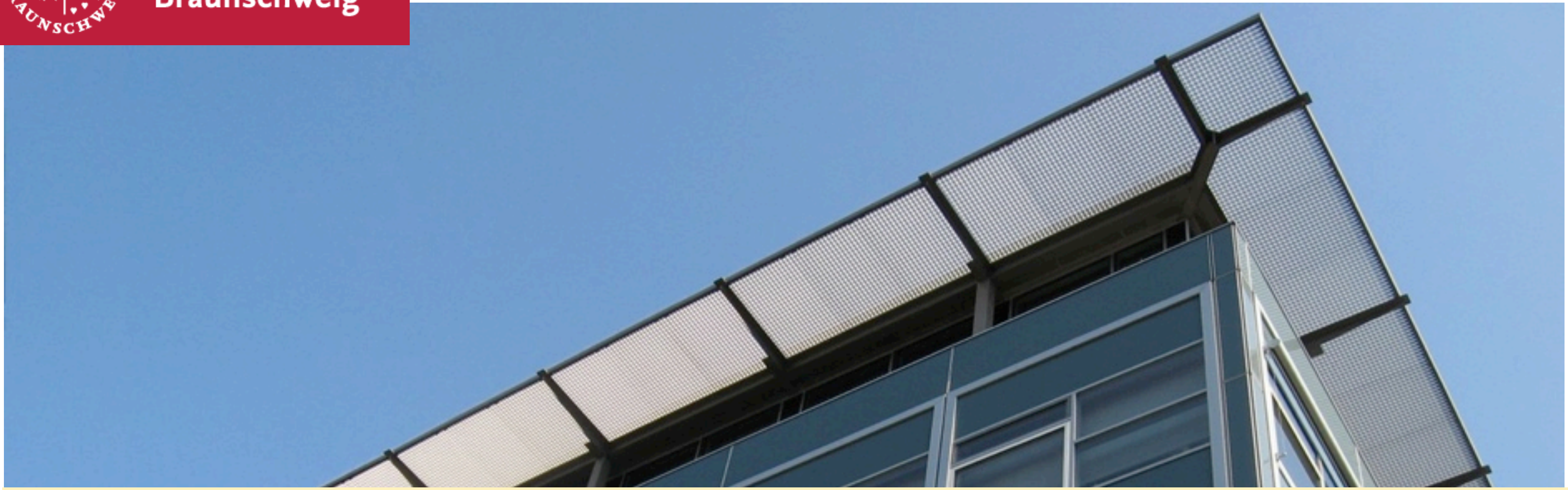
Technische Universität Braunschweig

Institute of Operating Systems and Computer Networks

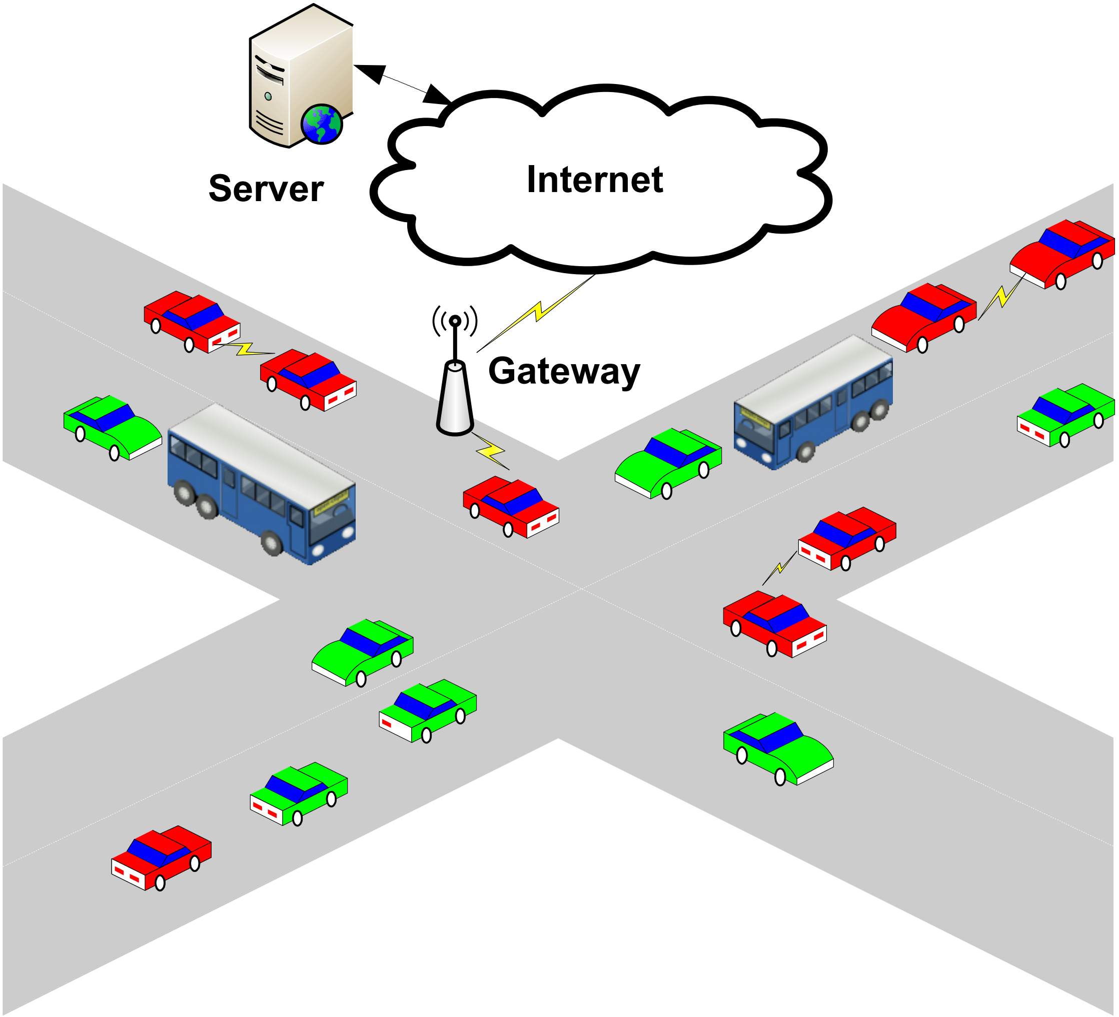


Detecting Blackhole and Greyhole Attacks in Vehicular Delay Tolerant Networks

Yinghui Guo, Sebastian Schildt and Lars Wolf

COMSNETS 2013, Bangalore

Vehicular Delay Tolerant Networks (VDTNs)



Only small penetration for first deployments

Backend/Internet Connection not always available

Centralistic backend based approach not suitable for all applications

🟥 VANET/VDTN enabled vehicle

🟩 legacy vehicle

Why Misbehavior Detection?

Open systems

- Future VANET Vision: Ubiquitous deployment of VANET/VDTN capable systems from different vendors
- Can not centralize security infrastructure

Big attack surface (even for closed systems)

- Proposed systems mostly realized using widely available commodity hard- and software
  - WiFi Technology
  - Off-the-shelf operating systems and hardware platforms

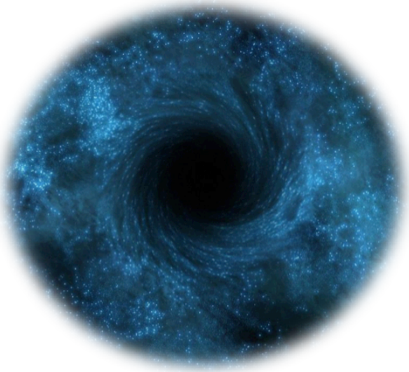
Misbehaviors can be the result of attacks or caused by hard- or software errors

Blackhole and Grayhole Attacks

A greyhole attacker drops a certain percentage of all messages it should send (Blackhole: 100%)

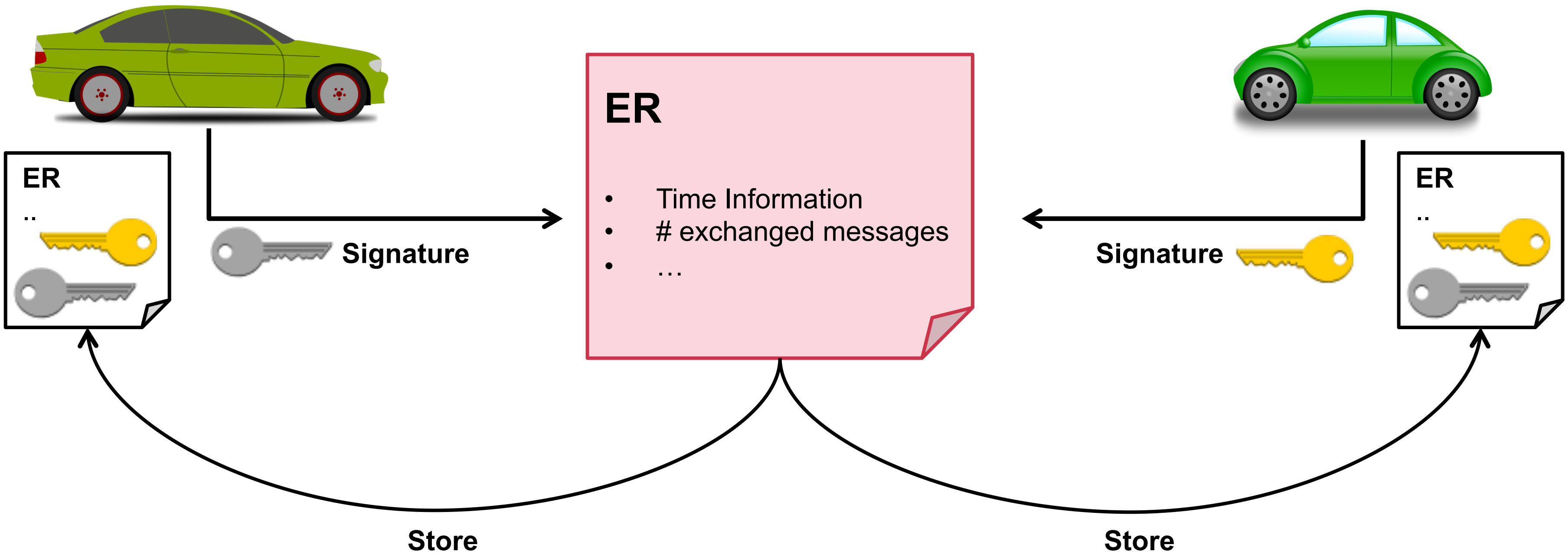
- A baseline attack to disrupt the network
- Hard- or software errors often manifest themselves in lost messages
- Can also be a symptom of more complex attack schemes such as certain attacks on the employed routing scheme

A good general property to measure network health



Encounter Records

Our system is based on Encounter Records*



* F. Li, J. Wu, and A. Srinivasan. Thwarting blackhole attacks in disruption-tolerant networks using encounter tickets. In INFOCOM 2009, IEEE, pages 2428–2436, Rio de Janeiro, Brazil, Apr. 2009.

Exchanged Encounter Records (ERs)

$$ER_i = ID_i, ID_j, sn_i, sn_j, t, Re_{i\rightarrow j}, Re_{j\rightarrow i}$$

$$Re_{i\rightarrow j} = \{(msg_{id}, msg_{src} | i \quad send \quad msg \quad to \quad j)\}$$

$$Re_{j\rightarrow i} = \{(msg_{id}, msg_{src} | j \quad send \quad msg \quad to \quad i)\}$$

$$sig_i = E_{RK_i}\{H(ER_i)\}$$

$$sig_j = E_{RK_j}\{H(ER_i)\}$$

$$ER_i^* = ER_i, sig_i, sig_j$$

Rules

- Consistency of sequence numbers and timestamps
  - $s_{n1} < s_{n2}$ implies $t_1 < t_2$
  - Last known valid s/t combination for a node stored in the Meeting List (ML)
  - If a node violates constraints it is put into the blacklist immediately

- Ratios regarding sent and received messages
  - Reputation System: Good behavior will be encouraged
  - Bad behavior leads to lower trust levels and ultimately to (temporary) inclusion into the blacklist

Ratios

Upon contact nodes exchange up to *w* of their newest Ers

Violations of thresholds lead to decreased trust level, compliance to the rules increases trust.

$$\theta = \frac{\sum_{m=0}^{m<w} N_{send}^{ER_m}}{\sum_{m=0}^{m<w} N_{recv}^{ER_m}}$$

Amount of send messages compared to received messages

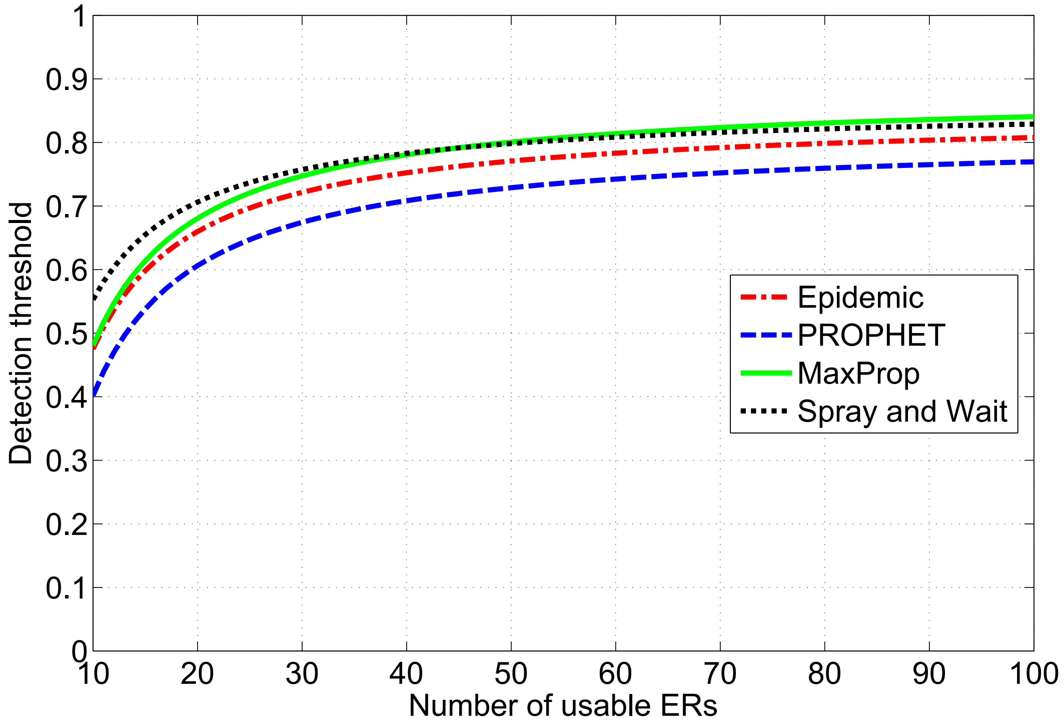
$$\psi = \frac{\sum_{m=0}^{m<w} N_{send}^{jER_m}}{\sum_{m=0}^{m<w} N_{send}^{ER_m}}$$

Sent messages, which are generated by a node itself, compared to sent messages generated by a third party

Detection Thresholds

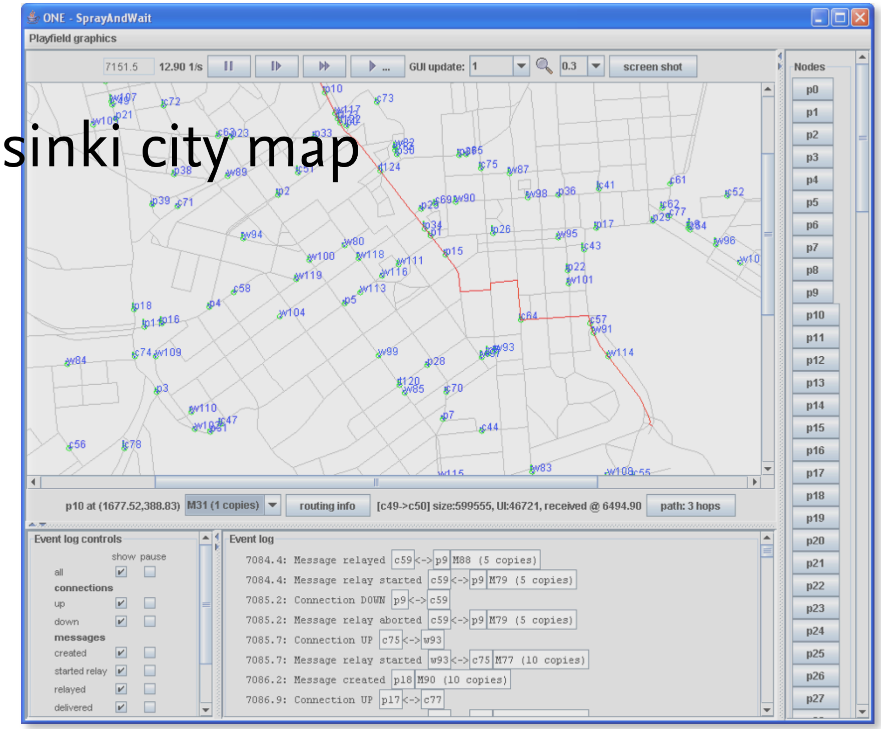
Strict thresholds when more ERs are available increase detection rate

Relaxed thresholds when little information is available decrease false positives



Simulations

- Used The ONE DTN simulator
- Routing: Epidemic, Spray and Wait, MaxProp, and PROPHET
- 40 vehicular nodes
- Transmission radius 100 m
- Map-based movement, Helsinki city map
- Area 4500 m × 3400 m
- 12 h simulation time



7151.5 12.90 1/s GUI update: 1 0.3

p10 at (1677.52,388.83) M31 (1 copies) [c49->c50] size:599555, UI:46721, received @ 6494.90 path: 3 hops

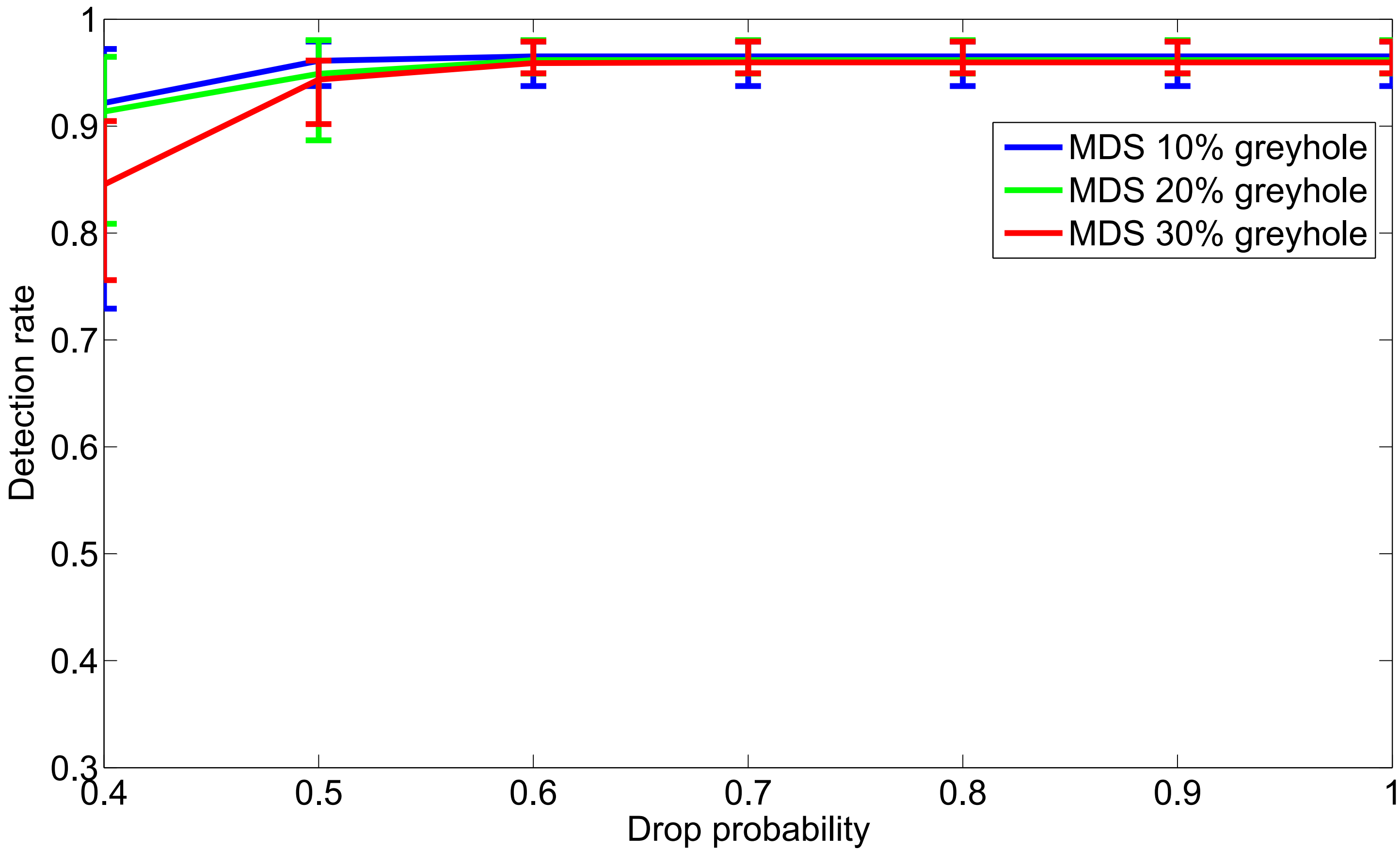
Event log controls

	show	pause
all	☑	□
connections		
up	☑	□
down	☑	□
messages		
created	☑	□
started relay	☑	□
relayed	☑	□
delivered	☑	□

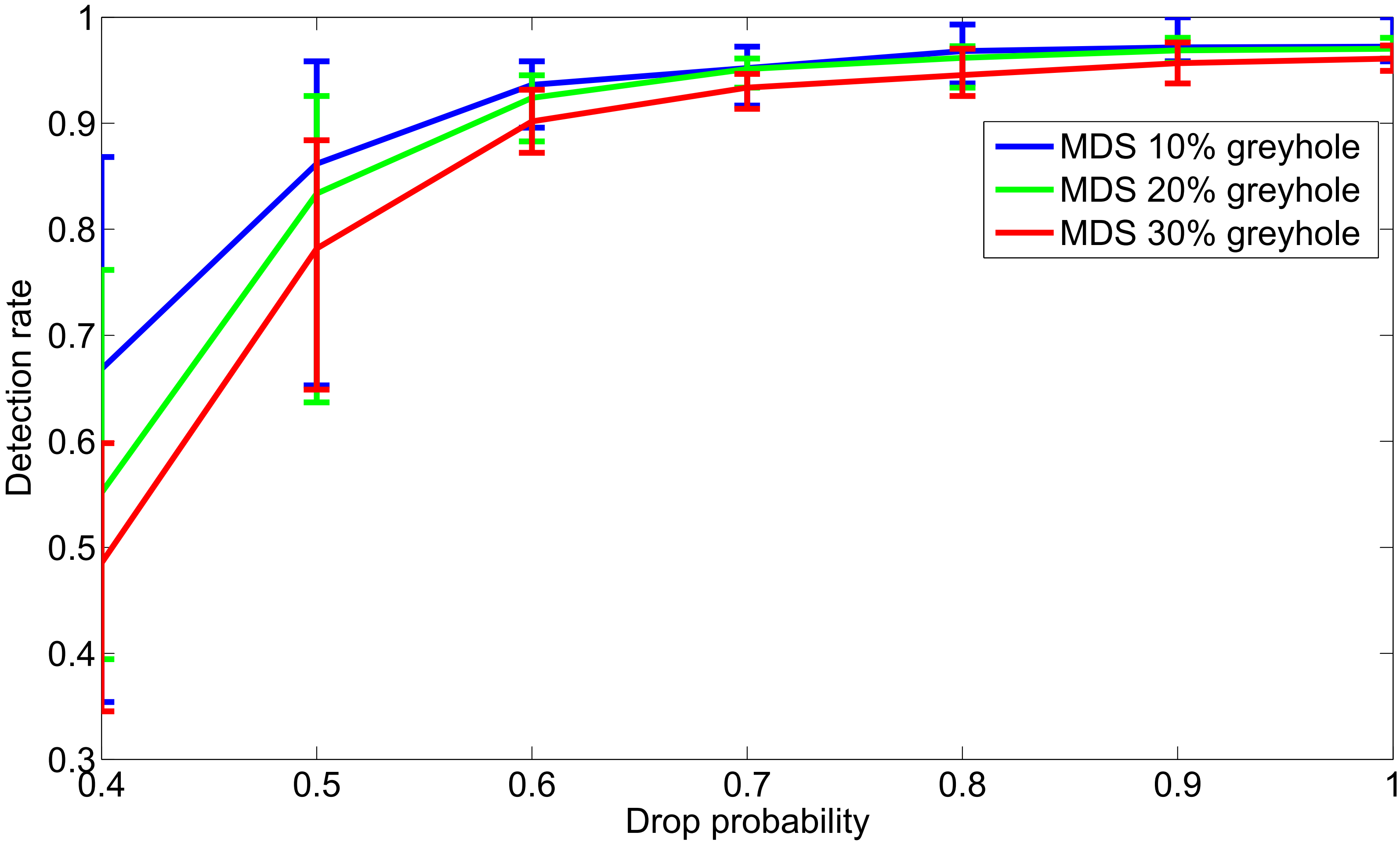
Event log

```
7084.4: Message relayed c59<->p9 M88 (5 copies)
7084.4: Message relay started c59<->p9 M79 (5 copies)
7085.2: Connection DOWN p9<->c59
7085.2: Message relay aborted c59<->p9 M79 (5 copies)
7085.7: Connection UP c75<->w93
7085.7: Message relay started w93<->c75 M77 (10 copies)
7086.2: Message created p18 M90 (10 copies)
7086.9: Connection UP p17<->c77
```

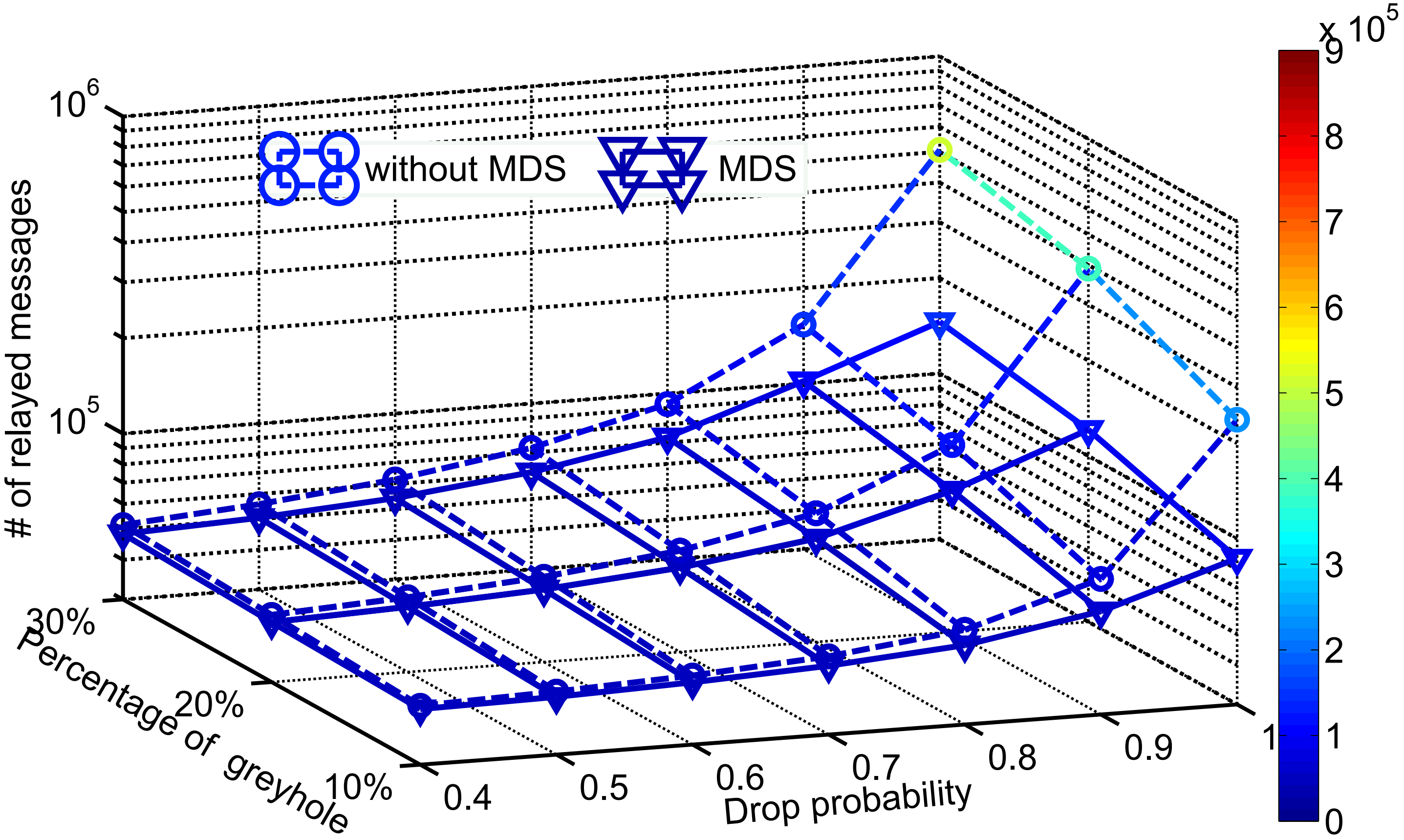
Detection Rate, Epidemic Routing



Detection Rate, Spray & Wait

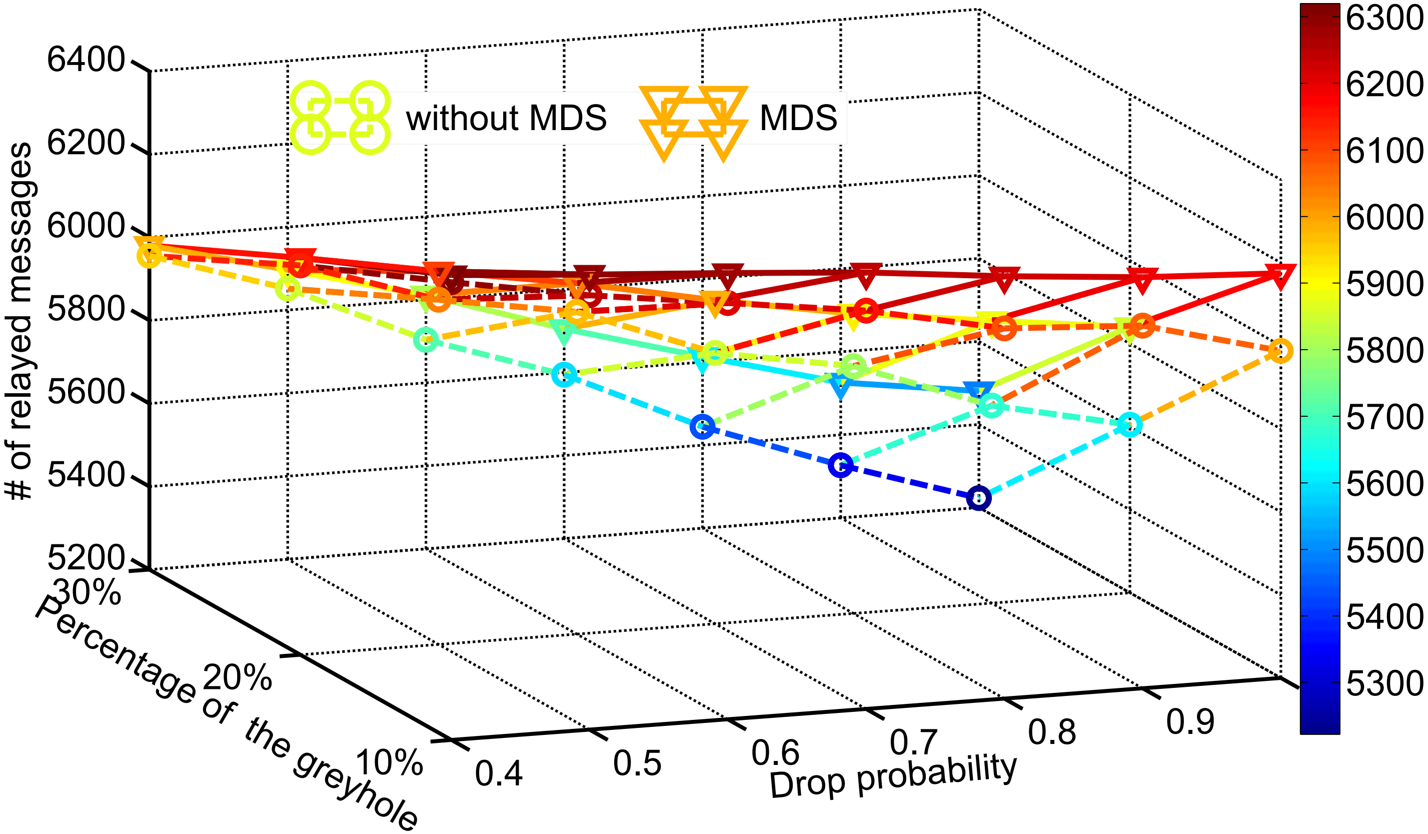


Energy Consumption, Epidemic Routing



MDS reduces useless transmissions

Energy Consumption, Spray & Wait



MDS protects limited replications, increases delivery rate

Conclusion

- Future VANETs will have a DTN structure
- Misbehavior detection is needed to exclude non-conforming nodes and keep the system healthy
- The proposed system
  - detects blackhole and greyhole behaviors
  - has a high detection rate
  - significantly reduces energy usage for routing protocols with unlimited replication
  - increases delivery rate for routing protocols with limited replication

Thank you! Questions?

guo@ibr.cs.tu-bs.de