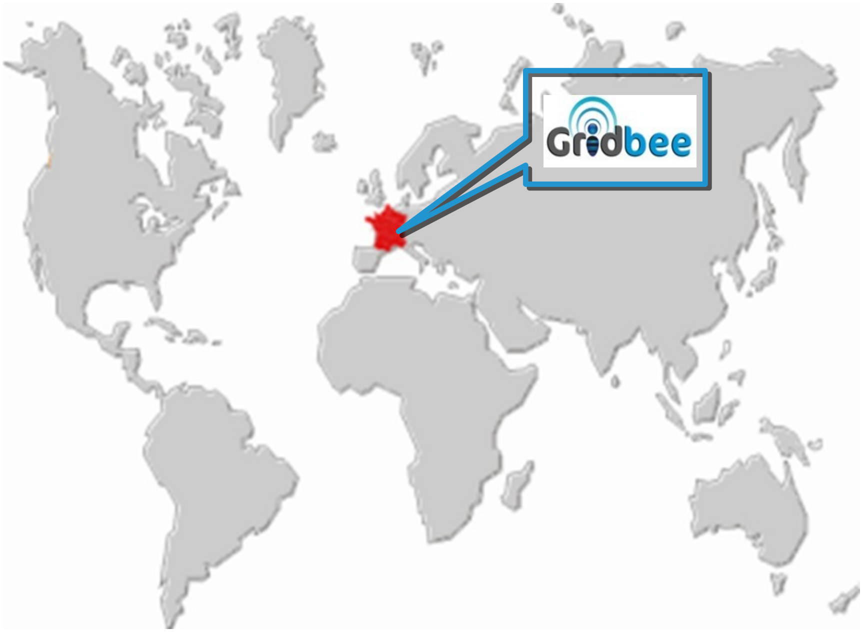
Modeling a node capture attack in a secure Wireless Sensor Networks

Authors: SMACHE Meriem: PhD Student, École des Mines de Saint-Étienne
meriem.smache@gridbeecom.com

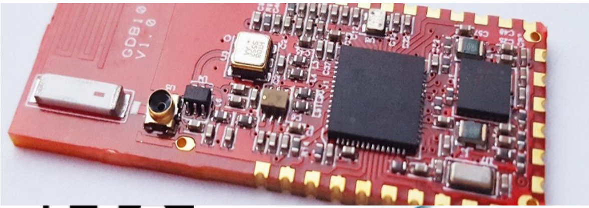
EL MRABET Nadia, TRIA Assia,
GIL-QUIJANO Javier, RIOU Emmanuel, CHAPUT Gregory.

PhD Student (15 /02/2016): Gridbee Communications



- ✓ Founded in 2014
- ✓ Located in Grasse, near Sophia Antipolis
- ✓ French Rivera
- ✓ WI SUN
- ✓ RF communication Module 802.15.4g

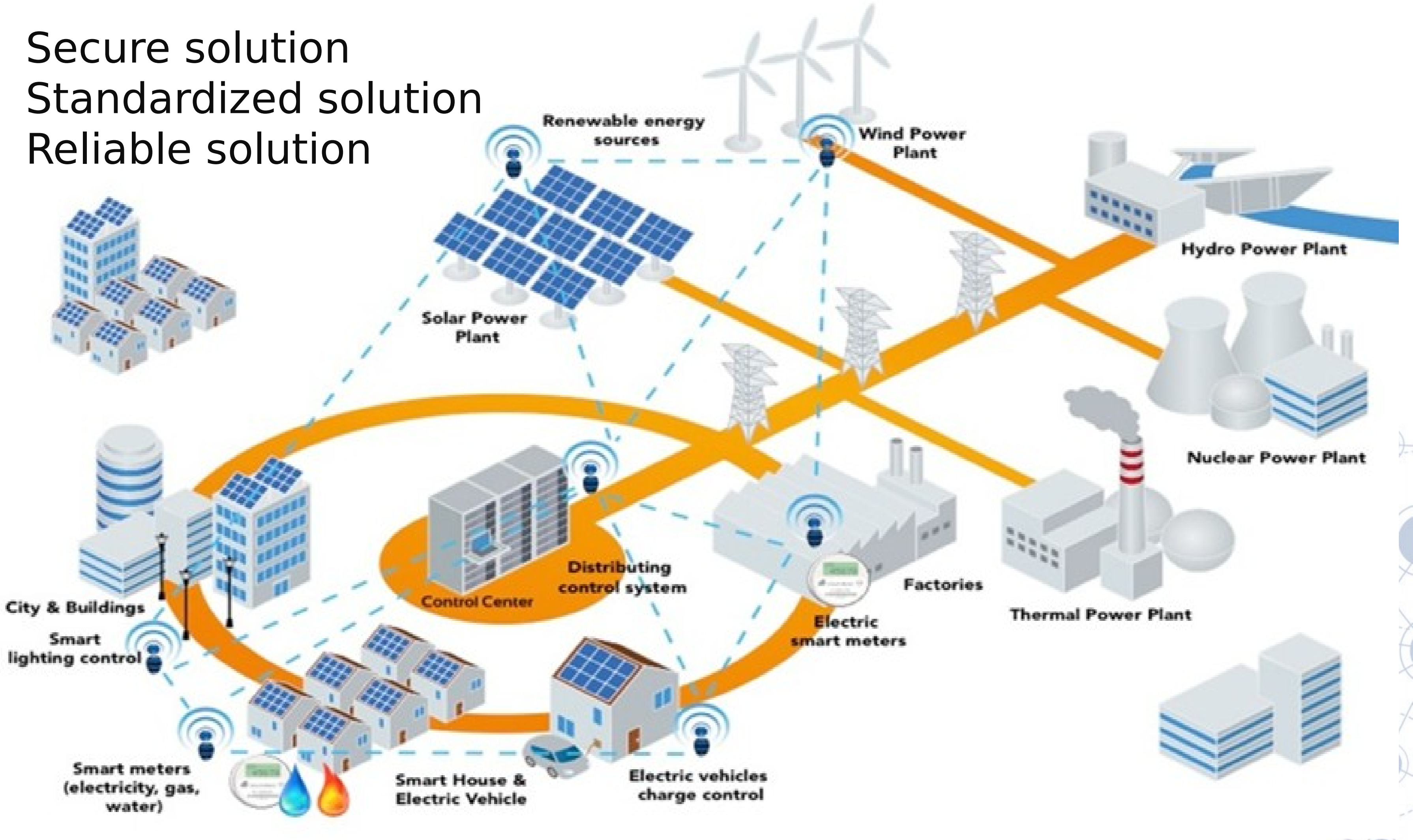
Team of 15 wireless communication experts



Wi SUN Alliance · cap energies · EUA energy&utilities alliance · SECURED COMMUNICATING SOLUTIONS A WORLD-CLASS CLUSTER · IEEE

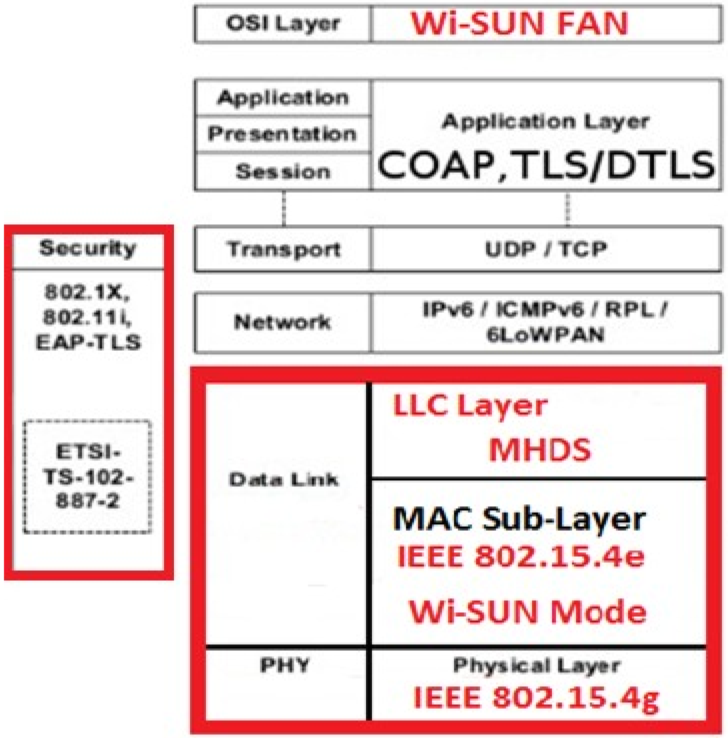
Wireless Mesh Network in Smart Grid

- ✓ Secure solution
- ✓ Standardized solution
- ✓ Reliable solution



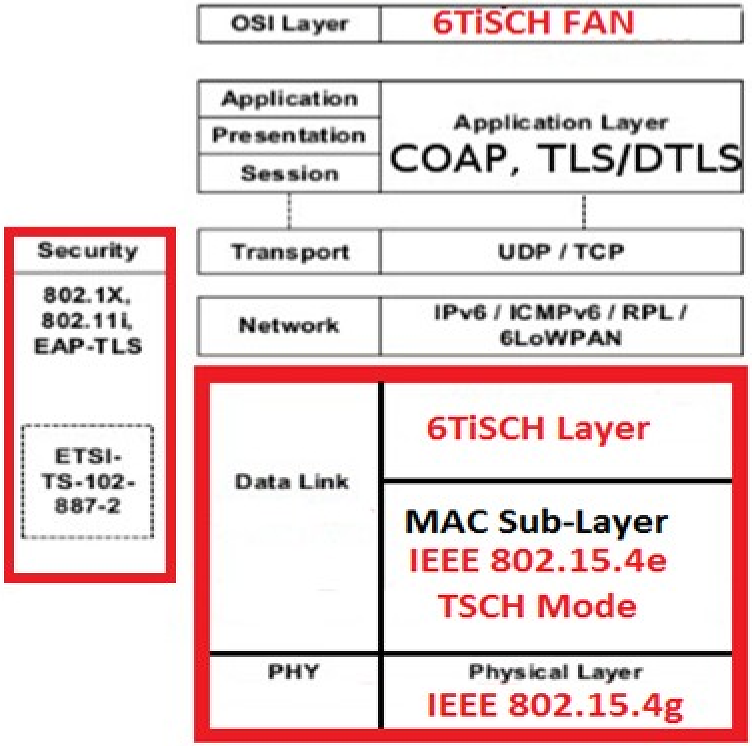
Security Model architecture (1)

Secure protocol stack for Wireless sensor network



OSI Layer	Wi-SUN FAN
Application Presentation Session	Application Layer COAP,TLS/DTLS
Transport	UDP / TCP
Network	IPv6 / ICMPv6 / RPL / 6LoWPAN
Data Link	LLC Layer MHDS
	MAC Sub-Layer IEEE 802.15.4e Wi-SUN Mode
PHY	Physical Layer IEEE 802.15.4g

Security
802.1X, 802.11i, EAP-TLS
ETSI-TS-102-887-2



OSI Layer	6TiSCH FAN
Application Presentation Session	Application Layer COAP, TLS/DTLS
Transport	UDP / TCP
Network	IPv6 / ICMPv6 / RPL / 6LoWPAN
Data Link	6TiSCH Layer
	MAC Sub-Layer IEEE 802.15.4e TSCH Mode
PHY	Physical Layer IEEE 802.15.4g

Security
802.1X, 802.11i, EAP-TLS
ETSI-TS-102-887-2

Wi-SUN: Standard (FAN)

6TiSCH: Industry 4.0

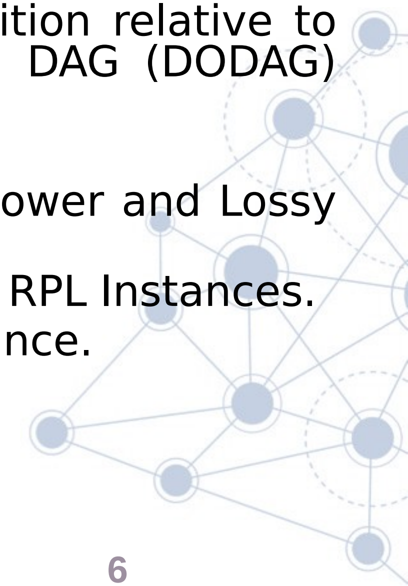
Security Model architecture (2)

We have two types of security mechanisms:

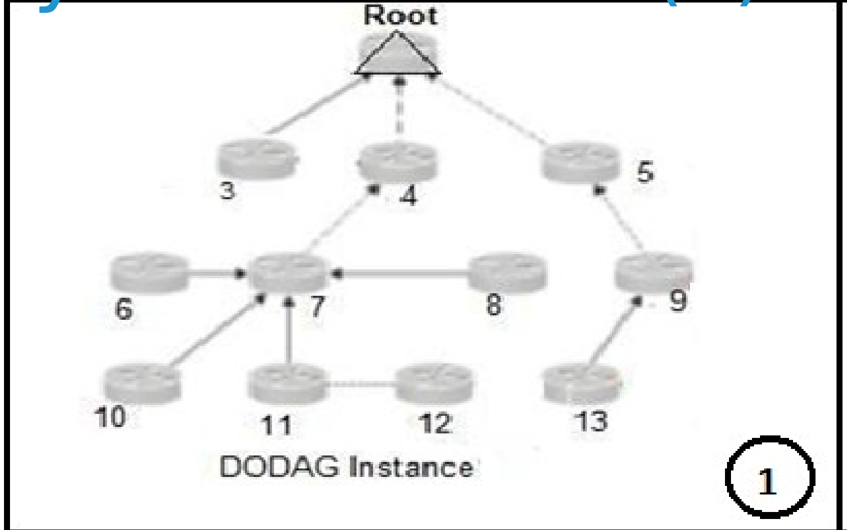
1. Non-Cryptographic mechanism: Synchronization
2. Cryptographic Mechanisms

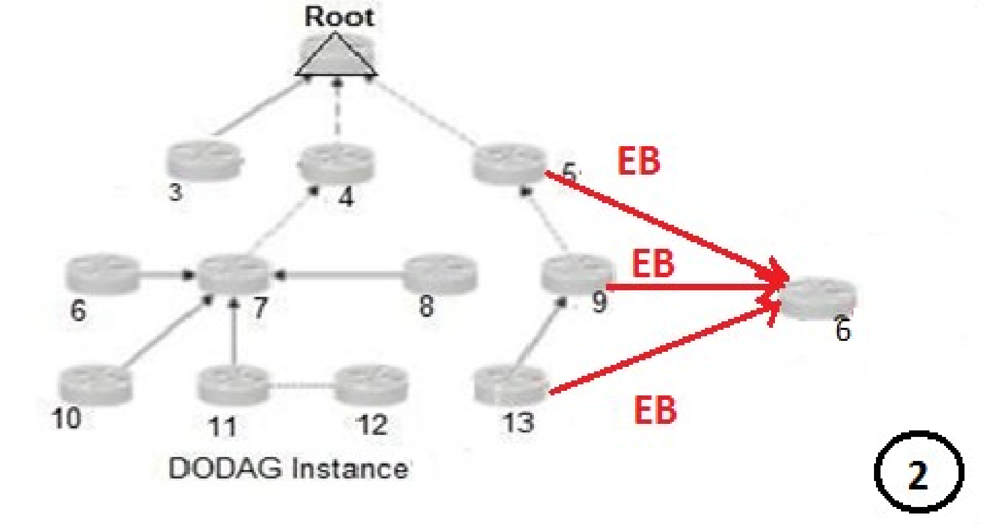
Non-Cryptographic mechanism: Synchronization (1)

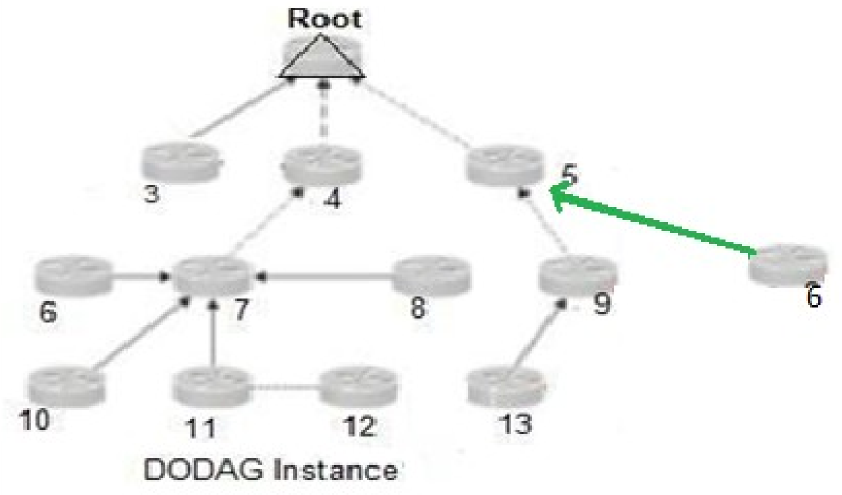
- Time Slotted Channel Hopping mode (TSCH):
  - Nodes must keep synchronization in the network by:
    - Broadcasting Enhanced Beacon (EB) frames every EB_Period.
    - Sending a keep-alive packet to their parents every keep-alive-Period.
  - EB frames contains information of synchronization such as 1-byte join-priority which:
    - Gives information to make a better decision of which node to join.
    - Represents node's rank, i-e, the node's individual position relative to other nodes with respect of the Destination-Oriented DAG (DODAG) root:
      - DODAG has part of the Routing Protocol for Low-Power and Lossy Networks (RPL) Instance.
      - Each RPL Instance operates independently of other RPL Instances.
      - RPL node must belong to one DODAG in a RPL Instance.



Non-Cryptographic mechanism: Synchronization (2)







- ✓ A node wishing to join the network listens for EBs.
- ✓ Since EBs are sent on all frequencies, the joining node can listen on any frequency until it hears an EB.
- ✓ The new node enables the TSCH mode of IEEE802.15.4e.

3

Cryptographic mechanism

Primary Key:

- Preloaded at the device.
- Decrypt EB message before joining the network.

Master key:

- Stored within the memory of the device.
- Secure EB messages and data frames exchanged after a successful authentication.
- Shared with the Authentication server (AS).

Network key:

- Control access to the mesh network.
- Updated when the Master Key expires.
- Secure the broadcast messages and MAC frames exchanged between nodes.

Individual key:

- Re-authentication.
- Shared with the AS.

The life time of keys=The life time the Pana Session.

⇨ ID, the master key, individual key are the support of cryptographic. security.

⇨

Threat an Attack Model

- Node capture is a kind of compound attack, resulting from the combination of **passive**, **active**, and **physical** attacks by an intelligent adversary:

a) **Short Attack**:
Attacker who can compromise a node in less than five minutes.

b) **Medium Attack:**
Attacker who can compromise a node in less than thirty minutes.

c) **Long Attack:**
Attacker who takes more than thirty minutes to compromise a node.

Attack Model: Assumptions

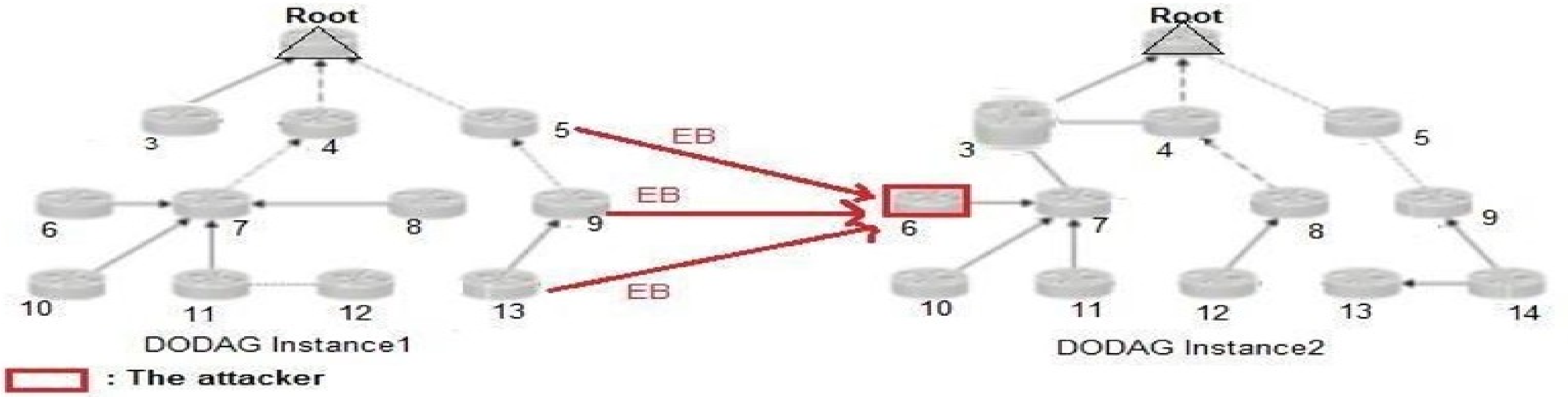
A1	▪ Network is active and formed: IEEE802.15.4e protocol stack. ▪ RPL node must belong to one DODAG in a RPL Instance ▪ Authentication per DODAG. ▪ Each node is assigned by an **ID and (Master-key/Derived keys)** saved in its memory.
A2	▪ Keys are periodically updated **every Pana_Session**. ▪ The Pana_Session-Period expires when the Master key needs to be updated or when the nodes asks for re-authentication.
A3	▪ Malicious node is part of another DODAG. ▪ It isn't able to send any Data frame or EB before authentication to the new DODAG and having a rank.
A4	▪ The attacker can extract information from the unencrypted Header of Data Frame. ▪ The malicious node **expects** the Pana_Session- Period: It calculates an average of this value with taking by using its Master-key used in its actual DODAG.

Threat an attack model

We have three fundamentals steps:

1. Step 1: Eavesdropping and the choice of victim nodes (Passive attack)
2. Step 2: Extract the individual key, the master key and the ID: (physical attacker)
3. Step 3: Cloning: (active attacker)

Step 1: Eavesdropping and the choice of victim nodes (Passive attack)



- The attacker seems like it wants to join a new DODAG, it initiates a channel scan over a given list of channels.

- The malicious node searches for all coordinators transmitting EB frames within a specific period.

- The choice of the victim node is based in two criteria:
  {the lowest join priority, the longest EB_Period}.

- A lower value of join priority indicates that connection to the beaconing device is a shorter route distance to the network root.

Step 2: Extract the individual key, the master key and the ID: (physical attacker)

- After the selection of the node, the goal of the attacker is to extract three fundamentals parameters of the victim node **{ID, Master key, Individual key}** by reading out the memory.

- The Challenge of our attacker is to keep the victim node synchronized to the network:

    - The victim node must send its EB and its keep_Alive packet in their exact time.

- **Solution:** This step is modelled as a generalized stochastic process. It is decomposed into three fundamental events:

{Ev1= attack the ID; Ev2= attack the Master-key; Ev3=attack the individual key} where:

Event_Period < EB_Period.

⇒ *Node_Capture_Attack_Period < Pana- Session_Period*

⇒

Step 3: Cloning: (active attacker)

- The adversary clones the victim-node by loading its cryptographic information, individual key, master key and ID onto generic node.
  - This clone is easily inserted into arbitrary locations within the same network.

- It isn't activated since the victim node asks for a re-authentication.

- It differentiates the Authentication Server from other victim-node's neighbors by:
  - Extracting the identity of nodes from the unencrypted payload of the exchanged messages.

- The Cloned node obliged the victim node to ask for a re-authentication by:
  - Capture victim's data packets and spoofing them to its neighbors.
  - Deleting all the acknowledgment packets sent to the victim node.

- The victim node is isolated, it asks the AS for a new re-authentication, but it is replaced by the cloned node by:
  - Dropping the request attack for authentication and communicating with AS by using the victim node`s ID.
- The cloned Node is authenticated in the network by using the victim’s individual Key.

Conclusion

- We presented a model of node capture attack in a secure wireless sensor networks.
  - We described typical security architecture for WSN.
  - We discussed the ability to decompose the attack in three steps:
    - Eavesdropping and the choice of victim nodes (Passive attack).
    - Extract the individual key, the master key and the ID: (physical attacker).
    - Cloning: (active attacker).

- We have already started to implement this attack by using Wireless mesh network provided by Gridbee Communications.

Thanks for your attention!

Meriem Smache, Nadia El Mrabet, Jesus-Javier Gilquijano, Assia Tria, Emmanuel Riou, Chaput Gregory: ***Modeling a node capture attack in a secure wireless sensor networks***. WF-IoT 2016: 188-193

Web site: http://www.gridbeecom.com

Contact: meriem.smache@gridbeecom.com