© Aleksander M., Korchenko O., Karpinski M., Odarchenko R. Vulnerability investigation for Internet of things sensor subnetworks architecture for different types of attacks // Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 1, p. 12-19.

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ СЕНСОРНИХ ПІДМЕРЕЖ АРХІТЕКТУРИ ІНТЕРНЕТУ РЕЧЕЙ ДО РІЗНИХ ТИПІВ АТАК

Марек Алєксандер[1,2], Олександр Корченко[1], Микола Карпінський[3], Роман Одарченко[1],

[1]Національний авіаційний університет, Україна
[2]Державна вища технічна школа у Новому Сончі, Польща
[3]Університет у Бельсько-Бялій, Польща

АЛЄКСАНДЕР Марек Богуслав, к.т.н.

Рік і місце народження: 1974 рік, Новий Сонч, Польща
Освіта: AGH Університет науки й технологій, 2000; Військовий університет технологій 2004.
Посада: асоційований професор, докторант НАУ з 2014 року.
Наукові інтереси: криптологія, математичне моделювання, безпроводові сенсорні мережі.
Публікації: автор більш ніж 40 наукових статей.
E-mail: aleksmar@pwsz-ns.edu.pl

КОРЧЕНКО Олександр Григорович, д.т.н.

Рік і місце народження: 1961 рік, Київ, Україна**.**
Освіта: Київський інститут інженерів цивільної авіації (з 2000 року Національний авіаційний університет), 1983 рік.
Посада: завідувач кафедри безпеки інформаційних технологій з 2004 року.
Наукові інтереси: інформаційна і авіаційна безпека.
Публікації: більше 300 наукових публікацій, серед яких монографії, словники, навчальні посібники, підручники, наукові статті та патенти на винаходи.
E-mail: agkorchenko@gmail.com

КАРПІНСЬКИЙ Микола Петрович, д.т.н.

Рік і місце народження: 1958 рік, Чітинська обл., РФ**.**
Освіта: Львівський політехнічний інститут, 1980 рік.
Посада: завідувач кафедри безпеки інформаційних технологій з 2004 року.
Наукові інтереси: кібербезпека, безпека комп'ютерних систем та безпроводових технологій, криптографічні методи захисту інформації.
Публікації: більше 200 наукових публікацій, серед яких монографії, навчальні посібники, підручники, наукові статті та патенти на винаходи.
E-mail: mkarpinski@ath.bielsko.pl

ОДАРЧЕНКО Роман Сергійович, к.т.н.

Рік та місце народження: 1988 рік, с. Култук Слюдянського р-ну Іркутської області, РФ
Освіта: Національний авіаційний університет, 2010 рік.
Посада: доцент кафедри телекомунікаційних систем з 2012 року.
Наукові інтереси: стільникові мережі зв'язку нового покоління та їх системи безпеки.
Публікації: більше 90 наукових публікацій, серед яких наукові статті та патенти на винаходи.
E-mail: odarchenko.r.s@mail.ru

Анотація. *У роботі проаналізовано сучасну архітектуру концепції Інтернету речей. Показана актуальність проведення досліджень в даному напрямку. Проаналізовано особливості, місце та перспективи розвитку сучасних безпровідних сенсорних підмереж, зокрема, в концепції Інтернету речей. Розглянуті найбільш популярні стандарти, які використовуються для їх побудови. Наведені основні вимоги до*

пристроїв, що складають архітектуру сучасних безпровідних сенсорних мереж, зокрема висока енергоефективність, портативність, автономність. Було розглянуто основні види мережевих атак в сенсорних підсистемах у відповідності до еталонної моделі взаємодії відкритих систем, зокрема фізичного, канального, мережевого, транспортного та прикладного рівнів, з огляду на проблеми забезпечення інформаційної безпеки. Особливу увагу у роботі приділено DoS-атакам. Тому було визначено проблемні місця систем захисту саме до них та наведено їх таксономію. Однією з таких проблем є DoS-атаки в розподіленій архітектурі доступу, що можуть бути використані зловмисниками для здійснення крадіжок з незахищених пристроїв, таких як датчики і маршрутизатори, а також використання їх в якості ботів для атаки на третіх осіб. Результати проведеного дослідження надали змогу запропонувати розширену класифікацію механізмів забезпечення безпеки, що дозволять мінімізувати потенційні збитки від різних типів атак, направлених на порушення конфіденційності, цілісності та доступності.

Ключові слова: *безпровідна сенсорна мережа; протокол; технологія ZigBee; трафік; стандарт IEEE 802.15.4; маршрутизація, IoT, DoS-атаки.*

Вступ

Інтернет речей (IoT) – концепція обчислювальної мережі фізичних об'єктів, оснащених вбудованими технологіями для взаємодії один з одним або із зовнішнім середовищем, яка розглядає організацію таких мереж як явище, здатне перебудувати економічні та суспільні процеси, що виключає з частини дій і операцій необхідність участі людини [1].

Інтернет речей давно перестав бути концепцією. Тепер цей цікавий і перспективний технологічний тренд активно втілюється в життя. В якості «речей» в такій мережі можуть виступати будь-які об'єкти фізичного світу, яким можна присвоїти IP-адреси і які здатні передавати дані.

Багато компаній вже випускають «розумні» пристрої з можливістю підключення до Інтернету речей. Можна згадати і про розумні будинки [2], які по своїй суті є однією з найменших підсистем єдиної мережі IoT. І щоб трохи краще уявити собі «ієрархію» в рамках Інтернету речей [3], а також проблеми масової реалізації концепції, розглянемо приклад того, як може виглядати архітектура IoT (рис. 1) [4].

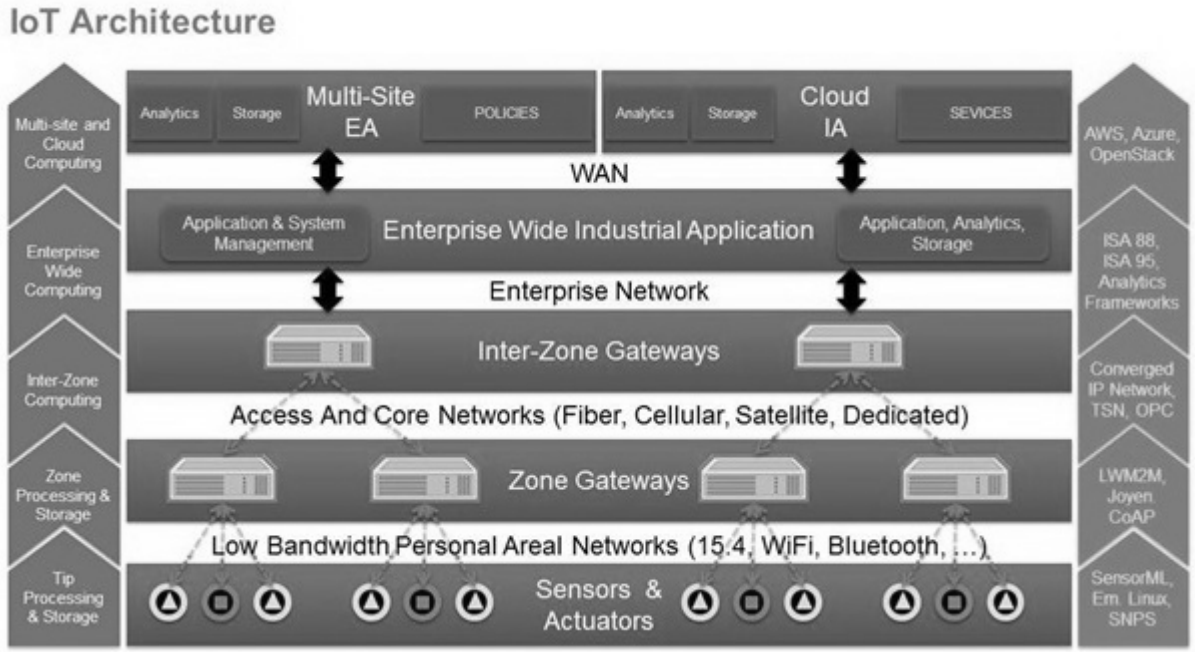

Рис. 1 Орієнтовна архітектура IoT

Інтернет речей, архітектура якого зображена на рис. 1, вже допомагає мільярдам людей. Тисячі розумних, підключених пристроїв надають нові можливості для людей в усьому світі та значно знижують витрати. На жаль, це зростання підключених пристроїв приносить підвищені ризики безпеки. При цьому дослідження щодо підвищення рівня безпеки IoT можна розділити на чотири основні напрямки: захист комунікацій, захист пристроїв, управління пристроями, і розробка нових моделей довіри.

В результаті проведеного аналізу [5-7] було виявлено такі проблеми і уразливості Інтернету речей:

1) DoS-атаки в Інтернеті речей. Оскільки все більше і більше пристроїв підключаються до мережі, вони збільшують кількість категорії пристроїв, які легко захоплюються в ботнети і можуть бути використані для розподілених нападів. Використання розподілених атак робить більш важким процес відстеження джерела атаки, в той же час полегшуючи можливість фізичного пошкодження пристроїв і компрометації додатків, на які вони орієнтовані.

2) Прослуховування в Інтернеті речей. Було виявлено, що пасивні атаки можуть призначатися для каналів зв'язку, таких як Інтернет, локальні

проводові мережі і безпровідні мережі, для отримання даних з потоку інформації. Очевидно, що якщо зловмисник отримає доступ до певної інфраструктури, то він може відновити інформацію, що передається через неї. Поки заходи безпеки спрямовані на захист даних і інформації, ймовірність того, що зловмисник зможе отримати доступ до самої системи і вкрасти дані, є досить великою. Однією з найсерйозніших проблем в масштабному розумінні Інтернету речей, з точки зору користувача, є управління даними.

3) Захоплення вузлів в Інтернеті речей. Такі речі, як вуличні ліхтарі і побутова техніка, фізично знаходяться в специфічних умовах, і, замість того, щоб вивести їх з ладу, зловмисники можуть спробувати зняти інформацію з цих речей. Замість атаки на сам пристрій зловмисник може бути націлений на інфраструктуру, яка використовується для зберігання даних організації або для їх обробки. Якщо, з іншого боку, фактичні дані в Інтернеті речей розподілені, то для створення і обробки інформації будуть використовуватися різні об'єкти. Це означає, що зловмисникам знадобиться багато часу і сил, щоб контролювати таку велику кількість ресурсів.

4) Фізична безпека датчиків. Фізичні атаки можуть пошкодити датчики пристроїв Інтернету речей або навіть привести їх у повністю непрацездатний стан, що являє собою явну загрозу безпеці. Наприклад, зловмисник може увійти в будинок, де розташований датчик, і виявити супутні електронні та фізичні сигнали інших сенсорів за допомогою обладнання для виявлення радіо-, тепло-, магнітних, візуальних та інших електронних сигналів. Потім зловмисник може визначити розташування датчиків на підставі властивостей сигналів, після чого вони можуть бути відключені фізично, знищені або вкрадені. Фізичне руйнування може бути здійснено з використанням нагрівання, фізичної сили або порушення цілісності кількох датчиків, що робить в результаті датчик нефункціональним.

Як видно, проблемних місць в архітектурі Інтернету речей безліч. Тому, на думку авторів, необхідно розділити архітектуру IoT (рис. 1) на декілька складових підсистем, які потребують підвищення рівня захисту. Таким чином, предметом розгляду даної роботи було обрано сенсорну мережу, в якій однією із актуальних задач є оцінка імовірності виникнення та протидії DoS-атакам.

Аналіз досліджень і публікацій

Питання функціонування існуючих протоколів в безпровідних мережах розглядаються багатьма вченими, наприклад, в [8-10]. Проблеми забезпечення енергоефективності сенсорних мереж та її вплив на безпеку вирішувались в [11]. Дослідженням безпровідних сенсорних мереж в системах охоронної сигналізації займалися в роботах [12-14]. Типи та вплив різних типів атак на сенсорні мережі досліджували в [15-18]. Стандартні методи захисту у мережах ZigBee наведено в [19-20]. У роботах [21-22] розглядається новий напрямок дослідних робіт в області безпровідних сенсорних мереж WSN (wireless sensor network) – літаючі сенсорні мережі (ЛСС). В роботі [23] досліджувався один з напрямків забезпечення інформаційної безпеки ЛСС від впливу DoS-атак з потенційно високими збитками при їх реалізації. Проте комплексного аналізу потенційних збитків, видів DoS-атак, механізмів захисту в концепції Інтернету речей проведено не було.

Постановка завдання дослідження

Таким чином, *метою* роботи є визначення вразливостей сенсорних мереж в архітектурі Інтернету речей до DoS-атак.

Поставлена мета передбачає вирішення наступних завдань:

1) Оцінка імовірності виникнення DoS-атак в архітектурі Інтернету речей;

2) Дослідження проблемних місць в архітектурі сенсорних мереж Інтернету речей;

3) Дослідження класифікацій DoS-атак в сенсорних мережах та визначення найбільш небезпечних типів атак;

4) Розробка практичних рекомендацій по використанню заходів протидії DoS-атакам;

5) Окреслення напрямків подальших наукових досліджень.

Основна частина дослідження

Нові технології можуть значно полегшити життя людей, але разом з тим, часто з'являються нові загрози кібербезпеці. Найближчим часом кіберзлочинці зможуть створити DDoS-ботнети небаченої раніше потужності, які будуть складатися з вразливих пристроїв Інтернету речей.

За звітом Verizon Data Breach Investigation Report [24], можна стверджувати що в нинішньому році кількість DDoS-атак збільшилася як мінімум удвічі. Зловмисники використовують невірно налаштовані служби, наприклад, NTP, DNS і SSDP, що дозволяє їм підміняти вихідні IP-адреси і відправляти величезну кількість запитів на цільові сервери.

Більшість DDoS-атак в даний час здійснюються за застарілим протоколом IPv4, але зловмисники все частіше вдаються до IPv6. За даними CNET [25], відносна новизна IPv6 не дозволяє провайдерам і адміністраторам належним чином контролювати мережевий трафік і проводити фільтрацію шкідливих пакетів. Крім цього, шлюзові пристрої, що зв'язують IPv4- і IPv6-мережі, змушені зберігати інформацію про весь трафік мережі, що через них передається, через що зловмисникам стає простіше їх зламати.

Інтернет речей також став привабливим вектором здійснення DDoS-атак. Згідно із звітом компанії InfoSec Institute [26], більшість «розумних» пристроїв для дому та малого бізнесу майже не захищені від атак зловмисників. У багатьох пристроях Інтернету речей містяться серйозні уразливості, а налаштування систем безпеки, що

встановлюються за замовчуванням, не витримують ніякої критики.

Використовуючи відсутність повноцінних засобів моніторингу IPv6-трафіку, слабкий рівень захисту IPv4/IPv6-шлюзів і величезну кількість незахищених пристроїв Інтернету речей, зловмисники, як вже стверджувалось, зможуть створювати DDoS-ботнети величезних масштабів.

Так, наприклад, в березні 2016 року багато користувачів мережі Інтернет в Європі зіткнулися із затримками і короткочасною недоступністю безлічі сайтів. Їх основною була потужна DDoS-атака, що досягала 300 Гбіт/с. Масштаб атаки був такий, що її відчули навіть найбільші точки обміну трафіком європейських столиць.

Удар прийняла на себе CDN CloudFlare [27], що надає в тому числі і захист від DDoS. Атака почалася 18 березня і на наступний день зросла до 90 Гб/с. 21 березня атака перервалася, але 22 продовжилася з новою силою, збільшившись до 120 Гб/с. Так як вивести з ладу саму CloudFlare не вдалося, атакуючі незабаром переключилися на провайдерів, з якими працює CloudFlare, і збільшили потужність атаки до рекордних 300 Гб/с. Атака торкнулася мережі найбільших провайдерів, які в окремі моменти виявлялися перевантаженими. 23 березня значні проблеми були на лондонській точці обміну трафіком (IXP). У годину пік, коли трафік зазвичай складає близько півтора терабіт, вона не справлялася з навантаженням. Цей провал добре видно на графіку (рис. 2) [28].

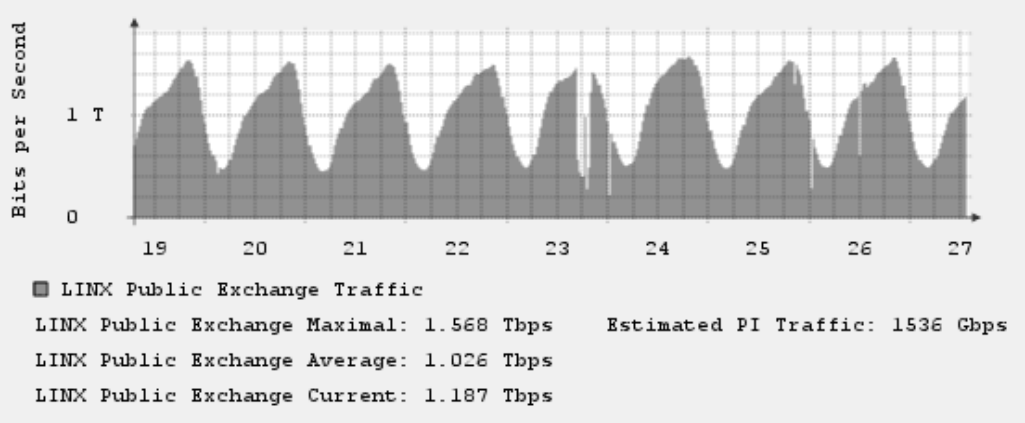

Рис. 2 Графік залежності навантаження на мережу

Тепер перейдемо до детального розгляду вразливостей саме безпровідних сенсорних мереж (БСМ), які можуть нести величезну загрозу в архітектурі Інтернету речей. В загальному розумінні сенсорна мережа – це безліч маленьких зчитувальних пристроїв (датчиків), здатних реєструвати зміни різних параметрів навколишнього середовища і транслювати ці параметри іншим подібним пристроям, що знаходяться в зоні досяжності, з певною метою, наприклад: відеоспостереження, моніторинг навколишнього середовища тощо [18]. На рис. 3 [29] показано, наприклад, схему потенційної DoS-атаки в сенсорній мережі.

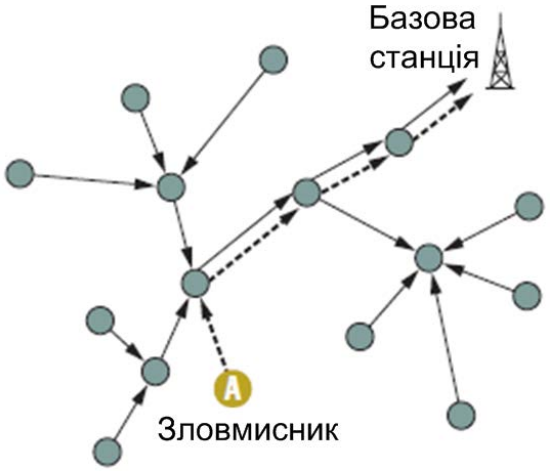

Рис. 3 Схема потенційної DoS атаки в сенсорній мережі

Одним з напрямків досліджень в області сенсорних мереж є вибір архітектури взаємодії між різними типами таких мереж, забезпечення безпечного обміну даними між ними. Вирішення цього завдання визначається багатьма показниками, одним з яких є забезпечення захисту від DoS-атак у збірних сенсорних вузлах. Реалізація зловмисником таких атак може привести до значних збитків, виражених у втраті або нелегітимній зміні інформації від сенсорних датчиків. Вирішення поставленого завдання засноване на визначенні рівня ризику безпеки таких сенсорних вузлів. Аналіз цих кількісних значень дозволяє прийняти найбільш ефективну схему взаємодії мереж. Кількісні значення цих рівнів можуть бути використані для посилення захищеності деяких збірних сенсорних вузлів з повторним розрахунком рівнів безпеки зазначених DoS-атак. При вирішенні цього завдання слід враховувати такі характеристики, як вартість, технічні можливості взаємодії мереж та ін.

Як видно з рис. 4, спрощена БСМ складається з однієї базової станції (БС), що виконує на верхньому рівні функцію збірних сенсорних вузлів, і двох ЗСВ транзитного рівня (ЗСВ1 і ЗСВ 2). БС збирає інформацію сенсорних датчиків з ЗСВ1 і ЗСВ2, а кожен з цих ЗСВ збирає інформацію датчиків з двох головних кластерів [30].

На рис. 5 приведена ієрархічна модель наслідків від DoS-атак на збірні сенсорні вузли сенсорних мереж. На верхньому рівні наводиться глобальна характеристика наслідків DoS-атаки на

ЗСВ транзитного і верхнього рівнів, на проміжному – поділ наслідків атак за рівнем впливу на базові станції і збитки збірних сенсорних вузлів транзитного рівня. Нижній рівень характеризує такі втрати: від реалізації DoS-атаки в ЗСВ 1 транзитного рівня – С1; від реалізації DoS-атаки в ЗСВ 2 – С2; від реалізації DoS-атаки в БС - С3.

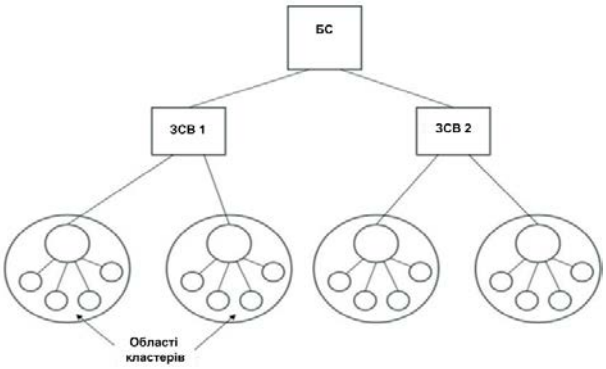

Рис. 4 Спрощена структура безпровідної сенсорної мережі

Ці втрати залежать від конкретних додатків, що використовуються на сенсорних датчиках.

Рис.5 Ієрархічна модель наслідків DoS-атак збірних сенсорних вузлів

Наприклад, в сенсорній мережі «розумне місто» (smart city) такими додатками можу бути: моніторинг шуму, світла, забруднення навколишнього середовища, руху транспортних засобів, екстрена медична послуга і ін. [22].

Як відзначалось в роботі [21], більш висока достовірність ранжування безпеки загроз досягається при однаковій розмірності завданої шкоди. В даному прикладі сенсорної мережі для багатьох з наведених додатків наслідки DoS-атак можуть бути виражені фінансовими втратами.

На сенсорні вузли та базову станцію можуть бути направлені наступні типи DoS-атак в залежності від різних параметрів (рис. 6). У [31] наведено дану таксономію більш детально із повним аналізом DoS-атак, в залежності від природи їх виникнення. А в табл. 1 [32] показано розподіл DoS-атак за рівнями моделі OSI.

Механізми боротьби із DoS-атаками у сенсорних мережах

З табл. 1 та рис. 6 видно, який широкий спектр DoS-атак можливий на сенсорні мережі. Тому надалі необхідно більш детально розглянути заходи протидії для мінімізації наслідків або зовсім їх унеможливлення. Серед проаналізованих механізмів забезпечення безпеки, зокрема конфіденційності, цілісності та доступності, в [33] розглянемо наступні.

Розподіл ключів шифрування

Як одна з основних послуг безпеки, установка парних ключів дозволяє сенсорним вузлам взаємодіяти один з одним доволі безпечно, використовуючи технології криптографії такі, як шифрування та аутентифікація. При установці криптографічного ключа двома або більше учасниками слід дотримуватися двох основних кроків: установка довіреного зв'язку між учасниками, і обчислення криптографічного ключа.

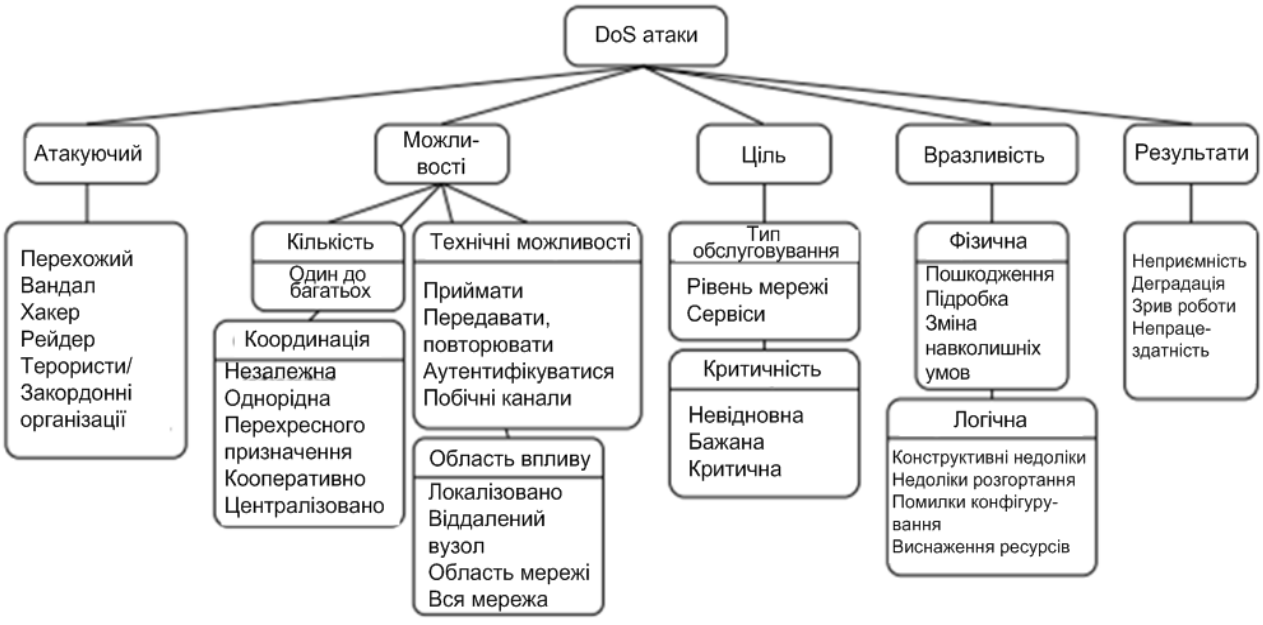

Рис. 6 Таксономія DoS-атак в безпровідних сенсорних мережах

Розподіл DoS-атак за рівнями моделі OSI Таблиця 1

Рівень	Тип атаки	Заходи протидії
Фізичний рівень	JAMMING (глушіння)	Розширення спектру, пріоритетні повідомлення, картування областей
	TAMPERING (підробка)	Випробувальні пакети проти підробки, використання нечутливих до відмов протоколів
Канальний рівень	Колізії	Корегувальне кодування
	Виснаження	Обмеження швидкості передавання даних
	Збір інформації	Використання захисту проти повторних відправлень, сильна аутентифікація на канальному рівні
Мережевий рівень	Фальсифікація маршрутної інформації	Аутентифікація, використання захисту проти повторних відправлень
	Селективне просування	Використання різних маршрутів, підтвердження доставки
	Sinkhole-атака	Перевірка надмірності
	Атака Sybil	Аутентифікація, надмірність, моніторинг
Транспортний рівень	Флуд-атаки	Клієнтські пазли
	Розсинхронізація	Аутентифікація
Прикладний рівень	DoS-атака на базі маршруту	Аутентифікація, використання захисту проти повторних відправлень
	Перепрограмування	

Основні технології шифрування

Забезпечення процесу управління ключами конфіденційністю й аутентифікації на рівні групи являється непростим завданням через мережі типу ad-hoc, непостійність зв'язку і обмеження ресурсів середовища розподіленої сенсорної мережі. У [34] описуються протоколи управління ключами, що врівноважують безпеку і обмеження ресурсів для підтримки даних послуг. Такі протоколи управління ключами можуть бути класифіковані як протоколи з попереднім розміщенням, арбітражною логікою, самодостатні, автономні, протоколи шифрування. Протоколи кодування з попередніми розміщенням дозволяють компенсувати високі витрати на передачу сенсорних вузлів через більш інтенсивні попередні початкові конфігурації. Деякі попередні конфігурації завжди необхідні, але можуть знизити гнучкість і вплинути на безпеку. Інші технології вимагають менше вихідних конфігурацій. У протоколах шифрування з арбітражною логікою [35] використовується точка централізованого розподілу ключа для установки і підтримки ключа в сенсорній мережі.

Таким чином, як бачимо, основні послуги криптографії, такі як широкомовна аутентифікація і управління ключами, це необхідна умова для забезпечення безпеки і стабільності додатків сенсорних мереж. Інші основні послуги також вимагають серйозного дослідження. Прикладами таких послуг є тимчасова синхронізація, безпечне визначення місця розташування, захищений збір даних і робота всередині мережі, організація груп, вибір головного в групі. Більш того, необхідно проводити безперервне виявлення вторгнень в сенсорну мережу, особливо через те, що сенсорні вузли, які тимчасово не обслуговуються, можуть бути легко захоплені і зламані. Тому можна сміливо стверджувати, що дослідження безпеки сенсорних мереж скоріше за все вплине на розвиток самих сенсорних мереж, особливо в контексті розповсюдження засад концепції Інтернету речей.

Висновки

У результаті проведеного дослідження були визначені різні проблеми і недоліки використання технологій Інтернету речей, особливо їх переважання в повсякденному житті. Очевидним є те, що Інтернет речей робить наше життя простіше, але існують значні труднощі в його використанні. Однією з таких проблем є DoS-атаки в розподіленій архітектурі доступу, що можуть бути використані зловмисниками для здійснення крадіжок з незахищених пристроїв, таких як датчики і маршрутизатори, а також використання їх в якості ботів для атаки на треті особи. Кількість пристроїв, які опиняться під загрозою DoS-атак, досить велика. Ще однією проблемою є прослуховуванням в архітектурі Інтернету речей, тим більше зловмисники можуть використовувати канали зв'язку для отримання інформації та даних із загального інформаційного потоку. Крім того, було також встановлено, що захоплені вузли становлять загрозу для Інтернету речей; зокрема, коли ресурси вузла обмежені і є певна розподілена організована структура, відбувається динамічна зміна топології мережі.

Таким чином, можна сміливо стверджувати, що дослідження, присвячені проблемам, виявленим в даній роботі, і пошукам шляхів їх вирішення, є вкрай актуальними, що в майбутньому дозволить підвищити рівень забезпечення безпеки в сенсорних підмережах зокрема та у всій архітектурі Інтернету речей.

Література

[1] «Интернет вещей» — реальность или перспектива? [Електронний ресурс]. — Режим доступу: http://www.mate-expo.ru/ru/article/internet-veshchey-realnost-ili-perspektiva.

[2] «Умный дом»: 5 технологий будущего [Електронний ресурс]. — Режим доступу: http://www.lookatme.ru/mag/live/future-research/194385-smart-home.

[3] Интернет верей. Как изменится вся наша жизнь на очередном витке развития Всемирной сети

Cisco IBSG © Корпорация Cisco и/или ее дочерние компании, 2011.

[4] Jack Tison, SVP Emerging Business, Panduit-October 2015 3 Steps for Evolving IoT Architectures [Електронний ресурс]. — Режим доступу: http://www.industrial-ip.org/en/industrial-ip/internet-of-things/3-steps-for-evolving-iot-architectures.

[5] Интернет вещей открывает киберпреступникам новое поле деятельности [Електронний ресурс]. — Режим доступу: http://www.klaipeda1945.org/sensatsii/34031/.

[6] Эксперты предупредили о растущем количестве киберугроз в сфере «Интернета вещей» [Електронний ресурс]. — Режим доступу: http://www.securitylab.ru/news/480244.php.

[7] Интернет вещей ставит под угрозу безопасность пользователей [Електронний ресурс]. — Режим доступу: http://umvs.kr.ua/internet-veschej-stavit-pod-ugrozu-bezopasnost-polzovatelej.

[8] Heinzelman W.R. Energy-Efficient Communication Protocol for Wireless Microsensor Networks / W.R. Heinzelman, A.Chandrakasan and H.Balakrishnan // IEEE Proceedings of the 33rd Hawaii International Conference on System Sciences. – 2000. – P. 1–10.

[9] Akl, A. An investigation of self-organization in wireless sensor networks / A. Akl, T.Gayraud and P.Berthou // IEEE International Conference on Networking, Sensing and Control (ICNSC). - 2001. – P. 1-6.

[10] Sohrabi K. Protocols for Self-Organization of a Wireless Sensor Network / K. Sohrabi, J. Gao, V.Ailawadhi and G.J. Pottie // Personal Communications, IEEE. – October 2000. – Vol. 7. – N 5. – P. 16-27.

[11] Баскаков С.С. Исследование способов повышения эффективности маршрутизации по виртуальным координатам в беспроводных сенсорных сетях // Вестник МГТУ им. Н. Э. Баумана. Сер. Приборостроение. – 2009. – № 2. – С. 112–124.

[12] Pathan A.S.K.; Hyung-Woo Lee; Choong Seon Hong, Security in wireless sensor networks: issues and challenges Advanced Communication echnology (ICACT). – 2006. – P.6.

[13] Zia T., Zomaya A., Security Issues in Wireless Sensor Networks, Systems and Networks Communications (ICSNC). – 2006. – P.40.

[14] Adrian Perrig, John Stankovic, David Wagner, Security in Wireless Sensor Networks Communications of the ACM. – 2004. – P.53-57.

[15] Chris Karlof, David Wagner, Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, AdHoc Networks (elsevier). – 2003. – P.299-302.

[16] Hu Y., C. Perrig, Johnson D.B. Packet leashes: a defense against wormhole attacks in wireless networks // Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. — Vol. 3. — 3 April 2003. — P. 1976-1986.

[17] Blackert W.J., Gregg D.M., Castner A.K., Kyle E.M., Hom R.L. and Jokerst R.M. Analyzing interaction between distributed denial of service attacks and mitigation technologies // Proc. DARPA Information Survivability Conference and Exposition, — Vol.1. — 24 April, — 2003. — P. 26—36.

[18] Постольский С.П. Обзор проблемных областей в безопасности беспроводных сенсорных сетей, атак и механизмов их защиты // Научное сообщество студентов XXI столетия. техн. науки: сб. ст. по мат. XXXII междунар. студ. науч.-практ. конф. № 5 (31). [Електронний ресурс]. — Режим доступу: http://sibac.info/archive/technic/5(31).pdf.

[19] Akl A. An investigation of self-organization in wireless sensor networks / A. Akl, T.Gayraud and P. Berthou // IEEE International Conference on Networking, Sensing and Control. — 2001. — P. 1-6.

[20] Sohrabi K. Protocols for Self-Organization of a Wireless Sensor Network / K. Sohrabi, J.Gao, V.Ailawadhi, G.J. Pottie // Personal Communications, IEEE. — October 2000. — Vol. 7. — N 5. — P. 16–27.

[21] Yao Jiang, KangFeng Zheng. Evaluation Model for DoS Attack Eff ect in Softswitch Network // International Conference on Communications and Intelligence Information Security (ICCIIS). – 2010. – P. 88-91.

[22] Матвеев В.А., Морозов А.М., Бельфер Р.А. Оценка уровня риска угрозы безопасности фрода в сети VoIP по протоколу SIP // Электросвязь. — 2014. — №6 — С. 35–38

[23] Матвеев В.А., Бельфер Р.А., Глинская Е.В. Угрозы и методы защиты в сборных сенсорных узлах летающих сенсорных сетей. Вопросы кибербезопасности. — 2015. — №5 (13).

[24] 2015 Data Breach Investigations Report [Електронний ресурс]. — Режим доступу: http://www.verizon enterprise.com/DBIR/2015/.

[25] CNET Content Solutions [Електронний ресурс]. — Режим доступу: http://cnetcontent.com/product-data.

[26] Infosec [Електронний ресурс]. — Режим доступу:http://www.infosecinstitute.com/infosec_institute/instructors.html.

[27] Cloudflare [Електронний ресурс]. — Режим доступу: https://www.cloudflare.com/features-cdn.

[28] Одна из самых больших DDoS-атак в истории https://habrahabr.ru/post/174483/.

[29] G.V. Crosby, N. Pissinou and J. Gadze, A Framework for Trust-Based Cluster Head Election in Wireless Sensor Networks, Proc. 2nd IEEE Workshop Dependability and Security in Sensor Networks and Systems. — IEEE Press. — 2006. — P. 13–22.

[30] Гольдштейн Б.С., Кучерявый А.Е. Сети связи пост-NGN. — СПб.: БХВ-Петербург. — 2013. — 160 с.

[31] Anthony D. Wood and John A. Stankovic A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks.

[32] Annie Jenniefer1, John Raybin Jose Techniques for Identifying Denial of Service Attack in Wireless Sensor Network: a Survey International Journal of Advanced Research in Computer and Communication Engineering. — Vol. 3. — Issue 6. — June 2014.

[33] Raymond D. R. and Midkiff S. F. (2008). Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. — IEEE Pervasive Computing. — January-March 2008. — P. 74-81.

[34] Управління ключами в інформаційній системі [Електронний ресурс]. — Режим доступу: http://pidruchniki.com/13410927/informatika/upravlinnya_klyuchami_informatsiyniy_sistemi.

[35] Н. Смарт Криптография. — М.: Техносфера. — 2005. — 528 с.

УДК 621.391 (045)

Александер М.Б., Корченко А.Г., Карпинский Н.П., Одарченко Р.С. Исследование уязвимостей сенсорных подсетей архитектуры Интернета вещей для разных типов атак

Аннотация. *В работе проанализировано современную архитектуру концепции Интернета вещей. Показана актуальность проведения исследований в данном направлении. Проанализированы особенности, место и перспективы развития современных беспроводных сенсорных подсетей, в частности, в концепции Интернета вещей. Рассмотрены наиболее популярные стандарты, которые используются для их построения. Приведены основные требования к устройствам, составляющим архитектуру современных беспроводных сенсорных сетей, в частности, высокая энергоэффективность, портативность, автономность. Были рассмотрены основные виды сетевых атак в сенсорных подсистемах в соответствии с эталонной моделью взаимодействия открытых систем, в частности, физического, канального, сетевого, транспортного и прикладного уровней, учитывая проблемы обеспечения информационной безопасности. Особое внимание в работе уделено DoS-атакам. Поэтому было определено проблемные места систем защиты именно к ним и приведено их таксономию. Одной из таких проблем является DoS-атаки в распределенной архитектуре доступа, которые могут быть использованы злоумышленниками для совершения краж из незащищенных устройств, таких как датчики и маршрутизаторы, а также использование их в качестве ботов для атаки на третьи лица. В результате проведенных исследований появилась возможность предложить расширенную классификацию механизмов обеспечения безопасности в них, которые позволят минимизировать потенциальные убытки от различных типов атак, направленных на нарушение конфиденциальности, целостности и доступности.*

Ключевые слова: *беспроводная сенсорная сеть; протокол; технология ZigBee; трафик; стандарт IEEE 802.15.4; маршрутизация, IoT, DoS-атаки.*

Aleksander M., Korchenko O., Karpinski M., Odarchenko R. Vulnerability investigation for Internet of things sensor subnetworks architecture for different types of attacks

Abstract. *The paper analyzes the contemporary the Internet of things concept architecture . Relevance of research in this area was shown. The features, location and prospects of modern wireless sensor subnetworks, including the concept of the Internet of things were analyzed. Considered the most popular standards used for their construction. The basic requirements for the devices that make up the modern architecture of wireless sensor networks, including high energy efficiency, portability, autonomy. The basic types of network attacks in sensor subsystems according to the reference model OSI, including physical, data link, network, transport and application levels, were given. Particular attention is paid to DoS attacks. So problem areas of defense was identified and was given their taxonomy. One of these problems is the DoS-attack in a distributed access architecture that can be used to perform malicious theft of unprotected devices such as routers and sensors, and use them as bots to attack third parties. This study provided the opportunity to offer an expanded classification of security mechanisms in them that will minimize potential damage from various types of attacks aimed at the breach of confidentiality, integrity and availability.*

Key words: *wireless sensor networks, protocol, ZigBee technology, traffic, IEEE 802.15.4 Standard, routing, IoT, DoS attack.*

Отримано *9 лютого 2016 року*, затверджено редколегією *1 березня 2016 року*