Adaptive CUSUM Algorithm to Detect Malicious Behaviours in Wireless Mesh Networks

Presented by Badis Hammi

Authors : Juliette Dromard (1), Rida Khatoun (2) and Lyes Khoukhi (1)

(1) University of Technology of Troyes - Troyes, France
(2) Telechom ParisTech - Paris, France

June 30, 2014

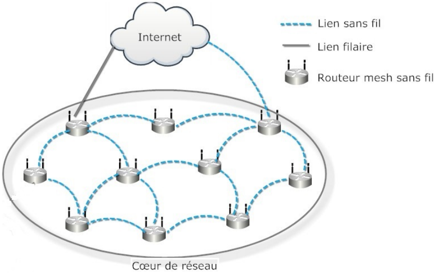
Contents

1. Introduction and problematic
   - Wireless Mesh Networks
   - Problematic
2. Existing solutions
   - Trust systems
   - Limits of trust systems
3. Our trust system
   - Modelization of the packet rate not overheard
   - Our IDS
   - Trust computation
4. Evaluation
5. Conclusion

Wireless Mesh Networks

Many advantages

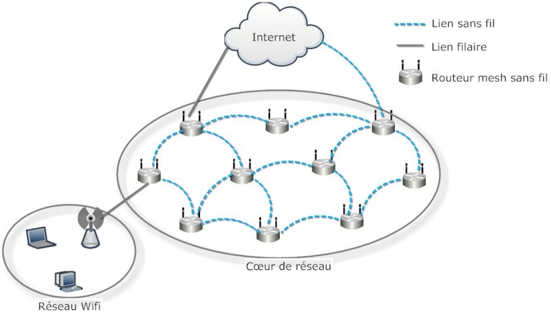
- Low cost network, easy and fast to deploy and maintain, and can interconnect heterogeneous networks



Wireless Mesh Networks

Many advantages

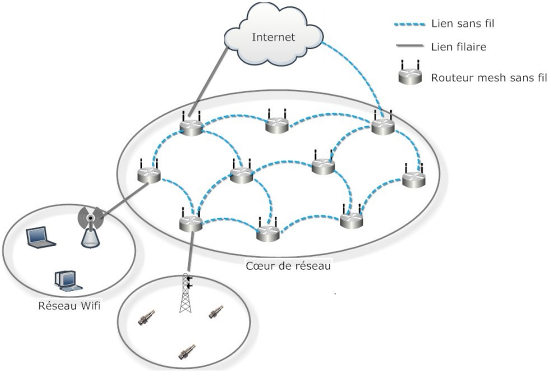
- Low cost network, easy and fast to deploy and maintain, and can interconnect heterogeneous networks



Wireless Mesh Networks

Many advantages

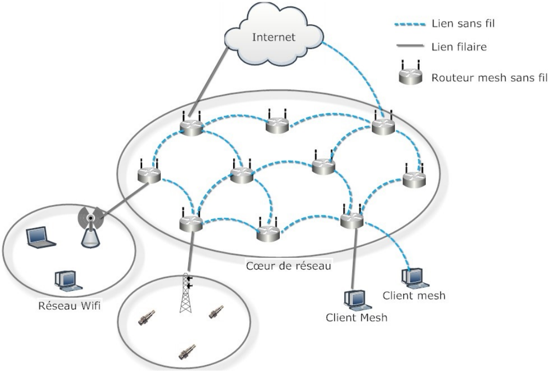
- Low cost network, easy and fast to deploy and maintain, and can interconnect heterogeneous networks



Wireless Mesh Networks

Many advantages

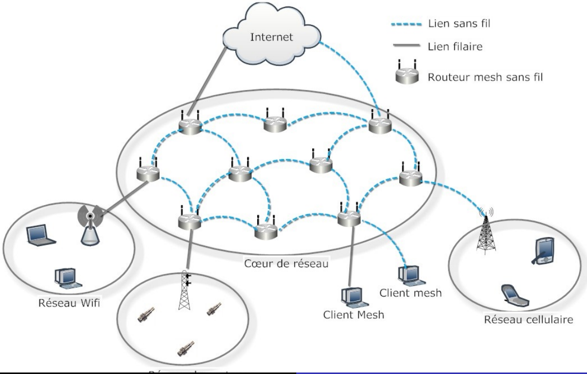
- Low cost network, easy and fast to deploy and maintain, and can interconnect heterogeneous networks



Wireless Mesh Networks

Many advantages

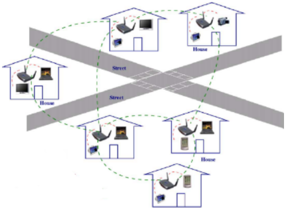
- Low cost network, easy and fast to deploy and maintain, and can interconnect heterogeneous networks

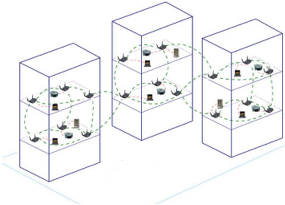


Wireless Mesh Networks

Many possible applications

- Replace actual networks (MAN, network company...)

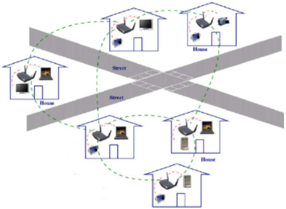


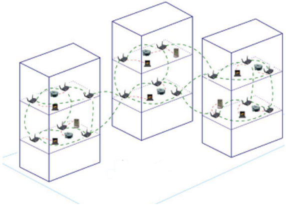


Wireless Mesh Networks

Many possible applications

- Replace actual networks (MAN, network company...)





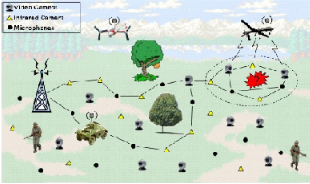
Remark

- Deployed with success as a metropolitan network (west of London, Houston)

Wireless Mesh Networks

Many possible applications

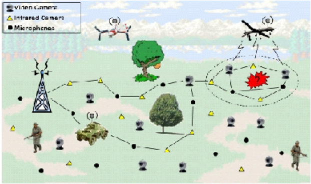
- Replace actual networks (MAN, network company...)
- Offer connexion in areas where actual networks are too expansive, damaged or hard to deploy



Wireless Mesh Networks

Many possible applications

- Replace actual networks (MAN, network company...)
- Offer connexion in areas where actual networks are too expansive, damaged or hard to deploy



Remark

- Used as a complement of actual networks

Problematic

In terms of security

- Routers can be physically or logically captured
- Only one malicious node can deteriorate the whole network
    - Grayhole, Blackhole, send false routing information, modify messages...

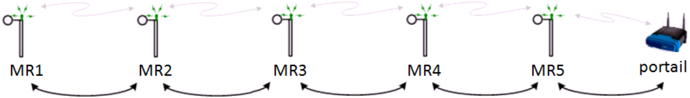


Figure: WMN made up of five mesh routers

Problematic

In terms of security

- Routers can be physically or logically captured
- Only one malicious node can deteriorate the whole network
  - Grayhole, Blackhole, send false routing information, modify messages...

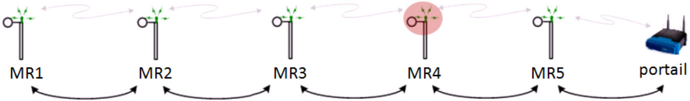


Figure: Blackhole : a malicious mesh router which does not forward any packet

Problematic

In terms of security

- Routers can be physically or logically captured
- Only one malicious node can deteriorate the whole network
  - Grayhole, Blackhole, send false routing information, modify messages...

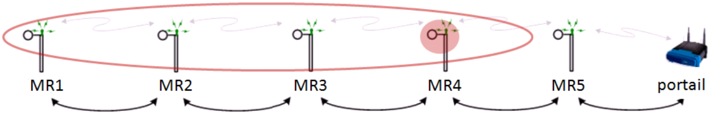


Figure: Only MR5 can still send data on the Internet

1. Introduction and problematic
   - Wireless Mesh Networks
   - Problematic
2. Existing solutions
   - Trust systems
   - Limits of trust systems
3. Our trust system
   - Modelization of the packet rate not overheard
   - Our IDS
   - Trust computation
4. Evaluation
5. Conclusion

Security issues in WMNs

- Easy to capture mesh routers
- Disruption of the whole network with only one malicious node
- Solutions based on cryptographic materials
  - Protect the network against external attacks (do not posses the adequate cryptographic material) but not internal ones

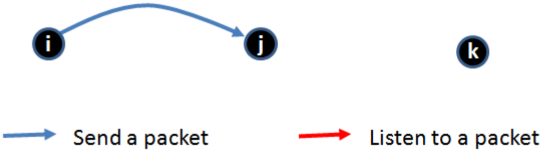
Solution : Trust systems

- Implement on every node a trust module
  - Monitor their neighboring nodes
  - Assign to each neighbor a level of trust which reflects its behavior
- Isolate nodes which have a low level of trust and/or urge them to cooperate

Trust system

Neighboring's nodes monitoring

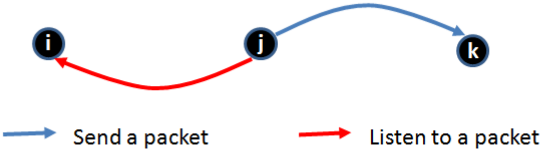
- Generally performed by the Watchdog IDS
  - Implemented on every node of the network
  - Check whether its neighbors forward correctly its data
  - Record the rate of packets its neighbors forward correctly
  - Detect Greenhole and Blackhole
- Compute, thanks to the data collected by Watchdog, the trust they have in each of their neighbors



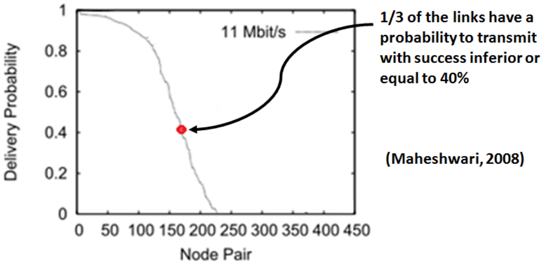
Trust system

Neighboring's nodes monitoring

- Generally performed by the Watchdog IDS
  - Implemented on every node of the network
  - Check whether its neighbors forward correctly its data
  - Record the rate of packets its neighbor forwards correctly
  - Detect Greenhole and Blackhole
- Compute, thanks to the data collected by Watchdog, the trust they have in each of their neighbors



Trust systems



1/3 of the links have a probability to transmit with success inferior or equal to 40%

(Maheshwari, 2008)

Show the number of node pairs in an experimental 802.11b WMN which delivery success probability is inferior or equal to a certain threshold

Limit of Trust systems based on the Watchdog IDS

- Important packet loss rate on mesh networks' links
- Assign unfairly a low level of trust to a node
    - Lead to an important number of false positives

1. Introduction and problematic
   - Wireless Mesh Networks
   - Problematic
2. Existing solutions
   - Trust systems
   - Limits of trust systems
3. Our trust system
   - Modelization of the packet rate not overheard
   - Our IDS
   - Trust computation
4. Evaluation
5. Conclusion

Objectives

- Detect bad nodes in presence of packet loss over WMN's links
  - Bad node : a malicious, selfish or faulty node
- The aim of this detection
  - Decrease the number of false positives compared to existing solutions
  - For further isolate bad nodes and/ or urge them to cooperate

Our solution

- Trust system based on Watchdog
- The rate of packets a node should overhear from one neighbor must be known in advance
- Compare the rate of packets it overhears its neighbors forwarding with the rate of packets it should overhear
- Propose a method to compute the level of trust of each node

Modelization of the packet rate not overheard

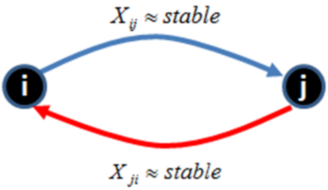
Studies on links' packet loss rate

- (Aguayo et Al., 2004) show via experimental measurements that
  "averaging over long time intervals smoothes out fluctuations" of links' packet loss rate
- (Jiang et Al., 2010) show that via experiments on 802.11b wireless links that links' quality
  "at different times are more or less similar and that the packet loss rates with same distance almost follow the same distribution, no matter the traffic is heavy or not"

Modelization of the packet rate not overheard

Modelization of the packet rate not overheard

- Assume that the packet loss rate at a link is quite stable over time
  - Packet rate that a node does not overhear its neighbor forwarding, when this latter is good, is stable
  - Packet rate that a node does not overhear its neighbor forwarding, when this latter is bad, changes

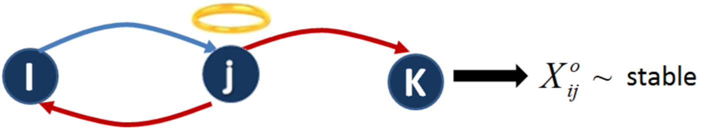


X_{ij} Packet loss rate over the link *(i,j)*

Modelization of the packet rate not overheard

Modelization of the packet rate not overheard

- Assume that the packet loss rate at a link is quite stable over time
    - Packet rate that a node does not overhear its neighbor forwarding, when this latter is good, is stable
    - Packet rate that a node does not overhear its neighbor forwarding, when this latter is bad, changes



X_{ij}^{o} Packet rate that node i does not overhear j forwarding to k

Our IDS

Our IDS 's requirements

- Each node knows at the network deployment, the mean and the standard deviation of the packet rate it may not overhear for each of its neighbors when they are honest

Our IDS

- Implemented on each node
- Monitor the packet rate not overheard from each neighbor
- Perform periodically the CUSUM method to check whether the packet rate no overheard from its neighbor changes
  - if CUSUM does not launch any alert, it records that the neighbor had a good behavior during the last interactions
  - if CUSUM launches an alert, it records that the neighbor had a bad behavior during the last interactions

Trust computation

Trust computation

- Consider the nodes' past behavior
- More a node's trust is close to 1 (0) and more its trust is good (bad)

$$R_{ij} = \beta R_{ij}^{old} + (1 - \beta) a_{ij}$$

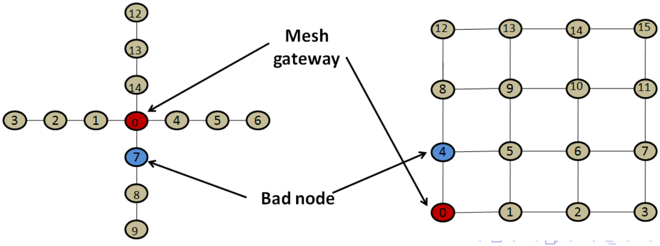
- β : weight of the past interactions
- R_{ij}^{old} : trust that node i has about node j
- a_{ij} : result obtained from the IDS
    - equals 1 if node i's last interactions with j were good
    - equals 0 otherwise

1. Introduction and problematic
   - Wireless Mesh Networks
   - Problematic
2. Existing solutions
   - Trust systems
   - Limits of trust systems
3. Our trust system
   - Modelization of the packet rate not overheard
   - Our IDS
   - Trust computation
4. Evaluation
5. Conclusion

Evaluation

Evaluation on ns2

- Show that our solution assigns to nodes a trust which reflects their real behavior and not the quality of their links
- Compare our solution with a trust system based on Watchdog which does not consider packet loss rate (Sen, 2010)
- Send a flow of rate 20kb/s (each node)


Mesh gateway
Bad node

Parameters of simulation

Level	**Parameter**	**Value**
Signal propagation	Two-ray-ground model	
Packet loss rate	Mean of the rate	$U(0, 0.5)$
	Sandard deviation of the rate	$U(0, 0.5)$
Physical	Rate	54Mbit/s
	Frequency	$2, 4GHz$
	PLCP preamble	$20\mu s$
MAC	CSMA/CA	

- In the following, we compare our solution with different percentage p of packets the bad node drops.

Evaluation with a cross topology

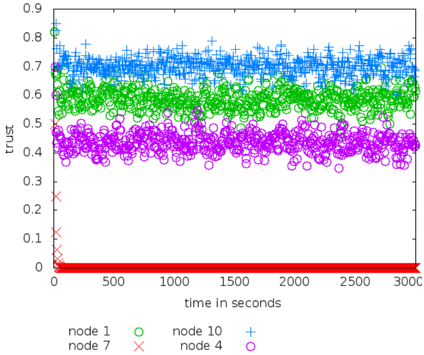


Figure: The reference solution when $p = 100\%$

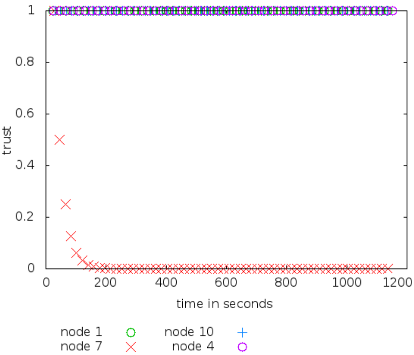


Figure: Our solution when $p = 100\%$

Evaluation with a cross topology

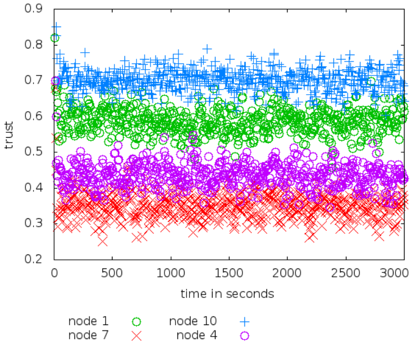


Figure: The reference solution when $p = 50\%$

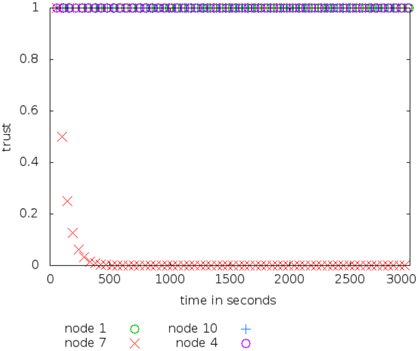


Figure: Our solution when $p = 50\%$

Evaluation with a cross topology

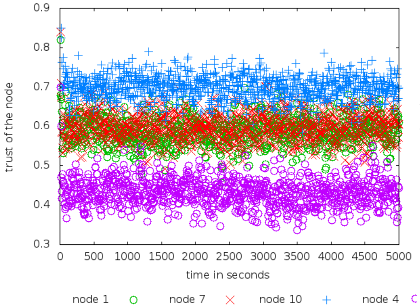


Figure: The reference solution when $p = 20$ %

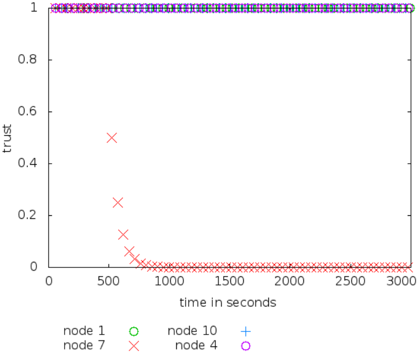


Figure: Our solution when $p = 20$ %

Context

- Security issues in WMNs
- Reputation systems may solve them
- May launch false positives due to packet loss on wireless links

Our trust reputation system

- Modelization of the packet loss rate over links as stable over time
- IDS based on the CUSUM method to detect change in the packet rate not overheard from one neighbor
- Method to compute the trust of a node according to the IDS's feedback

Evaluation on ns2

- Compare our trust system to a generic one
- Show that our solution assigns a trust value which reflects nodes' real behavior and not the quality of their links
- Better detect bad nodes than existing solutions
- May take time to detect bad nodes

Future works

- Decrease the time needed to detect bad nodes
- Add a method to isolate and/ or urge bad nodes to cooperate
- Detect more attacks such as flooding, MAC disruption...