Le Wireless Sensor Networks e la sicurezza

Tullio Facchinetti
University of Pavia
tullio.facchinetti@unipv.it

15 settembre 2009

Sommario

Il presente documento rappresenta una sintesi di alcuni tra i più significativi contributi alla letteratura scientifica riguardanti le applicazioni delle Wireless Sensor Networks (WSN).

Il documento si concentra esclusivamente sulle applicazioni delle WSN proposte nella letteratura scientifica. Vengono pertanto tralasciati i tantissimi lavori di ricerca dedicati esclusivamente agli aspetti tecnologici delle WSN, ma che non presentano una applicazione pratica. Gli aspetti tecnologici che non vengono presi in considerazione, ma che sono essenziali per la realizzazione di una WSN includono i protocolli di comunicazione, le strategie per il risparmio energetico, la modellizzazione di reti e nodi sensore, le politiche di dislocazione dei nodi, ecc. Tali aspetti sono oggetto di centinaia di pubblicazioni scientifiche, ma non sono direttamente collegati ad applicazioni pratiche delle WSN. Infatti, le soluzioni proposte sono spesso oggetto di verifica sperimentale per mezzo di simulazioni al calcolatore piuttosto che di implementazioni reali.

1 Le Wireless Sensor Networks

Nel campo della ricerca relativa ai sistemi distribuiti, da utilizzarsi sia per applicazioni di sicurezza che per un certo numero di altre applicazioni di monitoraggio, sta prendendo piede negli ultimi anni il tema delle cosiddette Wireless Sensor Networks.

Nella loro concezione “teorica”, una Wireless Sensor Network (WSN), o rete di sensori wireless, consiste di un numero potenzialmente molto elevato di nodi dotati di capacita computazionali, sensoriali e di comunicazione wireless. I nodi vengono posizionati nell’ambiente da monitorare e comunicano tra loro per organizzare al meglio la gestione della rete e dell’applicazione di monitoraggio. Strettamente parlando, una WSN si può occupare del solo monitoraggio, in quanto il singolo nodo dispone di

soli sensori atti a misurare il valore di opportune variabili di interesse (es. temperatura, rumore acustico, accelerazioni, umidità, ecc.), mentre non sono equipaggiati con dispositivi di attuazione. Inoltre, i nodi sono generalmente alimentati a batteria per facilitarne l'installazione, e questo è uno dei fattori che limitano il tempo di vita del singolo sensore e di conseguenza dell'intera rete.

Il fatto di essere composte da un gran numero di sensori economici dovrebbe garantire l'affidabilitá necessaria alle applicazioni anche se alcuni o molti nodi vengono danneggiati oppure smettono di funzionare a causa dell'esaurimento delle batterie. La perdita di nodi è quindi tollerabile sia dal punto di vista economico che da quello della qualità del servizio fornito dalla rete. Questo aspetto è quello che maggiormente differenzia una WSN dai tradizionali sistemi distribuiti, nei quali spesso i singoli nodi sono molto complessi e costosi. Dal momento che si può disporre di meno nodi per ragioni di costo, la perdita di anche un solo nodo può rappresentare un grosso onere economico e può impattare in modo molto negativo sulla qualità del servizio offerto dalla rete.

Gli aspetti chiave di una WSN dal punto di vista della tecnologia realizzativa si possono riassumere nei seguenti punti:

- nodi sensore piccoli e dal costo molto basso (idealmente pochi dollari/euro per nodo)
- capacità computazionale e di memorizzazione molto limitate
- possibilità di comunicare su canale wireless con velocità di comunicazione relativamente limitare (centinaia di Kbit/sec)

Le caratteristiche menzionate sono tutte orientate a permettere la realizzazione di reti composte da molti nodi sensore (fino a decine di migliaia di nodi) con costi ragionevoli.

Nei paragrafi precedenti si sono considerate le caratteristiche teoriche delle WSN. In realtà, allo stato attuale, non è possibile realizzare nodi sensore con i costi necessari per permettere l'implementazione di una WSN avente un numero molto elevato di nodi. Per questo motivo, gli approcci che sono attualmente considerati nello sviluppo della ricerca sulle WSN si basano essenzialmente sulla *simulazione* di reti composte da un gran numero di nodi e sulla sperimentazione pratica con reti composte da un numero molto più basso di nodi, che spesso non superano la decina.

Per gli stessi motivi economici che sono alla base della limitata diffusione di WSN con un gran numero di nodi, in molti lavori di ricerca si parla impropriamente di WSN

anche quando i nodi non sono necessariamente piccoli, economici e con limitate capacità computazionali e di comunicazione. Sono nate delle varianti, per esempio le Industrial Wireless Sensor Networks, che si avvicinano sempre più al più vecchio aspetto delle reti wireless ad-hoc, nelle quali i nodi sono semplicemente nodi intelligenti, con potenza di calcolo e velocità di comunicazione relativamente elevati, connessi tra loro da un canale wireless. Quindi, per lo più, queste ultime tipologie di reti abbracciano le problematiche delle WSN limitatamente alle tematiche della comunicazione wireless e della fault-tolerance.

2 Monitoraggio e sicurezza

2.1 Security

Quando si pensa ad applicazioni orientate alla sicurezza, sia essa sicurezza di impianti, territori, sul lavoro, ecc., si intende generalmente parlare di applicazioni nelle quali la tecnologia in uso viene impiegata per diminuire il grado di pericolosità di una determinata situazione. In questa tipologia di applicazioni, pertanto, sono incluse tutti gli impieghi che vanno dal controllo degli accessi ad un impianto o ad un'area territoriale, al monitoraggio di eventi potenzialmente pericolosi, come incendi, scosse sismiche, ecc.

Nel campo della ricerca sulle WSN il termine italiano "sicurezza" si potrebbe erroneamente tradurre come "security". In realtà, c'è una notevole differenza tra "security" e le applicazioni di sicurezza precedentemente accennate. Con il termine "security" applicato alle WSN, infatti, ci si riferisce a tutti gli aspetti legati alla *sicurezza del funzionamento* di una WSN. In altri termini, si investigano aspetti legati alla compromissione delle funionalità di una WSN. Tale compromissione può essere per esempio ottenuta mediante la violazione dell'integrità della WSN da parte di agenti malevoli che ne prendono il controllo, oppure e all'interferenza nelle normali funzionalità della rete. Per esempio, un attaccante potrebbe disturbare le comunicazioni wireless tra i nodi per impedire che questi si scambino le informazioni necessarie al loro corretto funzionamento.

Sebbene gli aspetti di security siano importanti per la realizzazione di una WSN, essi non rappresentano altro che uno dei fattori di cui tener conto per l'implementazione di WSN in applicazioni critiche, insieme ad altri fattori già citati come il risparmio energetico, la fault-tolerance e l'efficienza nella gestione delle limitate risorse a dispo-

sizione dei singoli nodi. Una estesa trattazione degli aspetti relativi alla sicurezza nelle WSN è disponibile in [12].

2.2 Surveillance

Quando si intende parlare di "applicazioni di sicurezza", il termine corretto da utilizzare nel contesto delle WSN è *surveillance*. Infatti, dal momento che una WSN è composta da nodi equipaggiati unicamente con (opportuni) sensori, il tipico impiego di una WSN è esclusivamente orientato al monitoraggio.

Il monitoraggio, o *surveillance*, è una attività tipicamente associata alle applicazioni di sicurezza: per esempio, la sicurezza di un'area sensibile viene garantita grazie alla sorveglianza del suo perimetro e delle zone più esposte a potenziali violazioni.

3 WSN per applicazioni di sicurezza

3.1 Monitoraggio dell'accesso ad aree riservate

Una delle principali applicazioni di sicurezza è da sempre costituita dal controllo dell'accesso di persone o, ultimante, droni robotici, non autorizzati in aree ad accesso limitato. Questo tipo di applicazione è fondamentale non solo in campo militare, scenario nel quale ha dapprima trovato la principale applicazione, ma anche in ambito industriale e civile. Si pensi, ad esempio, al monitoraggio dell'accesso a cantieri edili, aree espositive, impianti industriali, ecc.

In [2] viene presentata una applicazione di monitoraggio in tempo reale di un'area di circa 5040 metri quadrati. Lo scopo dell'infrastruttura di rilevamento è quello di individuare eventuali accessi non autorizzati e di fornire adeguato supporto alle unità di sicurezza che devono intervenire per prevenire e catturare gli autori dell'accesso non autorizzato.

Una delle caratteristiche di rilievo del lavoro proposto è quello di rappresentare sostanzialmente la sperimentazione su più ampia scala si una WSN. Sono stati infatti utilizzati 144 nodi sensore opportunamente posizionati nell'area di interesse. Inoltre, si è riscontrata l'assoluta necessità di evitare falsi positivi nell'identificazione delle intrusioni, che sono però tipicamente piuttosto frequenti e sono dovute a vari problemi di lettura e filtraggio dei dati letti dai sensori e dell'integrazione delle informazioni raccolte da diversi nodi sensore.

3.2 Monitoraggio delle vibrazioni di edifici

Una delle applicazioni nelle quali le WSN stanno trovando un impiego sempre più ampio sono quelle orientate al monitoraggio delle vibrazioni che interessano un edificio. L'edificio in questione può essere costiuito da

Il rilevamento delle vibrazioni consiste essenzialmente nella rilevazione delle accelerazioni a cui sono sottoposti i nodi sensore installati in modo solidale alla struttura dell'edificio. I sensori tipicamente utilizzati sono accelerometri basati sulla tecnologia MEMS (Micro Electro-Mechanical Systems), cioè circuiti integrati in silicio in grado di misurare delle grandezze fisiche e meccaniche come l'accelerazione. I MEMS hanno il vantaggio di essere compatti, con dimensioni di pochi millimetri quadrati, consumare poco ed essere estremamente economici.

In [13], gli autori presentano Wisden, una WSN ingegnerizzata per il monitoraggio strutturale di edifici, al fine di caratterizzare i materiali e i metodi utilizzati per la costruzione. L'approccio proposto consta di due meccanismi innovativi, relativi ad un livello di trasporto[1] affidabile basato su un recupero ibrido delle informazioni perse sia a livello end-to-end, cioè della comunicazione tra il nodo sorgente e quello destinazione, sia a livello hop-by-hop, cioè a livello della comunicazione tra due nodi adiacenti. Inoltre, viene proposto un meccanismo di timestamping particolarmente efficiente che, tra l'altro, non richiede una sincronizzazione globale dei clock dei singoli nodi. Viene inoltre ipotizzata la possibilità di comprimere il flusso di dati per mezzo di tecniche basate su wavelet, al fine di ridurre la quantità di informazioni che è necessario trasmettere e quindi di ottimizzare l'utilizzo della limitata banda di trasmissione disponibile. Le tecniche presentate sono state valutate sperimentalmente implementandole su nodi sensore Mica-2 [1].

3.3 Monitoraggio del traffico

Il monitoraggio del traffico veicolare costituisce un campo di applicazione naturale per le WSN. Vari tipi di approcci e diverse tecnologie di sensori possono essere impiegate per questo scopo, a seconda delle informazioni che si desidera rilevare circa lo stato del traffico. Le possibilità spaziano dalla semplice rilevazione di veicoli rumorosi, all'individuazione di situazioni di traffico anomale che possono essere indice di incidenti o altri eventi imprevisti, e che possono quindi essere segnalati tempestivamente ad unità di pronto intervento o agli stessi conducenti per smistare il traffico lungo strade me-

[1] Il data transport layer si colloca al livello 4 dello standard ISO/OSI [14], lo stesso dei protocolli TCP e UDP.

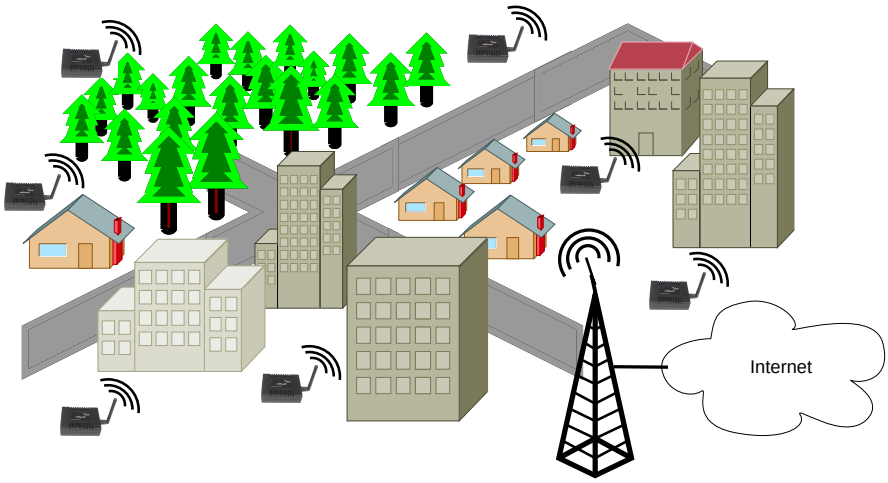

Figura 1: Esempio di WSN dislocata in ambiente urbano; sono visibili i nodi sensore e la stazione base a sua volta collegata alla rete Internet.

no congestionate. In figura 1 è riportato un esempio di WSN per il monitoraggio di un ambiente urbano, nella quale sono facilmente individuabili i nodi sensore collegati via wireless tra loro, oltre ad una stazione base che colleziona i dati generati da tutti i sensori, li memorizza e li elabora opportunamente per renderli disponibili tramite Internet.

In [3] viene presentato il prototipo di Traffic-Dot, un nodo sensore sviluppato per il monitoraggio del traffico veicolare che sfrutta un sensore magnetico per rilevare il passaggio dei veicoli. Il nodo può essere posizionato senza grossi vincoli sulla pavimentazione stradale, in quanto è incapsulato in un contenitore in grado di sopportare il peso di un normale veicolo. Il software di comunicazione è predisposto per limitare al massimo il consumo dell'energia fornita dalle batterie, e permettere un tempo di vita del singolo nodo stimato in diversi anni. Particolare attenzione è posta sia nella gestione del trasduttore, che viene spento dopo ogni campionamento periodico, che sul protocollo di comunicazione (PEDAMACS).

Alcuni aspetti urbanistici di utilizzo delle WSN sono presentati in [9, 8]. In questi articoli gli autori descrivono le problematiche di impiego delle WSN per applicazioni di monitoraggio di ambienti urbani, finalizzato alla pianificazione della gestione del territorio. Sono discussi alcuni possibili approcci alla realizzazione di una WSN, con rifles-

sioni sul design dell'infrastruttura e sul dimensionamento delle sue parti piú rilevanti, quali ad esempio la collocazione dei nodi e la topologia della rete che ne deriva. Viene inoltre presentata l'integrazione di una WSN con programmi GIS (Geographic(al) Information Systems) per la visualizzazione dei dati acquisiti dai nodi sensore.

3.4 Monitoraggio di ambienti ostili

Per monitoraggio di ambienti ostili si intende in modo generico l'utilizzo di WSN i cui nodi devono essere posizionati in ambienti nei quali agenti ostili intendono opporsi all'azione di sorveglianza con tutti i mezzi possibili.

In [5] viene affrontato il problema di mantenere operativa una WSN in ambiente ostile, nel quale un'altra rete di sensori viene posizionata per disturbare il funzionamento della rete di monitoraggio. Vengono considerate varie tipologie di possibili interferenze nel corretto funzionamento della rete. Per esempio, la rete ostile è in grado di captare le trasmissioni della WSN ed eventualmente di trasmettere falsi messaggi per comprometterne il normale funzionamento (tecniche di disinformazione). Inoltre, le comunicazioni della WSN di interesse sono criptate, e l'approccio proposto è studiato per garantire una comunicazione affidabile anche se le chiavi di cifratura vengono temporaneamente compromesse o non sono disponibili. La WSN deve avere un lifetime sufficientemente lungo per garantire il compimento della missione per la quale è stata predisposta. Per questo motivo, deve essere in grado di resistere ad attacchi che mirano a far consumare più energia di quanta è prevista per il suo normale funzionamento. Le tecniche proposte sono pensate per il caso in cui l'attaccante sia costituito a sua volta da una rete di sensori automatizzata per disturbare in ogni modo la WSN di monitoraggio. Nonostante ciò, le metodologie sviluppate si possono applicare anche al caso in cui un attaccante sia stato in grado di modificare un sottoinsieme dei nodi della WSN per fargli compiere le azioni di disturbo illustrate.

3.5 Monitoraggio in ambienti assistenziali

Il monitoraggio di ambienti assistenziali mira a mantenere aggirnate le informazioni riguardanti pazienti di cliniche, ospedali, case di riposo e centri di cura e riabilitazione nei quali i pazienti sono tipicamente liberi di circolare ma dove i pazienti stessi non hanno la piena autonomia. Dal momento che un paziente potrebbe involontariamente smarrirsi o semplicemente tardare all'appuntamento con un medico, è spesso importante monitorarne gli spostamenti, ed eventualmente collezionare informazioni relative al suo stato di salute in ogni istante.

In questo tipo di applicazioni, la flessibilità di posizionamento dei sensori di una WSN, unitamente alle caratteristiche di auto-configurabilità della rete, determinano i principali vantaggi di una WSN rispetto ad altre soluzioni.

In [11] viene proposta l'architettura di un sistema di monitoraggio basato su WSN espressamente sviluppata per il controllo di pazienti la cui salute è sottoposta ad un continuo monitoraggio remoto. Una delle principali caratteristiche di una rete di questo tipo è l'economicità: i costi non devono essere infatti eccessivi per impedirne il reale utilizzo in casi concreti.

3.6 Visual sensor networks

Una tendenza recente nello sviluppo di WSN è quello di dotare i singoli nodi sensore di micro-telecamere, con lo scopo di realizzare una infrastruttura di monitoraggio visuale distribuita molto versatile e efficace. Questa possibilità è garantita dagli ultimi sviluppi nella realizzazione di telecamere miniaturizzate dall'ingombro e dai consumi estremamente ridotti. Vista la miniaturizzazione del sensore visuale, è spesso impossibile arrivare a risoluzioni molto spinte dell'immagine. In genere ci si accontenta di una qualità relativamente bassa delle singole immagini, ma il fatto di avere molti nodi sensore permette di ricostruire uno scenario dinamico a partire dalla fusione dei contributi di molti nodi sensore.

In [7] viene descritto SensEye, una infrastruttura per la video-sorvelianza mediante una WSN i cui nodi sensore sono dotati di micro-camera. La caratteristica principale dell'approccio proposto è quello di essere multi-modale e multi-livello. La rete è infatti organizzata gerarchicamente, e ad ogni livello corrisponde un determinato servizio a cui sono associati nodi sensore opportunamente equipaggiati. Questa caratteristica, secondo gli autori, permette una maggiore scalabilità, una migliore affidabilità della rete e, allo stesso tempo, costi minori e una migliore capacità di coprire l'area oggetto del monitoraggio.

Un altro esempio di applicazione di video-sorveglianza basata su WSN è riportata in [4]. Anche in questo caso si mettono in risalto le caratteristiche multi-modali dell'infrastruttura, ovvero l'intergrazione di vari tipi di sensori che completano le informazioni fornite dalle telecamere. In questo caso specifico, una rete di normali telecamere è integrata da una WSN dotata di micro-camere all'infrarosso. Le informazioni ottenute da queste ultime servono per rendere non ambigua l'informazion prodotta dalle telecamere. Per esempio, è possibile distinguere facilmente tra una porta che si apre ed un essere umano che si sposta: in entrambi i casi la rete di telecamere riporta delle

variazioni nella scena ripresa, e grazie alla presenza o meno di segnale nell'intervallo dell'infrarosso, che è rilevata solo nel caso di presenza di una persona, è possibile capire immediatamente di quale tra i due eventi si tratta.

3.7 Monitoraggio di condutture

Una interessante applicazione delle WSN è quella del monitoraggio di condutture e tubazioni dell'acqua presentata in [10]. Il problema è quello di rilevare eventuali perdite dovute all'invecchiamento delle condutture, nonchè di controllare eventuali bloccaggi nel flusso dell'acqua e allagamenti nei collettori delle acque. L'articolo descrive PipeNet, un sistema per la sorveglianza in tempo reale di condutture d'acqua di grandi dimensioni, in grado di acquisire informazioni su parametri idraulici e acustico/vibrazionali con una elevata frequenza di campionamento. I maggiori problemi affrontati nella ricerca includono l'elevata frequenza di acquisizione, il mantenimento di un sufficiente duty-cycle di rilevamento e la precisa sincronizzazione tra l'acquisizione distribuita dai vari nodi sensore. Tutte le funzionalità devono essere garantite sotto un vincolo di risparmio energetico molto stringente per ottenere un lifetime elevato dell'infrastruttura di sorveglianza. Uno degli aspetti maggiormente interessanti del lavoro proposto consiste nella sperimentazione pratica in un caso di studio reale, oltre che un'estesa elaborazione statistica dei dati acquisiti che ha permesso un'accurata valutazione della soluzione proposta.

3.8 Miscellanea

In [6] vengono presentati due esempi di implementazione di una WSN per la sorveglianza all'interno di un complesso industriale e per la sorveglianza combinata tra ambiente indoor e outdoor. Le esperienze di implementazione delle WSN hanno permesso agli autori di dedurre che una efficace realizzazione di una WSN non può essere soltanto basata sulla adattività dei protocolli di comunicazione, ovvero della scelta tra le politiche di scambio dei messaggi più adatta a seconda della situazione. Gli autori argomentano la necessità di implementare dei protocolli in grado di monitorare la WSN durante l'installazione e il funzionamento. Questa funzionalità permette di eliminare molti falsi allarmi dovuti ad erronee segnalazioni da parte di nodi difettosi o comunque affetti da problemi hardware/software. Un esempio in particolare è costituito dalla possibilià di individuare consumi eccessivi di energia dovuti a dei bug che determinano l'accensione del modulo radio per un tempo maggiore di quanto strettamente necessario.

Riferimenti bibliografici

[1] The CrossBow MICA2 mote. `http://www.xbow.com/Products/productdetails.aspx?sid=174`.

[2] P. Chen, S. Oh, M. Manzo, B. Sinopoli, C. Sharp, K. Whitehouse, G. Tolle, J. Jeong, P. Dutta, J. Hui, S. Shaffert, S. Kim, J. Taneja, B. Zhu, T. Roosta, M. Howard, D. Culler, and S. Sastry. Experiments in instrumenting wireless sensor networks for real-time surveillance. 2006.

[3] S. Coleri, S. Y. Cheung, and P. Varaiya. Sensor networks for monitoring traffic, August 2004.

[4] R. Cucchiara, A. Prati, R. Vezzani, L. Benini, E. Farella, and P. Zappi. Using a wireless sensor network to enhance video surveillance. *Journal of Ubiquitous Computing and Intelligence*, 2005.

[5] A. Czarlinska, W. Luh, and D. Kundur. G-E-M sensor networks for mission critical surveillance in hostile environments.

[6] N. Finne, J. Eriksson, A. Dunkels, and T. Voigt. Experiences from two sensor network deployments – self-monitoring and self-configuration keys to success.

[7] P. Kulkarni, D. Ganesan, and P. Shenoy. The case for multitier camera sensor networks. In *(NOSSDAV)*, Stevenson, Washington, USA, June 2005.

[8] R. D. Lotto, T. Facchinetti, P. Gamba, and E. Goldoni. Wireless sensor networks for monitoring urban environments: evaluation and practical considerations. 2009. book chapter, to appear.

[9] R. D. Lotto, T. Facchinetti, P. Gamba, and E. Goldoni. Wireless sensor networks for planning processes: applications and case study. 2009. book chapter, to appear.

[10] I. Stoianov, L. Nachman, S. Madden, and T. Tokmouline. PIPENET: A wireless sensor network for pipeline monitoring. In *(IPSN)*, Cambridge, Massachusetts, U.S.A., April 2007.

[11] G. Virone, A. Wood, L. Selavo, Q. Cao, L. Fang, T. Doan, Z. He, R. Stoleru, S. Lin, and J. Stankovic. An advanced wireless sensor network for health monitoring.

[12] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary. *Wireless Sensor Network Security: A Survey*, chapter 17. Security in Distributed, Grid, and Pervasive Computing. Auerbach Publications, CRC Press, Yang Xiao edition, 2006.

[13] N. Xu, S. Rangwala, K. K. Chintalapudi, D. Ganesan, A. Broad, R. Govindan, and D. Estrin. A wireless sensor network for structural monitoring. In *(SenSys)*, Baltimore, Maryland, USA, November 2004.

[14] H. Zimmermann. OSI reference model – the ISO model of architecture for open systems. *IEEE Transactions on Communications*, 28(4):425–432, April 1980.