technology
from seed

On the Use of Radio Resource Tests in Wireless ad hoc Networks

Diogo Mónica, João Leitão, Luís Rodrigues, Carlos Ribeiro
INESC-ID/IST
{diogo.monica, joao.c.leitao, ler, carlos.ribeiro} @ist.utl.pt

Road Map

technology
from seed

- Introduction
- Radio Resource Tests
- Analysis
- Summary

Introduction – Wireless ad hoc Networks

technology from seed

inesc id lisboa

Securing Wireless ad hoc Networks is particularly difficult

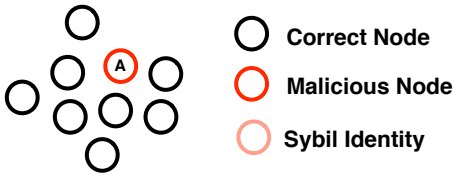
- Denial-of-service
- Eavesdropping
- Node hijacking
- Impersonation
  - Sybil Attack

Introduction – The Sybil Attack

technology from seed

inesc id lisboa

A Sybil attack happens when a malicious node participates with multiple identities in a system



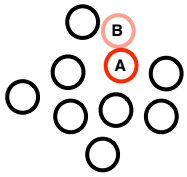
The sybil identity can be generated by the malicious node, or stolen from an existing correct node

Introduction – The Sybil Attack

technology from seed

inesc id lisboa

A Sybil attack happens when a malicious node participates with multiple identities in a system



Correct Node

Malicious Node

Sybil Identity

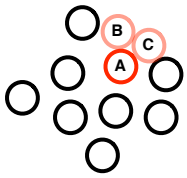
The sybil identity can be generated by the malicious node, or stolen from an existing correct node

Introduction – The Sybil Attack

technology from seed

inesc id lisboa

A Sybil attack happens when a malicious node participates with multiple identities in a system



Correct Node

Malicious Node

Sybil Identity

The sybil identity can be generated by the malicious node, or stolen from an existing correct node

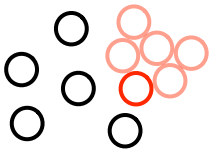
Introduction – The Sybil Attack

technology from seed

inesc id lisboa

Easily defeats quorum systems, or other voting schemes

Votes from Correct Nodes: 5
Votes from Malicious Node: 6



Correct Node
Malicious Node
Sybil Identity

In order to obtain a majority in a network with 5 correct nodes, a malicious node has to create 5 sybil identities

Introduction – Resource Tests

technology from seed

inesc id lisboa

In resource testing we determine if a set of identities possess fewer aggregated resources than would be expected

- Computational Power
- Storage
- Network Bandwidth
- …
- Radio Resource

Road Map

technology from seed

inesc id lisboa

Introduction

➢ Radio Resource Tests

Analysis

Summary

Radio Resource Tests

technology from seed

inesc id lisboa

Radio Resource Tests (RRTs) assume that each node has access to a single radio device, and builds upon the limitations of these devices

The first RRT was introduced by Newsome et. al 2004

We will call it Sender Test

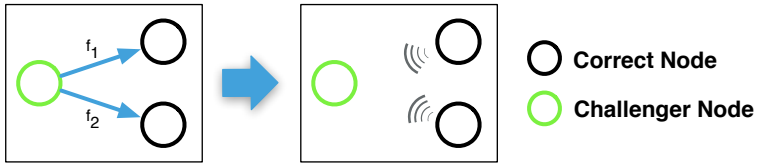
Radio Resource Tests – Sender Test

technology from seed

inesc id lisboa

Sender Test (SST)

- The Sender Test is based on the assumption that nodes cannot simultaneously transmit in more than one channel



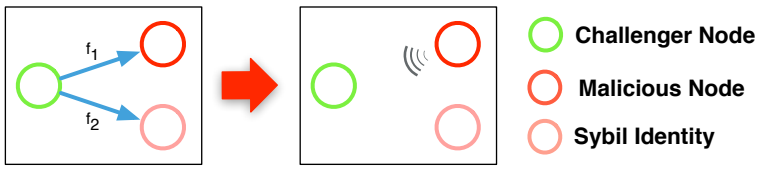
Radio Resource Tests – Sender Test

technology from seed

inesc id lisboa

Sender Test (SST)

- The Sender Test is based on the assumption that nodes cannot simultaneously transmit in more than one channel



Radio Resource Tests – Detection Probability

technology from seed

inesc id lisboa

The challenger is unable listen in more than one channel at the same time, so we repeat the test *r* times

- Denoting by *h* the number of simultaneously tested identities, and by p_d the probability of detection of a Sybil Identity in a test, we have

$$p_d = 1 - \left(1 - \frac{1}{h}\right)^r$$

Radio Resource Tests – Contribution

technology from seed

inesc id lisboa

We introduce two new tests and an optimization for the Sender Test

- Optimized Sender Test (oSST)
- Receiver Test (SRT)
- Collision Test (FCT)

Radio Resource Tests - Framework

technology from seed

inesc id lisboa

Each RRT is characterized by a set of parameters, RRT(h, c, w)

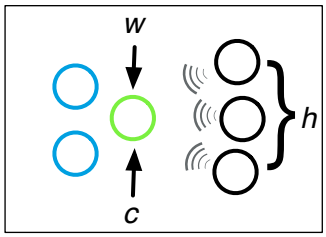
- *h* – Size of the set of simultaneously tested identities
- *c* – Number of challenger identities actively participating in the test
- *w* – Number of tester nodes that extract information from the test

Radio Resource Tests – Sender Test

technology from seed

inesc id lisboa

The Sender Test is a RRT(K,1,1)



Tested Nodes
Challenger Node
Non-participating nodes

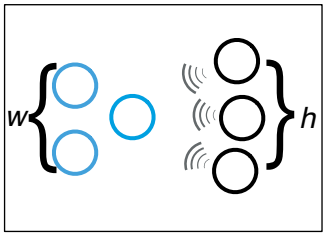
- *h* is limited by the number of available channels (K)
- *c* is one, since the challenger needs to assign in which channel identities transmit in
- *w* is one since only the challenger extracts information from the test

Radio Resource Tests – Optimized Receiver Test

technology from seed

inesc id lisboa

The Optimized Sender Test is a RRT(K,0,N-K)



Tested Nodes

Non-participating nodes

- *h* is limited by the number of available channels (K)
- *c* is zero, since the channels can be chosen deterministically
- *w* is N – K, since every node not participating in the test can extract information from it

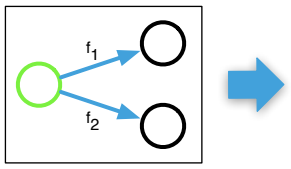
Radio Resource Tests – Receiver Test

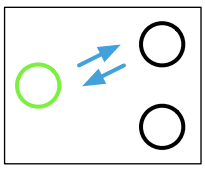
technology from seed

inesc id lisboa

Receiver Test

- The Simultaneous Receiver Test is based on the assumption that nodes cannot simultaneously listen in more than one channel





Correct Node

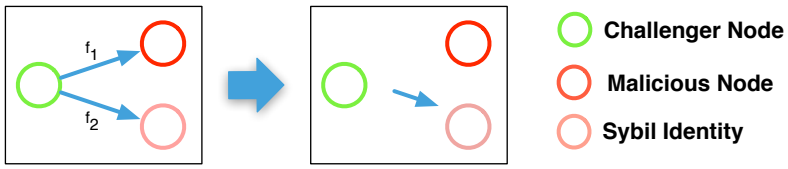
Challenger Node

technology from seed

inesc id lisboa

Receiver Test

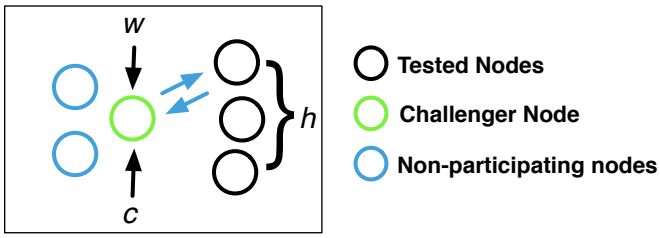
- The Simultaneous Receiver Test is based on the assumption that nodes cannot simultaneously listen in more than one channel



technology from seed

inesc id lisboa

The Receiver Test is a RRT(K,1,1)



- *h* is limited by the number of available channels K
- *c* is one, since the challenger needs to send a challenge on one of the channels
- *w* is one since only the challenger can extract information from the test (no other node knows the chosen channel)

Road Map

technology from seed

inesc id lisboa

Introduction
Radio Resource Tests
➢ Analysis
Summary

Radio Resource Tests - Analysis

technology from seed

inesc id lisboa

We compared the tests using the following metrics

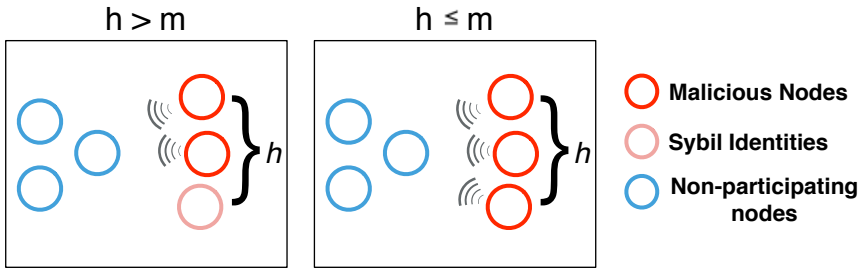
- Vulnerability to collusion
- Message cost
- Resource consumption
- Synchronization requirements
- Number of messages needed to achieve a desired probability of detection

Analysis – Optimized Sender Test – Vulnerability to collusion

technology from seed

inesc id lisboa

Vulnerability to collusion

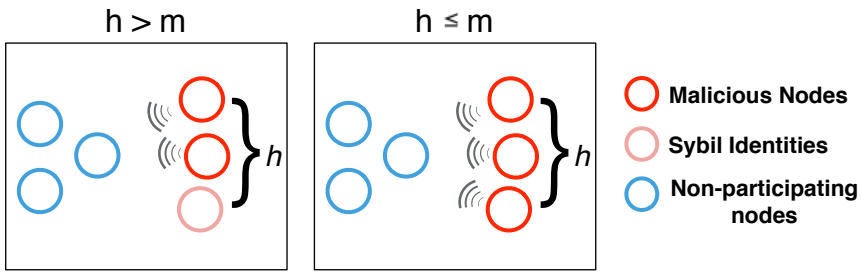


Analysis – Optimized Sender Test – Vulnerability to collusion

technology from seed

inesc id lisboa

Vulnerability to collusion



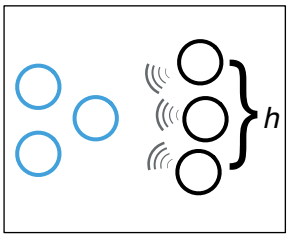
The Optimized Sender Test Handles at most $h - 1$ colluding malicious nodes (m)

Analysis – Optimized Sender Test – Message Cost

technology from seed

inesc id lisboa

Message Cost



Tested Nodes

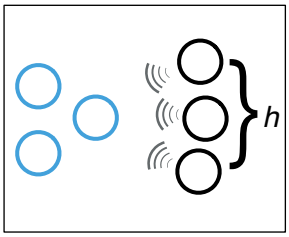
Non-participating nodes

Analysis – Optimized Sender Test – Message Cost

technology from seed

inesc id lisboa

Message Cost



Tested Nodes

Non-participating nodes

In the Optimized Sender Test, tested nodes send a total of *h* messages per round

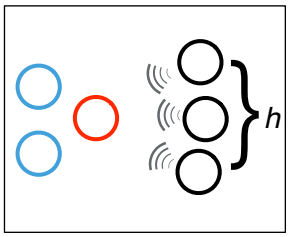
Analysis – Optimized Sender Test – Resource Consumption

technology from seed

inesc id lisboa

Resource Consumption (DoS Opportunity)

Malicious Tester



- Malicious Nodes
- Tested Nodes
- Non-participating nodes

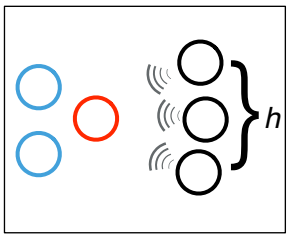
Analysis – Optimized Sender Test – Resource Consumption

technology from seed

inesc id lisboa

Resource Consumption (DoS Opportunity)

Malicious Tester



- Malicious Nodes
- Tested Nodes
- Non-participating nodes

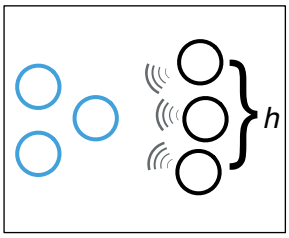
In the Optimized Sender Test, when there is a malicious tester, $\Delta = rh - 1$.

Analysis – Optimized Sender Test – Synchronization Requirements

technology from seed

inesc id lisboa

Synchronization Requirements



Tested Nodes

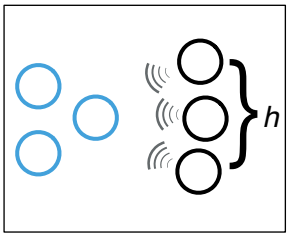
Non-participating nodes

Analysis – Optimized Sender Test – Synchronization Requirements

technology from seed

inesc id lisboa

Synchronization Requirements



Tested Nodes

Non-participating nodes

In the Optimized Sender Test, tested nodes are required to transmit simultaneously

Analysis – Comparison Table

technology from seed

inesc id lisboa

Metric	Tests		
	Optimized Sender Test	Receiver Test	Collision Test
Collusion	h - 1	h - 1	1
Message Cost	h	2	2
Resource Consumption (malicious tester)	rh -1	0	r
Synchronization	Strong	Strong	Weak

Analysis – Comparison Table

technology from seed

inesc id lisboa

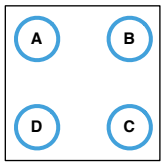
Metric	Tests		
	Optimized Sender Test	Receiver Test	Collision Test
Collusion	h - 1	h - 1	1
Message Cost	h	2	2
Resource Consumption (malicious tester)	rh -1	0	r
Synchronization	Strong	Strong	Weak

Analysis – Testing a Population of Nodes

technology from seed

inesc id lisboa

Testing a group of nodes



Tested Nodes

Tester Nodes

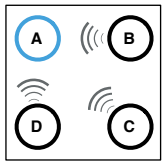
Every node in the one-hop neighborhood has to test every other node

Analysis – Testing a Population of Nodes

technology from seed

inesc id lisboa

Testing a group of nodes



Tested Nodes

Tester Nodes

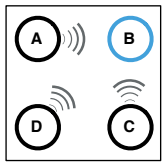
Every node in the one-hop neighborhood has to test every other node

Analysis – Testing a Population of Nodes

technology from seed

inesc id lisboa

Testing a group of nodes



Tested Nodes

Tester Nodes

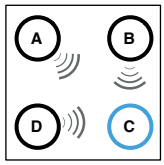
Every node in the one-hop neighborhood has to test every other node

Analysis – Testing a Population of Nodes

technology from seed

inesc id lisboa

Testing a group of nodes



Tested Nodes

Tester Nodes

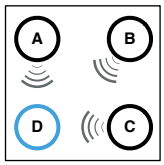
Every node in the one-hop neighborhood has to test every other node

Analysis – Testing a Population of Nodes

technology from seed

inesc id lisboa

Testing a group of nodes



Tested Nodes

Tester Nodes

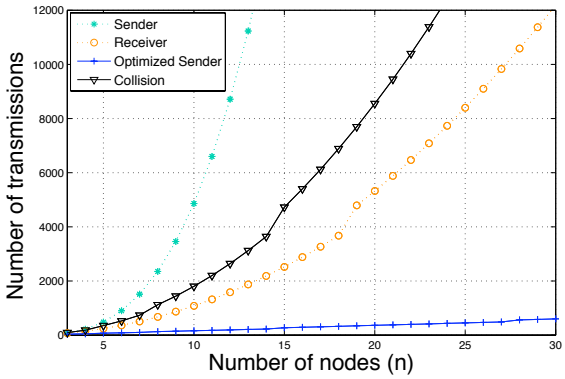
Every node in the one-hop neighborhood has to test every other node

Radio Resource Tests - Performance

technology from seed

inesc id lisboa

Performance in number of messages



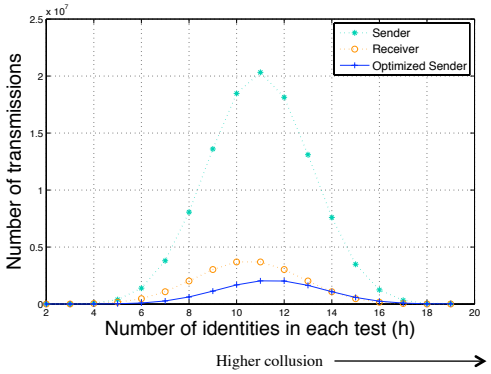
For a probability of sybil detection of 0.95.

Radio Resource Tests - Performance

technology from seed

inesc id lisboa

Performance with collusion tolerance



For a network with 20 nodes and a probability of sybil detection of 0.95.

Radio Resource Tests – Application Scenarios

technology from seed

inesc id lisboa

Application Scenarios

Test	Best Performance Context
Optimized Sender Test	No DoS threat
Receiver Test	High collusion and/or DoS threat
Collision Test	One Channel

Road Map

technology from seed

inesc id lisboa

Introduction
Radio Resource Tests
Analysis
➢ Summary

Summary

technology from seed

inesc id lisboa

- Radio Resource Tests are a viable mechanism for detecting sybil identities in Wireless ad hoc Networks
- We presented two new RRTs and an optimization to an existing RRT
- We presented a framework to compare the RRTs
- We analyzed all the tests both in isolation, and when used to test a one-hop neighborhood.
- We have shown that each test is best adapted to a specific scenario, which we described.


technology
from seed
inesc id
lisboa