View metadata, citation and similar papers at core.ac.uk
brought to you by CORE

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (10), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.10.5466
УДК 004.056

Карпенко Андрій Олександрович
науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID: 0000-0002-8372-6303

Бондаренко Тетяна Василівна
науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID: 0000-0002-2879-2041

Овсянніков Вячеслав Володимирович
провідний науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID: 0000-0003-0186-6220

Мартинюк Валерій Віталійович
провідний науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID: 0000-0003-0244-7861

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖАХ

Анотація. У даній роботі розглянута проблема забезпечення інформаційної безпеки в бездротових сенсорних мережах. Проведено аналіз існуючих рекомендацій по забезпеченню інформаційної безпеки в бездротових сенсорних мережах. Виявлено, що одна з ключових проблем забезпечення інформаційної безпеки полягає в апаратних обмеженнях сенсорних вузлів мережі. Обґрунтовано, що використання більш складних криптографічних механізмів захисту викличе збільшення навантаження на мережу. Наведено вимоги для забезпечення безпеки та їх опис. Розглянуто основні групи і типи загроз інформаційної безпеки в бездротових сенсорних мережах. Представлено класифікацію атак і захисту бездротових сенсорних мереж згідно моделі OSI. Розглянуто і проаналізовано існуючі рішення по забезпеченню інформаційної безпеки. Виявлено недоліки та вразливості розглянутих рішень. Розглянуто метод криптографії з відкритим ключем, виявлені основні переваги та недоліки даного методу. Проведено аналіз та порівняння методів шифрування ECC і RSA. Обгрунтовано, що використання ECC в бездротових сенсорних мережах більш ефективно, ніж RSA. Розглянуто метод криптографії з симетричним ключем, зазначені основні переваги та недоліки даного методу. Виявлено, що криптографічні методи з використанням симетричного ключа є більш пріоритетними для використання в бездротових сенсорних мережах. Розглянуто протоколи управління криптографічними ключами в бездротових сенсорних мережах. Наведено класифікацію протоколів управління ключами. Розглянуто протоколи безпечної маршрутизації. Наведено класифікацію протоколів безпечної маршрутизації. Розглянуто методи безпечної агрегації даних. Виявлено протиріччя між вимогами до конфідиційності та агрегування даних. Розглянуто метод визначення вторгнень, виявлені основні переваги та недоліки даного методу. Результати даної роботи доцільно використовувати при проектуванні бездротових сенсорних мереж.

Ключові слова: бездротова сенсорна мережа; інформаційна безпека; мережева модель OSI; автентифікація; криптографія; система виявлення вторгнень.

© А. О. Карпенко, Т .В. Бондаренко, В. В. Овсянніков, В. В. Мартинюк, 2020.

1. ВСТУП

Бездротова сенсорна мережа (БСМ) – це розподілена мережа, що самоорганізується та складається із безлічі датчиків (сенсорів) і виконуючих пристроїв, об'єднаних між собою за допомогою радіосигналу.

Вузлами БСМ є малогабаритні пристрої, кожен з яких в тій чи іншій мірі має обмежені можливості обробки інформації, малу ємність акумуляторної батареї, а також низьку пропускну здатність каналу зв'язку. На практиці параметри розглянутих пристроїв варіюються в залежності від їх ролі в мережі і призначення в цілому.

Такі мережі дозволяють вирішити проблеми збору різноманітної інформації (метеорологія, телемедицина, військові операції, надзвичайні ситуації та ін.), особливо з огляду на можливість швидкого розгортання мережі з наявними вимогами до сенсорного поля БСМ. Так як в розгортанні мережі відсутній монтаж проводів, вона має можливість переміщатися (гетерогенна мережа), що відмінно підходить для стаціонарно-бездротових і переносних пристроїв.

Організація зв'язку сенсорних вузлів БСМ визначається стандартом IEEE 802.15.4. Існує безліч факторів, що впливають на властивості розгортання мережі: характеристики області розташування сенсорного поля, розподіл і кількість одиниць мережі, їх параметри і т.д.

Дослідження БСМ займає ключове місце в науковій діяльності в області систем, мереж і телекомунікаційних пристроїв. Істотну роль в дослідженні і розвитку бездротових сенсорних мереж займають питання інформаційної безпеки (ІБ), що не дозволяють в подальшому використовувати всі перспективи і потенційні переваги розглянутої технології. Більшість пристроїв БСМ займають своє місце в життєдіяльності людини або процесах організацій і представляють собою системи, призначення яких - збір і аналіз докладних даних про будь-яку активність або про окремі заходи. Крім того, дані технології припускають організацію доступу до інформації певної групи осіб. Інновації такого масштабу неминуче викличуть зростання рівня інцидентів кіберзлочинності, а задіяні в автоматизації сектори діяльності зіткнуться з більш гнучкими і різноманітними загрозами інформаційній безпеки на всіх рівнях мережевої моделі OSI.

На даний момент розроблено безліч приватних рішень питань ІБ в БСМ, однак більше 60% систем, що використовують дану технологію, є слабозахищеними. Саме вирішення проблеми ІБ є одним з ключових параметрів щодо подальшої верифікації технології в повсюдну діяльність людини. Саме тому, важливо визначити ступінь впливу загроз ІБ на БСМ для конкретних користувальницьких умов і сфери застосування бездротової сенсорної мережі, для подальших операцій по їх усуненню та запобіганню.

Метою даної роботи є аналіз особливостей функціонування бездротових сенсорних мереж з точки зору вразливостей і схильності до мережевих загроз.

2. ДОСЛІДЖЕННЯ ПРОБЛЕМ ЗАБЕЗПЕЧЕННЯ ІБ В БСМ

Досліджуючи особливість проблем забезпечення ІБ в БСМ, звернемося до рекомендації ITU-T X.1311 — «Структура безпеки для всепроникаючих сенсорних мереж». Дана рекомендація визначає категорії взаємозв'язків БСМ:

- Взаємодія вузла мережі зі шлюзом (базовою станцією);
- Взаємодія шлюзу з вузлом мережі;

- Взаємодія шлюзу з усіма одиницями сенсорної мережі;
- Взаємодія між вузлами сенсорної мережі (в тому числі взаємозв'язок ключового вузла кластера БСМ з одиницями кластера і взаємодія двох сусідніх вузлів мережі);
- Взаємодія шлюзу і групи сенсорних вузлів, виділених по деякому параметру.

Аналізована рекомендація повністю характеризує БСМ. Виняток становить взаємодія ключових вузлів кластерів між собою.

Відзначимо, що в рекомендації ITU-T X.1311 присутні твердження щодо проблем використання стандартних механізмів і засобів захисту в мережах зв'язку на тлі особливостей побудови і функціонування БСМ. Застосування типових схем/систем криптографічних ключів ускладнено внаслідок певних вимог до характеристик вузлів сенсорної мережі, а саме енергоспоживанню, обчислювальної потужності і обсягу пам'яті пристроїв. Дані вимоги є причиною вразливості сенсорних вузлів, в силу відсутності економічної можливості забезпечення захисту належного рівня при масовому використанні. Однією із серйозних проблем забезпечення безпеки є шлюз мережі, який концентрує в собі всю інформацію, передану одиницями БСМ, і являє собою найбільш привабливу точку для проведення атаки. В мережах із застосуванням кластерної структури, основна загроза доводиться на вузли-маршрутизатори, які відповідають за комунікацію одиниць кластера в цілому. Підсумком подібних кібератак може бути впровадження зловмисником помилкових пакетів даних, що в свою чергу призводить до дуплікації або спотворенню даних маршрутизації.

Отже, описані вразливості тісно пов'язані з обмеженнями вузлів БСМ, як наслідок відсутність можливості застосування типізованих механізмів захисту на платформі малогабаритного пристрою.

Таким чином проблема щодо забезпечення інформаційної безпеки полягає в апаратних обмеженнях сенсорних вузлів:

- енергоресурси;
- обчислювальна потужність;
- обсяг пам'яті;
- дальність поширення сигналу.

Енерговитрати сенсорних вузлів мережі класифікуються наступним чином:

- робота датчика сенсорного вузла мережі;
- передача пакетів даних в мережі;
- мікропроцесорні обчислення.

Проведене дослідження [1] показало, що кожен біт переданий сенсорним вузлом в мережі споживає ідентичну кількість енергії, що приблизно як 900 виконаних команд мікропроцесором. Отже, передача інформаційних пакетів між вузлами БСМ є більш енерговитратною, ніж обчислювальні операції, виконувані мікропроцесором; в той час будь-які існуючі криптографічні механізми захисту мають на увазі збільшення розміру переданого пакета даних, що прямо впливає на підвищення енергоспоживання при їх використанні. Відзначимо, що використання більш складних криптографічних механізмів захисту викличе збільшення навантаження на обчислювальну потужність мікропроцесора з подальшим негативним впливом на енергоємність сенсорного вузла мережі.

ISSN 2663 - 4023

3. ВИМОГИ ЩОДО ЗАБЕЗПЕЧЕННЯ ІБ В БСМ

Для забезпечення інформаційної безпеки в БСМ необхідне виконання наступних критеріїв:

- конфіденційність;
- цілісність інформації;
- автентифікація;
- доступність;
- суворе виконання зобов'язань;
- принцип новизни даних.

Конфіденційність даних має на увазі, що пакети даних, які передаються в мережі, не можуть бути прочитані пасивними зловмисниками, і можуть бути прочитані тільки тими користувачами або вузлами мережі, яким вони призначалися. Цілісність інформації підтверджує, що інформаційні пакети які передаються не були змінені проміжними вузлами мережі на їх шляху до одержувача. Автентифікація надає інформацію про справжність вузлів мережі, а саме чи є вузол-відправник довіреним, забезпечуючи надійність походження пакету даних. Критерій доступності гарантує працездатність мережевих сервісів, наприклад, чи доступна мережа для обміну повідомленнями. Під критерієм суворого виконання зобов'язань мається на увазі, що вузол-відправник інформації не може заперечувати свою вихідну операцію передачі даних. Принцип новизни даних забезпечує актуальність даних в мережі, і при цьому гарантує відсутність можливості відтворення застарілих даних.

Механізми забезпечення інформаційної безпеки в БСМ, зазвичай реалізуються за допомогою криптографічних методів. Однак вже описані в даній роботі апаратні обмеження не дозволяють застосовувати існуючі надійні методи, що в свою чергу частково або повністю не відповідає критеріям забезпечення ІБ в БСМ, роблячи їх не практичними для застосування.

4. ДОСЛІДЖЕННЯ ОСНОВНИХ ТИПІВ ЗАГРОЗ ІБ В БСМ

Відповідно до технічних обмежень сенсорних вузлів та переліку вимог до забезпечення ІБ — БСМ можуть бути вразливі для більшості різних типів атак:

- Загрози секретності і автентифікації: існує сукупність факторів, що впливають на можливість зловмисника реалізації атаки підслуховування, відтворення, модифікації і підміни пакетів даних в мережі;
- Загрози доступності: найбільш популярним різновидом даного типу загроз є відмова обслуговування мережі (DOS-атака) реалізована на будь-якому рівні мережевої структури сенсорної мережі.
- Загрози цілісності інформації: ключова ідея зловмисника полягає у впровадженні неправдивих відомостей в потоки даних. Прикладом може служити скомпрометований зловмисником вузол, за допомогою якого організовуються неправдиві повідомлення між вузлами БСМ.

Важливим фактором для успішного проведення більшості описаних атак є підтримка функціонування мережі, в силу збереження можливості зловмисником якомога довше проводити маніпуляції з потоками даних.

Розглядаючи архітектуру БСМ і розподіл загроз згідно до мережевої моделі OSI, загрози можна класифікувати наступним чином (Табл. 1).

ISSN 2663 - 4023

Таблиця 1

Розподіл атак і захисту в БСМ по моделі OSI

Network	Attacks	Defense
Physical	Jamming Tampering	Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change tamper-proofing, hiding
Link	Collision Exhaustion Unfairness	Error-correcting code Rate limitation Small frames
Network and routing	Spoofed, altered or replayed routing information Selective forwarding Sinkhole Sybil Wormholes Flood attacks Acknowledgment spoofing	Egress filtering, authentication, monitoring Redundancy, probing Authentication, monitoring, redundancy Authentication, probing Authentication, packet leashes by using geographic and temporal information Authentication, verify the bidirectional link Authentication
Transport	Flooding Desynchronization	Client puzzles Authentication

5. ДОСЛІДЖЕННЯ РІШЕНЬ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІБ В БСМ

Вибір найбільш підходящого для окремого випадку використання БСМ криптографічного методу має ключове значення безпеки мережі в цілому, так як всі інші служби безпеки з ним пов'язані. Як зазначалося раніше, всі використовувані методи забезпечення безпеки повинні відповідати наявним в БСМ обмеженням — в випадку з криптографічними методами, їх відповідність оцінюється по обсягу використаного коду, додає об'єму до пакетів даних, часу обробки команд і енергоспоживанню.

Криптографічні методи, що розглядаються в дослідженнях по БСМ, можна класифікувати наступним чином:

- Криптографія з відкритим ключем;
- Криптографія з симетричним ключем;
- Протоколи керування криптографічними ключами;
- Протоколи безпечної маршрутизації;
- Безпечна агрегація даних;
- Методи визначення вторгнень.

5.1. Криптографія з відкритим ключем

Більшість дослідників проблем інформаційної безпеки вважають, що використання криптографії з відкритим ключем є небажаним для застосування в БСМ. Прикладом криптографічних протоколів з відкритим ключем є протоколи Diffie-Hellman і RSA.

Криптографічні методи засновані на обчисленнях і зазвичай використовують кілька тисяч дій множення для виконання однієї операції. В умовах експлуатації вузлів в БСМ під впливом, наприклад DOS-атаки, криптографічні методи з відкритим ключем будуть проводити операції шифрування і дешифрування від десяти секунд до декількох хвилин. В дослідженні [5] в ході експерименту було виявлено, що мікропроцесору потрібні тисячі нано джоулів енергії для виконання простої операції множення з 128-

бітовим результатом. Криптографічні методи з використанням симетричного ключа витрачають значно менше ресурсів, ніж методи з відкритим ключем. Процесор MC68328 dragonball з використанням RSA витрачає близько 42 мдж на шифрування 1024-бітного блоку даних. А для 128-бітного блоку AES - споживання становить 0,106 мдж [5].

Дослідження [6] підтверджує, що застосування криптографічних методів на основі відкритих ключів можливо в БСМ, при їх оптимізації і зниженні споживання ними енергії.

Методи з використанням відкритого ключа представлені схемою Робіна, RSA і ECC. Більшість сучасних досліджень присвячені RSA і методу з використанням еліптичних кривих — ECC. Однією з переваг останнього є однакові показники безпеки при меншому розмірі ключа в порівнянні з RSA. Таким чином зменшується навантаження вузлів шляхом зниження витрат на обробку і передачу інформації.

Таблиця 2

Порівняння часу виконання операцій в ECC і RSA

Algorithm	Operation time (s)
ECC secp160rp1	0.81s
ECC secp224rp1	2.19s
RSA-1024 public-key e = 2^{16}+1	0.43s
RSA-1024 private key w. CRT[1]	10.99
RSA-2048 public-key e = 2^{16}+1	1.94s
RSA-2048 private-key w.CRT[1]	83.26
[1] Chinese Remainder Theory	

Таблиця 2 відображає тимчасове порівняння виконуваних операцій на процесорі Atmel atmega128 [7]. Часова характеристика виконання операції визначається в ECC середнім множенням точки, а в RSA за допомогою модулярної експоненційної. Представлені в таблиці 2 secp160r1 і secp224r1 — дві стандартизовані еліптичні криві ECC [8], а RSA використовує ціле число e = 2^{16} + 1 в якості відкритого ключа. Таким чином, при використанні розглянутого відкритого ключа, RSA зовсім трохи перевершує ECC в швидкодії. Однак, множення точки ECC перевершує RSA-операції секретного ключа на порядок. Операції секретних ключів в RSA мають високі часові характеристики, що робить використання методу в обмежених ресурсами сенсорних вузлах мережі слабо реалізованим. Так як в ECC операції з використанням відкритих і секретних ключів використовують однакові операції множення — аналогічна RSA проблема в методі ECC відсутня.

Результати дослідження енерговитрат на аутентифікацію і обмін ключами [9], з використанням шифрування RSA і ECC, представлені в таблиці 3. Ключі ECC створюються і піддаються перевірці з використанням алгоритму побудови цифрового підпису на основі еліптичних кривих (ECDSA). В даному випадку використовувався протокол обміну ключами, який представляє собою спрощену версію встановлення зв'язку SSL; в ній бере участь ініціатор зв'язку клієнт і сервер.

Таблиця 3

Витрати енергії на автентифікацію і обмін ключами на основі шифрування RSA та ECC

Algorithm	Signature		Key Exchange	
	Sign	Verify	Client	Server
RSA-1024	304	11.9	15.4	304
ECDSA-160	22.82	45.09	22.3	22.3
RSA-2048	2302.7	53.7	57.2	2302.7
ECDSA-224	61.54	121.98	60.4	60.4

Кожен сенсорний вузол мережі має сертифікат, який був підписаний базовим вузлом БСМ з використанням закритого ключа RSA або ECC. В даному процесі при використанні обох методів необхідно підтвердження виданих сертифікатів і узгодження ключів сеансу зв'язку. З таблиці 3 видно, що підпис ECDSA порівняно з RSA менше споживає енергії і в той же час перевірки ECDSA знаходяться в межах розумного діапазону перевірок RSA. Відповідно ECC має перевагу на стороні сервера і відсутня суттєва різниця енерговитрат на стороні клієнта. Відзначимо, що перевага ECC над RSA зростає при збільшенні розмірів ключів з точки зору часових характеристик і енерговитрат. Спираючись на наведені дослідження, можна зробити висновок, що використання ECC в БСМ більш ефективно, ніж RSA.

Незважаючи на наведені аргументи на користь використання криптографічних методів з відкритим ключем в БСМ, вони все одно є досить енерговитратними.

5.2. Криптографія з симетричним ключем

Внаслідок використання в пристроях БСМ малих енергоресурсів і слабких обчислювальних потужностей використання криптографічних методів з відкритим ключем обмежене. В даному пункті розглянемо ряд досліджень, основна увага яких приділяється криптографічним методам з використанням симетричних ключів в БСМ.

Найбільш поширеними алгоритмами шифрування з симетричним ключем є RC4, RC5, IDEA, MD5 і SHA-1. Згідно представленим результатами роботи[10] MD5 і SHA-1 викликали більше енергоспоживання ніж алгоритми шифрування RC4, RC5 і IDEA.

Робота [11] представляє собою порівняння і аналіз методів з використанням симетричного ключа RC5 і TEA. Крім того, в роботі були розглянуті наступні блокові шифри на системах IAR: RC5 і RC6, Rijndael, MISTY1, KASUMI і Camellia. Основними параметрами визначені обсяг коду, пам'ять даних і цикли CPU. В результаті проведених експериментів було встановлено, що Rijndael підходить для забезпечення високої безпеки та енергоефективності в БСМ, в той час як MISTY1 підходить для зберігання даних і забезпечує енергоефективність. В цілому дослідження можна позиціонувати як ресурс для визначення криптографічного методу з симетричним ключем для використання в БСМ.

У зв'язку з обмеженими ресурсами пристроїв БСМ, криптографічні методи з використанням симетричного ключа є більш пріоритетними для використання в мережах даного типу.

5.3. Використання протоколів управління криптографічними ключами в БСМ

Основним механізмом забезпечення безпеки мережевих сервісів і додатків БСМ є використання протоколів управління криптографічними ключами. Головна функція протоколів, це установка необхідних ключів між вузлами мережі, яким необхідно обмінюватися даними. Відзначимо, що вони повинні підтримувати можливість додавання і видалення вузлів з сенсорної мережі. По причині обмежених ресурсів пристроїв БСМ протоколи управління ключами в БСМ відрізняються від аналогічних рішень в ad-hoc мережах.

На підставі розглянутих раніше пунктів можна стверджувати, що більшість протоколів управління ключами засновані на криптографічних методах з симетричними ключами.

Рисунок 1 відображає класифікацію протоколів управління ключами в БСМ.

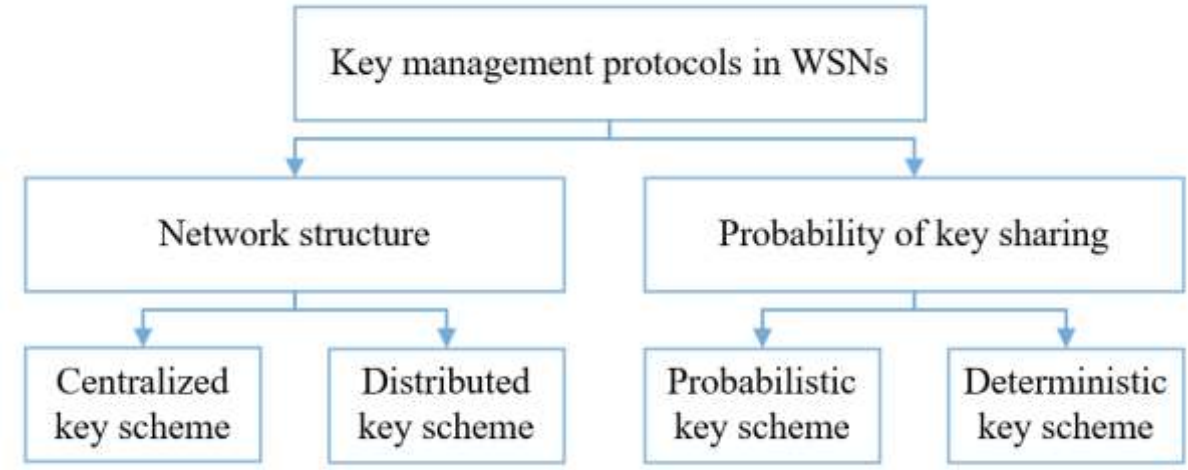

Рис. 1. Класифікація протоколів керування ключами в БСМ

Протоколи управління ключами в загальному вигляді можна класифікувати як централізовані і розподілені, а в залежності від ймовірності спільного використання ключа парою сенсорних вузлів, протоколи можна розділити на імовірнісні і детерміновані.

5.4. Використання протоколів безпечної маршрутизації

Безліч протоколів маршрутизації було розроблено спеціально для використання в БСМ. Їх можна класифікувати згідно до мережевої структури БСМ: flat-based маршрутизація, ієрархічна маршрутизація і маршрутизація на основі розташування.

При використанні flat-based маршрутизації мається на увазі, що всі вузли мають однакові функції, ролі в мережі і технічні характеристики пристроїв. Ієрархічна маршрутизація передбачає різні ролі пристроїв в мережі і їх різні технічні характеристики. Маршрутизація на основі розташування переважно використовує тільки інформацію щодо геолокації пристроїв мережі. Незважаючи на широку базу знань і рішень даного питання, тільки невелика частина розроблених протоколів маршрутизації здатна ефективно вирішувати проблему безпеки в БСМ. Зауважимо, що в

розглянутих протоколах здебільшого відсутні служби безпеки, що робить їх вразливими для більшості загроз БСМ.

Протоколи маршрутизації на основі ієрархії і розташування вузлів, які не використовують служби безпеки, також схильні до мережевих загроз[3]. Прикладом служить енергозалежна маршрутизація (GEAR), яка вимагає постійний обмін інформацією про місцезнаходження між сусідніми вузлами мережі.

Маршрутизація з використанням служб безпеки ad-hoc мереж аналогічна маршрутизації в БСМ і добре вивчена, проте застосовувані механізми забезпечення безпеки неможливо використовувати в сенсорних мережах через принципові відмінності технологій.

Протокол маршрутизації повинен гарантувати цілісність, автентифікацію і доступність інформації. Однак при наявності зовнішніх загроз мережі, якщо вони реалізуються за допомогою потужних пристроїв, розглянуті цілі можуть бути не досягнуті. Найкращий захист, на який може розраховувати мережа — це поступова відмова функціонування замість моментального виходу з ладу. Для реалізації такого підходу, необхідно, щоб робота протоколу маршрутизації погіршувалася повільніше, ніж зростала кількість скомпрометованих вузлів щодо всього обсягу вузлів в сенсорній мережі [3].

Варто зазначити, що протоколи безпечної маршрутизації в БСМ сильно залежать від використання протоколів управління криптографічними ключами, так як перед початком роботи протоколу маршрутизації вузлів мережі вже повинні бути видані ключі безпеки. Фундаментальним заходом безпеки в БСМ є широкомовна аутентифікація, за допомогою якої базова станція буде транслювати автентифіковані дані по всій сенсорної мережі.

5.5. Використання методів безпечної агрегації даних

Відправка інформаційних пакетів грає ключову роль у витрачанні енергоресурсів БСМ. Експеримент в роботі [4] визначає, що при використанні протоколу SNEP на передачу пакетів даних припадає понад 70% енерговитрат. Агрегація даних дозволить зменшити енергоспоживання мережі шляхом усунення надмірно деталізованих даних, що передаються в БСМ.

Для успішного застосування безпечної агрегації необхідно забезпечити аутентифікацію, конфіденційність і цілісність даних. Важливо відзначити, що агрегація даних вимагає коректної взаємодії вузлів-датчиків для ідентифікації шкідливих вузлів мережі.

Однак в даному аспекті спостерігається протиріччя між вимогами до конфіденційності та агрегування даних. Принципи конфіденційності мають на увазі передачу інформації в зашифрованих пакетах, в той час як агрегування зазвичай ґрунтується на відкритих даних. Простим рішенням даного протиріччя є наскрізне шифрування і дешифрування даних перед викликом функцій агрегації. Але проблема полягає в тому, що операції шифрування і дешифрування даних споживають значно більше енергії, що вкрай важливо в рамках БСМ.

5.6. Використання методів визначення вторгнень

Механізми безпеки, реалізовані в протоколах маршрутизації і агрегування даних, повинні перешкоджати злому безпеки мережі, проте вони не здатні забезпечити абсолютну безпеку БСМ. Так як вузли мережі можуть бути захоплені зловмисником, то не важко буде за їх допомогою впровадити в мережу неправдиві дані. Автентифікації і шифрування даних недостатньо для забезпечення повної безпеки. Інший підхід до захисту БСМ включає механізми для виявлення та реагування на вторгнення в мережу.

Система виявлення вторгнень (IDS) контролює хост або мережу в цілому для виявлення підозрілих дій за межами нормальної і очікуваної поведінки [2]. Вона заснована на припущенні, що існує помітна різниця в поведінці шкідливого і законного вузла мережі. На основі моделі аналізу виявлення вторгнень, IDS в ad-hoc мережах класифікуються на rule-based (засновані на правилах) і anomaly-based (засновані на аномаліях). IDS на основі правил мають низький рівень помилкових тривог, в той час як засновані на аномаліях - високий.

Однак БСМ, як правило, залежать від базової топології, нормального використання, очікуваних шаблонів зв'язку і т.д., тому недоцільно попередньо встановлювати деякі фіксовані шаблони в датчиках до їх розгортання. Більш того, через обмеження в вузлах сенсорної мережі, вивчення і виявлення цих параметрів після розгортання вимагає часу і енергії.

Таким чином, існуючі IDS в мережах ad-hoc не можуть бути адаптовані до БСМ. В даний час основна увага приділяється тому, як проводиться виявлення і усунення неправдивої інформації. Варто відзначити, що скомпрометовані вузли завжди можуть вводити неправдиву інформацію в сенсорну мережу. Таким чином, коректна комунікація сусідніх вузлів необхідна для прийняття рішень по загрозам в мережі.

6. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

В даній роботі була досліджена і проаналізована проблематика забезпечення ІБ в БСМ; досліджені основні групи і типи загроз, а також розглянуті актуальні рішення розглянутої проблеми в даний час.

Обґрунтована потреба в забезпеченні інформаційної безпеки, оскільки можливості БСМ безперервно ростуть і все більше сфер діяльності знаходить застосування даної технології. Визначено, що характеристики вузлів БСМ сильно обмежують реалізацію вже існуючих методів забезпечення безпеки в рамках даної технології.

Виявлено, що в більшості проведених досліджень [12] - [14] хоча і обговорюється безпека сенсорних мереж, тільки деякі з них враховують унікальні обмеження БСМ. Проблеми безпеки в БСМ простежуються на кожному мережевому рівні, вирішення яких полягає в застосуванні криптографії, управління ключами, захищеної маршрутизації, безпечної агрегації даних і виявленні вторгнень. Незважаючи на те, що обговорювані методи безпеки викликають підвищене енергоспоживання, вони вкрай необхідні і часто використовуються в реальних сенсорних мережах.

У майбутній роботі планується розробити математичну модель для визначення і аналізу ступеня впливу загроз на інформаційну безпеку в БСМ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] “System architecture directions for networked sensors” / J. Hill et al. ACM SIGARCH Computer Architecture News. 2000. Vol. 28, no. 5. P. 93-104. URL: https://doi.org/10.1145/378995.379006 (date of access: 17.09.2020).
[2] Jain U., Hussain M. “Wireless Sensor Networks: Attacks and Countermeasures”. SSRN Electronic Journal. 2018. URL: https://doi.org/10.2139/ssrn.3170185 (date of access: 17.09.2020).
[3] Karlof C., Wagner D. “Secure routing in wireless sensor networks: attacks and countermeasures”. Ad Hoc Networks. 2003. Vol. 1, no. 2-3. P. 293-315. URL: https://doi.org/10.1016/s1570-8705(03)00008-8 (date of access: 17.09.2020).
[4] Perrig et al., “SPINS: Security Protocols for Sensor Networks”, Wireless Networks, vol. 8, no. 5, Sept. 2002, pp. 521–34.
[5] “Constraints and approaches for distributed sensor network security”, NAI Labs, Tech. Report 00-010, 2000
[6] M. O. Rabin, “Digitalized Signatures and Public-Key Functions as Intractable as Factorization”, Tech. Rep., Cambridge, MA, 1979.
[7] “Recommended Elliptic Curve Domain Parameters”, SECG Std. SEC2, 2000. URL: www.secg.org/SEC2-Ver-1.0.pdf (date of access: 17.09.2020).
[8] A. S. Wander, “Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks”, Third IEEE International Conference on Pervasive Computing and Communications, Mar. 2005., doi: 10.1109/PERCOM.2005.18
[9] Hankerson, D., Vanstone, S. And Menezes, A., 2011. “Guide To Elliptic Curve Cryptography”. New York: Springer.
[10] Y. W. Law et al., “Assessing Security-Critical Energy-Efficient Sensor Networks”, Proc. 18th IFIP TC11 Int'l. Conf. Info. Security, Security, and Privacy in the Age of Uncertainty (SEC), Athens, Greece, May 2003, pp. 459– 63.
[11] Y. W. Law, J. M. Doumen, and P. H. Hartel, “Benchmarking Block Ciphers for Wireless Sensor Networks (Extended Abstract)”, 1st IEEE Int'l. Conf. Mobile Ad-hoc and Sensor Systems, IEEE Computer Society Press, Oct. 2004.
[12] Семенов, Ю. В. Умные всепроникающие сети / Ю. В. Семенов, А. Е. Кучерявый, В. О. Пяттаев. - «Экспо – Телеком», 2011. – С. 44–47.
[13] Кучерявый, А. Е. Самоорганизующиеся сети / А. В. Прокопьев, Е. А. Кучерявый. – спб. : Любавич, 2011. – 312 с.
[14] Recommendation X.1311. Security Framework for Ubiquitous Sensor Networks // ITU-T, Geneva. — February 2011.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (10), 2020
ISSN 2663 - 4023

Andrii Karpenko
Researcher
Military Institute of Telecommunication and Information Technologies named after the Heroes of Kruty, Kyiv, Ukraine
ORCID: 0000-0002-8372-6303

Tetiana Bondarenko
Researcher
Military Institute of Telecommunication and Information Technologies named after the Heroes of Kruty, Kyiv, Ukraine
ORCID: 0000-0002-2879-2041

Viacheslav Ovsiannikov
Leading researcher
Military Institute of Telecommunication and Information Technologies named after the Heroes of Kruty, Kyiv, Ukraine
ORCID: 0000-0003-0186-6220

Valerii Martyniuk
Leading researcher
Military Institute of Telecommunication and Information Technologies named after the Heroes of Kruty, Kyiv, Ukraine
ORCID: 0000-0003-0244-7861

ENSURING INFORMATION SECURITY IN WIRELESS SENSOR NETWORKS

Abstract. The problem of information security in wireless sensor networks is considered in this paper. An analysis of existing recommendations for information security in wireless sensor networks. It was found that one of the key problems of information security is the hardware limitations of the sensor nodes of the network. It is substantiated that the use of more complex cryptographic protection mechanisms will increase the load on the network. Safety requirements and their description are given. The main groups and types of information security threats in wireless sensor networks are considered. The classification of attacks and protection of wireless sensor networks according to the OSI model is presented. The existing solutions for information security are considered and analyzed. The shortcomings and vulnerabilities of the considered solutions are revealed. The method of public key cryptography is considered, the main advantages and disadvantages of this method are revealed. The analysis and comparison of ECC and RSA encryption methods are carried out. It is substantiated that the use of ECC in wireless sensor networks is more efficient than RSA. The method of cryptography with a symmetric key is considered, the main advantages and disadvantages of this method are indicated. It was found that cryptographic methods using a symmetric key are more priority for use in wireless sensor networks. Cryptographic key management protocols in wireless sensor networks are considered. The classification of key management protocols is given. Secure routing protocols are considered. The classification of secure routing protocols is given. Methods of secure data aggregation are considered. Contradictions between the requirements for confidentiality and data aggregation have been revealed. The method of intrusion detection is considered, the main advantages and disadvantages of this method are revealed. The results of this work should be used in the design of wireless sensor networks.

Keywords: wireless sensor network; information security; OSI network model; authentication; cryptography; intrusion detection system.

REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] "System architecture directions for networked sensors" / J. Hill et al. ACM SIGARCH Computer Architecture News. 2000. Vol. 28, no. 5. P. 93-104. URL: https://doi.org/10.1145/378995.379006 (date of access: 17.09.2020).
[2] Jain U., Hussain M. "Wireless Sensor Networks: Attacks and Countermeasures". SSRN Electronic Journal. 2018. URL: https://doi.org/10.2139/ssrn.3170185 (date of access: 17.09.2020).
[3] Karlof C., Wagner D. "Secure routing in wireless sensor networks: attacks and countermeasures". Ad Hoc Networks. 2003. Vol. 1, no. 2-3. P. 293-315. URL: https://doi.org/10.1016/s1570-8705(03)00008-8 (date of access: 17.09.2020).
[4] Perrig et al., "SPINS: Security Protocols for Sensor Networks," Wireless Networks, vol. 8, no. 5, Sept. 2002, pp. 521–34.
[5] "Constraints and approaches for distributed sensor network security", NAI Labs, Tech. Report 00-010, 2000
[6] M. O. Rabin, "Digitalized Signatures and Public-Key Functions as Intractable as Factorization", Tech. Rep., Cambridge, MA, 1979.
[7] "Recommended Elliptic Curve Domain Parameters", SECG Std. SEC2, 2000. URL: www.secg.org/SEC2-Ver-1.0.pdf (date of access: 17.09.2020).
[8] A. S. Wander, "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks", Third IEEE International Conference on Pervasive Computing and Communications, Mar. 2005., doi: 10.1109 / PERCOM.2005.18
[9] Hankerson, D., Vanstone, S. And Menezes, A., 2011. "Guide To Elliptic Curve Cryptography". New York: Springer.
[10] Y. W. Law et al., "Assessing Security-Critical Energy-Efficient Sensor Networks", Proc. 18th IFIP TC11 Int'l. Conf. Info. Security, Security, and Privacy in the Age of Uncertainty (SEC), Athens, Greece, May 2003, pp. 459– 63.
[11] Y. W. Law, J. M. Doumen, and P. H. Hartel, "Benchmarking Block Ciphers for Wireless Sensor Networks (Extended Abstract)," 1st IEEE Int'l. Conf. Mobile Ad-hoc and Sensor Systems, IEEE Computer Society Press, Oct. 2004.
[12] Semenov, Yu. V. Smart all-penetrating networks / Yu. V. Semenov, AE Kucheryavy, VO Pyattaev. - «Expo - Telecom», 2011. - P. 44–47.
[13] Kucheryavy, AE Self-organizing networks / AV Prokopyev, EA Kucheryavy. - спб. : Любавич, 2011. - 312 с.
[14] Recommendation X.1311. Security Framework for Ubiquitous Sensor Networks // ITU-T, Geneva. - February 2011.

(cc) BY-NC-SA
This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.