Seguretat en xarxes de sensors

Enric Herce Yébenes
Miguel Ribes Franco
Director: Juan Vicente Capella Hernández

Curs 2010/2011

Índex de continguts

1 Motivació i objectius del treball

1.1 Introducció

Les xarxes de sensors tenen el seu origen en iniciatives militars de la mà de DARPA , encara que actualment s'utilitzen en diferents aspectes civils o industrials com la monitorització de pacients o control del trafic en certes zones[1, 2, 3].

El seu funcionament es basa en la col·locació d'una serie de sensors col·locats en una certa zona geogràfica on treballen de manera conjunta per oferir la informació a una estació base.

Cal remarcar que aquests sensors tenen unes capacitats molt limitades en tots els nivells ja que el seu reduïda grandària provoca una limitació energètica important la qual limita les possibilitats de cada sensor. [4]

Aquesta limitació comporta molts problemes entre els que destaca la seguretat, tant a nivell físic com a nivell de transmissió.

A causa de les debilitats que hem esmentat es necessari dissenyar uns mecanismes de seguretat adaptats a aquesta tecnologia per reduir al màxim les vulnerabilitats respectant el consum energètic.

1.2 Motivació

La nostra intenció al realitzar aquest treball d'investigació és aprendre tot el possible sobre les xarxes de sensors, la seguretat en xarxes i l'aplicació dels seus principis al cas concret de les xarxes de sensors. Les xarxes de sensors son una tecnologia desconeguda per a nosaltres i tant pel seu concepte com per les seues aplicacions ens hem sentit atrets a conèixer-les mes en profunditat.

Ens motiva també el repte d'aplicar aquests coneixements a un cas real com es el protocol EDETA i contribuir d'alguna manera al desenvolupament que s'està duent a terme al nostre centre.

1.3 Objectius del treball

Aquest treball es centra en certs aspectes de la seguretat en les xarxes de sensors i possibles mesures de seguretat per protegir-les de les vulnerabilitats tractades. Per poder abordar aquests aspectes es necessari tractar en profunditat el funcionament d'aquest tipus de xarxa, que es veurà en el **segon capítol**.

A continuació, en el **tercer capítol**, si que entrarem al tema de la seguretat on estudiarem per separat les diferents classes d'atacs i diferents propostes per protegir-les. La intenció es explicar amb detall que es cada atac i per què es important protegir les xarxes d'aquests atacs i no d'altres per, després, encarar algunes solucions que s'han donat i que algun dia poden ser aplicables a les xarxes de sensors.

En el **quart capítol** i com aspecte no menys important tractarem com es poden implementar algunes de les defenses estudiades en un protocol desenvolupat a la Universitat Politècnica de València conegut com a EDETA. L'objectiu d'aquest quart capítol es tractar com s'implementarien en un sistema real tractant entre altres el consum energètic i el cost en missatges.

Per últim tindrem un **cinquè capítol** amb una valoració de tot el treball.

Pel que fa al repartiment del treball, ambdós autors ens hem repartit equitativament totes les tasques, tant de búsqueda d'informació com de redacció, concentrant-se cadascú en diferents seccions del projecte, pero no en exclusiva, estànt el treball dels dos present en totes les parts del document.

D'aquesta manera, Miquel ha concentrat el seu treball en el segon capitol, referent al funcionament de les xarxes de sensors, mentre que Enric ha desenvolupat la major part del capitol tercer, que parla mes en profunditat sobre la seguretat en aquest tipus de xarxes.

Pel que fa a l'analisi de protocols concrets (capitol 4), un s'ha encarregat de 3 d'ell, mentre que l'altre s'ha encarregat dels altres dos.

Finalment, les seccions d'introducció i conclusions han sidut redactades conjuntament pels dos autors.

2 Les xarxes de sensors

2.1 Introducció

Les xarxes de sensors estan pensades per poder actuar en diferents terrenys i situacions, el que comporta una disposició aleatòria dels nodes. Es per aquest motiu que les xarxes de sensors han de tenir protocols que faciliten l'auto-organització. A més a més els sensors han de ser capaços d'enviar només aquella informació necessitada.

A causa de les les característiques d'aquest tipus de xarxes com el major nombre de components que intervenen en la comunicació (molt superior als elements d'una xarxa tradicional), unes dràstiques limitacions energètiques o la propensió a tenir errors, trobem que s'han de canviar certs protocols de comunicació respecte als protocols clàssics de les xarxes standard.

2.2 Aproximació

Per poder entendre d'una manera més especialitzada el funcionament d'aquest tipus de xarxes, hem de parlar sobre certs factors de disseny i de la pila de protocols de comunicació.

Factors de disseny: Són tots els factors que s'han de tenir en compte per dissenyar una xarxa de sensors. Amb aquests factors podem determinar si es factible o no desplegar una xarxa de sensors tenint en compte el nombre de sensors aproximat que haurem de desplegar, el seu cost, les limitacions del hardware i la tolerància a errors dels sensors.

Exemple d'un node.

Sobre les limitacions del hardware s'ha de destacar que un node ha de tenir unes dimensions reduïdes, per tant totes les funcionalitats de captació d'informació han d'estar en poc espai. També tens una limitació energètica ja que cada sensor és independent entre si i disposa d'una bateria reduïda . Un excés de capacitats en un node pot fer que el consum es dispare. [5]

Com s'observa el consum energètic és de vital importància pel funcionament correcte de la xarxa. Un factor relacionat amb l'energia i no comentat es la resolució de

problemes vinculats a la comunicació com ara quan falla un node i s'ha calcular per on passaran els paquets de nou. És en aquesta qüestió on actualment es centra la investigació en el camp de les xarxes de sensors.

Altres factors igualment importants són la tipologia de la xarxa desplegada, l'entorn on es desplegaran els sensors i el mètode de comunicació dels nodes (radiofreqüència, Bluetoohth o Infraroig)

Pila de protocols: La pila de protocols per a xarxes de sensors intenta aconseguir un ús intel·ligent de l'energia disponible, mètodes de cooperació entre sensors, etc. La figura 1 mostra la pila de protocols utilitzada tant per els diferents nodes com per l'estació base:

- **Capa física:**

S'encarrega de triar la freqüència, la detecció de senyals, de la seva modulació i de xifrar les dades.

Les investigacions es centren en l'estalvi d'energia ja que el consum en grans xarxes és desproporcionat, ja sigui per les distàncies o per qüestions de modulació de senyals.

- **Capa d'enllaç de dades:**

S'encarrega de multiplexar els fluxos de dades, la detecció de paquets de dades, del control d'errors i de l'accés al medi.

Sobre aquest últim punt, s'ha de destacar que existeixen dos objectius. El primer d'ells és crear l'estructura de la xarxa establint els enllaços de comunicació entre els nodes. L'altre objectiu es trobar un mètode de comunicació eficient.

Com sempre, per a totes les solucions que es proposen sempre es busca un estalvi energètic important.

- **Capa de Xarxa:**

Aquesta capa es dissenya al voltant d'una sèrie de premisses: en primer lloc l'eficiència energètica, a continuació s'ha de tenir en compte que tota la informació s'envia a un punt central i per últim que la informació redundant (la mateixa informació que arriba a un node des de dos puts diferents) és útil només quan no tenim la certesa de treballar en una xarxa segura.

- **Capa de transport:**

S'utilitza especialment quan sabem que hi haurà un accés extern a la nostra xarxa. També es la capa encarregada del transport dels paquets de dades entre els diferents sensors i l'estació central.

Per al transport entre els nodes s'utilitzen protocols basats en UDP, mentre que per un accés extern s'utilitzaran els protocols TCP i UDP.

- **Capa d'aplicació:**

En aquesta capa, hi ha diversos protocols, cadascun orientat a una funció més o menys concreta.

2.3 Característiques de la comunicació

Per poder tenir una visió sobre la comunicació entre els diferents nodes i el punt central de recepció de dades de la xarxa, s'han de tenir en ment una sèrie de premisses com:

- No es poden utilitzar protocols de comunicació basats en IPs.

- Les dades s'han d'enviar a una estació central i ens podem trobar amb que per culpa del funcionament de la xarxa li arribi la mateixa informació des de dos punts diferents.

2.3.1 Factors que influeixen en la comunicació

- Xarxa dinàmica: Hem de tenir en compte totes les possibles distribucions i components d'una xarxa abans de desplegar-la.

- Desplegament dels nodes: En funció del desplegament (aleatori o organitzat) es fa ús d'un protocol o d'un altre

- Limitacions energètiques: Sempre es busca l'estalvi energètic.

- Models d'entrega de la informació: Segons l'objectiu de la xarxa pot interessar un flux constant d'entrega de dades, entregues cada cert temps, etc.

- Capacitats: Les capacitats operatives dels nodes.

- Agregació/Fusió de dades: L'agregació consisteix en eliminar els paquets duplicats. La fusió no és més que aquella situació on un node és capaç de generar una senyal més precisa reduint el soroll i utilitzant tècniques de combinació de senyals.

2.3.2 Aproximació a l'enrutament en les xarxes de sensors

El punt central de la nostra xarxa demana dades a una regió concreta i espera aquestes dades que provenen de sensors de la regió sol·licitada. Les dades es demanen mitjançant peticions i les aquestes són enviades utilitzant un sistema "attibute-based naming" per a saber les propietats dels paquets enviats al nostre punt central.

2.3.3 Protocols d'herència

Es basen en l'escalabilitat de les xarxes. S'intenta aconseguir una eficiència energètica considerable. Per aconseguir-ho es basa en una comunicació multi-salt i en l'us de l'agregació i fusió de les dades.

2.3.4 Altres protocols

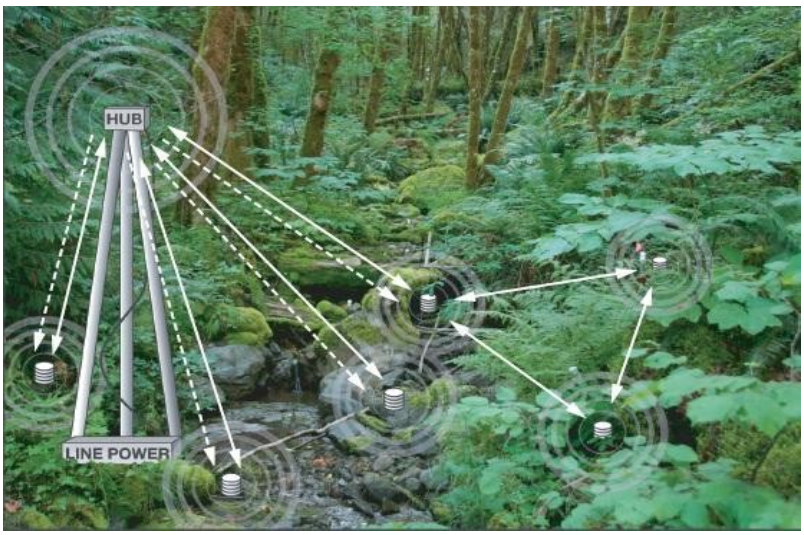
Routing protocol	*Data-centric*	*Hierarchical*	*Location-based*	*QoS*	*Network-flow*	*Data aggregation*
SPIN	✓					✓
Directed Diffusion	✓					✓
Rumor Routing	✓					✓
Shah et al.	✓		✓			
GBR	✓					✓
CADR	✓					
COUGAR	✓					✓
ACQUIRE	✓					
Fe et al.					✓	
LEACH		✓				✓
TEEN&APTEEN	✓	✓				✓
PEGASIS		✓				✓
Younis et al.		✓	✓			
Subramanian et al.		✓				✓
MECN&SMECN			✓			
GAF		✓	✓			
GEAR			✓			
Chang et al.		✓			✓	
Kalpakis et al.			✓		✓	
Akkaya et al.		✓		✓		
SAR				✓		
SPEED			✓	✓		

3 Seguretat en xarxes de sensors

3.1 Introducció

La seguretat en xarxes de sensors presenta grans reptes gràcies a les limitacions tant a nivell de comunicació com de consum i computació.

Aquestes limitacions es poden separar en funció de si estem davant de limitacions pròpies de cada node on trobaríem els problemes de computació, l'escassa potencia de cada node o les limitacions sobre el consum.



Els nodes poden estar expossats a un entorn natural

D'altra banda trobem les limitacions a la xarxa on s'inclouen les mateixes que trobem a les estructures ad hoc.

Per últim trobem les limitacions físiques que son les que poden afectar directament al node com poden ser danys provocats directament per l'home o per la natura, ja que els sensors poden ser desplegats a zones de risc o fins i tot poden anar muntats en soldats o vehicles [7].

3.2 Les xarxes de sensors i l'ad hoc

Les xarxes de de sensors són xarxes basades en ad hoc amb qui comparteixen alguns defectes com les limitacions de memòria, energia i freqüència. Aquestes limitacions juguen en contra de la seguretat i provoquen que sigui tot un repte garantir la confidencialitat de la comunicació, la integritat del missatge, l'autenticació de l'origen dels missatges i la disponibilitat dels nodes és tot un repte.

3.3 Classes de seguretat

També s'han d'avaluar quines són les amenaces més habituals, les quals solen produir-se a través de:

- Interrupció de funcionament: Això passa quan un dels responsables de la comunicació desapareix.

- Intercepció de dades.

- Modificació de la informació: Té lloc després de la intercepció de dades i pot provocar un atac per DoS.

- Fabricació: L'atacant afegeix informació errònia fent que la xarxa deixe de ser de confiança.

3.4 Possibles amenaces a una xarxa de sensors:

- Captura d'informació passiva: un atacant recull la informació dels nodes si no està xifrada.

- Subversió d'un node: si un atacant captura un node, a mes d'accedir a la seua informació, podria accedir a les seues claus d'encriptació, posant en perill tota la xarxa.

- Fals node: un atacant col·locaria un node maliciós per a injectar dades incorrectes a la xarxa.

3.4.1 Atacs mes freqüents

- **Bucles produïts durant l'enrutament**: Aquest tipus d'atac consistix a interferir en un diàleg entre nodes. Els missatges d'error falsos es poden generar quan l'atacant itera i repetix la informació enviada. Aquests bucles servixen per atraure o refusar el tràfic de xarxa en un determinat node i per incrementar la latència.

- **Retransmissió selectiva**: En aquesta ocasió el que realitza un node maligne, prèviament col·locat, és apartar algun missatge en comptes de retransmetre tots els que li arriben. Partint de la base de que tots els nodes són fiables en una xarxa de sensors, es provoca que al refusar alguns missatges, es fa creure a la xarxa que la ruta que va fins al punt central passant pel nostre node és la més ràpida, atraient cap a nosaltres més quantitat d'informació.

Les xarxes multi-salt com les de sensors, poden estar basades en la suposició de que els nodes participen respecte dels missatges que reben(contestar quan reben algun missatge o paquet). En un atac per retransmissió selectiva els nodes malignes poden refusar el re-enviament de certs missatges assegurant-se que no es propagaran més enllà del nostre node.

Una senzilla manera d'utilitzar aquesta classe d'atac és la de provocar que el nostre node siga un forat negre (atrauria molta informació però sense mostrar-se a ningú) que no conteste a cap dels missatges que li arriben provocant un mal funcionament de la xarxa. El problema es que els nodes veïns poden arribar a la conclusió de que es tracta d'un node avariat i es busque una altra ruta.

Una altra manera més subtil d'atacar amb aquest mètode es quan l'atacant contesta a certs paquets. Un rival interessat en l'eliminació o modificació de paquets de dades originals d'un cert grup de nodes poden, probablement, contestar a certs missatges i dissimular el mal funcionament de la xarxa, Tanmateix, és possible que l'atacant puga "escoltar" un flux que passa per nodes veïns i pot ser capaç d'emular el re-enviament selectiu causant una col·lisió en el paquet re-enviat que acaba d'escoltar. [8]

Però realitzar aquesta tasca pot ser molt difícil i habitualment aquesta classe d'atac es desviarà a un tipus d'atac similar al Sybil que vorem a continuació.

- **Sinkhole Attacks**: Per aquesta classe d'atac, consisteix en atraure cap a un node molt de tràfic. Contra més aprop estiga de l'estació central, més eficient serà l'atac.

- **Sybil**: Ara ens trobem davant una classe d'atac el qual es basa en que un node presenta diverses identitats per altres nodes de la xarxa. Entre altres coses també representa una amenaça per als protocols de enrutament, ja que aquests protocols en moltes ocasions necessiten intercanviar informació entre veïns per generar una ruta ràpida. Amb això el que es provoca es que podem estar infiltrats en més d'un node.

- **Wormholes**: Els atacs wormhole són una classe d'atac en el que la part que es vol infiltrar a la nostra xarxa rep una informació i la re-envia amb cert retard a altres nodes. En realitat la major utilitat d'aquesta classe d'atacs radica en tenir dos nodes malignes a la xarxa els quals generen un túnel provocant que un node recol·lecte informació i la envie cap a l'altre amb el retard esmentat.

De manera general aquesta classe d'atac també es pot utilitzar per aprofitar-se de les condicions de carrera. Una condició de carrera en aquest cas passa quan un node ha d'actuar d'una determinada manera a causa d'alguna instància d'un node i ignora la resta d'instàncies que rep fins que fa l'acció necessitada. En aquest cas un adversari pot ser capaç d'influir en la tipologia de la xarxa resultant.

Els wormhole són eficaços tant si la informació que es retransmet per la xarxa està xifrada com si està encriptada.

Per últim mencionar que aquesta classe d'atac es realment útil si es combina amb un atac de la classe sybil (aconseguiríem una detecció molt complicada) o amb retransmissió selectiva. [9]

- **Flood Attacks**: Ací el que es fa es enviar un missatge a tots els nodes simulant ser l'estació central provocant un desgast energètic elevat en els nodes. Això passa perquè al pensar que es el node central es contestarà sempre als missatges enviats pel fals node.

Una variant d'aquest atac es el HELLO flood. Alguns protocols requereixen que els nodes s'identifiquen a la xarxa. Per fer-ho envien missatges de la classe HELLO via broadcast per anunciar-se, i tots els nodes dins del seu radi l'acceptaran com a node veí vàlid. Però tot això pot ser fals ja que un atacant amb suficient capacitat operativa pot enviar per broadcast a tots els nodes d'una xarxa per molt llunyans que estiguen un missatge del tipus HELLO. D'aquesta manera quedaria infiltrat a la xarxa com un node més, el qual, a més a més, es veí de tots els nodes. [10]

Per exemple, una utilitat després de fer aquesta classe d'atac seria que es publiqués una ruta de gran qualitat (anunciada per l'atacant) i que passa per aquest fals node. Les conseqüències d'això serien fatals ja que deixaria la xarxa en un estat de confusió total ja que per una part els nodes més llunyans enviarien els paquets a través d'un node fora del seu radi(ells pensen que es un veí) i aquests mia arribarien al destí. Per altra banda, els altres nodes podrien arribar a utilitzat tots la mateixa ruta saturant la xarxa. [11]

Però el més greu apart d'aquesta saturació seria que tots els nodes que estarien dins el radi d'abast del fals node enviarien tota la informació directament cap a l'atacant, i podria arribar a donar-se el cas de que nodes que estan fora del radi i que poden perdre's o triar altres rutes per poder enviar les dades, podrien passar a l'atacant la seua informació.

- **DoS**: A nivell físic trobem atacs de denegació de servei, interferint amb les senyals de radio, el protocol de xarxa, o fins i tot amb la duració de les bateries dels nodes.

3.5 Criptografia

Degut a la topologia dinàmica i la falta de recursos, es difícil utilitzar la criptografia de manera eficient en les xarxes de sensors. La distribució de claus es produeix juntament amb l'establiment de comunicació inicial.

El sistema ha de ser capaç de reconèixer nodes desplegats posteriorment, no fer-ho amb els nodes no autoritzats, treballar sense saber a priori quins nodes seran veïns i no ha de consumir molts recursos.

- Criptografia de clau publica

  La criptografia de clau pública no es factible a les xarxes de sensors per tres raons: requerix una capacitat computacional que els nodes no tenen. Encara que la tingueren, el consum de bateria a l'hora de fer els càlculs seria enorme i no oposaria ninguna resistència a la captura de nodes.

- Criptografia clau simètrica:

  En un sistema de clau simètrica, cada node compartiria una clau amb tots els altres nodes, i per tant emmagatzemaria n-1 claus. Els nodes capturats no revelarien ninguna informació sobre la comunicació, i les claus podrien ser anul·lades en cas de que un atacant les obtinguera d'un node capturat.

3.5.1 Sistemes de distribució de claus

- **Clau mestra:** tots els nodes porten precarregada una clau mestra, que serà la que s'utilitzarà per establir una comunicació inicial i compartir les seues claus pròpies. Casa node dedicarà part de la seua memòria a guarda les claus. Si la clau mestra queda compromesa, tota la seguretat de la xarxa queda compromesa també.

  Existix una variant d'aquest esquema, proposada per Dutertre, per a quan els nodes es despleguen en diverses fases. Els nodes guardarien, a part de la clau mestra, una clau de generació de claus, que utilitzarien per a identificar-se amb els nodes nous. Després els dos nodes generarien una clau per a la comunicació. [12]

- **Predistribució aleatòria bàsica:** a cada node es precarreguen varies clau aleatòries d'un grup de claus predefinit. Els nodes trobaran una clau en comú per establir la comunicació inicial, i la utilitzaran com a clau compartida. La quantitat de claus del grup inicial serà una tal que dos subgrups qualsevol dels que es posaran als nodes, compartiran com a mínim una clau amb una probabilitat p. Tots els subgrups de claus que es posen als nodes eixiran del mateix grup inicial, així que la seguretat quedarà compromesa si l'atacant aconsegueix conèixer aquest grup inicial de claus. La predistribució de les claus consistix en 5 passos:

  1. Generació d'un grup inicial de clau P, i dels seus identificadors.

  2. Extracció de k claus del grup P per a establir el subgrup de claus d'un sensor.

  3. Carregar el sensor amb les seues claus.

4. Guardar els identificadors de les claus i el l'identificador del node associat en un node controlador.

5. Per a cada node, carregar el node controlador amb la clau que compartixen.

Aquesta fase de predistribució ens assegurarà que facen falta poques claus per node per a que tinguen la probabilitat desitjada de compartir clau.
En una fase posterior, els nodes enviaran mitjançant difusió i en text pla els identificadors de les seues claus. Aquells que compartisquen claus crearan un canal de comunicació encriptada.
A tots els parells de nodes que no queden connectats directament, però que estiguen connectats indirectament per un altre camí se'ls assignarà una clau de camí, i quedaran comunicats.
El node controlador pot revocar nodes que hagen estat compromesos. Amb un missatge de difusió, informarà als altres nodes de quines son les claus d'aquest node. Açò es tradueix en una bona resistència de la xarxa contra nodes capturats.

- **Q-composite:** En aquesta variant es necessiten q claus en comú per iniciar la comunicació. El grup inicial de claus serà mes reduït i s'utilitza mes d'una clau per a establir comunicació entre dos nodes.

- **Multipath:** Cada parell de nodes mantindrà una relació de tots els camins que els comuniquen a través d'altres nodes. Si la clau que utilitzen es veu compromesa, per exemple per la captura d'un node que també conté eixa clau, la comunicació entre els dos nodes primers deixaria de ser segura. Aquest esquema permet que aquests nodes actualitzen la clau que utilitzen per a comunicar-se per un dels altres camins indirectes. Aquest esquema es molt costós, ja que cada node ha de descobrir i mantenir tots els camins que el comuniquen amb els altres, que poden ser molts i molt llargs.

- **Random pairwise:** En aquest esquema s'assigna una única clau a cada parell de nodes. Aquest esquema es resistent a la captura de nodes, a la seua generació i la seua replicació. A diferencia de les variants anteriors, en aquesta els nodes identifiquen la identitat les seus companys. [13]

Abans de desplegar els nodes, es generen identitats per a cadascun d'ells (fins i tot algunes mes (per si es despleguen mes nodes en el futur). S'assignen nodes els uns als altres aleatòriament, i es genera una clau per cada parell de nodes assignats. Una vegada disposats, els nodes es buscaran entre ells per trobar els que estan assignats.

- **Predistribució en espai múltiple:** Aquest esquema es basa en el mètode de Blom introduït en 1985, que permet a cada parell de nodes trobar una clau per a establir comunicació. La xarxa tindria la forma d'un graf, i només es requeriria que aquest

graf estigués connectat, així que els nodes haurien d'emmagatzemar poca informació. Es carregaria informació de les claus als nodes abans de desplegar-los, per a que durant la inicialització de la xarxa pogueren trobar claus entre ells i els veïns, i establir comunicació. [14]

- **Coneixement de la disposició:** Els nodes es preordenen abans de ser desplegats, i es genera una clau per a cada parell de nodes veïns. Una vegada desplegats els nodes podran iniciar una comunicació segura amb els seus veïns preassignats.

- **Estació base coneguda:** una estació base servix les claus a tots els parells de nodes. Es l'únic punt vulnerable de l'esquema, però les comunicacions amb el servidor serien costoses, i els nodes mes propers al servidor esgotarien la seua energia ràpidament.

- **Distribució de clau triple:** 3 claus: 2 precarregades a cada node i una generada a la xarxa per a un clúster. El lider del clúster podrà descartar paquets, i utilitzarà la clau per a desencriptar els missatges que li arriben i preparar-los per al següent salt. Els nodes també desencriptaran els missatges quan arriben del lider del clúster, i estaran identificats per una ID i una MAC.

3.6 Enrutament segur

Característiques a tenir en compte:

- La organització IP es impossible.

- Els nodes s'han d'auto-organitzar.

- La major part del temps la comunicació es produirà entre un node i el lider del clúster.

- Limitacions dels nodes (energia, etc).

- Canvis freqüents en la topologia de la xarxa.

- Xarxa centrada en la aplicació i les dades.

Hi ha pocs protocols proposats per a xarxes de sensors. SPINS es una suite de seguretat proposada per a xarxes amb pocs recursos. Es divideix en 2 blocs: SNEP i µTESLA. Totes les primitives de criptografia son compartides per aquests dos. Açò, sumat a que utilitza un sistema de de criptografia simètric, redueix la utilització de recursos. Les dades no es poden autenticar amb criptografia simètrica, ja que tots els nodes coneixen la clau, això que µTESLA introdueix asimetria utilitzant revelació de clau retardada i altres mètodes. [15]

SNEP: utilitza encriptació, i "message authentication code" (MAC) per a assegurar la integritat de les dades. Altres característiques d'aquest protocol son:

- **Seguretat semàntica:** abans d'enviar el missatge, s'envia una cadena de bits aleatoris. Així, un possible atacant no podrà inferir el missatge encara que conega parrells de text xifrat i text pla.

- **Autenticació de dades:** Si el MAC es verifica, s'assegura que les dades son enviades per qui diu que les ha enviat.

- **Prevenció de dades repetides:** Les dues parts de la comunicació compartixen un comptador que incrementen després de comunicar cada bloc. D'eixa manera s'evita que algú puga repetir el missatge.

- **Dades fresques:** gràcies també a aquest comptador, ens assegurem que el missatge que ens arriba no s'ha començat a enviar fins que hem rebut l'anterior i hem incrementat el comptador a ambdues parts.

µTESLA: El nombre de nodes que podran enviar estarà restringit. S'utilitza un sistema de clau simètrica, però aquesta clau no sempre està disponible, sinó que l'alliberarà l'estació base de tant en tant. Els nodes estaran sincronitzats amb l'estació base, i sabran quan es alliberarà la clau. Els nodes guardaran els paquets rebuts en un buffer. Quan arribe el moment, l'estació base alliberarà la clau per difusió. Una vegada rebuda la clau, es pot autenticar el paquet, i seguir amb les comunicacions.

També tenen desavantatges aquestos protocols. Assumptes com atacs DoS, anàlisi de trafic o captura de nodes no son tractats. A mes, SPINS assumeix que la topologia de la xarxa es estàtica, cosa que no es certa.

INSENS [16]: tolera les intrusions saltant-se els nodes maliciosos en lloc de detectar les intrusions. El diseny d'INSENS es basa en tres punts:

- Per a evitar atacs de DoS, els nodes no poden fer difusions. L'autenticació de la base es fa mitjançant hash d'una sola direcció. D'aquesta manera, els nodes no poden floodejar la xarxa, i aquesta pot operar correctament en presencia d'intrusos.

- La informació d'enrutament ha de ser autenticada, per a prevenir fals enrutament. A més, tots els càlculs complicats, com la topologia de la xarxa, es fan a l'estació base, per estalviar recursos alls nodes.

- INSENS utilitza criptografia simètrica. Per evitar els problemes que açò ocasiona amb un node intrús, s'utilitzen i mantenen múltiples camins, per evitar els nodes maliciosos.

TinySec: es una arquitectura de seguretat al nivell d'enllaç. Es una arquitectura genèrica, no pensada per a xarxes de sensors, però es lleugera, i es pot integrar en aquestes. Com que cada node pot llegir i modificar les dades per a agregar o evitar redundància, autenticar el paquet només quan arriba pot ser un problema, ja que no verifiquem res entre els dos extrems de la comunicació.. A nivell d'enllaç, un paquet maliciós seria detectat a l'instant d'introduir-se a la xarxa. TinySec utilitza MAC i encriptació simètrica, encara que la encriptació serà opcional. També, gracies a un vector inicialitzat, oferix seguretat semàntica i protecció contra repetició de missatges, de manera similar a la descrita en SNEP. [17]

4 EDETA

4.1 Sybil

Com s'ha explicat a les seccions anterior, en un atac Sybil, un node intrús pot adoptar múltiples identitats a la xarxa de sensors, es a dir, pot fer-se passar per diferents nodes (i de diferents tipus).

A les amenaces que comporta una suplantació d'identitat, hi ha que sumar el fet de que, al fer-se passar per diversos nodes al mateix temps, un node Sybil posa en perill la integritat de tot el sistema d'enrutament [18]. En una xarxa auto-configurada, on els nodes s'organitzaren entre ells i obtingueren les rutes de les dades dinàmicament, un node Sybil deformaria i desviaria moltes d'aquestes rutes.

Aquest es el cas d'EDETA. A EDETA, no només les rutes s'obtenen dinàmicament, segons la distribució i els rols dels nodes, sinó que a mes aquestes rutes es re-calculen cada cert temps, quan hi ha canvis de líder, per exemple. [19]

Una altra particularitat d'EDETA, es que els nodes fulla es comuniquen única i exclusivament amb el seu node líder. Si un node Sybil es fa passar per un líder, tots els seus nodes fulla podrien quedar directament incomunicats amb la resta de la xarxa. Si a mes, com seria d'esperar en un node Sybil, es fa passar per mes d'un node líder, es podrien formar clústers enormes amb el node Sybil com a únic líder.

Una altra possibilitat es que el node Sybil es fera passar per diversos nodes fulla, ocupant per complet un o mes clústers.

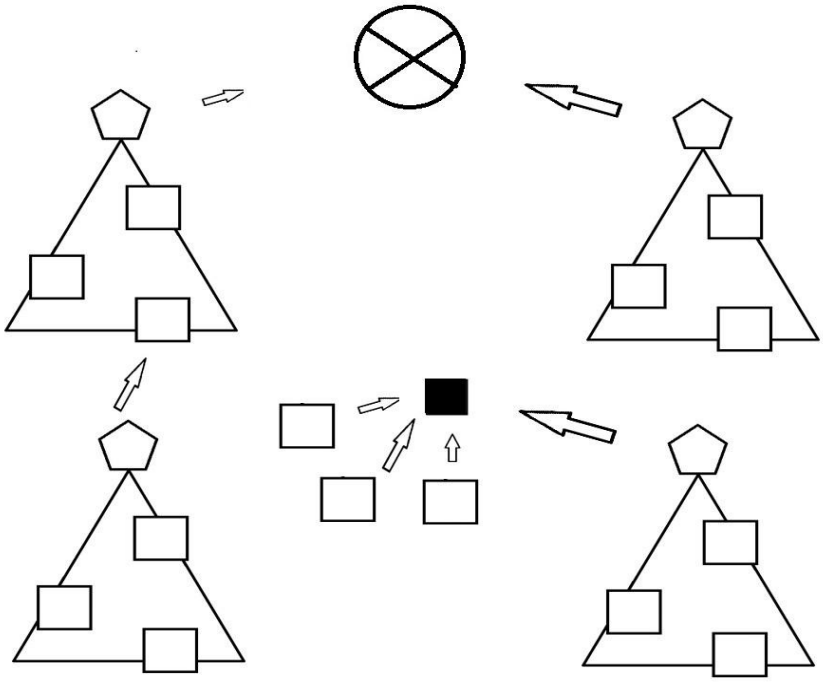


Diagrama d'un atac Sybil

La primera línia de defensa contra un atac Sybil es un sistema de validació de nodes. Alguns d'aquests sistemes ja s'han discutit a les seccions anteriors, i alguns d'ells, com la comprovació de recursos, els hem identificat com a no vàlids per a una xarxa de sensors. Amb recursos tan limitats, un node fals podria passar les proves fàcilment.

L'opció ideal, a priori, seria la de validació mitjançant claus predistribuides. Durant la fase de creació de l'arbre i els clústers, el líder i el node fulla es validarien mitjançant aquestes claus, i la fulla només passaria a formar part del clúster en cas de que ambdós nodes quedaren validats. Si la fulla no reconeguera al líder com un node vàlid, passaria a buscar-ne un altre. Si el líder no reconeguera a la fulla com a vàlida, no la deixaria unir-se al clúster.

De la mateixa manera, dos nodes líders es validarien l'un a l'altre abans de passar a comportar-se com a pare i fill. D'aquesta manera, si un node Sybil haguera pogut enganyar a diversos nodes fulla, aquests quedarien a la seua vegada incomunicats.

La implementació d'aquest sistema implicaria costos addicionals tant en la comunicació com en el processament de les claus per part de tots els nodes. Aquest cost seria relativament menut, ja que només es produiria durant la configuració de la xarxa.

Una alternativa, que concentraria els costos només sobre el líder, seria la comprovació de les ràdios. Durant la configuració de la xarxa, s'assignen canals de comunicació per a cada clúster, i per a la comunicació inter-clúster. Això significa que hi haurà un número limitat de freqüències utilitzades a la xarxa. Un node Sybil escoltarà i emetrà per moltes freqüències al mateix temps, així que si un node líder escoltara alguna cosa en freqüències no utilitzades, podria detectar els possibles nodes Sybil presents a la xarxa. Açò es podria fer al final de cada ronda de comunicació, mentre els nodes fulla dormen.

4.2 Suplantació

Un atac de suplantació, alteració o repetició es l'atac mes directe que pot sofrir una xarxa de sensors, i per tant, per simple que puga semblar, es un atac del qual ens hem de protegir. Per aquesta raó, aquestes tres variants han estat seleccionades com a un dels atacs per als quals implementarem una solució.

Al protocol EDETA, com a la majoria dels protocols per a xarxes de sensors, els nodes no tenen una identitat única. Per a que un node intrús es fera passar per un node vàlid, només hauria de seguir el protocol de comunicació de comunicació dels altres nodes. Si un node enviara trames vàlides, els altres nodes l'acceptarien com a un node vàlid sense mes comprovacions. D'aquesta manera, el node intrús podria interceptar les dades, introduir dades malicioses, o alterar les que ja circulen per la xarxa.

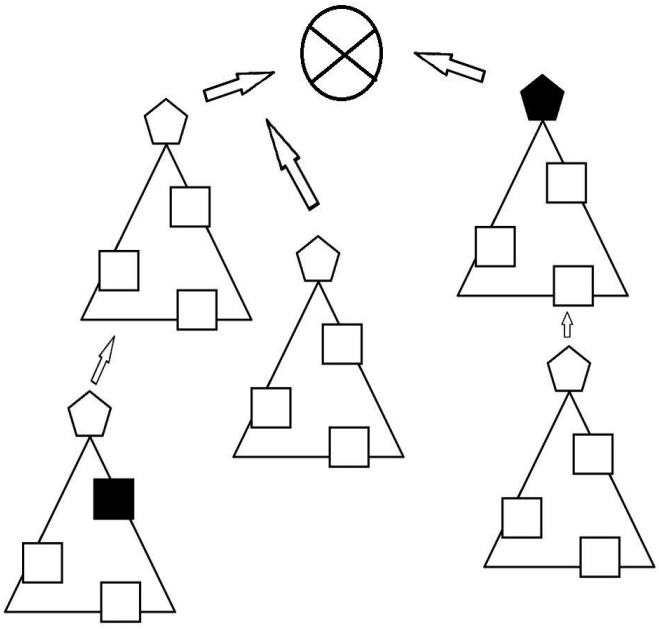


Diagrama d'un atac de suplantacio.

La solució elegida ha de garantir que cap node intrús puga fer-se passar per un node vàlid, i per a assolir-ho tenim dues alternatives:

- Autenticar els nodes abans de començar la comunicació

- Utilitzar encriptació.

Com es pot deduir, aquest atacs guarden similituds amb l'atac Sybil, i per tant també guardaran similituds les solucions.

Com s'ha argumentat a la secció de Sybil, implementar tot un sistema d'encriptació en la comunicació suposaria un gran cost tant computacional com energètic. Encara que queda com a una alternativa que es pot implementar si es necessari, considerem que la solució idònia es implantar un sistema d'autenticació de nodes mitjançant alguna variant de la predistribució de claus (que s'elegirà segons les característiques de la xarxa que vaja a instal·lar-se).

No només és la solució òptima, sinó que a mes la solució es la mateixa que en el cas de l'atac Sybil, així que no hem d'implementar solucions separades per a cada cas.

Així, en el temps de configuració de la xarxa, quan es creen els clústers i l'arbre, els nodes intercanviarien claus amb els nodes amb que volen associar-se. Només si es pogueren identificar l'un a l'altre com a vàlids, podrien passar a formar una associació Lider-Fulla o Líder-Líder. Si un node identificara a un altre com a no vàlid, l'associació no es produirà, i el node intentarà associar-se amb la seua següent opció. El node intrús quedarà d'aquesta manera aïllat de la resta de la xarxa.

El cost serà de dos missatges addicionals per cada associació que el node intente crear: un per a enviar les claus i un altre per acceptar o rebutjar les claus de l'altre node.

4.3 Retransmissió selectiva

La retransmissió selectiva es un dels atacs seleccionats per intentar protegir les xarxes de sensors EDETA gràcies a la important necessitat de fer arribar les dades al destí sense cap modificació, aconseguint la integritat de les dades i la no filtració de les mateixes.

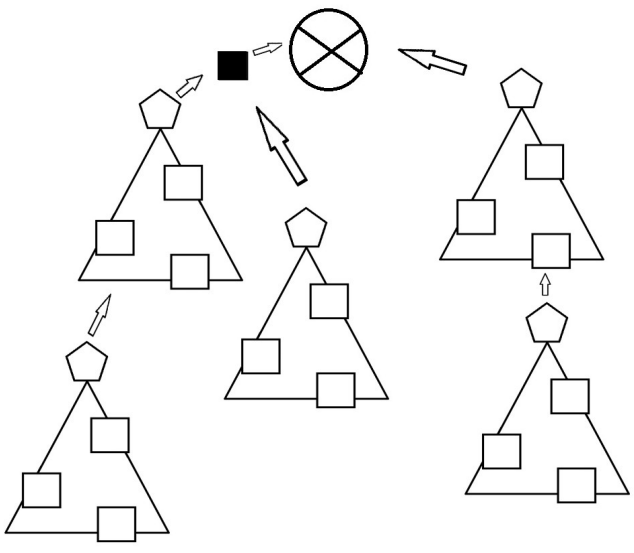


Diagrama d'un atac per retransmissió selectiva.

Aquesta importància sobre la conservació de les dades es vital per obtenir anàlisis fiables, etc.

Abans de parlar sobre el com implementem la defensa, hem de parlar sobre com el nostre protocol implementa l'encaminament dels missatges. EDETA utilitza una proposta basada en clústers i

arbres. El protocol en qüestió es el Intra-Cluster-Communication i a més a més d'estar basat en clúster, utilitza una pseudo aleatorització autorregulada per distribuir de manera equitativa el gast energètic entre els nodes de la xarxa, aconseguint maximitzar la vida de la mateixa. [20]

El funcionament es redueix a dividir la xarxa en diferents clústers on un d'ells actuarà com a lider i participarà de l'altra part de l'encaminament que es l'acció d'enviar dades al node central (protocol Inter-Cluster). Una dels principal avantatges es que gràcies a que el node lider no te la obligació de retransmetre les dades cap al node base, ens trobem davant d'un protocol molt escalable i que gaudeix d'una molt bona gestió energètica.

En resum, el funcionament del protocol és el següent:

- Fase d'inicialització: configuració de la xarxa.

- Fase de comunicació: més llarga que la d'inicialització per a minimitzar la sobrecàrrega, on es succeeixen una sèrie de rondes de comunicació.

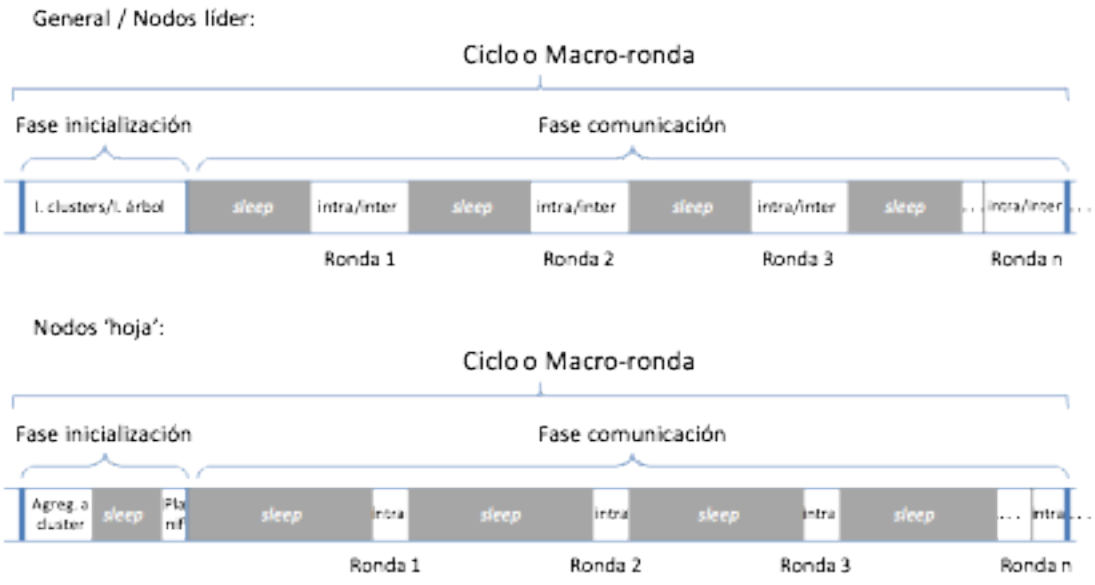


Figura X. Operación EDETA

De cara a la protecció sobre l'atac de la retransmissió selectiva, ens quedem amb la proposta "Higly-Resilient" que com ja hem comentat es basa en tenir una xarxa de sensors amb encaminament múltiple, cosa que EDETA permetria tant a nivell global com a nivell de clústers.

Per implementar aquest mètode ens fixem en la comunicació que es portaria a terme entre les diferents parts dels elements involucrats. Continuant l'explicació donada en apartats anteriors, la millor opció sobre aquesta protecció per EDETA es la que es

basa en la construcció dels diferents camins mitjançant una estructura de l'anomenada braided[21].

Aquest tipus d'estructura, menys eficient pel que fa a prestacions però amb molt bona gestió energètica i recuperació d'errors, es basa en la construcció de diversos camins entre dos punts. el mecanisme es el següent:

- El node central elabora una serie de camins fins al node al que vol sol·licitar informació, incloent la millor ruta (la qual podria ser una ruta afectada per un node maligne). Per enviar cada ruta, envia un missatge fins al node destí amb les rutes elaborades.

- El node rep les rutes i envia un missatge de confirmació

- S'envien les dades per les diferents rute (habitualment 3).

Seguint aquesta estructura podem observar que es cert el fet de l'estalvi energètic ja que el numero de missatges extra que intervenen en la comunicació és mínim, 2 per ruta, i no provoca tampoc un retard en l'enviament de les dades.

Per últim, el fet de tenir la xarxa subdividida en diferents clústers que augmenten el rendiment energètic, ens ofereix a priori poc marge de millor per aquest mètode de defensa.

La conclusió que podem extreure del procés es la justificació sobre el que ja s'ha dit anteriorment i es que l'atac de retransmissió selectiva es molt més impactant si es combina amb altres atacs com el sybil ja que per si sol, pot ser evitat conservant l'eficiència energètica tant important en les xarxes de sensors.

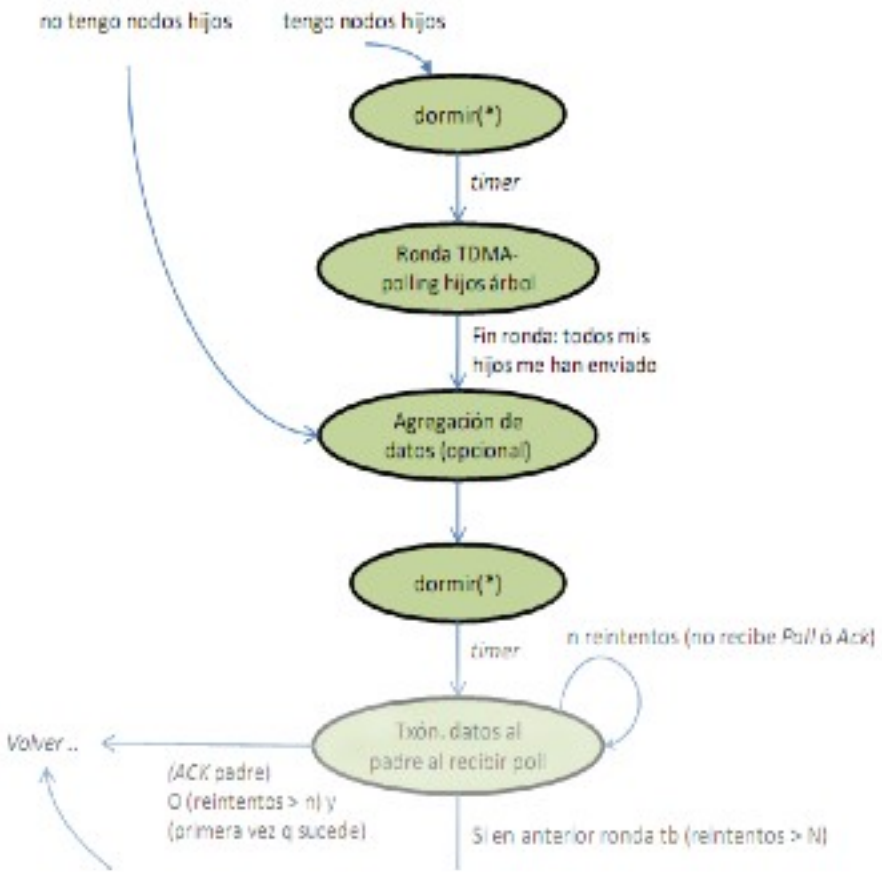
4.4 Hello Flood

En aquesta ocasió, trobem que el atac del tipus Hello flood és una vulnerabilitat present a les xarxes de sensors que es vital protegir a EDETA ja que al gestionar-se mitjançant una estructura de clústers fa que un atac exitós via Hello flood podria acabar amb tota l'operativitat de la xarxa ja sigui per pèrdua de informació o saturació.

Com ja hem parlat, EDETA utilitza una estructura dividida en clústers i utilitzarà, si implantem la solució a la retransmissió selectiva oferida en aquest document, un encaminament múltiple de la informació. A més, es necessari aclarir que entre els diferents clústers, EDETA utilitza un protocol anomenat inter-cluster-routing [22] el qual funciona intentant obtenir un màxim d'estalvi energètic ja que per passar a informació entre els firenets clústers fins arribar a l'estació base només en el moment

de la transferència es desperten. Això provoca que durant l'enviament de la informació dels nodes fill de cada clúster, el node pare estarà dormint. Aquest procés es pot observar a la següent figura amb major claredat:

Podem observar a més a més, que l'enviament només es durà a terme quan el node pare del clúster rebi l'ordre.



Per poder programar una bona defensa utilitzarem un mètode ja descrit el qual es basa en una limitació dels nodes veïns que es poden autenticar per clúster. El que aconseguim amb aquest mètode serà per una part aprofitar l'estructura de clústers del protocol EDETA (amb una implementació relativament senzilla) i evitar que un node maligne es coli a la nostra xarxa estan a gran distancia.

Com acabem de dir, aprofitant l'estructura d'EDETA, la implementació pot ser relativament senzilla ja que una vegada desplegats els diferents sensors i abans d'iniciar el normal funcionament de la xarxa, utilitzaríem una senzilla comunicació entre els diferents nodes fills i el seu pare identificant-se en aquell clúster. Això implicaria dos missatges:

- Identificació del node fill al node pare.

- Confirmació per part del pare al fill.

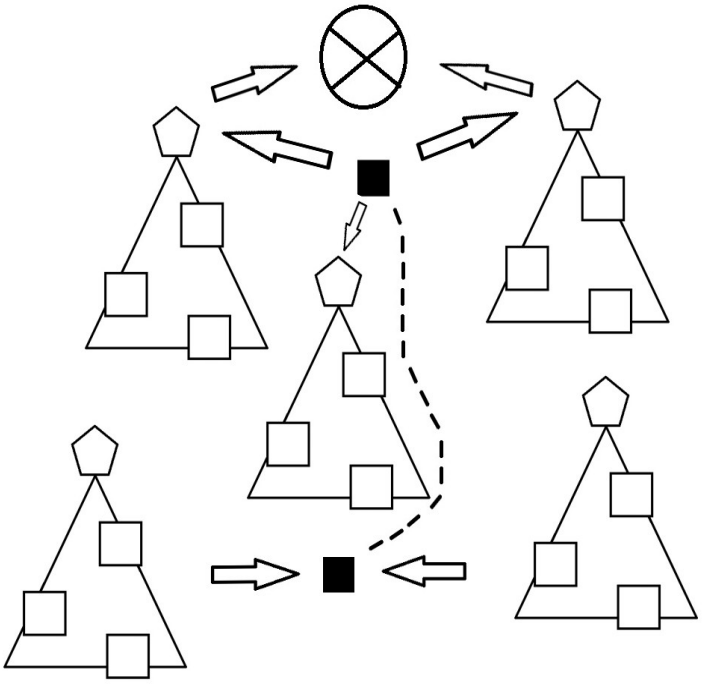
Amb aquest senzill mecanisme quedaria protegida la xarxa d'aquesta variant d'atac flood i aconseguiríem respectar un bon estalvi energètic ja que aprofitaríem al màxim la proposta d'arquitectura EDETA per xarxes de sensors.

El problema seria que un node maligne estiguera dins del rang d'un clúster i quedarà enquadrat com a fill legitim en un clúster on no tinguérem el màxim de nodes desplegats permesos. Per a solucionar això una proposta de millora d'aquest mecanisme de defensa radicaria en, una vegada desplegada la xarxa, impedir que més nodes pogueren ser afegits sense un permís especial de l'estació base de la xarxa.

4.5 Wormhole

Per el següent cas, hem d'indicar que el nostre motiu per el qual hem seleccionat l'atac de la classe wormhole per integrar-ho a la defensa d'EDETA es perquè les conseqüències d'un atac exitós provocarien en certes ocasions un funcionament radicalment diferent a el inicialment proposat ja que l'atacant podria disposar la capacitat per manipular la tipologia de la xarxa.

La solució per respondre a aquesta classe d'atac la trobem en un dels models de defensa proposats en l'apartat anterior. En concret en l'ultima solució proposada, l'inconvenient del qual es troba en que la nostra xarxa de sensors ha de ser estàtica. Una vegada solucionat aquest inconvenient on EDETA pot adaptar-s'hi, tenim que el principal argument de la defensa s'implementarà a través del càlcul dels RTT en el moment del desplegament de la xarxa.



Il·lustració : Diagrama d'un atac Wormhole

Aquests RTTS són calculats en tres fases diferenciades:

1.- La primera fase esta composta per l'enviament de 2 missatges: una

petició i una resposta. Aquests missatges s'utilitzen per construir una llista de tots els veïns.

2.- En aquesta fase el node arrel construirà un arbre on el resultat serà una relació entre tots els nodes de la xarxa. Mentre construeix l'arbre va obtenint els diferents RTT i una ruta concreta a seguir. L'RTT es calcula com a Trep-Treq

3.- Detecció d'un possible atac wormhole: Es en aquesta fase on es procedix a la detecció del possible atac. Si un RTT d'un node a un altre es més alt que el que tenim a la nostra llista, implica que es probable que tenim un node infiltrat.

L'avantatge de tenir-ho en EDETA es el tema dels clústers que permet fer subcalculs extra sense cost i tenir-ho tot encara més ben protegit.

Per augmentar l'efectivitat dels wormhole amb la solució proposada, poca cosa es pot fer ja que una correcta implementació permetria la detecció de pràcticament el 100% dels atacs amb un consum energètic més que acceptable i un nivell de falsos positius realment baix.

A més a més, seguint aquesta especificació proposada, no tindríem cap afegit extra ja que tot es basa en el càlcul dels diferents RTT.

5 Conclusions

Una vegada arribat a aquest punt, podem fer una vista enrere per veure quin va ser el nostre punt de partida i fer una petita avaluació de tot el nostre recorregut.

Les xarxes de sensors poden arribar a tenir molta utilitat en molts àmbits si tenen la inversió necessària. Tal i com reflectien les nostres motivacions el seu concepte és molt atractiu i durant l' elaboració de tot el projecte, em vist acomplerts gran part dels nostres objectius inicials ja que no només em descobert les possibilitats de les mateixes si no que també, gracies a endinsar-nos en aquesta classe de tecnologia, em après que encara que a pesar de tot el potencial, és una classe de tecnologia molt verda a nivell de seguretat.

El concepte de seguretat, per aquesta classe de xarxes cobra molta importància i un fil d' investigació molt important ja que tenim moltes limitacions. En aquest aspecte ha
ajudat molt el complement realitzat al fer l' estudi de diferents mètodes defensius al protocol EDETA desenvolupat al politècnic de València.

Tal i com hem esmentat, les xarxes de sensors tenen un gran futur. La realització

del projecte ens ha brindat l' oportunitat no només de realitzar un treball d'investigació, si no de poder intuir fins on poden arribar a ser d'importants ja que l' inversió es cada cop més elevada i es van trobant solucions més eficients als problemes de seguretat.

A pesar de tot, encara queda molt treball per a fer i nosaltres no em pogut abarcar tots els aspectes de les xarxes de sensors. No només s' ha de buscar un mètode eficient, si no que es molt important l' implementació sobre el protocol triat.

6 Referencies

[1] L. Schwiebert, S. Gupta, and J.Weinmann. Research challenges in wireless networks of biomedical sensors. En Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking (MobiCom), 2001.
[2]A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson. Wireless sensor networks for habitat monitoring. En Proceedings of the ACM International Workshop on Wireless Sensor Networks and Applications (WSNA), 2002.
[3] Mark A. Perillo and Wendi B. Heinzelman. Wireless Sensor Network Protocols. En Introduction to Wireless Sensor Networks. Department of Electrical and Computer EngineeringUniversity of Rochester.
[4] Power aware routing for mobile ad-hoc network. En Introduction.
[5] Power aware routing for mobile ad-hoc network. En Abstract.
[6] Kemal Akkaya and Mohamed Younis. A Survey on Routing Protocols for Wireless Sensor Networks. En Introduction. Department of Computer Science and Electrical Engineering University of Maryland, Baltimore County.
[7] Mark A. Perillo and Wendi B. Heinzelman. Wireless Sensor Network Protocols. En Taxonomy of Sensor Networks. Department of Electrical and Computer Engineering University of Rochester.
[8] C. Karlof and David Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. En Selective forwarding. Ad Hoc Networks 1 (2003) 293 –315
[9] C. Karlof and David Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. En Wormholes. Ad Hoc Networks 1 (2003) 293 –315
[10] Counter measure against HELLO flood attacks (bidirectional verification)
[11] C. Karlof and David Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. En HELLO flood attack. Ad Hoc Networks 1 (2003) 293 –315
[12] Seyit A. C. and B. Yenr. Key Distribution Mechanisms for Wireless Sensor Networks: a Survey. En Master key based key pre-distribution solutions. Rensselaer Polytechnic Institute.
[13] Seyit A. C. and B. Yenr. Key Distribution Mechanisms for Wireless Sensor Networks: a Survey. En Pair-wise key pre-distribution solutions. Rensselaer Polytechnic Institute.
[14] Seyit A. C. and B. Yenr. Key Distribution Mechanisms for Wireless Sensor

Networks: a Survey. En Key matrix based dynamic key generation solutions. Rensselaer Polytechnic Institute.
[15] T. Zia and Albert Y. Zomaya. Algorithms and protocols for wireless sensor networks - Security Issues and Countermeasures in Wireless Sensor Networks. En SPINS: Security Protocols for Sensor Networks. 2008.
[16] T. Zia and Albert Y. Zomaya. Algorithms and protocols for wireless sensor networks - Security Issues and Countermeasures in Wireless Sensor Networks. INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks. 2008.
[17] T. Zia and Albert Y. Zomaya. Algorithms and protocols for wireless sensor networks - Security Issues and Countermeasures in Wireless Sensor Networks. TinySec: A Link Layer Security Architecture. 2008.
[18] C. Karlof and David Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. En The sybil attack. Ad Hoc Networks 1 (2003) 293 –315
[19] J.V. Capella. Redes inalambricas de sensores:Una nueva arquitectura eficiente y robusta basada en jerarquia dinamica de grupos. Protocolo de encaminamiento EDETA. En Arquitectura propuesta. Departamento de informatica de sistemas y computadores, UPV. 2010.
[20] J.V. Capella. Redes inalambricas de sensores:Una nueva arquitectura eficiente y robusta basada en jerarquia dinamica de grupos. Protocolo de encaminamiento EDETA. En El protocolo Intra-Cluster-Communication. Departamento de informatica de sistemas y computadores, UPV. 2010.
[21] C. Karlof and David Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. En Selective forwarding. Ad Hoc Networks 1 (2003) 293 –315
[22] J.V. Capella. Redes inalambricas de sensores:Una nueva arquitectura eficiente y robusta basada en jerarquia dinamica de grupos. Protocolo de encaminamiento EDETA. En Arquitectura propuesta. Departamento de informatica de sistemas y computadores, UPV. 2010.