“AUTHENTICATION OF OPPNET NODES IN OPPNET ENVIRONMENTS”

ANIL KUMAR YEDUGANI
VENKATA VAMSI KRISHNA

DEPARTMENT OF COMPUTER SCIENCE
WESTERN MICHIGAN UNIVERSITY
INSTRUCTOR: PROF. LESZEK T. LILIEN
05 OCTOBER 2006
INTRODUCTION

• What are oppnets?
INTRODUCTION

• What are oppnets?
• Oppnet nodes
INTRODUCTION

• What are oppnets?
• Oppnet nodes
• Potential oppnet helpers
• Potential oppnet helpers

  ➢ Benevolent oppnets
  ➢ Malevolent oppnets
INTRODUCTION

- What are oppnets?
- Oppnet nodes
- Potential oppnet helpers
- Privacy and Security threats
Privacy and Security threats

- MITM
- DoS
- ID Spoofing (Masquerading)
- Packet dropping
A familiar routing protocol in ad-hoc networks for mobile devices to communicate in the oppnet environment.
Goal: to give a sketch of an overall balanced security solution, attempting to identify each attack and searching for defenses.

- Authentication is an essential and necessary component for avoiding threats in most of the Security architectures.
Authentication Authority:

We need an authentication authority, which may not be present in the ad-hoc network but provides keys for the nodes.
OLSR Cont...

Fig. 1. OLSR Attack Tree (OR-tree)
OLSR

- **Authenticated nodes** ("trust but verify")

  By default the behavior of authenticated nodes is assumed to be correct.

- **Unauthenticated nodes** ("protection")

  The aim is to prevent them disrupt the network.
OLSR

Preventing attacks from authenticated nodes:

- Generation of incorrect control messages
- Not forwarding data packets
- Not forwarding control messages

Preventing attacks from unauthenticated nodes:

- Wormhole attacks
- Replay attacks
- Preventing packet transmission
Summarizing the prevention of attacks

Authenticated nodes:
• The incorrect messages can be stopped from passing through the network by signing and advertised link on both ends of the link and then send link state messages by a remote third node for verification.
• The other two attacks are compromised nodes that do not forward messages or packets. Detecting this misbehavior is a big problem.

Unauthenticated nodes:
• In order to prevent wormhole attacks, a variant of the counting technique is used.
• Replay attacks – with timestamps.
• External methods- e.g Jamming is typically addressed by searching for the jamming devices
Conclusion...
References


Thank You