La couche physique comme source de confiance dans les réseaux de capteurs sans fil

Martin Peres
LaBRI
Université Bordeaux 1
Email : martin.peres@ensi-bourges.fr

Mohamed Aymen Chalouf
LaBRI
Université Bordeaux 1
Email : chalouf@labri.fr

Francine Krief
LaBRI
Université Bordeaux 1
Email : krief@labri.fr

***Résumé*—Les solutions d'authentification actuelles sont pour la plupart basées sur une forme de cryptographie ou de secret partagé. Ces méthodes sont particulièrement efficaces mais ne sont pas collaboratives. Dans cet article nous proposons une approche qui consiste à utiliser les propriétés physiques du médium de transmission pour calculer, lors de la réception d'un message, l'indice de confiance que l'on attribue à la source du message. Ceci permet de savoir s'il est nécessaire d'effectuer une authentification par cryptographie asymétrique ou si l'on peut avoir une confiance relative en la source. Dans le cas où les capteurs sont fixes et les communications peu perturbées par l'environnement, cet indice permet de rajouter une couche de contrôle au dessus d'un chiffrement symétrique pour vérifier davantage l'origine des messages. L'article s'attachera ensuite à expliquer en quoi la collaboration entre les noeuds permet d'améliorer la détection d'un noeud intrus ou malicieux.**

I. Introduction

Les réseaux de capteurs sans fil sont utilisés dans des domaines multiples tels que la surveillance de la qualité de l'air, de l'activité sismique, des incendies de forêt ou encore dans l'analyse de l'intégrité d'un bâtiment ou d'une zone pour faire de la détection d'intrusion. C'est sur ce dernier que nous travaillons dans le cadre du projet ANR DIAFORUS [1].

La sécurité de ces réseaux est un sujet de recherche actif depuis de nombreuses années. Ceci peut être expliqué par les contraintes drastiques ainsi que le besoin en sécurité envers les données collectées qui doivent être fiables et auditables. Cela est d'autant plus vrai que la mise en oeuvre de ces réseaux coûte cher.

II. État de l'art

A. La sécurité des réseaux

Dans l'informatique classique, l'intégrité et la confidentialité sont essentiellement résolues par des approches basées sur la cryptographie asymétrique telles que la signature électronique des messages ou le chiffrement du trafic réseau avec une négociation des paramètres de sécurité comme le handshake de SSL ou IKE d'IPSEC. Cependant, ces techniques sont gourmandes en ressources. Ceci induit une latence à l'émission ainsi qu'une sur-consommation énergétique importante [2][3] dans le cadre des réseaux de capteurs.

Pour diminuer l'empreinte sur les ressources lors de la phase d'échange de clé, l'utilisation d'algorithmes basés sur les courbes elliptiques [2][3] à la place de RSA [4] permet de réduire considérablement la consommation.

Des travaux comme SPINS [5] proposent des protocoles de sécurité adaptés aux réseaux de capteurs sans fil. SNEP permet par exemple de garantir la confidentialité et l'intégrité dans les communications point à point alors que μTESLA permet de garantir l'intégrité pour les communications de type broadcast.

B. La confiance et la réputation

La sécurité réseau ne suffit pas pour garantir la validité des informations car un attaquant peut compromettre un ou plusieurs noeuds du réseau par un accès physique ou à distance [6].

De plus, dans le cas de réseaux hétérogènes contenant des capteurs de différentes entreprises, il faut encourager la collaboration et punir les comportements égoïstes [7].

Les pistes de recherches actuelles pour répondre à ce problème consistent en l'attribution d'un score de réputation et de confiance [7] puis l'utilisation de ce score pour accepter ou non les données venant de ce capteur.

Le score de réputation est généralement calculé à partir du comportement d'un noeud vis à vis du routage, cependant, il est aussi possible de contrôler le comportement vis à vis d'autre protocoles de la couche physique à la couche applicative.

III. Proposition

Ce papier propose une nouvelle source d'information pour la gestion de la confiance et propose un protocole d'authentification qui permet, par exemple, de résoudre le problème de confiance nécessaire entre les noeuds d'un réseaux ayant fait le choix d'utiliser une clé réseau partagée.

Dans un premier temps, nous introduirons notre solution d'un point de vu local puis nous le généraliserons à un réseau. Pour finir, nous présenterons les attaques possibles et les limites de notre système.

A. Monitoring de la couche physique

Les solutions d'authentification actuelles sont essentiellement basées sur une forme de cryptographie ou de secret partagé. Bien que particulièrement efficaces, ces méthodes ne protègent pas toujours des attaques internes. En effet, dans le

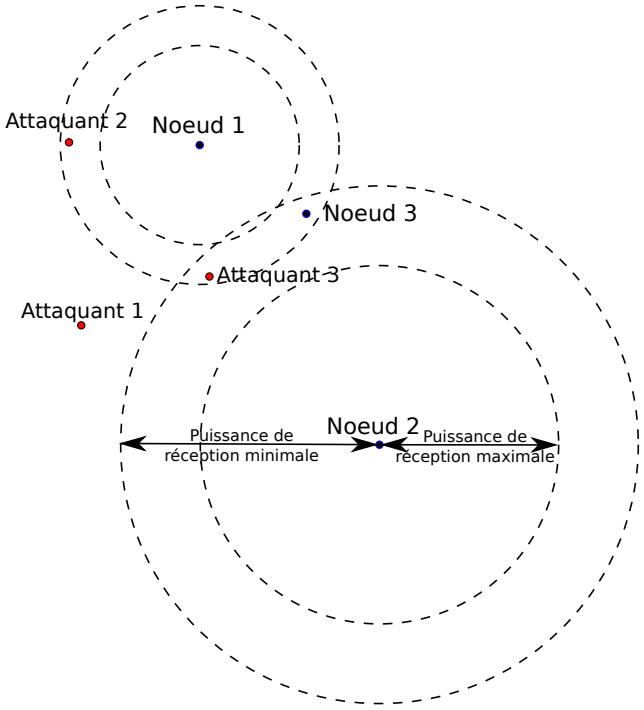

FIGURE 1. Triangulation distribuée : Les attaquants 1, 2 et 3 essayent de se faire passer pour le noeud 3

cas d'un réseau à clé partagée unique, n'importe quel noeud du réseau peut se faire passer pour un autre.

Il est cependant possible de valider l'origine d'une trame en se basant sur une caractéristique physique des réseaux de capteurs sans fil, leur sédentarité.

Il est en effet possible d'utiliser la puissance de réception d'une trame pour évaluer la probabilité que cette trame provienne bien de la présumée source.

Par expérience, un capteur peut associer à chaque noeud du réseau une puissance de réception minimale et maximale. Si l'on regarde la figure 1, on voit que cela suffit pour détecter l'attaquant 1 lorsqu'il veut se faire passer pour le noeud 3 auprès du noeud 1 mais il ne peut pas détecter les attaquants 2 et 3 lorsqu'ils essayent de faire la même chose.

L'indice de confiance est calculé par un noeud lors de la réception d'un message. Sa valeur va permettre à ce noeud de prendre une décision. En effet, lorsque l'indice de confiance est en dessous d'un certain seuil, ce noeud, destinataire du message, va demander à l'émetteur la transmission de la signature associée à ce message. Au contraire, si l'indice de confiance est au dessus du seuil, le capteur devra décider si il doit demander ou pas une signature à l'émetteur. Cela permet de détecter un éventuel noeud malicieux qui aurait réussi son attaque. Cependant, pour ne pas utiliser trop de ressources, ce choix devra être fait très rarement.

B. La triangulation distribuée

L'attaquant 2 de la figure 1 essaye de se faire passer pour le noeud 3 auprès du noeud 1. Le noeud 1 recevant une puissance normale, il ne peut se douter que le message est originaire de l'attaquant 2. Cependant, le noeud 2 détecte une puissance de réception anormalement faible, il va donc émettre une alerte destinée au noeud 1 pour le prévenir d'une potentielle attaque.

De plus, si un noeud détecte qu'un autre noeud essaye de se faire passer pour lui, il doit envoyer un message signé qui prouvera son identité et démasquera ainsi le noeud intrus/malicieux.

Un noeud doit donc attendre un certain temps après la réception d'une trame de façon à récupérer d'éventuels messages d'alerte. Ce noeud peut donc ensuite utiliser les informations qu'il a acquis pour améliorer son indice de confiance envers la trame et sur son émetteur.

Dernier étape, les noeud 1 et 3 devront ensuite diminuer le niveau de réputation du noeud 3 car celui-ci fait potentiellement l'objet d'une attaque.

C. Les limites et vulnérabilités de la triangulation distribuée

Du fait de la variabilité de l'atténuation du médium due à l'environnement, il est impossible de localiser très précisément un noeud. Ainsi, on ne peut pas différencier 2 noeuds très proches comme c'est le cas de l'attaquant 3 de la figure 1. Cependant, l'ajout de noeuds aide à augmenter la précision et pourrait permettre la détection de l'attaquant 3.

Il est aussi conseillé de cacher les capteurs de façon à empêcher un éventuel attaquant de pointer une antenne directionnelle vers l'un d'eux et ainsi, cours-circuiter la validation distribuée.

IV. CONCLUSION

Bien qu'il soit impossible d'identifier formellement un noeud par autre chose que la cryptographie, il est cependant possible de limiter fortement le sur-coût énergétique grâce à l'utilisation de la triangulation distribuée sans trop perdre de sécurité. Ce sur-coût sera évalué et d'autres caractéristiques de la couche physique seront exploités dans de futurs travaux.

RÉFÉRENCES

[1] LaBRI, "Diaforus," https://diaforus.labri.fr/doku.php, 2010, [Online ; accessed 15-May-2011].

[2] E. oliver Blaß and M. Zitterbart, "Towards acceptable public-key encryption in sensor networks," in *in The 2nd International Workshop on Ubiquitous Computing (ACM SIGMIS*, 2005, pp. 88–93.

[3] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in *Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications*. Washington, DC, USA : IEEE Computer Society, 2005, pp. 324–328.

[4] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, pp. 120–126, February 1978.

[5] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "Spins : security protocols for sensor networks," *Wirel. Netw.*, vol. 8, pp. 521–534, September 2002.

[6] W. Zhang, S. Das, and Y. Liu, "A trust based framework for secure data aggregation in wireless sensor networks," in *Sensor and Ad Hoc Communications and Networks, 2006. SECON '06. 2006 3rd Annual IEEE Communications Society on*, vol. 1, sept. 2006, pp. 60 –69.

[7] A. Srinivasan, J. Teitelbaum, H. Liang, J. Wu, and M. Cardei, *Algorithms and Protocols for Wireless Ad Hoc and Sensor Networks*. John Wiley & Sons, 2008, ch. Reputation and Trust-Based Systems for Ad Hoc and Sensor Networks.