д.т.н. Романюк В.А. (ВІТІ)
Веремійчук В.Є (ВІТІ)

АНАЛІЗ DoS АТАК НА БЕЗПРОВІДНІ СЕНСОРНІ МЕРЕЖІ

Розглянуто особливості побудови та функціонування безпровідних сенсорних мереж (БСМ) військового призначення: значна розмірність (сотні, тисячі вузлів), обмеженість ресурсів вузлів (енергії батареї, продуктивності процесора, пам'яті, потужності передавача, пропускної спроможності радіоканалу тощо), концентрація трафіка навколо шлюзу, використання радіо середовища тощо. Визначено їх вплив на захищеність БСМ, на реалізацію захисних механізмів та протоколів, на ефективність та специфіку атак на дані мережі.

Визначені основні впливи DoS атак: порушення функціонування всієї мережі або її частини, зниження продуктивності мережі (за рахунок збільшення кількості спам-повідомлень, перенаправлення трафіка, тощо), збільшення часу передачі або втрата пакетів і їх підтверджень, підвищення витрат ресурсів вузлів тощо.

Розглядаються методи DoS атак на безпровідні сенсорні мережі, проведена класифікація даних атак по рівню стеку протоколів OSI на які проводиться атака (табл. 1).

Таблиця 1

Рівень OSI	**DoS атака**
Фізичний	Jamming, Interference, Node tampering and destruction
Канальний	Collision, Exhaustion, Unfairness
Мережевий	Sybil, Selective forwarding, Sinkhole, Hello flooding
Транспортний	Flooding, Desynchronization
Прикладний	Overwhelming sensors or sensor overload, Path based attack

Атаки фізичного рівня направлені на перешкоджання передачі, глушіння сигналу чи створення завад, які перешкоджають передачі пакетів, також, знищення чи перезапис керуючої інформації вузла через прямий фізичний доступ до вузла.

DoS-атаки на канальному рівні використовують недоліки механізмів підключення та розподілу канального ресурсу при передачі пакетів для втручання в роботу мережі.

Атаки на мережевому рівні відбуваються шляхом оперування даними полів пакетів, фальсифікації маршрутної інформації та, як правило, направлені на порушення структури сенсорної мережі, створення помилкових маршрутів передачі, втрату інформації що передається між вузлами, створення масштабних збоїв у роботі системи.

Атаки на транспортному та прикладному рівні, я правило, направленні на збільшення енерговитрат системи.

Проведена оцінка небезпеки даних атак, на які вразливості системи вони направлені, зазначено потенційні наслідки проведення атаки. Розглянуто механізми, заходи та протоколи які дозволяють послабити, завадити або запобігти даним атакам, запропоновано нові методи які дозволяють ускладнити деякі типи атак на безпровідні сенсорні мережі, або повністю запобігти їм.

Захист та запобігання визначеним атакам пропонується здійснювати за допомогою протоколів шифрування або встановлення граничних обмежень на прийом, передачу повідомлень, час роботи вузла чи тривалість з'єднання. Оскільки найбільш захищені протоколи шифрування вимагають досить високих енергозатрат, в безпровідних сенсорних мережах перевага надається більш простим протоколам, які забезпечують відносну безпеку, проте, витрачають менше енергії при роботі, а недостача криптографічного потенціалу компенсується організаторськими методами, які дозволяють ускладнити атаку чи зменшити її вплив, тим самим підвищуючи ефективність інших протоколів захисту.