A Novel *k*-Parent Flooding Tree for Secure and Reliable Broadcasting in Sensor Networks
ICC 2007

Presented by L. C. Yang

2007/12/06

Outline

- Introduction
- Related Work
- k-FTM
- Simulation
- Conclusion

Introduction

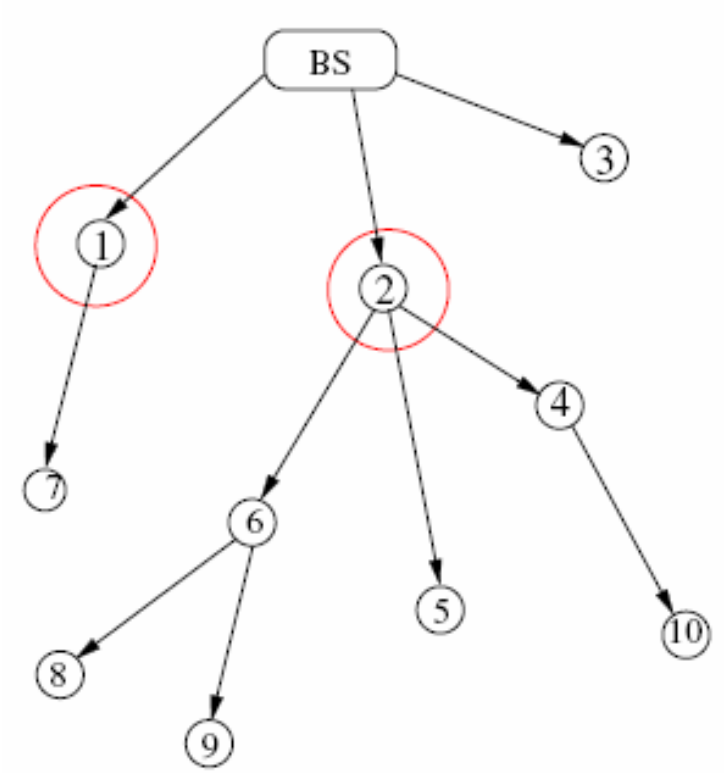
- Broadcast has two important metrics:

  -Reliability

  -Security

- Unlike reliability, very few researchers have addressed the security metric.

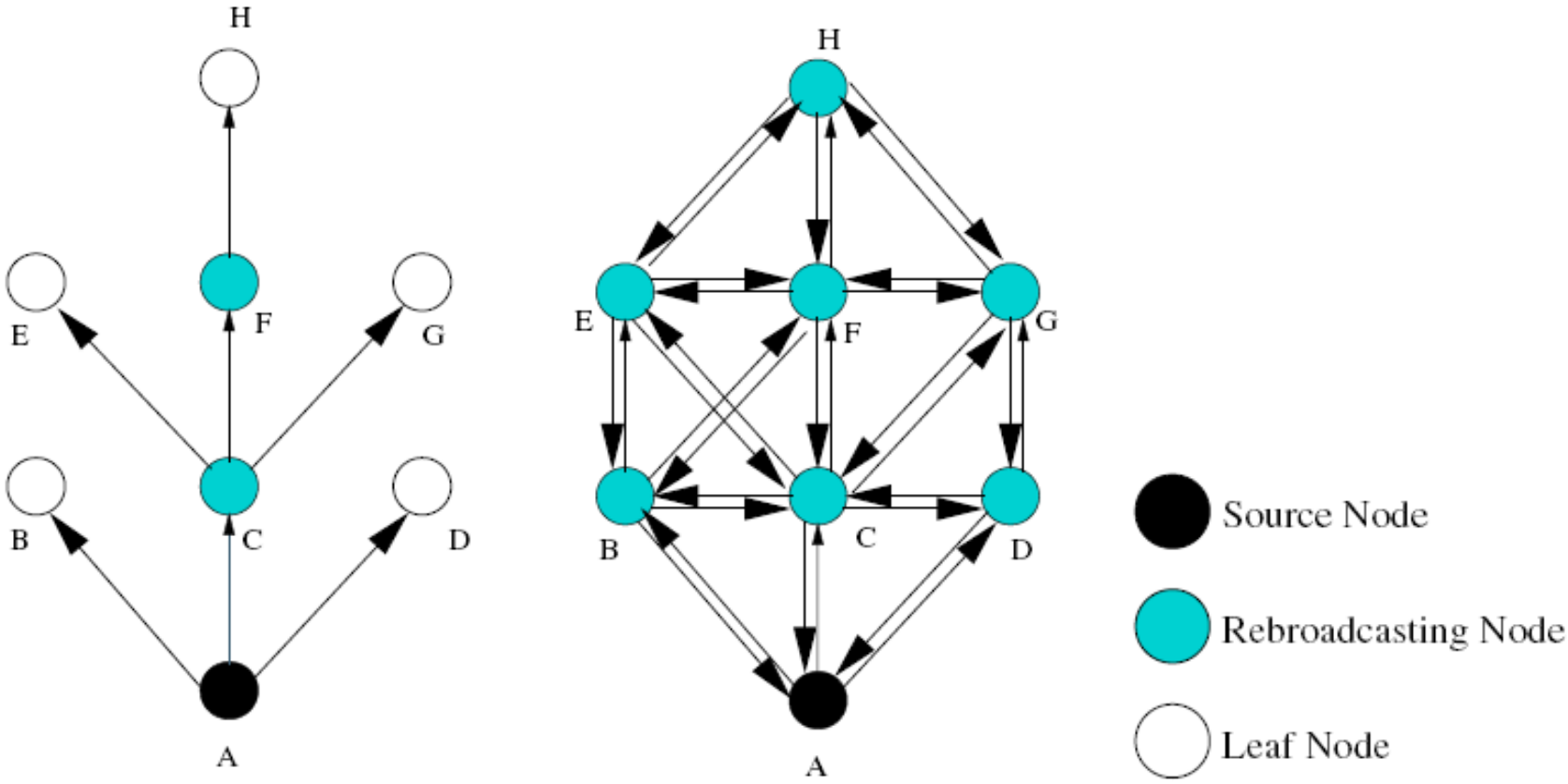
- **Denial-of-Broadcast Message attacks (DoBM)**



Blind flooding

- Advantage
  - -reliable
- Disadvantage
  - -high redundancy
  - -waste energy
  - -broadcast storm problem

Flooding Tree Model (FTM)



Flooding Tree Model (FTM)

- Advantage

  -Attacker can be immediately detected.

- Disadvantage

  -The attacker can cripple a substantial portion of the network by compromising a single node with a large subtree.

- k-FTM is proposed to retain the high detection rate of FTM but at the same time achieve a reliability close to blind flooding.

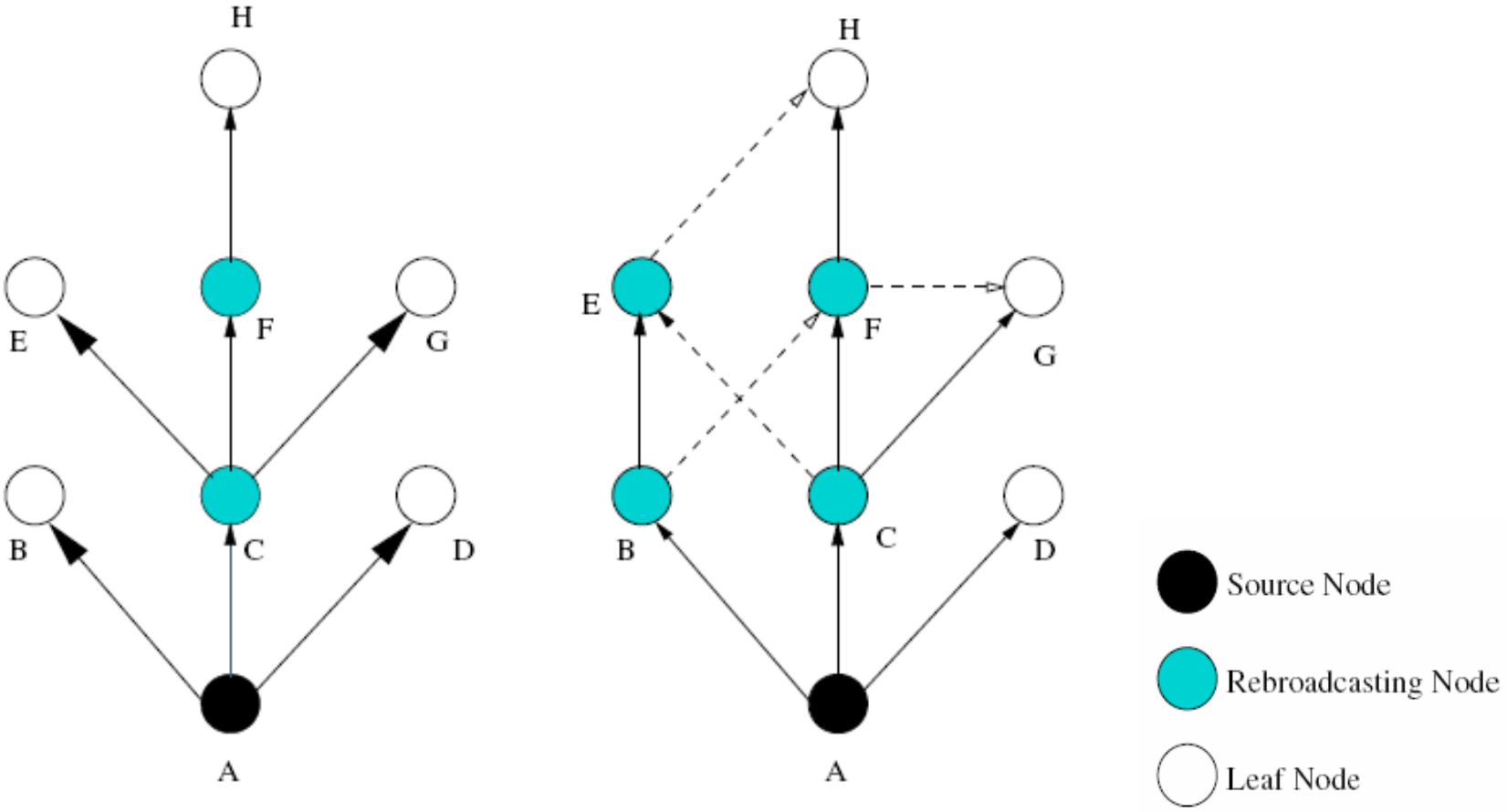
Related Work

- Internal Node Based Broadcasting algorithm
- Secure Implicit Sampling(SIS)

Attacker Model and Assumptions

- The attacker's sole motive is to block the broadcast message to as many nodes as possible.
- ACKs are encrypted using pairwise key between each node and the base station.
- Uniform transmission range and the rate of message propagation is uniform.

k-FTM


H
E
F
G
B
C
D
A
H
E
F
G
B
C
D
A
Source Node
Rebroadcasting Node
Leaf Node

Working of k-FTM

- The base station maintains a malicious counter $count^{i}_{mal}$ for each node i in the network to record its misbehavior.
- The base station also maintains a global counter,$count_{glo}$, that records the overall level of misbehavior in a network.
- The base station know the topology of the constructed k-FTM.

Working of k-FTM

- After k-FTM is constructed, the base station broadcasts encrypted messages, encoding in them which nodes are expected to acknowledge.

- If the nodes are expected to acknowledge,they send back an ACK.

Working of k-FTM

- The ACK of a node contains a k-bit field. If none of the *k*-parents of the sampled node *i* forward the message, then the base station will fail to receive an ACK from that node.
- If more than one non-ACK sampled nodes have same parent node i then i's $count^{i}_{mal}$ incremented and so is the global malicious counter $count_{glo}$.

Working of k-FTM

- The base station reconstructs the tree under three circumstances:

  - $count_{glo}$ exceeds the threshold.

  - $count^{i}_{mal}$ exceeds the node misbehavior threshold.

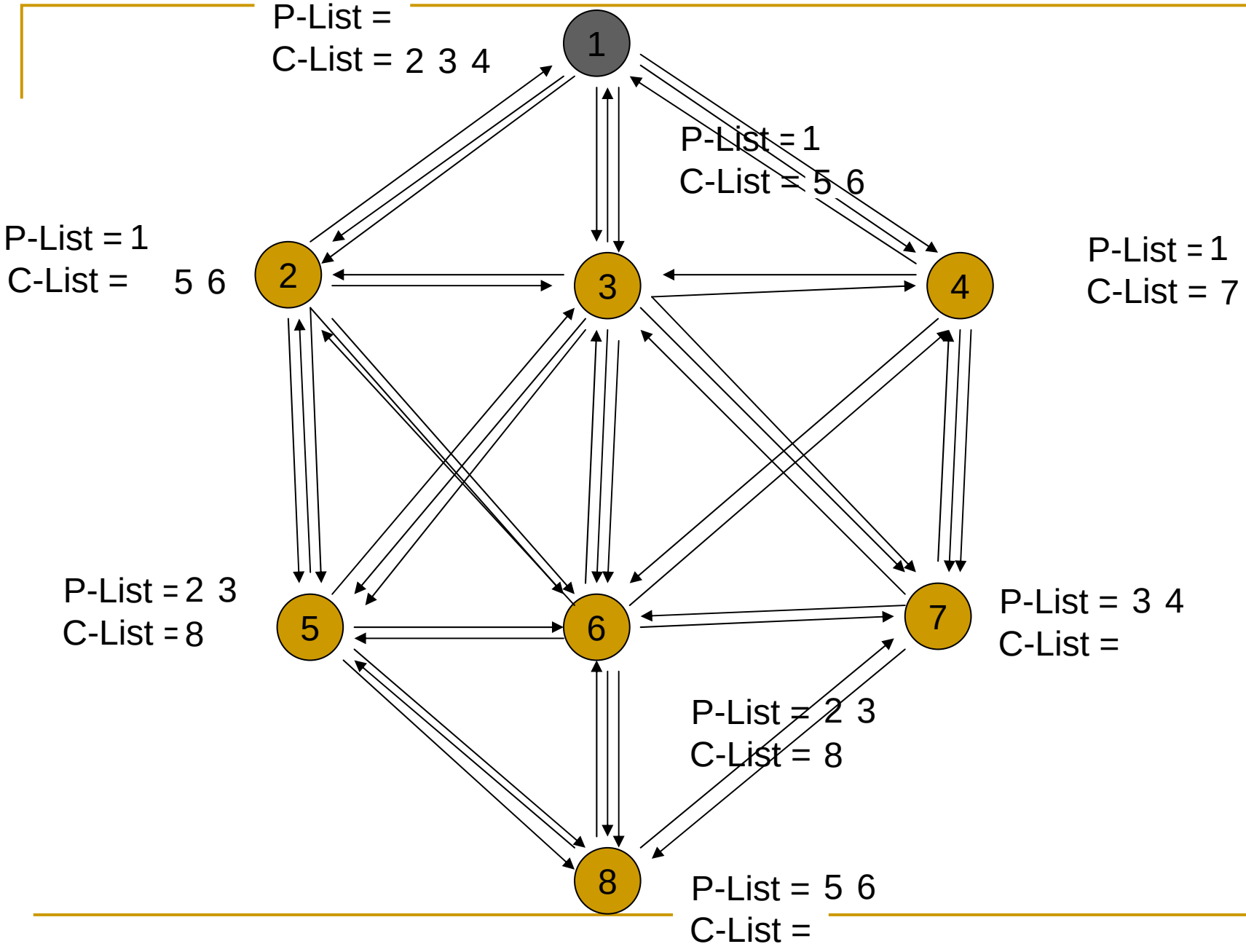
  - $Timeout_{tree}$ occurs.

Method for construct k-FTM

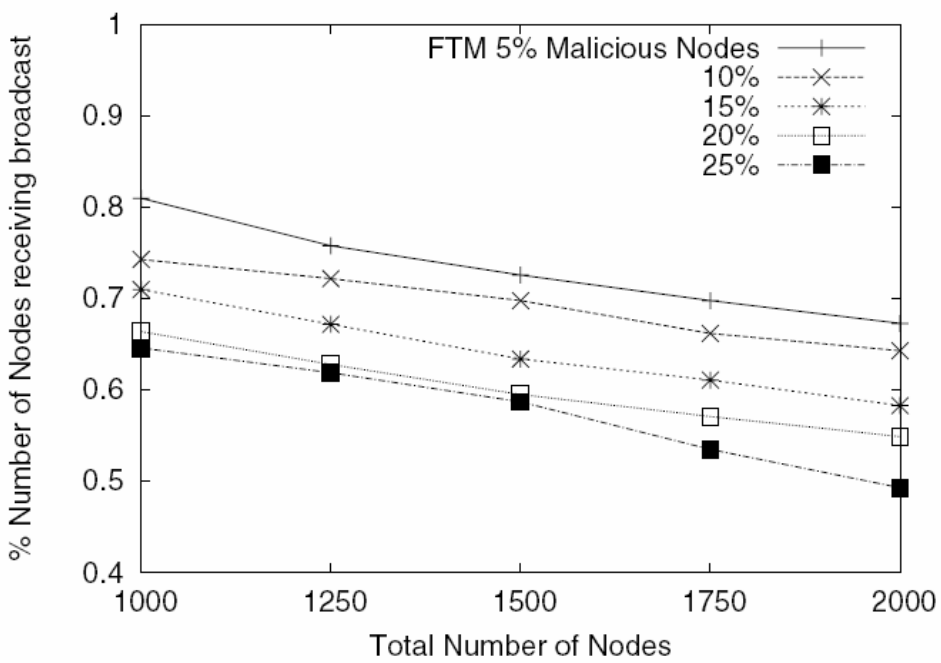
- Fastest First k-parents.

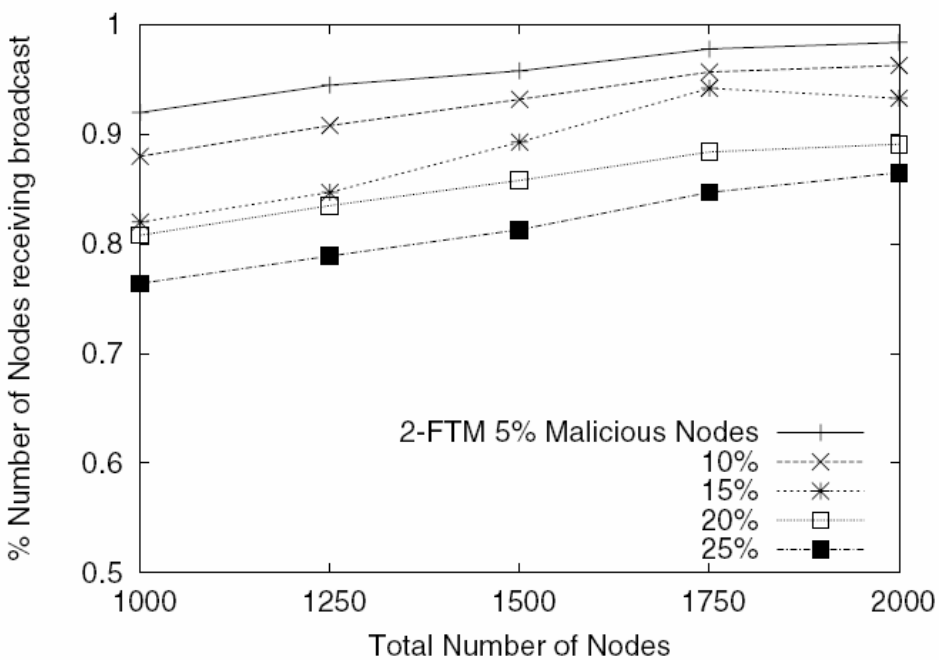
  A node acknowledges as child to the first *k* nodes from which it receives the *Hello* message.
- Disjoint Path k-parents.

- Improved Disjoint Path k-parents.

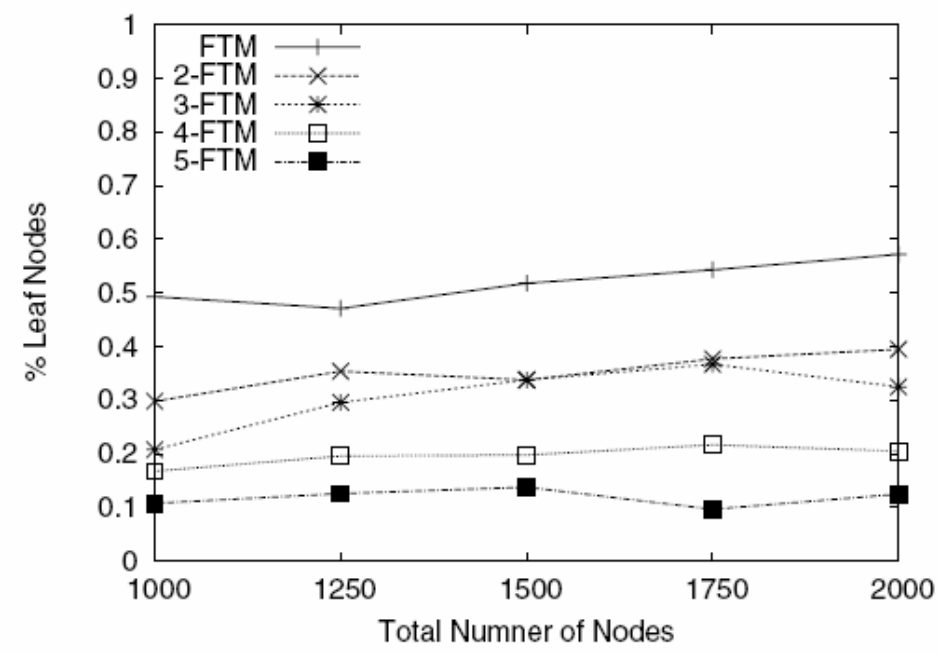

P-List =
C-List = 2 3 4
1
P-List = 1
C-List = 5 6
P-List = 1
C-List = 5 6
2
3
4
P-List = 1
C-List = 7
P-List = 2 3
C-List = 8
5
6
7
P-List = 3 4
C-List =
P-List = 2 3
C-List = 8
8
P-List = 5 6
C-List =

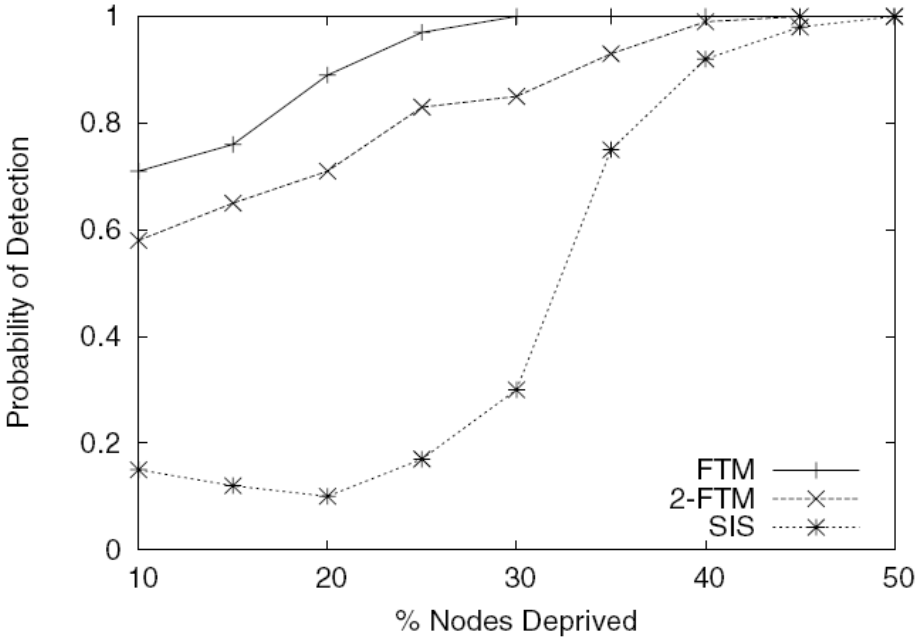
Simulation


FTM 5% Malicious Nodes
10%
15%
20%
25%
% Number of Nodes receiving broadcast
Total Number of Nodes
1
0.9
0.8
0.7
0.6
0.5
0.4
1000
1250
1500
1750
2000


2-FTM 5% Malicious Nodes
10%
15%
20%
25%
% Number of Nodes receiving broadcast
Total Number of Nodes
1
0.9
0.8
0.7
0.6
0.5
1000
1250
1500
1750
2000

Simulation


FTM
2-FTM
3-FTM
4-FTM
5-FTM
% Leaf Nodes
Total Numner of Nodes
1000
1250
1500
1750
2000
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1


Probability of Detection
% Nodes Deprived
FTM
2-FTM
SIS
10
20
30
40
50
0
0.2
0.4
0.6
0.8
1

Conclusion

- *k*-parent Flooding Tree Model to efficiently address both reliability and security metrics of broadcasting in wireless sensor networks.