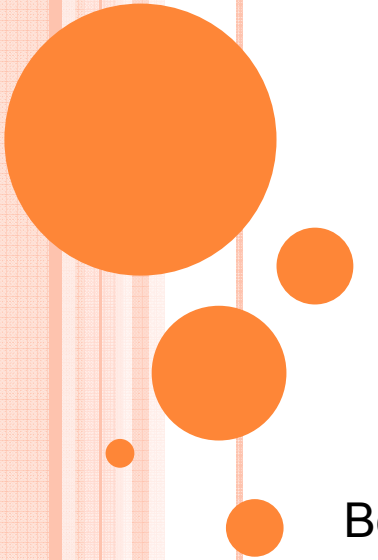
BSMR: Byzantine-Resilient Secure Multicast Routing in Multi-hop Wireless Networks

Reza Curtmola
Department of Computer Science
Johns Hopkins University

Cristina Nita Rotaru
Department of Computer Science
Purdue University



Behnam ASEFISARAY

Outline

- What Byzantine Means?
- Introduction
- Security Aspects in Networks
- Network and Systems Model
    - Network model
    - Multicast protocol
- Three level trust model
- Attacks in multicast multi-hop networks
- Attacks that studied in this Work
- Secure multicast routing protocol
    - Overview to BSMR
    - Authentication framework
        - Secure tree token dissemination
        - Hope count authentication
    - Route Discovery
    - Multicast tree maintenance
    - Selective data forwarding detection
- Simulation results

What Byzanine Means?

From WikiPedia :

Doğu Roma İmparatorluğu, (Yunanca: Βασιλεία τῶν Ῥωμαίων, Basileía tôn Rhōmaíōn "Rum İmparatorluğu";Latince: Imperium Romanum) ya da 16. yüzyılda Alman Hieronymus Wolff'un adlandırmasıyla[1] Bizans İmparatorluğu, Roma İmparatorluğu'nun 395'te Doğu ve Batı olarak ikiye ayrılmasıyla ortaya çıktı. BaşkentiRoma olan Batı Roma İmparatorluğu 5. yüzyıldaGermen kabilelerinin İtalya'yı istila etmesi sonucu yıkıldı. Merkezi Konstantinopolis (bugünkü İstanbul) olan ve Bizans İmparatorluğu da denen Doğu Roma İmparatorluğu ise, bin yılı aşkın süre varlığını sürdürdü. Bizans'ın ortaya çıkışı, Roma İmparatoru I. Constantinus'un başkenti, Roma'dan bugünkü İstanbul'a taşımasıyla da yakından ilişkilidir.

Introduction

✓ Multicast routing protocols deliver data from a **source** to **multiple destinations**.

✓ **Wireless** networks provide a **less robust** communication due to **frequent broken links** and a higher error rate.

✓ A major challenge in designing protocols for wireless networks is ensuring **robustness** to failures and resilience to attacks.

✓Multi-hop communication makes services more vulnerable to insider attacks.

✓Authentication **is not sufficient** to protect against insider attacks.

✓**Insider** attacks are also known as Byzantine attacks.

Security Aspects in Networks:

Security aspects in multicast protocols relate to either:

1-Routing specific security
-Management of the routing
-Structure and data forwarding

Or

0-Application specific security
-Data confidentiality
-Authenticity

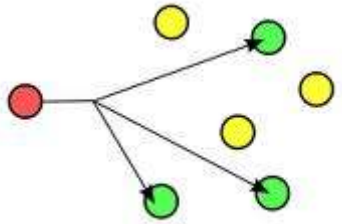
Network and System Model

Network Model:

- Multi-hop wireless network
- Wireless channel is symmetric
- Same transmitting power
- Same transmission range
- No GPS receiver or tightly synchronized clocks

Multicast Protocol :

- Tree based protocol
- On demand protocol
- Multicast group



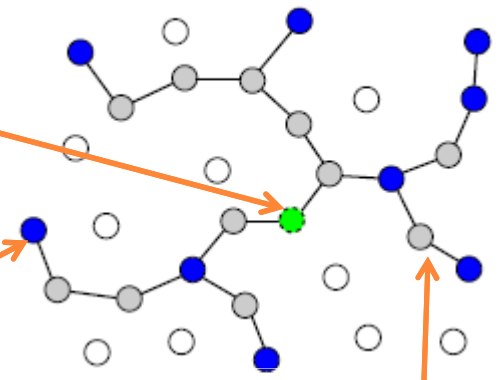
Main Operations:

- Route discovery
- Route activation
- Tree maintenance

Three Level TRUST Model:

Source:

must be continually available and assumed not to be compromised.



Group member nodes:

Are allowed to initiate requests for joining multicast groups.

Non-member nodes:

participate in the routing but cannot initiate group join requests.

Attacks in Multicast Multi-Hop Networks:

✓Byzantine behavior:

- Not forwarding packets
- Injecting
- Modifying
- Replaying
- Rushing packets
- Creating wormholes

✓We 

on the following three Byzantine attacks:

- **Black hole attack:** One or several adversaries forward only routing control packets, while dropping all data packets.
- **Wormhole attack:** Two colluding adversaries tunnel packets between each other.
- **Flood rushing attack:** One or several adversaries rush an authenticated flood through the network.

Secure Multicast Routing Protocol:

BSMR Overview:

✓Data is delivered from the source to the members of the multicast group.

✓Authentication ensures only authorized nodes can perform certain operations.

✓Mitigates inside attacks that try to prevent a node from establishing a route.

✓Resilience to selective data forwarding attacks by using a reliability metric.

Secure Multicast Routing Protocol:

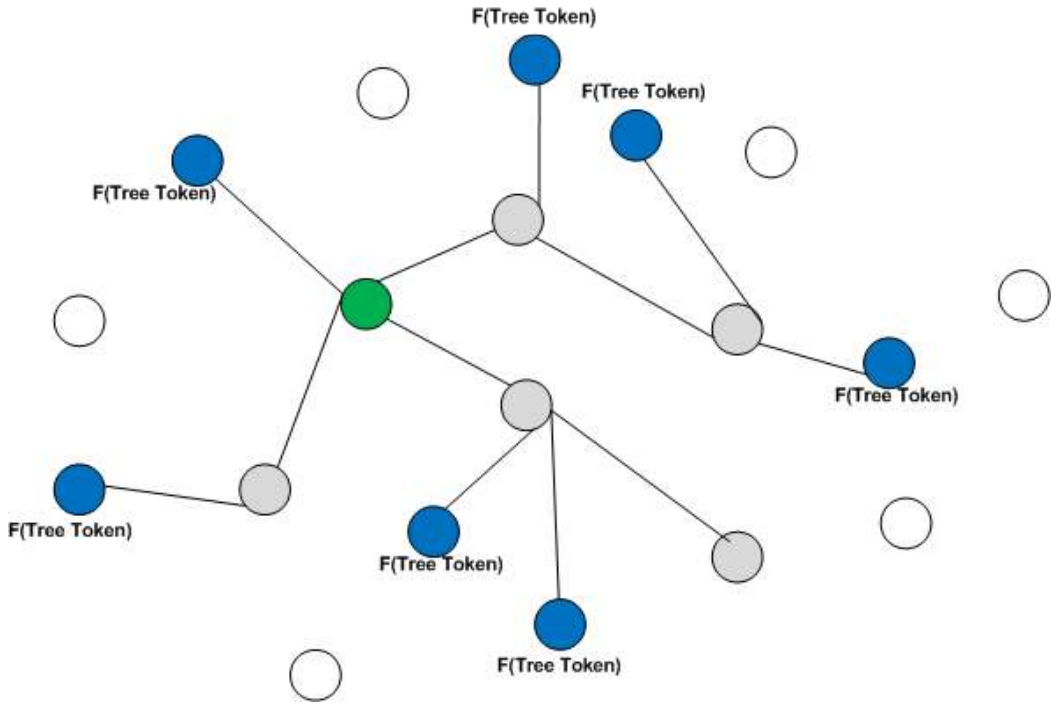
Authentication Framework:

- Prevents unauthorized nodes to be part of the network.
- Each node has a pair of public/private keys.
- Each node has an additional group certificate.

Secure Tree Token Dissemination:

-Token, periodically refreshed and disseminated by the group leader.

-Tree token authenticator **F(tree token)** .



Secure Multicast Routing Protocol:

Hope count authentication:

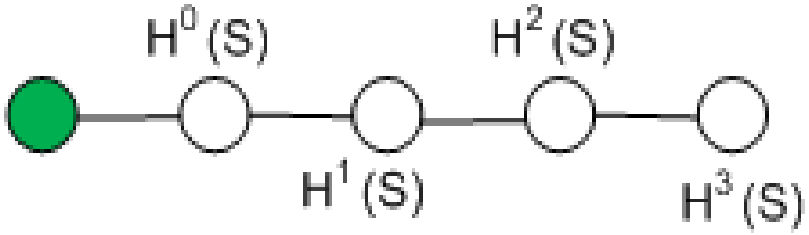
-To prevent tree nodes from claiming to be at a smaller hop distance than they actually are.

-Group leader chooses a random number **S** and

-Computes the value hop count anchor = $h^{max}(S)$

-Following information in messages sent in the multicast tree:

(hop count authenticator, d, MAX, $h^{max}(s)$)

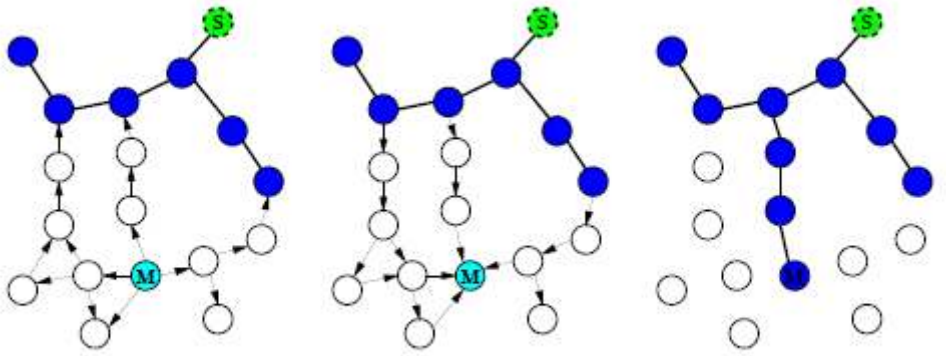


Secure Multicast Routing Protocol:

Route Discovery:

Route discovery allows a node that wants to join a group to find a route to the multicast tree.

- Group authenticated nodes can initiate route requests.
- If an adversarial-free path exists, it will be found.
-The path selection relies on the weights list.

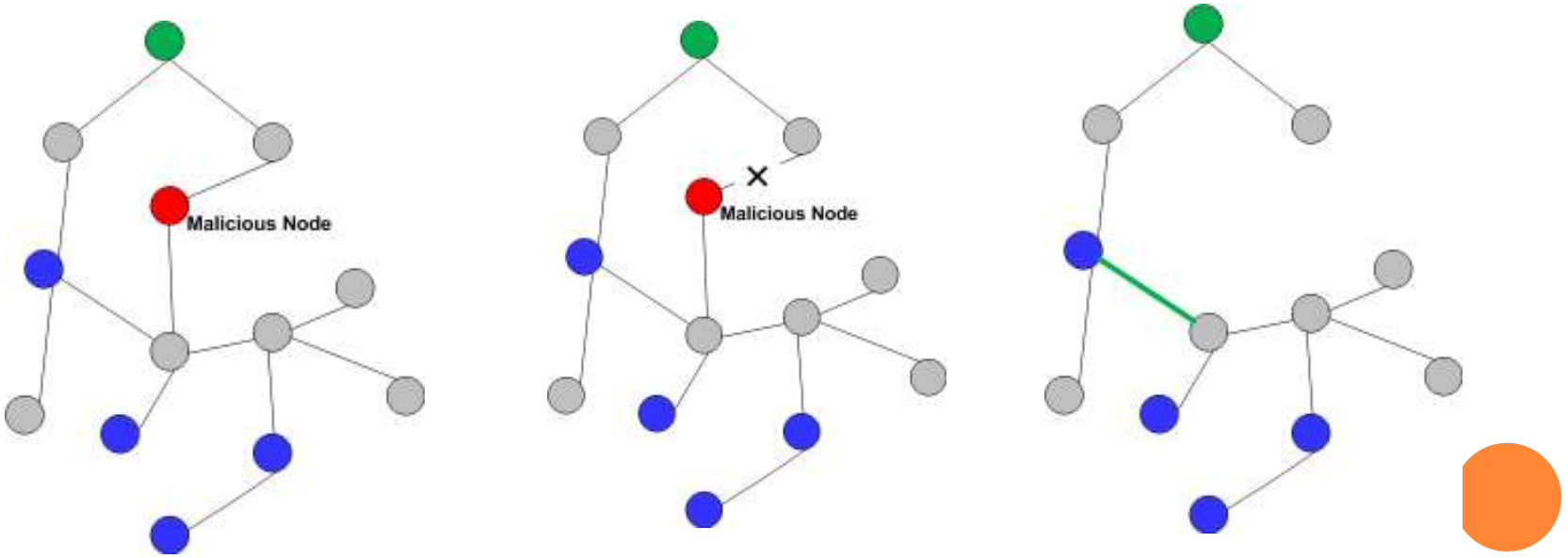


(a) RREQ (b) RREP (c) Route activation

Secure Multicast Routing Protocol:

Multicast tree maintenance

-If a malicious node prunes itself.
-The honest nodes in this sub tree will reconnect to the tree.
-The group leader periodically broadcasts in the entire network a signed GroupHello message.



Secure Multicast Routing Protocol:

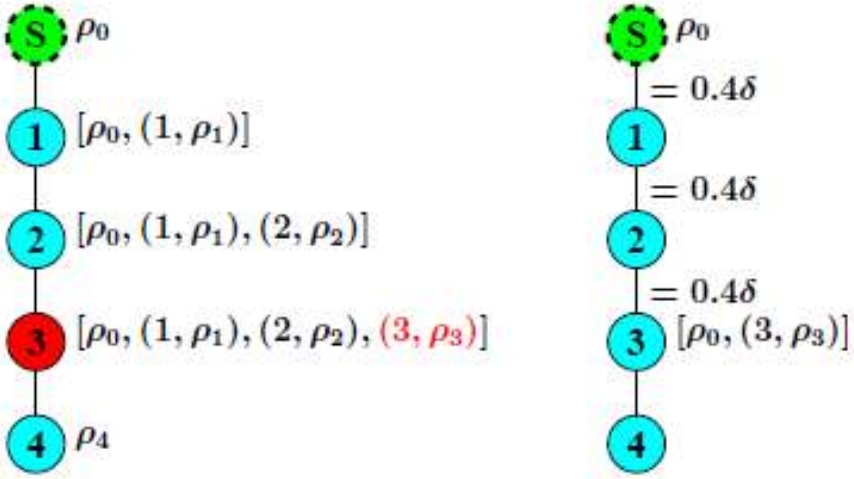
Selective data forwarding detection

-The source periodically signs and sends in the tree a multicast rate (MRATE) message that contains its data transmission rate P0 .

-Nodes may add their perceived transmission rate to it.

-**MRATE=(p0, (1,p1), (2,p2), (3,p3) …)**

- Detect if tree ancestors perform selective data forwarding attacks.



Simulation results:

Performance metric:

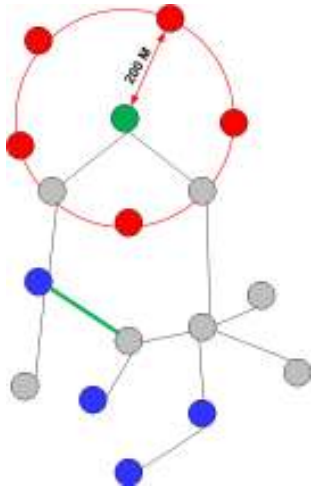
Packet delivery ratio : $PDR = P_r / (P_s \cdot N)$

We consider the following scenarios:

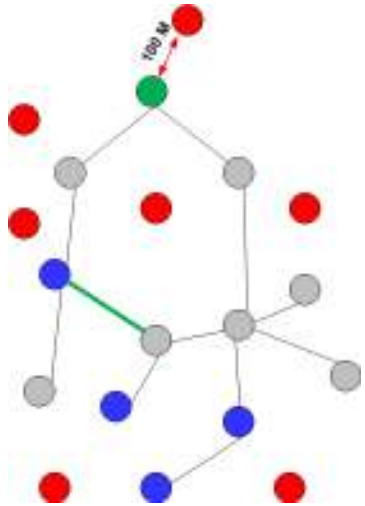
- Random placement: adversaries are placed randomly in the simulation area;

- Strategic placement: adversarial placement is as follows:

Black hole attack



Wormhole attack



Results:

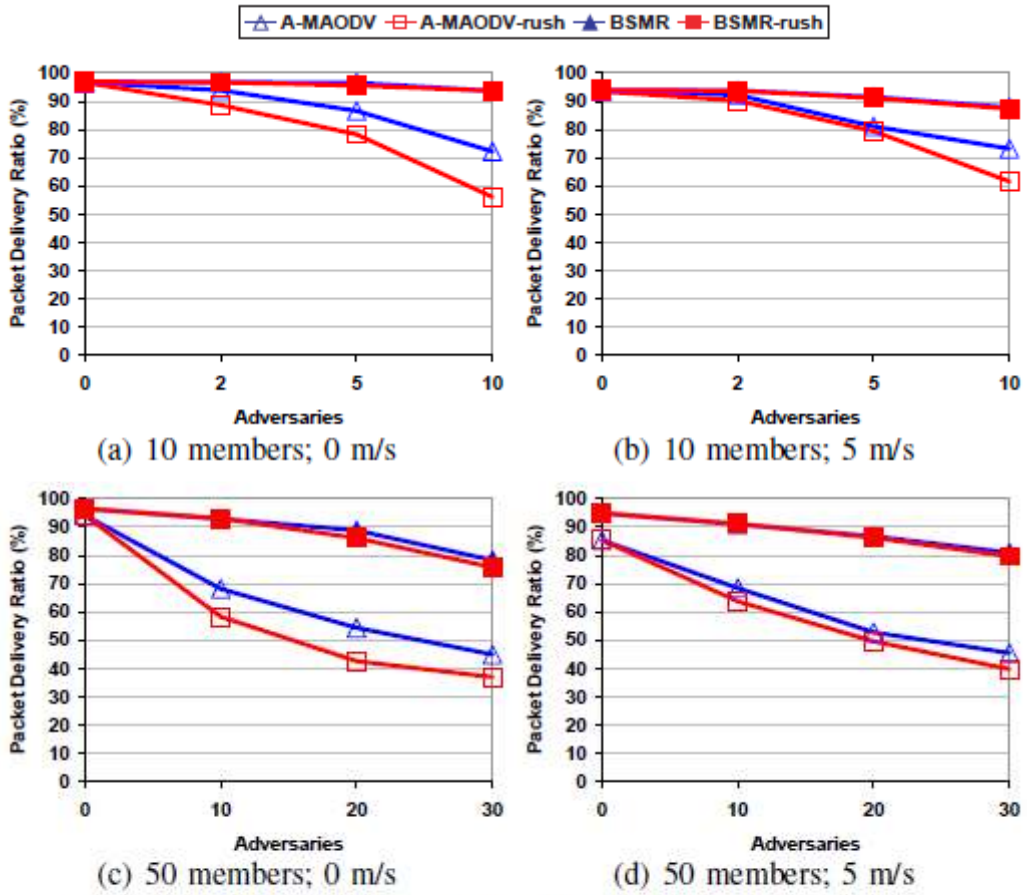


Fig. 7: Black hole attack and flood rushing combined with black hole: **Random placement (NJOIN)**

Results:

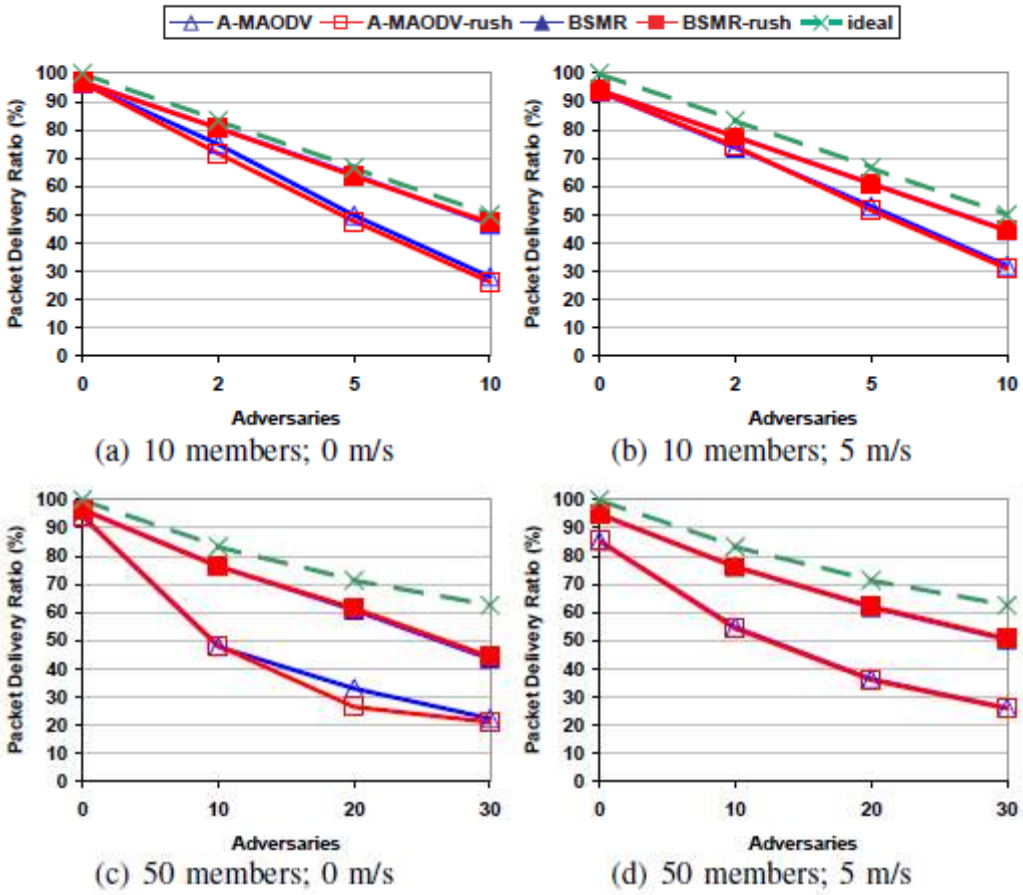
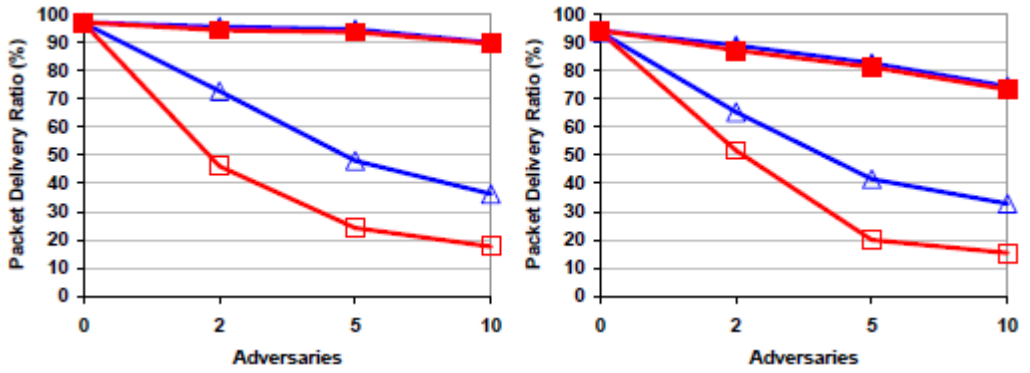


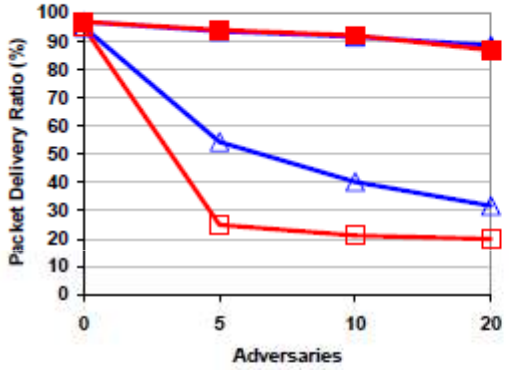
Fig. 9: Black hole attack and flood rushing combined with black hole: **Random placement (JOIN)**

Results:

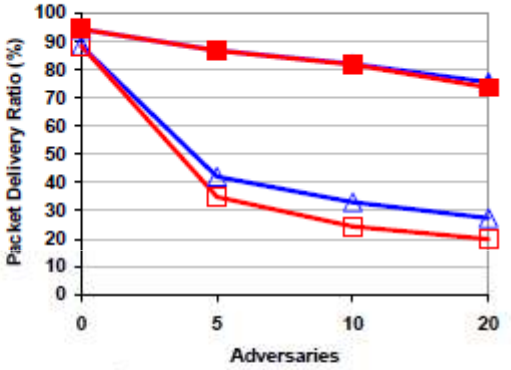


(a) 10 members; 0 m/s

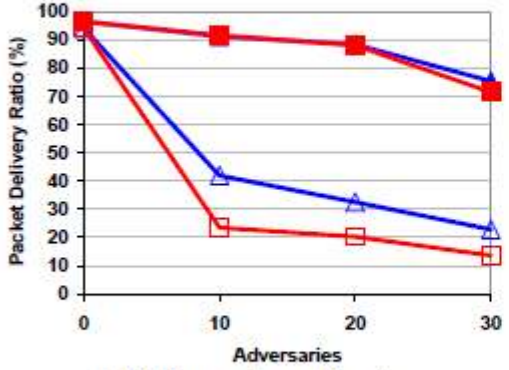
(b) 10 members; 5 m/s



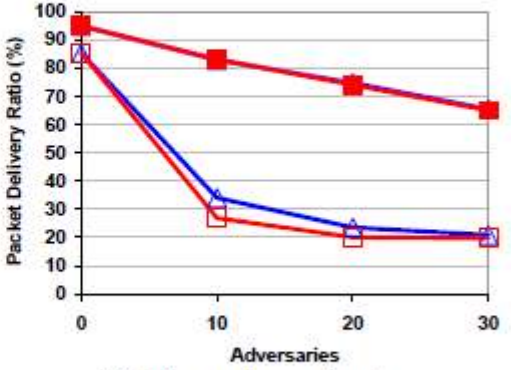
(c) 30 members; 0 m/s



(d) 30 members; 5 m/s



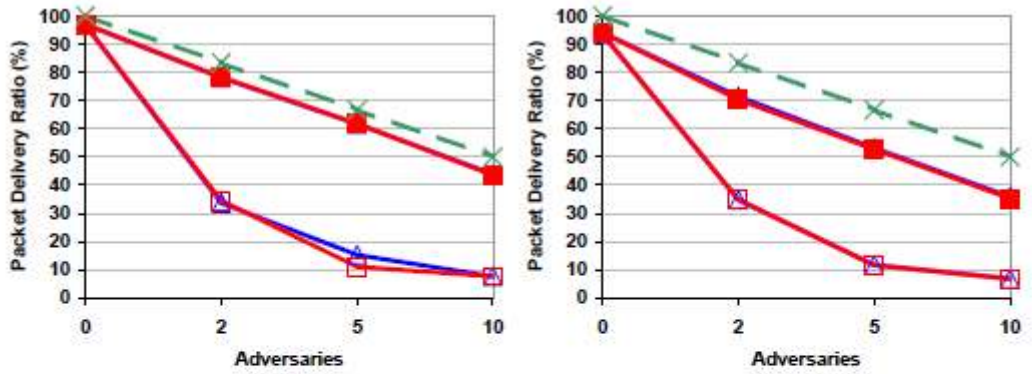
(e) 50 members; 0 m/s



(f) 50 members; 5 m/s

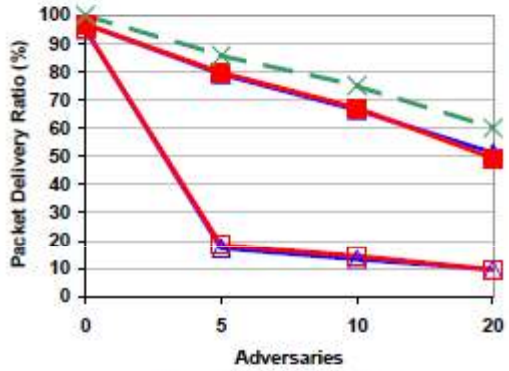
Fig. 8: Black hole attack and flood rushing combined with black hole: **Strategic placement (NJOIN)**

Results:

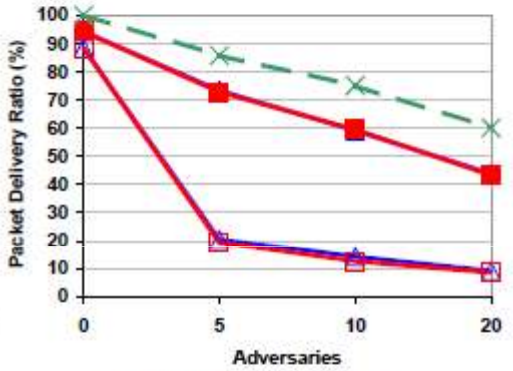


(a) 10 members; 0 m/s

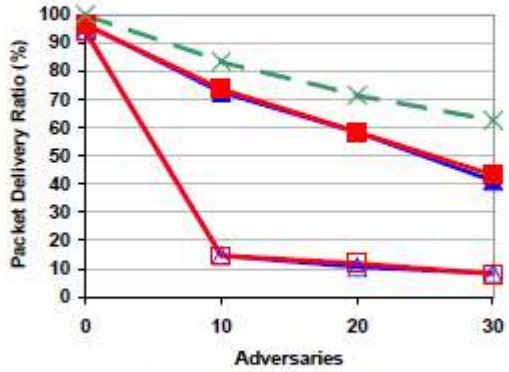
(b) 10 members; 5 m/s



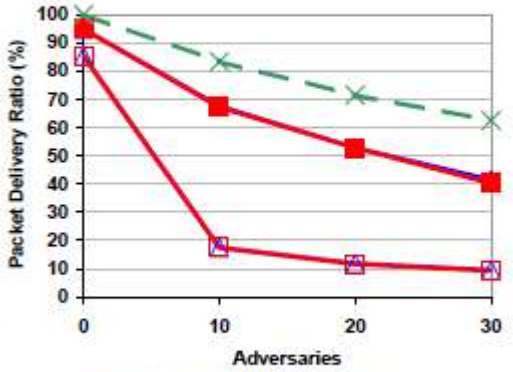
(c) 30 members; 0 m/s



(d) 30 members; 5 m/s



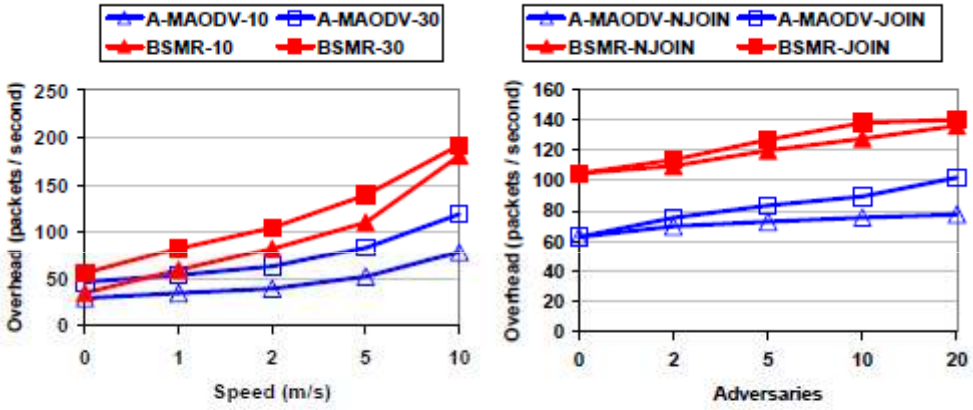
(e) 50 members; 0 m/s



(f) 50 members; 5 m/s

Fig. 10: Black hole attack and flood rushing combined with black hole: **Strategic placement (JOIN)**

Overhead:



(a) Non-adversarial scenario (group size $\in \{10, 30\}$)

(b) Attack scenario (group size = 30, 2m/s, strategic placement)

Fig. 15: BSMR total network overhead

Thank You

Any Question?