УДК 681.3, 004.45
Новак Д.В., Березко Л. О.
Національний університет "Львівська політехніка"
кафедра електронних обчислювальних машин

Системне програмне забезпечення мобільних мереж

Розглянуто проблему вразливості до атак з боку зловмисників при передачі даних через безкабельні мережі. Розглянуто існуючі способи захисту мереж та їх недоліки. Запропоновано рішення для забезпечення додаткового захисту мережі.

Ключові слова: безкабельні мережі, вразливості, шифрування.

The problem of vulnerability to attacks by malefactors when transmitting data over wireless networks is considered. The existing methods of network protection and their shortcomings are considered. A solution for additional network protection is proposed.

Keywords: wireless networks, vulnerabilities, encryption.

Вступ. В наш час безкабельні мережі набувають все більшого застосування. З кожним роком відсоток безкабельних мереж відносно кабельних збільшується і це буде продовжуватися й надалі. Безумовний плюс безкабельних мереж, таких як Wi-Fi або стільникових - це відсутність великої кількості кабелів, що є дуже зручно для користувачів.

Технологія Wi-Fi це безкабельний аналог стандарту Ethernet. Щоб задовільнити потреби користувачів в зручному доступі до інтернету точки доступу Wi-Fi зараз розміщені повсюди, в кафе, ресторанах, піцеріях, готелях, тощо. Зі збільшенням швидкості передачі даних мобільних мереж при введені стандартів 3G, 4G значно збільшилося й навантаження на них. Тому зараз велике розповсюдження Wi-Fi мереж допомагає зменшити навантаження на мережі стільникового зв'язку, що також є безумовним плюсом.

Але, на жаль, таке велике розповсюдження точок доступу Wi-Fi, до якої може під'єднатися ледь не кожен охочий викликає проблему захисту особистих даних при використанні Wi-Fi мереж. Зловмисники не втрачають можливості викрасти особисті дані, які будуть не достатньо захищені при передачі через мережу. В даній роботі розглядається рішення для забезпечення безпеки Wi-Fi мережі від втручання зловмисників. [1 - 3]

Стан проблеми. Публічні точки Wi-Fi не можуть гарантувати безпеку передачі даних, адже доступ до них має велика кількість людей. Часто вони навіть не мають паролів, що дозволяє підключитися до них буквально будь-кому бажаючому. Ще одним недоліком є те, що на відміну від кабельних мереж, де для того, щоб отримати доступ до трафіку потрібно фізично підключитися до них, безкабельні мережі передають дані у вигляді радіосигналів, перехопити які здатен кожний, хто знаходиться в зоні поширення сигналу. І якщо звичайний користувач відкидає весь трафік, який не призначений для нього зловмисник може отримати і той трафік, який для нього не призначений. [4, 5]

Ще одним способом доступу до особистих даних є підроблені точки доступу. Зловмисник дізнається інформацію про точку доступу, до якої буде підключатися клієнт. І після цього створює свою, підроблену, яка повністю копіює оригінальну.

Мережі, захищені за протоколом WEP не є захищеними також, адже вони використовують загальний ключ, який зловмисник здатен швидко підібрати перехопивши, декілька пакетів. Мережі захищені за протоколами WPA/WPA2 є безпечнішими, але все ж підлягають злому. Недоліком WPA є використання застарілого стандарту шифрування TKIP, а сам протокол був тимчасовою заміною для погано захищеного WEP. WPA2 в свою чергу не дає вам потрібного захисту, якщо зловмисник вже потрапив у вашу мережу. Часто власники не дуже переймаються паролем і він або дуже простий і швидко підбирається, або легко доступний. Тому для забезпечення безпечного користування мережею є важливою проблемою. [6]

Постановка задачі. Розробити програмне забезпечення додаткового захисту мережі від атак з боку зловмисників, що допоможе запобігти втрати особистих даних користувачами під'єднаних до точки доступу. Описати алгоритм роботи системи.

Розв'язання задачі. Для здійснення процесу ідентифікації до точки доступу запропоновано застосувати алгоритм шифрування повідомлень клієнта ключем відкритого типу. Це рішення допоможе вирішити проблему довіри до точки доступу за допомогою цифрових підписів. Електронний підпис створюється за допомогою закритого ключа, а її перевірка виконується відповідним відкритим ключем. Багато протоколів захисту, які забезпечують ідентифікацію, забезпечують проведення ідентифікації лише між клієнтом мережі та власне самою мережею. Тоді, зловмисник намагається під'єднати клієнта до своєї, підробленої точки доступу.

Якщо сигнал цієї точки буде кращим ніж в оригінальної і клієнт не замітить підміни, то у випадку підключення до неї всі дані користувача надходять прямо в руки зловмиснику при цьому користувач може навіть нічого не запідозрити. Адже якщо він вже раніше підключався до цієї точки і в нього не виникало жодних проблем то і на цей раз він повністю їй довіряє. [7, 8]

Для розв'язання задачі проблеми підроблених точок доступу, необхідно гарантувати, що клієнт буде здатен визначити чи точка доступу, до якої він намагається під'єднатися є довіреною та безпечною.

З іншого боку потрібно також переконатися, що зловмисник не проникне в мережу, адже проникнувши "в середину" йому буде набагато легше отримати конфіденційну інформацію, навіть якщо використовується протокол захисту WPA2.

Для розв'язання цієї задачі необхідно гарантувати, що для доступу в мережу клієнт має пройти процес автентифікації. І точка доступу має засвідчитись в справжності клієнта. Для цього пропонується використовувати тимчасові одноразові паролі, які будуть генеруватися на основі певного параметру і мають бути доступні лише довіреному клієнту.

Така комбінація захисту дозволить встановити додатковий шар захисту, який реалізує взаємну перевірку на справжність клієнта та точки доступу. Це гарантує не лише безпеку певного клієнта при підключені, а й безпеку інших клієнтів мережі, не дозволяючи зловмиснику проникнути в мережу.

При використанні криптографії з відкритим ключем (або асиметричної криптографії) використовується пара ключів: один ключ є відкритим (публічним), інший - закритим (приватним). В таких системах для зашифровування даних використовують один ключ, а для розшифровування - інший (звідси і назва - асиметричні). Перший ключ є відкритим і може бути опублікованим для використання усіма користувачами системи, які шифрують дані. Розшифровування даних за допомогою відкритого ключа неможливе. Для розшифровування даних отримувач зашифрованої інформації використовує другий ключ, який є секретним (закритим). Зрозуміло, що ключ розшифровування не може бути визначеним з ключа зашифровування. [9, 10]

Закритий ключ ніколи не передається по каналу зв'язку, адже його передача призведе до втрати довіри до такої системи. Відритий же ключ, навпаки, передається вільно. Головне досягнення асиметричного шифрування в тому, що воно дозволяє людям, що не мають наперед наявної домовленості про безпеку, обмінюватися секретними повідомленнями. Алгоритм роботи системи відображено на рис. 1.

Алгоритм роботи клієнтів з точками доступу є наступним:

1. Клієнт обирає точку доступу, яку він вважає довіреною.
2. Клієнт отримує відкритий ключ даної точки доступу і запам'ятовує його.
3. При наступному підключенні до цієї точки доступу, перед тим як починати передачу даних відбувається перевірка її оригінальності:
   - клієнт надсилає довільну послідовність байт точці доступу;
   - точка доступу підписує дану послідовність байтів своїм закритим ключем і надсилає назад клієнту;
   - клієнт перевіряє отриманий підпис за допомогою відкритого ключа.
4. У разі, якщо отриманий підпис не вірний відбувається розірвання з'єднання через недовіру до точки доступу.
5. При успішному підтвердженні точки доступу, вона в свою чергу розпочинає процедуру перевірки клієнта.

6. Клієнт на основі певних токенів, які його ідентифікують генерує тимчасовий пароль, який і використовує для підтвердження своєї справжності.

7. Якщо пароль вірний відбувається встановлення з’єднання з точкою доступу, в іншому випадку – ні.

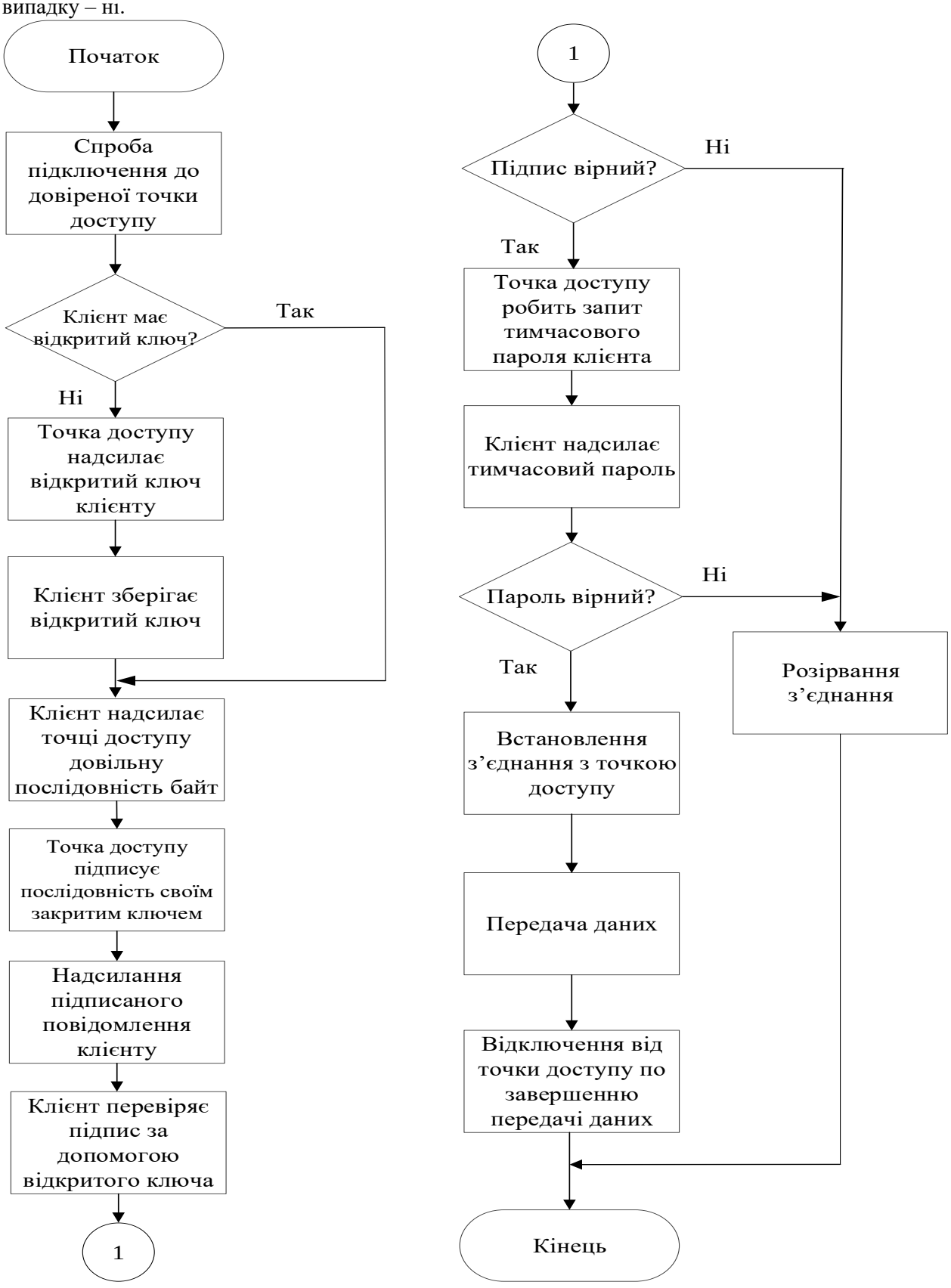

Рис. 1. Алгоритм роботи системи

Висновки. В результаті виконання даної роботи було розроблене програмне забезпечення для додаткового захисту мережі від атак з боку зловмисників, яке допомагає запобігти втрати особистих даних переданих через мережу, використовуючи взаємну перевірку на справжність клієнта та точки доступу. Було описано алгоритм роботи системи.

Література

1. Stewart S. Miller, Wi-fi Security, 2003.
2. Щербаков В.Б., Ермаков С.А. «Безопасность беспроводных сетей: стандарт IEEE 802.11». - М: РадиоСофт, 2010, - 255 с.
3. Пролетарский А.В., Баскаков И.В., Чирков Д.Н. «Беспроводные сети Wi-Fi». - М:Бином. Лаборатория знаний, 2007, - 178 с.
4. О. Юдін, Г. Конахович, О. Корченко, Захист інформації в мережах передачі даних: підруч. К.: Вид-во ТОВ НВП “ІНТЕРСЕРВІС”, 2009 - 714 с.
5. Kevin Beaver; Peter T. Davis; Devin K. Akin. Hacking Wireless Networks For Dummies, 2011 - p. 295.
6. Meyers, Mike. Managing and Troubleshooting Networks. Network+. McGraw Hill, 2004 – p. 800
7. Vanhoef, Mathy; Piessens, Frank. "Advanced Wi-Fi Attacks Using Commodity Hardware", 2014.
8. Vanhoef, Mathy; Piessens, Frank. "Predicting, Decrypting, and Abusing WPA2/802.11 Group Keys", 2016.
9. William Stallings. Cryptography and Network Security Principles and Practices, Fourth Edition, 2005 - p. 592
10. Robert Collins. Network Security Monitoring: Basics for Beginners. A Practical Guide Paperback, 2017.