УДК 004.056
DOI: 10.31673/2409-7292.2021.045963

Жуковський П.С.

АНАЛІЗ УРАЗЛИВОСТЕЙ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

В роботі проведено аналіз проблеми забезпечення кібербезпеки бездротових сенсорних мереж, визначено мету та завдання управління захистом бездротових сенсорних мереж. Визначено мету безпеки сенсорних мереж. Проведено аналіз уразливостей бездротових сенсорних мереж. На основі досліджень проведених в роботі розроблено рекомендації щодо застосування технології управління їх захистом на підприємстві.

Ключові слова: кібербезпека, бездротова сенсорна мережа, методи та засоби управління захистом кінцевих точок, технологія управління захистом комп'ютерної мережі.

Вступ

Бездротова сенсорна мережа (БСМ) є новою технологією для досліджень, оскільки мережа датчиків обробки – це група недорогих сенсорних вузлів, що самоорганізуються, яка створює мережу спонтанно. БСМ поєднує у собі вимірювання, обчислення та комунікації в одному маленькому пристрої під назвою вузол датчика (Sensor Node). Він в основному містить батареї, радіо, мікроконтролер та силові пристрої. Датчики у вузлі дають можливість отримувати дані, такі як температура, тиск, світло, рух, звук тощо. та здатні виконувати обробку даних. Основна мета додатків досягається завдяки взаємодії всіх сенсорних вузлів у мережах безпеки. Існує безліч сенсорних мережевих додатків, таких як моніторинг безпеки, збирання даних про навколишнє середовище, медична наука, військова техніка, стеження та ін.

Безпека стає надзвичайно важливим фактором, коли сенсорні мережі безладно розгортаються у ворожому середовищі. БСМ є передовою мережевою технологією, вона суттєво відрізняється від традиційних бездротових мереж. Це пов'язано з унікальними характеристиками датчиків вузлів БСМ. Таким чином, існуючі механізми безпеки традиційних бездротових мереж не застосовуються безпосередньо до БСМ. Мережі датчиків тісно взаємодіють із фізичним середовищем. Вузли датчиків також розгорнуті у тих областях, де атаки фізично доступні, і передають чутливі дані у мережі. Ця причина вимагає використання нових механізмів безпеки, існуючі традиційні механізми безпеки в БСМ обмежені застосування. Основне завдання полягає в тому, щоб розгорнути методи шифрування або їх аналоги в сенсорній мережі, що характеризується обмеженою пам'яттю, потужністю та можливістю обробки.

Мета роботи – розробка програмного засобу визначення атак на бездротову сенсорну мережу на основі штучної нейронної мережі.

Мета безпеки для сенсорних мереж. Сенсорна мережа - це особливий тип мережі, хоч і має деякі спільні властивості з комп'ютерною мережею (рис. 1). Зазвичай для захисту мережі потрібні кілька вимог безпеки. Ці вимоги повинні враховуватись при розробці протоколу безпеки, включаючи конфіденційність, цілісність та достовірність. Ефективний протокол безпеки повинен надавати послуги, щоб задовольнити ці вимоги.

Вимоги безпеки бездротової мережі датчиків можна класифікувати так:

Конфіденційність даних. Конфіденційність даних є найважливішою проблемою мережевої безпеки. Кожна мережа з будь-яким рівнем безпеки вирішуватиме цю проблему насамперед. У мережах датчиків конфіденційність належить до наступного: мережа датчиків має пропускати показання датчиків сусіднім абонентам. У військовій програмі дані, що зберігаються у вузлі датчика, можуть бути дуже чутливі. Багато додатках вузли пов'язують високочутливі дані, наприклад, розподіл ключів; тому надзвичайно важливо створити безпечний канал у бездротовій сенсорній мережі. Інформація про відкритий датчик, така як ідентифікатори датчиків та відкриті ключі, також має бути зашифрована певною мірою для захисту від атак з аналізом трафіку.

Цілісність даних. Цілісність даних у мережах датчиків необхідна для забезпечення надійності даних і відноситься до здатності підтвердити, що повідомлення не було змінено.

Навіть якщо в мережі є заходи щодо конфіденційності, все ще існує ймовірність того, що цілісність даних буде скомпрометована змінами. Цілісність мережі порушиться, коли:

шкідливий вузол, присутній у мережі, вводить неправдиві дані,

нестабільні умови, пов'язані з бездротовим каналом, спричиняють пошкодження або втрату даних.

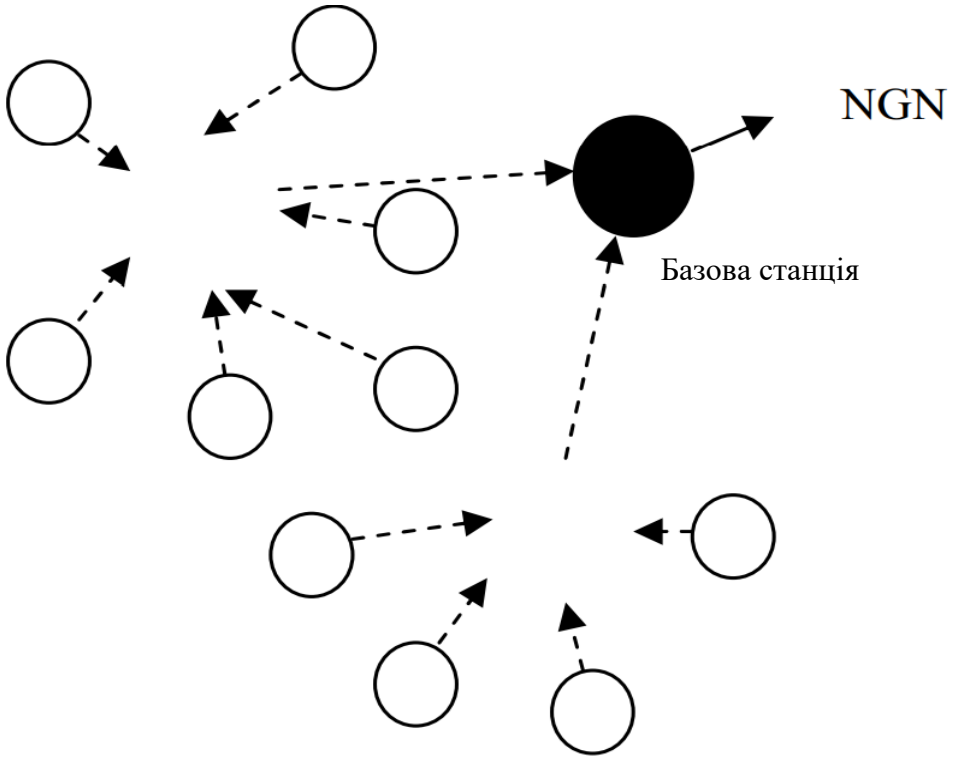

Рис. 1. Схема бездротової сенсорної мережі

Аутентифікація даних. Аутентифікація забезпечує достовірність повідомлень шляхом ідентифікації його походження. Противник не обмежується лише зміною пакета даних. Він може змінити весь пакетний потік, ввівши додаткові пакети. Тому одержувачу необхідно забезпечити, щоб дані, які у будь-якому процесі прийняття рішень, виходили з правильного джерела. З іншого боку, при побудові мережі датчиків аутентифікація необхідна для багатьох адміністративних завдань неформально, аутентифікація даних дозволяє одержувачу перевірити, чи дані відправлені заявленим відправником. У разі двостороннього зв'язку автентифікація даних може бути досягнута за допомогою суто симетричного механізму: відправник та одержувач спільно використовують секретний ключ для обчислення коду автентифікації повідомлення (MAC) всіх переданих даних.

Аналіз уразливостей бездротових сенсорних мереж

Відмова у обслуговуванні. Відмова в обслуговуванні (DoS) провадиться шляхом ненавмисної відмови вузлів або шкідливої дії. Найпростіша атака DoS намагається вичерпати ресурси, доступні вузлу-жертві, шляхом надсилання зайвих непотрібних пакетів і, таким чином, не дозволяє законним користувачам мережі отримати доступ до сервісів або ресурсів, на які вони мають право. DoS-атака має на увазі не тільки спробу противника зруйнувати або знищити мережу, але також будь-яку подію, яка зменшує можливості мережі надавати послугу. У бездротових мережах датчиків можуть виконуватись кілька типів DoS-атак у різних шарах. На фізичному рівні атаки DoS можуть зупиняти і фальсифікувати транзакції, на канальному рівні: зіткнення, виснаження, несправедливості, на мережному рівні, ігнорування та надмірне споживання ресурсів, перенапрямок, «чорні дірки», а на транспортному рівні атака може бути виконана шляхом шкідливості розсинхронізації.

Механізми запобігання DoS-атак включають захист мережевих ресурсів, відштовхування атак, надійну аутентифікацію та ідентифікацію трафіку [2].

Sybil атака. Атака Sybil - це мережна загроза, введена одним або декількома шкідливими вузлами, щоб оголосити численні незаконні ідентифікатори, щоб заплутати або навіть згорнути мережеві програми. Для статичних бездротових сенсорних мереж пропонується новий механізм виявлення, званий CRSD, який використовує силу прийнятого сигналу (RSS) для визначення відстані між двома ідентичностями та додатково визначає відношення позицій цікавих ідентифікаторів з використанням інформації RSS від кількох сусідніх вузлів, наприклад, за допомогою взаємодії вузлів. Атака Sybil виявляється, коли два або більше різних ідентифікаторів мають майже одне й те саме положення. Результати аналізу та моделювання показують, що, по-перше, атака Sybil значно погіршує продуктивність системи, а по-друге, CRSD може виявляти таку атаку в більшості випадків, тим самим ефективно захищаючи загальну ефективність [3].

Концепція атак Sybil (або кількох ідентифікаторів) визначається тим, що один вузол має кілька ідентифікаторів, щоб порушити відповідність між об'єктами та фізичними пристроями у мережах. Метод був запропонований з використанням довіреного центру сертифікації для перевірки фізичної ідентичності для запобігання атакам з множинною ідентифікацією. Атаки з декількома ідентифікаторами зазвичай використовують один зловмисний вузол, щоб заплутати сусідні вузли, викликаючи хаос серед них, поки, нарешті, вся мережа не втрутиться і, отже, неспроможна нормально функціонувати [4].

Напади на інформацію на маршруті. У БСМ датчики контролюють зміни конкретних параметрів або значень та повідомляють приймачеві на його вимогу. Під час надсилання звіту інформація в дорозі може бути змінена підробленою, знову відтворена або може зникнути. Оскільки бездротовий зв'язок вразливий для підслуховування, будь-який зловмисник може контролювати потік трафіку і вступати в дію для переривання, перехоплення, модифікації або виготовлення пакетів, таким чином надавати неправильну інформацію базовим станціям або приймачам. Оскільки вузли-датчики зазвичай мають короткий діапазон передачі і дефіцитний ресурс, зловмисник з високою обчислювальною потужністю і великим діапазоном зв'язку може одночасно атакувати кілька датчиків, щоб змінити фактичну інформацію під час передачі [2].

Атака "Чорна діра". Атака «Чорна діра» – активна атака, вона має дві властивості: перше, зловмисник споживає перехоплені пакети без будь-якого пересилання. По-друге, вузол використовує протокол мобільного розсилки, оголошуючи, що він має точний маршрут до цільового вузла, навіть якщо маршрут є підробленим з метою перехоплення пакетів [5]. У цій атаці шкідливий вузол діє як чорна діра, щоб залучити весь трафік у мережі датчиків. Зокрема, у протоколі, що ґрунтується на повені, зловмисник прислухається до запитів маршрутів, потім відповідає на цільові вузли, що він містить високу якість або найкоротший шлях до базової станції. Як тільки шкідливий пристрій зміг вставити себе між вузлами зв'язку (наприклад, приймачем і вузлом датчика), він може робити що-небудь з пакетами, що передаються між ними. Фактично, ця атака може торкнутися навіть вузлів, які значно віддалені від базових станцій [2].

Атака «Червоточина». Для типової атаки «Чорвоточина» потрібні два або більше зловмисників - зловмисних вузлів - у яких кращі комунікаційні ресурси, ніж у звичайних сенсорних вузлів. Зловмисник створює зв'язок із низькою затримкою (тобто тунель із високою пропускною здатністю) між двома або більше зловмисниками у мережі. Атакуючі просувають ці тунелі як високоякісні маршрути до базової станції. Отже, сусідні сенсорні вузли використовують ці тунелі у шляхах зв'язку, передаючи свої дані під контроль противників. Як тільки тунель встановлений, зловмисник збирає пакети даних на одному кінці тунелю, відправляє їх за допомогою тунелю (провідного або бездротового зв'язку) та повторює їх на іншому кінці. Атаки «Чорвоточина» можуть призвести до серйозних пошкоджень БСМ шляхом переривання або зміни інформаційного потоку до базової станції.

Крім того, якщо зловмисники не змінюють або не виготовляють пакети даних, криптографічні рішення самі по собі не можуть виявити атаки «червоточина» [6].

Атака переповнення "Hello Flood". "Hello Flood" використовує HELLO-пакети як зброю, щоб завантажити датчики в БСМ. При такій атаці зловмисник з високою радіопередачею (називається зловмисником класу ноутбука в діапазоні та потужності обробки відправляє HELLO-пакети кільком сенсорним вузлам, які розсіюються у великій області в БСМ. Таким чином, датчики переконані що противник – їхній сусід. Як наслідок, при відправленні інформації на базову станцію вузли-жертви намагаються пройти через атакуючого, оскільки вони знають, що це їхній сусід зрештою підроблений атакою [2].

Атака повторів. Нападники перехоплюють зашифровані пакети з сигнатурами та відправляють їх без внесення будь-яких змін, тому приймачі вважають їх вихідними пакетами. Використовуючи застарілу інформацію та автентифікацію законної особи, зловмисники можуть отримати секретні дані або корисну інформацію. Щоб запобігти таким атакам, можна додати тимчасову мітку або порядковий номер, щоб перевірити, чи не було відправлено цей запит чи ні. [4].

Вибіркова переадресація. Після отримання пакета зловмисники вибірково пересилають або не пересилають пакет або просто відправляють пакет, що містить інформацію про маршрутизацію, щоб запобігти його доступу до місця призначення. У цьому випадку пакет необхідно повторно передати, а мережевий трафік та споживання енергії збільшиться, і, отже, термін служби всієї мережі буде зменшено [4].

Аналіз засобів впливу на безпроводні сенсорні мережі

Атаки розділяють на два види: зовнішні та внутрішні. Зовнішні атаки є неавторизованими користувачами машин, які вони атакують, в той час як внутрішні порушники мають дозвіл на доступ до системи але не мають привелегій для супер користувацького режиму. Замаскований внутрішній порушник входить в систему як і інші користувачі, які мають законний доступ до конфіденційних даних, а таємний внутрішній зловмисник, найнебезпечніший, має можливість відключити аудитерський контроль для себе таким чином, що навіть після виявлення вторгнення, в логах системи не буде помітно пересування зловмисника по системі. Такі атаки можуть бути комбінованими або гібридними, в залежності від складності проникнення в систему та наявності доступу до головних модулів або компонентів мережі. Перелік основних типів атак наведено в таблиці 1.

Таблиця 1

Види комп’ютерних атак: характеристики та приклади

Назва атаки	Характеристика	Приклад
Вірус	Самовідтворювана програма, яка заражає систему без відома і дозволу користувача. Підвищує рівень зараження мережевої файлової системи, якщо доступ до системи здійснюється з іншого комп’ютера.	Trivial.88.D, Polyboot.B, Tuager
Хробак	Програма розповсюджується через мережеві служби в комп’ютерних системах без втручання користувача. Може завдати серйозної шкоди мережі, споживаючи пропускну здатність мережі	SQL Slammer, Mydoom, CodeRed Nimba
Троян	Шкідлива програма, яка не може самовідтворюватись, але може викликати серйозні проблеми з безпекою в комп'ютерній системі. Встановлюється як корисна програма, але насправді в неї секретний код, який може несанкціонований доступ до системи, дозволяючи програмі робити що завгодно в системі, та може бути викликаний коли завгодно, так як хакер отримує контроль над системою без дозволу користувача	HookDump, Back Orifice, Pinch, TDL-4, Trojan.Winlock
DoS-атака	Комплекс дій, націлених на блокування доступу до системних або мережевих ресурсів. Це реалізується шляхом примусу цільвого комп’ютера (комп’ютерів) до перезавантаження або споживання ресурсів. Користувачі цих систем не можуть адекватно працювати через відсутність обслуговування або перешкод, що створюються нестачею обчислювальних ресурсів	Buffer overflow, ping of death (PoD), TCP SYN, smurf, teardoop

Назва атаки	Характеристика	Приклад
Мережеві атаки	Будь-який процес, який використовується для зловмисних спроб підірвати безпеку мережі, починаючи з канального і закінчуючи прикладним рівнем, за допомогою різних засобів, такий як маніпуляції з мережевими протоколами. Незаконне використання облікових записів і прав користувачів, виконання дій з видалення мережевих ресурсів та пропускної здатності, виконання дій, що перешкоджають доступу авторизованих користувачів до мережевих служб	Packet injection, SYN flood
Фізичні атаки	Спроби пошкодити фізичні компоненти мережі або комп'ютера	Cool boot, evil maid
Злом паролю	Ціль – отримати пароль користувача в короткий період часу, зазвичай на таку атаку вказує серія невдалих входів в систему.	Dictionary attack, SQL injection attack
Атака по збору інформації	Збір інформації або знаходження відомих вразливостей, скануючи або зондуючи комп'ютерні або мережі	SYS scan, FIN scan, XMAS scan
Несанкціоноване підвищення прав користувача до суперкористувача	Такий тип атаки може використовувати вразливості для отримання прав супрекористування в системі при старті в якості звичайного користувача системи. Вразливості включають в себе перехват паролей, атаку по довіднику або соціальну інженерію.	Rookit, loadmodule, perl
Несанкціоноване отримання прав користувача	Здатність відправляти пакети в віддалену систему по мережі, не маючи ніякого облікового запису в цій системі, отримати доступ як у звичайного користувача або як суперкористувача та виконати шкідливі операції. Також виконання атаки на публічні служби (такі як HTTP та FTP) або під час з'єднання захищених служб (таких як POP та IMAP)	Warezelient, warezmaster, imap, ftp_wripe, multihop, phf, spyC
Зондування	Сканує мережі для визначення працюючих IP-адрес і збирає інформацію про вузол (що це за служба, яка операційна система використовується). Надає зловмиснику список потенційних вразливостей, які згодом можуть бути використані для атаки на окремі системи та служби	IPsweep, portsweep

Висновки

У даній роботі описано проблему виявлення виявлення атак на бездротову сенсорну мережу, проаналізовано застосування систем виявлень вторгнень для запобігання атак, так як саме ці системи являються основними складовими в забезпеченні безпеки IT інфраструктури. Систематизовано засоби впливу на безпроводні сенсорні мережі. Визначено, що такі атаки можуть бути комбінованими або гібридними, в залежності від складності проникнення в систему та наявності доступу до головних модулів або компонентів мережі.

Перелік посилань

1. Vinayak gupta, Brijesh kumar singh, parmesh war lal bhanwariya "An Introduction to security issues in wireless sensor networks" Journal of environment al science, computer science and engineering and technology (JECET); November 2013;vol.2 No.4,pp.1276-1285.

2. Al-Sakib Khan Pathan, Hyung-Woo Lee ,Choong Seon Hong "Security in wireless sensor networks: issues and challenges". The International conference on advanced computing and technologies (ICACT); 2006; february 20-22; pp.1043-1048.

3. Бельфер Р.А. Угрозы информационной безопасности в беспроводных самоорганизующихся сетях // Вестник МГТУ им. Н.Э. Баумана. — Сер. Приборостроение. Спец. вып. «Технические средства и системы защиты информации». 2011. С. 116–124.

4. Shaohe lv,xiaodong wang, xin zhav, xingming zhou, "Dtecting the Sybil attack cooperatively in wireless sensor network". computational intelligence and security,2008CIS '08' International conference vol.1; 13-17 dec 2008;pp.442- 446.

5. Cheng-Lung Yang, Wernhuar Tarng, Kuen-Rong Hsieh, Mingteh Chen "A security mechanism for clustered wireless sensor network based on elliptic curve cryptography". Intelligent internet systems IEEE dec 2010.

Надійшла: 22.10.2021 Рецензент: д.т.н., професор Кожухівський А.Д.