

Mobilne sieci przyszłości – architektura i bezpieczeństwo WiMAX i LTE

Ogromny rozwój szerokopasmowego bezprzewodowego dostępu do Internetu, którego jesteśmy świadkami coraz częściej wkracza w nasze codzienne życie. Każdy korzysta już z bezprzewodowego urządzenia mobilnego, które oferuje całą gamę mobilnych usług. Aby sprostać powstającym potrzebom na nowe usługi oraz szybkość transmisji danych niezbędne są nowoczesne techniki radiowe. Poniższy dokument przedstawia podstawy architektoniczne mobilnych sieci przyszłości: WiMAX oraz LTE. Obie sieci wyznaczają nowe standardy w szerokopasmowym dostępie bezprzewodowym, prezentują innowacyjne techniki zarządzania pasmem oraz modulacji czego wynikiem jest możliwość przesyłania informacji z prędkością nawet 1Gbps. W pracy zwrócono również uwagę na aspekt bezpieczeństwa realizowany w obu tych standardach, generowanie i wymianę kluczy kryptograficznych biorących udział w procesie uwierzytelnienia oraz bezpiecznej transmisji danych.

1. Wprowadzenie

Sieci bezprzewodowe coraz częściej są nieodzownym elementem naszego życia. Stają się wyznacznikiem nowych technologii, standaryzując nowe rozwiązania i możliwości technologiczne. Obecnie prawie 4 miliardy aktywnych subskrybentów korzysta z usług sieci komórkowych, pokrywając swym zasięgiem 85% globu. Sieci komórkowe ewaluowały wprowadzając coraz to nowe usługi i rozwiązania. Głównym wyznacznikiem rozwoju takich sieci, stała się prędkość przesyłanych danych. Pierwsza generacja sieci bezprzewodowych (1G) była ukierunkowana przede wszystkim na analogową transmisję głosową. Cyfrowe sieci drugiej generacji (2G) zwiększały przepustowość sieci oraz oferowały lepszą jakość transmisji głosu. Rozwinięcie kilku standardów pozwoliło również używać telefonów w roamingu zagranicznym. Sieci 2G upowszechniły się w dwóch standardach: GSM (ang. Global System for Mobile Communications) i CDMA (ang. Code Division Multiple Access). Oba standardy zostały stworzone przede wszystkim do transmisji głosowej. W późniejszych poprawkach systemy były rozszerzane o transmisję danych. W początkowych fazach transmisja ta była na poziomie połączeń *dial-up*. Kolejne kroki ewolucji telefonii komórkowej były skierowane na przejście do systemu 3G. Stworzono specjalne wytyczne takiego systemu (*peak* transmisji danych na poziomie 2Mb/s oraz pełna mobilność systemu). Jednak pierwsze standardy nie zapewniały założeń systemu co do transmisji danych. Rzeczywista prędkość przesyłanych danych była dużo niższa niż wcześniej zakładano. Dopiero projekt 3GPP2 dotyczący systemu HRPD (ang. High Rate Packet Data) [1] przedstawiał zaawansowane metody optymalizacji

kanału radiowego nastawione na zwiększenie prędkości transmisji (CDMS2000-1xEVDO (ang. Evolution Data Only)). Równolegle projekt 3GPP przedstawił standard HSPA (ang. High Speed Packet Access) [2] bazujący na WCDMA. Standard HSPA zawierał prawie identyczną listę poprawek w kanale radiowym co HRPD. Pozwalał na jednoczesną transmisję głosową i danych we wspólnym kanale transmisyjnym o szerokości 5 MHz. Oba te standardy stały się powszechne i są wykorzystywane w dostępie bezprzewodowym. Podczas dalszego rozwoju i wdrażania standardów HSPA i HRPD, komitet IEEE 802 LMSC (LAN/MAN Standard Committee) przedstawił standard IEEE 802.16e [3]. Standard ten był rozwinięciem obecnego już nomadycznego standardu 802.16. Standard 802.16e zakładał odmienną metodę modulacji OFDMA (ang. Orthogonal Frequency Division Multiple Access). Podział częstotliwości i dostęp przez wielu użytkowników jest realizowany przez przypisanie różnym użytkownikom różnych podkanałów. W porównaniu z sieciami HSPA i HRPD oferuje większą prędkość przysyłanych danych oraz wydajność spektralną. Pomimo iż standard IEEE 802.16 jest oficjalnie nazwany IEEE WirelessMAN, grupa WiMAX Forum zmieniła jego nazwę na WiMAX (ang. Worldwide Interoperability for Microwave Access). Jednocześnie z rozwojem sieci WiMAX jest rozwijany inny standard mobilnej sieci “przyszłości”. LTE (ang. Long-Term Evolution) jest przedstawiany jako następca standardu WCDMA/HSPA. W porównaniu z obecnymi technologiami radiowymi oferuje między innymi dużo wyższą prędkość przesyłanych danych, małe opóźnienia transmisji oraz większą ilość oferowanych usług.

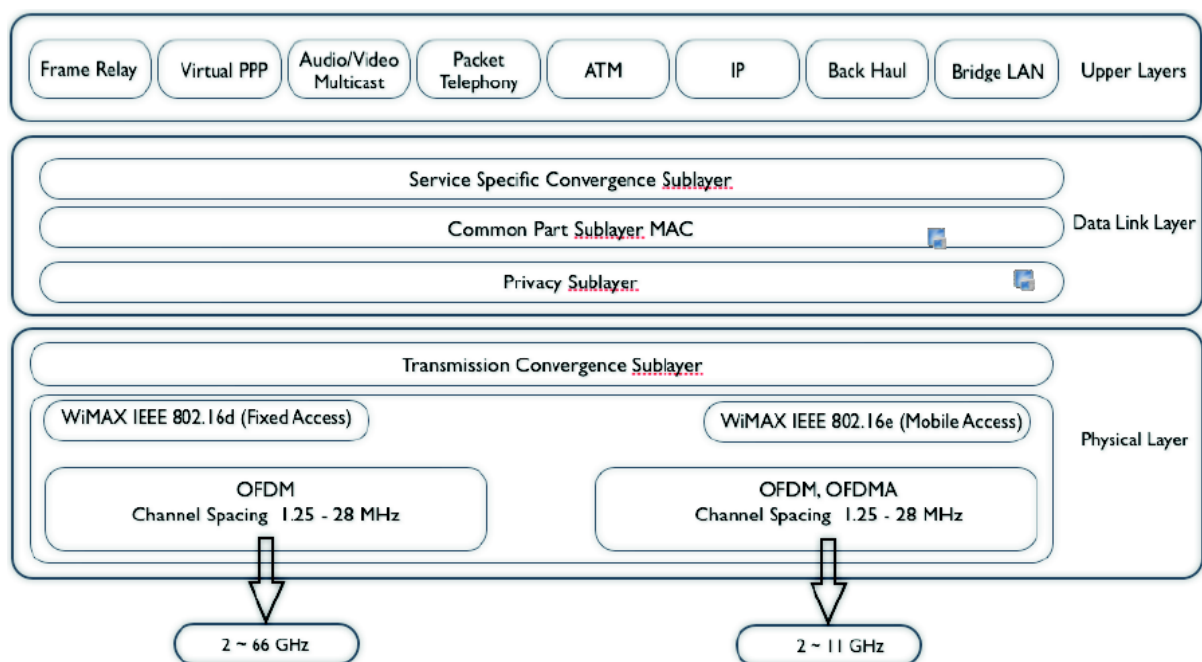
2. Standard IEEE 802.16

WiMAX jest radiową technologią bezprzewodową, której zasadę działania można odnieść i porównać do referencyjnego modelu IOS/OSI [Rys. 2.].

Wersje IEEE 802.16			
	802.16	802.16d	802.16e
Częstotliwość pracy	10-66 GHz	2-11 GHz	<6 GHz
Konfiguracja anten	LOS	LOS lub NLOS	NLOS
Przepływność	32 - 144 Mbit/s	do 100 Mbit/s	do 15 Mbit/s
Modulacja	QPSK, 16-QAM, 64-QAM	256 podnośnych OFDM	OFDMA
Mobilność	NIE	NIE	TAK, do 120 km/h
Szerokość kanału	20, 25, 28 MHz	od 1,25 do 28 MHz	5 MHz
Praktyczne zasięgi	1-5 km	5-10 km	1-5 km

Rys. 1. Specyfikacja standardu 802.16

Swym działaniem obejmuje dwie pierwsze warstwy modelu ISO: warstwę fizyczną i warstwę dostępu do medium transmisji MAC. Ideą tworzenia standardu 802.16 było zapewnienie szerokopasmowego radiowego dostępu do Internetu na dużych obszarach osiągając tym samym bardzo dużą szybkość transmisji oraz znaczny zasięg działania takiej sieci. Istnieje kilka standardów sieci WiMAX [Rys. 1.]. Począwszy od nomadycznego 802.16d, który wymaga widoczności optycznej nadajnika i odbiornika LOS (ang. Line-of-sight) po całkowicie mobilny standard 802.16e. Teoretycznie zasięg sieci WiMAX może wynosić nawet 50km, lecz w praktyce najlepsze parametry transmisji osiąga się w odległości nie większej niż 10 km od nadajnika. Istotne jest tutaj również to, aby nie występowały żadne fizyczne przeszkody w tzw. “pierwszej strefie Fresnela”, które to mogą skutecznie tłumić zasięg fal radiowych. Szybkość transmisji rzędu 75 Mb/s jest możliwa do osiągnięcia dzięki wykorzystaniu sprawdzonych rozwiązań warstwy fizycznej. Źródłem takich możliwości jest OFDM (ang. Orthogonal Frequency Division Multiplexing). Ta metoda modulacji wykorzystuje wiele ortogonalnych względem siebie podnośnych, w celu skompensowania zaników selektywnych wynikających z wielodrogowości przesyłanego sygnału. Pojedynczy strumień danych jest kodowany na wielu podnośnych. W ten sposób uzyskano dużą przepływność łącza, oraz lepiej zużytkowano pasmo radiowe. Bardziej zaawansowaną i ulepszoną wersją OFDM jest OFDMA. Dostęp do kanału możliwy jest dla wielu użytkowników jednocześnie. Osiągnięto to poprzez przypisanie różnym użytkownikom różnych podkanałów łącza. Jednocześnie w celu bardziej wydajnej obsługi użytkowników wprowadzono zarządzanie mocą nadawanego sygnału względem kanału transmisyjnego.



Rys. 2. Architektura sieci WiMAX

Warstwa fizyczna składa się z pięciu wariantów działania, w zależności od wykorzystywanego pasma radiowego oraz techniki modulacji:

- WirelessMAN-SC (modulacja SC (ang. *Single Carrier*), pasmo 10-66 GHz)
- WirelessMAN-Sca (modulacja SC, NLOS, pasmo <11GHz)
- WirelessMAN-OFDM (modulacja OFDM, pasmo <11GHz)
- WirelessMAN-OFDMA (modulacja OFDMA, pasmo <11 GHz, mobilność terminala)
- WirelessHUMAN (pasmo <11GHz nielicencjonowane)

Podwarstwa konwergencji (ang. *Transmission Convergence Sublayer*) występuje pomiędzy warstwami fizyczną a dostępu do medium MAC. Konwertuje ona zmienne długości jednostek danych protokołów MAC, na jednostki o stałej długości wykorzystywane w warstwie fizycznej.

Za zestawianie i obsługę połączeń z wykorzystaniem jednego fizycznego nośnika odpowiedzialna jest warstwa dostępu do nośnika MAC (ang. *Data Link Layer*). W jej ramach możemy wyróżnić trzy niezależne podwarstwy:

1. Podwarstwa CS (ang. *Service-Specific Convergence Sublayer*) – przyjmuje ruch oraz odpowiada za przekształcanie jednostek danych protokołów wyższych na zgodne ze specyfikacją warstwy MAC.
2. Podwarstwa MAC CPS (ang. *MAC Common Part Sublayer*) – odpowiada za dostęp do systemu, przydziela pasmo dla poszczególnych usług, inicjuje i zarządza połączeniami
3. Podwarstwa PS (ang. *Privacy Sublayer*) – zapewnia odpowiedni poziom zabezpieczeń pomiędzy stronami połączenia, wykorzystując certyfikaty cyfrowe i algorytmy szyfrujące.

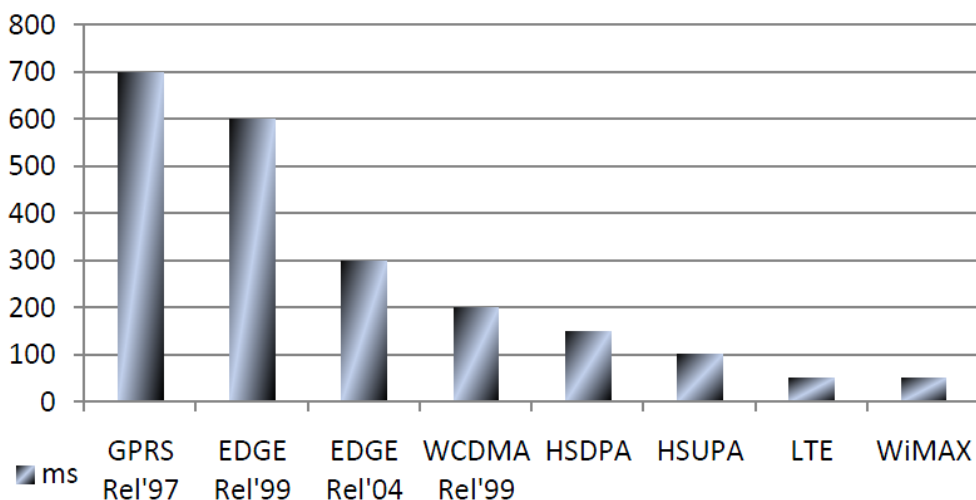
Architektura bezpieczeństwa WiMAX została zdefiniowana w specjalnej podwarstwie SS (ang. *Security Sublayer*). Już na etapie jej projektowania skupiono się na uniknięciu błędów jakie zostały popełnione w standardzie 802.11. Zawarte są w niej specjalne mechanizmy odpowiedzialne za uwierzytelnianie, integralność przesyłanych danych oraz poufność stron biorących udział w transmisji. Stronami tymi są SS (ang. *Subscriber Station*) i BS (ang. *Base Station*). Informacje niezbędne do bezpiecznej transmisji danych są zaimplementowane w tzw SA (ang. *Security Association*). Kontener ten zawiera między innymi wszystkie sprawdzone szyfry symetryczne i niesymetryczne (DES, 3DES, AES, RSA) mechanizmy ochrony integralności danych (HMAC, CMAC) oraz niezbędne certyfikaty cyfrowe X.509 wykorzystywane w protokole PKM (ang. *Privacy Key Management*). Protokół PKM jest używany w procesie logowania się urządzenia do sieci oraz uwierzytelnienia stacji klienckiej. Udoskonalona wersja protokołu PKM w wersji drugiej na etapie uwierzytelnienia wykorzystuje protokół EAP (ang. *Extensible Authentication Protocol*).

Wprowadzono również serwer AAA (Authentication, Authorization, Accounting) obsługujący EAP po stronie sieci. Protokół PKMv2 zakłada aby zarówno stacja kliencka jak i bazowa były wyposażone w certyfikat cyfrowy niezbędny do procesu uwierzytelnienia się stron biorących udział w komunikacji. WiMAX wspiera również tunele VPN, wykorzystywane w celach ochrony danych przesyłanych przez różnych użytkowników systemu w ramach tej samej stacji bazowej.

3. Sieci LTE

Standard LTE jest powszechnie nazywany systemem “prawie czwartej generacji”, uznawany jednocześnie za następcę systemu UMTS/HSPA. Nie spełnia bowiem wszystkich wymogów stawianych przez ITU (ang. International Communication Union) dla technologii 4G/IMT-Advanced. Grupa standaryzująca LTE-3GPP (ang. Third Generation Partnership Project) stworzyła pewne wymogi standardu LTE, które powinny być spełnione [4]. Podczas projektowania standardu skupiono się przede wszystkim na redukcji kosztów pojedynczego bitu transmisji, implementacji nowych, mobilnych usług i lepszym wykorzystaniu pasma radiowego, minimalizując jednocześnie poziom energii pobieranej przez urządzenia. Jego implementacja, podobnie jak w sieciach WiMAX, pozwoli całkowicie przejść na ruch pakietowy oparty na IP w sieciach mobilnych. Jednym z wymogów postawionych przez konsorcjum ITU jest przepustowość w kierunku do użytkownika i od użytkownika. Osiągnięcie poziomu 200 Mbit/s w *downlinku* oraz 50 Mbit/s w *uplinku* nie powinno stanowić większego problemu. Opóźnienia przy tym mają wynosić w granicach 10ms (w przypadku technologii HSPA wnoszą ok 70ms a 2G GSM od 70 do 200 ms) [Rys. 3.].

Poziomy opóźnień



Rys. 3. Poziomy opóźnień transmisji danych w sieciach radiowych

Standard LTE ma być systemem globalnym, używanym na całym świecie. Dlatego bardzo ważną kwestią jest odpowiedni dobór widma na potrzeby tego standardu. 3GPP przedstawiło bardzo szeroki zakres możliwych do wykorzystania na potrzeby LTE częstotliwości. W Polsce UKE na realizację szerokopasmowych sieci bezprzewodowych planuje przeznaczyć pasma 2010-2025 MHz oraz 2500-2690 MHz.

LTE	WiMAX
<ul style="list-style-type: none"> • Rozwijany przez 3GPP • Oparty na GSM, interfejs radiowy OFDM • Downlink – czysty OFDMA • Uplink – Single Carrier FDMA • Szerokość kanału 1.25 – 20 MHz • Szybkość transmisji 250 Mb/s 	<ul style="list-style-type: none"> • Rozwijany przez WiMAX Forum • Oparty na IEEE 802.16 (modulacja OFDMA) • Szybkość transmisji <ul style="list-style-type: none"> ○ 100 Mb/s mobilny WiMAX ○ 1 Gb/s nomadyczny WiMAX

Tab. 1. Porównanie standardów LTE i WiMAX

LTE wprowadza szereg ulepszonych technik wykorzystywanych w innych systemach radiowych. Zorientowane są one głównie na uzyskanie dużych przepustowości łącza oraz minimalne zużycie potrzebnego pasma radiowego. Wspomniane rozwiązania to :

- HARQ (ang. Hybrid Automatic Repeat Request) – mechanizm odpowiedzialny za bezbłędną transmisję danych oraz korygowanie ewentualnych, drobnych błędów.
- MIMO (ang. Multiple Input/Multiple Output) – technika radiowa wykorzystująca do nadawania i odbierania sygnału zestawu kilku macierzy antenowych w celu lepszej separacji sygnałów od siebie. Ogranicza się w ten sposób powstałą interferencją będącą skutkiem wielodrogowości przesyłanego sygnału oraz poprawia jakość transmisji. Tradycyjny system LTE wykorzystuje schemat 2x2 (2 anteny nadawcze i 2 anteny odbiorcze).
- OFDM (ang. Orthogonal Frequency Division Multiplex) – technika modulacji polegająca na jednoczesnym transmitowaniu wielu strumieni danych na ortogonalnych względem siebie częstotliwościach nośnych. W zastosowaniu LTE zapewnia szybkie przepustowości, zapewniając jednocześnie ochronę przed interferencjami z zewnątrz. Schemat dostępu do kanału różni się w zależności od typu transmisji. W *downlinku* w LTE wykorzystywany jest wielodostęp OFDMA (ang. Orthogonal Frequency Division Multiple Access), w *uplinku* SC-FDMA (ang. Single Carrier Frequency Division Multiple Access)
- SAE (ang. System Architecture Evolution)- modyfikacja sieci szkieletowej w celu uzyskania mniejszych opóźnień oraz wysokich przepustowości sieci. System SAE jest

ogromną zmianą w strukturze sieci radiowej. Architektura SAE zawiera jedynie dwa węzły: stacji bazowej LTE eNodeB (ang. Evolved NodeB) oraz sieci szkieletowej AGW (ang. Access GateWay).

Rozszerzeniem standardu LTE, nad którym ciągle trwają prace, jest LTE-Advanced. Specyfikacja tego standardu, zgodnego ze specyfikacją 4G, zakłada szereg wytycznych [5]. Zakłada się między innymi:

- duże przepływności, wspierające nowe usługi i aplikacje, osiągające przepustowość rzędu 1Gbit/s (w marcu 2010 na targach CTIA Wireless Huawei osiągnął szybkość 1,2 Gbit/s)
- pełna kompatybilność z innymi systemami radiowymi
- usługi mobilne wysokiej jakości
- możliwości użytkownika zgodnych urządzeń w roamingu na całym świecie
- wprowadzenie innowacyjnych usług mobilnych

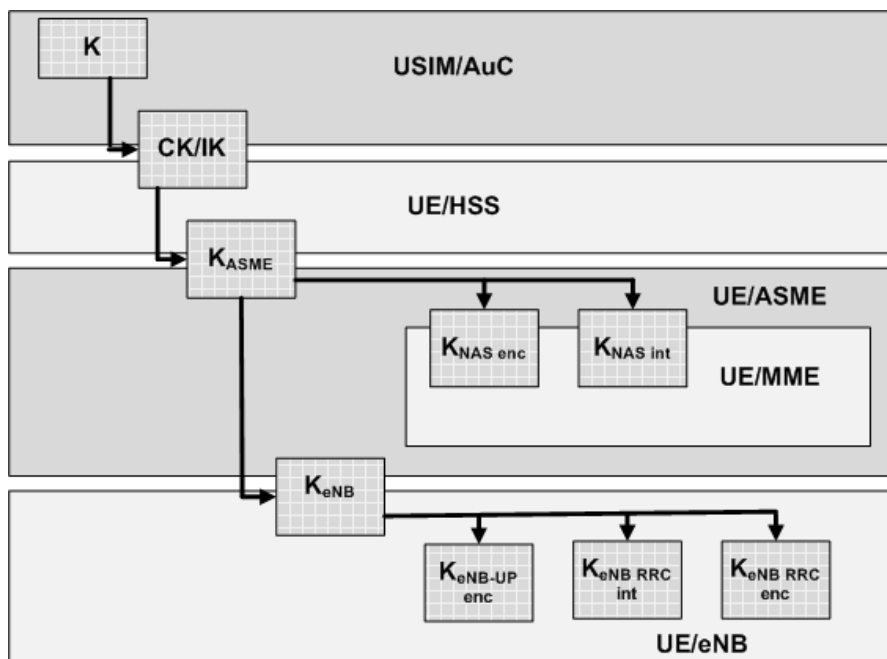
LTE-Advanced z technologicznego punktu widzenia ma być rozszerzeniem standardu LTE, stając się pierwszą siecią 4G na świecie. Modyfikacji ma być poddana przede wszystkim warstwa fizyczna sieci. Pozwoli to uzyskać dostęp do szerszych nośnych, a dodatkowe wprowadzenie zaawansowanych technik antenowych MIMO będzie skutkowało wyższymi prędkościami transmisji oraz większą pojemnością sieci. Zastosowanie multipleksacji przestrzennej pozwoli zwiększyć ilość anten do 4x4 (4 anteny nadawcze i 4 odbiorcze) w przypadku *uplinku*, a dodatkowo dzięki formowaniu wiązki uzyskać do 8x8 anten w *downlinku*. Wprowadzenie szerszego kanału radiowego pozwoli uzyskać zakładane przepustowości na poziomie 1Gbit/s.

W porównaniu do tradycyjnego LTE, szerokość kanału ma zostać zwiększona z 20MHz do 100 MHz, łącząc kilka nośnych o mniejszej szerokości. W ten sposób systemy LTE i LTE-A będą w pełni kompatybilne ze sobą, przy czym ilość dostępnych pasm dla poszczególnych użytkowników systemów będzie różna. Warto również dodać, że kanały o szerokości 20MHz, które będą tworzyć szerszy kanał na potrzeby LTE-A, nie muszą ze sobą sąsiadować. Oszczędzamy w ten sposób pasmo radiowe oraz lepiej nim zarządzamy.

Bardzo istotną kwestią jest zapewnienie odpowiedniego poziomu bezpieczeństwa w sieciach LTE. Migracja LTE do sieci pakietowej IP już sama w sobie jest ogromnym krokiem do przodu jeśli chodzi o bezpieczeństwo komunikacji i dostępu do sieci. Nie tylko pomija wszystkie błędy popełnione w klasycznych sieciach radiowych, ale również wprowadza mechanizmy pozwalające na uwierzytelnienie, autoryzację oraz audyt zarówno użytkownika jak i operatora LTE. Wykorzystuje również sprawdzone algorytmy szyfrujące, mechanizmy zarządzania siecią oraz certyfikaty cyfrowe.

Technologia LTE wprowadza całkowicie nową architekturę oraz hierarchię zarządzania kluczami bezpieczeństwa. Rezygnuje z obecnie wykorzystywanych kart SIM (ang. Subscriber Identity Module), a wprowadza karty USIM (ang. Universal Subscriber Identity Module). Wykorzystują one klucz 128 bitowy, z możliwością rozszerzenia do 256 bitów.

Rozszerzona hierarchia kluczy wykorzystywana w LTE pozwala na szybsze generowanie i odświeżanie kluczy w procesie przełączania się pomiędzy stacjami nadawczymi, również w ramach sieci 2G/3G. Poniższy rysunek ilustruje taką strukturę kluczy [Rys 4.].



Rys. 4. Struktura kluczy w sieciach LTE

Uwierzytelnienie subskrybenta odbywa się z wykorzystaniem mechanizmu AKA (ang. Authentication and Key Agreement), pomiędzy UE (ang. User Equipment) a MME (ang. Mobility Management Entity). Dodatkowy moduł ASME (ang. Access Security Management Entity), rozmieszczony razem z MME, jest odpowiedzialny za ochronę sygnalizacji NAS (ang. Network Access Server or Nonaccess Stratum). Proces szyfrowania oraz sprawdzania integralności danych odbywa się z wykorzystaniem algorytmu AES oraz SNOW 3G. Klucze wykorzystywane do ochrony NAS są ulokowane osobno i znajdują się w eNB (ang. E-UTRAN nodeB) oraz EPC (ang. Evolved Packet Core). Moduł ASME otrzymuje klucz K_{ASME} niezbędny w procesie uwierzytelnienia z UE. ASME przekazuje dalej ten klucz do MME, jak również wysyła klucze wygenerowane i pochodzące z K_{ASME} do eNB. Klucze K_{NAS} i K_{eNB} pozyskane z K_{ASME} , nie opuszczają EPC. Klucze K_{eNB-UP} i $K_{eNB-RRC}$ uzyskiwane są z K_{eNB} , eNB oraz UE. Kiedy UE przechodzi w stan uśpienia klucze te są usuwane. Klucze K_{NAS} są używane do zabezpieczenia i szyfrowania

komunikacji NAS. Klucz K_{eNB-UP} jest używany do zabezpieczenia komunikacji U-Plane, a klucz $K_{eNB-RRC}$ jest używany wyłącznie do ochrony ruchu RRC (ang. Radio Resource Controller). W przypadku gdy klucze są skorumpowane (uszkodzone), UE ponownie przeprowadza procedurę negocjacji.

4. Podsumowanie

Gigantyczny rozwój sieci telekomunikacyjnych, którego jesteśmy świadkami, prowadzi do rozwoju nowych technologii i świadczonych tą drogą usług. Coraz większa grupa użytkowników korzysta z mobilnych urządzeń dostępowych, które coraz bardziej swoją funkcjonalnością oraz możliwościami przypominają komputery stacjonarne. Urządzenia takie dają dostęp do różnych wcieleń osób z nich korzystających, bez względu na miejsce w których obecnie się znajdują. Dlatego dostęp do Internetu realizowany za pomocą technologii bezprzewodowych jest priorytetem w dalszym rozwoju takich technologii. Bezprzewodowe sieci teleinformatyczne stanowią trzon takiej przyszłości. Następną generacją mobilności wymaga aby połączenia cechowały się niskimi opóźnieniami, a sieci szkieletowe były skalowalne i tańsze w utrzymaniu. Zarówno sieci WiMAX jak i LTE są technologiami, które mogą sprostać tym wymaganiom. Są również podobne do siebie technologicznie przez co wzajemnie mogą się uzupełniać. Dlatego integracja obu tych sieci jest kluczowa z punktu widzenia operatorów telekomunikacyjnych. Zatem dowodzenie oraz jednoznaczne rozstrzygnięcie, która technologia jest lepsza dla użytkownika jest niemożliwe. Patrząc pod kątem wykorzystywanych technik radiowych, kodowania czy zaawansowanych systemów antenowych MIMO, oba systemy są niemal identyczne. Oparte są na protokołach IP, więc dane transmitowane są w pakietach. Z racji tego, że infrastruktura sieci WiMAX jest pochodną IEEE, jest bardziej otwarta na nowe ulepszenia i dostosowana do wprowadzania ewentualnych zmian w najbliższej przyszłości. Zarówno standard 802.16e jak i LTE 3,9G zostały już ukończone. Aktualnie producenci wprowadzają urządzenia oraz usługi na rynek, czego będziemy świadkami wkrótce. Najbliższa przyszłość przyniesie skok technologiczny w szybkim bezprzewodowym dostępie do Internetu, a mnogość usług (VoIP, VOD, DVB-H) sprawi, że coraz bardziej będziemy uzależnieni od "jednego pudełka" jakim będzie urządzenie mobilne. Technologia, która zdolna będzie dostarczyć użytkownikowi odpowiednie pokrycie sygnałem radiowym, dużą przepływność oraz szeroką gamę usług wygra tę potyczkę. Z kolei sam system, z którego będzie korzystał końcowy użytkownik pozostanie sprawą mało istotną.

Literatura

1. 3GPP2 TSG C.S0024-0 v2.0, cdma2000 High Rate Packet Data Air Interface Specification.
2. 3GPP TSG RAN TR 25.848 v4.0.0, Physical Layer Aspects of UTRA High Speed Downlink Packet Access.
3. IEEE Std 802.16e-2005, Air Interface for Fixed and Mobile Broadband Wireless Access Systems
4. 3GPP LTE, <http://www.3gpp.org/article/lte>
5. "Raport ITU-R M.2134 - Requirements related to technical performance for IMT-Advanced radio interface" ; ITU
6. F. Khan, LTE for 4G Mobile Broadband, Cambridge University Press, 2009
7. <http://www.lte-4g.info/>
8. WiMAX Telecom - <http://www.wimax-telecom.net/en/index.php>
9. WiMAX Forum - <http://www.wimaxforum.org/home/>
10. WiMAX-Vision.com: 'Why MIMO needs beamforming', (September 2006)—
<http://www.wimax-vision.com/newt/l/wimaxvision/viewarticle.html?artid=20017410725>
11. T. Shon, W. Choi, An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions
12. Ł. Kucharzewski, Z. Kotulski, Sieci WiMAX – architektura i bezpieczeństwo danych, Konferencja IBIZA, 2009
13. S. Ahson, M. Ilyas, WiMAX Standards and Security, Aurebach Publications, Taylor & Francis Group, 2008
14. Y. Zhang, Handbook of Research on Wireless Security, Idea Group Publishing, 2008
15. M. Ergen , Mobile Broadband Including WiMAX and LTE, Springer, 2009
16. Yang F., Zhou H., Zhang L., Feng J., An Improved Security Scheme in WMAN Based on IEEE Standard 802.16, Proceedings of International Conference on Wireless Communications, Networking and Mobile Computing”, tom 2, 2005
17. J. Hasan, Security Issues of IEEE 802.16 (WiMAX), School of Computer and Information Science, Edith Cowan University, Australia
18. M. Pawłowski, P. Matusz, J. Woźniak, WiMAX – nowy standard szerokopasmowych sieci bezprzewodowych (1), Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne nr 7, 2005
19. P. Zawadzki P, Podsystem bezpieczeństwa sieci WiMAX, Przegląd Telekomunikacyjny nr 2-3, 2007
20. K. Cabaj, W. Mazurczyk, K. Szczypiorski, Bezpieczeństwo bezprzewodowych sieci WiMAX, Enigma 2007 – XI Krajowa Konferencja Kryptografii i Ochrony Informacji, Warszawa, 23-25 maja 2007
21. H. Li, G. Fan, J. Qiu, X. Lin, GDKA: A Group-Based Key Distribution Algorithm for WiMAX MBS Security, Department of Electronic Engineering, Tsinghua University, Beijing, China, Intel China Research Center, Beijing, China, Graduate School at Shenzhen, Tsinghua University, Shenzhen, Guangdong, China