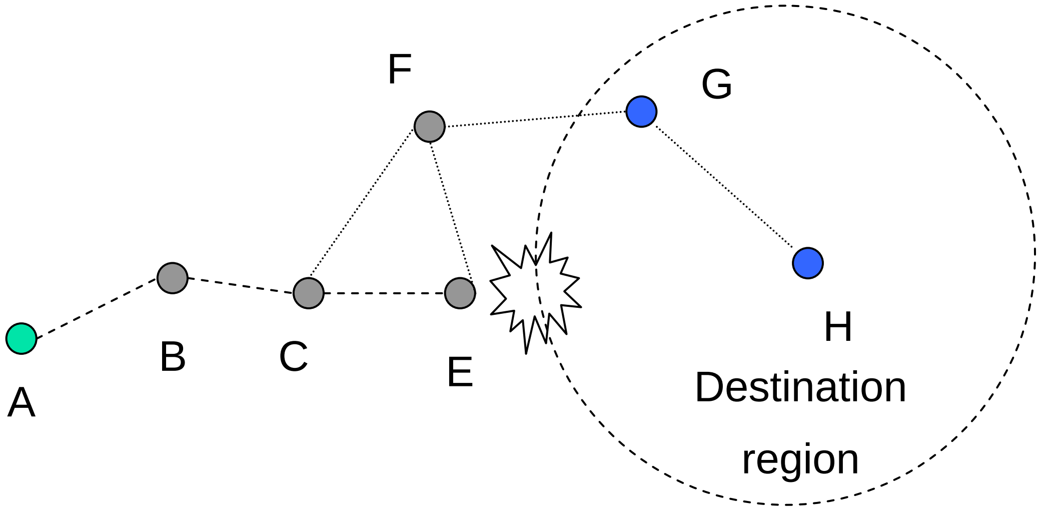
When a packet reaches a region where greedy forwarding is impossible

-> Perimeter forwarding: route the packet around the perimeter of the region according to right-hand rule



Cached Greedy GeoCast

- Designed for use in ad hoc networks with high velocities
- Add cache at the routing layer when instant forwarding is impossible due to local maximum
- Use beaconing system that allows constant neighbor awareness
- Cache check if message can be forwarded to a newly discovered neighbor

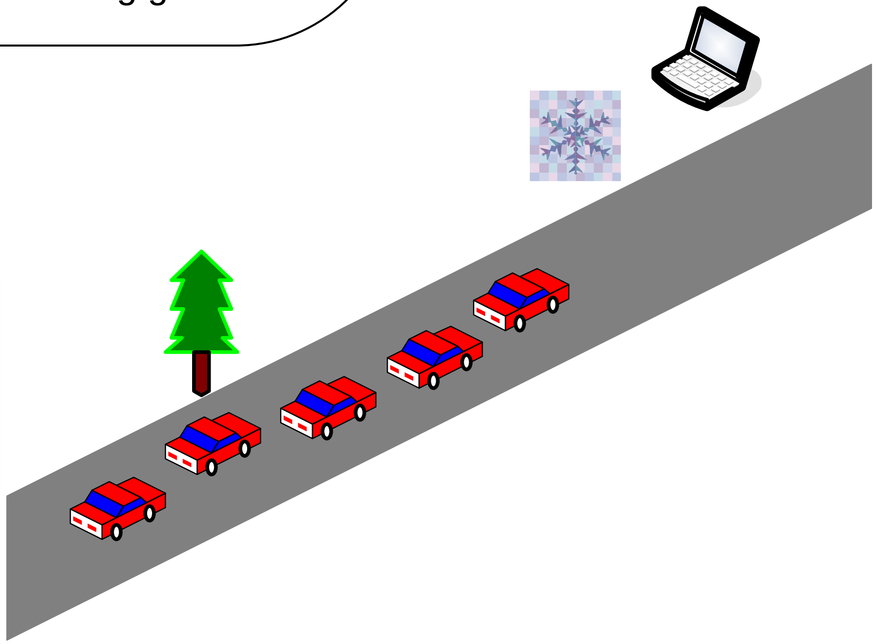


Attacks on VANET

- Cheating with position / speed / identity
- Masquerade
- Message suppression
- Disruption of network operation
- Identity disclosure
- Bogus information / alteration

Forging of Warning Message

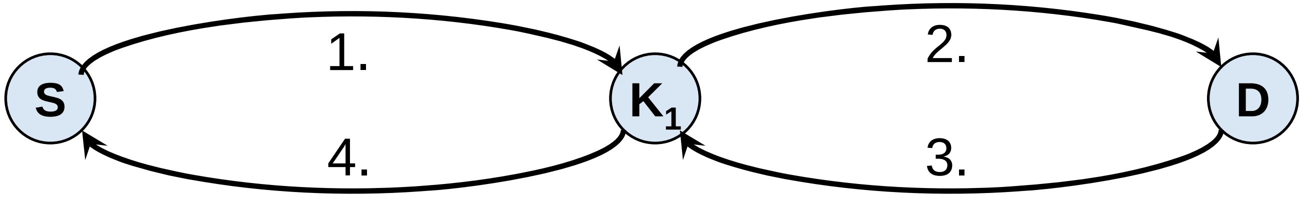
Vehicle-based road condition warning
This in-vehicle application will detect marginal road conditions using on-board systems and sensors (e.g. stability control, ABS), and transmit a road condition warning to approaching vehicles using geocast..



Secure Dynamic Source Routing

- Routing Protocol, that prevents manipulation of routing information
- Security Goals:
  - Ensures integrity of source route
  - Ensures freshness of source route
  - Authenticates all participating nodes
  - Exchange of secret session keys between all participating nodes
- Properties
  - Based on DSR
  - Small overhead

SDSR route discovery



1. *RREQ* | S | D | *ID* | *DHPK$_S$* | *N$_1$* | *SR* {S} | sig$_{SKS}$

2. *RREQ* | S | D | *ID* | *DHPK$_S$* | *N$_2$* | *SR* {S,K$_1$} | sig$_{SKS}$

3. *RREP* | S | D | *ID* | *DHPK$_S$* | *N$_2$* | *SR* {S,K$_1$,D} | sig$_{SKS}$ | sig$_{SKD}$

DHPK$_D$ | *E$_{SKD}$(h(k$_{SD}$))*

4. *RREP* | S | D | *ID* | *DHPK$_S$* | *N$_1$* | *SR* {S,K$_1$,D} | sig$_{SKS}$ | sig$_{SKD}$

DHPK$_D$ | *E$_{SKD}$(h(k$_{SD}$))* | *DHPK$_1$* | *E$_{SK1}$(h(k$_{S1}$))*

[illegible] nodes:

- [illegible]

- [illegible]), K$_1$/S resp.

Secure Dynamic Source Routing

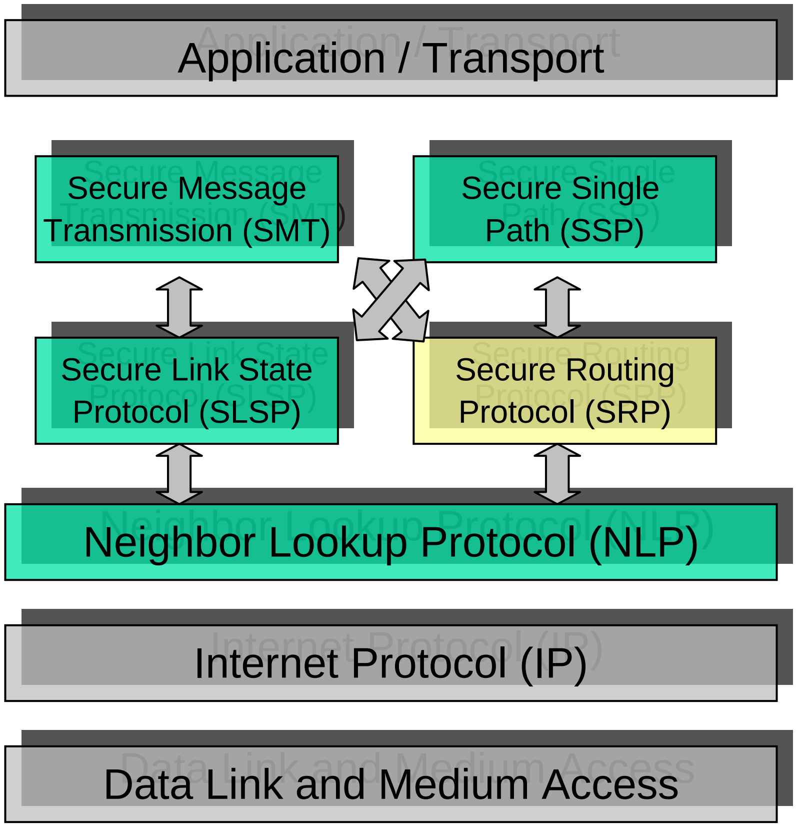
- Additional components:
  - Bidirectional key agreement
  - Distribution of public keys and certificates
  - Route Maintenance
- Optimization:
  - Piggybacking
  - Route Request Unicasting
  - Reuse of session keys

Secure Routing Protocol

Secure communication protocol suite

Secure transmission

Secure route discovery



Application / Transport

Secure Message Transmission (SMT)

Secure Single Path (SSP)

Secure Link State Protocol (SLSP)

Secure Routing Protocol (SRP)

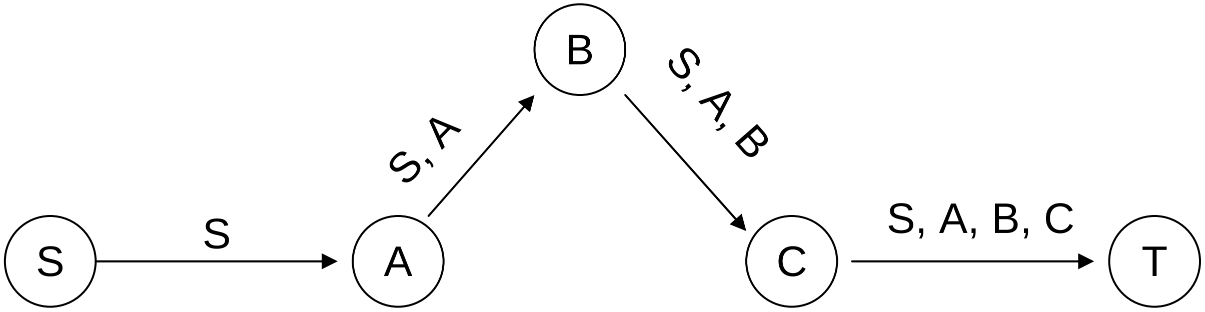
Neighbor Lookup Protocol (NLP)

Internet Protocol (IP)

Data Link and Medium Access

SRP route request

- SRP requires a security association between source node S and destination node T



SRP Header

Type	reserved	Q_{ID}	Q_{seq}	SRP MAC

Q_{ID} S generates 32-bit random number, for intermediate nodes as a means to identify the request

Q_{seq} increase for each destination

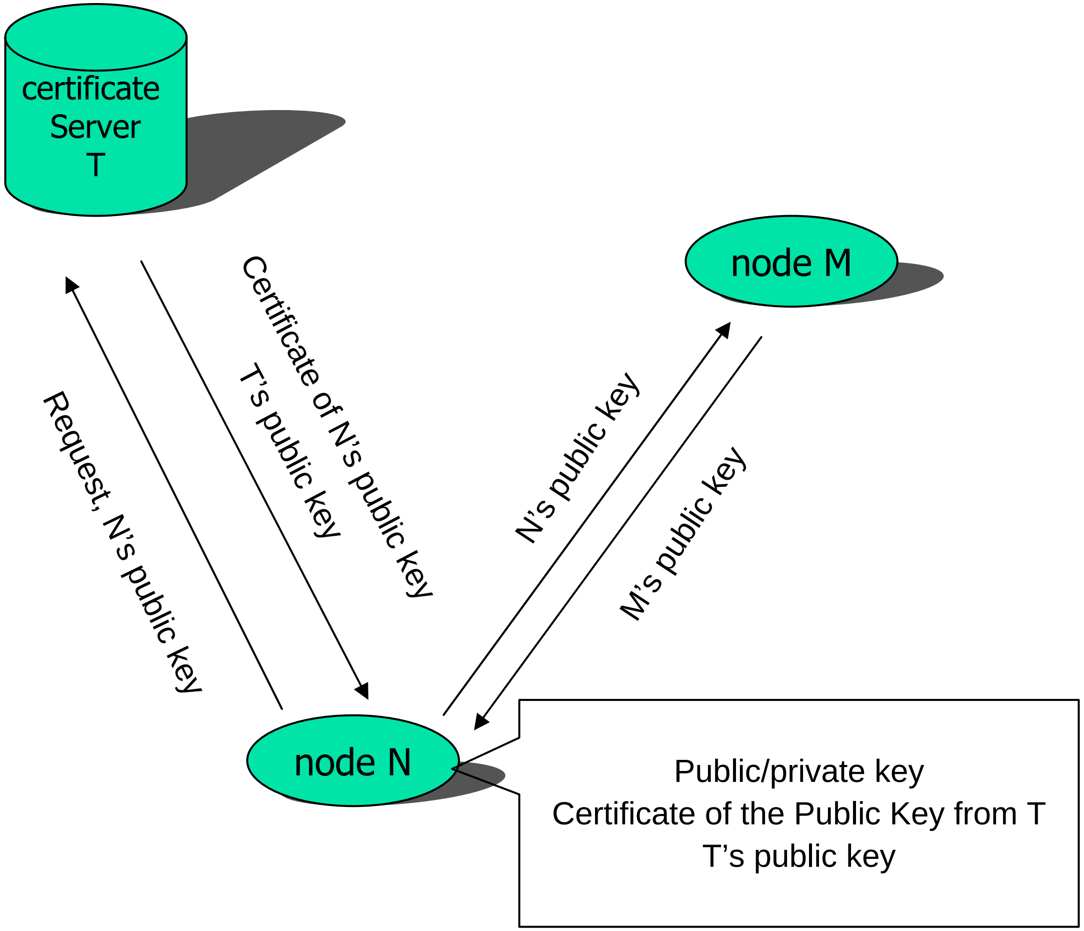
SRP MAC generated by one-way hash function over IP header, the basic route request packet, and shared key

SPAAR

- Secure Position Aided Ad hoc Routing
  - Use position information to improve performance and security
  - Node must know the approximate geographic location of the destination
  - Nodes only accept messages from one-hop neighbors
- Use asymmetric cryptography, message signed with node’s private key and encrypted with neighbor’s public key

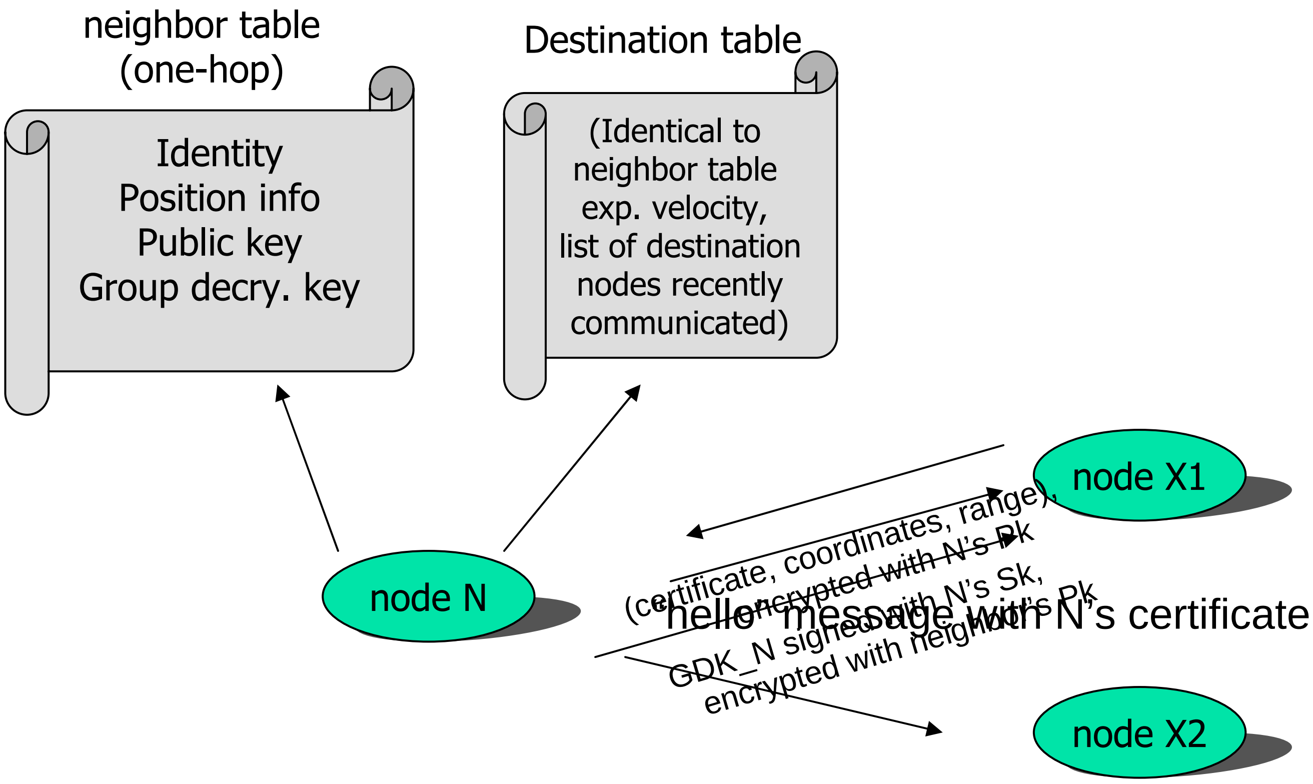
SPAAR

Setup phase



Public/private key
Certificate of the Public Key from T
T's public key

SPAAR



neighbor table (one-hop)

Identity
Position info
Public key
Group decry. key

Destination table

(Identical to neighbor table exp. velocity, list of destination nodes recently communicated)

node N

node X1

node X2

“hello” message with N’s certificate

(certificate, coordinates, range), encrypted with N’s Pk

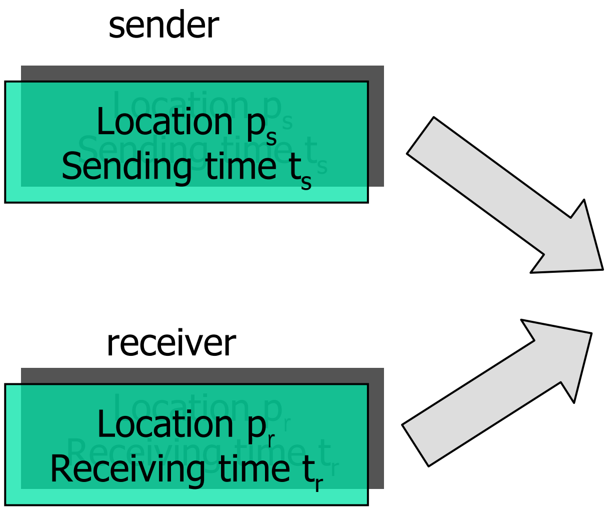
GDK_N signed with N’s Sk, encrypted with neighbor’s Pk

SPAAR

- Asymmetric cryptograph on both end-to-end and hop-to-hop communications
- Adaptation to topology changes depends on interval of hello messages
- Geographic routing reduce overhead

Packet leash

- Mechanism for defending against wormhole attack
  - A leash is any information added to a packet to restrict the packet’s maximum transmission distance
  - Needs time and location information



sender

Location p_s
Sending time t_s

receiver

Location p_r
Receiving time t_r

Upper bound distance

$$d_{sr} \leq ||p_s - p_r|| + 2\nu \cdot (t_r - t_s + \Delta) + \delta.$$

V: upper bound on node velocity

Δ: Synchronization jitter

δ: Maximum relative error in location info

IEEE802.11i

- Security mechanisms for IEEE 802.11, provide confidentiality, data origin authenticity, integrity, replay protection
- Designed basically for an infrastructure WLAN
- Does not address
  - Multi-hopping
  - Routing mechanisms
  - Broadcast / Multicast
  - Privacy protection
- But may be used as a first inspiration

Conclusion

- Lots of research on routing in ad hoc networks, but not enough on other VANET message transmission methods
- Many works on secure topology-based routing, but not enough on secure position-based routing
- Difficult to design secure routing/communication protocols for VANET without concrete application security requirements

Questions?