УДК 004.056.53
Кравець О. –ст. гр. СІм-51
Тернопільський національний технічний університет імені Івана Пулюя

АСПЕКТИ ЗАХИЩЕНОСТІ ТЕХНОЛОГІЇ CDMA

Науковий керівник: к.т.н., доцент Луцків А.М.

У зв'язку з недостатніми функціональними можливостями систем безпровідного зв'язку попередніх поколінь замінюються новими, зокрема поколінь 2.5G та 3G. До них належить технологія CDMA (Code Division Multiple Access) – система множинного доступу з кодовим розділенням. Технологія CDMA не підрозділяє абонентів на фіксованих і мобільних і не обмежує їх в доступі до послуг мережі при переміщенні. Існує декілька варіантів технології CDMA, до 3G найбільш близьким є широкосмуговий множинний доступ – WCDMA, що забезпечує більш високу передачу даних, а також EV-DV. CDMA є широкосмуговою системою із шумоподібними сигналами. Шумоподібність сигналів полягає в тому, що коли в ефірі на одній частоті, в один і той же час працюють декілька абонентів, сигнали накладаються один на одний. Технологія є водночас завадостійкою, що забезпечує при виникненні в широкій смузі частот (1,23 МГц) сигналу-перешкоди вузького діапазону (<150кГц), сигнал прийметься майже неспотвореним.

Важливим аспектом використання технології CDMA є використовувані в ній технології захисту інформації. CDMA передбачає: автентифікацію повідомлень, верифікацію базової станції (чого не було в стандарті GSM) і терміналу абонента, можливість використання біометричних систем обмеження доступу до терміналу абонента, шифрування/дешифрування додатковими криптомодулями, можливість зміни частот із зміною місця, передавання пакетів на різних частотах, системи контролю доступу до базової станції та мережевого обладнання, використання шумоподібних сигналів з кодовим доступом. Для забезпечення захищеності використовуються наступні засоби захисту інформації: фізичний рівень (сигнальне скремблювання безпровідного зв’язку, технологія частотного скремблювання радіозв’язку, розширений спектр частот (кожний фрагмент ідентифікується цифровим кодом, який знають термінал отримувача та базова станція), теоретично жодний інший термінал не може отримати адресоване не йому повідомлення, для кожного передавання існують мільйони кодових комбінацій), канальний та мережевий рівень (забезпечення конфіденційності на канальному та мережевому рівнях, шифрування кожного сегменту дейтаграми перед передаванням, ключ використовується в автентифікації та шифруванні кадрів TDMA перед передаванням), транспортний рівень (є можливість використання протоколу SSL), прикладний рівень передбачає автентифікацію користувачів за логіном/паролем користувача, стратегію ідентифікації користувача за допомогою перевірки правильності його реакції на непередбачуваний запит системи, перевірку цілісності повідомлень, хешування для генерування MAC, шифрування: RC5; 3DES; Rijndael, використання цифрового підпису: PKI, RSA, ECDSA, ECC.

З метою шифрування сенсів зв'язку використовуються алгоритми шифрування: блоковий UEA1/UIA1 (KASUMI) та потоковий UEA2/UIA2 (SNOW 3G). Причому алгоритм UEA1/UIA1 на сьогодні вважається ненадійним. У ході досліджень автором здійснюється дослідження криптостійкості потокових шифрів, до яких належить надійний на сьогодні SNOW 3G.