УДК 004.75

[1]В.В. Мостовий, [2]О.В. Понедільник, [2]І.М. Пастушок
[1]Тернопільський національний економічний університет, Україна
[2]Ковельський промислово-економічний коледж Луцького НТУ, Україна

ЗАХИСТ БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖ ВІД АТАК

V.V. Mostovyy, O.V. Ponedilnyk, I.M. Pastushok

PROTECTION OF WIRELESS SENSOR NETWORKS AGAINST ATTACKS

На сьогодні багато систем моніторингу і управління різними об’єктами реалізуються на основі безпровідних сенсорних мереж (БСМ) і можуть бути використані для таких об’єктів як: будівлі, споруди, автомобільний рух, медичні показники здоров’я людини, природні ресурси, військова галузь і т. д.

БСМ є принципово новим типом безпровідних мереж, які будуються на основі необмеженої кількості невеликих датчиків з обмеженим зарядом батареї, призначених для збору інформації і контролю об’єктів [1].

БСМ вразливі до великої кількості пасивних і активних атак [2, 3]. Пасивні атаки, як правило, здійснюються зовнішнім зловмисником і направлені на перехоплення або відстеження мережевого трафіку. Основна кількість атак здійснюється на мережевому рівні, тому при розробці засобів захисту БСМ необхідно враховувати цю особливість. Крім цього, рішення в області забезпечення безпеки у БСМ має бути енергоефективним. Під цією вимогою розуміється те, що вузол не повинен виконувати складних обчислень, а також необхідно скоротити часові і енергетичні витрати на обмін повідомленнями.

При розробці системи управління захистом для БСМ, однією з основних задач є забезпечення захисту центрального вузла, як ключового об’єкту мережі, який забезпечує передачу повідомлень як всередині кластера, так і за його межами. Для цього необхідно контролювати роботу головного вузла кластера як з рівними в ієрархії вузлами, так і вищестоящим вузлом. Більшість підходів до визначення довіри заснована на оцінці кількості успішних і неуспішних подій вузла, що не дозволяє робити протидію таким атакам, як відмова в обслуговуванні, затоплення, і т. п. Отже, необхідно розширити спектр атак, яким здатна протистояти захищена мережа. Крім того, БСМ має властивості розширюваності і мобільності вузлів, отже, необхідно забезпечити захист мережі на етапі зміни конфігурації і додавання нових вузлів в мережу, при цьому захист не повинен істотно ускладнювати роботу мережі.

Перспективним напрямом забезпечення захисту безпровідних сенсорних мереж є використання штучних нейронних мереж [4], які добре себе зарекомендували при побудові систем захисту від комп’ютерних атак.

Література

1. Бойко Ю.М. Концептуальні особливості реалізації безпровідних сенсорних мереж / Ю.М. Бойко, В.М. Локазюк, В.В. Мішан // Вісник Хмельницького національного університету. – 2010. – № 2. – С. 94–97.

2. Kalaiselvan K., Gurpreet Singh. Detection and Isolation of Black Hole Attack in Wireless Sensor Networks // International Journal of Innovative Research in Science, Engineering and Technology. – 2015. – Vol. 4, Issue 5. – P. 23–31.

3. Mosmi Tiwari, Jitendra Choudhary. Study of Wormhole Attack in Wireless Sensor Networks // International Journal of Computer Application. – 2015. –Vol. 5, Issue 4. – P. 1–5.

4. Komar M., Sachenko A., Bezobrazov S., Golovko V. Intelligent Cyber Defense System Using Artificial Neural Network and Immune System Techniques // Communications in Computer and Information Science. – 2017. – Vol. 783. – P. 36-55.