Securing AODV Against Wormhole Attacks in Emergency MANET Multimedia Communications

PEACE meeting

10/09/09

Manos Panaousis

e.panaousis@kingston.ac.uk

WMN Group

Kingston University London

PEACE

IP-based Emergency Application and serviCes for nExt generation networks

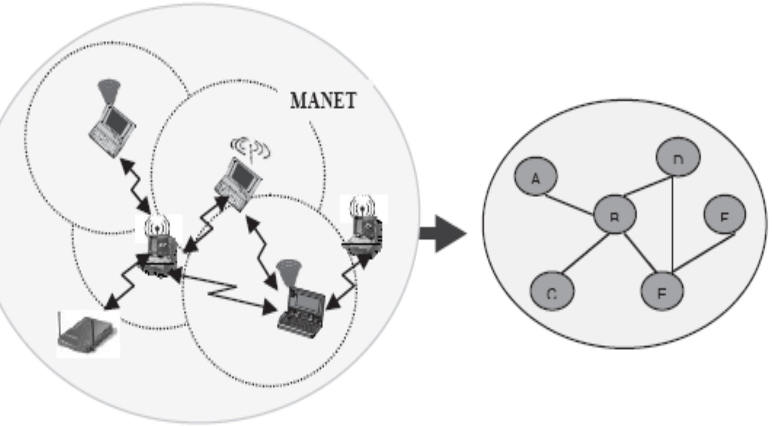
Kingston University London

Roadmap

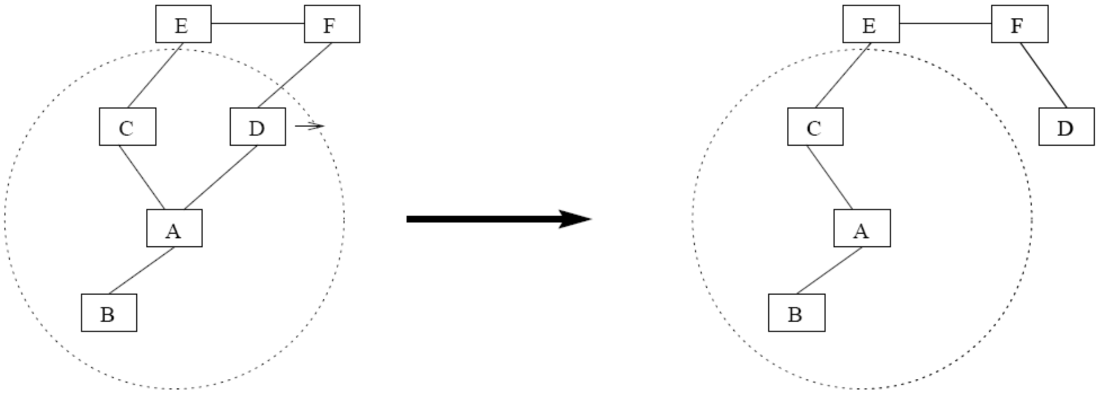
- Mobile Ad-Hoc Networks (MANETs)
- Attacks in MANETs
- Security in MANETs
- AODV-WADR (Ad hoc On demand Distance Vector Wormhole Attack Detection Reaction)
- Performance Evaluation
- Conclusions

Mobile Ad-hoc NETworks (MANETs)

- MANET is a wireless multihop network
- MANET does not have fixed infrastructure
- Mobile nodes act as routers



Topology change in MANET
due to nodes' mobility



Attacks in MANETs

- Active and passive attacks (packet dropping and eavesdropping)

- Internal and external attacks from compromised and malicious nodes that do not belong to the MANET

- Man-in-the-middle attacks (an attacker is based between two legitimate nodes to intercept packets)

- Impersonation attacks (an attacker impersonate another node to masquerade himself)

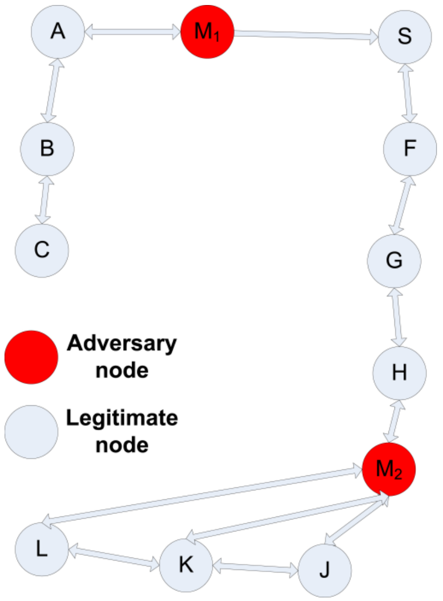
- Denial of Service (DoS) attacks (an attacker drops legitimate packets)

Security in MANETs

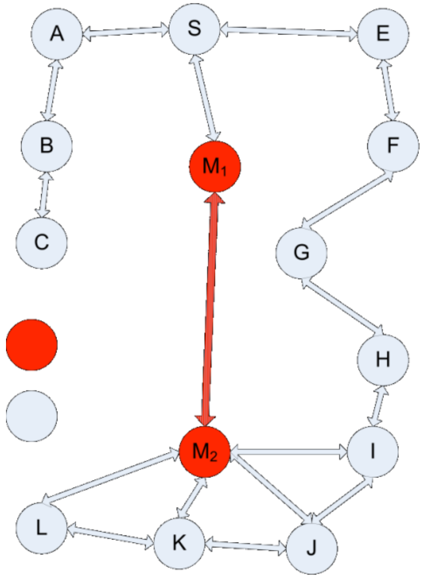
- Authentication: ensures that MANET nodes are not pretenders
- Confidentiality: ensures that information is accessible only to those authorized to have access
- Integrity: ensures that nodes' messages are forwarded to the destination without any malicious alteration
- Non-repudiation: no node can deny the sending or receiving of messages
- Key Management: generation, exchange, storage, safeguarding, use and refreshment of keys

Wormhole Attacks in MANETs

- Most of the routing protocols have been developed without secure mechanisms
- Wormhole attacks
  - In-band wormhole attack



  - Out-band wormhole attack



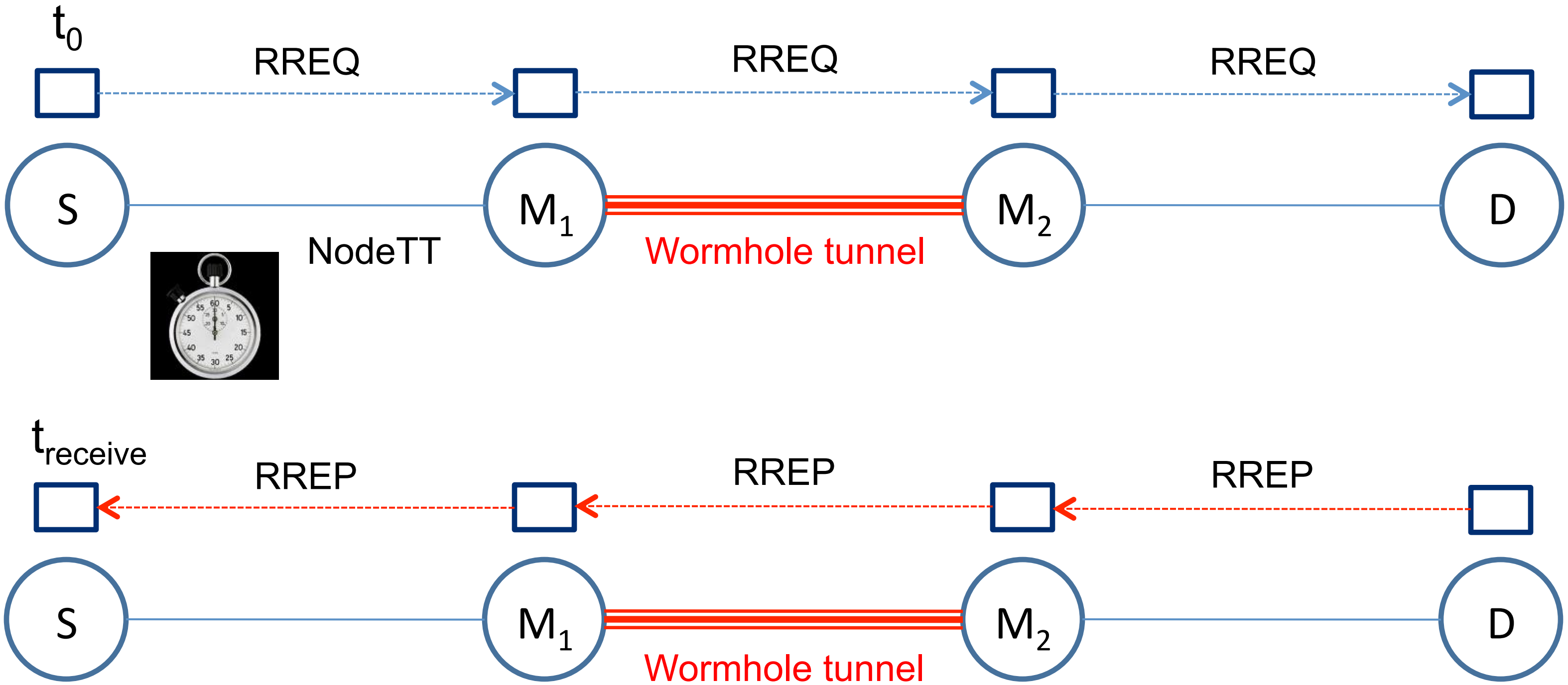
Out-band Wormhole Attack

- Two adversaries create a wormhole tunnel, flood wrong routing information though the MANET
- Intercept packets
- Replay packets in different areas of the MANET
- Disrupt the appropriate function of the AODV protocol

Ad hoc On demand Distance Vector Wormhole Attack Detection Reaction

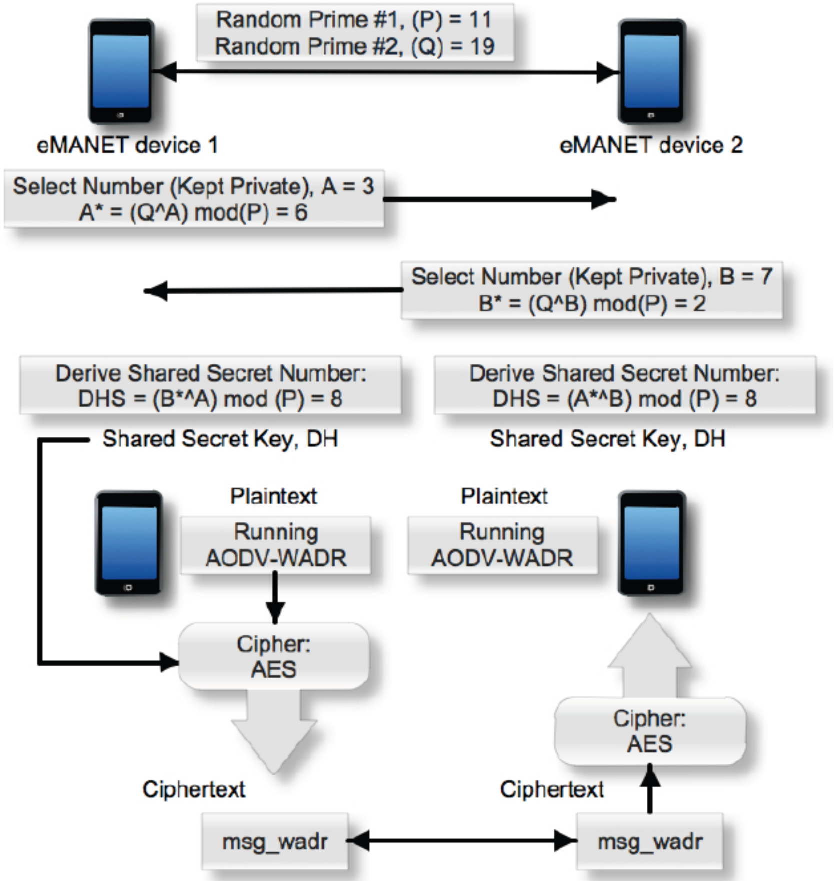
- AODV-WADR defends AODV (IETF RFC 3561) protocol against out-band wormhole attacks using timing and cryptographic mechanisms
- Wormhole tunnels introduce delays in the communication links
- Long delays in packet transmission are treated as suspicious and wormhole detection must be performed
- Establishment of symmetric keys to decrypt wormhole detection packets
- Detected wormhole nodes are excluded from MANET and added to a blacklist (*blacklist_wadr*) temporally

AODV-WADR Algorithm



- **if** $t_{receive}$ > 6 * NodeTT **then** *S* suspects a wormhole tunnel
- *S* establishes a *Diffie-Hellman Exponential Key Exchange* session with *D*

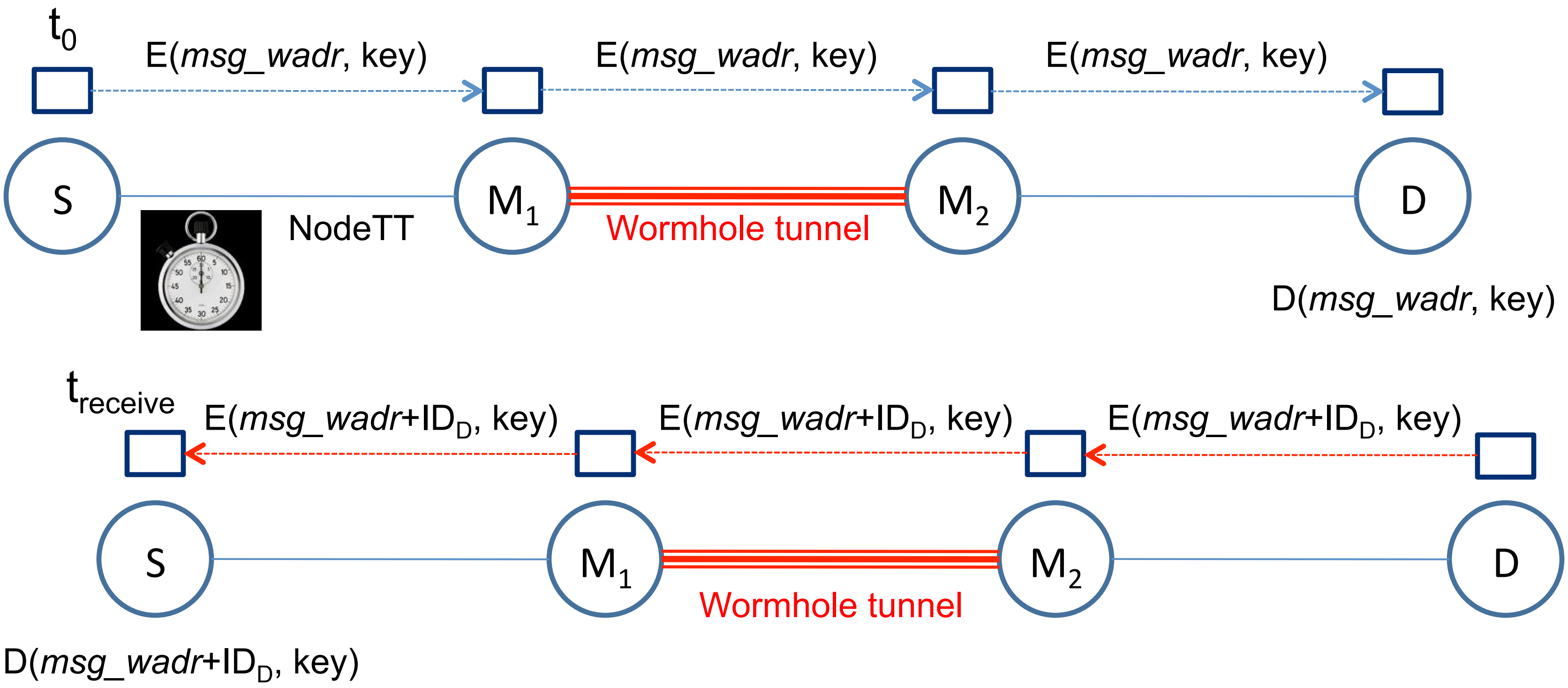
Diffie-Hellman Algorithm



- **if** *S* does not receive an answer from *D* within NetTT time, *S* adds M_1 to *blacklist_wadr*

- **else** *S*, *D* share a common symmetric AES (Advanced Encryption Standard) key

AODV-WADR Algorithm (cont.)



- **if** $t_{receive}$ > 6 * NodeTT+ t_{crypt} **then** *S* detects a wormhole tunnel

- *S* adds M_1 to *blacklist_wadr* to prevent other nodes to communicate with M_1

Simulation Parameters

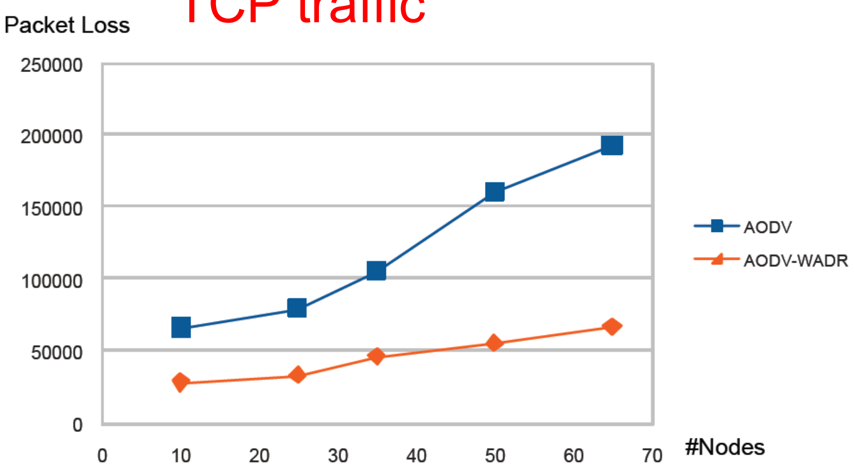
Examined approaches	AODV, AODV-WADR
Pause Time	5 sec
Number of Nodes	10, 25, 35, 50, 65
Data Rate	64 kbps
Nodes' Speed	1, 2 m/s
Simulation Time	1000 sec
Mobility Model	Mission Critical Mobility
Simulation Areas	1000m x 1000m, 2000m x 2000m
Traffic Types	UDP, TCP

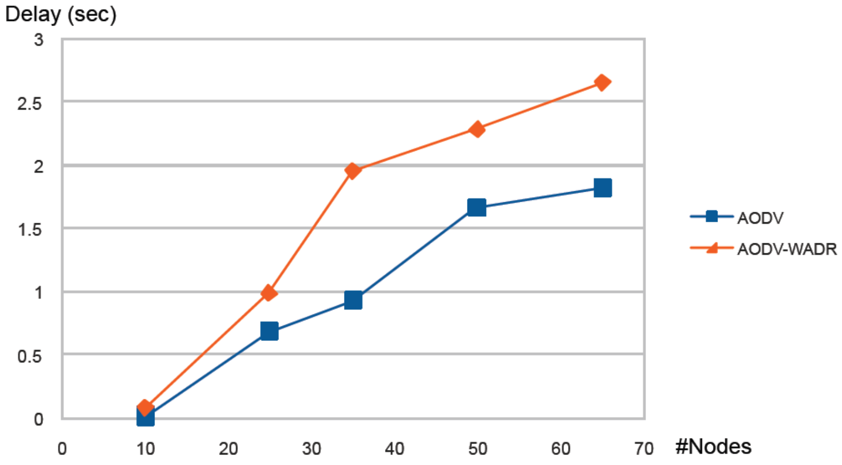
- simulates the movement of nodes during an emergency case such as a forest fire or a terrorist attack

- implements two-way ground propagation model and the Random Waypoint mobility model considering obstacles

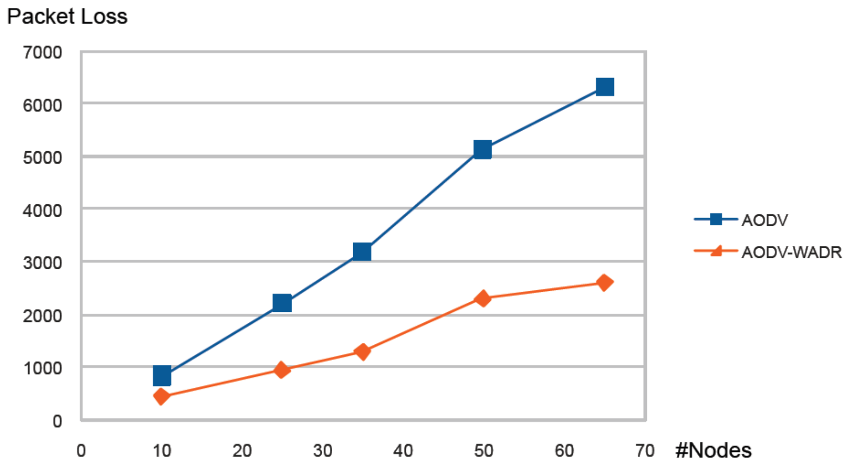
Performance Evaluation for 1km x 1km area

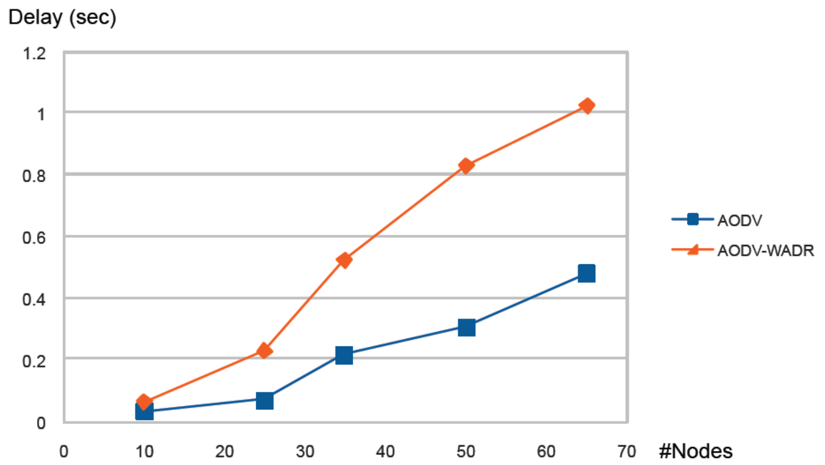
TCP traffic





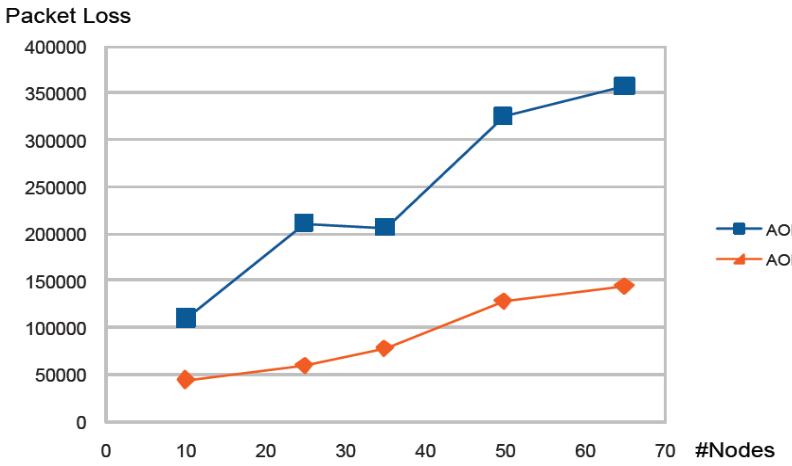
UDP traffic



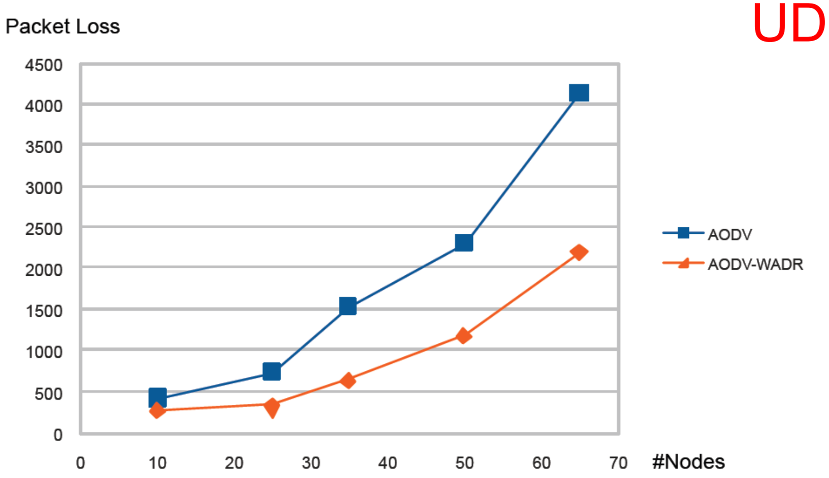


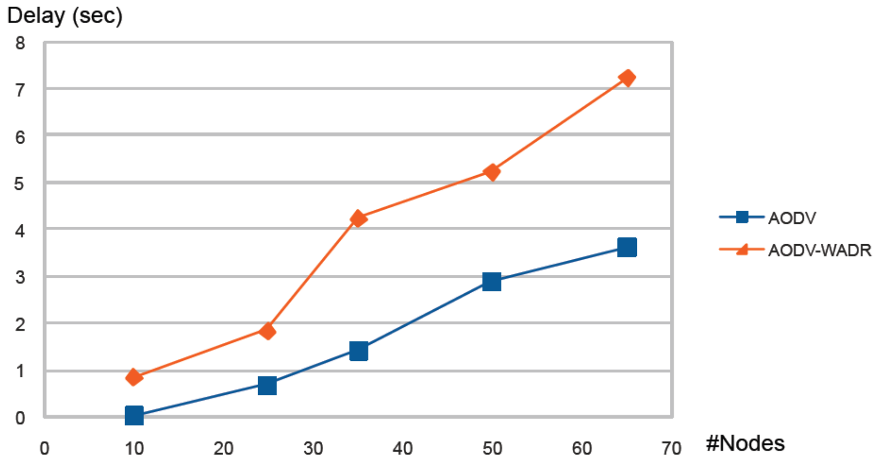
Performance Evaluation for 2km x 2km area

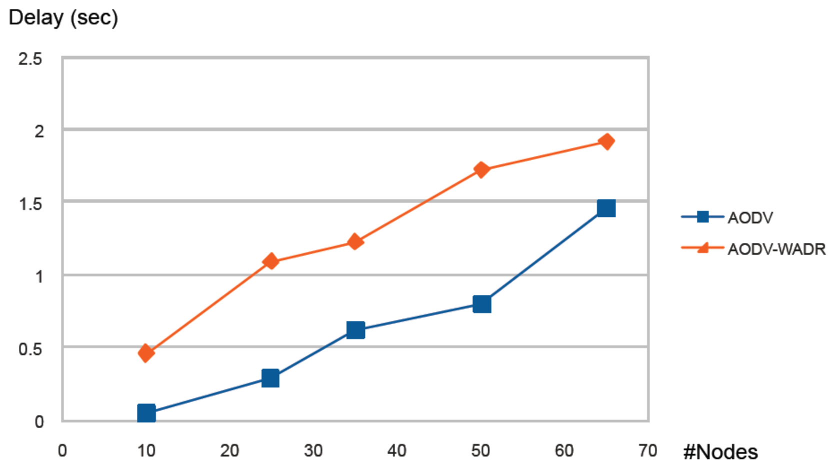
TCP traffic



UDP

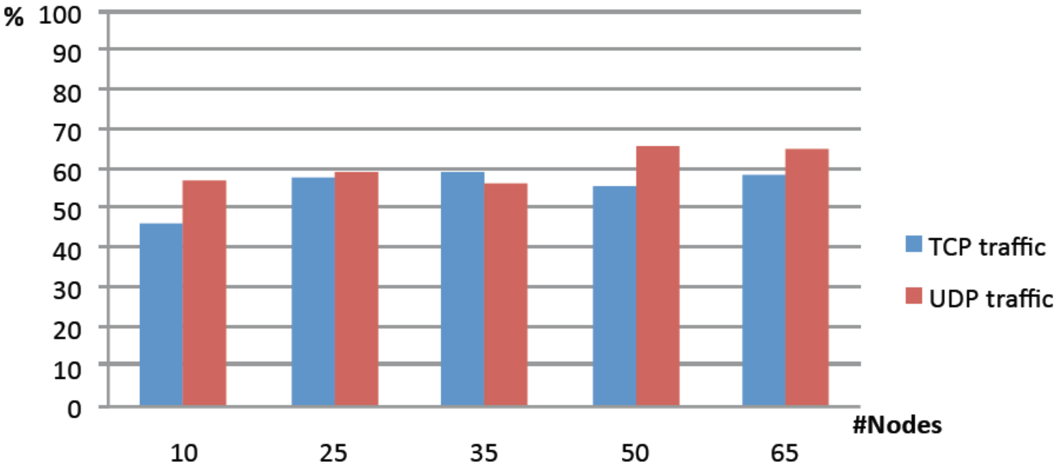




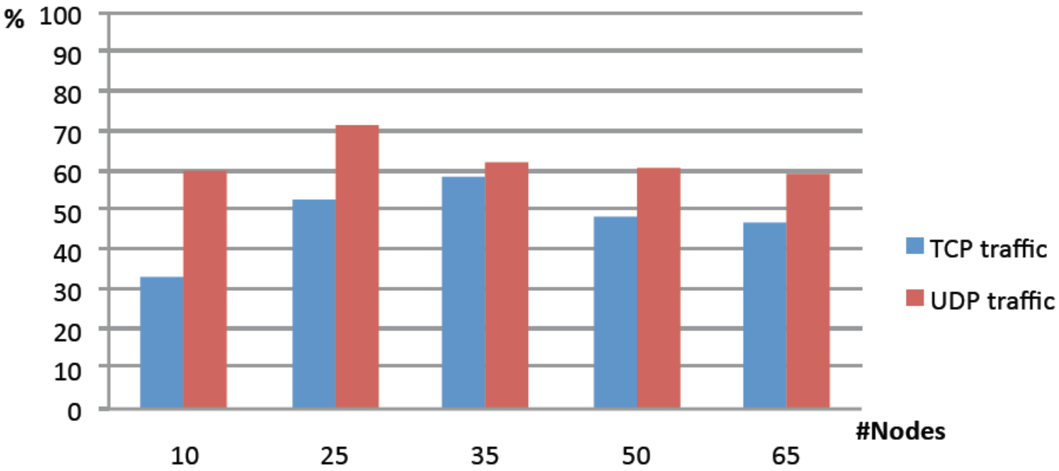


Perfomance Evaluation (cont.)

- The packet loss improvement for a 1km x 1km area



- The packet loss improvement for a 2km x 2km area



Conclusions

- Wormhole attack is a well-known attack against routing protocols in MANETs
- AODV-WADR defends AODV against wormhole out-band wormhole attacks
- The performance of AODV-WADR is more efficient than the performance of AODV, in terms of packet loss in presence of wormhole attacks
- The delay introduced by AODV-WADR is affordable and it is very close to the AODV delay

Thank you for your attention.

Any questions?