Problemy bezpieczeństwa w bezprzewodowych sieciach sensorowych

Tadeusz Goszczyński
Przemysłowy Instytut Automatyki i Pomiarów PIAP

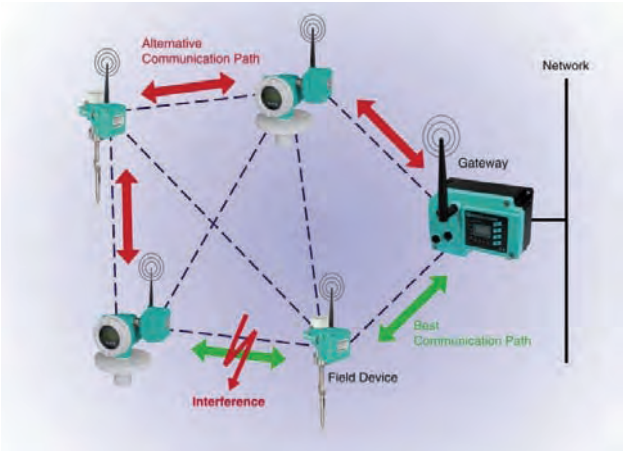
Streszczenie: Bezprzewodowe sieci sensorowe, ze względu na rozmieszczenie ich elementów w terenie, są narażone na szereg zagrożeń. Zagrożenia te mogą wynikać ze świadomych akcji ludzi starających się ją nielegalnie wykorzystać lub unieszkodliwić takich, jak ataki terrorystyczne, podsłuchiwanie transmisji, czy podszywanie się pod użytkownika. Mogą one jednak być rezultatem zakłóceń środowiskowych, takich jak silny sygnał radiowy lub pożar. Sieci sensorowe w większości zastosowań mają ograniczone zasoby energii i możliwości obliczeniowe węzłów w porównaniu z kablowymi sieciami informatycznymi. Tym ambitniejsze staje się zadanie zapewnienia im bezpiecznej pracy, w taki sposób, by nawet przy problemach ze środowiskiem lub podczas wrogich ataków ze strony ludzi mogły spełniać swoją zasadniczą funkcję zbierania danych z czujników i przesyłaniu tych danych użytkownikowi zgodnie z jego potrzebami. Ze względu na rosnące zapotrzebowanie na sieci sensorowe w różnych dziedzinach działań człowieka, powstaje w ostatnich latach wiele prac naukowych dotyczących systemów zapewniających ich bezpieczną pracę. Niniejsza publikacja ma na celu przybliżenie czytelnikom, a szczególnie projektantom systemów wykorzystujących sieci sensorowe, efektów tych prac oraz usystematyzowanie problemów w tej dziedzinie.

Słowa kluczowe: bezprzewodowe sieci sensorowe, sieci mobilne, wykrywanie ataków, bezpieczeństwo

W pracy przedstawiono podstawowe cechy najczęściej spotykanych ataków oraz techniki stosowane w sieciach sensorowych dla uzyskania bezpieczeństwa protokołu komunikacji, zabezpieczenia stacji bazowych przed identyfikacją i atakiem. Całkowita anonimowość jest niemożliwa, ale opisano sposoby uzyskania kompromisu między anonimowością a potrzebami systemu monitorowania. Opisano techniki wykrywania intruzów w sieci i udaremniania ataku złośliwym węzłom, które zdobyły już jeden lub kilka kluczy kryptograficznych zaatakowanej sieci, oraz techniki bezpiecznego grupowania danych. Następnie przedstawiono sposoby obrony przed fizycznymi atakami, techniki wykrywania ataków i na zakończenie perspektywy w tej dziedzinie.

Stosowanie bezprzewodowych sieci sensorowych wymaga poważnego zaangażowania w zapewnienie bezpieczeństwa ich pracy. Sieci bezprzewodowe narażone są szczególnie na szereg zagrożeń, jak np. ataki terrorystyczne, podsłuchiwanie transmisji lub podszywanie się pod użytkownika. Ataki destabilizujące pracę sieci są, niestety, dosyć łatwe do wykonania. Wygenerowanie silnego sygnału elektromagnetycznego w pobliżu sieci może skutecznie zablokować transmisję, natomiast po zdobyciu danych autoryzujących użytkownika można podszyć się pod niego, aby fałszować zbierane dane lub wykonywać kolejne ataki na sieć. W celu odparcia takich ataków opracowywane są nowe techniki i systemy. Nie są to jednak jeszcze w pełni zadowalające rozwiązania, gdyż mogą zostać złamane w czasie dłuższej pracy sieci.

Przy projektowaniu i wdrażaniu sieci należy wykonać ocenę ryzyka. Analiza zagrożeń powinna wskazać środki konieczne do zabezpieczenia systemu. Podstawowym wymaganiem jest zapewnienie łączności między wszystkimi węzłami sieci. Pierwsze sprawdzenia powinny być przeprowadzone na etapie projektowania instalacji. Po wykonaniu instalacji należy stworzyć mapę zasięgu sieci oraz poziomu sygnałów w poszczególnych miejscach instalacji w terenie. Kolejne testy muszą być wykonywane w określonych odstępach czasu, gdyż na wyniki mogą wpływać pojawiające się w terenie nowe źródła zakłóceń elektromagnetycznych. Aby uniknąć skutków zakłóceń, czasem może być konieczna zmiana kanału transmisji. Okresowo przeprowadzana ocena dostępności węzłów pozwala na utrzymanie niezawodnego działania sieci bezprzewodowej. W tym celu administrator sieci musi mieć dostęp z jednej ze stacji do systemu konfiguracji sieci i możliwość aktualizacji oprogramowania firmowego. Nie może to jednak narażać instalacji na niebezpieczeństwo. W wypadku awarii punktu dostępowego, sąsiednie punkty muszą przejąć jego zadania (rys. 1). Aby punkty dostępowe nie zakłócały się wzajemnie, muszą mieć możliwość automatycznego wyboru kanału transmisyjnego. Należy także zapewnić alternatywne drogi komunikacji. Bezpieczeństwo sieci musi być koniecznie wbudowane w system już na etapie projektowania. Systemy sieciowe, które w trakcie pracy były uzupełniane o funkcje bezpieczeństwa, okazały się w wielu przypadkach zawodne.



Rys. 1. Przykładowy schemat sieci firmy Pepperl+Fuchs GmbH
Fig. 1. Example of network proposed by Pepperl+Fuchs GmbH

1. Rodzaje ataków na sieć

Zagłuszanie silnym sygnałem radiowym. Taki atak na szczęście może zostać łatwo wykryty, gdy węzły nie mogą się porozumiewać. Jako obrona zalecana jest komunikacja w rozproszonym paśmie, co jednak zwiększa koszty, pobór mocy i złożoność projektu. Dla różnych typów zagłuszania skuteczne są różne strategie. Jeżeli zagłuszanie jest stałe, wtedy węzły mogą zastosować mniejszą częstość wysyłania przesyłek i próbować przetrzymać przeciwnika stosując oszczędzanie energii. Dla zagłuszania przerywanego skuteczne mogą być: stosowanie priorytetów dla ważnych wiadomości, współpraca węzłów w gromadzeniu i forwardowaniu ważnych wiadomości lub nawet zawiadomienie stacji bazowej. Gdy zagłuszanie zostanie zlokalizowane, wtedy węzły otaczające dotknięty nim region mogą współpracować przy zapewnieniu komunikacji, omijając ten region. Zagłuszanie można też zwalczać przez stosowanie redundancji ścieżek i kilku różnych technologii przesyłania (optyczna lub w podczerwieni) lub nadawanie na różnych częstotliwościach.
Ataki na warstwę połączeń mogą dążyć do przełamania stosowanego protokołu dostępu do medium. Spowodowanie kolizji w zaledwie kilku bitach transmisji może być bardzo skutecznym sposobem zakłócenia całego pakietu transmisji przy małej energii zużywanej przez napastnika. Skutki takich ataków można próbować naprawiać przez zastosowanie specjalnych funkcji korygujących błędy. Obecnie takie funkcje są jednak bardziej skuteczne przeciw przypadkowym błędom niż przeciw błędom złośliwym, a ponadto wymagają dodatkowego przetwarzania danych i generowania dodatkowych przesyłek.

Atak typu Sybil polega na tym, że przeciwnik w jednym podstawionym węźle umieszcza wiele identyfikatorów ID i w ten sposób dezorganizuje rutowanie przesyłek w sieci, przepuszczając przez ten węzeł wiele ścieżek transmisji, a w przypadku głosowania w sieci dając wiele głosów.

Atak typu dziura (*sinkhole*). Aktywny atak sinkhole ma na celu zwabienie przesyłanych wiadomości do węzła napastnika. Napastnik najpierw przejmuje jakiś węzeł w sieci i wysyła żądanie podania drogi do stacji bazowej *Request Route* nie badając, czy ścieżka dostępu już istnieje. Następnie jest wysyłana przesyłka *Route Reply*, w której zawarte są dane o maksymalnej liczbie sekwencji oraz minimalnej liczbie przeskoków. Sąsiadujące węzły wysyłają wtedy posiadane dane do tego węzła (lub przesyłają żądanie dalej), a w odpowiedzi otrzymują od przejętego węzła dane z poleceniem wprowadzenia do swoich tablic rutowania przejętego węzła jako najlepszej ścieżki do stacji bazowej. Takie postępowanie tworzy czarną dziurę i zamyka tę przestrzeń sieci. Bierny atak sinkhole jest podobny do aktywnego. Jedynie zamiast nadawania żądania *Request Route*, przejęty węzeł atakuje odpowiadając na prawdziwe żądanie *Request Route* od dowolnego węzła w sieci przesyłką *Route Reply*. Jeżeli węzły w tym obszarze nie mają żadnego nowego pomiaru, by nadać przesyłkę w tym czasie, to przejęty węzeł nie otrzyma żadnego żądania *Request Route*. Jest go więc trudniej wykryć, bo częstotliwość ataków jest przypadkowa.

Atak przez analizę ruchu w sieci polega na analizowaniu przez napastnika kierunku ruchu przesyłek w celu odnalezienia stacji bazowej, aby zaatakować ją bezpośrednio.

Atak przez kopiowanie. Węzeł napastnika kopiuje identyfikację autentycznego węzła sieci, aby być traktowanym przez sieć tak jak on i móc wykonać właściwy atak.

Przejęcie węzła to atak, w którym napastnik zmienia kod programu w pamięci atakowanego węzła. Polecany sposób ochrony węzłów przed fizycznym przejęciem to ukrycie lub zamaskowanie węzłów. Nie zawsze jednak jest to możliwe. Zaleca się wtedy, by węzły reagowały na atak usuwaniem systemu kodowania i pamięci programu. Zapewnia to odporność na takie ataki, lecz powoduje wzrost kosztów węzłów sieci. Skuteczny jest również system, w którym zarządzający siecią, po potwierdzeniu swojej autentyczności, może usunąć kryptograficzne klucze i informacje o sensorze, co do którego zachodzi podejrzenie, że został przejęty przez atakującego.

2. Techniki stosowane do zapewnienia bezpieczeństwa transmisji

Tradycyjne protokoły sieciowe nie zapewniają bezpieczeństwa sieciom sensorowym, dlatego konieczne jest stosowanie specjalnych technik.

2.1. Ataki w warstwie rutingu

W [1] autorzy analizują różnego typu ataki na różne protokoły rutingu. Między innymi biorą pod uwagę fałszowanie, zmienianie lub powtarzanie informacji rutingowych, wybiórczy forwarding, ataki typu dziura, ataki typu Sybil, zalew przesyłek „*hallo*" i podrabianie potwierdzeń odbioru. Przedstawiają oni także modele zagrożeń i analizę bezpieczeństwa oraz rozważania dotyczące przeciwdziałania, a także projektowania bezpiecznych protokołów rutingu dla sieci sensorowych. Natomiast w [2, 3] autorzy proponują ciekawe podejście do zagadnienia bezpieczeństwa polegające na stworzeniu protokołu, który będzie działać prawidłowo tolerując ataki na sieć przez zastosowanie redundancji ścieżek transmisji. Wykorzystują oni między innymi mechanizm komunikacji kodowanej, w którym tylko stacje bazowe mogą rozsyłać informacje. Węzły sieci sensorowej mogą mieć wspólny klucz szyfrowy tylko ze stacją bazową i tylko ona może wykonywać obliczenia związane z tworzeniem tablic rutingu. W [4] autorzy przedstawiają rozważania nad strategią rutingu wielościeżkowego, w których wyróżniają dwa rodzaje ataków: próba izolacji stacji bazowej i próba jej lokalizacji. Przeciwko atakom izolacyjnym zaproponowali oni strategię wielościeżkowego rutingu, a przeciwko atakom lokalizacyjnym strategie klastrowe: kodowanie i rozkodowywanie przy każdej przesyłce oraz kontrolę częstotliwości wysyłania nowych przesyłek. Technika [2] ma na celu złagodzenie skutków ataku wykonanego przez intruza, ale także przypadkowego działania przez uszkodzony lub w wyniku zakłócenia źle działający węzeł sieci. Zaleca się wielokrotne przesyłanie tych samych wiadomości wykorzystując stosowaną w sieci redundancję. Wiadomość jest wysyłana równocześnie wzdłuż kilku odmiennych ścieżek z nadzieją na to, że co najmniej jedną z nich dotrze do celu. Aby odróżnić, które wiadomości docierające do celu są autentyczne, należy zastosować identyfikację potwierdzającą integralność wiadomości. Jest to wykonywane w trzech fazach. W pierwszej fazie stacja bazowa nadaje wiadomość

typu żądanie do każdego sąsiada, która jest następnie przesyłana w całej sieci. W drugiej fazie stacja bazowa zbiera lokalnie informacje o zdolności połączeniowej od każdego węzła. W końcowej fazie stacja bazowa wyznacza tablice rutingu dla każdego węzła. Tablice te zawierają informacje o redundancji stosowane do nadmiarowego przesyłania wiadomości. Ponieważ atakujący węzeł mógłby podszywać się pod (symulować) stację bazową przez wysyłanie podrobionej wiadomości typu żądanie, w celu zidentyfikowania wiadomości wypływających rzeczywiście od stacji bazowej stosowane są jednostronne kody łańcuchowe.

Protokół rutowania TRANS (*Trust Routing for Location Aware Sensor Networks*) jest stosowany w sieciach scentralizowanych. Wykorzystuje on synchronizację i asymetryczną kryptografię oraz system μTESLA by zapewnić uwierzytelnienie wiadomości i poufność. Dzięki temu gwarantuje on, że wiadomość jest przesyłana ścieżką wyłącznie z zaufanymi węzłami stosując rutowanie uwzględniające położenie węzłów. Stacja bazowa rozsyła zaszyfrowane wiadomości do wszystkich swoich sąsiadów. Ale tylko zaufani sąsiedzi będą posiadali wspólny klucz konieczny do odkodowania wiadomości. Zaufany sąsiad dodaje wtedy swoją lokalizację (dla powrotu), koduje nową wiadomość z jego własnym dzielonym kluczem i przesyła dalej wiadomość do sąsiada położonego najbliżej celu. Gdy tylko wiadomość osiągnie cel, odbiorca może poświadczyć źródło (stację bazową) stosując MAC (kod identyfikacji wiadomości), odpowiedni dla stacji bazowej. Aby potwierdzić odbiór lub odpowiedzieć na wiadomość, węzeł docelowy może przesłać wiadomość zwrotną tą samą zaufaną ścieżką dostępu, którą doszła pierwsza wiadomość [5]. W bezprzewodowych sieciach sensorowych pojedynczy węzeł może bardzo łatwo zakłócić cały protokół rutowania przez przeszkadzanie w procesie szukania trasy. Zaproponowany w [6] bezpieczny protokół szukania trasy gwarantuje, po spełnieniu kilku warunków, że będą uzyskiwane poprawne informacje topologiczne. Ten scenariusz jest zbliżony do protokołu TRANS. Bezpieczeństwo polega na zastosowaniu MAC i akumulacji tożsamości węzła wzdłuż trasy przebytej przez wiadomość. W ten sposób węzeł źródłowy może odkryć topologię sieci sensorowej, jako że każdy węzeł wzdłuż trasy od źródła do celu dopisuje swój identyfikator do wiadomości. Aby mieć pewność, że wiadomość nie została zmieniona, tworzony jest kod MAC, który może zostać zweryfikowany zarówno w źródle, jak i w miejscu docelowym wiadomości powrotnej.

Tab. 1. Środki obrony stosowane przeciw różnym atakom
Tab. 1. Classification of attacks and the countermeasures

Warstwa sieciowa	Rodzaj ataku	Środki obrony
Fizyczna	Zagłuszanie	Rozproszone pasmo Priorytety Mniejsze wypełnienie Mapowanie Zmiana trybu
	Oszukiwanie	Zabezpieczenia Ukrywanie się
Połączeń	Kolizje	Korekcja kodu
	Przeciążenie	Ograniczenie obciążenia
	Złe zachowanie	Zmniejszenie ramek
Sieć i rutowanie	Omijanie/zachłanność	Redundancja, próbkowanie
	Samonaprowadzanie	Szyfrowanie
	Mylenie drogi	Filtrowanie wypływu
	Czarne dziury	Autoryzacja, monitoring Redundancja
Transport	Trasowanie rozpływowe	Klient wybiera połączenia
	Rozsynchronizowanie	Uwierzytelnienie

2.2. Ataki typu Sybil

Aby bronić się przed takim atakiem, sieć musi mieć mechanizm stwierdzający, czy przedstawiona przez węzeł identyfikacja jest jego jedyną identyfikacją. W [7] autorzy opisują metodę uprawomocnienia tożsamości przez sprawdzenie zasobów sieci. W takim teście zaufany węzeł wyznacza każdemu ze swoich sąsiadów inny kanał do komunikacji i oczekuje na odpowiedź. Następnie losowo wybiera kanał i nasłuchuje. Jeżeli węzeł wykryje transmisję to przyjmuje, że węzeł nadający na tym kanale jest węzłem fizycznym. W przeciwnym przypadku oznacza to, że tożsamość wyznaczona dla tego kanału nie jest fizyczną tożsamością. Inna technika obrony przed atakiem Sybil polega na wstępnej dystrybucji przypadkowych kluczy. Przy ograniczonej liczbie kluczy oferowanej przez sieć, atakujący węzeł, który losowo generuje sobie tożsamości, nie uzyska wystarczającej liczby kluczy, by przyjąć wielokrotne tożsamości i w ten sposób będzie niezdolny do wymiany wiadomości w sieci (nieważna tożsamość nie może kodować ani odkodowywać wiadomości).

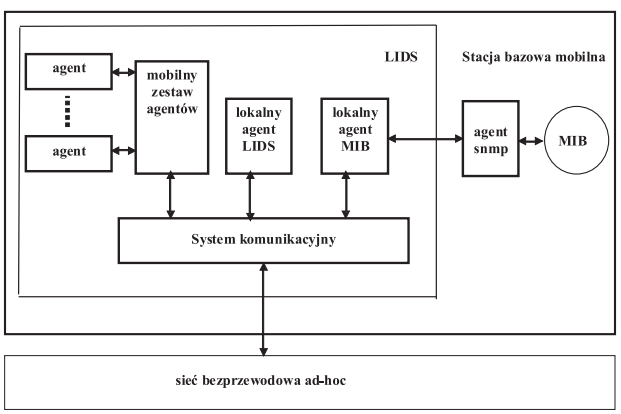
2.3. Ochrona stacji bazowej

Atak na stację bazową jest najgroźniejszy w skutkach. Dlatego atakujący starają się ją rozpoznać analizując ruch w sieci. Czasem specjalnie generując takie zdarzenia, które monitorowane są przez sieć, a następnie podsłuchując ruch w sieci i porównując jego natężenie w różnych miejscach, uzyskują wskazówki co do położenia stacji bazowej. W celu ochrony przed takimi atakami zaproponowano zastosowanie techniki ochrony [8] – przypadkowe forwardowanie przesyłek, w której czasami forwarduje się pakiet do węzła innego niż węzeł–rodzic sensora. To utrudnia rozpoznanie czystej ścieżki od sensora do stacji bazowej i pomaga zmniejszyć szybkość działania ataku monitorującego, ale nie chroni przed atakiem stosującym porównanie czasu przesyłania. Do obrony przed takim atakiem autorzy proponują strategię propagowania fraktali, która efektywnie „ukrywa" stację bazową przed atakami. Według tej strategii dowolny węzeł będzie (z pewnym prawdopodobieństwem) generował fałszywy pakiet wtedy, gdy jego sąsiad będzie wysyłać oryginalny pakiet do stacji bazowej. Fałszywy pakiet jest wysłany losowo do innego sąsiada, który może również wygenerować fałszywy pakiet. Po pewnym czasie fałszywe pakiety forwardowane przestają być przesyłane. To bardzo utrudnia atakującemu rozpoznanie stacji bazowej poprzez pomiary czasu przesyłania. Ponadto zastosowanie protokołu bezpiecznej komunikacji, takiego jak np. SPINS [9], może zapobiegać podsłuchiwaniu i chronić przed aktywnymi atakami na stację bazową.

2.4. Wykrywanie intruzów

W [10] autorzy klasyfikują systemy wykrywania wtargnięcia IDS oraz układy wykrywające wtargnięcia bazujące na sygnaturze, na anomaliach i na specyfikacji cech protokołu. Systemy takie wykorzystują zapisy z auditów systemu i z dzienników logowania.

IDS oparty na sygnaturach monitoruje sieć szukając specyficznych sygnatur, które są objawami wtargnięcia. Techniki sygnaturowe są efektywne w wykrywaniu ataków i nie generują wielu fałszywych alarmów. Wadą ich jest jednak to, że nie są zdolne do wykrywania nowych ataków o nieznanych sygnaturach. W IDS opartym na anomaliach zdefiniowane jest zachowanie standardowe i jakiekolwiek odchylenie od tego zachowania wyzwala system wykrywania wtargnięć. Podobnie działa IDS oparty na specyfikacji, który definiuje zestaw cech protokołu będących przejawami jego poprawnego działania. W [11] opisano architekturę wykrywania włamań do sieci opartą na lokalnym systemie wykrywania wtargnięcia (LIDS) w każdym węźle. Aby rozciągnąć system na całą sieć, lokalne systemy w sieci powinny współpracować ze sobą wymieniając dwa typy danych: dane bezpieczeństwa i alarmy przy wykryciu włamania. Dane bezpieczeństwa są wymieniane z hostami innych podsieci, natomiast alarmy o włamaniach powinny być stosowane do informowania innych lokalnych systemów wykrywania włamań. Obrazowe odwzorowanie architektury LIDS jest przedstawione na rys. 2.



Rys. 2. Architektura LIDS wg [11]
Fig. 2. LIDS architecture acc. to [11]

Zmienne z bazy MIB (baza danych zarządzania) są udostępniane przez protokół SNMP (*Simple Network Management Protocol*) uruchamiany na mobilnych hostach. Lokalna MIB jest przeznaczona do współpracy z agentami SNMP i dostarcza zmienne MIB od lokalnych LIDS lub mobilnych agentów. Mobilne agenty są odpowiedzialne za zbieranie i przetwarzanie danych od zdalnych hostów, szczególnie żądań protokołu SNMP. Agenty są zdolne do migracji między indywidualnymi hostami i mogą przesyłać dane z powrotem do ich własnych systemów LIDS. Lokalne agenty systemu LIDS są odpowiedzialne za wykrywanie i odpowiednie reakcje na lokalne wtargnięcia oraz reagowanie na zdarzenia wygenerowane przez zdalne węzły. Proponowane jest też rozważenie zastosowania kontroli SNMP jako źródła kontroli dla każdego LIDS — mobilne agenty będą wtedy odpowiedzialne za transport przesyłek. Do rozpoznania włamania sugerowane jest wykrywanie złego użycia albo anomalii. Po wykryciu włamania LIDS powinien przesłać informację o tym włamaniu do innych LIDS w sieci. Możliwe reakcje to zmuszenie potencjalnego intruza do ponownego uwierzytelnienia lub zignorowanie podejrzanego węzła, kiedy wykonuje czynności związane ze współpracą z siecią.

2.5. Bezpieczeństwo agregacji danych

Agregator jest odpowiedzialny za zbieranie nieopracowanych danych od podsieci węzłów i przetwarzanie/agregowanie ich na użyteczne dane. Taka technika jest szczególnie narażona na atak, gdy do agregowania danych stosowany jest pojedynczy węzeł. Techniki grupowania danych (agregacji) są dyskutowane w [12]. W zaproponowanym algorytmie węzły mają wyznaczone poziomy. Kiedy węzeł transmituje wiadomość, liczba przeskoków, którą ona wykonuje, jest proporcjonalna do poziomu węzła. Węzeł może zmieniać swój poziom w trakcie pracy sieci. Zastosowanie tej techniki powoduje, że węzły wyższego poziomu są w stanie porozumieć się przez klastry, podczas gdy sąsiednie węzły niższego poziomu już tego nie mogą. To skutecznie umożliwia wykonywanie lokalnych obliczeń w klastrach, a jednocześnie węzły wyższego poziomu mogą skoordynować te informacje, aby uzyskać rozwiązanie globalne. W technice zaproponowanej w [13] stosowany jest język TAG, podobny do używanego w bazach danych, do generowania zapytań przeznaczonych do badania sieci sensorowych. Jest to podejście ogólnego przeznaczenia, w którym stacja bazowa definiuje zapytania w tym języku, a sensory wysyłają w odpowiedzi dane z powrotem do stacji bazowej zgodnie ze schematem drzewa rutowania. W każdym punkcie drzewa dane są agregowane zgodnie ze schematem i zgodnie z odpowiednią funkcją agregacji, zdefiniowaną w zapytaniu.

W ukrytym ataku napastnik stara się wykonać niepoprawną agregację wyników dla użytkownika, tak by ten nie wiedział o tym ataku. Dlatego celem pracy [14] jest umożliwienie użytkownikowi potwierdzenia, że akceptuje on końcową wartość jako poprawną lub odrzucenia niepoprawnych wyników, gdy uważa, że wartości zostały zmienione przez atakującego. W pracy [15] autorzy proponują nową technikę agregacji, w której do zapewnienia bezpieczeństwa stosowany jest protokół μTESLA. Węzły organizują się w strukturę drzewa, w której wewnętrzne węzły działają jako agregatory. Protokół ten osiąga asymetrię przez opóźnione zamknięcie symetrycznych kluczy. Węzły–rodzice nie są wtedy zdolne do natychmiastowego zweryfikowania autentyczności danych węzła–dziecka, ponieważ klucz wygenerowany przez kod uwierzytelnienia wiadomości (MAC) nie będzie jeszcze ujawniony. Ta technika nie gwarantuje jednak, że węzły i agregatory dostarczą poprawnych wartości. Dlatego stacja bazowa musi być odpowiedzialna za rozprowadzanie tymczasowych kluczy do sieci, jak również klucza μTESLA do stacji bazowej, stosowanego do uprawomocniania kodu MAC. Węzły weryfikują kod uwierzytelnienia wiadomości swoich dzieci i są odpowiedzialne za kontrolowanie, czy kody te są właściwe.

Tab. 2. Wyniki symulacji wykrywania ataków wg [17]
Tab. 2. Simulation results acc. to [17]

Rodzaj ataku	Opis ataku	Wpływ na pracę sieci	Wykryte (%)	Ważne analizowane cechy
Okresowy błąd rutowania	Atakujący stale wysyła błędy rutowania	MAŁY: tylko gdy trasa idzie przez węzeł atakujący	95	Liczba błędów rutowania
Bierna dziura (sinkhole)	Atakujący odpowiada na żądanie trasy podając błędną trasę	ŚREDNI: tylko gdy żądanie trasy dotrze do węzła atakującego	70	Średnie i standardowe odchylenie liczby przeskoków
Aktywna dziura (sinkhole)	Atakujący żąda trasy do stacji bazowej i sam na to odpowiada	BARDZO DUŻY: zawsze skuteczny	100	Liczba zmian drogi do stacji bazowej

3. Sposoby obrony przed fizycznymi atakami

Jedno z możliwych rozwiązań, proponowanych do obrony węzłów po ich fizycznym przejęciu przez atakującego, jest ich samouszkodzenie. Węzeł niszczy sam siebie, niszcząc wszystkie dane i klucze, kiedy rozpoznaje atak. Taki mechanizm można stosować tylko w dużej bezprzewodowej sieci sensorowej, która ma wystarczającą redundancję w zakresie informacji, o ile koszt sensora jest znacznie mniejszy niż strata spowodowana włamaniem. Niestety istnieją techniki umożliwiające odczytanie zabezpieczonego oprogramowania i danych z kart typu *smartcard* (ręczne mikro-sondowanie, cięcie laserowe, manipulacje skupioną jonową wiązką światła). Po analizie tych technik autorzy w [16] podają przykłady środków zaradczych, które znacznie utrudniają ataki:

- losowo generowany sygnał zegarowy wprowadzający opóźnienia o przypadkowej wielkości pomiędzy każde dostrzegalne oddziaływanie na sensor a ważne operacje, które mogą być narażone na atak;
- zastosowanie procesorów o architekturze wielowątkowej, która umożliwia projektowanie wielowątkowego oprogramowania dzielonego sprzętowo na procesorze i losowo na poziomie instrukcji procesora;
- wbudowanie wewnętrznych autotestów w czujnikach, które spowodują awarię procesora po wykryciu próby ataku na sensor;
- zniszczenie specjalnych obwodów elektrycznych do testów – uniemożliwienie ataku ręcznego mikrosondowania;
- uniemożliwienie licznikowi programu dostępu do pełnej strefy adresowej;
- zastosowanie w górnej warstwie sensora dodatkowej warstwy metalowej, by uniemożliwić mikrosondowanie.

4. Wykrywanie anomalii

Dla wykrywanie włamań do sieci można też zastosować technikę wykrywanie anomalii w ruchu w danej sieci. Metoda wykrywania ataków przez wyróżnianie w sieci przesyłek normalnych i anomalnych [17] polega na porównaniu wybranego zestawu cech każdej przesyłki z cechami przesyłek uznanymi za typowe dla danej sieci. W tym celu określono zestaw 12 cech, których wartości należy wyznaczyć dla każdej sieci, z czego 9 cech jest zależnych od ruchu w sieci (dotyczą warunków przepływu przez węzeł) a 3 cechy nie (dotyczą warunków rutowania). Każdy anomalny ruch w sieci jest traktowany jako atak. W tym celu bada się najpierw zachowanie sieci w fazie treningu. Na końcu fazy treningu klastry w przestrzeni cech, które zawierają mniej niż ustalony procent wszystkich punktów są oznaczane jako anomalne. W ten sposób, w czasie pracy sieci każda przesyłka, w każdym węźle zostaje oceniona: jako normalna lub jako anomalna, czyli stanowiąca atak. Ważną cechą tej techniki wykrywania ataków na sieć jest to, że nie wymaga ona dodatkowej komunikacji pomiędzy węzłami sieci i pozwala przez to na zmniejszenie wymagań dotyczących źródeł energii w węzłach.

5. Perspektywy bezpieczeństwa

Ważnym aspektem bezpieczeństwa, szczególnie w mobilnych sieciach sensorowych, są systemy kodowania. Autorzy w [18] przedstawiają rozwiązanie problemu bezpieczeństwa dla mobilnych sieci sensorowych, przy czym zakładają że węzły w mobilnych sieciach są nieco większe niż w stacjonarnych ze względu na energię potrzebną do ruchu. Proponują więc zarządzanie grupami typu *multicast*. Węzły są grupowane w oparciu o bliskość położenia, a następnie tworzone są struktury drzewa bezpieczeństwa. Umieszczenie sensora na ruchomym elemencie może skutkować wzmocnieniem jego bezpieczeństwa w zakresie poufności, w tym szczególnie poufności jego lokalizacji. Dobrym przykładem jest system Cricket [19] przeznaczony do lokalizacji wewnątrz budynkowych. Węzły systemu wykorzystują rozmieszczone w budynku radiolatarnie do określenia swojego położenia. Dzięki temu sensory położenia mogą być umieszczane w węzłach mobilnych a nie instalowane w infrastrukturze budynku. Informacja o położeniu nie jest wtedy ujawniana w trakcie procesu jej uzyskiwania i może być dostarczona tylko do zainteresowanych osób w bezpieczny i poufny sposób. Przy projektowaniu nowych jeszcze bardziej bezpiecznych sieci potrzebne będą zaawansowane metody obliczeniowe do wyznaczania stopnia zaufania dla różnych rozwiązań projektowanych sieci sensorowych.

Na zakończenie można przytoczyć dwie prace idące w tym właśnie kierunku. W pracy [20] autorzy przedstawiają praktyczny sposób na obliczanie wskaźnika zaufania dla sieci bezprzewodowych. Zastosowano tu teorię grafów do wyznaczania ścieżki od węzła źródłowego do węzła docelowego i obliczania odpowiadającej jej wartości wskaźnika zaufania bezpieczeństwa sieci. Inni autorzy [21] przedstawiają technikę osiągania dla sieci typu ad-hoc oczekiwanego stopnia zaufania przy wymaganiach określających minimalne zapotrzebowanie na pojemność pamięci w węźle mobilnym. Wyliczenia oparte są na metodach probabilistycznych opartych na modelu o rozproszonym zaufaniu.

Bibliografia

1. Karlof C., Wagner D. (2003): *Secure routing in wireless sensor networks: Attacks and countermeasures.* Proc. 1st Int. Workshop on Sensor Network Protocols and Applications (SNPA'03).
2. Deng J., Han R., Mishra S. (2002): INSENS: *Intrusion-Tolerant Routing in Wireless Sensor Networks*, Technical Report CU-CS-939-02. Dept. Computer Science, Univ. Colorado.
3. Deng J., Han R., Mishra S. (2003): *A performance evaluation of intrusion-tolerant routing in wireless sensor networks*, Proc. IEEE Int. Workshop on Information Processing in Sensor Networks (IPSN'03), s. 349–364.
4. Deng J., Han R., Mishra S. (2004): *Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks*, IEEE International Conf. Dependable Systems and Networks (DSN(2004)), Florencja, Włochy.
5. Tanachaiwiwat S., Dave P., Bhindwale R., Helmy A.: (2003) *Poster abstract secure locations: routing on trust and isolating compromised sensors in locationaware sensor networks.* Proceedings of the 1st International Conference on Embedded Networked Sensor Systems, s. 324–325. ACM Press.
6. Papadimitratos P., Haas Z. (2002): *Secure routing for mobile ad hoc networks.* Proceedings of the SCS Communication Networks and Distributed System Modeling and Simulation Conference (CNDS 2002).
7. Newsome J., Shi E., Song D., Perrig A. (2004): *The Sybil attack in sensor networks: analysis & defences.* Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, s. 259–268. ACM Press.
8. Deng J., Han R., Mishra S. (2004): *Countermeasuers against traffic analysis in wireless sensor networks.* Technical Report CU-CS-987-04, University of Colorado at Boulder.
9. Perrig A., Szewczyk R., Tygar J., Wen V., Culler D. E. (2002): *Spins: security protocols for sensor networks.* Wireless Networking, s. 521–534.
10. Brutch P., Ko C. (2003): *Challenges in intrusion detection for wireless ad-hoc networks.* Symposium on Applications and the Internet Workshops (SAINT'03 Workshops).
11. Albers P., Camp O. (2002): *Security in ad hoc networks: A general intrusion detection architecture enhancing trust based approaches.* 1st International Workshop on Wireless Information Systems, 4th International Conference on Enterprise Information Systems.
12. Estrin, D. Govindan R., Heidemann J., Kumar S. (1999): *Next century challenges: Scalable coordination in sensor networks.* Mobile Computing and Networking, s. 263–270.
13. Madden S., Franklin M.J., Hellerstein J., Hong W. (2002): *Tag: a tiny aggregation service for ad-hoc sensor networks.* SIGOPS Oper. Syst. Rev. s. 131–146.
14. Przydatek B., Song D., Perrig A. (2003): *Sia: Secure information aggregation in sensor networks*, [www.cs.berkeley.edu/~dawnsong/papers/sia.pdf].
15. Hu L. Evans D. (2003): *Secure aggregation for wireless networks. SAINTW '03*: Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops), s. 384. IEEE Computer Society.
16. Anderson R. Kuhn M. (1997): *Low cost attacks on tamper resistant devices.* IWSP: International Workshop on Security Protocols, LNCS.
17. Loo Ch., Yong M. Leckie Ch., Palaniswami M.: *Intrusion Detection for Routing Attacks in Sensor Networks* [http://ww2.cs.mu.oz.au/~caleckie/ijdsn.pdf].
18. Kaya T., Lin G., Noubir G., Yilmaz A. (2003): *Secure multicast groups on ad hoc networks.* Proceedings of the 1st ACM workshop on Security of Ad hoc and Sensor Networks (SASN '03), s. 94–102. ACM Press.
19. Priyantha N., Chakraborty A., Balakrishnan H. (2000): *The cricket locationsupport system.* Proc. of the Sixth Annual ACM International Conference on Mobile Computing and Networking (MOBICOM), 08/2000.
20. Zhu H., Bao F., Deng R., Kim K. (2004): *Computing of trust in wireless networks.* Proceedings of 60th IEEE Vehicular Technology Conference, Los Angles, Kalifornia, USA, 09/2004.
21. Ren K., Li T., Wan Z., Bao F., Deng R., Kim K. (2004): *Highly reliable trust establishment scheme in ad hoc networks.* Computer Networks: The International Journal of Computer and Telecommunications Networking, s. 687–699, 08/2004.

Safety issues in wireless sensor networks

Abstract: Wireless sensor networks are exposed to danger of attacks from people and from environment. Sensor nodes often have limited computation and communication resources and battery power. The resource constraints and security issues make designing mechanisms for safety of communication in large sensor networks particularly challenging. The growing research activity in the field of wireless sensor network security is very interesting for designers of data acquisition systems. Familiarity with the current publications in this field will be greatly helpful. In the paper major topics in wireless sensor networks security are presented. Next, classification of attacks, and known corresponding defensive measures are discussed. In the conclusion the perspectives for building a safe mobile sensor networks are introduced.

Keywords: wireless sensor networks, mobile networks, attack detection, safety

mgr inż. Tadeusz Goszczyński

Od 40 lat pracuje w PIAP, Warszawa. Zaczynał od analogowych systemów automatyki. Laureat zespołowej Nagrody Państwowej za system automatyki stosowany w polskich elektrowniach. Następnie kierownik trzech Projektów Celowych zakończonych produkcją w PIAP stanowisk do legalizacji ciepłomierzy (TEC-LEG nagrodzone Złotym Medalem na Targach AUTOMATICON). Nagrodzony w konkursie Mistrz Techniki NOT za Zestaw przenośny do sprawdzania ciepłomierzy. Autor podręcznika o sieci LonWorks, licznych publikacji i 12 uzyskanych patentów.

e-mail: tgoszczynski@piap.pl