УДК 004.056.5

АНАЛІЗ ЦІЛЕЙ АТАК НАМЕРЕЖІ МОБІЛЬНОГО ЗВ'ЯЗКУ СТАНДАРТУLTE З ІНТЕГРОВАНИМИ ФЕМТОСОТАМИ

Нікітенко К.О.

Кухарська Н.П., ЛДУ БЖД, доцент, канд. фіз.-мат. наук

ЛДУ БЖД

Ринок мобільного зв'язку на даний час перебуває у стані радикальних змін, зумовлених стрімким ростом попиту з боку абонентів на комплексні мультимедійні послуги. На сьогоднішній день мільйони пристроїв підключені до Інтернету і хмарних технологій з використанням 4G і LTE мереж рухомого радіотелефонного зв'язку. Проте з високим рівнем урбанізації стільниковий зв'язок у певних точках не може задовольнити всіх потреб користувача. У зв'язку з цим постає питання про надання якісного каналу зв'язку в будь-якому місці. Одним з ефективних варіантів вирішення цієї проблеми є використання інтегрованих фемтосот(ІФ) для створення локальної мережі передачі даних в межах приміщення– інноваційної технології поліпшення якості зв'язку, що використовує у ролі транспорту протокол IP. У зв'язку з цим, забезпечення конфіденційності, цілісності та доступності циркулюючої в фемтосотах інформації, єодним з найбільш важливих аспектів для користувачів пристроїв з підтримкою стільникових систем мобільного зв'язку(ССМЗ) нового покоління.

При проведенні атак на стільникові мережі характерна така послідовність дій [1]:

1. вивчення мережі і її зони покриття;
2. планування методики огляду місця розгортання і проведення атаки;
3. збір, підготовка та конфігурація обладнання та програмного забезпечення, необхідних для виконання запланованих дій;
4. огляд місця розгортання мережі, визначення її кордонів і рівня сигналу уздовж периметра;
5. аналіз трафіку в мережі і подолання виявлених заходів протидії;
6. підключення до мережі та аналіз її структури;
7. пасивний аналіз трафіку від хостів і оцінка безпеки протоколів, використовуваних в мережі;
8. проведення активних атак проти абонентів, що представляють інтерес.

Розглянемо основні цілі атак як джерела загрози інформаційної безпеки ССМЗ стандарту LTE з ІФ. На рис. 1 стрілками позначені три вразливі елементи: (а) повітряний інтерфейс між мобільним пристроєм (UE) і фемтостільниковою базовою станцією (БС); (Б) безпосередньо фемтос-

тільникова базова станція (БС) (H(e)NB); (В) широкосмугове з'єднання між фемтосотою і шлюзом безпеки (SecGW).

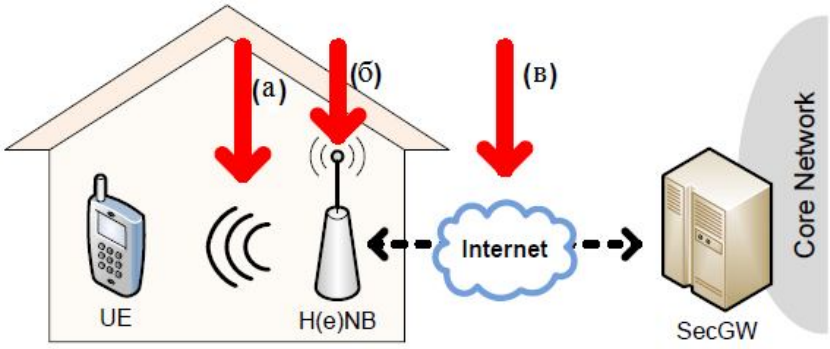

Рис. 1. Цілі атакзловмисників на стільникові мережі з ІФ

Атаки на повітряний інтерфейс. У пасивному варіанті зловмисник прослуховує канал зв'язку між мобільним пристроєм і базовою станцією; в активному – на додачу до прослуховування, зловмисник здійснює несанкціонований впливна вже циркулюючий трафік. Щоправда, можливості активних атак істотно знижені за рахунок застосування криптографічного захисту інформації, яка передається. Позаяк, пасивні атаки, такі як аналіз трафіку і відстеження місця розташування користувачів, все ще можливі[2].

*Атаки на фемтостільникові базові станції.*З точки зору зловмисника фемтосоти відкривають нові можливості для реалізації деструктивних впливів. Наприклад, зловмисникові набагато легше отримати доступ до фемтосоти розташованої в приміщенні, ніж до БС розташованої на даху. Фізичний розмір, якість матеріалів, більш дешеві компоненти і IP-інтерфейс фемтосоти роблять її більш вразливою для атак зворотного проектування і несанкціонованого доступу, в порівнянні з традиційними, дорожчими і висококласними БС. Оскільки шифрування даних користувача, що транслюються через ефір, припиняється на рівні фемтосоти, апаратне втручання в пристрій дає змогу розкрити конфіденційну інформацію користувача, який нічого не запідозрить. Наприклад, якщо зловмисник деактивує систему ClosedSubscriberGroup (CSG) і тим самим змусить фемтосоти приймати всіх зовнішніх користувачів без необхідності попередньої реєстрації, то він отримає можливість несанкціоновано аналізувати їх трафік. Крім того, атаки на кшталт підміна довіреного об'єкта, атаки на мережеві служби з використанням протоколів Інтернет, атаки-повідомлення помилкового позиціонування або атаки несанкціонованої переконфігурації радіоапаратури ускладнюють оператору мобільного зв'язку процес управління інтерференцією і засобами контролю живлення, що несприятливо позначиться на якості обслуговування[3].

Атаки на опорну широкосмугову мережу. Витік інформації про точку доступу ядра мережі в мережу Інтернет має серйозні наслідки: це провокує велику кількість мережевих атак на операторів стільникового мережі мобільного зв'язку, таких як відмова в обслуговуванні (DoS) або підміна довіреного об'єкта.

ЛІТЕРАТУРА

1. Елисеев Н. Фемтосоты в мобильной связи – преимущества и решения [Электронный ресурс] / Н. Елисеев // Первая миля. Выпуск #2/2007. – Режим доступа : http://www.lastmile.su/journal/article/2154.
2. Borgaonkar R., Redon K., and J. Seifert. Security analysis of a femtocell de-vice. In Proceedings of the 4th international conference on Security of information and networks, SIN ’11, ACM, 2011. – pp.95–102.
3. Shwetha H.K, Prof. D. Jayaramaiah Study and Analysis of Security Issues in Next Generation Mobile Network // International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 4, Jul-Aug 2013. – pp.942-946.