УДК 681.3

М. Карпінський, Р. Трембач, У. Трач

Тернопільський національний економічний університет

ОРГАНІЗАЦІЯ СИСТЕМИ ЗАХИСТУ БЕЗПРОВІДНОЇ СЕНСОРНОЇ МЕРЕЖІ ВІД АТАК ТИПУ SYBIL

Можливості використання бездротових мереж практично безмежні. Вони можуть використовуватися в багатьох областях. Динамічний розвиток сенсорних мереж в останні роки став можливим завдяки значному прогресу в області бездротового зв'язку, а також розробки ефективних електронних системи (процесори, пам'ять, перетворювачі).

Через розташування сенсорної мережі на великих площах, вона піддаються впливу багатьох ризиків. Ці ризики можуть бути пов'язані з різними впливами, такими як сильний сигнал радіо чи вогонь, і свідомі дії людей, які намагаються незаконно підслуховувати або видавати себе за користувача.

Для використання бездротових сенсорних мереж необхідно вжити заходів, щоб захистити їх щодо потенційних загроз.

Метою цього дослідження є опис різних форм атак Sybil та огляд існуючих алгоритмів для виявлення і нейтралізації цих нападів.

Кожен з методів захисту від атак Sybil, має різні взаємозамінні особливості[1-2]. Більшість з методів не в змозі захистити нас від будь-якого виду атаки Sybil.Методи захисту перевірки радіо ресурсів можна реалізувати за допомогою користувальницького пристрою для прийому /передачі радіохвиль, а також з точки зору споживання енергії. Перевірка позиції може тільки обмежити число вузлів атаки, а зловмисник не в стані визначити положення вузола з дуже високою точністю. Реєстрація вузла вимагає людської праці, додавати вузли в мережі, а також необхідність підтримки безпечної роботи вузла та посилання запитів, що стосуються інформації про топологію. Ми вважаємо, що метод захисту, представлені випадковим розподілом ключів, є найбільш перспективним. Дана технологія може бути використана у якості ефективного засобу від атак типу Sybil без додаткових витрат. Попередній випадковий розподіл ключів буде використовуватися в багатьох схемах для створення захищеного зв'язку, з тієї причини, що це принципи криптографії. Ці принципи є ефективними для випадку вразливих вузлів. Зокрема, використання багатопросторової схеми розподілу ключів довело свої переваги, коли кожен з вузлів може мати 200 ключів. Зловмисникові необхідно передати більше 400 вузлів, перш ніж він буде мати принаймні 5% можливості ввести нові тотожності для використання в атаці Sybil.

Наступним важливим кроком є безпечні методи непрямого контролю, коли мережа не буде мати центральної робочої станції. Це дозволить використання методів прямої перевірки, що можна зробити з однієї станції, так як методи захисту ресурсів будуть застосовуватися для непрямої перевірки.

Література

1 H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In IEEE Symposium on Security and Privacy, May 2003.

2 B. S. Manoj, R. Ananthapadmanabha, and C. Siva Ram Murthy. Multi-hop cellular networks: architecture and protocols for best-effort and real-time communication. J. Parallel Distrib. Comput., 65(6):767–791, 2005.