УДК 004.732: 004.728

Дуднік А.С., к.т.н
Бондаренко Ю.В.

МЕТОД ЗАСТОСУВАННЯ ПРОТОКОЛУ БТР ДЛЯ НАДІЙНОСТІ ПЕРЕДАЧІ ДАНИХ БЕЗПРОВОДОВИХ КОМП'ЮТЕРНИХ МЕРЕЖ

Інститут комп'ютерних інформаційних технологій
Національний авіаційний університет

Безпроводові комп'ютерні мережі є відносно новим типом комп'ютерних систем, які використовуються в народному господарстві і в об'єктах спеціального призначення; вони характеризуються різнотипністю і великою щільністю інформаційного трафіку, що передається в умовах потужного потоку завад, неоднорідною структурою і великою кількістю інтегрованих мережевих засобів із недостатнім рівнем захисту інформації

Вступ

Особливістю об'єкта дослідження є протиріччя між високими вимогами до показників *QoS* на верхніх рівнях *EM OSI/ISO* і реально дуже обмеженими значеннями показників нижніх рівнів, які утворюють транспортну службу безпроводової комп'ютерної мережі.

Іншою особливістю безпроводових комп'ютерних мереж є обмеженість безпечному передаванні інформації, що обумовлено вимогою до їх мобільності.

Актуальність

Реальне значення продуктивності, спроможності підтримувати відповідні показники *QoS* безпроводової комп'ютерної мережі, залежить від вибраних стратегій (технологій) підготовки даних і передавання їх в радіоефірі. В разі вибору неефективної стратегії в мережі, щодо безпечної передачі даних, можлива втрата конфіденційності інформації і, як наслідок, все що трималося в таємниці і робилося секретно стає відомим для небажаних користувачів.

Класичні методи забезпечення безпеки передачі даних не є досконалими як і *EM OSI* .

Таким чином, тема даної роботи, присвяченої застосуванню протоколу БТР для надійності передачі даних безпроводових комп'ютерних мереж стандарту IEEE 802.11, є актуальною і являє собою науковий і практичний інтерес.

Об'єкт дослідження – технологія безпечного транспортування даних в комп'ютерних мережах і системах управління комп'ютерних мереж, побудованих на безпроводових технологіях та згідно з *EM OSI/ISO.*

Предмет дослідження – методи покращання надійності передавання даних в комп'ютерних мережах, побудованих на безпроводових технологіях і згідно з моделлю *OSI/ISO* за критерієм безпеки.

Методи досліджень. Методи, що основані на теорії безпеки передавання даних.

Мета

Метою даної статті є удосконалення технології безпроводового транспортування даних за рахунок перерозподілу, в рамках системи мережевого управління, функцій міжрівневої взаємодії в мережах, побудованих згідно з *EM OSI/ISO*, що дає змогу підвищити надійність *NMS* і мережі в цілому за рахунок скорочення кількості ітерацій перетворення даних.

Розробка методів підвищеної безпеки транспортування даних в мережах.

Розробка засобів підвищення безпеки системи транспортування даних в безпроводових комп'ютерних мережах можуть бути застосовані при модернізації апаратно-програмного забезпечення засобів управління мережею, а також відповідних систем операційної підтримки.

Запропонована, на основі розробленого в роботі методу, модель процесу ау-

тентифікації може підвищити надійність безпроводового передавання даних.

Постановка задачі

TCP/IP — це абревіатура терміну *Transmission Control Protocol/Internet Protocol* (Протокол керування передачею/міжмережевий протокол). Фактично *TCP/IP* не один протокол, а декілька. Саме тому його часто називають набором, або комплектом протоколів, серед яких *TCP* і *IP* — два основні. Фактично *TCP/IP* представляє цей базовий набір протоколів, відповідальний за розбивання вихідного повідомлення на пакети (*TCP*), доставку пакетів на вузол адресата (*IP*) і збирання (відновлення) вихідного повідомлення з пакетів (*TCP*).

TCP/IP — зародився в результаті досліджень, профінансованих Управлінням перспективних науково-дослідних розробок (*Advanced Research Project Agency, ARPA*) уряду США в 1970-х роках. Цей протокол був розроблений для того, щоб обчислювальні мережі дослідницьких центрів в усьому світі могли бути об'єднані у формі віртуальної «мережі мереж» (*Internetwork*). Первісна мережа Інтернет була створена в результаті перетворення існуючого конгломерату обчислювальних мереж, що носили назву *ARPAnet*, за допомогою *TCP/IP*.

Великий внесок у розвиток стеку протоколів *TCP/I*P, що одержав свою назву завдяки популярним протоколам *IP* і *TCP*, вніс університет Берклі, реалізувавши протоколи стека у своїй версії *OC UNIX*. Популярність цієї операційної системи привела до широкого поширення протоколів *TCP*, *IP* та інших протоколів стека. Сьогодні цей стек використовується для зв'язку комп'ютерів світової інформаційної мережі Інтернет, а також у багатьох корпоративних мережах.

Існують розбіжності у тому, як вписати модель *TCP*/*IP* в модель *OSI*, оскільки рівні в цих моделях не збігаються. До того ж, модель *OSI* не використовує додатковий рівень - «*Internetworking*» - між транспортним та мережевим рівнями. Прикладом спірного протоколу може бути *ARP* або *STP*. Ось як традиційно протоколи *TCP*/*IP* вписуються в модель OSI:

Прикладний: *HTTP, SMTP, SNMP, FTP, Telnet, SSH, SCP, SMB, NFS, RTSP, BGP*

Представлення: *XDR, AFP, ТРБ, SSL*

Сеансовий *ISO 8327/CCITT X.225, RPC, NetBIOS, PPTP, L2TP, ASP*

Транспортний : *TCP, UDP, SCTP, SPX, RTP, ATP, DCCP, GRE*

Мережевий *IP, ICMP, IGMP, CLNP, OSPF, RIP, IPX, DDP*

Канальний : *Ethernet, Token ring, HDLC, PPP, X.25, Frame relay, ISDN, ATM, MPLS.*

Фізичний електричні дроти, радіозв'язок, волоконно-оптичні дроти, інфрачервоне випромінювання

Прикладний: *HTTP, RTP, FTP, DNS*

Транспортний: *TCP, UDP, SCTP, DCCP (RIP*, протоколи маршрутизації, подібні *OSPF*, що працюють по верх *IP*, є частиною мережевого рівня)

Мережевий: для *TCP*/*IP* це *IP* (допоміжні протоколи, на зразок *ICMP* і *IGMP*, працюють поверх *IP*, але теж відносяться до мережевого рівня; протокол *ARP* є самостійним допоміжним протоколом, працюючим поверх канального рівня)

Канальний *Ethernet*, *IEEE* 802.11 *Wireless Ethernet, SLIP, Token Ring, ATM і MPLS*, фізичне середовище і принципи кодування інформації, *T1*, *E1*

Розв'язання задачі

На сьогоднішній день стає очевидним, що, незважаючи на всі проблеми, пов'язані с безпекою, надійністю і складністю експлуатації, бездротові рішення сімейства 802.*11a/b/g* все ж стали невід'ємною частиною інфраструктури багатьох корпоративних, домашніх і навіть операторських мереж. Частково це відбулося, тому що більшість цих проблем на сучасному етапі розвитку *Wi-Fi* пішли в минуле. Бездротові мережі у всіх відносинах стали набагато розумніші і швидше: з'явився *QoS*, інтелектуальні антени (технологія *MIMO*), реальні швидкості досягли 40 Мбіт / с (наприклад, технології *SuperG*,

SuperAG від *Atheros*). Крім цього, великі зміни відбулися і в наборі технологій, що забезпечують безпеку бездротових мереж. Про це поговоримо більш докладно.

У часи, коли *Wi-Fi* був тільки для обраних, для захисту бездротових мереж використовувалося *WEP*-шифрування і *MAC*-фільтри. Всього цього швидко стало не вистачати, *WEP* визнали небезпечним через статичності ключів шифрування і відсутності механізмів аутентифікації, *MAC*-фільтри особливої безпеки теж не надавали. Почалася розробка нового стандарту *IEEE* 802.11i, який був покликаний вирішити всі назрілі проблеми безпеки. На півдорозі до 802.11i з'явився набір технологій під загальною назвою *WPA* (*Wi-Fi Protected Access*) - частина ще не готового стандарту 802.11i. *WPA* включає в себе засоби для аутентифікації користувачів, шифрування за допомогою динамічних *WEP*-ключів (*TKIP/MIC*). Потім 802.11i нарешті закінчили, і на світ з'явився *WPA2*. До всього вищепереліченого додалася підтримка більш стійкого шифрування *AES* (*Advanced Encryption Standard*), яке працює спільно з протоколом безпеки *CCMP* (*Counter with Cipher Block Chaining Message Authentication Code Protocol* - це більш досконалий аналог *TKIP* в *WPA*). *WPA2* поступово став з'являтися в нових моделях точок доступу (наприклад, *D-Link DWL-3200AP*), але поки це скоріше екзотика. Всі продукти, що підтримують *WPA2*, назад сумісні з устаткуванням, що підтримує *WPA*.

І *WPA*, і *WPA2* включають в себе розвинені засоби контролю доступу до бездротової мережі на основі стандарту *IEEE* 802.1x. В архітектурі 802.1x використовується кілька обов'язкових логічних елементів:

n Клієнт. У ролі клієнта виступає *Supplicant*-програма на клієнтському комп'ютері керуюча процесом аутентифікації.

n Аутентифікатор. Це точка доступу, яка виконує функції посередника між клієнтом і сервером аутентифікації. Аутентифікатором в тому числі може бути і провідний комутатор, тому 802.1x використовується в різних мережах.

n Сервер аутентифікації - *RADIUS*-сервер.

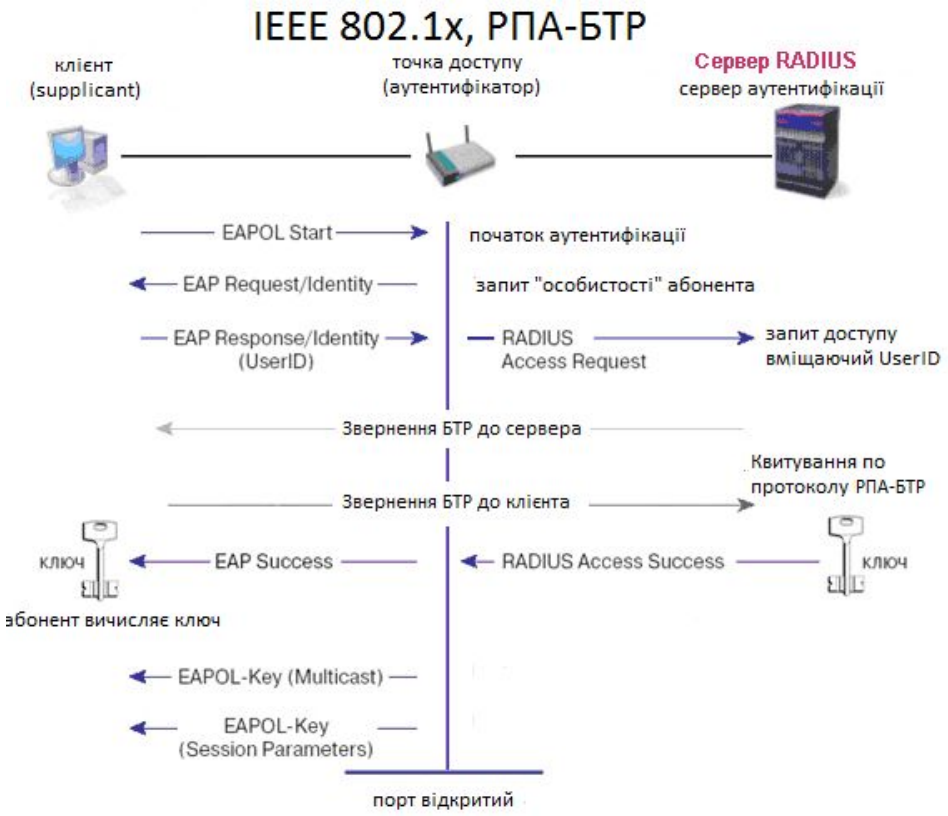

Рис.1. Процес аутентифікації 802.1x РПА-ТРБ.

У IEEE 802.1x допускається використання різних методів і алгоритмів аутентифікації. Це можливо завдяки протоколу *EAP (Extensible Authentication Protocol)*, в який «вкладаються» атрибути, відповідні тому чи іншому методу аутентифікації. Тому існує багато різновидів 802.1x *EAP: EAP-MD5, EAP-PEAP, EAP-LEAP, EAP-SIM* і т. д. Далі буде описана реалізація аутентифікації в бездротовій мережі на основі цифрових сертифікатів - 802.1x РПА-ТРБ. Цей метод найбільш часто використовується в корпоративних бездротових мережах і відрізняється досить високим ступенем захищеності. Крім того, РПА-ТРБ іноді є одним з основних методів захисту в мережах бездротових провайдерів. Аутентифікація 802.1x РПА-ТРБ

В основі РПА-ТРБ лежить протокол *SSL* v3.0, проте на відміну від традиційної аутентифікації по протоколу *SSL* (наприклад, при організації захищеного http-з'єднання - *HTTPS*) в РПА-ТРБ відбувається взаємна аутентифікація клієнта і сервера. Клієнт (суплікант) і сервер *RADIUS* повинні підтримувати метод аутентифікації РПА-ТРБ; точка доступу повинна підтримувати аутентифікацію 802.1x/*EAP* і не обов'язково повинна знати, який метод аутентифікації використовується в конкретному випадку. На рис.1 зображено процес аутентифікації в бездротовій мережі з використанням РПА-ТРБ.

Тут доречно закінчити невелике лірично-теоретичне відступ, який необхідно, для того щоб отримати приблизне уявлення про те, що криється в надрах безпечної безпровідної мережі. Далі буде запропонована практична реалізація описаних вище концепцій. В якості сервера *RADIUS* буде використовуватися комп'ютер під управлінням *FreeBSD* 5.3 с пакетом *FreeRADIUS*. Для організації інфраструктури *PKI* (*Public Key Infrastructure*) буде застосований пакет *OpenSSL*. Вся бездротова мережа буде будуватися на базі недорогого і надійного бездротового обладнання *D-Link*. Передбачається, що на клієнтських машинах встановлена *Windows XP SP2*, тому в цій операційній системі є вбудований суплікант, а нещодавно випущений корпорацією *Microsoft update* додає і підтримку *WPA2*.

Висновки

Удосконалено технологію безпроводового транспортування даних за рахунок перерозподілу, в рамках системи мережевого управління, функцій міжрівневої взаємодії в мережах, побудованих згідно з *EM OSI/ISO*, що дає змогу підвищити надійність *NMS* і мережі в цілому за рахунок скорочення кількості ітерацій перетворення даних.

Проведено порівняльний аналіз моделі *OSI* та протоколу *TSP/IP*. Розглянуто розбіжності того, як вписати стек протоколів *TSP/IP* в модель *OSI*.

Запропонована, на основі розробленого в роботі методу, модель процесу аутентифікації може підвищити надійність безпроводового передавання даних.

Список літератури

1. Олифер В.Г. Компьютерные сети / В.Г. Олифер, Н.А. Олифер – С -Пб.: Питер Пресс, 2008. – 957 с.

2. Педжман Р. Основы построения беспроводных локальных сетей стандарта 802.11 / Р. Педжман, Л. Джонатан – М.: Издательский дом «Вильямс», 2004. – 304 с.

Статтю подано до редакції 5.09.2013