La triangulation distribuée : une source de confiance

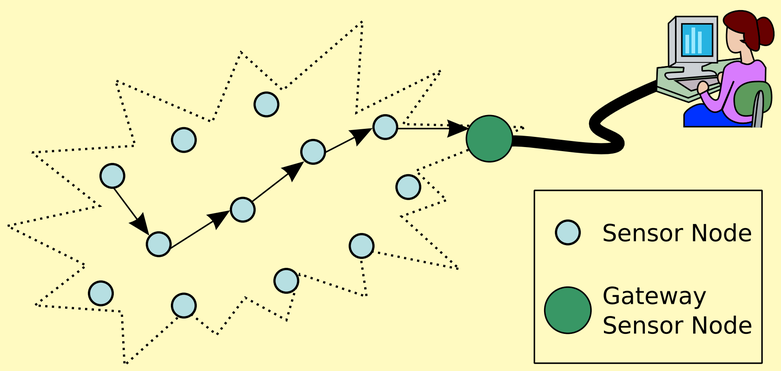
martin.peres@ensi-bourges.fr ; {chalouf, krief}@labri.fr

Réseaux de capteurs sans fil

Un capteur est un ordinateur miniature. Un aperçu des ressources disponibles pour le capteur mica2dot de Crossbow est donné par le tableau suivant.

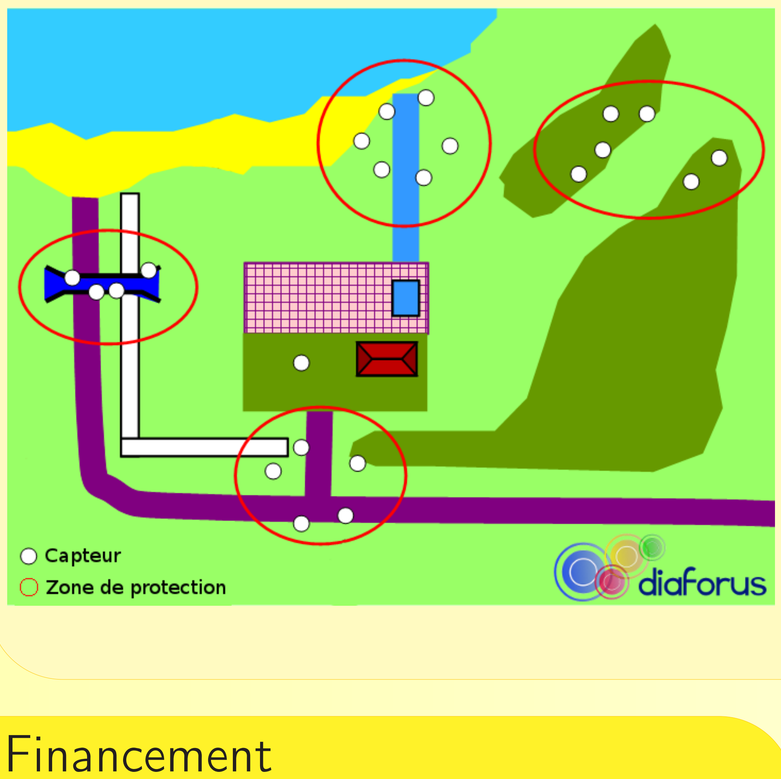
Type	Value
Type de microcontroleur	AVR, 8 bits
Fréquence de fonctionnement	4 MHz
Mémoire programme	128 Ko
Taille de la mémoire vive	4 Ko
Alimentation	560 mAh
uC repos avec timer actif	0.054 mW
uC actif radio off	36 mW
uC actif, radio écoute passive	66 mW
uC actif, radio TX/RX	117 mW

Un réseau de capteurs sans fil est constitué de plusieurs capteurs ainsi que d'une passerelle. Les noeuds communiquent entre eux et participent au routage pour remonter les informations venant des capteurs vers la passerelle. La passerelle fait ensuite le lien entre le réseau de capteurs sans fil et un réseau plus conventionnel. La figure suivante explique ce fonctionnement.



Diaforus

Diaforus est un projet proposé par l'agence nationale de la recherche (ANR). Il a pour but la création d'un framework proposant de la coopération et du raisonnement à l'intérieur d'un réseau de capteurs sans fil hétérogène.
La coopération entre les différents noeuds et un niveau de sécurité adaptatif à l'intérieur du réseau permettent un comportement évolutif en fonction du contexte, ce qui permet d'économiser de l'énergie.
Lors de sa démonstration, ce framework sera utilisé dans le cadre de la détection d'intrusion.
Un exemple de déploiement du projet Diaforus autour d'une villa:



Financement

Ces recherches sont financées par l'ANR dans le cadre du projet Diaforus qui devrait se terminer en septembre 2012.

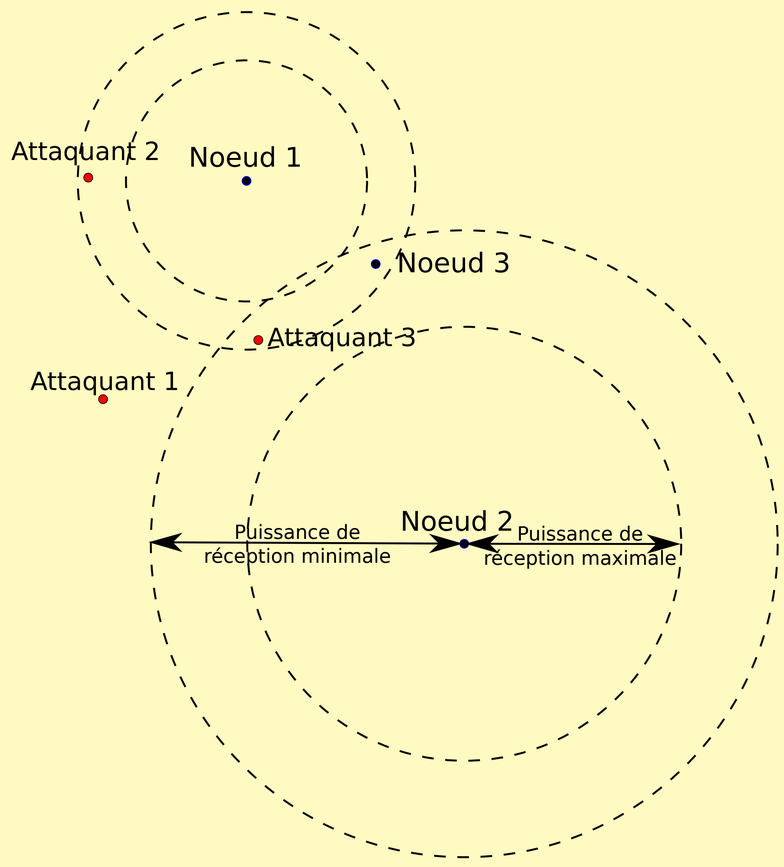
Problématique

La sécurité dans les réseaux de capteurs dépend actuellement beaucoup de la cryptographie.
Cependant, sans co-processeur cryptographique, l'utilisation du chiffrement symétrique AES-128 double la consommation nécessaire à une transmission. La signature d'un message en utilisant la cryptographie asymétrique (ECDSA) peut, à elle seule, multiplier par 10 le coût d'une transmission.

Dans le cadre du projet Diaforus, nous nous sommes intéressés à la diminution du coût de la sécurité dans les réseaux de capteurs.

La triangulation distribuée

Par apprentissage, la triangulation distribuée permet à un noeud d'associer une puissance de réception usuelle à tous les noeuds environnants. Lors de la réception d'un paquet, si la puissance de celle-ci est hors des bornes habituelles, un noeud est en droit de douter de la légitimité du message.



Dans cette figure, les attaquants essayent de se faire passer pour le Noeud 3 auprès du Noeud 1. Le Noeud 1 peut détecter l'Attaquant 1 mais pas les attaquants 2 et 3.
Pour les détecter, il faut mettre en place de la collaboration entre les noeuds du réseau. Tout noeud du réseau doit écouter les en-têtes réseau échangées et contrôler la puissance de réception. Si cette puissance est anormale, une alerte doit être émise au destinataire du paquet.
Avec cette collaboration, le Noeud 2 peut émettre une alerte quand l'Attaquant 2 essaye de se faire passer pour le Noeud 1. Le Noeud 3 peut aussi émettre une alerte quand celui-ci détecte qu'un autre capteur essaye d'usurper son identité.
Le noeud destinataire peut ensuite choisir d'accepter/rejeter le message ou de demander une signature ou une autre forme d'authentification.

Contribution

C'est dans cette optique que nous avons décidé de chercher des solutions pour la sécurité.
Notre proposition est d'utiliser la couche physique, le médium de communication, comme une source d'authentification et de confiance.
L'idée générale revient à utiliser le réseau de capteurs pour trianguler la source d'un message.
L'authentification est donc faite sur une caractéristique immuable, l'atténuation de la couche physique au lieu de faire seulement confiance à un secret partagé et/ou à la cryptographie.
Cette solution est donc potentiellement moins gourmande en mémoire et en énergie.

Domaine d'application

Le domaine d'application de la triangulation distribuée est:
- réseau de capteurs fixe;
- capteurs communiquant à vue;
- environnement peu perturbé;
- capteurs non-localisables facilement de façon à être moins vulnérables aux attaques utilisant des antennes directionnelles pour empêcher la collaboration entre les noeuds.

La confiance et réputation

La confiance et la réputation sont en général basés sur les informations relatives au routage.
Notre contribution peut être mise à profit comme source de confiance qui peut être utilisée lors de l'agrégation de données, mais aussi pour le bon fonctionnement de notre proposition.
En effet, il faut récompenser les noeuds participants à la détection d'attaques mais il faut aussi punir les noeuds émettant de fausses alertes.

Évaluation

Un protocole expérimental a été défini et étudié d'un point de vue théorique.
Le tableau suivant présente la surconsommation énergétique globale maximale par message due à la triangulation distribuée en fonction du nombre de noeuds, et de la probabilité qu'un message ne soit pas reçu avec la bonne puissance.

Proba. / Nb. noeuds	2	10	100
1	105.66	705.6	6705
0.1	10.566	70.56	670.5
0.01	1.0566	7.056	67.05

Le second tableau compare les coûts de transmission d'un message en fonction du nombre de noeuds et compare ce coût avec le surcoût induit par la triangulation distribuée.

Nb. noeuds	2	10	100
Coût trans.	9.63	47.7	428.4
DT-OH p=1	1097%	1479%	1565%
DT-OH p=1%	10.97%	14.79%	15.65%
DT-OH p=1‰	1.097%	1.479%	1.565%

Conclusion

Le coût de la triangulation distribuée dépend énormément de la probabilité d'occurrence d'un message ayant une puissance de réception sortant des bornes ordinaires.
C'est pour cela qu'il est important que les capteurs soient disposés de manière à ce qu'ils puissent communiquer à vue. Ainsi, ils seront moins sensibles à l'environnement, ce qui devrait diminuer le coût de la contribution.
Le surcoût réel sera évalué dans des travaux futurs à partir de résultats expérimentaux.