Proposition de recherche doctorale

Securite et detection d'anomalies dans les reseaux de capteurs sans fils medicaux

Mots clés :

- **Directeur de thèse** : ahmed MEHAOUA
- **Co-encadrant(s)** :
- **Unité de recherche** : Laboratoire d'Informatique PAris DEscartes
- **Ecole doctorale** : École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal**: Divers

Résumé du projet de recherche (Langue 1)

Les progrès réalisés ces dernières décennies dans les domaines de la microélectronique et des technologies de communication sans fil, ont permis de produire avec un coût raisonnable des micro capteurs, qui sont de véritables systèmes embarqués. Le déploiement de plusieurs d'entre eux sur le corps humain, en vue de collecter et transmettre des données physiologiques (température, pression artérielle, humidité, rythme cardiaque, …) vers un ou plusieurs points de collecte, d'une manière autonome, forme un réseau de capteurs sans fil - Wireless Body Sensor Networks (WBSN). L'utilisation de ces capteurs dans le domaine médicale, apporte des nouveaux conforts aux patients (spécialement pour la surveillance à distance de personnes à mobilité réduite). Les réseaux des capteurs sont utilisés aujourd'hui dans la médecine pour surveiller certains signes vitaux. L'utilisation des réseaux sans fil pourra améliorer la qualité du soin (comme l'absence d'une installation électrique contraignante, encombrement de fils reliant les capteurs à l'unité de traitement, facilité de mise en place, liberté du mouvement pour le patient, etc.). Ces réseaux de capteurs sans fils soulèvent de nouveaux défis en termes de sécurité (authentification) et de protection contre les anomalies (pannes, attaques, intrusions, …) des émetteurs. Le mode de communication sans fil utilisé entre ces capteurs et l'unité de traitement (sink) accentue ces vulnérabilités. Les réseaux de capteur sont des réseaux avec des fortes contraintes en termes d'énergie, de mémoire, capacité de traitement limité, etc. Par exemple, la mémoire d'un capteur est parfois insuffisante pour stocker le code et les variables utilisées par les algorithmes de cryptographie asymétrique. La détection et la prévention automatiques des anomalies est un aspect majeur dans ce type de réseau sans fil. L'important étant d'empêcher les utilisateurs malicieux de capturer les paquets ou d'injecter des informations erronées dans ce réseau pour perturber le fonctionnement des capteurs ou l'intégrité des données. L'injection de données erronées (nuisance) soit par un utilisateur malicieux dans le réseau, soit par le dysfonctionnement d'un capteur peuvent avoir des influences inattendues sur le fonctionnement du réseau. L'identification d'un comportement anormale pour isoler ce capteur et pour rétablir un mode de fonctionnement normale est un des objectives principales de cette thèse. L'utilisation de méthodes de détection d'anomalies permet ainsi de détecter ce comportement en fournissant au point de collecte la possibilité de filtrer les trafics nuisibles. L'objectif de ce travail de recherche est la mise en place de modèles et de mécanismes de sécurisation et de fiabilisation du réseau de capteurs médicaux qui est adaptée aux contraintes de ses systèmes embarqués, pour la détection des anomalies et la sécurisation des communications entre les capteurs et l'unité de traitement ou de collection de données (sink).

Résumé du projet de recherche (Langue 2)

Ce travail de recherche consistera à : • Réaliser un état d'art sur les problèmes et solutions de sécurité et de détection d'anomalies dans les réseaux de capteurs sans fils médicaux ; • Proposer et évaluer des algorithmes et mécanismes automatiques de détection d'anomalies pour fiabiliser le réseau et les communications. Ceux-ci pourront être basés sur des techniques d'apprentissage automatique et/ou d'analyses statistiques : réseaux bayesiens, Filtres de Bloom, chaînes de Markov Cachés, etc …. • Evaluation des propositions par résolution analytique, simulations et expérimentations

Informations complémentaires (Langue 2)

Références : [COD04] Division of Engineering and Apllied Sciences of Havard University. CodeBlue: Wireless Sensor Networks for Medical Care. http://www.eecs.havard.edu/mdw/proj/codeblue/ [KAM07] G. Kambourakis, E. Klaoudatou, S. Gritzalis, "Securing Medical Sensor Environments: The Codeblue framework case", ARES 2007 The 2nd International Conference on Availability, Reliability, and Security, pp. 637-643, April 2007, Vienna, Austria. [LIU05] A. Liu and P. Ning, “TinyECC: Elliptic Curve Cryptography for Sensor Networks”, v0.1, http://discovery.csc.ncsu.edu/software/TinyECC/, Sept. 2005 [MAL04] D. J. Malan, M. Welsh, and M. D. Smith, “A Public-Key Infrastructure for TinyOS Based on Elliptic Curve Cryptography”, IEEE Int. Conf. on Sensor and Ad Hoc Communications and Networks, Oct. 2004. [MAL07] Malasri, K. and Wang, L. 2007. Addressing security in medical sensor networks. In Proceedings of the 1st ACM SIGMOBILE international Workshop on Systems and Networking Support For Healthcare and Assisted Living Environments (San Juan, Puerto Rico, June 11 - 11, 2007). HealthNet '07. [MALAN 08] David J. Malan, Matt Welsh, and Micheal D. Smith, “Implementing public-key infrastructure for sensor networks,” ACM Trans. Sen. Netw., 2008 [MIC93] Michèle Basseville and Igor V. Nikiforov, Detection of Abrupt changes – Theory and Application, 1993, Prentice-Hall. [TIN02] TinyOS embedded operating system for sensors network, http://www.tinyos.net [WAT04] R. Watro, D. Kong, S.-F. Cuti, C. Gardiner, C. Lynn, and P. Kruus, “TinyPK: Securing Sensor Networks with Public Key Technology,” ACM SASN, Oct. 2004. [YUA04] Yuan-Hsiang, L., Jan, I.C., et al.: A wireless PDA-based physiological monitoring system for patient transport. IEEE Transactions on Information Technology in Biomedicine 8, 439 (2004)