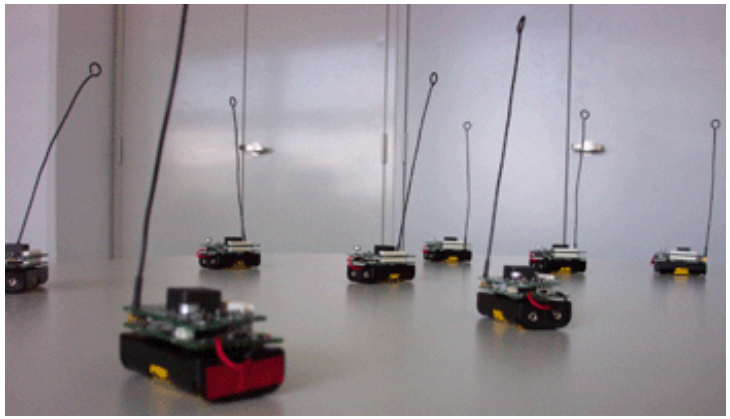
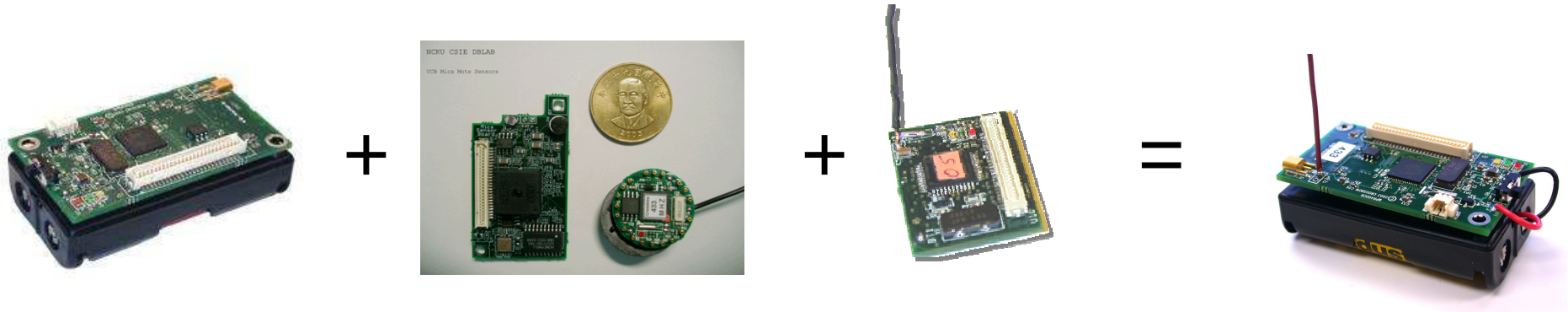
La Sécurité des Capteurs et Réseaux de Capteurs

Claude Castelluccia
PLANETE, INRIA
Juin 2008



Les Réseaux De Capteurs

- Les réseaux de capteurs sont:
  - Composés de plusieurs noeuds, déployés +/- aléatoirement, qui forment un réseau multi-saut
  - Chaque noeud est un capteur (température, pression, humidité, etc.) et un “routeur”



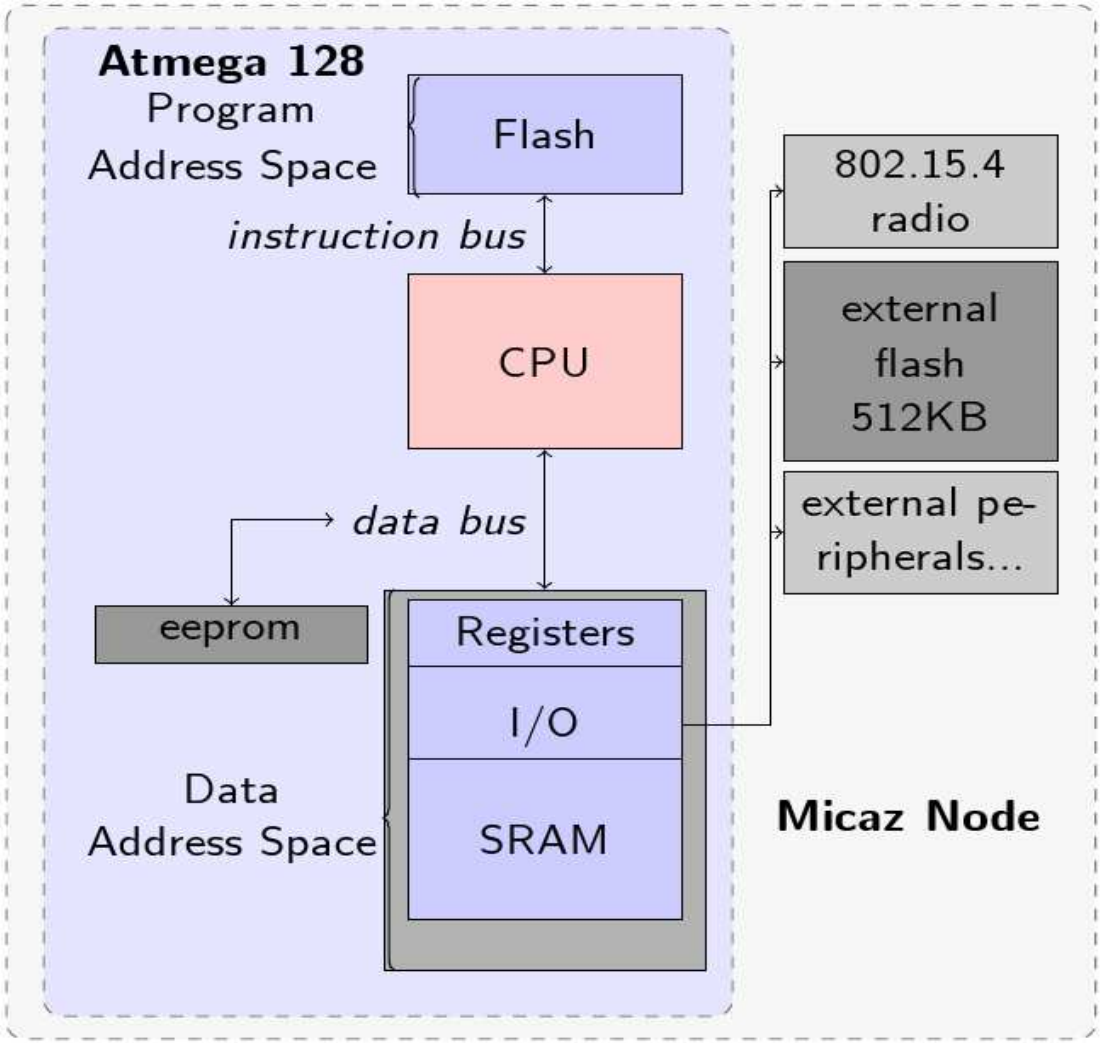
Computation

Sensing

Wireless Communication

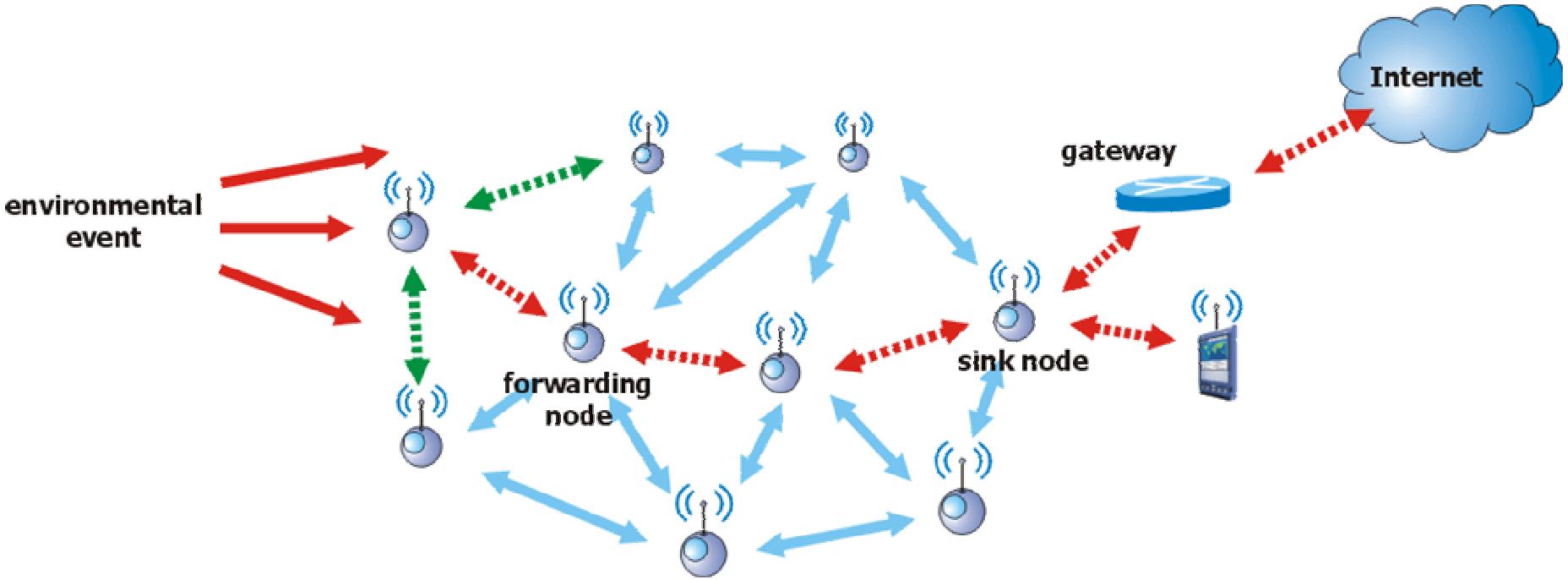
Architecture Type (Micaz Node)

- RAM:
  - Data memory- 4KOctets
- ROM/Flash:
  - program memory- 128kOctets
- External Flash: 512KB
- Processeur:
  - Atmel AVR Atmega 128 8-bit / 8MHz

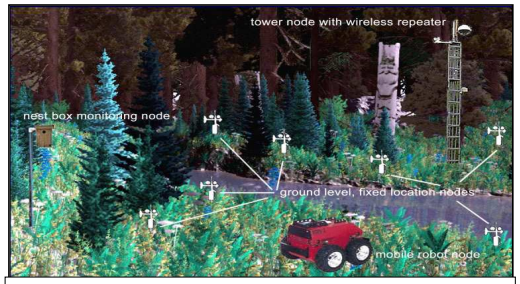


Architecture Reseau

- Architecture en arbre
  - Les capteurs sont les feuilles
  - La station de base est la racine



Applications



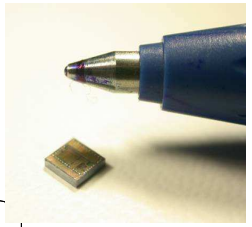
Environmental Monitoring

Interactive VR Game

Wearable Computing

Disaster Recovery

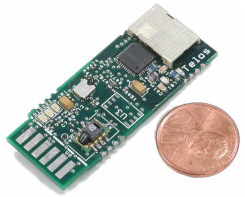
Earth Science & Exploration



Context-Aware Computing

Immerse Environments

Wireless Sensor Networks



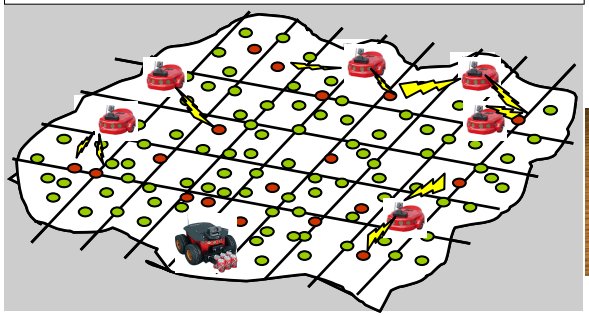
Biological Monitoring

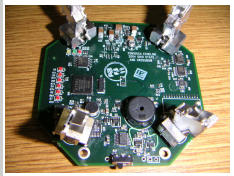
Hazard Detection

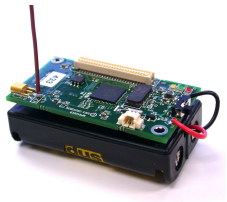
Smart Environment

Linear Structure Protection

Military Surveillance







Road Safety

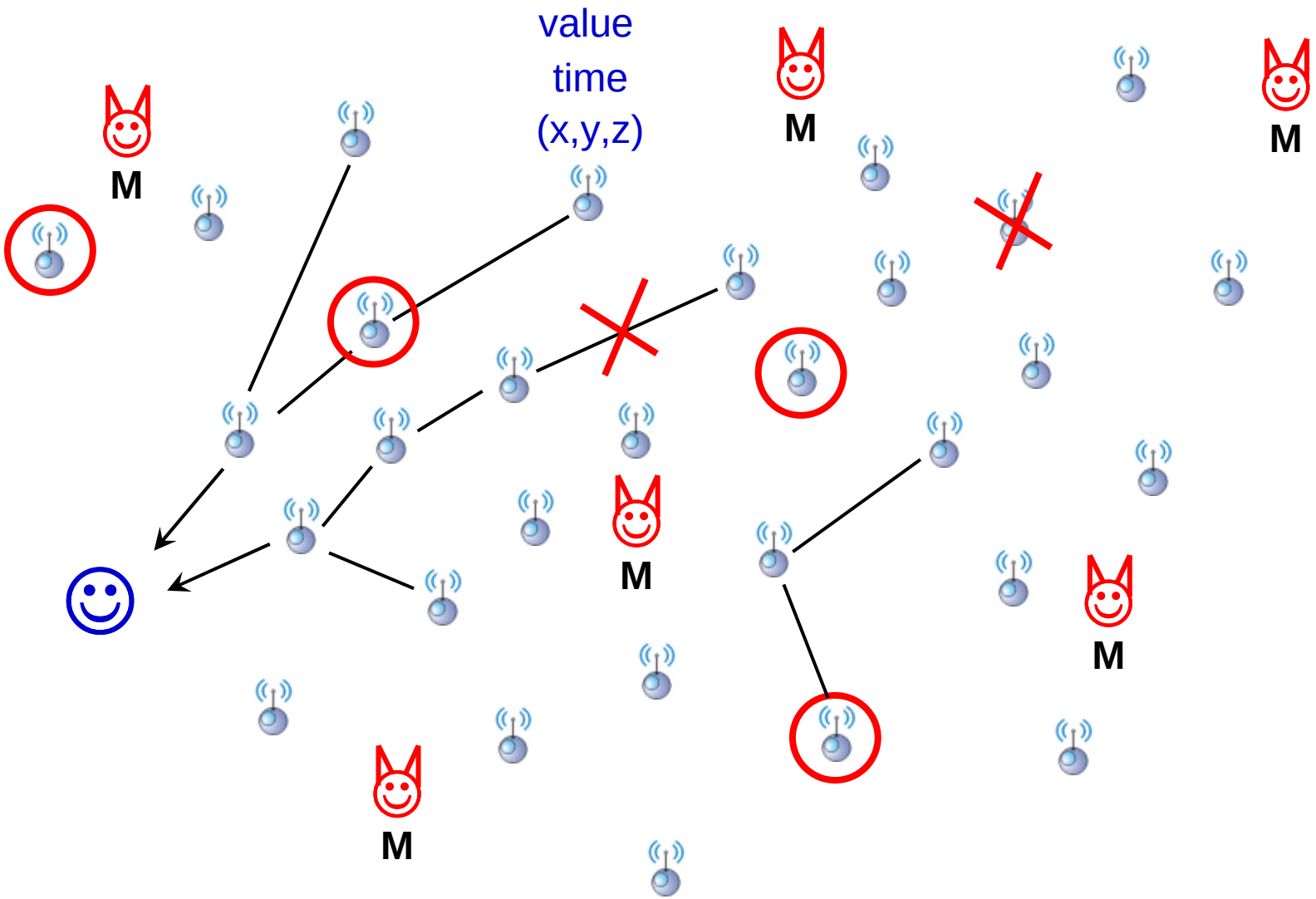
La Sécurité des RdCs

- Problème difficile car…

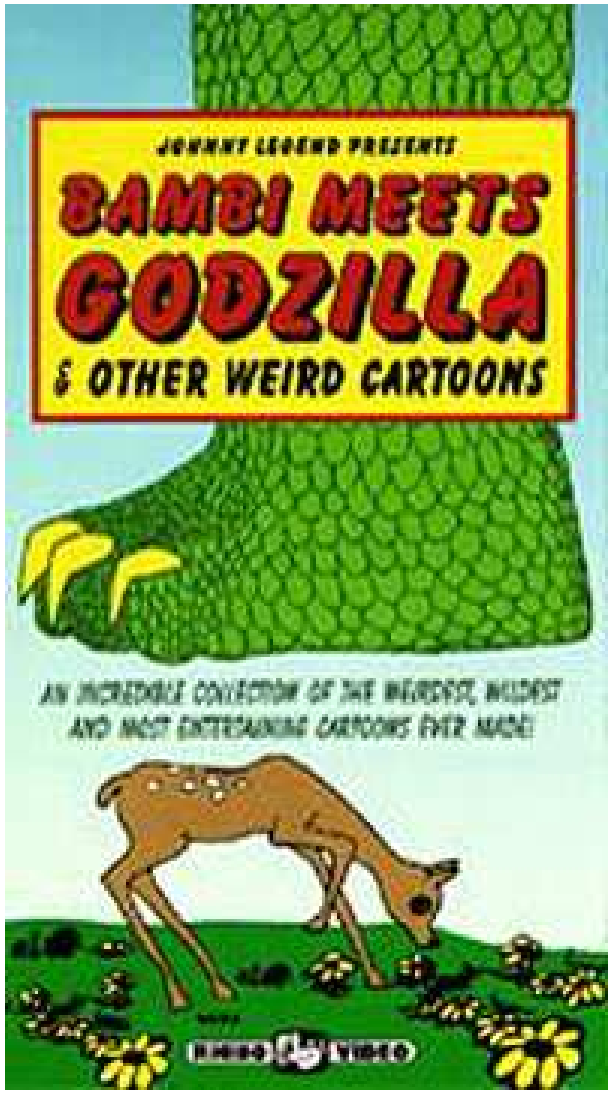
- Mémoire limitée (128 KB Program Flash)
- CPU limitée
- Énergie limitée (2x1.5V)

- Facilement accessible car déployé dans environnements ouverts
- Peu protégé car doit être bon marché …

La Sécurité des RdCs



La Securite des RdCs (2)



← **ATTAQUANT**

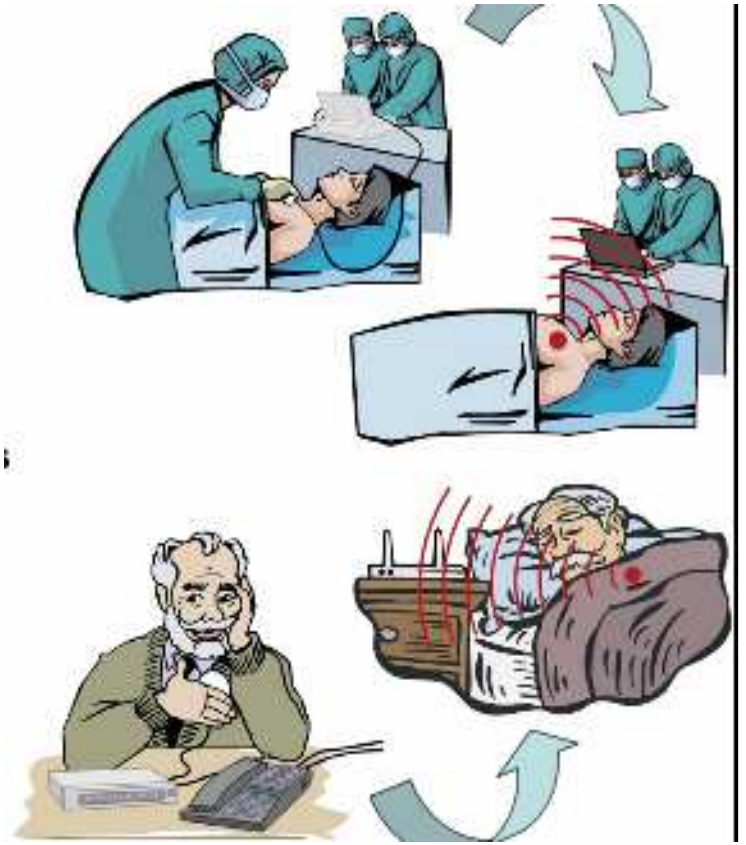
← **RESEAU**

La Sécurité des RdCs (2)..

- Problèmes très divers selon applications
  - Intégrité/confidentialité des données
  - Protocoles d'échange de clefs efficaces
    - Sachant que crypto a clef publique n'est pas possible
  - Sécurité du routage
  - Sécurité des problèmes de localisation
  - Agrégation sécurisée
  - …
- Illustrations
  1. Applications médicales: les pacemakers
     - 1 ou 2 nœuds
     - Noeuds difficilement accessibles
     - Le prix n'est pas forcement un problème
  2. Applications de surveillances (militaires ou autres)
     - 100, 1000+ nœuds
     - Noeuds facilement accessibles
     - Le coût doit être minimal

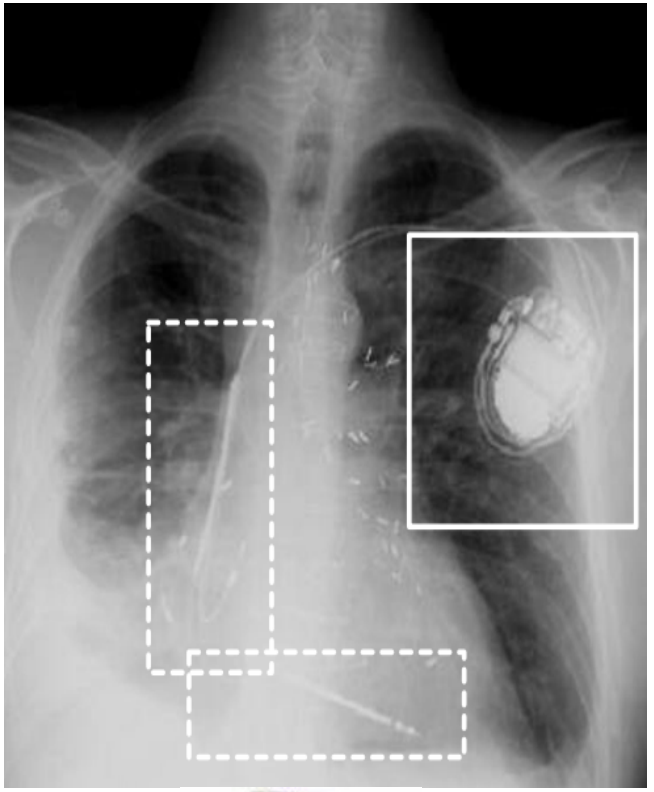
Application #1: Les Implants Médicaux

- De plus en plus d'implants médicaux possèdent des interfaces sans fil
  - Permet de configurer
  - Permet de stocker et récupérer des informations
  - Permet de surveiller a distance..
- Les implants cardiaques (défibrillateurs, pacemakers) en sont un bon exemple
  - Stimulateur Cardiaque (Pacemakers): émet périodiquement des petits stimulis électriques au coeur
  - Défibrillateur: émet des stimulis plus puissants pour restaurer un rythme "normal"

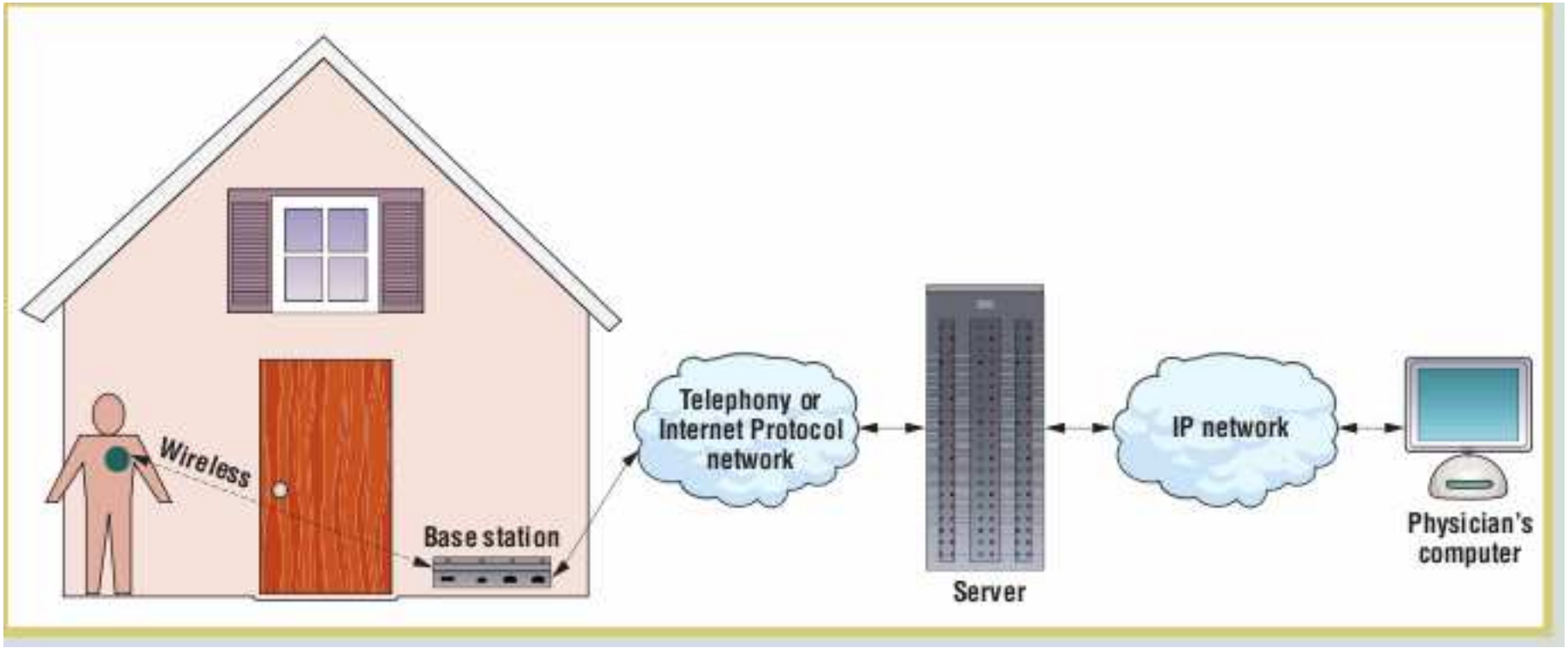


Les implants médicaux: Pacemakers/défibrillateurs

- Systèmes Actuels
  - Ultra-low-power CPU + 128 ko. RAM (donnée patient, log,…)
  - Communication par induction
  - Portée faible
    - Contact avec patient
  - Bande passante limitée
- Nouveaux systèmes
  - Portée de qq mètres (~2m)
    - Permet surveillance a distance des patients
    - Facilite la programmation et installation
  - Bande passante plus importante (~400 kbits/s)
    - Permet de nouvelles applications
    - Diminue le temps de consultation



Les implants medicaux: Nouvelle Applications



Securité des stimulateurs/défibrillateurs

- Les systèmes actuelles ne fournissent aucune sécurité (contrôle d'accès, intégrité, confidentialité)
- Un attaquant peut facilement:
  - Lire les données mesurées et stockées
  - Lire les données du patient (nom,médecin,…)
  - Modifier les paramètres!
  - Désactiver l'implant!
- Pas de panique! Aucune attaque reportée pour l'instant!
- Voir [1] pour détails

[1] Halperin and al., Pacemakers and implantable cardiac defibrillators: Software radio attacks amd zero-power defenses, IEEE Security and Privacy, Oakland, 2008.

Sécurité des pacemakers

- Juger inutile car nécessite d'être proche du patient
  - Mais attaquant peut utiliser un équipement non standard (amplificateur, antenne puissante,…)
- Coûteux en terme de ressource
  - CPU, bande passante, mais surtout énergie!
  - Réduit la durée de vie!
- Compromis Sécurité/Sureté!
  - La sécurité ne doit pas mettre la vie du patient en danger en cas d'urgence!
    - Les attaquants ne doivent pas avoir accès aux données
    - …mais les données doivent être disponibles en cas d'urgence!

Sécurité des pacemakers/ Un problème très difficile…

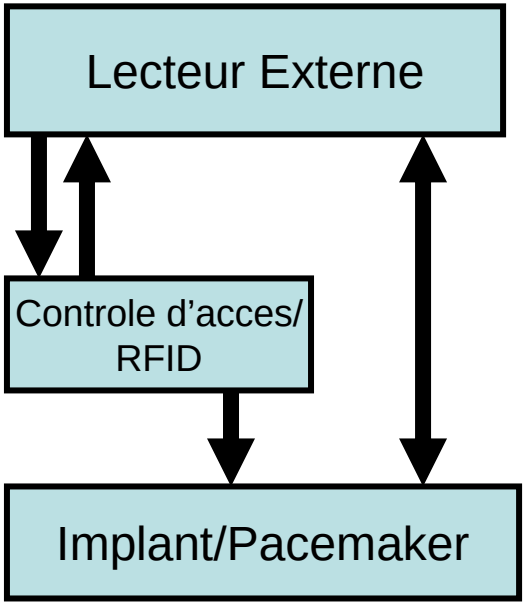
- Authentification des lecteurs
  - Gestion des clefs est difficile?
    - Capteur configuré avec une clef et la clef est donnée au médecin traitant…
    - Mais comment faire si le patient voyage ou admit d'urgence?
    - Carte a puce?
    - Pas de solution idéale!!…
  - Comment révoquer des lecteurs?
    - PKI?

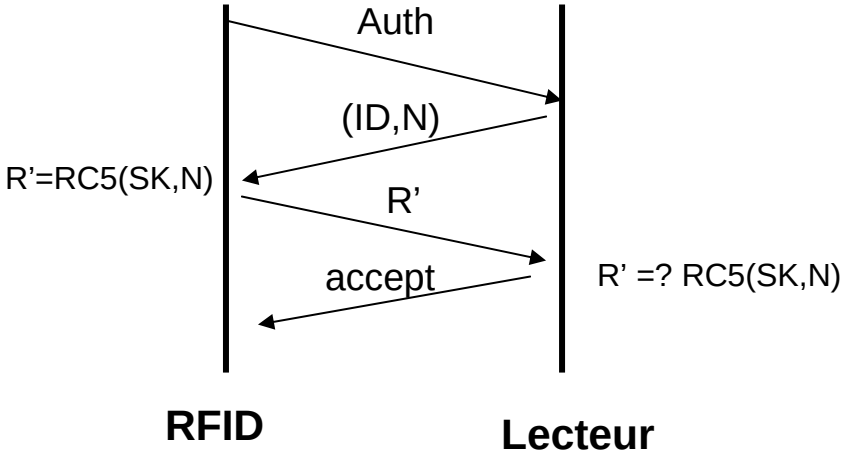
Sécuriser les Pacemakers (2)

- Comment éviter les attaques de type déni de service??
  - Cryptographie/Sécurité Coûte cher en terme d'énergie
  - Un attaquant pourrait émettre des fausses requêtes d'authentification/autorisation
  - Le capteur consommerait sa pile pour rien ☹

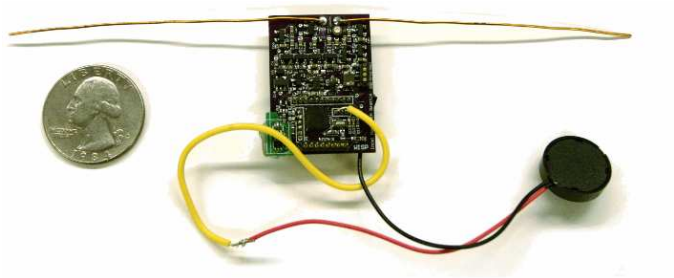
Solution contre DoS: Défense sans pile!

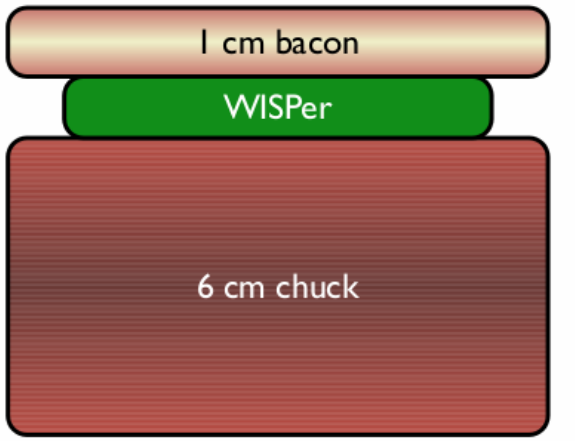
- Combiner RFID/Capteurs
  - RFID (passive) sert de “pare-feu”
    - RFID implémente le contrôle d’accès et vérifie que le lecteur est autorise
    - Si le lecteur est autorisé alors il peut communiquer avec le capteur…sinon le RFID bloque l’accès
      - Comme RFID est passive, il ne consomme pas d’énergie ☺
- Le RFID pourrait émettre un son/vibration pour avertir le patient de l’interaction





Expérimentations





RFID peut etre alimenter et effectuer authentification en utilisant des technologies standards (915Mhz)

Conclusions

- Les concepts de “zero-power notification, authentification” sont très prometteurs
- Mais la crypto ne suffit pas… simple fait d’émettre révèle beaucoup d’infos.
  - Le patient est porteur d’un pacemaker…
  - Information potentiellement intéressante pour assureurs, employeurs ☹
  - Atteinte a la protection de la vie privée..
- Besoin de protocoles qui ne s’activent qu’en présence de lecteurs autorises
  - …mais qui sont détectables et accessibles en cas d’urgence!!!
- Le patient doit être mis dans “la boucle”
  - Car ca le rassure (Usable Security and Privacy)
  - ….mais sans trop lui demander…

[2] Halperin and Al. Security and Privacy for Implantable Medical Devices, March 2008.

Application #2: Surveillance

Surveillance des feux de foret

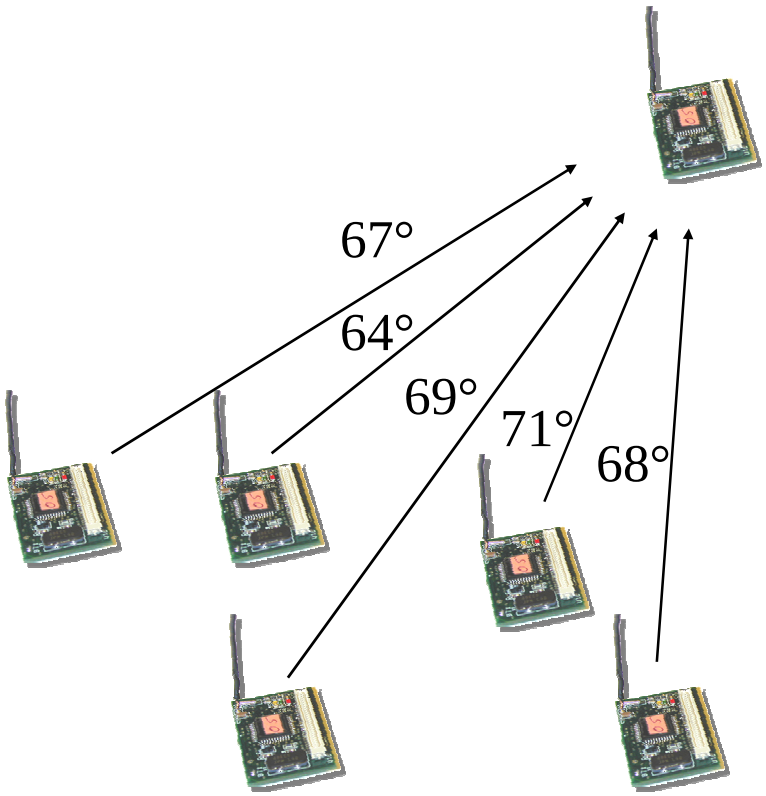
Surveillance de l'Environnement/Infrastructure

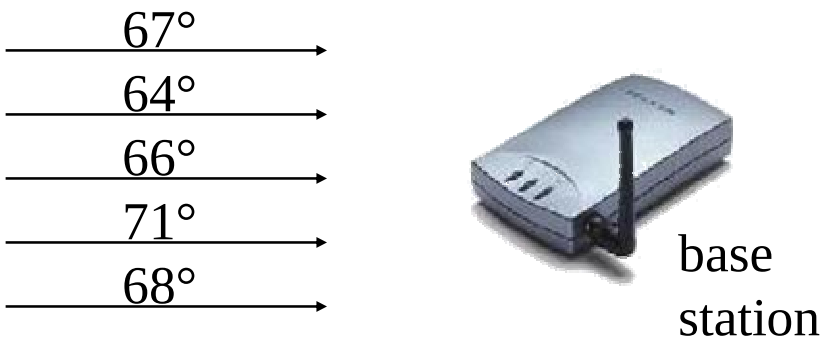
Quelles sont les problèmes de sécurité?

- Caractéristiques:
  - Nombre important de capteurs (!= implants)
  - Capteurs bon marches (!= implants)
  - Capteurs facilement accessibles (!=implants)
- Problèmes de sécurité:
  - Sécurité de l'infrastructure
  - Distribution/Échange des clefs sans PK crypto.
  - Agrégation des données chiffrées
  - Sécurité des services réseaux
    - Routage, localisation, sync. des horloges
  - Fiabilité/Tolérance aux fautes
    - Sécurité probabiliste

Agrégation des données

- Besoin de minimiser les transmissions
  - Radio est très consommatrice d'énergie:
    1 bit transmit ≈ 1000 CPU ops
- Agrégation: données compressée/traitées dans réseau
- Ex. Sans agrégation





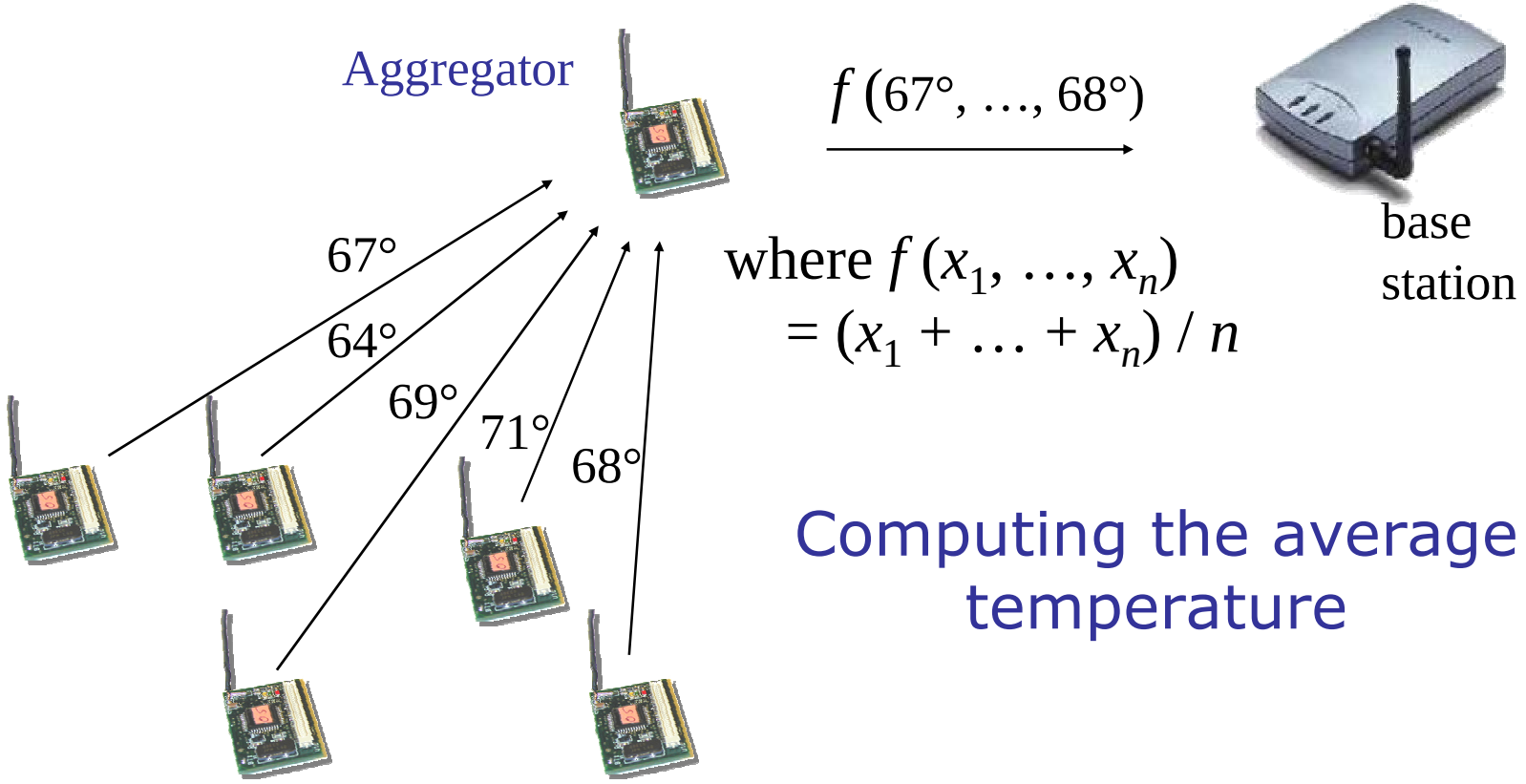
$$f(67°, \ldots, 68°)$$

where $f(x_1, \ldots, x_n) = (x_1 + \ldots + x_n) / n$

Calcul de la temperature moyenne

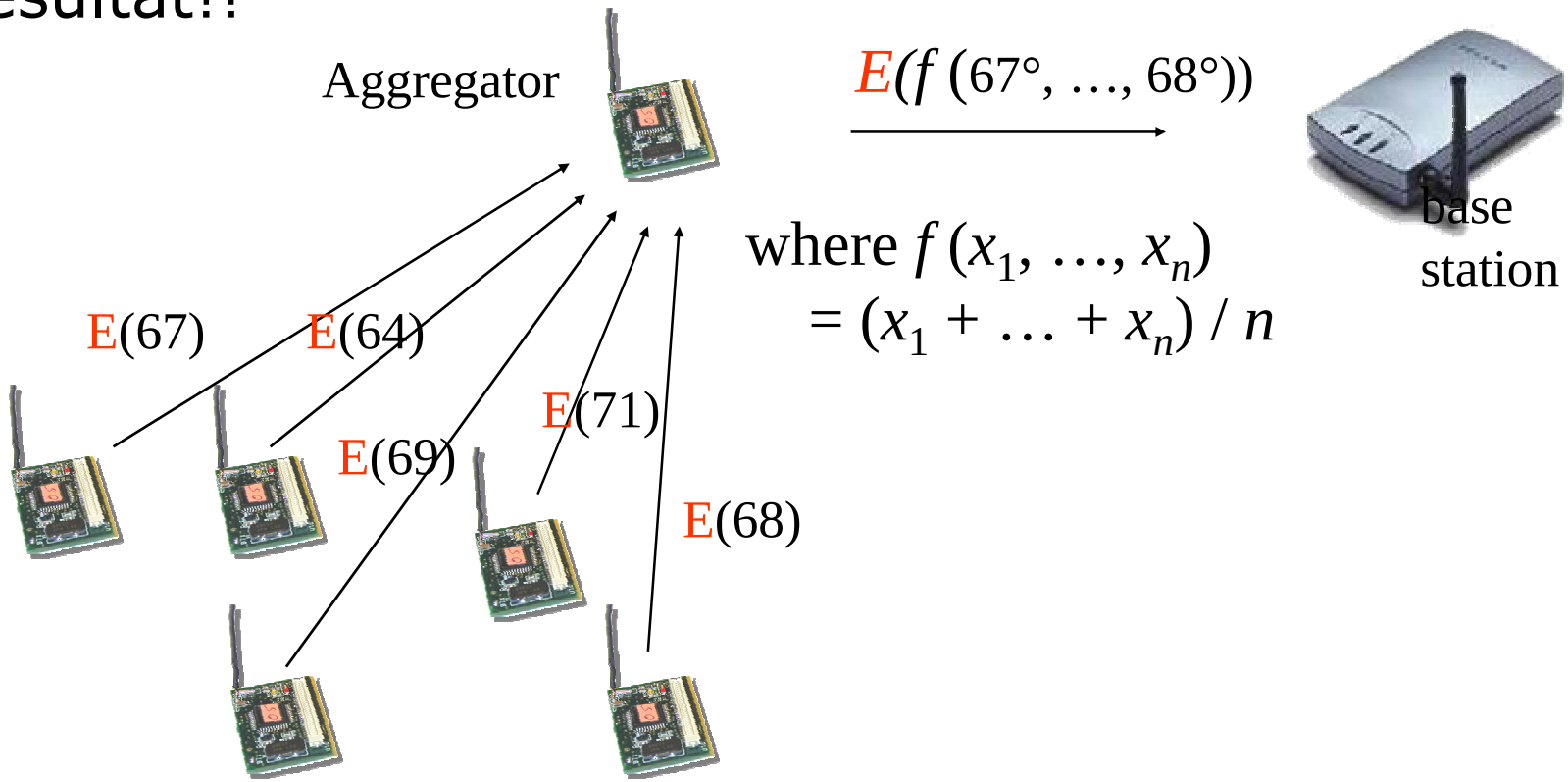
Agrégation des données (2)

- Ex. Sans agregation



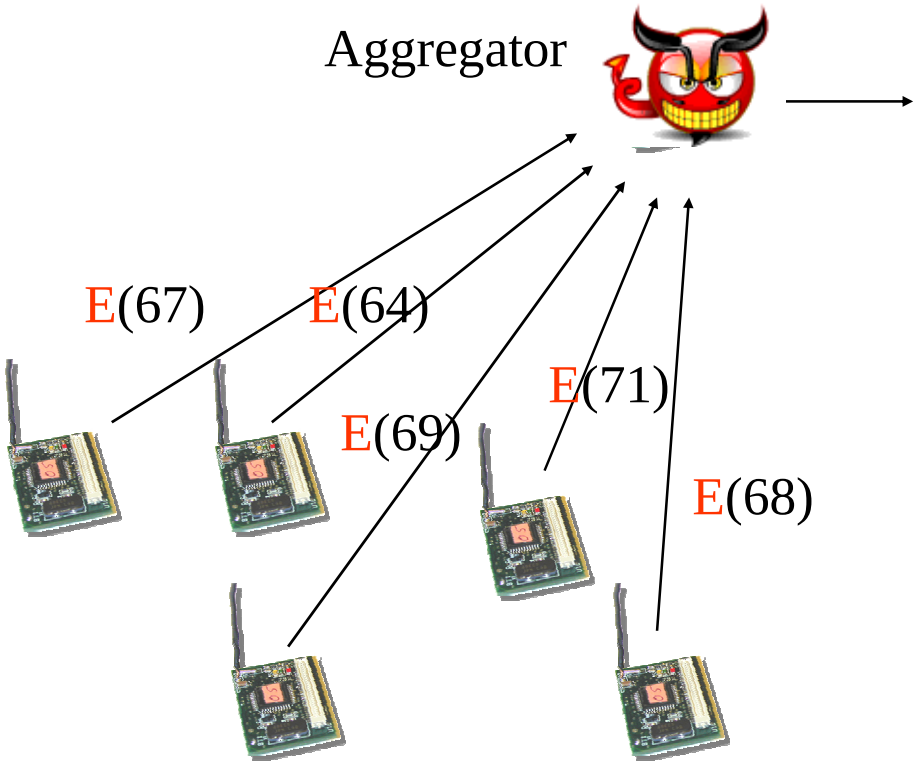
Sécuriser Agrégation des données
Approche saut-a-saut

- Chaque noeud chiffre+authentifie ses données avec une clef qu'il partage avec agregateur local
- Agregateur déchiffre+vérifie authentification+calcule moyenne+chiffre résultat!!



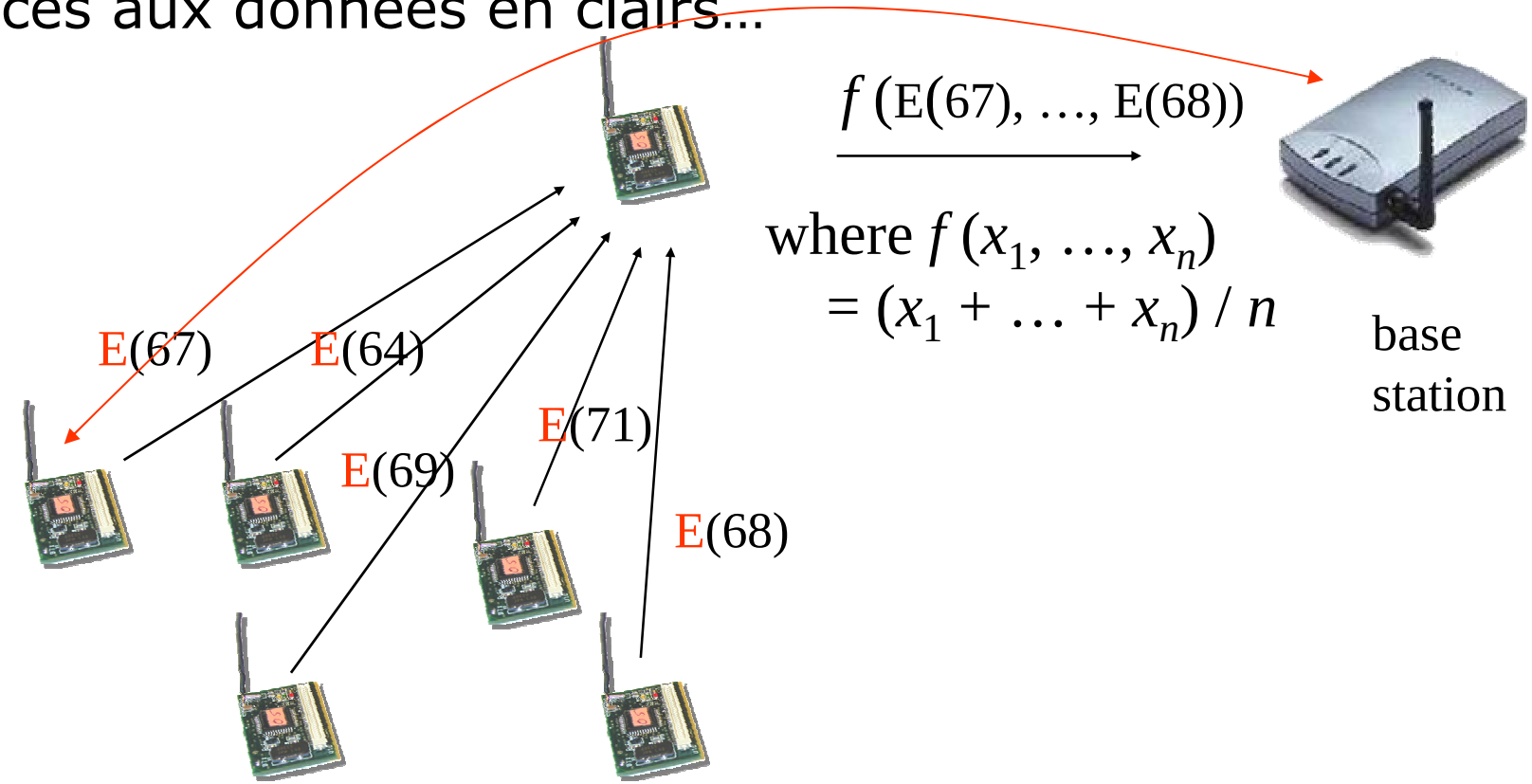
Sécuriser Agrégation des données (2)

- Coûteux…et fait hypothèse que Agregateur n’est pas compromis!
- Un agregateur compromis peut accéder aux données
  - Cible privilégiée pour attaquant!



Sécuriser Agrégation des données Une approche bout-en-bout

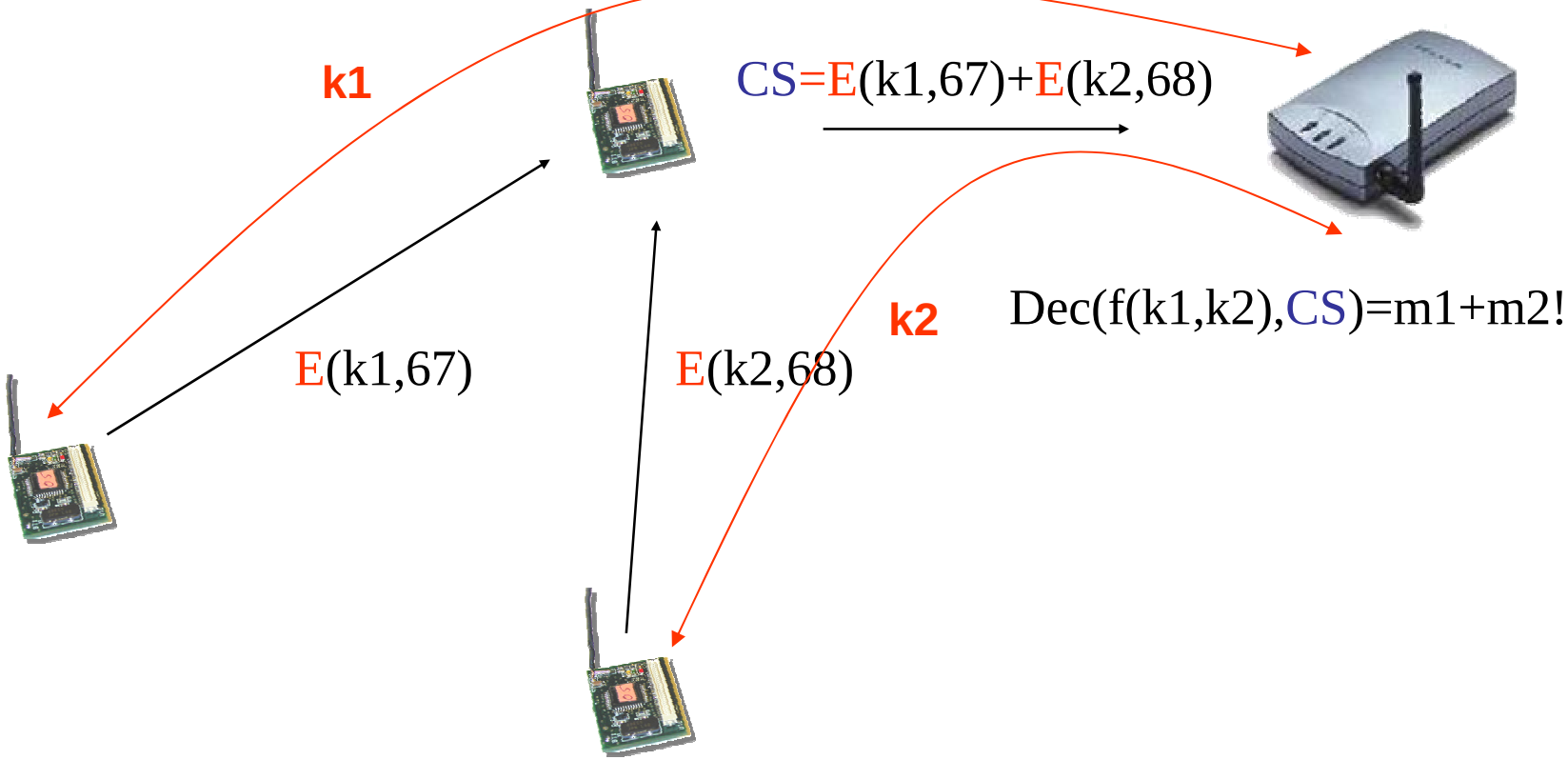
- Chaque noeud chiffre ses données avec une clef il partage avec la station de base (pas l'agregateur!!)
  - Gestion de clefs simplifiée + sécurité forte
- Agregateur manipule données chiffrées, et n'a jamais accès aux données en clairs…



Sécuriser Agrégation des données Une approche bout-en-bout (2)

- Besoin d'un algorithme de chiffrement homomorphe par l'addition…

1. S=Enc(k1,m1)+Enc(k2,m2) =Enc(f(k1,k2),m1+m2)
2. Dec(f(k1,k2),S)=m1+m2



Notre Proposition *[Mobiquituous05,Esorics07,MASS07]*

- Algorithme
  - C=Enc(m) = ki + m (mod max)
  - Dec(c) = c – ki (mod max)
  - Addition: CS=enc(m1)+enc(m2)=k1+m1+k2+m2 (mod max)
  - Decryption of Addition:

    Dec(k1,k2, CS)=C-(k1+k2) (mod max) = m1+m2
- Propriétés
  - Très efficace en terme de CPU (adapte aux WSN)
  - Sécurité prouvable

[3] Efficient Aggregation of Encrypted Data in Wireless Sensor Networks *C. Castelluccia, E. Mykletun and G. Tsudik, ACM/IEEE Mobiquitous Conference, July 2005, San Diego, USA.*

Sécuriser Agrégation des données: Conclusion

- Agregateurs additionnent les données chiffrées
- La station de base déchiffre et retrouve la somme des données!
- Un agregateur compromis n'a plus accès aux données!
- Efficace car agregateurs ne doivent pas déchiffrer + chiffrer résultats!
- Il existe encore des problèmes a résoudre:
  - Comment assurer l'intégrité/authenticité des données agrégées?
  - Comment éviter/détecter la modification de l'environnement par un attaquant ??

Activités a l'INRIA (EPI Planète)

- Protocoles d'échange de clefs efficaces
  - ROK: Robust Key Exchange protocoles
- Agrégation des données
  - Agrégation des données chiffrées
  - Authentification/Intégrité des données agrégées
- Génération de nombres aléatoires pour Capteurs (TinyRNG)
- Virus pour capteurs
  - Premier virus sur capteurs Micaz (architecture harvard)!
  - …en combinant plusieurs techniques (return-to-libc, fake stack injection,…)
- Sécurité des systèmes RFID

The FP6 IST UbiSec&Sens Project (http://www.ist-ubisecsens.org/)

- Partenaires:
  - NEC Network Development Laboratories (DE) , RWTH Aachen (DE), INRIA (FR), IHP Microelectronics (DE), INOV (PT), Budapest University of Technology and Economics (HU), Ruhr University Bochum (DE)

- Project Goals
  - to provide a complete toolbox of security and reliability aware components for sensor network application development,
  - application scenarios of agriculture, road services and homeland security

Pour plus d’information…

- http://planete.inrialpes.fr/~ccastel
- Claude.castelluccia@inria.fr

Merci!