KRZYSZTOF CABAJ[1,3], WOJCIECH MAZURCZYK[2,3], KRZYSZTOF SZCZYPIORSKI[2,3]

[1] Instytut Informatyki, Politechnika Warszawska, email: *kcabaj@elka.pw.edu.pl*
[2] Instytut Telekomunikacji, Politechnika Warszawska, email: *{wm, ksz}@tele.pw.edu.pl*
[3] SecGroup.PL - Network Security Group, Politechnika Warszawska

Bezpieczeństwo bezprzewodowych sieci WiMAX

Streszczenie

W artykule przedstawiono mechanizmy zapewniające bezpieczeństwo w sieciach WiMAX. Omówiono zmiany dotyczące mechanizmów zabezpieczeń w kolejnych standardach rodziny 802.16, które miały na celu poprawienie wykrytych podatności. Przeanalizowano również potencjale luki, które mogą być wykorzystane w celu zaatakowania sieci WiMAX. W pierwszej części omówiono architekturę sieci WiMAX, oraz najważniejsze pojęcia używane w dalszej części pracy (takie jak: asocjacja bezpieczeństwa, połączenie zarządzalne). Szczególny nacisk położono również na zaprezentowanie różnego typu połączeń występujących pomiędzy stacją bazową a terminalem abonenckim. W dalszej części artykułu opisano wszystkie etapy niezbędne do realizacji bezpiecznej wymiany danych dla stacji abonenckiej działającej w sieci WiMAX. Szczegółowo scharakteryzowano przebieg procesu uwierzytelniania z wykorzystaniem certyfikatów cyfrowych, sposób generowania i wymiany kluczy oraz ich późniejsze wykorzystanie do zapewnienia usług ochrony informacji. Przedstawiono również opis specjalistycznej infrastruktury klucza publicznego (PKI), którą będą musieli stworzyć producenci sprzętu i operatorzy sieci WiMAX.

1. Wprowadzenie do sieci WiMAX

Celem niniejszego rozdziału jest krótka charakterystyka sieci WiMAX (*World Interoperability for Microwave Access*) - IEEE 802.16 [4 ,5], porównanie ich z sieciami WiFi (IEEE 802.11) [1, 2], oraz możliwe przyszłe kierunki rozwoju sieci opartych na standardzie 802.16.

Popularność sieci WiFi pokazała jak wygodnym rozwiązaniem jest nieskrępowany kablami dostęp do sieci teleinformatycznych. Najlepiej o popularności tego typu sieci świadczą wbudowane fabrycznie w laptopy karty WiFi i pojawiające się w wielu miejscach darmowe punkty dostępowe (HotSpot'y). Największym problemem w pierwszym okresie wdrażania sieci WiFi stała się ochrona transmisji danych, która spowodowała, że przez długi okres sieci WiFi nie były uważane za bezpieczne. Dopiero wprowadzenie standardu 802.11i [3] pozwala na budowanie sieci WLAN gwarantujących bezpieczeństwo przesyłanych danych. Drugim, do tej pory nie rozwiązanym zagadnieniem, jest stosunkowo mały zasięg sieci WiFi. Jednak zmiany w tym aspekcie najpewniej nie zostaną wprowadzone, a panaceum jest wykorzystanie innych standardów sieciowych np. WiMAX. W sieciach WiMAX będzie możliwe uzyskanie zasięgu dochodzącego nawet do kilkunastu kilometrów. Pierwszym i jak na razie głównym zastosowaniem tych sieci jest tzw. ostatnia mila, czyli odcinek pomiędzy siedzibą abonenta a najbliższym urządzeniem komutującym należącym do operatora. Stąd też sieci WiMAX znajdują idealne zastosowane w terenie słabo zurbanizowanym, tym bardziej, że możliwa jest praca sieci w trybie NLOS (*Non Line Of Sight*), czyli kiedy odbiornik nie musi bezpośrednio „widzieć" anteny. Podstawową zaletą tego trybu jest prostota instalacji, nie wymagająca skomplikowanego podłączenia anteny urządzenia abonenckiego w sposób wymagający widoczności stacji bazowej. Jednak sieci WiMAX oferują nie tylko tryb stacjonarny (dokładniej nomadyczny), w nowszych wersjach standardu zapewniona jest pełna mobilność użytkowników, poprzez wprowadzenie znanego z sieci komórkowych mechanizmu *handover*. Mechanizm ten umożliwia przezroczyste przenoszenie całego stanu sesji komunikacyjnej do innej stacji bazowej, gwarantującej lepszą jakość sygnału. Wprowadzanie tego mechanizmu wraz z zapewnieniem większej przepustowości, w porównaniu z sieciami komórkowymi, może spowodować uruchomienie za pomocą tej technologii dostępu do usług takich jak: cyfrowe radio i telewizja czy usług typu wideo na żądanie (*Video on Demand, VoD*).

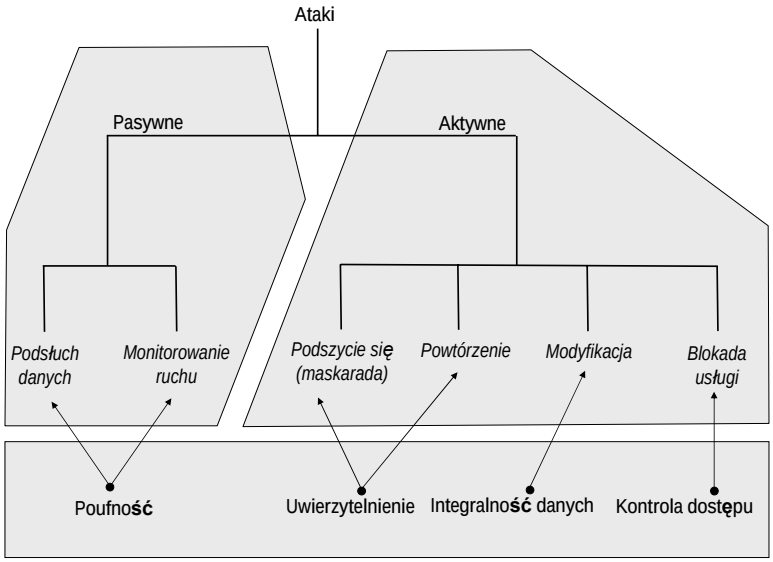
Co jest ważne i godne podkreślenia, aspekty związane z bezpieczeństwem zostały rozpatrywane i uwzględnione od samego początku powstawania standardu sieci WiMAX. Nie grozi zatem sytuacja z początków wdrażania standardu 802.11, gdy okazało się, że nie jest możliwe zbudowanie sieci gwarantujących wysokie bezpieczeństwo ich użytkownikom. Z tego powodu w stosie protokołów WiMAX została wprowadzona specjalna podwarstwa odpowiedzialna za zapewnienie bezpieczeństwa komunikującym się urządzeniem (*Security Sublayer*). W tej podwarstwie realizowane jest uwierzytelnienie komunikujących się stron oraz zapewnianie poufności i integralności przesyłanych danych. Więcej informacji na ten temat znajduje się w dalszej części artykułu tj. w punkcie 5.

2. Zagrożenia związane z sieciami radiowymi

Zagrożenia na jakie narażona jest sieć WiMAX są typowe dla sieci radiowych. Rozważana przez nas taksonomia ataków przyjmuje postać za [6] i wyróżnia następujące ataki:

- **pasywne** – nieautoryzowana działalność, w której atakujący nie modyfikuje zawartości ramek, a jedynie biernie nasłuchuje transmisji w kanale:
  - **podsłuch danych** – atakujący przechwytuje informacje wymieniane pomiędzy legalnymi użytkownikami,
  - **monitorowanie ruchu** – intruz śledzi transmisje pomiędzy legalnymi użytkownikami, w celu analizy cech stacji i ich aktywności,

- **aktywne** – nieautoryzowana działalność, w której atakujący czynnie bierze udział w transmisji w kanale:
  - **podszycie się** (maskarada) – atakujący udaje legalnego użytkownika lub usługę sieciową,
  - **powtórzenie** – włamywacz po przechwyceniu za pomocą podsłuchu informacji retransmituje ją tak jak legalny użytkownik,
  - **modyfikacja** – intruz kasuje, dodaje, zmienia wiadomość wysłaną przez legalnego użytkownika,
  - **blokada usługi** – atakujący destabilizuje pracę sieci, uniemożliwiając poprawną komunikację.



Rys. 1. Podział ataków na sieć WiMAX

Na Rysunku 1 taksonomia została przedstawiona w sposób graficzny. Pod rodzajami ataków zostały wymienione usługi ochrony informacji, które mogą zminimalizować lub przy prawidłowym wdrożeniu zredukować praktycznie do zera część z wymienionych zagrożeń.

Jak wspomniano, tworząc standard WiMAX starano się uniknąć błędów popełnionych przy opracowywaniu standardu 802.11. Wykorzystano silne algorytmy kryptograficzne do zapewnienia usług ochrony informacji. Do zapewnienia poufności danych zastosowano algorytmy symetryczne **DES** (*Data Encryption Standard*), **3DES** (*Triple DES*), **AES** (*Advanced Encryption Standard*) oraz asymetryczny **RSA** (*Rivest, Shamir, Adleman*). Z wyjątkiem algorytmu DES, który z powodu długości klucza dzisiaj jest już nie zalecany (lecz nadal jest o wiele silniejszy niż stosowany powszechnie w sieciach WiFi mechanizm **WEP** (*Wired Equivalent Privacy*) pozostałe algorytmy uważane są za bezpieczne. Do zapewnienie integralności danych zostały użyte natomiast mechanizmy rodziny MAC: **HMAC** (*Keyed-Hash Message Authentication Code*) lub **CMAC** (*Cipher-based Message Authentication Code*). Za zapewnienie autoryzacji oraz uwierzytelnienia odpowiedzialny jest protokół **PKM** (*Privacy Key Management*). Wykorzystuje on m.in. szyfrowanie asymetryczne i certyfikaty klucza publicznego wystawiane dla każdego urządzenia działającego w sieci WiMAX.

Oprócz wymienionych powyżej podstawowych usług ochrony informacji, nie można zapomnieć o zarządzaniu kluczami. Brak tych mechanizmów w sieciach WiFi spowodował, że w początkowym okresie ich rozwoju, szyfrowanie danych było często wyłączane z powodu braku protokołów dystrybucji kluczy. W WiMAX

wymiana kluczy jest nierozerwalnie związana z procesem logowania do sieci i uwierzytelnianiem stacji. Usługa zarządzania kluczami w sieciach WiMAX wspierana jest również przez, wspomniany powyżej, protokół PKM.

3. Architektura bezpieczeństwa sieci WiMAX

Sieci WiMAX mogą działać w dwóch trybach – tryb punkt-wielopunkt oraz tryb kraty. Pierwszy z wymienionych trybów w dzisiejszych zastosowaniach wydaje się najpraktyczniejszy. Punktem centralnym jest stacja bazowa, za pomocą której komunikują się wszystkie pozostałe urządzenia w sieci WiMAX. Jest to także miejsce styku z innymi sieciami podłączonymi za pomocą kabla. Mamy tutaj sytuację podobną do sieci WiFi działającej z punktem dostępowym (*Access Point, AP*). Tryb kraty wydaje się być interesującym rozwiązaniem w sytuacji kiedy pewne stacje bazowe nie mają bezpośredniej łączności z częścią przewodową sieci. W takim wypadku zamiast łącza przewodowego do sieci zewnętrznej wykorzystywane jest połączenia radiowe do innej stacji bazowej. Tryb kraty, gdzie każde urządzenie abonenckie mogłoby komunikować się z każdym wydaje się rozwiązaniem niepraktycznym. Tym bardziej, że urządzenia abonenckie mają ograniczoną moc nadajnika. Z tego powodu tryb kraty nie będzie w dalszej części artykułu omawiany.

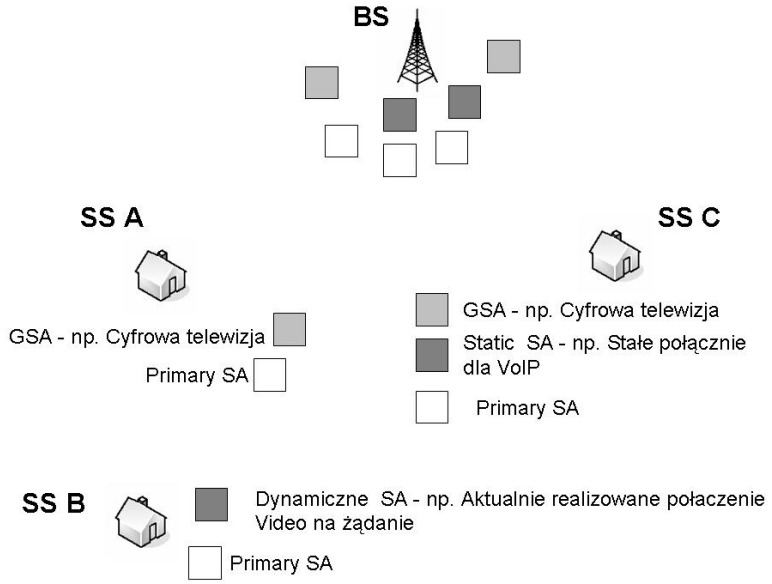
Wszystkie urządzenia abonenckie (*Subscriber Station, SS*) komunikują się ze stacją bazowa (*Base Station, BS*). Stacja bazowa odpowiedzialna jest za zarządzanie pasmem i zezwala na transmisję poszczególnych urządzeń. Każde urządzenie w sieci WiMAX posiada adres MAC, za pomocą którego jest identyfikowane. W aktualnych standardach możliwe jest przesyłanie za pomocą sieci WiMAX danych za wykorzystując protokoły ATM, 802.3 (ramki ethernetowe), 802.1q (ramki ethernetowe różnych VLAN'ów) oraz pakiety IPv4 i IPv6. Co ciekawsze możliwe jest stworzenie wielu niezależnych strumieni danych dla każdego urządzenie działającego w sieci. Każde takie połączenie posiada wynegocjowane oddzielnie parametry bezpieczeństwa. Wszystkie informacje na temat parametrów bezpieczeństwa przechowywane są w strukturze danych zwanej asocjacją bezpieczeństwa (*Security Association, SA*). W niej przechowywane są wszystkie dane pozwalające na zaszyfrowanie, odszyfrowanie czy sprawdzenie integralności przesyłanych danych. Tutaj znajdują się informacje o wynegocjowanych i aktualnie używanych algorytmach kryptograficznych, aktualnie używane klucze, ich czasy obowiązywania oraz wszelkie inne informacje potrzebne do normalnej pracy algorytmów kryptograficznych. Dla ustalonego zestawu algorytmów utrzymywane są dwa komplety informacji odpowiadające dwóm możliwym do wykorzystania kluczom – starszemu i nowszemu. Takie podejście pozwala na przechodzenie z jednego klucza, którego czas obowiązywania się zakończył, do następnego bez zaistnienia sytuacji kiedy klucz z powodu cyklicznej zmiany jest nieaktualny. Dla każdego połączenia muszą istnieć odpowiadające sobie asocjacje bezpieczeństwa w SS i BS rozróżniane przez identyfikator **SAID** (*Security Association ID*).

Mając na uwadze przyszłe zastosowania sieci WiMAX wprowadzono kilka rodzajów połączeń i odpowiadających im asocjacji bezpieczeństwa. Każda SS posiada co najmniej jedną podstawową asocjację bezpieczeństwa (*Primary SA*) odpowiedzialną za obsługę połączenia służącego do zarządzania komunikacją pomiędzy parą SS i BS. Te połączenie jest wykorzystywane jedynie przez te dwa urządzenia. Poza nim możliwe jest utworzenie dowolnej liczby tzw. statycznych asocjacji pomiędzy daną SS i BS. Za ich pomocą mogą być przesyłane inne dane, przykładowo ruch telefonii VoIP czy zwykłe dane komputerowe.

Oprócz opisanych powyżej statycznych asocjacji w standardzie 802.16 zostały wprowadzone jeszcze dwa rodzaje asocjacji – dynamiczne i grupowe. Asocjacje dynamiczne tworzone są na specjalne życzenie stacji klienckiej przy pomocy komunikatów DSA-XXX. Wysłanie tych komunikatów, czyli podjęcie decyzji o nawiązaniu nowego połączenia jest sterowane przez oprogramowanie warstw wyższych. Przykładowo nowe połączenie może być nawiązane w celu uzyskania zamówionego materiału (Wideo na żądanie), czy skonfigurowania nowego kanału wirtualnego (*Virtual Chanel, VC*) lub ścieżki (*Virtual Path, VP*) w przypadku, gdy stacja abonencka działa jak urządzenie ATM (Asynchronous Transfer Mode).

Asocjacje grupowe (*Group Security Association, GSA*) służą do obsługi ruchu typu multicast lub broadcast w sieciach WiMAX. Połączenia te mogą być szczególnie efektywnie wykorzystane do realizacji transmisji cyfrowej telewizji, czy cyfrowego radia za pomocą sieci WiMAX. Jak sugeruje sama nazwa, transmisja tego typu jest odbierana przez wiele stacji. Żeby ułatwić proces zmiany kluczy w tym trybie transmisji, nowe klucze są przesyłane w komunikatach *Group Key Update*, do wszystkich zainteresowanych stacji.

Na rysunku 2 przedstawiony jest stan przykładowej sieci WiMAX składającej się z jednej BS i trzech stacji SS.

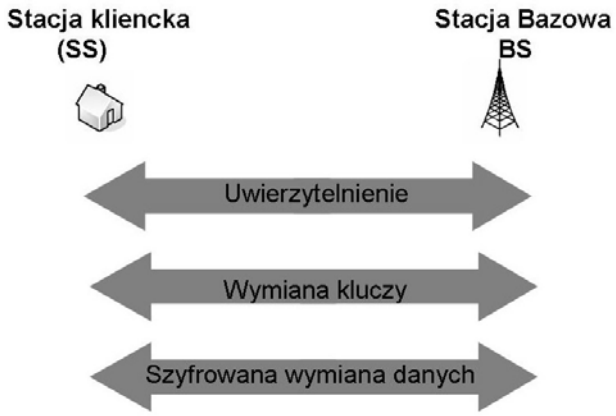


Rys. 2. Przykłady komunikacji w sieci WiMAX oraz odpowiadające im asocjacje bezpieczeństwa

Schematycznie za pomocą różnokolorowych kwadratów zaznaczone są asocjacje bezpieczeństwa wynegocjowane podczas procesu logowanie do sieci WiMAX. Wszystkie stacje posiadają po jednej głównej asocjacji bezpieczeństwa. Poza nią mają jeszcze inne połączenia służące do wymiany pozostałych danych. Przykładowo stacja B posiada dynamicznie wynegocjowane połączenie, przez które dostarczany jest do klienta zamówiony film. Stacja C posiada statyczną asocjację odpowiedzialną za obsługę połączeń VoIP. Jak wspomniano w niektórych przypadkach przydatna jest możliwość wykorzystania transmisji z jednego urządzenia do wielu. Przykładem idealnego zastosowania takiego rozwiązania jest np. transmisja telewizji cyfrowej. Ponieważ dane tego typu są identyczne dla wielu odbiorców opłacalnym wydaje się transmisja jednego strumienia danych odbieranego przez wielu odbiorców. Na rysunku 2 w ten sposób dostarcza jest telewizja cyfrowa dla stacji A i C. Co jest warte podkreślenia każde z przedstawionych połączeń ma oddzielnie wynegocjowane parametry bezpieczeństwa. Nie jest możliwe zatem, aby jakiekolwiek dane zostały odczytane przez nieuprawnione osoby.

4. Logowanie urządzenia w sieci

Ogólny przebieg procesu podłączenia się i uzyskiwania dostępu w sieciach WiMAX przedstawiono na rysunku 3.

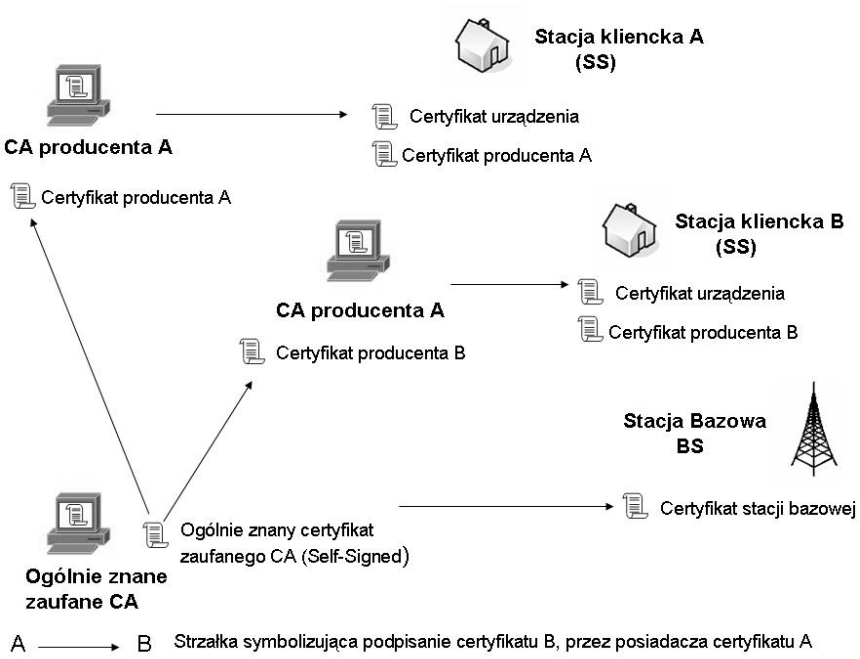


Rys. 3. Ogólny schemat wymiany informacji pomiędzy stacją kliencką a stacją bazową

4.1 Proces uwierzytelnienia

Każde urządzenie abonenckie musi przejść proces uwierzytelnienia w stacji bazowej, aby móc wymieniać informacje z innymi urządzeniami w sieci WiMAX lub uzyskać dostęp do innych urządzeń podłączonych do stacji bazowej łączem kablowym. Uwierzytelnienie realizowane jest za pomocą certyfikatów cyfrowych standardu X.509. Każde urządzenie abonenckie w sieci WiMAX zgodnie ze standardem powinno posiadać dwa

certyfikaty. Pierwszy jest certyfikatem producenta; w skład jego opisu powinny wchodzić: nazwa kraju oraz nazwa producenta. Certyfikat ten umożliwia sprawdzenie autentyczności certyfikatu urządzenia. Może on być podpisany przez samego producenta (*Self-signed Certificate*). Podpisanie go przez ogólnie znaną organizację, zajmującą się poświadczaniem certyfikatów, zwiększa bezpieczeństwo. W takim przypadku operator ma możliwość niezależnego sprawdzenia autentyczności certyfikatu producenta, wysyłanego do stacji bazowej podczas wstępnej fazy uwierzytelniania urządzenia w sieci. Drugim certyfikatem jest indywidualny certyfikat stacji abonenckiej. W jego skład powinna wchodzić: nazwa producenta urządzenia, kraj produkcji oraz numer seryjny i adres MAC stacji abonenckiej. Najbezpieczniejszym rozwiązaniem wydaje się generowanie obu certyfikatów w procesie produkcji urządzenia. Jednak standard przewiduje możliwość wygenerowania kluczy i certyfikatów samoczynnie przez urządzenie. W tej sytuacji klucze i certyfikat muszą być wygenerowane przed próbą włączenia się danego urządzenia do sieci. Na rysunku 4 zaprezentowano schemat pokazujący jakie certyfikaty biorą udział w procesie uwierzytelniania stacji SS.



Rys. 4. Infrastruktura Klucza Publicznego (PKI) w sieciach WiMAX

Wszystkie etapy uwierzytelnienia realizowane są przez protokół **PKM** (Privacy Key Management). W standardzie 802.16e-2005 [3] została zdefiniowana nowa wersja protokołu **PKMv2**. W wersji tej przewidziano możliwość uwierzytelniania stacji bazowych, co wiąże się z wygenerowaniem certyfikatów dla każdej stacji. Certyfikaty stacji bazowej powinny zawierać nazwę kraju, nazwę operatora oraz numer seryjny i unikalny w sieci operatora identyfikator stacji. Zmiana ta przy prawidłowym wdrożeniu bezpieczeństwa uniemożliwi podszycie się atakującego pod stację bazową i przeprowadzenie ataków przechwytywania przez podmiot pośredniczący (*Man In The Middle*). Oprócz tego wprowadzono możliwość skorzystania z umożliwia skorzystanie z serwera **AAA** (*Authentication Authorization Accounting*) za pomocą protokołów rodziny **EAP** (*Extensible Authentication Protocol*) [9].
Szczegółowy opis protokołów PKMv1 i PKMv2 zawarty został w [7].

4.2 Proces wymiany kluczy

Po pomyślnym uwierzytelnieniu, następuje faza odpowiedzialna za uzgodnienie używanych algorytmów kryptograficznych i wymianę kluczy, także realizowana przez protokół PKM. Bezpieczeństwo tej fazy opiera się na algorytmie RSA i kluczach publicznych zawartych we wcześniej wymienianych certyfikatach. Ze względów wydajnościowych w obu protokołach PKM są stworzone hierarchie kluczy i jedynie klucz główny jest wymieniany w ten sposób. Efektem tej fazy jest uzgodnienie pomiędzy stacją bazową a kliencka klucza **AK** (*Authorization Key*). Klucz ten (czy pre-AK w PKMv2), jak wspomniano, podczas transportu do stacji abonenckiej zaszyfrowany jest przy pomocy publicznego klucza algorytmu RSA. Wykorzystywany jest tutaj algorytm RSA zgodny ze specyfikacją PKCS #1 (Public-Key Cryptography Standards). Klucz jest 1024 bitowy a publicznie znany wykładnik przyjmuje wartość 65537 (0x010001). Klucz publiczny przekazywany jest do stacji bazowej w certyfikacie zgodnym z protokołem X.509.

Na podstawie wcześniej uzgodnionego klucza generowane są klucze **KEK** (*Key Encryption Key*), które służą do zabezpieczenia kluczy sesyjnych **TEK** (*Traffic Encryption Key*). Te ostatnie służą do bezpiecznej wymiany danych użytkowych. Aktualnie w sieciach WiMAX do szyfrowania kluczy TEK można wykorzystać jeden z czterech następujących algorytmów: 3DES w trybie EDE (Encryption Decryption Encryption) ze 128 bitowym kluczem, RSA z 1024 bitowym kluczem, AES w trybie ECB (Electronic Code Book) z 128 bitowym kluczem i dodany w standardzie 802.16e-2005 AES w trybie Key-Wrap ze 128 bitowym kluczem.

4.3 Proces szyfrowanej wymiany danych oraz zapewnienia integralności

Po zakończeniu fazy wymiany kluczy stacja abonencka powinna mieć stworzone lokalnie wszystkie statyczne asocjacje bezpieczeństwa. Od tego momentu możliwa jest już w pełni bezpieczna wymiana danych zabezpieczonych we wcześniej wynegocjowany sposób (wybrany algorytm szyfrowania). Uzgodnione klucze są ważne przez ustalony okres i po pewnym czasie są zmieniane. W celu nieprzerwanej pracy przez cały czas stacja bazowa utrzymuje po dwa komplety kluczy. Wszystkie dane użytkowe transmitowane w sieci mogą podlegać szyfrowaniu przy pomocy jednego z algorytmów: DES (w trybie CBC) lub AES (w trybach CCM, CBC lub CTC).

Zapewnienie integralności w sieci WiMAX może dotyczyć dwóch rodzajów transmisji – danych użytkownika sieci i informacji zarządzających. Dla pierwszego przypadku w momencie konfiguracji można zdecydować, że transmitowane ramki z danymi użytkowymi oprócz szyfrowania zostaną także uwierzytelnione. W tym celu używany jest algorytm AES w trybie CCM. W takim wypadku dane zostaną zaszyfrowana o także do ramki zostanie dodany 8 bajtowy ICV (Integrity Check Value). Natomiast integralność wiadomości zarządzających jest zapewniana za pomocą algorytmów HMAC [10] w połączeniu z funkcją skrótu SHA-1 lub algorytmu CMAC [8]. W takim wypadku wybrane ramki zarządzania będą miały na końcu dodane pole, które zawiera kod uwierzytelniający wiadomość policzony dla aktualnej zawartości i zabezpieczony wcześniej uzgodnionym kluczem. Do wyliczania kodu uwierzytelniającego wiadomość używane są klucze ustalone w trakcie uwierzytelniania za pomocą protokołu PKM

5. Potencjalne luki w zabezpieczeniach

Analiza stanu bezpieczeństwa sieci WiMAX wypada o wiele lepiej niż analiza stanu bezpieczeństwa sieci WiFi, nawet po kilku latach od ich upowszechnienia. Przy opracowywaniu standardu 802.16 nie popełniono błędów znanych z sieci WiFi. Główne różnice polegają na zastosowaniu odpowiednich algorytmów kryptograficznych (np. RSA, AES) oraz wprowadzeniu wszystkich mechanizmów w początkowej wersji standardu (protokół PKM do zarządzania kluczami, PKI do zarządzania certyfikatami itp.). Jest jednak parę aspektów związanych z bezpieczeństwem, które potencjalnie mogą wpłynąć na obniżenie poziom bezpieczeństwa sieci WiMAX. Największe wątpliwości budzą opcje umożliwiające wyłączenie z powodów wydajnościowych oraz z powodu potencjalnych problemów konfiguracyjnych wspieranych mechanizmów zabezpieczeń.

Dodatkowo w standardach 802.16 nie wspomniano o obowiązku skorzystania z certyfikatów producenta do sprawdzenia autentyczności przesyłanych certyfikatów urządzeń. Przesyłany certyfikat producenta urządzenia pełni rolę jedynie informacyjną. Nie wymuszono także tego by był on podpisany przez wiarygodną organizację zajmującą się dostarczaniem certyfikatów oraz aby sprawdzana była jego autentyczność. Braki te mogą prowadzić do pomniejszenia roli certyfikatów, co w efekcie może wpłynąć na zmniejszenie poziomu bezpieczeństwa całej sieci, a to w praktyce może zredukować do zera przydatność tego rozwiązania.

Musimy pamiętać, że producenci urządzeń muszą być uważani za zaufane trzecie strony, podobnie jak producenci kart SIM w telefonii GSM. To na producentach spoczywa obowiązek odpowiedniego zabezpieczenia informacji związanych z procesem wgrywania i ewentualnego przechowywania informacji na temat kluczy prywatnych. Zatem to oni będą musieli stworzyć na potrzeby produkowanych urządzeń własne centra certyfikacji (*Certification Authority, CA*).

Jak wspomniano. wszystkie dane użytkowe transmitowane w sieci mogą podlegać szyfrowaniu przy pomocy algorytmu DES (w trybie CBC) lub AES (w trybach CCM, CBC lub CTC). Dla danych o mniejszym stopniu ważności lub dla urządzeń nie posiadających zaimplementowanych funkcji kryptograficznych istnieje również możliwość wyboru braku szyfrowania przesyłanych danych. Pozostawienie takiej możliwości jest troską o najprostsze urządzenia, które nie byłyby w stanie wykonać skomplikowanych obliczeniowo operacji kryptograficznych. Jednak z punktu widzenia bezpieczeństwa danych takie podejście może prowadzić do sytuacji, jak w przytaczanym przykładzie początków wdrażania sieci WiFi, kiedy użytkownicy wyłączali zabezpieczenia nie chcąc utrudniać sobie pracy. Jedyną pociechą w tym wypadku jest fakt, że standard przewidział możliwość odmówienia uwierzytelnienia stacji, która nie obsługuje wymaganych w danej sieci standardów bezpieczeństwa.

Potencjalnym niebezpieczeństwem może być również rezygnacja z szyfrowania wiadomości zarządzających, poza tymi niosącymi klucze. Brak szyfrowania powoduje ujawnienie informacji, które to następnie mogą być wykorzystane do przeprowadzenia kolejnych ataków. Przykładowo: cenną informacją, z punktu widzenia atakującego, jest wybrany algorytm szyfrowania używany przez dane urządzenie, czy ilości aktywnych asocjacji bezpieczeństwa dla danej stacji.

Podobnym problemem może być brak możliwości sprawdzenia integralności danych użytkowych przy wyborze niektórych algorytmów szyfrowania. Pozwala to na przeprowadzeniu ataków odmowy usługi polegających na zalaniu stacji pakietami wygenerowanymi przez atakującego. Bez sprawdzenia integralności wszystkie takie pakiety będą poddawane rozszyfrowywaniu i interpretacji, co pochłonie zasoby atakowanego urządzenia.

6. Podsumowanie

Sieci WiMAX wydają się bardzo ciekawą alternatywą zapewniającą łączności o parametrach pośrednich między sieciami WiFi a sieciami 3G. Obecnie zastosowanie sieci budowanych w oparciu o technologię WiMAX powinno rozwiązać problem ostatniej mili, w szczególności na terenach słabo zurbanizowanych. Wprowadzenie rozwiązań takich jak możliwość szyfrowanej komunikacji typu *multicast*, czy mechanizm *handover* oraz jej dostępne pasmo umożliwią wykorzystanie w przyszłości tych sieci do dostarczania materiałów multimedialnych na urządzenia mobilne. Na szczególną uwagę zasługuję bardzo poważne i przemyślane podejście do bezpieczeństwa. Wydaje się, że sieci WiMAX pozwolą na budowanie w pełni bezpiecznych sieci radiowych. Na pewno nie grozi nam sytuacją z początków wdrażania sieci WiFi, kiedy okazało się że pierwsze standardy nie zapewniały oczekiwanego poziomu bezpieczeństwa, a kolejne rozwiązania były jedynie łatami, bądź dodatkami. W sieciach WiMAX funkcje zapewniające bezpieczne korzystanie z sieci są integralną częścią najważniejszych protokołów umożliwiających działanie sieci.

Literatura:

[1] IEEE 802.11b-1999 Supplement to 802.11-1999,Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band
[2] IEEE 802.11g-2003 Amendment 4: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band
[3] IEEE 802.11i-2004 Amendment 6: Medium Access Control (MAC) Security Enhancements
[4] IEEE 802.16a-2004 IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems
[5] IEEE 802.16e-2005 IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands.
[6] K. Szczypiorski (kier.), K. Cabaj, I. Margasiński - Analiza zagrożeń i ochrona danych w sieciach bezprzewodowych - Warszawa, listopad 2005, Instytut Telekomunikacji PW na zlecenie Instytutu Łączności w ramach Programu Wieloletniego - "Rozwój Telekomunikacji i Poczty w Dobie Społeczeństwa Informacyjnego"
[7] K. Cabaj, W. Mazurczyk, K. Szczypiorski, Zarządzanie kluczami w sieciach WiMAX, Materiały: XI Krajowa Konferencja Zastosowań Kryptografii Enigma'2007, 23-25 maja 2007, Warszawa
[8] M. Dworkin: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST Special Publication 800-38B, maj 2005
[9] B. Aboba, L. Blank, J. Vollbrecht, Extensible Authentication Protocol (EAP), Request for Comments: 3748, Czerwiec 2004
[10] H. Krawczyk, M. Bellare, R. Canetti, HMAC: Keyed-Hashing for Message Authentication, Request for Comments: 2104, Luty 1997