di **Alessandra Flammini**

Fonte: www.teexblog.blogspot.com

Questione di cyber-security

A fronte dei vantaggi che offrono, le reti wireless industriali, note come WSN-Wireless Sensor Network, possono essere soggette ad attacchi come accade nel mondo ICT. Ecco come difendersi

I recenti sviluppi nella realizzazione di dispositivi elettronici, in particolare di quelli destinati ai sistemi di comunicazione wireless, hanno permesso lo sviluppo di nodi sensori multifunzionali a basso costo e basso consumo, quindi in grado di essere utilizzati per l'implementazione di reti di sensori wireless, spesso identificate con l'acronimo WSN-Wireless Sensor Network, che rappresentano un significativo passo avanti rispetto alle tradizionali reti di sensori cablate.

Reti wireless per l'automazione e cyber-security

Una WSN può semplificare notevolmente tanto la fase di commissioning quanto la manutenzione d'impianto, grazie alle enormi scalabilità e flessibilità offerte, essenzialmente dettate dalla potenziale assenza 'fisica' non solo dell'infrastruttura di comunicazione, ma anche di quella di alimentazione. Per tutti questi motivi, le WSN sono subito state accolte con entusiasmo nell'ambito dell'automazione industriale, dove si propongono come sostituti, laddove possibile, dei fieldbus cablati tradizionali. Ovviamente, l'impiego in compiti mission-critical richiede un'attenta valutazione delle problematiche di sicurezza: è evidente che l'uso improprio dei dati trasmessi e/o la loro manipolazione intenzionale può causare perdite indesiderate di informazioni e, in ultima analisi, effetti anche disastrosi.

Tornando indietro a un passato recente possiamo ricordare gli effetti dell'emergenza 'Stuxnet', il malware per i PLC che ha trovato completamente impreparato il mondo dell'automazione industriale. Va anche sottolineato che, mentre alcune caratteristiche della WSN sono comparabili a quelle di una tradizionale rete wireless, per esempio basata su Wlan, altre peculiarità introducono differenze notevoli, che possono influire significativamente sugli aspetti inerenti la sicurezza. Le principali differenze sono: il fatto che il numero dei nodi presenti in una rete e/o la loro densità può essere molto elevata; che i nodi possono essere soggetti

a guasti/interruzioni di servizio dovuti all'impiego in ambienti gravosi e a vincoli energetici stringenti; che la topologia della rete può cambiare nel tempo a causa di guasti o di mobilità dei nodi; che i nodi sono limitati nelle risorse di calcolo e di memoria. I vincoli dimensionali, la necessità di avere bassi costi e di una fonte di alimentazione autonoma, quindi necessariamente limitata, per esempio, rendono le WSN più suscettibili agli attacchi di tipo denial-of-service. Gli stessi requisiti citati prima rendono le tecniche avanzate per l'anti-jamming e l'uso della crittografia a chiave pubblica, diffusa nel mondo ITC, generalmente impossibili da applicare. Va inoltre ricordato che i vincoli sui consumi si traducono generalmente in un'organizzazione gerarchica dei dati trasmessi e in una loro progressiva aggregazione, che deve ovviamente essere sicura per garantire l'integrità e la riservatezza delle informazioni trasportate.

L'ovvia soluzione, che prevede comunque il ricorso alla crittografia, anche se nella variante a chiave simmetrica, deve tenere in conto le caratteristiche dei protocolli di routing e deve essere sufficientemente flessibile da permettere un grado più basso di sicurezza per i dati meno importanti, risparmiando in questo modo la fonte energetica, e consentire livelli di sicurezza più elevati per i dati sensibili, ammettendo ovviamente un consumo di energia più elevato. È inoltre di grande importanza la capacità di identificare gli attacchi, distinguendoli dalle situazioni in cui l'integrità dei dati è garantita, così come è necessario saper identificare i nodi compromessi. Altrettanto importanti sono la gestione e la distribuzione delle chiavi di cifratura, che incidono pesantemente anche sulla capacità di memoria che i nodi devono possedere. I meccanismi di sicurezza in una WSN devono consentire un'efficiente distribuzione delle chiavi, pur mantenendo affidabile e deterministica la capacità di comunicazione tra i nodi.

I servizi di sicurezza

Entrando più nel dettaglio, ricordiamo che l'obiettivo di un servizio di sicurezza all'interno di una WSN è proteggere le informazioni da manomissione/distruzione, che si traduce nel garantire: 'availability', che assicura che i servizi di rete siano disponibili anche in presenza di attacchi di tipo denial-of-service; 'authorization', che garantisce che solo gli utenti autorizzati possano accedere alla rete; 'authentication', che assicura la veridicità della comunicazione da un nodo all'altro, evitando che un nodo 'maligno' si mascheri come uno autorizzato; 'confidentiality', che assicura che un dato messaggio possa essere compreso solamente dai destinatari; 'integrity', che assicura che un messaggio non venga modificato durante l'instradamento verso la destinazione; 'non-repudiation', ovvero l'impossibilità per un nodo di ritrasmettere un messaggio che è stato precedentemente inviato; 'freshness', che implica l'impossibilità di riprodurre messaggi antecedenti a un certo riferimento temporale. Inoltre, poiché in una rete WSN i dispositivi possono scomparire e riapparire dinamicamente nella rete a causa di guasti e/o malfunzionamenti, è bene che un nodo non sia in grado di leggere messaggi posteriori al suo abbandono della rete e, similmente, messaggi antecedenti al suo ingresso.


Fonte: www.prisonplanet.com

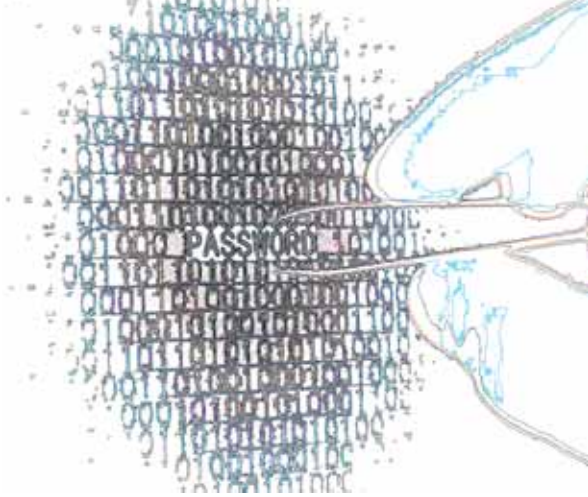
Le tipologie di attacco

Per quanto riguarda le tipologie di attacco, queste sono convenzionalmente classificate nelle due categorie: 'Attacchi Interni' piuttosto che 'Esterni', ovvero attacchi originati da nodi che non appartengono alla WSN oppure attacchi tali per cui i nodi di una stessa WSN si comportano in modo non 'autorizzato'; 'Attacchi Passivi' piuttosto che 'Attivi', i primi basati sull'intercettazione o il monitoraggio del normale traffico; i secondi che prevedono invece un'alterazione del flusso dei dati scambiati.

Volendo invece classificare le tipologie di attacco in base al livello dello stack protocollare nel quale agiscono e partendo dal livello fisico, ovvero dallo strato incaricato di selezionare la frequenza operativa e la modulazione adottata, si suole parlare di 'tampering' e 'jamming'. Con quest'ultimo si indica l'impiego di una fonte di disturbo abbastanza potente da rendere impossibile il funzionamento dell'intera rete, o quantomeno di una sua sottosezione. Le strategie di difesa normalmente adottate si basano su tecniche di modulazione a spettro espanso. Tra queste il frequency hopping è caratterizzato da una rapida commutazione del canale utilizzato all'interno della trasmissione di uno stesso messaggio, o per messaggi consecutivi, affidandosi a una sequenza pseudo-casuale nota sia al trasmettitore, sia al ricevitore. Tuttavia, essendo il numero di canali disponibili generalmente limitato, un malintenzionato può generalmente essere in grado di sopprimerli tutti contemporaneamente. Una possibile alternativa è ricorrere all'uso di tecniche a divisione di codice, diffuse nelle reti mobili, che consentono di recuperare il messaggio anche in presenza di una forte interferenza; tali tecniche richiedono comunque una maggiore complessità di progettazione e un consumo energetico superiore. Nel caso del 'tampering' è il nodo a essere soggetto a possibili manomissioni. Avendo per esempio accesso fisico a un nodo, è possibile estrarre da esso informazioni sensibili, come le chiavi di crittografia; inoltre, il nodo può essere modificato o sostituito.

Passando al livello del collegamento dati, responsabile dell'accesso al mezzo e dell'inoltro di un messaggio tra nodi 'contigui', gli attacchi di solito si basano su 'collisions', 'exhaustion' e 'unfairness'. Con collisions si intende la deliberata introduzione in rete di traffico allo scopo di distruggere i messaggi, a causa della loro sovrapposizione temporale. L'effetto è 'costoso' in termini di efficienza della rete, a causa del meccanismo di back-off esponenziale presente in molti protocolli di accesso al mezzo. Una possibile difesa è l'uso di codici correttori, che consentono di recuperare l'informazione di un messaggio parzialmente corrotto. La exhaustion utilizza le ripetute collisioni con lo scopo di esaurire le risorse di rete o energetiche. La continua ritrasmissione dei messaggi corrotti, per esempio, può facilmente causare un prematuro esaurimento della banda e delle batterie. Opportune scelte protocollari, che pongono un limite al massimo numero di riprove ammesso, possono limitare gli effetti potenzialmente dannosi. Infine, l'ultima possibilità di attacco, definita unfairness,

Fonte: www.texblog.blogspot.com



prevede la capacità di un nodo 'malintenzionato' di accaparrarsi risorse al fine di causare un comportamento non deterministico degli altri nodi. L'utilizzo di time slot di breve durata attenua l'impatto di tali attacchi, poiché riduce il tempo che il nodo malintenzionato ha a disposizione per acquisire il canale di comunicazione. Gli attacchi a livello rete normalmente si basano sulla contraffazione, alterazione o replica delle informazioni di routing, allo scopo di interrompere il traffico. I potenziali effetti possono essere ridotti o eliminati ricorrendo a opportune tecniche di autenticazione. Motivi di efficienza energetica spingono poi gli algoritmi di routing a selezionare i percorsi basati su tratte brevi, che possono essere implementate a bassa potenza. Un nodo malintenzionato può utilizzare una potenza di trasmissione particolarmente elevata (anche fuori dalle specifiche) per falsare il 'costo' della tratta e attrarre su di sé la maggior parte dei percorsi all'interno della rete. Va comunque sottolineato che una trasmissione a bassa potenza è vantaggiosa, proprio in virtù dell'area ridotta coperta, che ne rende difficile l'intercettazione. Infine, un nodo malintenzionato può deliberatamente trasmettere messaggi di conferma ACK alterati, per esempio al fine di far credere attivo un nodo non più presente in rete.

Un ulteriore livello a volte presente nei wireless fieldbus è denominato 'di trasporto' e garantisce l'esistenza di una connessione end-to-end stabile e affidabile. Le tipologie di attacco perpetuate a questo livello sono denominate rispettivamente 'flooding' e 'desynchronization'. Nel caso del flooding, un nodo malintenzionato può ripetutamente fare nuove richieste di connessione, così da esaurire le risorse del nodo sotto attacco con la conseguenza di non essere più in grado di soddisfare le richieste dei nodi legittimi. Una possibile contromisura si basa sull'uso dello stesso approccio seguito dall'attaccante: si richiede per ogni tentativo di connessione un 'esercizio' computazionale, così da rendere impossibile un numero elevato di richieste da parte di un singolo nodo. In molte applicazioni, infatti, il sovraccarico generato in questo modo è trascurabile se comparato all'effetto dell'attacco. Con il termine desincronizzazione invece ci si riferisce, in realtà, alla distruzione di una connessione esistente. La finalità dell'utente malintenzionato è esaurire le risorse del nodo ricevente sommergendolo di messaggi corrotti che lo obbligano a un numero elevato di ritrasmissioni. In questo caso, la contromisura più efficace prevede il ricorso a una procedura di autenticazione dei messaggi. Una soluzione molto diffusa prevede l'aggiunta di un campo MIC-Message Integrity Code, che permette al destinatario di verificare se il messaggio appena ricevuto sia stato alterato. È inoltre possibile includere/basare il MIC su informazioni tempo-varianti, quali time stamp o numeri di sequenza, che ne accrescono l'efficacia. Nell'ambito dell'automazione industriale, dove la ridondanza è spesso richiesta, un'ulteriore possibile forma di attacco è nota come 'Sybil', nella quale un nodo presenta più identità alla rete; in una logica di ridondanza due su tre, per esempio, un nodo compromesso può fingere di essere due dei tre nodi interessati e ingannare gli algoritmi di ridondanza.

La cifratura

Alla base di ogni sevizio di sicurezza in una rete WSN risiede ovviamente la cifratura dei messaggi scambiati, il che rende di vitale importanza la selezione del metodo crittografico più appropriato. In particolare, a causa delle scarse risorse disponibili, i metodi crittografici utilizzati devono essere valutati in base alle dimensioni del codice richiesto per implementarli, alla memoria richiesta, al tempo di elaborazione e, non ultimo, al consumo energetico. Normalmente nelle applicazioni industriali si ricorre a meccanismi di cifratura simmetrici, nei quali la stessa chiave, che quindi non viene distinta in pubblica e privata, come nel caso dei più complessi algoritmi utilizzati in genere nel mondo ICT, viene utilizzata sia per la cifratura, sia per il processo opposto. Nello specifico, grazie all'enorme diffusione dello standard Ieee 802.15.4 nelle soluzioni destinate all'automazione industriale, inclusi i ben noti WirelessHart e ISA100.11a, il meccanismo di cifratura più diffuso risulta essere AES nella sua variante con chiave a 128 bit. Generalmente, si prevede l'utilizzo di un parametro 'nonce' (termine derivato dalla contrazione di 'number used once', ovvero un parametro numerico che viene utilizzato una sola volta), derivato dal sincronismo temporale che i wireless fieldbus impongono ai nodi. In WirelessHart, per esempio, tale parametro è ricavato dall'indice del time slot corrente, mentre in ISA100 è derivato dall'ora conforme alla notazione TAI (Atomic International Time). Questo accorgimento permette, come già detto, di evitare che un semplice reinoltro del traffico catturato possa essere accettato da un nodo. Inoltre, la maggior parte dei dispositivi radio compatibili con tale standard fornisce un accele-

ratore hardware per la computazione di tale algoritmo (AES128), sgravando quindi il processore e riducendo in maniera notevole i consumi e i tempi di elaborazione.
Di vitale importanza è dunque il meccanismo di gestione delle 'chiavi', al plurale perché potenzialmente ogni transazione sorgente-destinazione, o perlomeno ogni sessione di comunicazione, potrebbe averne una diversa. Normalmente il nodo viene preconfigurato in fase d'installazione con una chiave la cui validità è limitata alla sola fase di affiliazione e che per questo è detta anche 'chiave di join'. La procedura di affiliazione è probabilmente la più critica dal punto di vista della sicurezza, motivo per cui in ISA100, per esempio, è prevista la possibilità che questa avvenga ricorrendo a meccanismi di cifratura asimmetrici. In WirelessHart invece è esplicitamente richiesto che la chiave di join sia configurata tramite connessione cablata. Lo scambio delle chiavi successive è invece effettuato 'over the air', ma con messaggi già comunque cifrati.
Pensando alla fisionomia di un impianto produttivo, che è comunque piuttosto rigida se paragonata alle applicazioni ICT, lo schema di distribuzione delle chiavi è solitamente centralizzato, ovvero esiste un'unica entità, spesso il security manager, che controlla la generazione, rigenerazione e distribuzione delle chiavi. Generalmente, eccezion fatta per la già citata join key, che sovente è unica per tutta la rete, le chiavi di sessione vengono cambiate automaticamente in maniera periodica, garantendo che sia insufficiente il semplice ascolto del traffico su un intervallo sufficientemente lungo per una loro scoperta.

Tirando le fila

Le reti di tipo WSN già oggi disponibili sono una soluzione promettente per molte delle applicazioni che non possono essere soddisfatte ricorrendo alle tradizionali soluzioni cablate. La necessità di garantire la continuità della trasmissione e, soprattutto, la robustezza contro eventuali attacchi esterni rendono particolarmente importante la problematica della cyber-security. Le soluzioni normalmente adottate nel mondo ICT non sono utilizzabili, a causa delle notevoli restrizioni a cui i nodi di una WSN sono soggetti.
Comunque, l'uso della cifratura a chiave simmetrica e un frequente cambio delle chiavi rendono inutile il solo ascolto del traffico in aria per la manomissione dei messaggi. Inoltre, i meccanismi di autenticazione rendono identificabili (quindi neutralizzabili) gli attacchi in corso.
In ultima analisi, si può affermare che il grado di sicurezza di una WSN sia equivalente a quella di una tradizionale rete cablata. Molti aspetti restano però soddisfatti solo parzialmente, per esempio le problematiche inerenti la mobilità dei nodi, oggi solo parzialmente considerata nei wireless fieldbus, e la trasmissione di flussi di dati continui, come quelli generati da una telecamera, rispetto ai più semplici dati di campo 'discreti', come valori di temperatura, flusso, pressione ecc.

Fonti: Wang Yong, G. Attebury, B. Ramamurthy, "A survey of security issues in wireless sensor networks", Communications Surveys & Tutorials, Ieee, vol.8, n.2, pp.2-23, Second Quarter 2006 - doi: 10.1109/COMST.2006.315852