Marcin Waraksa
Jerzy Żurek
Akademia Morska w Gdyni

BEZPIECZEŃSTWO TRANSMISJI DANYCH W BEZPRZEWODOWYCH SIECIACH SENSOROWYCH

Bezprzewodowe sieci sensorowe – podobnie jak inne systemy teleinformatyczne – stają się atrakcyjnym celem dla osób i instytucji zajmujących się pozyskiwaniem danych i/lub uzyskiwania dostępu do danych/infrastruktury sieciowej. Ataki na bezprzewodowe sieci sensorowe można podzielić na dwie grupy: ataki pasywne i aktywne. W artykule przedstawiono obydwie grupy ataków wraz przykładami. Ponadto opisano metody oraz techniki przeciwdziałania atakom na bezprzewodowe sieci sensorowe.

1. ZAGROŻENIA BEZPIECZEŃSTWA W BEZPRZEWODOWYCH SIECIACH SENSOROWYCH

Ataki na bezpieczeństwo systemów teleinformatycznych (a takimi bez wątpienia są bezprzewodowe sieci sensorowe – WSN) można podzielić na dwie zasadnicze grupy: **ataki pasywne** oraz **ataki aktywne**. Atakami pasywnymi określa się wszelkie próby nieautoryzowanego dostępu do danych bądź do infrastruktury systemu telekomunikacyjnego (ICT), w których adwersarz nie korzysta z emisji sygnałów mogących zakłócić lub wręcz uniemożliwić poprawną pracę danego systemu teleinformatycznego. Z kolei atakami aktywnymi są wszelkie próby nieautoryzowanego dostępu danych bądź do infrastruktury systemu telekomunikacyjnego przy użyciu przez atakującego emisji jakichkolwiek sygnałów lub działań, które mogą zostać wykryte.

Oprócz ataków na bezpieczeństwo infrastruktury ICT ważnym aspektem bezpieczeństwa tych systemów jest sama groźba naruszenia systemu bezpieczeństwa danego systemu teleinformatycznego. Nieświadomi zagrożenia użytkownicy często narażają poszczególne węzły systemu na ryzyko nieautoryzowanej modyfikacji, zniszczenia lub przechwycenia danych wrażliwych lub na nieautoryzowany dostęp do danych lub infrastruktury intruzom.

2. ATAKI PASYWNE

Przeprowadzając atak pasywny na bezprzewodową sieć sensorową, atakujący kamufluje swoją obecność oraz usiłuje uzyskać dostęp do danych transmitowanych w WSN poprzez bierny nasłuch takiej sieci. Należy tu także wziąć pod uwagę fakt, że poza transmisją radiową w WSN można zastosować inne bezprzewodowe metody transmisji danych (np. optoelektroniczne, podczerwień). Z oczywistych względów takie media są stosunkowo rzadko wykorzystywane, a ze względu na swoje charakterystyki kierunkowe trudno jest atakującemu w sposób niezauważony podsłuchać transmisję danych.

Ataki pasywne można podzielić na dwie grupy [1]:

- podsłuch transmisji danych,
- analiza ruchu wewnątrz danej sieci.

2.1. Podsłuch transmisji danych w WSN

Jedną z metod ataku pasywnego na WSN stanowi podsłuch danych transmitowanych pomiędzy węzłami takiej sieci. Ze względu na cechy charakterystyczne medium radiowego WSN, w których transmisja danych odbywa się w sposób jawny, jest stosunkowo podatna na taki rodzaj ataku pasywnego. Aby zminimalizować ryzyko wystąpienia takiego zdarzenia, transceivery stosowane w węzłach WSN dysponują nadajnikami małej mocy – przez co minimalizowany jest zasięg łączności do określonego obszaru, równocześnie – co ma znaczenie dla długotrwałości pracy takiego węzła – minimalizowana jest konsumpcja energii elektrycznej przez węzeł. W takim wypadku atakujący musi znaleźć się stosunkowo blisko węzła/węzłów WSN, aby umożliwić sobie skuteczny podsłuch transmisji w paśmie radiowym.

W celu zabezpieczenia się przed takim zdarzeniem należy stosować mechanizmy kryptograficzne w WSN, a tam, gdzie nie jest to wymagane lub możliwe – wprowadzać nadzór nad personelem poruszającym się w okolicy działania WSN oraz starać się monitorować emisję radiową z danego obszaru (dotyczy to głównie obiektów zamkniętych).

2.2. Analiza ruchu w WSN

Inną pasywną metodą ataku na WSN stanowi analiza ruchu wewnątrz sieci. W tym przypadku intencją atakującego nie jest poznanie zawartości transmitowanych wewnątrz WSN pakietów danych (jak przy podsłuchu transmisji w WSN), lecz uzyskanie wiedzy o topologii bezprzewodowej sieci sensorowej. Ze względu na charakter WSN część węzłów jest w znaczny sposób obciążona transmisją informacji (np. węzły znajdujące się sąsiedztwie styku WSN ze stacją bazową (*sink node*) agregującą dane z sieci sensorowej i transmitującą je dalej (np. do serwerów bazodanowych w celu dalszej obróbki danych) poprzez klasyczne sieci kompute-

rowe. Zwiększone obciążenie transmisją danych tych węzłów wiąże się również z retransmisją informacji przesłanych od sąsiadujących węzłów WSN do stacji bazowej. Innymi węzłami o stosunkowo dużym obciążeniu interfejsu komunikacyjnego są węzły nadzorujące klastry WSN (klastry tworzone są w celu zwiększenia skalowalności WSN). Wówczas węzeł zbiera dane pochodzące tylko z danego klastra i retransmituje je do wyższych warstw systemu.

W związku z powyższym zebranie informacji na podstawie analizy ruchu w WSN daje intruzowi wiedzę o krytycznych węzłach sieci sensorowej pod względem zapewnienia poprawnej pracy sieci.

Najczęściej do analizy ruchu w WSN stosuje się następujące techniki [1]:

- analiza ruchu w warstwie fizycznej – stosujący tę technikę ataku pasywnego nasłuchuje tylko sygnału nośnego, a natężenie ruchu jest określane dla pojedynczego węzła;
- analiza ruchu w warstwie łącza danych (i w wyższych) – analiza informacji przekazywanych w warstwie łącza danych (oraz w wyższych warstwach) umożliwi atakującemu poznanie topologii danej sieci WSN oraz używanych algorytmów trasowania (*routingu*);
- analiza ruchu poprzez korelację zdarzeń – opierając się na korelacji informacji o detekcji zdarzeń lub transmisji danych wewnątrz WSN, atakujący jest w stanie zdobyć dokładne informacje o routingu zastosowanym w WSN oraz o węzłach routujących;
- aktywna analiza ruchu w WSN – pomimo że analiza ruchu jest pasywnym atakiem na WSN, ta technika ataku może być również potraktowana jako jedna z aktywnych metod; wiąże się ona z fizycznym zniszczeniem określonych węzłów w WSN, a przez to z wymuszeniem aktywacji mechanizmów samoorganizacji WSN. W ten sposób atakujący może pozyskać wartościowe informacje odnośnie do tworzenia topologii sieci i jej zarządzania.

3. ATAKI AKTYWNE

W przeciwieństwie do przedstawionych powyżej pasywnych metod ataku na WSN, korzystając z aktywnych form ataku, intruz wpływa pośrednio lub bezpośrednio na zawartość informacji przesyłanych przez WSN i/lub na możliwości operacyjne sieci sensorowych. Ataki tego rodzaju są łatwiejsze do wykrycia – w porównaniu do ataków pasywnych, ponieważ mają bezpośredni wpływ na jakość pracy sieci sensorowej. Efektem ataku aktywnego może być np. degradacja usług w WSN lub w skrajnych przypadkach – brak dostępu do niektórych usług lub wręcz całkowita utrata kontroli nad WSN, lub jej zniszczenie.

Ataki aktywne można podzielić na kilka grup [1, 5]:

- ataki fizyczne – zniszczenie węzła, manipulowanie węzłem, EMP – *Electromagnetic Pulse*);
- ataki na integralność, poufność lub prywatność danych (w tym nieautoryzowany dostęp do danych);

- ataki na usługi (*Denial-of-Service* – DoS) – ataki zorientowane na poszczególne warstwy sieci modelu ISO/OSI, począwszy od warstwy fizycznej do warstwy aplikacji włącznie).

3.1. Ataki fizyczne

Zniszczenie węzła

Bezpośrednie ataki na infrastrukturę sprzętową WSN są groźne w przypadku sieci i/lub systemów taktycznych, związanych z pozyskiwaniem informacji o zdarzeniach na polu walki. Tego rodzaju ataki służą zmniejszeniu obszaru monitorowanego przez daną sieć sensorową lub całkowitemu unieszkodliwieniu danej WSN.

Manipulowanie węzłem

Manipulowanie węzłami sieci WSN ma za zadanie odwrócenie uwagi operatora danej sieci sensorowej od głównego ataku, jakimi mogą być ataki typu maskowanie (*spoofing*) lub DoS.

EMP

Ataki za pomocą wysokoenergetycznego krótkotrwałego impulsu elektromagnetycznego na infrastrukturę WSN mają na celu unicestwienie – w wąskim sensie znaczenia tego słowa: danej sieci sensorowej, a w szerokim znaczeniu: wszystkich urządzeń elektronicznych znajdujących się w polu rażenia EMP.

3.2. Ataki na integralność, poufność lub prywatność danych

Bezprzewodowe sieci sensorowe są bardzo podatne na tego typu ataki – związane jest to bezpośrednio z samą ideą WSN, czyli z mobilnością poszczególnych węzłów, brakiem stałego przyporządkowania do pozycji geograficznej, samoorganizacją sieci. Istnieje stosunkowo duża liczba możliwych scenariuszy przeprowadzenia tego typu ataku. Atakujący może uzyskać dostęp do konkretnego węzła sieci lub zainstalować swój węzeł, który będzie z jednej strony punktem dostępowym do WSN dla atakującego, a od strony operatora WSN będzie postrzegany jako „legalny" węzeł sieci. Po uzyskaniu dostępu do WSN atakujący może przykładowo rozgłaszać błędną pozycję danego węzła, podszywać się pod „autoryzowane" węzły, przechwytywać, a następnie modyfikować i odsyłać zmodyfikowane informacje w WSN.

Ataki ukierunkowane na integralność lub poufność danych są szczególnie niebezpieczne, gdyż umożliwiają atakującemu nieautoryzowany dostęp do WSN i do danych przez niego transmitowanych. Specjalną formą ataku maskującego jest atak Sybilla (*Sybil Attack*), polegający na podszywaniu się poprzez rozgłaszanie

przez złośliwy węzeł wielu identyfikatorów lub na skompromitowaniu legalnego węzła sieci i przejęciu jego identyfikatora wraz z dostępem do infrastruktury WSN. Ten typ ataku często jest przeprowadzany przeciwko systemom korelacji i agregacji danych. Ataki Sybilla mogą być również skierowane przeciwko algorytmom routingu oraz algorytmom określającym lokalizację poszczególnych węzłów sieci. Warto jeszcze pamiętać, że związana z atakiem Sybilla liczba transmitowanych przez szkodliwy węzeł identyfikacji pomaga w ukryciu ataku.

3.3. Ataki na usługi – *Denial-of-Service* (DoS)

Ataki DoS w sieciach sensorowych polegają na doprowadzeniu do przeciążenia zaatakowanych węzłów WSN, a przez to uniemożliwieniu pozyskania danych z zaatakowanych węzłów lub uniemożliwieniu korzystania z usług oferowanych przez zaatakowaną sieć sensorową. Ataki DoS zorientowane są na wszystkie warstwy modelu sieci ISO/OSI.

Ataki DoS w warstwie fizycznej

Atakiem na usługi przeprowadzonym na pierwszą warstwę modelu ISO/OSI sieci sensorowych jest zakłócanie częstotliwości radiowych w paśmie wykorzystywanym przez daną sieć sensorową. Dobrze skonstruowany i przeprowadzony atak DoS wymierzony w warstwę fizyczną jest w stanie zablokować całą sieć sensorową – nawet w przypadku, gdy liczba zaatakowanych węzłów jest dużo mniejsza od ogólnej liczby węzłów [2]. Atakując węzły krytyczne dla działania sieci sensorowej, jak np. bramę (umożliwiającą transmisję danych do sieci komputerowych, węzłów agregacji lub przetwarzania danych), można zablokować transmisję informacji z sensorów do systemów ich przetwarzania.

Ataki DoS w warstwie łącza danych

Ataki DoS w warstwie łącza danych sprowadzają się do zalania węzła dużą ilością informacji, przez co drastycznie zwiększają prawdopodobieństwo kolizji pakietów lub zmuszają zaatakowany węzeł do nieprzerwanej retransmisji pakietów. Atakujący może w ten sposób doprowadzić do szybkiego wyczerpania zasobów energetycznych węzła. Inną techniką ataku DoS w warstwie łącza danych jest wykorzystanie ramek RTS/CTS (*Ready-to-Send/Clear-to-Send*). Po każdym wysłaniu RTS węzeł ją wysyłający oczekuje na CTS. Doprowadzenie do kolizji z ramką CTS spowoduje ponowienie wysłania ramki RTS – przez to atakowany węzeł nie będzie w stanie zestawić połączenia, kolejne próby doprowadzą do wyczerpania baterii w obydwu węzłach [6].

Bardziej wyrafinowane ataki DoS w warstwie łącza danych tworzy się na podstawie schematu adresowania w tej warstwie, np. powodując wyczerpanie się przestrzeni adresowej w danej sieci, co prowadzi do sytuacji, w której węzły WSN nie będą w stanie uzyskać dostępu do danej sieci sensorowej [1].

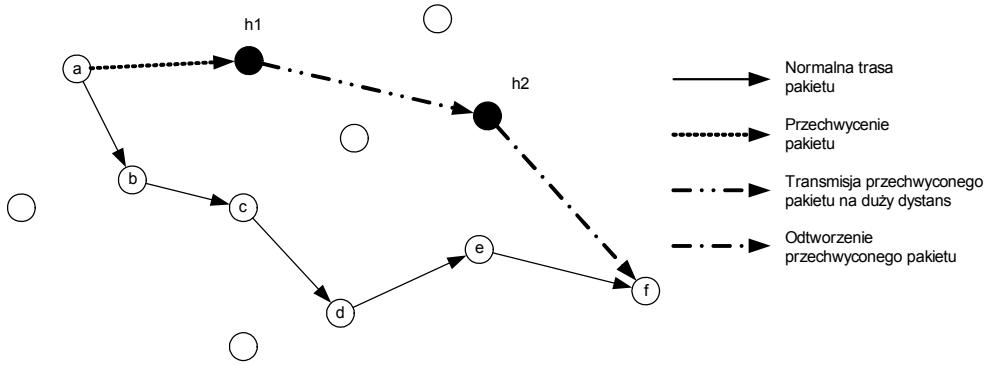
Ataki DoS na algorytmy routingu

Algorytmy routingu w sieciach sensorowych muszą sprostać wyzwaniom stawianym przez nowe techniki ataków DoS zorientowanych na te algorytmy. Ataki te można podzielić na dwie kategorie [4]:

- ataki zaburzające routing – ich celem jest wprowadzenie dysfunkcji w schemacie trasowania w obrębie danej WSN i uniemożliwienie tym samym świadczenia określonych usług przez zaatakowaną sieć;
- ataki absorbujące zasoby WSN – ich celem jest obciążenie zasobów sieciowych, takich jak pasmo częstotliwości, dostępna pamięć węzła, moc obliczeniowa czy też zmagazynowana w bateriach energia elektryczna.

Wśród tego rodzaju ataków na protokoły routingu w WSN najczęściej się spotyka [1, 2, 4, 6]:

- sfałszowane, zmienione lub odtworzone informacje o routingu – atakujący, poprzez modyfikację informacji o routingu ma wpływ na poprawność działania algorytmów trasowania w WSN;
- *HELLO flood attack* – szkodliwy węzeł dokonujący tego rodzaju ataku DoS rozsyła do wszystkich sąsiadujących węzłów informacje o routingu z dużą mocą, przez co każdy węzeł będący w zasięgu węzła szkodliwego traktuje go jako węzeł sąsiedzki; w efekcie tego wszystkie właściwe węzły WSN wysyłają pakiety danych do węzła szkodliwego;
- *Blackhole attack* – w tym przypadku atakujący przygotowuje węzeł szkodliwy, aby pełnił on rolę węzła pośredniczącego w trasowaniu danych w WSN, a następnie nieprzekazywaniu tych danych dalej (niszczeniu danych);
- *Sinkhole attack* – zmodyfikowany wariant *Blackhole attack*. W odróżnieniu od poprzedniej metody szkodliwy węzeł bierze udział w możliwie dużej liczbie tras w WSN, zbierając dane z właściwych węzłów i nie przekazując ich dalej.
- *Sybil attack* – szkodliwy węzeł poprzez rozgłaszanie informacji o wielu identyfikatorach i lokalizacjach geograficznych jednocześnie, wobec czego właściwe węzły WSN traktują taki szkodliwy węzeł jako węzeł sąsiedzki przekazujący dane dalej;
- *Wormhole attack* – w tym przypadku atakujący korzysta z dwóch węzłów będących pod jego kontrolą. Ten typ ataku polega na odebraniu wiadomości z węzła „a" przez „h1", przekazaniu go do odległego „h2" z wykorzystaniem kanału niedostępnego dla pozostałych węzłów w WSN, a następnie na przekazaniu przez „h2" odebranych od „h1" danych węzłowi docelowemu (właściwego dla danej WSN) (rys. 1). Wówczas pakiet po przejściu przez trasę a-b-c-d-e-f jest dyskryminowany w węźle docelowym, ponieważ przebył dłuższą trasę (mierzoną liczbą przeskoków pomiędzy węzłami pośredniczącymi). Ataki tego typu mają destrukcyjny wpływ na wiele usług sieciowych, takich jak synchronizacja czasowa, lokalizacja oraz fuzja danych. Ponadto ten typ ataku jest trudny do wykrycia.



Rys. 1. Atak typu *Wormhole*

Ataki w warstwie transportowej

Warstwa transportowa odpowiedzialna jest za zestawienie połączeń pomiędzy urządzeniami sieciowymi. W tej warstwie modelu ISO/OSI umiejscowione są m.in. doskonale znane protokoły TCP (*Transmission Control Protocol*) oraz UDP (*User Datagram Protocol*). Ze względu na znaczną liczbę możliwych ataków na protokoły warstwy transportowej, jak również na liczbę protokołów zastosowanych do tego celu w WSN poniżej przedstawiono przykładowe (najczęściej spotykane w środowisku sieci sensorowych) rodzaje ataków [1, 4]:

- fałszowanie potwierdzeń – fałszywe (*spoofed*) potwierdzenia protokołów transportowych doprowadzają do nadmiernej segmentacji emitowanych pakietów danych, co doprowadza do przeciążenia oraz degradacji pojemności sieci;
- powtarzanie potwierdzenia – w niektórych protokołach transportowych (np. TCP-Reno) wielokrotne potwierdzenie odebrania segmentu danych wskazuje na negatywne potwierdzenie; skutkuje to w węźle źródłowym koniecznością powtórnej transmisji poprzednio wysłanego segmentu danych;
- zakłócanie potwierdzenia – złośliwy węzeł może zakłócić segment pakietu danych zawierający wiadomość potwierdzenia (ACK), co może doprowadzić do zakończenia połączenia pomiędzy dwoma węzłami;
- zmiana numeru sekwencyjnego – w protokołach transportowych takich jak RMST (*Reliable Multi-Segment Transport*) lub PSFQ (*Pump Slowly, Fetch Quickly*) atakujący może zmienić numer sekwencji danego fragmentu danych, informując tym samym węzeł docelowy o braku części pofragmentowanych danych – co przekłada się na uniemożliwienie poprawnej defragmentacji pakietu w węźle docelowym;
- fałszowanie żądania nawiązania połączenia – atakujący poprzez wysyłanie dużej liczby żądań nawiązania połączenia z określonym węzłem doprowadza do znacznego obciążenia jego zasobów, uniemożliwiając tym samym nawiązanie połączenia z właściwymi węzłami sieci sensorowej. Tak zaatakowany węzeł sieci WSN nie będzie akceptować żądań zestawienia połączenia z innymi węzłami.

Ataki w warstwie aplikacji

Warstwa aplikacji jest równie podatna na ataki typu DoS – podobnie jak niższe warstwy modelu ISO/OSI. Ponadto protokoły odpowiadające za synchronizację czasu pomiędzy węzłami, protokoły lokalizacji przestrzennej poszczególnych węzłów, protokoły agregacji i fuzji danych również są narażone na różnego typu ataki mające na celu uniemożliwienie dostępu do usług zbudowanych na podstawie wymienionych protokołów. Przykładowym atakiem w warstwie aplikacji może być transmisja z mniejszą lub większą niż pożądana mocą wyjściową ze szkodliwego węzła – może to utrudniać poprawną lokalizację węzłów.

4. ZAPEWNIENIE BEZPIECZEŃSTWA TRANSMISJI DANYCH W BEZPRZEWODOWYCH SIECIACH SENSOROWYCH

Ponieważ liczba zagrożeń, na jakie narażone są bezprzewodowe sieci sensorowe, jest znaczna (powyżej przytoczono tylko najważniejsze, z punktu widzenia autorów), niezbędne jest stosowanie zaawansowanych metod i algorytmów ograniczających do minimum ryzyko powodzenia ataku na węzeł/sieć WSN. Do najważniejszych metod zwiększających bezpieczeństwo transmisji w WSN należy zaliczyć:

- techniki rozpraszania widma – utrudniające skuteczne zakłócanie transmisji radiowej;
- metody kryptograficzne – zabezpieczające integralność i poufność przesyłanych danych;
- specjalną konstrukcję sprzętową węzłów utrudniającą dostęp do układów wewnętrznych (przechowujących na przykład klucze tajne, informacje o algorytmach kryptograficznych) lub też implementację mechanizmów kasujących wrażliwe dane w momencie otwarcia obudowy węzła;
- stosowanie dedykowanych, a przy tym bezpiecznych protokołów transmisji danych [2] – takich jak SNEP (*Security Network Encription Protocol*) lub wersja mikroprotokołu TESLA (*μTESLA – Timed, Efficient, Streaming, Loss-tolerant Authentication*).

4.1. Przeciwdziałanie atakom zewnętrznym oraz bezpieczeństwo warstwy łącza danych

Większości ataków pochodzących z zewnątrz bezprzewodowej sieci sensorowej na protokoły routingu można uniknąć poprzez stosowanie prostych mechanizmów szyfrowania w warstwie łącza danych z wykorzystaniem globalnie współdzielonego klucza szyfrującego. Mechanizmy te zapobiegną również zewnętrznym atakom typu *Sybil* – ponieważ poszczególne węzły sieci sensorowej będą w stanie odrzucić identyfikatory wysyłane przez nieuprawniony węzeł spoza danej sieci sensorowej – co zablokuje dostęp takiemu węzłowi do infrastruktury sieciowej.

Metoda ta jest nieefektywna w razie ataku z wewnątrz WSN lub z wykorzystaniem skompromitowanych węzłów bezprzewodowej sieci sensorowej. Wewnętrzny intruz jest wstanie fałszować lub wstrzykiwać nieprawdziwe informacje o routingu, atakować z wykorzystaniem metody *sinkhole*, selektywnie retransmitować wybrane pakiety danych czy też rozgłaszać pakiety, korzystając z mechanizmów *HELLO flood* lub *Sybil*. W celu zapobieżenia takim atakom niezbędne są znacznie bardziej zaawansowane metody obrony.

4.2. Metody zabezpieczenia przed wewnętrznym atakiem *Denial-of-Service*

Przeciwdziałanie atakom Sybil

Jedną z metod zapobiegania atakom *Sybil* pochodzącym z wnętrza bezprzewodowej sieci sensorowej jest współdzielenie przez każdy węzeł z zaufaną stacją bazową unikatowego klucza symetrycznego. Obydwa węzły mogą wówczas (np. z wykorzystaniem protokołów typu Needham-Schroeder [4]) zweryfikować swoją tożsamość oraz stworzyć klucz współdzielony. Następnie para takich węzłów może – z wykorzystaniem klucza współdzielonego – nawiązać szyfrowane połączenie pomiędzy sobą. W celu zapobieżenia wewnętrznemu intruzowi stworzenia kluczy współdzielonych z poszczególnymi węzłami w stacjach bazowych ogranicza się liczbę sąsiadujących węzłów, z którymi dana stacja może nawiązać połączenie. W sytuacji przekroczenia przez stację bazową tej liczby zostanie zgłoszony przez nią komunikat błędu nawiązania połączenia. W przypadku węzłów skompromitowanych łączność ze stacją bazową jest ograniczona tylko do zweryfikowanej grupy sąsiadujących węzłów. Skompromitowane węzły nadal mogą nawiązywać połączenia ze stacją bazową lub oddalonymi (o określoną liczbę przeskoków) punktami agregacji danych, jednak nie będą w stanie dokonać tego z wykorzystaniem innych niż zweryfikowanych wcześniej węzłów WSN. Ponadto adwersarz – pomimo pomyślnego zestawienia robaczej dziury (*wormhole*) nie będzie w stanie podsłuchiwać lub modyfikować komunikacji pomiędzy nimi.

Przeciwdziałanie atakom HELLO floods

Jedną z metod przeciwdziałania atakom *HELLO floods* jest weryfikacja tożsamości każdego węzła z zaufaną stacją bazową (poprzez wykorzystanie metody opisanej powyżej). Ponieważ jest to weryfikacja dwukierunkowa połączenia ataki *HELLO floods* zostaną powstrzymane (nawet w przypadku użycia przez intruza węzłów z czułymi odbiornikami i o stosunkowo dużej mocy nadawczej). Niestety, mechanizm ten nie sprawdza się w przypadku korzystania przez intruza ze skompromitowanych węzłów w sieci. Ze względu jednak na wspomnianą wcześniej dwukierunkowość weryfikacji skompromitowany węzeł przy próbie dokonania autoryzacji swojej tożsamości z dużą liczbą węzłów WSN wygeneruje alarm w systemie.

Przeciwdziałanie atakom Wormhole oraz Sinkhole

Obecnie nie ma możliwości zabezpieczenia bezprzewodowych sieci sensorowych przeciwko atakom typu *Wormhole* oraz *Sinkhole*, m.in. przez to, że są bardzo trudne do wykrycia i zlokalizowania. W pracy [3] przedstawiono technikę detekcji ataków typu *Wormhole*, która wymaga jednak bardzo dokładnej synchronizacji czasowej, co nie jest obecnie osiągalne dla większości aplikacji sieci sensorowych. Jedynym rozwiązaniem tego problemu wydaje się być precyzyjne projektowanie protokołów routingu – tak aby unikać zjawiska wyścigu warunków trasowania [4].

PODSUMOWANIE

Bezprzewodowe sieci sensorowe – podobnie jak inne sieci teleinformatyczne – narażone są na znaczną liczbę zagrożeń pochodzących zarówno z zewnątrz, jak i z wewnątrz WSN. Bezprzewodowe sieci sensorowe wymagają zapewnienia integralności oraz poufności, a także ochrony węzłów i danych przesyłanych z ich wykorzystaniem. Ma to szczególne znaczenie przy ciągle rosnącej liczbie aplikacji (ze szczególnym naciskiem na aplikacje militarne, bezpieczeństwa publicznego lub medyczne). Przy opracowywaniu mechanizmów, algorytmów lub protokołów zwiększających bezpieczeństwo transmisji informacji w WSN należy także brać pod uwagę ograniczenia narzucone przez unikatowe cechy charakterystyczne dla WSN, takie jak somoorganizacja, dyslokacja, ograniczenia sprzętowe, łatwość kompromitacji węzłów i protokołów. W związku ze zwiększającą się bez przerwy liczbą aplikacji WSN z jednej strony, a rosnącą liczbą zagrożeń i ataków z drugiej zagadnienia związane z bezpieczeństwem transmisji danych w bezprzewodowych sieciach sensorowych są przedmiotem badań w liczących się ośrodkach naukowo-badawczych na całym świecie. Wraz z ewolucją WSN niezbędna jest także ewolucja mechanizmów ich zabezpieczenia przed niepożądanymi działaniami.

LITERATURA

1. Cayirci E., Rong C., *Security in Wireless Ad Hoc and Sensor Networks*, John Wiley & Sons, Ltd., 2009.
2. Dargie W., Poellabauer C., *Fundamentals of Wireless Sensor Networks*, John Wiley & Sons, Ltd., 2010.
3. Hu Y.-C., Perrig A., Johnson D.B., *Packet leashes: a defense against wormhole attacks in wireless networks,* IEEE Infocom, 2003.
4. Karlof C., Wagner D., *Secure Routing in Wireless Sensor Networks, Attacks and Countermeasures,* Ad Hoc and Sensor Networks, 2003, 1, s. 293–315.
5. Sarma H.K.D., Kar A., *Security Threats in Wireless Sensor Networks,* Elsevier, October 2006.
6. Wood A.D., Stnakovic J.A., *Denial of Service in Sensor Networks,* IEEE Computer, October 2002, 35(10), s. 54–62.

INFORMATION SECURITY IN WIRELESS SENSOR NETWORKS

Summary

Wireless sensor networks – as well as other IT systems – are became an attractive target for individuals and institutions involved in the illegal data acquisition and/or obtaining an access to the network infrastructure. The attacks on wireless sensor networks, in general, may be divided into two groups: passive and active attacks. In this article the authors present both types of the attacks – including their examples. Furthermore, the authors also describe methods and techniques how to prevent attacks on the wireless sensor networks.