Protejarea evenimentelor in Wireless Sensor Networks

Stefan Contiu,
Master, UTCN 2014

In prima parte a referatului se prezinta concepte generale si arhitectura WSN. Se evidenteaza de asemenea vulnerabilitatile generale specifice acestor retele.

In a doua parte, lucrarea se concentreaza asupra unei metode pentru protejarea sursei si timpului raportarii evenimentelor ce se transmit prin mesaje in WSN. Aceasta metoda presupune introducerea in mod intelligent de traffic “dummy” in retea. Deoarece traficul poate creste considerabil, o parte din mesajele “dummy” trebuie inlaturate. Se prezinta o metoda de filtrare prin utilizarea unor Proxy-uri. De asemenea se prezinta un algoritm pentru pozitionarea optima a proxyurilor in topoligia retelei.

Referatul se inchieie prin prezentarea unor concluzii si a referintelor bibliografice.

1. Prezentare Wireless Sensor Networks

1.1. Descriere si Arhitectura

O retea de senzori wireless(Wireless Sensor Networks), WSN pe scurt, este o retea distribuita in spatiu, de senzori autonomi. Acestia monitorizeaza anumite evenimente sau conditii fizice ale mediului inconjurator. Datele monitorizate sunt trimise catre un centru de comanda, numit si senzorul baza.

O astfel de retea poate avea de la cativa pana la sute sau mii de noduri[1] care sunt conectate la unul sau mai multi senzori. Un senzor este alcatuit din mai multe parti: un transmitator radio,

un microcontroller, un circuit electronic si o sursa de energie. Fig 1. prezinta structura unui astfel de nod, ce este cunoscut si sub numele de “Mote”[3].

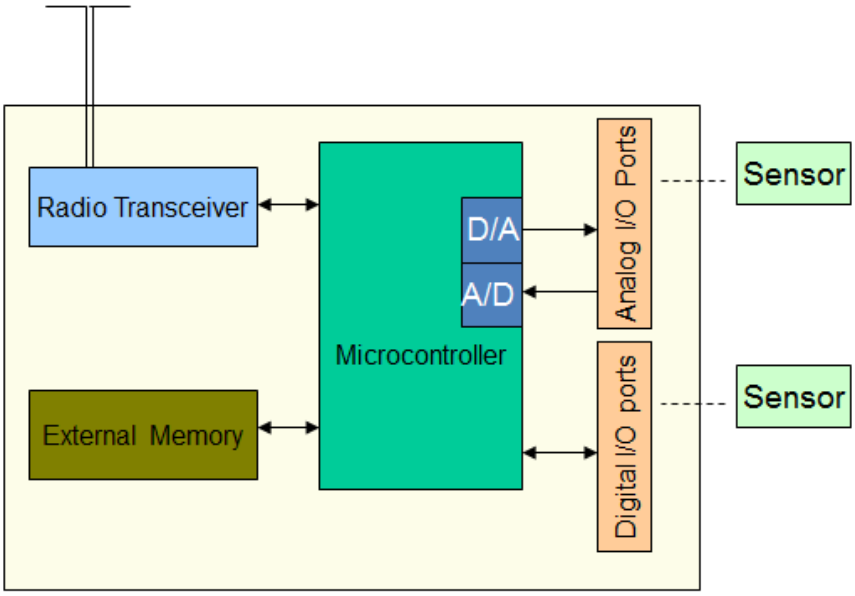

Fig 1. Structura unui nod autonom dintr-o retea WSN.

Topologia unei retele WSN poate varia de la una simpla in forma de stea pana la una avansata de tipul multi-hop wireless mesh. Tehnicile de propagare a mesajelor in aceste retele sunt routing sau flooding. Fig. 2. prezinta arhitectura unei retele de senzori wireless multi-hop.

1.2. Comparatie cu retelele Ad-Hoc

In comparatie cu retelele Ad-Hoc, urmatoarele sunt specifice pentru retelele de senzori wireless[2]:

- Retelele de senzori wireless sunt instalalte pe o scara foarte mare. Pot exista intre cateva sute si cateva mii de noduri in aceste retele.
- Fata de calculatoare sau telefoane, nodurile din retelele de senzori pot sa aiba baterii cu o singura durata de viata. In unele scenarii, dupa ce bateria s-a consumat se poate considera ca nodul senzor nu mai este folosibil.
- In retelele de senzori nu exista neaparat identificatori globali. Pe cand retelele ad-hoc folosesc adrese MAC pe 48 sau 64 de biti).
- Queriurile facute in retelele de senzori pot fi axate mai mult pe date si mai putin pe adresare. De exemplu un query intr-o retea ce monitorizeaza temperaturi poate fi: “Ce noduri au temperatura mai mare de 35C?” fata de “Ce temperatura are un nod respectiv?”

- Aggregarea Datelor. Informatia este comunicata de la noduri catre Base Station prin transmisie hop by hop. Pentru a se conserva energie aceasta informatie este aggregata in noduri senzor intermediare. Aggregarea reduce traficul din retea si deci reduce consumul de energie pentru nodurile senzor.

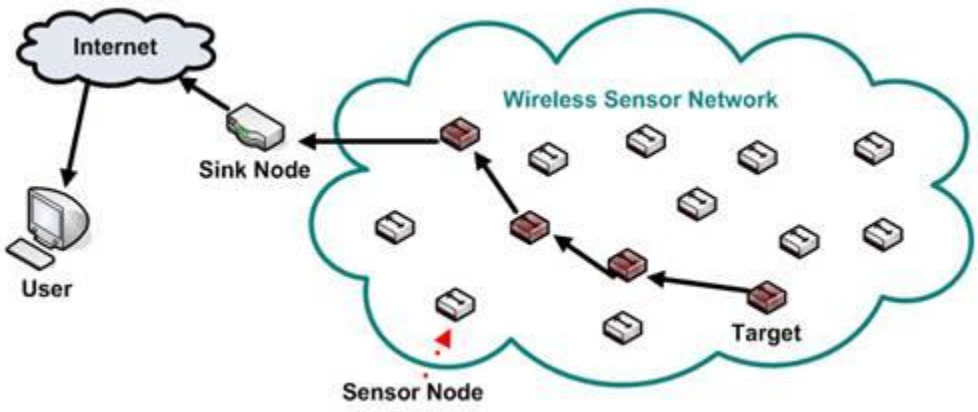

Fig. 2 : Arhitectura unei retele de senzori wireless

1.3. Vulnerabilitati Generale ale WSN

1.3.1. Interceptia

Cum s-a mentionat si mai sus, nodurile senzor comunica prin canale wireless si deci tot traficul este suscectibil interceptarii. Incerceptia comunicarii poate duce la aflarea unor informatii private ca si parole, parametrii sistemelor de securitate, detalii despre sistemul care este monitorizat etc. Aceste informatii pot deshide calea spre alte tipuri de atacuri. Solutia in retele ad-hoc traditionale este de a cripta pachetele. Dar din cauza naturii resurselor de calcul in retelele sensor, optiunea criptarii se dovedeste imposibila.

1.3.2. Coruperea

Unul sau mai multe noduri senzor ar putea fi capturate(electronic) continuand sa functioneze ca membri valizi ai retelei. Acest nod capturat ar putea fi folosit pentru a incercepta comunicatiile, a injecta date false, coruperea mecanismul de rutare sau ar putea lansa alte atacuri din interiorul retelei.

1.3.3. Falsificarea

Un intrus rau intentionat ar putea adauga un nod fals retelei. Acest nod ar putea funciona ca si un membru legitim a retelei si ar putea divulga informatii, corupe fluxul de comunicatii dintre noduri sau ar putea injecta date false.

1.3.4. Denial of Service

Un intrus rau intentionat ar putea lansa atacuri Denial of Service folosind orice tehnica cunoscuta aplicabila retelelor ad-hoc traditionale, de exemplu signal jamming si traffic flooding. Nodurile senzor afectate de atacuri Denial of Service ar putea fi incapabile sa simta fenomenul

sau ar putea acumula inregistrari incorecte. In plus, un atac de tip Denial of Service orientat spre statia baza, ar face ca toata reteaua sa devina nefolositoare.

1.3.5. Corupere Fizica

Nodurile pot fi scoase din retea pentru a fi analizate off-line. Aceasta analiza ar putea ajuta un atacator sa descopere chei folosite pentru criptare sau sa invete structura retelei. Daca statia baza este membru al retelei de senzori atunci statia baza reprezinta un “Single Point of Failure” pentru toata reteaua.

2. Protejarea mesajelor in Wireless Sensor Networks

Interceptia mesajelor in cadrul unui atac global, poate oferii atacatorului informatii private precum nodul sursa si timpul la care un mesaj a fost detectat. Este asadar nevoie de un mecanism pentru protejarea acestor atribute in cazul in care atacatorul poate intercepta traficul Wireless.

Tehnica de protectie descrisa mai jos presupune urmatoarele doua “best-practice”-uri:

- Introducerea de traffic “dummy” in retea.
- Trimiterea(inaintarea) mesajelor(dummy sau veritabile) pe baza unor intervale de timp.
- Filtrarea mesajelor “dummy” cu cat acestea se apropie de Base Station(sink node) pentru prevenirea exploziei de trafic in retea.

2.1. Modelul Sistemului

2.1.1. Modelul Retelei

O retea de senzori este divizata in mai multe casute(ca un grid) unde fiecare pereche de noduri aflate in celule alaturate pot comunica direct unele cu celelalte. O celula este unitatea minima unde se detecteaza evenimente, iar capul unei celule(cell head) coordoneaza toata actiunile din interiorul celulei. Fiecare celula are un identificator(numar intreg) associate, cu valoare in intervalul [1..n]. Fiecare nod senzor este constient de celula in care se afla. Exista o statie de baza care este localizata in centrul retelei si foloseste drept centru collector pentru datele evenimentelor. Rapoartele care sunt associate evenimentelor contin urmatoarele informatii:

- ID-ul celulei in care a fost detectat evenimentul.
- Tipul evenimentului.
- Timpul la care evenimentul a fost detectat.

2.1.2. Modelul Atacului

Se presupune ca atacatorul este:

- Extern – atacatorul nu va compromite sau controla niciunul dintre senzori.
- Pasiv – atacatorul nu va folosi tehnici de atac active, ca si injectarea de traffic, blocarea canalelor sau denial of service.

- Global – atacatorul poate colecta si analiza toate informatiile din retea.

De exemplu, atacatorul ar putea face urmatoarele: mai intai ar examina continutul unui mesaj pentru a descoperi locatia sursa a mesajului. Apoi, chiar daca mesajul este criptat, este usor sa identifice sursa mesajului daca acesta ramane la fel pe toata durata de viata. In al treilea rand ar putea sa conduca analize mai avansate pentru monitorizarea si corelarea timpului mesajelor.[4]

2.2. Introducerea de mesaje “dummy”

In prima faza, inainte de instalarea retelei, se alege o multime de noduri

Imediat dupa instalarea retelei fiecare nod Proxy va trimite un mesaj broadcast “hello” ce contine TTL (time to live) destul de mare incat sa ajunga la toate nodurile senzor din retea. Fiecare nod ce primeste mesajul “hello” inregistreaza proxy-ul cel mai apropiat de el ca si proxy-ul sau default. Fiecare nod senzor trimite inapoi un raspuns proxy-ului sau pentru ca aceste sa stie ce noduri serveste.

De asemenea, fiecare nod stabileste o cheie individuala de securitate cu proxy-ul sau. Fiecare proxy are la randul sau o cheie individuala cu Statia Baza. Cand reteaua este operationala, fiecare nod trimite prin Unicast mesaje criptate proxy-ului sau default, printr-un protocol multi-hop de routare. Intervalele de timp la care aceste mesaje sunt transmise urmeaza o distributie exponentiala. Acest lucru va contribui la conditia de neobservare a sursei msajelor. Cand un nod senzor detecteaza un eveniment, amana transmiterea mesajului criptat pana la urmatorul interval probabilistic, astfel incat, chiar daca atacatorul face o analiza bazata pe timp, nu va putea diferentia intre mesaje reale si mesaje “dummy”.

Dupa ce un Proxy primeste un mesaj, se vor executa urmatoarele operatii pentru a reduce traficul si a prezerva anonimitatea sursei evenimentului:

1. Se decripteaza evenimentul astfel incat proxy-ul sa poata diferentia intre evenimente reale si false.
2. Se renunta la mesaj daca este considerat fals. In cazul in care mesajul este veritabil, se cripteaza din nou.
3. Se pune acest mesaj veritabil (criptat din nou) in buffer-ul de mesaje al proxy-ului. Dupa un interval de timp, un mesaj(veritabil sau nu) va fi trimis din acest nod proxy.

2.3. Amplasarea Proxy-urilor in locatii optime

2.3.1. Definirea Problemei

Instalarea Proxy-urilor in locatii corecte este o problema cruciala pentru performanta retelelor de senzori. De exemplu daca toate proxy-urile sunt plasate unul langa celalalt, traficul din retea nu se poate reduce in mod optim. In mod similar, daca toate proxy-urile sunt plasate departe de statia de baza, numarul de mesaje false filtrate va fi foarte mic. De asemenea, se considera

ca, criteriul de optimizare pentru alegerea locatiilor este minimizarea traficului agregat din toata reteaua. Traficul agregat din toata reteaua se defineste ca:

rata de traffic x marimea unui mesaj x numarul de salturi

2.3.2. Pseudo-cod al algoritmului de plasare pentru Proxy-uri

Intrare : o topologie a unei retele bazata pe celule(grid), cu multimea nodurilor *V*, numarul nodurilor fiind *n.*

Iesire : o multime P reprezentand proxy-urile.

Procedura :

1: $P \leftarrow \emptyset; P' \leftarrow \emptyset; \{cost(\emptyset) = \infty\}$
2: **for** $k \leftarrow 1$ *to* $n-1$ **do**
3: $placement(k); \{ Update\ P' \}$
4: **if** $cost(P') < cost(P)$ **then**
5: $P \leftarrow P';$
6: **end if**
7: **end for**
8: return P;
9:
10: **placement**(*k*)
11: $P'[0] \leftarrow BS;$
12: **for** $i \leftarrow 1$ *to* k **do**
13: $P'[i] \leftarrow i; \{ Initializeaza\ P'[0] \dots P'[k] \}$
14: **end for**
15: **for** $\forall i \in P' and\ \forall j \notin P' and\ i, j \in V$ **do**
16: $P'' \leftarrow P' - i + j; \{ Interschimba\ i\ si\ j \}$
17: **if** $cost(P'') < cost(P')$ **then**
18: $P' \leftarrow P'';$
19: **end if**
20: **end for**; $\{Bucla\ se\ termina\ dupa\ ce\ incercam\ toate\ combinatiile\ de\ i\ si\ j\}$

Fiind dat k, numarul proxy-urilor ce trebuie instalate, incepem cu o multime cu elemente aleatoare P' de marimea k, ce folosesc BS ca si proxy default. In fiecare pas al algoritmului se propune inter-schimbarea unui nod din multimea P' cu un nod ce nu e membru al P', daca o astfel de inter-schimbare reduce traficul agregat al retelei. Daca aceasta inter-schimbare are loc, atunci modificam multimea P'. Repetam acest process pana cand nu mai exista posibile inter-schimbari. In acest punct, costul aggregat al traficului din retea ajunge la un minim local.

In urma experimentelor [4], s-a dedus ca acest algoritm tinde sa aiba o complexitate in cazul mediu de $O(n^4)$.

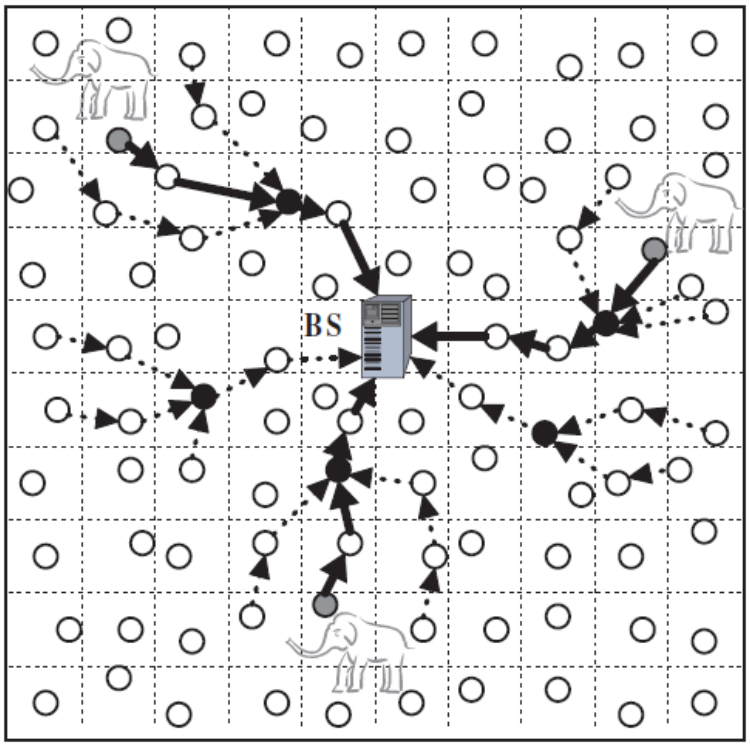

Figura 1 : Exemplificarea Proxy-Based Filter. Cercurile albe reprezinta surse. Cercurile negre reprezinta Proxy-uri. Liniile intrerupte reprezinta mesaje false, liniile continue mesaje reale.

3. Concluzii

Protejarea sursei si timpului raportarii evenimentelor in retele WSN se poate realiza prin introducerea de trafic “dummy”. Pentru prevenirea exploziei traficului din retea se opteaza pentru filtrarea pachetelor “dummy” de catre noduri Proxy. Alegerea nodurilor Proxy se determina printr-un algoritm euristic ce garanteaza un minim local pentru traficul agregat din retea.

4. Bibliografie

[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

[5] Waltenegus Dargie, Christian Poellabauer, Fundamentals of Wireless Sensor Networks Theory and Practice, Wiley Series, 2010.