STUDIA INFORMATICA 2012
Volume 33 Number 3A (107)

Janusz GÓRSKI, Alan TUROWER
Politechnika Gdańska, Wydział Elektroniki, Telekomunikacji i Informatyki

ZARZĄDZANIE ZAUFANIEM W BEZPRZEWODOWYCH SIECIACH CZUJNIKÓW – STUDIUM PRZYPADKU

Streszczenie. W artykule przedstawiono studium przypadku, dotyczące zastosowania bezprzewodowej sieci czujników do wspomagania pacjenta z nadwagą w jego środowisku domowym. Przyjęto, że sieć wykorzystuje metodę rozproszonego zarządzania zaufaniem i pokazano, że metoda ta umożliwia wykrycie i izolację czujników realizujących działania sprzeczne z polityką sieci. Ilościowe oszacowanie czasu niezbędnego do wykrycia takich węzłów sieci zostało dokonane na drodze symulacyjnej, z wykorzystaniem dedykowanego symulatora. W podsumowaniu wskazano problemy, które będą przedmiotem dalszych badań zmierzających w kierunku doskonalenia proponowanej metody zarządzania zaufaniem oraz jej oceny.

Słowa kluczowe: bezprzewodowe sieci sensorów, zastosowania medyczne, zaufanie, bezpieczeństwo

TRUST MANAGEMENT IN WSN – A CASE STUDY

Summary. The paper presents a case study related to application of WSN to supporting a patient with overweight in his/her home environment. It was assumed that the network implements a method of distributed trust management and is was demonstrated that this method provides for detection and isolation of sensors violating the network policies. Quantitative estimates of time necessary to detect such malicious nodes were obtained with the help of a dedicated network simulator. In conclusion we identified problems which will be further investigated, targeting at improvement and assessment of the proposed trust management method.

Keywords: wireless sensor networks, medical applications, trust, security

1. Wstęp

Bezprzewodowe sieci czujników (ang. *Wireless Sensor Networks – WSN*) zwiększają swoje znaczenie w wielu obszarach zastosowań, w tym w opiece zdrowotnej, obronności, zarządzaniu bezpieczeństwem, monitoringu środowiska i innych. Rośnie złożoność takich sieci oraz gwałtownie zwiększa się różnorodność i stopień skomplikowania związanych z nimi zastosowań. Powoduje to, że zarządzanie takimi sieciami staje przed coraz bardziej trudnymi do pogodzenia celami bezpieczeństwa, wydajności i elastyczności. Dodatkowe trudności wynikają z tego, że różne węzły lub podsieci mogą być zarządzane przez różne osoby lub organizacje. Oprócz niedoskonałości technicznych i błędów ludzkich, muszą być również brane pod uwagę szkodliwe działania intencjonalne.

Zapewnianie bezpieczeństwa sieci czujników poprzez kopiowanie praktyk z tradycyjnych sieci nie jest skuteczne, ponieważ czujniki podlegają innym ograniczeniom niż węzły takich sieci. Podstawowa różnica polega na ograniczeniu zasobów czujników (pamięć, moc obliczeniowa, energia zasilania), co powoduje, że ulokowanie w czujniku zaawansowanych mechanizmów bezpieczeństwa, które często wymagają znacznych zasobów, nie jest możliwe.

Jednym ze sposobów radzenia sobie z tymi ograniczeniami jest jawne odwołanie się do pojęcia zaufania. Wychodzi się tu z założenia, że wiedza na temat wiarygodności poszczególnych węzłów może być budowana w sposób kolektywny (przy współudziale wielu innych węzłów), a następnie udostępniana w sieci po to, by mogły być podejmowane decyzje, uwzględniające tę wiarygodność. Zakłada się tu również, że taki sposób zarządzania będzie tańszy (w sensie konsumpcji zasobów), a jednocześnie jakość podejmowanych decyzji nie ulegnie znaczącemu pogorszeniu. W szczególności, rozróżnienie wiarygodnych i nierzetelnych węzłów pozwoli na podjęcie decyzji prowadzących do izolacji i wykluczenia z sieci węzłów z bardzo niskim poziomem zaufania.

Celem tego artykułu jest przedstawienie zarządzania zaufaniem w sieci WSN jako skutecznej techniki wspierającej bezpieczeństwo sieci WSN. Przedstawiono w nim autorską metodę zarządzania zaufaniem i studium przypadku.

2. Powiązane prace

Wykorzystanie WSN w aplikacjach wspierających codzienne życie jest bardzo aktualnym tematem [1]. Szczególnie istotne są zastosowania w medycynie i wspomaganiu zdrowego stylu życia, ponieważ średnia wieku społeczeństwa rośnie i coraz istotniejsze stanie się zapewnienie odpowiedniej opieki medycznej w domu pacjenta. Propozycję takiego systemu przedstawiono w [2], gdzie zaprezentowano architekturę oraz eksperymenty laboratoryjne

nad ciągłą opieką medyczną nad pacjentami przy wykorzystaniu bezprzewodowych sieci sensorów. Uzyskane wyniki sugerują niższe koszty oraz lepszą jakość takiej opieki. W trakcie prac nad platformą ANGEL [3] tworzącą środowisko do realizacji różnych zastosowań wykorzystujących sieci czujników, ukierunkowanych na wspomaganie zastosowań medycznych oraz związanych ze środowiskiem domowym, również zademonstrowano przykłady takich systemów. W [4] przedstawiono narzędzia umożliwiające symulacje WSN pod kątem zastosowań medycznych, jak również istniejące aplikacje wykorzystujące bezprzewodowe sieci sensorów w medycynie.

Propozycję zarządzania zaufaniem w sieciach WSN przedstawiono w [5]. Rozwiązanie to polega na rozszerzeniu protokołu LEACH (ang. *Low-Energy Adaptive Clustering Hierarchy* [6] o zarządzanie zaufaniem, przy zachowaniu wszystkich zalet oryginalnego protokołu, takich jak wsparcie dynamicznych zmian w sieci oraz ograniczenie liczby informacji przesyłanych pomiędzy węzłami w celu wyznaczania ścieżek (ang. *routing*).

Podejście opisane w niniejszej pracy różni się od prac innych tym, że jest całkowicie zdecentralizowane, zarówno zmiany głowy klastra, jak i izolacja głowy klastra z sieci nie wpływa na działanie mechanizmu. Ponadto struktury, w których są przechowywane dane o zaufaniu, zajmują stosunkowo mało miejsca, co pozwala na stosowanie mechanizmu w skromniejszych sprzętowo urządzeniach kosztem nieco większej liczby wymienianych w sieci wiadomości. Opisana tu metoda nie modyfikuje ani nie wpływa na protokół routingu, zatem może być stosowana z dowolnym protokołem routingu używanym w WSN.

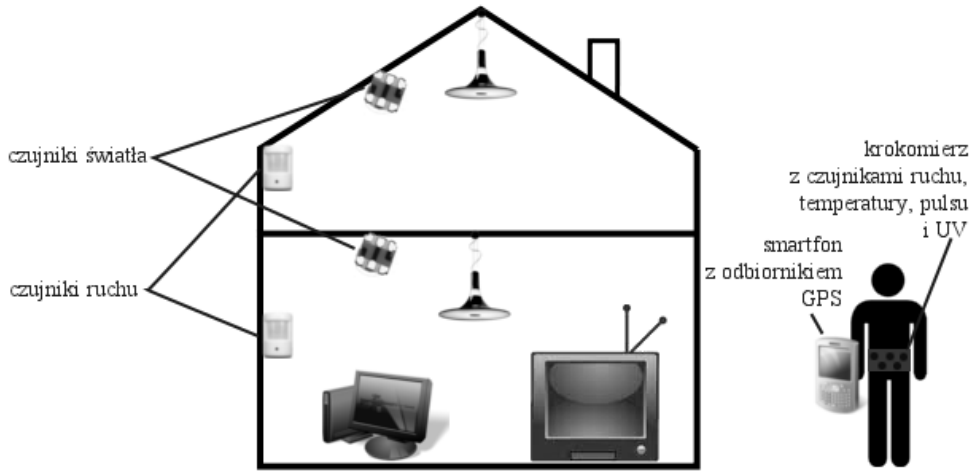
3. Studium przypadku – opieka nad pacjentem w środowisku domowym

Szczególnie istotnym obszarem zastosowań WSN jest opieka zdrowotna. Można tu osiągnąć wiele korzyści, na przykład uwolnienie pacjenta od kłopotliwych przewodów i wynikające stąd poczucie swobody czy leczenie lżej chorych pacjentów w ich domach, co powoduje obniżenie kosztów opieki medycznej oraz mniejszy stres u pacjentów.

Przykład użycia WSN w domu pacjenta zaprezentowano w scenariuszu demonstracyjnym projektu ANGEL [3]. Poglądowe przedstawienie tego scenariusza zaprezentowano na rys. 1.

Bohaterem scenariusza jest Bob, który ma nadwagę i chce schudnąć. Jego lekarz zalecił mu terapię światłem i ćwiczenia aerobowe. Przebieg leczenia jest wspomagany siecią WSN. Składa się ona z czujników ruchu, dzięki czemu lampy lecznicze są włączane tylko w pomieszczeniach, w których przebywa Bob. Dodatkowo czujniki światła kontrolują poziom oświetlenia, by lampy nie były włączane, gdy jest wystarczająco jasno. Bob jest również wyposażony w urządzenie, które na bieżąco przesyła do systemu informacje o podejmowanych

przez niego ćwiczeniach (zaawansowana forma krokomierza). Czujnik UV przesyła dodatkowo informację o tym, czy Bob znajduje się w domu czy też na zewnątrz. Bob jest również wyposażony w czujniki mierzące puls oraz temperaturę jego ciała. Dzięki temu istnieje możliwość oceny stanu jego zdrowia, na przykład wykrycia ataku serca. W takim przypadku system natychmiast powiadamia pogotowie i informuje o miejscu pobytu Boba, wykorzystując dane z odbiornika GPS, który Bob również ma przy sobie.



Rys. 1. Opieka nad pacjentem w środowisku domowym
Fig. 1. Patient care in a home environment

Cały system jest zarządzany poprzez interfejs dostępny z przeglądarki internetowej. Interfejs ten jest dostępny zarówno z komputera, jak i z urządzenia typu PDA, które Bob ma przy sobie (np. smartfon). Informacje dotyczące Boba mogą być również wyświetlane na innych urządzeniach, na przykład na telewizorze zaopatrzonym w odpowiednią przystawkę umożliwiającą mu współpracę z siecią WSN. W dowolnym czasie Bob ma możliwość zasięgania porady lekarskiej, zaś lekarz ma bieżący dostęp do wyników pacjenta. System może również przypominać Bobowi o zaplanowanych ćwiczeniach, śledzić postęp w realizacji zaplanowanych zadań oraz na różne sposoby motywować Boba do wykonywania ćwiczeń.

W aplikacjach medycznych istotną kwestią jest ryzyko, dotyczące bezpieczeństwa i prywatności. Wadliwe funkcjonowanie systemu może w pewnych warunkach zagrozić zdrowiu, a nawet życiu pacjenta (na przykład ordynując ćwiczenia lub terapię pozostające w wyraźnym konflikcie z jego stanem zdrowia). Może również prowadzić do ujawnienia danych dotyczących zdrowia i środowiska Boba podmiotom do tego nieuprawnionym, co naruszy prawo Boba do zachowania prywatności.

Ochronę danych medycznych nakazują zarówno krajowe, jak i europejskie przepisy o ochronie danych osobowych [7]. Można tu wymienić Art. 27. Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych [8], Art. 6. Konwencji Nr 108 Rady Europy, Art. 8. Dyrektywy 95/46/WE [9] czy Rozporządzenie Ministra Zdrowia w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej oraz sposobu jej przetwarzania [10].

Rozwiązanie przyjęte w projekcie ANGEL polega na tym, że Bob ma możliwość przekazywania do systemu informacji na temat kontekstu, w którym się aktualnie znajduje (nazywanego *profilem*) [11]. Na podstawie tej informacji system ujawnia lub ukrywa dane, których wyświetlenie mogłoby naruszyć prywatność Boba. Na przykład, dane dotyczące stanu zdrowia są wyświetlane na ekranie telewizora, który znajduje się w domu, jeżeli Bob wybiera profil „jestem sam". Jednak gdy wybierze profil „jestem ze znajomymi", na ekranie pojawiają się jedynie informacje o warunkach środowiskowych panujących w mieszkaniu, natomiast informacje o stanie zdrowia zostają ukryte. Bob ma również możliwość autoryzacji urządzeń innych niż jego własny telewizor i smartfon – może na przykład przekierować dane na telewizor Sary, jeżeli znajdzie się w jej domu.

Cały system składa się z wielu współpracujących ze sobą czujników. Stworzenie takiego systemu przy użyciu czujników przewodowych nie byłoby praktycznie możliwe. Jednakże użycie WSN nakłada wiele wymagań, np. czujniki muszą być dostatecznie małe, by nie wpływać na komfort użytkowania oraz muszą być energooszczędne, aby wykluczyć częste wymiany baterii. Również zasięg sygnałów radiowych z czujników podlega ograniczeniom.

4. Rozproszone zarządzanie zaufaniem

Metody zarządzania zaufaniem zdobywają coraz większą popularność, ponieważ umożliwiają skuteczne zapewnianie bezpieczeństwa przy jednoczesnym utrzymaniu w rozsądnych granicach kosztownej w WSN transmisji danych oraz nakładów na obliczenia związane z zabezpieczeniami kryptograficznymi.

Ocena zaufania pokładanego w węzłach sieci może być scentralizowana lub rozproszona. W przypadku dużych sieci ocena scentralizowana dokonywana przez dedykowany węzeł prowadzi do problemów z wydajnością i do nadmiernej koncentracji ruchu w sieci. Ograniczenia takiego nie mają metody, w których ocena ta jest rozproszona, prowadzona ze współudziałem większej grupy węzłów. Dlatego w dalszej dyskusji założono, że każdy węzeł w sieci bierze udział w ocenie wiarygodności i zaufania, a podejmowane decyzje mają wpływ na sąsiedztwo węzła. Metoda taka została zaproponowana w [12, 13].

Założono, że sieć ma strukturę drzewiastą i istnieją w niej trzy rodzaje węzłów:

- *zbiornik* – węzeł o znacznych możliwościach obliczeniowych, podłączony do stałego źródła energii, który przetwarza wszystkie otrzymane dane,
- *liście* – węzły, których głównym zadaniem jest pomiar i przekazywanie zmierzonych danych,
- *routery* – węzły, które oprócz pomiarów i przekazu mierzonych przez siebie danych przekazują również dane od liści znajdujących się zbyt daleko od *zbiornika*, w jego stronę.

Wprowadzenie do sieci modelu rozproszonego zarządzania zaufaniem umożliwia wykrywanie uszkodzonych węzłów przez ich sąsiadów (tzn. przez te węzły, które mogą się z nimi bezpośrednio komunikować). Dzięki temu nakłady na to zadanie są rozłożone bardziej równomiernie niż przy zastosowaniu zarządzania scentralizowanego. Istota tego modelu polega na tym, że każdy węzeł przechowuje dane o zaufaniu do pozostałych węzłów z jego otoczenia i na tej podstawie niezależnie od innych podejmuje własne decyzje. Na dane przechowywane w węźle, odnoszące się do zaufania do innych węzłów, mają również wpływ jego sąsiedzi. Węzły nie tylko obserwują zachowania innych węzłów, ale również przekazują sobie wzajemnie rekomendacje dotyczące tych węzłów. W wynikowej ocenie zaufania rekomendacje te brane są pod uwagę tym bardziej, im bardziej zaufany jest węzeł rekomendujący.

W omawianym mechanizmie każdy z węzłów w sieci pełni dwie role. Może być poddawany ocenie – gdy wysyła komunikat do innego węzła, i ten inny węzeł ocenia swoje zaufanie do nadawcy. Może także być oceniającym – gdy otrzymuje komunikat od innego węzła i ocenia swoje zaufanie do nadawcy. Jedynie zbiornik nie jest poddawany ocenie – założono, że dopóki jest dostępny, pozostaje godny zaufania.

Podczas odbioru komunikatu decyzja o zaufaniu do nadawcy jest podejmowana na podstawie następujących czynników:

- zgodności z polityką sieci – odbiorca weryfikuje zachowanie nadawcy oraz otrzymaną wiadomość pod względem zgodności z polityką sieci;
- reputacji – odbiorca bierze pod uwagę swoje zaufanie do nadawcy z uwzględnieniem wpływu na nie rekomendacji otrzymanych od innych węzłów.

W zależności od wyniku oceny zaufania, oceniający może zachować się na dwa sposoby. Jeśli ocena wypadła pozytywnie, kontynuuje przetwarzanie wiadomości i odpowiednio modyfikuje swój poziom zaufania do nadawcy. Jeśli natomiast przypisuje wiadomości nadawcy zbyt niski poziom zaufania, odrzuca przekazaną wiadomość (nie przetwarza odebranych danych) i obniża swój poziom zaufania do nadawcy. Dodatkowo, zgodnie z przyjętą polityką, przekazuje (jako rekomendacje) aktualną ocenę zaufania swoim sąsiadom.

Każdy nowy węzeł otrzymuje poziom *neutralnego zaufania* – jest to swoisty kredyt udzielony węzłowi (pozostałe węzły nie mają jeszcze żadnych informacji związanych z jego wiarygodnością). Następnie, w zależności od jego zachowania, jego reputacja może się zmienić. Gdy reputacja spadnie poniżej wartości nazwanej *punktem odcięcia*, węzeł jest postrzegany jako niewiarygodny i wiadomości otrzymywane od tego węzła są odrzucane bez weryfikacji ich zgodności z polityką sieci. W zależności od zaufania przypisywanego węzłom zmieniane są również trasy przesyłania wiadomości (ang. *routing*) tak, aby dane nie były przekazywane przez niezaufane węzły. Jeśli reputacja węzła spadnie poniżej punktu odcięcia, nie może on odzyskać zaufania, chyba że wskutek specjalnie w tym celu skonstruowanej procedury przywracania węzłów (może się to wiązać na przykład z koniecznością manualnej inspekcji węzła, jego wymianą itp.).

Przyjęto, że w zaprezentowanym wcześniej studium przypadku każdy z wykorzystywanych tam czujników zarządza zaufaniem, zgodnie z przedstawionymi wcześniej zasadami. Dzięki temu dane odbierane z węzłów zaufanych mogą być poddawane mniej zaawansowanym środkom z punktu widzenia oceny ich bezpieczeństwa, co korzystnie odbije się na wydajności i długowieczności sieci. Natomiast węzły, do których zaufanie spadnie zbyt nisko, zostaną poddane izolacji i przestaną być zagrożeniem dla usług świadczonych przez sieć.

Gdy węzeł zostanie wyizolowany, może się okazać, że od sieci zostanie odcięty jakiś jej fragment, składający się z zaufanych węzłów, których jedyna droga do zbiornika prowadziła przez wyizolowany węzeł. Można temu zapobiec poprzez zwiększenie gęstości rozmieszczenia węzłów – wtedy ze znacznie większym prawdopodobieństwem będzie istniała droga od omawianej podsieci do zbiornika, prowadząca tylko przez zaufane węzły. Założono, że w wypadku wyizolowania fragmentu sieci jej administrator powinien zostać powiadomiony przez przekazanie informacji, że zbiornik nie otrzymuje danych z pewnego podzbioru czujek.

Poniżej zaprezentowano dwa przykładowe scenariusze, które demonstrują przydatność zarządzania zaufaniem w omawianym systemie.

4.1. Awaria sensora

Sensor może ulec awarii i w efekcie przestaje przesyłać dane lub przesyła dane błędne. Brak danych może być stosunkowo łatwo wykryty, przy odpowiednim doborze protokołów wymiany tych danych. Założono, że dane przekłamane można wykryć, zanim dotrą do zbiornika danych (stosując odpowiednie testy). W efekcie, zaufanie do nadawcy zostanie obniżone, co w konsekwencji może doprowadzić do odcięcia źródła przekłamań danych. Na przykład, jeżeli czujnik światła zacznie przesyłać informacje o natężaniu oświetlenia przekraczającym wartości ustawione w polityce sieci, zostanie to wykryte (poprzez odpowiednie asercje sprawdzające), dzięki czemu lampy w domu Boba nie włączą się. Jeśli nieprawidłowe dane zostaną przesłane wielokrotnie, zaufanie do czujnika zostanie obniżone do poziomu wykluczenia z sieci. Odpowiednie powiadomienia mogą zostać wysłane do zbiornika danych i wyświetlone na odbiorniku telewizyjnym oraz smartfonie Boba. Dane z uszkodzonego czujnika nie będą odbierane do czasu naprawy i zresetowania związanego z nim poziomu zaufania w sieci. Reset może nastąpić poprzez interwencję administratora systemu lub wstawienie nowego czujnika, który otrzymuje domyślny, inicjalny poziom zaufania.

4.2. Nieuczciwy dostawca usług

Bob może zechcieć włączyć do systemu kolejne urządzenia bądź dodać nowe usługi do już istniejących. Daje to możliwość dołączenia do systemu urządzeń pracujących pod kontrolą oprogramowania, mogącego mieć szkodliwy wpływ na działanie systemu, a przez to za-

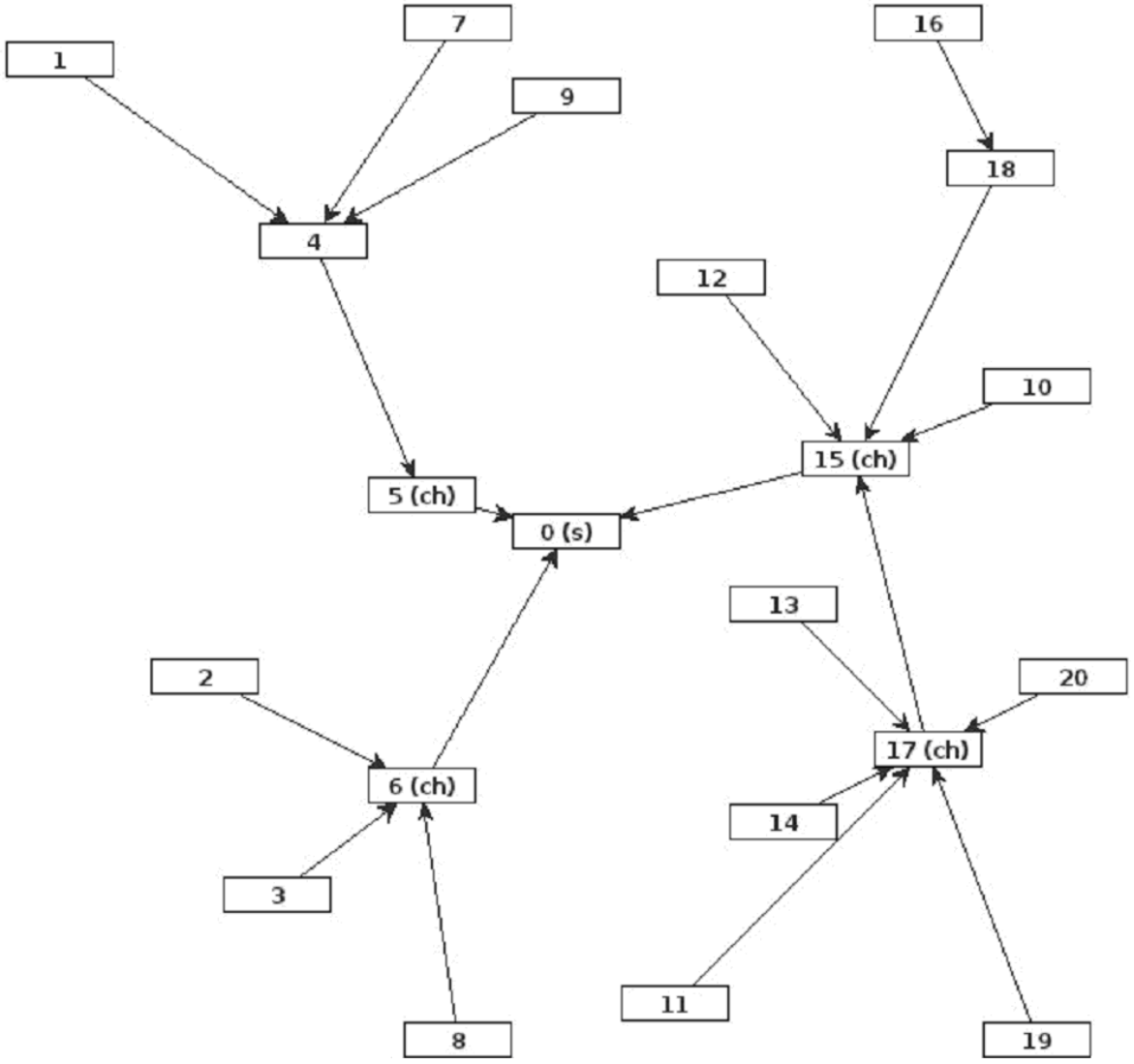
grozić zdrowiu, a w skrajnej sytuacji nawet życiu Boba. Jeżeli Bob autoryzował nowe urządzenie w systemie, może mieć ono dostęp do jego informacji osobowych. Jeśli jednak urządzenie będzie usiłowało wykonać akcje niedozwolone dla przypisanej mu roli i/lub zabronione przez politykę sieci i zostanie to wykryte przez którykolwiek z pozostałych węzłów, zaufanie do niego zostanie zmniejszone i w konsekwencji urządzenie zostanie wykluczone z sieci. Odpowiednie powiadomienia będą wysłane do zbiornika danych i wyświetlone na urządzeniach dostępowych Boba, dzięki czemu może on szybko dowiedzieć się o potencjalnym zagrożeniu wynikającym z podłączenia nowego urządzenia.

5. Skuteczność zarządzania zaufaniem

W poprzednich pracach [12, 13] przedstawiono metodę oceny skuteczności zaproponowanego tam modelu zarządzania zaufaniem. Metoda ta wykorzystuje dedykowany symulator sieci WSN. Przeprowadzone badania wskazują, że przy odpowiedniej strukturze, uwzględniającej klastry dla większych sieci, przedstawiony wyżej mechanizm zarządzania zaufaniem umożliwia wykrywanie ‘złośliwych’ sensorów realizujących działania niezgodne z polityką sieci i ich wykluczanie. Dotychczasowe badania sugerują również, że czas konieczny do zlokalizowania i wykluczenia wadliwego sensora jest liniowo zależny od liczby sensorów w sieci, gdy sieć nie jest podzielona na klastry [12, 13], natomiast przy klastrowej strukturze sieci jest praktycznie stały [13].

Poniżej przedstawiono wyniki symulacji zarządzania zaufaniem w sieci realizującej scenariusz opieki nad Bobem. Założono, że sieć składa się z 20 węzłów, przy czym niektóre węzły nie mogą przesłać swoich danych bezpośrednio do zbiornika i muszą korzystać z pośrednictwa innych węzłów. Węzły oddalone są od siebie od kilku centymetrów do kilku metrów i są podzielone na cztery klastry. Rolę zbiornika pełni smartfon Boba. Założono, że sieć obejmuje powierzchnię niewykraczającą poza obszar ***S*** o wymiarach 30 na 30 metrów. Rozkład węzłów w badanym przypadku przedstawiono na rys. 2. Oznaczenie *(ch)* wskazuje na głowę klastra, zaś *(s)* na zbiornik. Strzałki wskazują ścieżki routingu (na początku symulacji) z kierunkiem przepływu danych od węzłów do zbiornika.

Czas w symulatorze mierzony jest w *turach symulacji*. W trakcie jednej tury każdy z węzłów asynchronicznie wykonuje wszystkie przypisane mu akcje: wysyła jedną wiadomość do zbiornika, przekazuje wiadomości wysłane przez inne węzły (jeśli jest routerem), odbiera ewentualną wiadomość rozgłaszaną przez zbiornik i wykonuje procedurę aktualizacji danych o zaufaniu. Przyjęto, że zasięg każdego węzła nie przekracza 10 metrów (w projekcie ANGEL założono, że czujniki komunikują się na bazie protokołu ZigBee [14]). Przyjęto również, że zbiornik znajduje się na środku obszaru ***S***.



Rys. 2. Rozkład węzłów w badanej sieci
Fig. 2. Nodes distribution during experiments

Przy powyższych założeniach przeprowadzono dwa eksperymenty:

- EI: uszkodzeniu uległy węzły pracujące od dłuższego czasu w sieci; w tej sytuacji założono, że inicjalnie węzły te mają wysoki poziom zaufania;
- EII: do sieci zostały dołączone węzły wykonujące działania niedozwolone w polityce sieci; w tej sytuacji założono, że węzły te rozpoczynają swój udział w sieci z neutralnym poziomem zaufania.

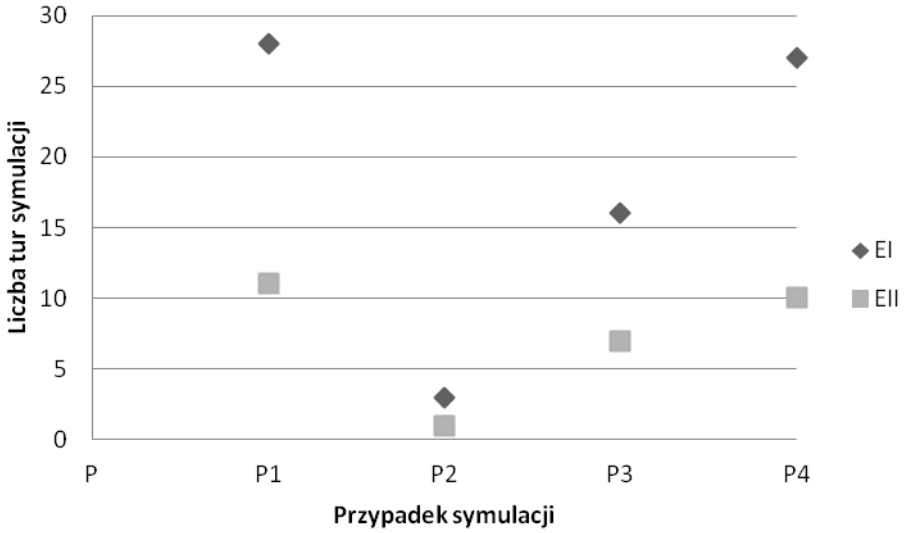
Każdy z powyższych eksperymentów przeprowadzono dla czterech poniższych przypadków:

- P1: uszkodzeniu uległ węzeł będący liściem;
- P2: uszkodzeniu uległ węzeł będący głową klastra;
- P3: uszkodzeniu uległy dwa węzły, jeden będący liściem, jeden będący głową klastra – na przykład Bob się przewrócił, uszkadzając czujniki umieszczone na jego ciele lub czujniki korzystały ze wspólnego źródła zasilania, które uległo awarii;

- P4: uszkodzeniu uległy trzy węzły, dwa będące liśćmi znajdującymi się w jednym klastrze, jeden będący głową tego klastra.

W eksperymentach EI i EII założono, że wiadomości niespełniające polityki sieci stanowią 70% transmisji od uszkodzonego/'złośliwego' węzła, zaś każdy inny węzeł może wysłać taką wiadomość z 2% prawdopodobieństwem (ze względu na możliwe błędy transmisji). W każdej turze symulacji zbiornik rozsyła wiadomość skierowaną do wszystkich węzłów w sieci (*broadcast*). Wszystkie węzły sieci otrzymują inicjalną wartość zaufania $z = 100$ w skali od 0 do 100, a więc założono że od dłuższego czasu sieć działa bez zakłóceń. W eksperymencie EI również węzły uszkodzone mają inicjalną wartość zaufania $z = 100$. Natomiast w eksperymencie EII przyjęto, że węzły 'złośliwe' rozpoczynają pracę z neutralnym poziomem zaufania, $z = 50$.

Na rys. 3 przedstawiono wyniki symulacji dla poszczególnych eksperymentów. Na osi pionowej reprezentowane są tury symulacji, natomiast na osi poziomej zaznaczono przypadki odnoszące się do eksperymentów.



Rys. 3. Czas (mierzony liczbą tur symulacji) konieczny do wykrycia wszystkich uszkodzonych / nieuczciwych węzłów w sieci dla poszczególnych przypadków testowych
Fig. 3. Time (number of simulation turns) needed to detect all faulty / dishonest nodes in the network for each case set

Jak widać na rys. 3, czas wykrycia wadliwego węzła zależy od jego aktywności w sieci – ponieważ głowy klastrów przekazują znacznie więcej wiadomości niż liście, ich wykrycie i izolacja następują szybciej. Rysunek 3 ilustruje także, w jaki sposób czas wykrycia i izolacji węzłów uszkodzonych znajdujących sie w jednym klastrze zależy od liczby tych węzłów oraz w jaki sposób czas ten zależy od inicjalnego poziomu zaufania do tych węzłów.

6. Podsumowanie

W niniejszym artykule zaprezentowano przykładowy scenariusz wykorzystania bezprzewodowej sieci czujników oraz niektóre zagrożenia, którym można zapobiegać poprzez użycie mechanizmu zarządzania zaufaniem, który został przez nas zaproponowany w [13, 14]. Przedstawiono wyniki analiz, które zostały wykonane z pomocą specjalnie w tym celu opracowanego symulatora. Wyniki te ilustrują skuteczność mechanizmu zarządzania zaufaniem, w sytuacji gdy czujniki ulegają uszkodzeniom oraz w sytuacji gdy w sieci pojawiają się węzły wykonujące celowe działania destrukcyjne.

W dotychczasowych badaniach przyjmowano wiele założeń, które będą usuwane w toku dalszych prac.

Istotną kwestią jest celowa zmiana zachowania węzła, taka by najpierw zdobyć zaufanie węzłów w sieci, a potem ją zaatakować. Węzeł taki osiągnie wysoki poziom zaufania i może być obdarzony w sieci „specjalnymi względami" dotyczącymi bezpieczeństwa. Stąd ważne jest, by mechanizm zarządzania zaufaniem możliwie szybko wykrył także taki przypadek i wyizolował dany węzeł. W ramach dalszych badań zostaną rozważone rozszerzenia algorytmu wyznaczania zaufania do węzła tak, aby decyzja ta była podejmowana nie tylko na podstawie bieżącej obserwacji oraz odebranych rekomendacji, ale również w zależności od jego przeszłych akcji. Rejestracja historii zachowań węzła tworzy warunki do wykrywania sygnatur ataków i odpowiedniej modyfikacji zaufania. Jednak takie rozwiązania spowodują zwiększenia nakładów obliczeniowych w węzłach, a więc muszą być wprowadzane jedynie tam, gdzie będzie to uzasadnione.

Głębszej analizy wymaga również wpływ mobilności sieci na decyzje związane z wykluczaniem węzłów, które utraciły zaufanie. Mobilność powoduje, że węzeł, który ma niski poziom zaufania ze strony węzłów, z którymi też współpracuje, może nawiązać kontakt z węzłem nowym, który przydzieli mu neutralny poziom zaufania. Może to spowodować, że mobilność będzie stanowiła sposób na 'ucieczkę' przed utratą zaufania, mimo że węzeł będzie prowadził działania destruktywne.

Odrębnej analizy wymagają również scenariusze, w których przedmiotem ataku jest sam mechanizm zarządzania zaufaniem. Dotychczas zakładano, że mechanizm zarządzania zaufaniem działa zawsze poprawnie.

Węzły oceniają wzajemnie swoje zachowania (komunikaty) i na tej podstawie podejmują decyzje o zaufaniu. Możliwe jest więc, że węzeł utraci zaufanie, dlatego że przekazał wadliwy komunikat odebrany od innego węzła, któremu ufał. Może to doprowadzić do wykluczeń węzłów poprawnych, znajdujących się na ścieżce od węzła wadliwego do zbiornika. Jest to tym bardziej możliwe, jeżeli założymy, że środki detekcji uszkodzeń będą wzmacniane w stosunku do węzłów niezaufanych, a rozluźniane w stosunku do węzłów zaufanych.

W dalszych badaniach zostanie położony nacisk na znalezienie rozsądnego kompromisu pomiędzy dokładnością lokalizacji węzłów uszkodzonych a elastycznym doborem zabezpieczeń, w zależności od wzajemnego zaufania pomiędzy węzłami sieci.

BIBLIOGRAFIA

1. Stankovic J. A.: Wireless Sensor Networks for In-Home Healthcare: Potential and Challenges, Technical Report CS-2006-11, Uniwersytet Virginia, 2005.
2. Virone G. i in.: An Advanced Wireless Sensor Network for Health Monitoring, w Proceedings of the Transdisciplinary Conference on Distributed Diagnosis and Home Healthcare, 2006.
3. Description of Final ANGEL Demonstrator w ANGEL Project Report; Deliverable D5.2, ANGEL Project, 2007.
4. Neves P. i in.: Simulation tools for wireless sensor networks in medicine: a comparative study, w in Proceedings of the First International Conference on Biomedical Electronics and Devices, IODEVICES 2008, Funchal, Madeira, Portugalia, 2008, s. 111÷114.
5. Song F., Zhao B.: Trust-based LEACH Protocol for Wireless Sensor Networks, w Second International Conference on Future Generation Communication and Networking, 2008, s. 202÷207.
6. Heinzelman W. R., Chandrakasan A., Balakrishnan H.: Energy-Efficient Communication Protocol for Wireless Microsensor Networks, w Proc. of the Hawaii International Conference on System Sciences, 2000.
7. Borucki B.: Ochrona poufności i bezpieczeństwa medycznych danych osobowych, ICM UW http://kardionet.icm.edu.pl/c/document_library/get_file?p_l_id=10415&folderId=12450&name=DLFE-602.pdf, 2008; odczytany 11.03.2012.
8. Ustawa o ochronie danych osobowych, Dz.U. 1997 Nr 133 poz. 883 z późniejszymi zmianami.
9. European Union Directive on Data Protection, Off. J. Eur. Commun., Vol. 31 (281), 1995.
10. Rozporządzenie ministra zdrowia z dnia 21 grudnia 2006 r. w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej oraz sposobu jej przetwarzania, Dz.U. 2006 Nr 247 poz. 1819.
11. Gołaszewski G., Górski J.: Context sensitive privacy management in a distributed environment, Lecture Notes in Computer Science, 2010, LNCS 6426, Springer, s. 639÷655.
12. Górski J., Turower A., Wardziński A.: Distributed Trust Management Model for Wireless Sensor Networks, na Sixth International Conference on Dependability and Computer Systems DepCoS-RELCOMEX, 2011.

13. Górski J., Turower A.: Two-tier distributed trust management model for wireless sensor networks, na Forum Innowacji Młodych Badaczy, 2011.
14. IEEE: Standard 802.15.4.

Wpłynęło do Redakcji 19 marca 2012 r.

Abstract

Wireless Sensor Networks are used in applications which require high dependability, like healthcare, environmental monitoring, defence and others. Deployed sensors are often left unattended which make them vulnerable to physical damage, shortage of energy supply or intentional attacks. Trust management helps to differentiate between trustworthy and untrustworthy sensors without excessive investment in sophisticated network diagnostic and protection mechanisms which can be too costly comparing to the limited computational and energy resources of the sensors. Distributed trust management models provide for uniform distribution of the responsibility for trust assessment and related decision making. The paper presents the model of distributed trust management in wireless sensor networks. It discusses its importance for the security of the network and presents a case study in which the method was used. The results of simulations assessing the effectiveness of the method are presented and the directions of further research are indicated.

Adresy

Janusz GÓRSKI: Politechnika Gdańska, Wydział Elektroniki, Telekomunikacji i Informatyki, ul. Narutowicza 11/12,80-233 Gdańsk, Polska, jango@eti.pg.gda.pl
Alan TUROWER: Politechnika Gdańska, Wydział Elektroniki, Telekomunikacji i Informatyki, ul. Narutowicza 11/12,80-233 Gdańsk, Polska, alan.turower@eti.pg.gda.pl