ulm university universität uulm

Secure Routing for Vehicular Networks

SEVECOM Kickoff Workshop • 2nd February 2006

Frank Kargl • frank.kargl@uni-ulm.de

Outline

- Routing in MANETs
- Secure Routing in MANETs
- Secure Routing in VANETs
- Security Requirements in VANETs
- Architectural Proposal

Routing

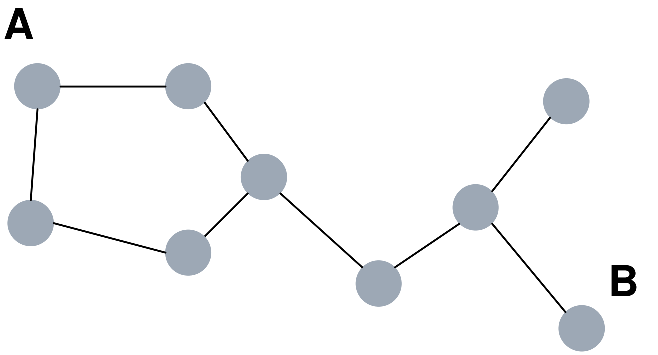
Shortest Path Problem:

In a weighted graph *G=(N, E)* with $E=\{e_1 \ldots e_n\}$ and respective edge weights $g_1 \ldots g_n$ find the shortest path $P \varepsilon N$ from *A* to *B* (*A,B* e *G*) with minimal path cost C_{AB}

$$C_{AB} = \sum_i g_i \forall i \mid k_i \in P$$

Traditional Routing-Algorithms

- Distance Vector (Bellman-Ford)
  e.g. Routing Information Protocol
  (RIP, RFC 1387-1389)
- Link State (Dijkstra SPF)
  e.g. Open Shortest Path First
  (OSPF, RFC 2328)
- Policy-based Routing
  e.g. Border Gateway Protocol
  (BGP, RFC 1771)



MANET Routing

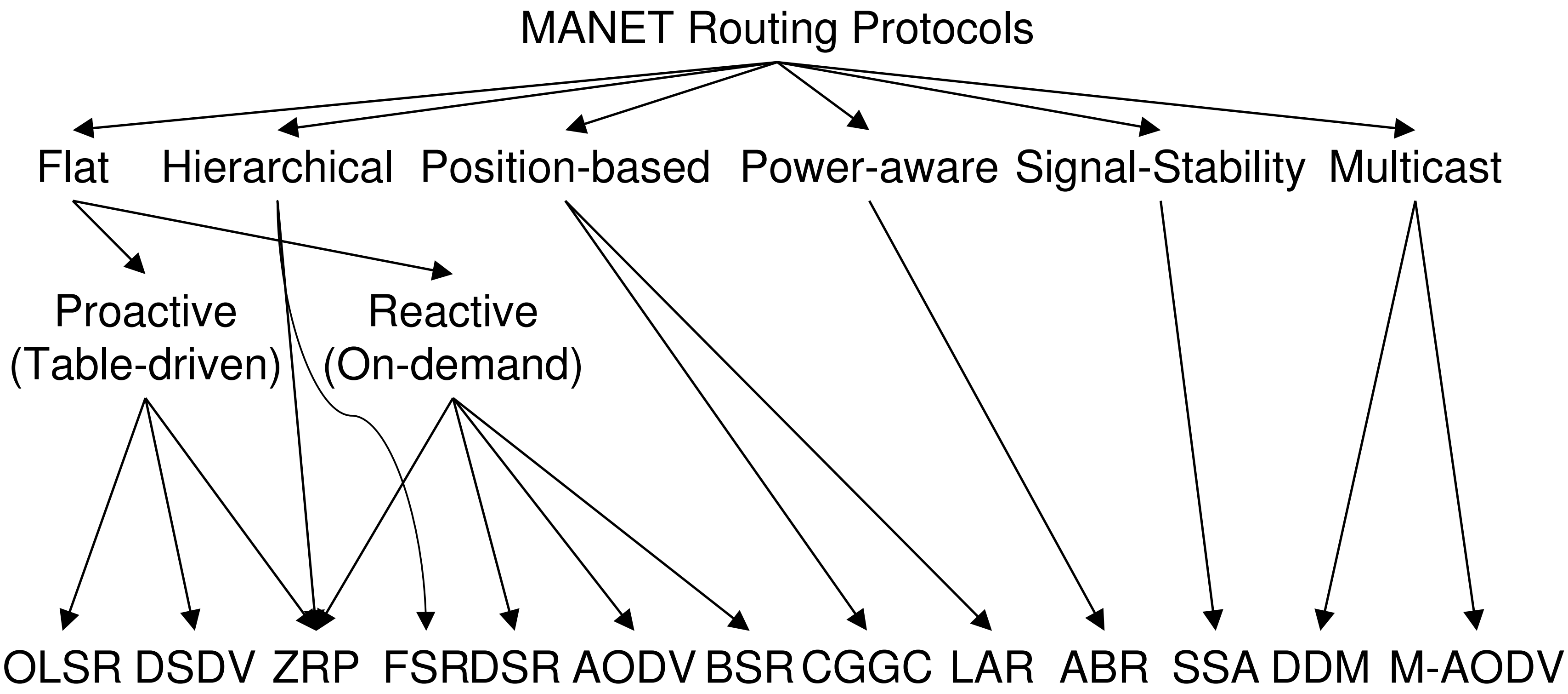
Traditional Routing Protocols
- do not converge fast enough
- are not energy efficient

MANET Properties
- Rapidly changing topology
- Small bandwidth
- Small resources (processor/memory/battery)

Military Applications > 30 years (PRNET 1973)

Since 1997 IETF WG MANET
- RFC 2501:
  Routing Protocol Issues and Evaluation Considerations
- RFCs for different routing protocols
  - AODV (RFC 3561)
  - OLSR (RFC 3626)
  - TBRPF (RFC 3684)
- Drafts
  - Dynamic Source Routing (DSR)
  - Dynamic MANET On-demand (DYMO) Routing

Different Classes of Protocols



MANET Routing Protocols

Flat Hierarchical Position-based Power-aware Signal-Stability Multicast

Proactive (Table-driven)

Reactive (On-demand)

OLSR DSDV ZRP FSR DSR AODV BSR CGGC LAR ABR SSA DDM M-AODV

and many more ...

Secure Routing in MANETs

Potential Requirements

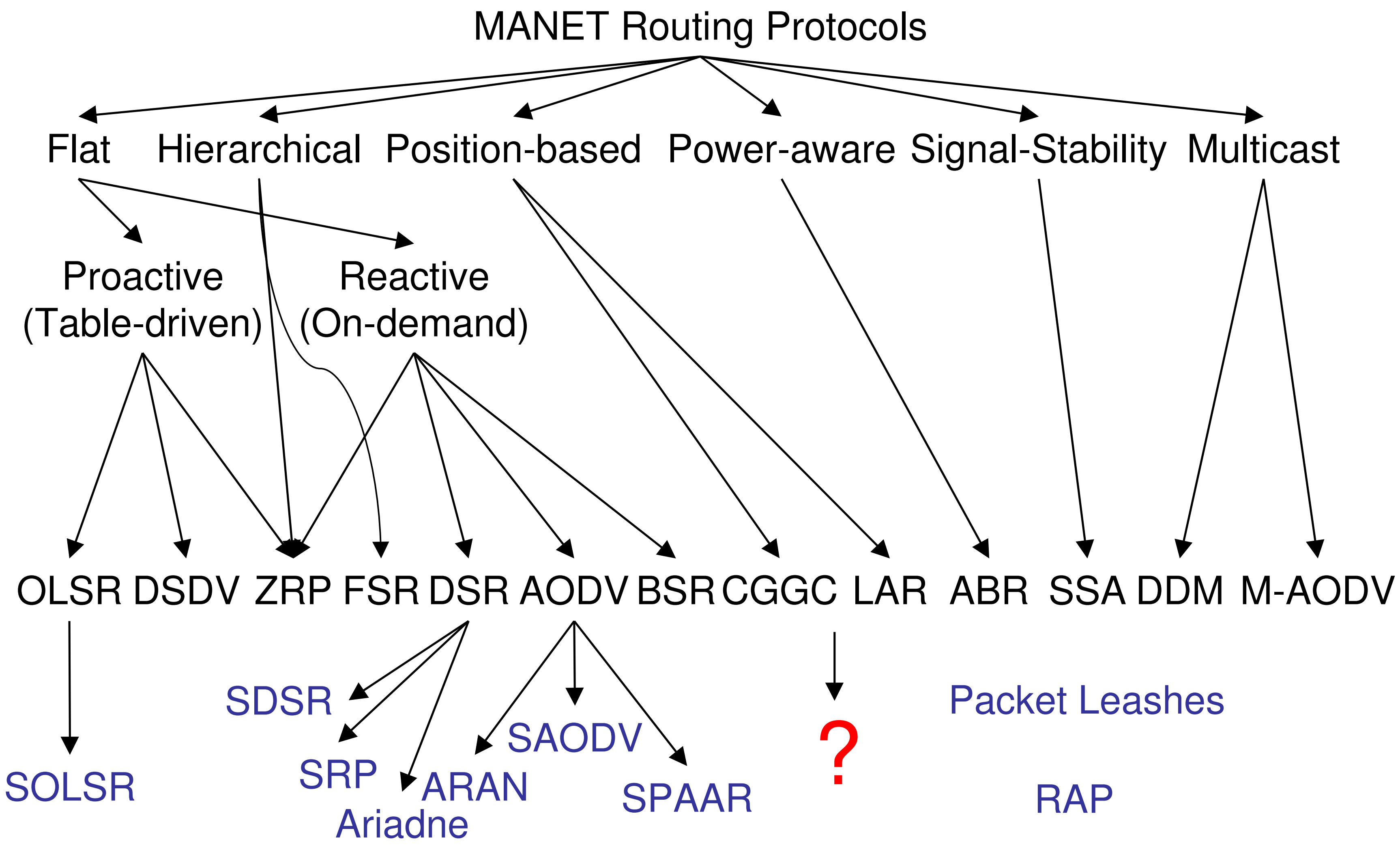
- Confidentiality
- Authenticity
- Integrity
- Availability
- Accountability / Non-Repudiation
- Access Control
- Privacy

Typical Attacks on MANET Routing

Attack Goals

- Selfish Behavior
  - don’t participate in routing
  - don’t relay data
- DoS
  - Blackhole Routing
  - Destroy Topology
  - Flooding / Overloading
- Information Access
  - Blackhole Routing (don’t drop packets)
  - Wormhole Attack
  - Rushing Attack
- Modification
  - Blackhole Routing (modify packets)
  - Wormhole Attack
  - Rushing Attack
- Privacy Attacks
  - Location Tracking
  - Communication profiling

Secure Routing Protocols for MANETs



Secure MANET Routing

Function	SAODV	Ariadne	ARAN	SRP (old)	SDSR
Key distribution	assumed	assumed	integrated	assumed	integrated
Node authentic.	endpoints	all	all	endpoints	all
Secure RREQ	yes (can extend)	yes	yes (can extend)	no	yes
Secure RREP	yes	yes	yes	yes	yes
Guarantee freshn.	yes	yes	yes	yes	yes
Exch. sessionkeys	no	no	no	no	yes
Use cached routes	yes	no	no	no	no
Performance	□	O	□	□□	O
Assumptions	none	sync. clocks	sync. clocks	none	none

Secure Routing in VANETs

- Position-based Routing
  - Not topology-based / neither proactive nor reactive
- Potential attack vectors on position-based routing?
  - Forged Positions (blackhole / selfish)
  - Multiple Identities / Sybil-Attack (blackhole / selfish)
  - Drop packets (selfish / DoS)
  - Overload neighbor caches (DoS)
  - Eavesdrop
  - Modify data

Security Requirements in VANETs

App.	Confid.	Authent.	Integrity	Avail.	Non-Rep.	Acc. Con.	Privacy
Intersec. Coll. Warn.		?	X	?	?		X
Autom. Lane Merging		?	X	X	?		X
Emerg. Vehicle Warn.		X	X	X	?	?	
Road Work Warn.		X	X			?	
Car-2-Car Messag.	X	X	X			?	?

C2C eSafety

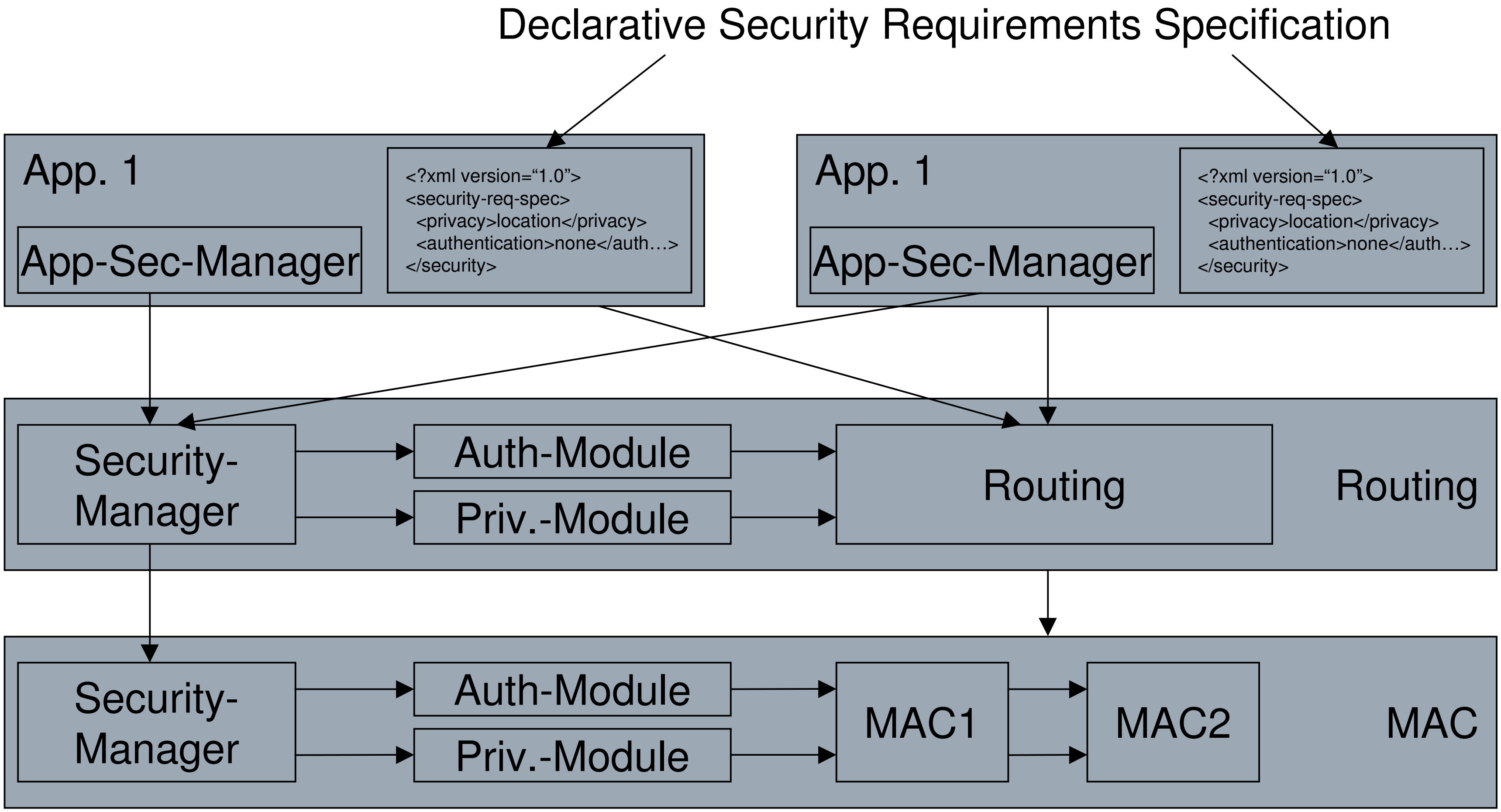
C2I eS

C2C Ent.

Conclusions

- No security solution fits all application requirements
- Even contradicting requirements between multiple concurrent applications
  - Lane Merging Application: needs location of other cars
  - C2C Messaging: needs identities of other cars
- Solution
  - Application declare their security requirements
  - Security modules on each level are configured according to the specifications (Application, Routing, MAC)
  - Merging of requirements
  - Contradicting requirements resolved via priorities (crash warning > C2C messaging)

Architectural Proposal



```
<?xml version="1.0">
<security-req-spec>
  <privacy>location</privacy>
  <authentication>none</auth…>
</security>
```

```
<?xml version="1.0">
<security-req-spec>
  <privacy>location</privacy>
  <authentication>none</auth…>
</security>
```

Next steps

- Decide on routing / communication protocols in associated projects
- Analyze potential applications and their requirements
- Analyze / categorize security / privacy hazards
- Architecture
  - Design / choose
    Security Requirements Declaration Language (SRDL)
  - Decide on modules on routing / MAC layer
- Solve individual problems
  - Authentication
  - Secure Beaconing / Position Verification
  - Confidentiality/Integrity
  - Availability / DoS-Protection (IDS?)
- Relationships between areas!!!
  - Authentication ↔ Confidentiality
  - Changing MACs ↔ Routing Efficiency

The End

Comments & Discussion