Proceedings of the 15th Conference STUDENT EEICT 2009. – Brno: NOVPRESS s.r.o., 2009. – P. 254– 258. ISBN: 978-80-214-3870-5.

6. Семенова О. О. Фазі-контролер трафіка для телекомунікаційних мереж / О.О. Семенова, О.О. Войцеховська // Інформаційні технології та комп'ютерна інженерія – 2007. – № 2. – С. 128– 131.

7. Семенова О.О. Керування у АТМ-мережах за допомогою інтелектуальних технологій / О.О. Семенова, А.О. Семенов, В.В. Чухов // Вимірювальна та обчислювальна техніка у технологічних процесах. – 2010. – № 2. – С. 260– 264.

Надійшла до редакції
7.3.2011 р.

УДК 004: 004.65

Ю.В. ХМЕЛЬНИЦЬКИЙ
Хмельницький національний університет

ОСОБЛИВОСТІ ФІЗИЧНОГО РІВНЯ МЕРЕЖ СТАНДАРТУ IEEE 802.16

В статті розглянуто принципи систем широкосмугового радіо доступу з інтеграцією послуг. При побудові систем стало зрозуміло, що основні принципи, закладені в без провідникових системах на попередніх етапах, потребують значної корекції. На сигнальному рівні першочергове значення дістало оптимальне використання спектрального ресурсу радіоканалу при будь-яких співвідношеннях „швидкість – завадо захищеність".

In the article the principles of broadband radio access integrated services. When building systems, it became clear that the basic principles laid without conducting system in the previous stages, require a significant correction. At the signal staflax level priority had received optimal use of radio spectrum resource in any ratio speed – prevent security.

Ключові слова: широкосмугове радіо, радіоканал.

Вступ

При створенні систем широкосмугового радіо доступу з інтеграцією послуг стало зрозуміло, що основні принципи, закладені в без провідникові системи на попередніх етапах, потребують значної корекції. На сигнальному рівні першочергове значення дістало оптимальне використання спектрального ресурсу радіоканалу при будь-яких співвідношеннях „швидкість – завадо захищеність". На рівні протоколів стало необхідним забезпечувати заданий рівень якості обслуговування (QoS) будь-якому абоненту мережі. З цією метою в 2004 році був розроблений стандарт IEEE 802.16-2004, що являє собою розраховану на введення в міських бездротових мережах (WirelessMAN) технологію без провідного широкосмугового доступу операторського класу. Часто використовується комерційна назва стандарту WiMax (Worldwide Interoperability for Microwave Access), що походить від назви міжнародної організації WiMax Forum, в яку входять ряд комунікаційних компаній.

Основне призначення даних мереж – це надання послуг абонентам по високошвидкісній і високоякісний безпровідній передачі даних, голосу і відео на відстані в декілька десятків кілометрів. У жовтні 2007 року International Telecommunication Union (ITU-R) включив технологію WIMAX стандарту IEEE 802.16 в сімейство стандартів мобільного зв'язку 3G. У мережах WIMAX реалізовані найостанніші досягнення науки і техніки в області радіозв'язку, телекомунікації і комп'ютерних мереж. Стандарт IEEE 802.16 визначає застосування:

- на фізичному рівні широкосмугового радіосигналу OFDM з множиною під несучих;
- на канальному рівні використовується сучасний протокол множинного (багато станційного) доступу Time Divion Multiply Access (TDMA) і Scalable OFDM Access (SOFDMA);
- на мережевому (транспортному) рівні в мережах WIMAX застосовується IP-протокол передачі даних, що широко використовуваний в більшості сучасних мережах передачі даних, зокрема, в мережі Інтернет.

В більшості випадків проектування мереж WiMax є досить складним і неоднозначним процесом. Розрахунок покриття відбувається на основі вимірювань рівня завад на місцевості, що потребує значних витрат коштів та часу.

Стандарти IEEE 802.16 в системах безпровідного доступу

WIMAX, скорочення від "Міжнародної взаємодії для Сприяння Мікрохвильовому Доступу", є ефективним рішенням для "останньої милі", що має на меті надання широкосмуговій мережі від WISP безпосередньо до будинків і офісів. Технологія WIMAX ґрунтується на стандарті IEEE 802.16, який у свою чергу визначає стандарт ефірного інтерфейсу WIRELESSMAN для безпровідних мереж, призначених для обслуговування крупних регіонів. Оригінальний стандарт IEEE 802.16 призначений для WIMAX в діапазоні частот 10 – 66 Ггц і припускає роботу в режимі "прямої видимості" – line of sight (LOS). Пізніше версія стандарту IEEE 802.16a була розвинена для використання в ліцензійних і звільнених від ліцензування діапазонах частот від 2 до 11 Ггц для режиму "без прямої видимості" (NLOS). Стандарт IEEE 802.16d, який також відомий як IEEE 802.16-2004, є новою версією IEEE 802.16a і є рішенням для широкосмугового

доступу для останньої милі. Цей стандарт є стандартом фіксованого зв'язку, тому що він припускає використання користувачем нерухомої антени. Стандарт IEEE 802.16e, який називається також "мобільним WIMAX", є поправкою до стандарту 802.16d і додає "мобільність" до даного стандарту. Тоді як застосування фіксованого WIMAX в режимі "точка-багатоточка" надає широкосмуговий доступ до будинків і фірм, "мобільний WIMAX" припускає повну мобільність клієнтів стільникових мереж при наданні дійсно широкосмугових послуг.

Для WIMAX застосовуються як ліцензійні, так і неліцензійні частотні спектри. Завдяки використанню направлених антен, WIMAX дозволяє отримати великі відстані передачі, які можуть досягати приблизно 30 миль (50Км). Тоді як 802.16 може надати максимальну пропускну спроможність приблизно 124 Мбіт/с, 802.16a може досягти пропускної спроможності тільки 70 Мбіт/с, оскільки він повинен долати труднощі, викликані умовами режиму NLOS в діапазоні 2-11 Ггц.

WIMAX використовує схему OFDM з 256 несучими, що дозволяє йому досягти високої швидкості даних, збільшення приблизно в таке ж число разів тривалості елементарного символу, одночасно приймати прямій і відбиті від перешкод сигнали або взагалі працювати тільки по відбитих сигналах поза межами прямої видимості. Режим OFDMA передбачає роботу на 2048 піднесуть відразу з декількома абонентами в режимі OFDM. При стандартній кількості піднесуть – 256, забезпечується одночасна робота з 8 абонентами. Мобільна версія WIMAX, 802.16e, використовує Множинний Доступ з Ортогональним Частотним Мультиплексуванням (OFDMA), який не тільки ділить ті, що несуть на безліч тих, що піднесуть (як в OFDM), але також групує ці що множинні піднесуть в під канали. Крім того, WIMAX покладається на протокол доступу на основі запиту надання, який, на відміну від доступу на основі твердження, використовуваного в Wi-Fi, не дозволяє виникати колізіям даних і, таким чином, ефективніше використовує наданий діапазон частот. Як "фіксований WIMAX", так і "мобільні WIMAX" мають змінні смуги пропускання шириною від 1,5 до 20МГц для того, щоб забезпечити можливість передачі на великі відстані і до різного устаткування користувачів.

Протоколи фізичного рівня описують методи організації дуплексу, способи адаптації, методи множинного доступу і модуляції.

Передбачені режими тимчасового і частотного дуплексу. Вид модуляції і кодування можуть змінюватися адаптивний від пакету до пакету індивідуально для кожного абонента, що дозволяє збільшити реальну пропускну спроможність приблизно удвічі в порівнянні з не адаптивними системами. Передача від АС до БС будується на комбінації двох методів багато станційного доступу: DAMA – доступ за запитом і TDMA – доступ з тимчасовим розділенням. Структура пакетів фізичного рівня підтримує змінну довжину пакету MAC рівня. Передбачена рандомізація, завадостійке кодування і три методи модуляції: QPSK, 16QAM і 64QAM. Два останні методи передбачено для АС як опціональні.

Передача від БС до АС ведеться в режимі тимчасового дуплексу в єдиному потоці для всіх АС одного сектора. Передавач здійснює рандомізацію, перешкодостійке кодування і модуляцію QPSK, 16QAM і 64QAM. Останній метод модуляції передбачений для БС як опціональний. Інформація в системі передається фреймами, які діляться на два субфрейми. Перший використовується для передачі БС, другої, – АС.

Стандартом також рекомендуються смуги частот і відповідні швидкості передачі при різних видах модуляції. Максимальна швидкість передачі, передбачена в стандарті, – 134,4 Мбіт/с при смузі 28 Мгц і модуляцій 64QAM.

У першій версії стандарту передбачалося використання діапазону частот 10-66 Ггц для якого рекомендувався режим передачі на одній несучій – single-carrier (SC). Особливості розповсюдження радіохвиль цього діапазону обмежують можливості роботи умовами прямої видимості. У типових міських умовах це дозволяє підключити близько 50 % абонентів, що знаходяться в межах робочої дальності від базової станції. До останніх 50 % прямої видимості, як правило, немає. Тому в процесі роботи над стандартом діапазон частот був розширений включенням смуги 2-11 Ггц, в якій, крім SC, передбачені ще і режими ортогонального частотного мультиплексування (Orthogonal Frequency Division Multiplexing – OFDM) і множинного доступу на основі ортогонального частотного мультиплексування (Orthogonal Frequency Division Multiply Access – OFDMA).

У стандарті також описані моделі середовищ розповсюдження радіохвиль і на цій основі сформульовані вимоги до параметрів радіоустаткування. Передбачені можливості автоматичного регулювання посилення, динамічного вибору частоти в неліцензійних діапазонах. Крім топології точка-багатоточка стандартом опціонально передбачена повно зв'язна топологія – Mesh Mode, що дозволяє забезпечити прямий зв'язок АС, подолати перешкоди, характерні для неліцензійних діапазонів, за рахунок вибору напряму прийому, вільного від них, створювати добре масштабовані мережі і працювати поза прямою видимістю навіть в одно частотному режимі SC, за рахунок ретрансляції сигналів АС.

Протягом достатнього тривалого періоду часу користувачі мереж Широкосмугового Безпровідного Доступу (BWA) чекають ефективного рішення задачі доставки високошвидкісного Інтернет в їх офіси і житлові приміщення, у тому числі і до тих віддалених пунктів, де традиційні послуги широкосмугового доступу на даний момент не реалізовуються. Після публікації в повному об'ємі розвиненого промислового стандарту IEEE802.16, що є самою передовою технологією, яка для забезпечення сумісності устаткування узгоджена з промисловістю, з'явилася надія на здійснення цих очікувань.

Стандарт IEEE 802.16, перша версія якого була закінчена в жовтні 2001 і видана 8 квітня 2002, – це

стандарт безпровідного інтерфейсу Wireless MAN для безпровідних мереж (MAN), здатних охопити послугами мегаполіси, який призначений для того, щоб забезпечити передачу по високочастотних радіоканалах голосу і даних до офісів і житлових приміщень клієнтів. Консорціум промисловців всього світу, який здійснює Сприяння Мікрохвильовому Доступу, широко відомий як Консорціум WIMAX, сприяє розвитку стандарту IEEE 802.16, а також здійснює перевірку устаткування і його сертифікацію на предмет відповідності даному стандарту. Тому стандарт IEEE 802.16 часто сприймається як WIMAX сьогодні.

Стандарт IEEE 802.16a/d визначає три різних PHY (Фізичних рівня) – WirelessMAN-SCa, WIRELESSMAN-OFDM і WIRELESSMAN-OFDMA, які у взаємодії з рівнем MAC дають можливість забезпечити надійний безперервний зв'язок. На першому етапі творцями стандарту був вивчений і реалізований PHY, відповідний варіанту WIRELESSMAN-OFDM. Були також вивчені і реалізовані різні методи, які формують PHY так, щоб забезпечити найбільш реалістичну систему. Перш ніж здійснити всі ці кроки, були проведені детальні дослідження різних технологій широкосмугового доступу. Потім розробниками стандарту були детально вивчені механізми функціонування безпровідних каналів, і лише після цього був короткий огляд моделі PHY системи WIMAX. Були також вивчені різні застосовні види модуляції, а функціональні можливості кожної поліпшуючої параметри техніки вивчалася послідовно одна за іншою з погляду тих переваг, які вони надають системі. Нарешті, для підтвердження встановлених залежностей були приведені результати моделювання.

WIMAX передбачає процедуру введення в мережу нових станцій користувачів (або вузла користувачів) і їх ініціалізацію при першому підключенні до мережі. Нижче розглянута процедура введення в мережі по схемі "точка-багатоточка". У стандарті приведений спрощений алгоритм введення в мережу нової станції при сприятливому закінченні процедури. З іншими можливими сценаріями введення, включаючи і невдалу спробу, слід ознайомитися безпосередньо в стандарті IEEE 802.16.2004 (Revel). Процедура введення нової станції в мережу передбачає проходження наступних ступенів.

1. Сканування приймачем низхідного каналу і встановлення синхронізації з системним часом базової станції.
2. Отримання параметрів на передачу (для повідомлення UCD).
3. Становлення в чергу діставання доступу.
4. Ведення переговорів по базових можливостей.
5. Авторизація і обмін ключами шифрування.
6. Виконання реєстрації.
7. Створення з'єднання (зв'язки).
8. Встановлення загального часу і лати.
9. Оперативне отримання з системи необхідних параметрів.
10. Установка параметрів з'єднань (включаючи отримання набору CID).

Ступені 7, 8, 9 станція SS проходить самостійно в процесі реєстрації при сприятливому результаті обміну повідомленнями REG-REQ/REG-RSP.

Кожна SS повинна містити наступну інформацію, встановлену в устаткування виробником:

- 48-бітова універсальна MAC-адрес. Ця адреса потрібна для ідентифікації SS в процесі введення і ініціалізації;
- інформацію для кодування, використовувану для аутентифікації SS і забезпечення процесу шифрування в цілях безпеки передачі.

Фізичний рівень підтримки системи OFDM – MAN

Фізичний рівень, що забезпечує передачу інформації в мережі міського значення MAN-OFDM, заснований на технології OFDM, як найбільш пристосованою для застосування в умовах непрямої видимості. Для умовної прямої видимості стандартами 802.16 і 802.!6– 2004 передбачено використовувати пряме розширення спектру тільки з однією SC, що несе {Single Carrier), як технічно більш простій. У будь-якій системі зв'язку, тим більше в гаком ненадійному канаті, як радіо ефір, завжди виникають помилки. Для забезпечення високої достовірності даних, що приймаються, існують три основні підходи:

- застосування код, що виявляють помилки;
- застосування механізму прямого виправлення помилок FEC з використанням коду, що дозволяють коректувати виявлені помилки:
- застосування протоколів, що здійснюють процедуру автоматичного запиту повторної передачі неякісних кадрів, – ARQ.

Застосування цих способів можливе лише за рахунок введення при передачі крім даних трафіку ще і додаткових біт (або навіть декілька байт) які коректують код. В результаті частка корисного трафіку загалом у потоці даних в каналах з надмірним кодуванням зменшується. Для збереження швидкості передачі корисного т рафіку доводиться загальну швидкість передачі даних (т рафік + надмірні коди) збільшувати. Це плата за підвищення достовірності доставки даних т рафіку. Операції кодування, а на приймальному кінці декодування виконуються на фізичному рівні. Саме на цьому рівні дані готуються (кодуються) для передачі по каналу зв'язку, що включає середовище передачі. Тому цей процес називають канальним кодуванням (на приймальному кінці – канальним декодуванням). Після канального кодування дані подаються безпосередньо на модулятор для перетворення в радіосигнал.

В процесі канального кодування потік бітів, що отримується з MAC-уровня. піддається рандомізації. Обов'язковим є введення кодів, що забезпечують пряму корекцію помилок FEC. Стандартом передбачено використовувати для FEC ланцюговий код Рідка– Соломона (RS– CC) спільно із загортальним кодуванням. Опційно передбачається застосовувати або блокове турбокодування. або згортальне турбокодування.

Спектральна ефективність OFDM сигналу системи WIMAX

Технологія широкосмугових радіосигналів (ШПС) була розроблена в середині минулого століття і спочатку застосовувалася військовими з метою підвищення скритності і перешкодостійкості зв'язку. Найважливішою гідністю широкосмугових систем є висока швидкість передачі даних. При цьому поняття широкосмугової (broadband) трактується не тільки як використання радіосигналу з широким частотним спектром, але і як здатність системи забезпечити високу швидкість передачі даних, необхідну для мультисервісного обслуговування (доступ в Інтернет, передача даних, голосу, відео і ін.).

У системах WIMAX застосовується широкосмуговий Orthogonal Frequency Division Multiplexing (OFDM) сигнал, утворений з безлічі рознесених по частотному спектру вузько смугових сигналів. Застосування OFDM сигналу забезпечує системі WIMAX найвищу в класі BWA спектральну ефективність (швидкість передачі даних в одному Герці смуги частотного спектру), можливість роботи поза прямою видимістю, найвищі енергетичні параметри зв'язку забезпечують високу дальність зв'язку, можливість ефективного обслуговування мобільних абонентів.

Спектральна ефективність системи оцінюється максимальною можливою швидкістю передачі даних (кількість переданих біт/с) системи в одиниці смуги займаних частот в один Герц. Висока спектральна ефективність системи WIMAX досягається за рахунок розподілу передачі інформації по паралельних під каналах тих, що піднесуть сигналу OFDM. OFDM є множиною вузько смугових рознесених по частоті сигналів-піднесущих (subcarrier). OFDM сигнал формується таким чином. Деяка високошвидкісна послідовність імпульсів спочатку ділиться на безліч паралельних цифрових потоків з імпульсами більшої тривалості.

Найважливішою відмінністю OFDM технології від простого розділення радіосигналу по декількох паралельних частотних каналах є ортогональность тих, що піднесуть в груповому спектрі OFDM сигналу. Фізичний сенс ортогональності полягає в підмішуванні в структуру кожної спеціальної мітки, що піднесе, – певної унікальної кількості синусоїдальних коливань сигналу, що розрізняються по фазі на 90 град. (ортогональних функцій), що дозволяє демультиплексору на основі аналізу даних влучний розділяти сигнали, що піднесуть, навіть у разі часткового перекриття їх частотних спектрів. Виділення тих, що несуть в загальному спектрі звичайного багатоканального сигналу унаслідок обмежених технологічних можливостей сучасних смугових частотних фільтрів вимагає достатньо великого частотного рознесення тих, що несуть, що обмежує збільшення їх кількості в заданій смузі частот. Виділення тих, що несуть в груповому спектрі OFDM сигналу при демультиплексуванні проводиться за допомогою ортогональних перетворень сигналів. Це допускає можливість перекриття спектрів що сусідніх піднесуть, що дозволяє значно збільшити частотну щільність їх розміщення в спектрі сигналу і підвищити спектральну ефективність.

Метод селекції сигналів і перешкод (шуму) на основі аналізу їх структури застосовується в технології широкосмугового радіозв'язку з середини 1990-х років. Вперше даний метод був використаний в технології розширення спектру DSSS для формування і виділення на тлі перешкод широкосмугового шумоподібного сигналу, що утворюється шляхом множення (мультиплексування) вузько смугового сигналу на випадкову швидкісну послідовність імпульсів. Дана технологія була реалізована в безпровідних локальних мережах першого покоління Wireless LAN (WLAN) стандарту IEEE 802.11, системах супутникової навігації GPS. Метод виділення сигналів по закладених при їх формуванні цифрових кодах також реалізований в мобільному зв'язку стандарту Code Division Multiply Access (CDMA).

Застосування OFDM сигналу дозволяє WIMAX мережам забезпечити вищу швидкість передачі даних по порівнянню системами з тією, що однією несе, що досягається за рахунок розподілу передачі інформації по безлічі паралельних частотних каналів.

Використання OFDM, в принципі, не є специфічною особливістю технології WIMAX. Модуляція OFDM також застосовується, наприклад, в системах Wi-Fi стандарту IEEE 802.11a/g. Проте OFDM в технології WIMAX стандарту IEEE 802.16 має значно більше число тих, що піднесуть, визначають вищу спектральну ефективність систем WIMAX в порівнянні з системами стандарту IEEE 802.11a/g.

Висновки

Головною перешкодою масовому впровадженню мереж широкосмугового безпровідного доступу до Інтернет-ресурсів, що базуються на технології WIMAX, є ті труднощі, які виникають на фізичному рівні і є наслідком так званого "багатопроменевого режиму розповсюдження" в радіоканалі, що виникає в умовах "без прямої видимості" (non-line-of-sight), скорочено NLOS. З розглянутих вище результатів, можна зробити висновок, що система з просторово-частотним кодуванням спільно з кодами Ріда-Соломона і загортальними кодами при їх використанні в WIMAX PHY ефективно використовує розділення в часі, просторове розділення і розділення по частоті, пропоновані для каналів із завмираннями, і забезпечує високі параметри при низькому SNR.

Література

1. Широкополосные беспроводные сети передачи информации. Вишневський В.М., М: . Техносфера, 2005.
2. Цифровая связь. Б.Скляр. Москва, Санкт-Петербург, Киев, 2003.
3. http://www.softco.ru/80216.htm.

Надійшла до редакції
14.3.2011 р.

УДК 004: 004.65

О.Ю. ХМЕЛЬНИЦЬКИЙ
Хмельницький національний університет

УТОЧНЕННЯ ЗАГРОЗ ТА АНАЛІЗ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

В статті розглянуто принципи захисту інформації, що базуються на сучасних методах криптографії – які вирішують два головних питання: надійність і швидкодія. Розробка шифрів та програмного забезпечення, що відповідає цим умовам, знаходиться в центрі уваги дослідження. Головною причиною захисту інформації з використанням криптографії є здатність закриття конфіденційної інформації з певними гарантіями для її власника.

In the article the principles of information security, based on modern methods of cryptography – that solve two major issues: the reliability and performance. Development of codes and software that meets these conditions is the focus of research. The main prchynoyu protection using cryptography is the ability to close the confidential information with certain guarantees for its owner.

Ключові слова: криптографія, захист інформації.

Для більшості організацій захист мережевих ресурсів від несанкціонованого доступу на сьогодні стає однією з найгостріших проблем. Тривогу викликає той факт, що Internet в даний час використовується для транспортування і зберігання різних даних і конфіденційної корпоративної інформації. Такі побоювання є обгрунтованими, оскільки обмін даними переважно відбувається через відкриті базові мережі.

Існуючі методи захисту інформації базуються на сучасних методах криптографії – які повинні вирішити, в першу чергу, два головних питання: надійність і швидкодія. Розробка шифрів та програмного забезпечення, що відповідає цим умовам, знаходиться в центрі уваги багатьох досліджень [1]. Сильною стороною використання криптографії є здатність закриття конфіденційної інформації з певними гарантіями для її власника. Хоча цей напрям також має свої недоліки:

- труднощі розподілу зашифрованої інформації між декількома користувачами;
- накладні витрати від можливого зниження швидкості.

Фахівці в області захисту інформації пропонують розділяти систему безпеки на дві частини: внутрішню і зовнішню [1]. У внутрішній частині здійснюється, в основному, контроль доступу шляхом ідентифікації і аутентифікації користувачів при допуску в мережу і при доступі в базу даних. Крім цього шифруються і ідентифікуються дані під час їхньої передачі і зберігання. Безпека в зовнішній частині мережі в основному досягається криптографічними засобами.

По результатах проведених досліджень було визначено основні вразливі місця в мережевих системах [2]. Ними, як правило, є апаратура, інформаційний сервер, паролі і середовище передачі даних. Якщо інформаційний сервер може бути захищений організаційними заходами, то середовище передачі даних так не захистиш. Один із підходів захисту інформації за допомогою шифрування є використання спеціального програмного забезпечення. Стисло розглянемо деякі з них що з'явилися останнім часом.

Відома фірма RSA Data Security випустила нову версію популярного інструментального комплекту BSafe для мови програмування Internet-додатків Java. Новий продукт RSA, одержав назву Jsafe. За допомогою якого розробники зможуть вбудовувати в Java-додатки і аплети різні функції забезпечення безпеки, зокрема шифрування з відкритим і закритим ключем. JSafe функціонує на рівень нижче за Java-інтерфейс прикладного програмування Crypto API. Розробники можуть, таким чином, використовувати звичайний Crypto API, необхідно тільки вказати, що додаток повинен використовувати механізм криптозахисту JSafe. До складу JSafe входять алгоритми шифрування із закритим ключем RC2, RC4 і RC5, алгоритми формування сертифікатів цілісності повідомлень MD-5 і SHA-1, а також алгоритми хешування для формування цифрових підписів. Крім того, JSafe підтримує такі стандарти управління цифровими сертифікатами і обміну повідомленнями, як формат повідомлень PCKS#7 і алгоритм аналізу цифрових сертифікатів X.509.

Відомий інструментальний комплект JDK (Java Development Kit) версії 1.1 фірми JavaSoft надає лише обмежений набір таких засобів, включаючи шифрування на основі стандартних алгоритмів, проте він не підтримує методів шифрування з відкритим і закритим ключем. Саме ці методи складають основу сучасних засобів захищеної передачі даних по Internet, зокрема протоколу SSL (Secure Socket Level – захищений шар сокета).