Protejarea Mesajelor in Wireless Sensor Networks

Stefan Contiu – UTCN 2015

Cuprins

- Descriere WSN
- Diferente fata de retele Ad-Hoc
- Vulnerabilitati ale WSN
- Protejarea mesajelor in WSN
- Concluzii
- Referinte

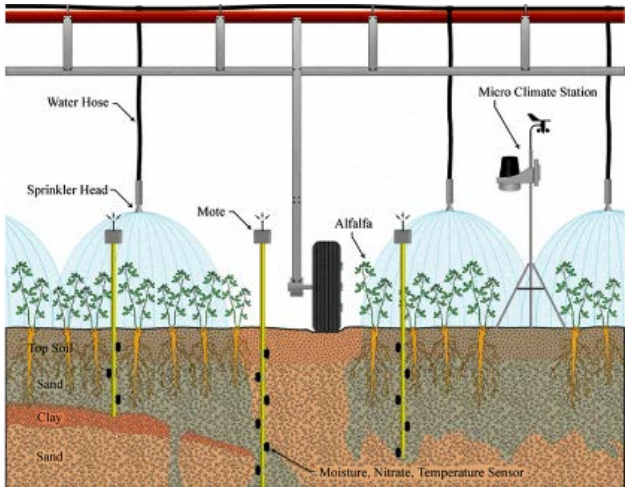
Definitia WSN

- Retea de senzori autonomi distribuiti in spatiu.
- Senzorii monitorizeaza evenimente sau conditii fizice ale mediului inconjurator.
- Datele monitorizate sunt trimise catre un centru de comanda, numit si senzorul Baza.

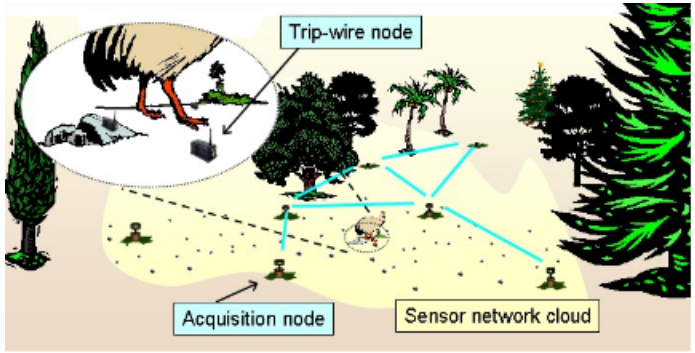
Aplicatii ale WSN

Domeniul Militar

Agricultura, Detectia Incendiilor, Inundatiilor



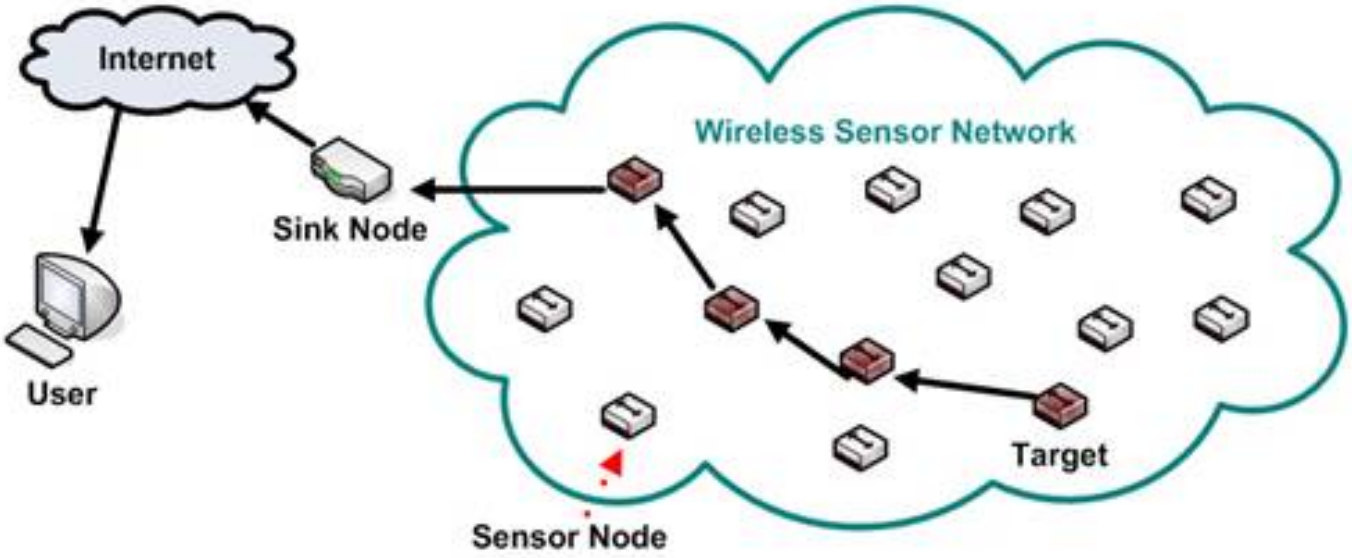
Supravegherea animalelor salbatice



Monitorizare Medicala a Pacientilor

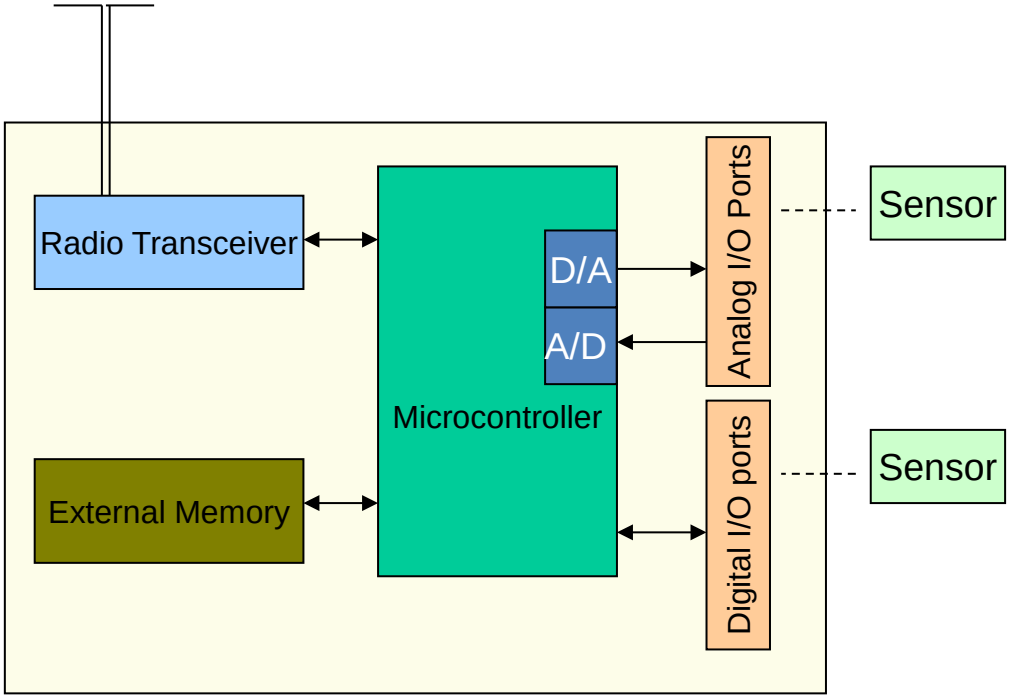
* imagini preluate din Raj Jain [2].

Arhitectura WSN



- Topologia cea mai raspandita : ***multi-hop***.
- Tehnica de propagare a mesajelor in retea: ***rooting*** sau ***flooding***.

Arhitectura Sensor Node (Mote)



- Functioneaza ca un calculator cu putere redusa.
- Ruleaza sisteme de operare simplificate(TinyOS, LifeOS, Contiki etc.)

* imagine preluata din Gajaweera [3].

WSN vs. Retele Ad-Hoc

- Functionaza pe scara foarte larga(sute, mii de noduri).
- Bateriile nodului senzor nu se pot inlocuii intotdeauna.
- Nodurile senzori nu au intotdeauna Identificatori Globali.
- Queriile pot fi axate pe date si nu adrese.

Vulnerabilitati ale WSN

- Interceptia canalelor Wireless.
- Coruperea sau falsificarea nodurilor senzor.
- Denaial of Service asuprea nodurilor senzor sau statia de baza.
- Coruperea Fizica, analiza off-line a nodurilor senzor.

Interceptia mesajelor in WSN

- Un atacator(global) ce monitoriza pasiv toate comunicatiile din retea, poate observa:
  - Sursa Mesajelor (senzorii care au detectat evenimente)
  - Timpul la care s-au produs(raportat) evenimentele.
- Solutie in cazul interceptiei:
  - Introducerea de trafic “dummy” in retea pentru derutarea atacatorului.
  - Filtrarea mesajelor dummy pentru prevenirea exploziei de trafic.

Solutie : trafic “dummy”

- Fiecare nod senzor din retea genereaza mesaje dummy pentru distragerea atacatorilor:
  - Toate mesajele vor avea aceasi lungime si vor fi criptate pentru prevenirea analizei continutului lor.
  - Additional, se introduce un “delay” in raportarea si inaintarea mesajelor in retea.
- Problema: pachetele dummy vor creste in mod considerabil traficul din retea.

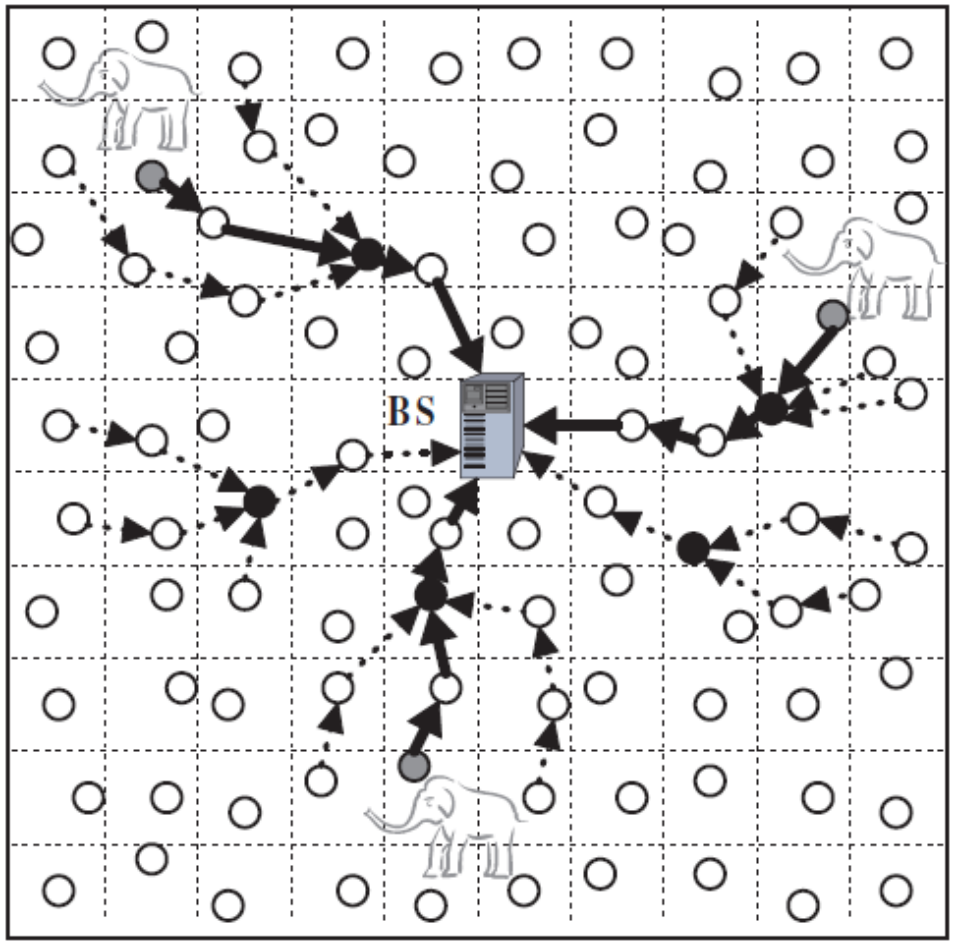
Filtrarea Pachetelor “Dummy”

- Filtrarea mesajelor dummy se va realiza de noduri Proxy in calea lor catre Base Station(sink node).
- Nodurile Proxy:
  - Alegerea nodurilor proxy se face inainte de instalarea retelei printr-un algoritm euristic.
  - Inregistrarea nodurilor senzor cu un Proxy, la instalarea retelei:
    - Fiecare nod Proxy face un broadcasts(mesaj “hello” cu TTL).
    - Fiecare nod senzor decide care e cel mai apropiat Proxy.
    - Se stabileste o chieie individuala pentru fiecare (nod, proxy).
  - Cand reteaua este operationala:
    - Fiecare nod senzor trimite mesaje criptate prin unicast catre proxy-ul sau.

Amplasarea Proxy-urilor

- Cea mai buna amplasare elimina pro-activ mesajele dummy, minimizeaza traficului in retea.
- Determinarea celor mai bune locatii pentru Proxy este o problema NP-hard.
- Se opteaza pentru folosirea unui algoritm bazat pe Local Search Heuristics:
  - Se alege aleator o multime de Proxy.
  - In mod repetat se incearca interschimbarea unui Proxy din aceasta multime cu unul extern. Daca performanta agregata a traficului se imbunatateste, intesrchimbarea are loc.
- Experimental s-a dedus complexitatea medie : O(n^4).

Exemplu amplasare Proxy-uri



Legenda:

- Cercuri albe : noduri sursa
- Cercuri gri: noduri care au inregistrat un eveniment
- Cercuri negre: noduri Proxy

- Sageti intrerupte: mesaje false
- Sageti continue: mesaje adevarate

* imagine preluata din Yang et all. [4]

Concluzii

- Protejarea sursei si aparitiei evenimentelor in WSN se poate realiza prin introducerea de traffic “dummy”.
- Amplasarea proxy-urilor pentru reducerea traficului “dummy” se poate determina printr-un algoritm euristic.

References

- [1] http://en.wikipedia.org/wiki/Wireless_sensor_network
- [2] Raj Jain, CSE 574S, Wireless Sensor Networks: http://www.cse.wustl.edu/~jain/cse574-10/index.html
- [3] Nuwan Gajaweera, Wireless Sensor Networks: www.ent.mrt.ac.lk/dialog/documents/ERU-2-wsn.ppt
- [4] Yi Yang, Min Shao, Sencun Zhu, Bhuvan Urgaonkar, Guohong Cao: Towards Event Source Unobservability with Minimum Network Traffic in Sensor Networks: http://www.cse.psu.edu/~szhu/papers/proxyfilter.pdf
- Waltenegus Dargie, Christian Poellabauer, Fundamentals of Wireless Sensor Networks Theory and Practice, Wiley Series, 2010.