УДК 004.056

# ПРИНЦИПИ РЕАЛІЗАЦІЇ АТАК НА ПРОМИСЛОВИЙ ІНТЕРНЕТ РЕЧЕЙ ТА ЗАСОБИ ПРОТИДІЇ

В. Ю. Кисіль[1], І. В. Стьопочкіна[1]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

**Анотація**

В роботі досліджено склад засобів промислового Інтернету речей, побудовано модель загроз для протоколів Industrial IoT. Виділено основні вразливості та запропоновано покращення безпеки у протоколі Modbus.

*Ключові слова*: Internet of Things, SCADA-системи, протоколи обміну даними, атака, вразливість, промисловий Інтернет речей

## Вступ

Інтернет речей (англ. Internet of Things, IoT) – це способи взаємодії фізичних об'єктів, пристроїв і систем між собою і з навколишнім світом із застосуванням різних технологій зв'язку і стандартів з'єднання.

Періодом бурхливого розвитку Інтернету речей стали 2000-і. Тоді як в 1990-х вся діяльність, пов'язана з IoT, носила в основному теоретичний характер – концепції, обговорення, окремі ідеї, в 2000-х і 2010-х стали масово з'являтися і запускатися успішні IoT-проекти в реальності. Крім того, почали розвиватися масштабні проекти, засновані на технологіях IoT – розумні міста, розумне виробництво, розумний транспорт, безпілотні автомобілі і багато іншого. Не в останню чергу це стало можливим завдяки активному прогресу в сфері інформаційних технологій – повсюдного поширення бездротового з'єднання, підвищення пропускної здатності інтернет-зв'язку, виникнення енергоефективних мереж дальнього радіусу дії і ін.[1].

Сфери застосування технологій Інтернету речей вкрай великі. Тому очевидною є важливість використання в їх функціонуванні найактуальніших методів захисту від вразливостей та атак.

## 1. Модель загроз для засобів промислового Інтернету речей

Розглянемо модель загроз для основних протоколів обміну даними промислового Інтернету речей (Табл. 1).

З таблиці 1 можна визначити, що Modbus є найбільш поширеним протоколом, що використовується в SCADA-системах. Він не є захищеним, так як відсутня аутентифікація та шифрування. Тому дуже важливо покращити його захищеність з точки зору безпеки.

## 2. Способи зв'язку в Industrial IoT

Задачі, які вирішує провідний зв'язок для IIoT [2]:

- Обмін технологічною інформацією між блоками АСУ ТП;
- Передача керуючих сигналів між центром управління та технологічною лінією;
- Комунікації між контролерами і підключення до них датчиків і виконуючих пристроїв;
- Фізична захищеність каналу зв'язку;

Задачі, які вирішує безпровідний зв'язок для IIoT:

- Віддалене керування (Industry 4.0, керування роботами);
- Одержання характеристик зовнішнього середовища(температура, час і т.д.);
- Синхронізація процесів у віддалених філіях промислової установи;
- Велика дальність передачі даних;
- Низьке енергоспоживання;
- Комплексна безпека і вбудовані ідентифікація і аутентифікація;

## 3. Склад засобів промислового Інтернету речей

До складу Industrial IoT входять [2]:

- SCADA-система;
- АСУ ТП(автоматизована система управління технологічним процесом);
- Центр обробки даних;
- Сенсори, лічильники, датчики, регулятори, програмно-логічні контролери;
- Зовнішнє середовище для зберігання даних(хмарні технології);

Засоби промислового Інтернету речей зображено на рис. 1.

Табл. 1. Модель загроз для промислового Інтернету речей

| Протоколи | Рівень | Задачі | Вразливості | Топологія |
|---|---|---|---|---|
| Modbus (провідний) | Фізичний Канальний Прикладний | Організація зв'язку між цифровими пристроями в області релейного захисту і автоматики. Може використовуватись для передачі даних через послідовні лінії зв'язку RS-485, RS-422, RS-232, а також мережі TCP/IP (Modbus TCP). Розроблений для використання в програмно-логічних контролерах. | Відсутні аутентифікація і шифрування. Комунікація проходить в незахищеному режимі. | Шина |
| CAN (Controller Area Network), (провідний) | Фізичний Канальний Прикладний (CANopen, DeviceNet) | Об'єднання в єдину мережу різних виконуючих пристроїв і датчиків. Зв'язок даних в пересувних системах, машинах, технічному обладнанні й промисловій автоматизації | Невелика кількість даних, які можна передати в одному пакеті(до 8 байт). Великий розмір службових даних в пакеті. Незахищений заголовок. Переповнення буфера. | Шина |
| DNP3 (Distributed Network Protocol), (провідний) | Фізичний Канальний Прикладний | Підтримка роботи з подіями типу: зміна стану і подія з міткою часу. Обмін даними по мережах Ethernet і через інтерфейси RS232/RS485. Використання при передачі повідомлення великого розміру. Широкомовна розсилка повідомлень. Віддалене конфігурування програмно-логічних контролерів. Наявне розширення для безпечної аутентифікації. | Атака «людина посередині». Переповнення довжини поля. | Точка-точка, шина, зірка, дерево |
| 6LoWPAN (безпровідний) | Канальний Мережний | Забезпечити взаємодію безпровідних персональних мереж IEEE 802.15 з мережами IP. Стиснення заголовка IP пакета. Зменшення споживання електроенергії. | Відмова в обслуговуванні. Атака на фрагментацію пакетів. | Mesh-мережа |
| LoRaWAN (безпровідний) | Канальний | Сумісність з існуючими мережами/технологіями безпровідної передачі даних. Обслуговування десятків-сотень тисяч пристроїв. Забезпечення великої зони дії і малого енергоспоживання кінцевих пристроїв. Зчитування показників лічильників газу, води, електроенергії. | Атаки eavesdropping, bit flipping, ACK spoofing, replay attack. | Зірка |
| SigFox (безпровідний) | Фізичний | Передача невеликого об'єму даних. Забезпечення великого територіального охоплення безпровідною мережею. Застосування: безпровідні сенсорні мережі, автоматизація збору показань пристроїв обліку, системи промислового моніторингу і керування. | Відсутнє шифрування | Зірка |

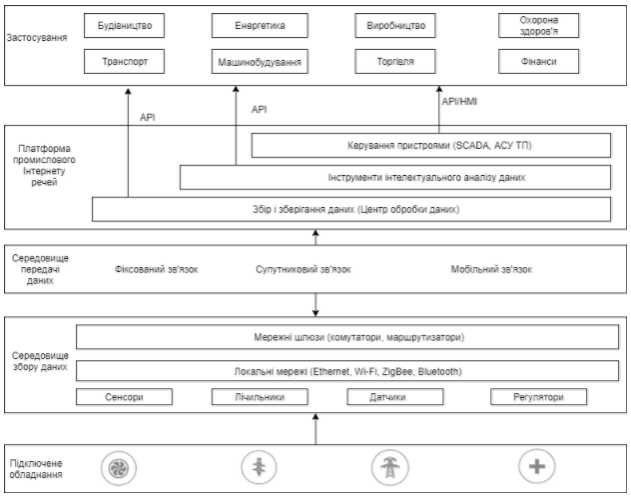


Рис. 1. Структура промислового Інтернету речей

## 4. Оцінка вразливостей протоколу обміну даними Modbus

Як бачимо з Рис. 2, в протоколі Modbus можна виділити такі 2 вразливості: CVE-2017-6032 та CVE-2017-6034 [3].

**Опис CVE-2017-6032.** Протокол Modbus, що використовує Schneider Electric, є вразливим до атаки повним перебором, викликаної недоліком слабкості, пов'язаної з сеансами. Використовуючи технологію повного перебору, віддалений атакуючий може використовувати цю вразливість для отримання інформації про сеанс(в тому числі логін і пароль) [4].

**Опис CVE-2017-6034.** Протокол Modbus, що використовує Schneider Electric, може дозволити віддаленому зловмисникові обійти обмеження безпеки, яке викликане неможливістю застосування механізму шифрування в протоколі обміну даними Modbus. Перехопивши трафік обміну даними протоколу Modbus, віддалений атакуючий може використовувати цю вразливість для відтворення команд, таких як запуск, зупинка, вивантаження та завантаження даних [5].

Обидві вразливості спричинені відсутністю захищеної аутентифікації та шифрування. Тому необхідно покращити аутентифікацію, додавши перевірку TLS. Це дозволить передавати логін та пароль користувача у зашифрованому вигляді, при цьому буде збережена цілісність інформації.

## 5. Напрямки покращення аутентифікації Modbus

Розглянемо структуру пакета Modbus TCP (Рис. 3) [6].

**Варіанти впровадження покращень при передачі даних із використанням Modbus.**

1) Варіант 1. Пакет Modbus із впровадженими до поля даних полями перевірки: нове поле= ЕЦП(поле даних Modbus). Недоліки: заголовки пакета прикладного рівня Modbus не контролюються ЕЦП, яке формується на нижчому рівні.
2) Варіант 2. Інкапсуляція пакета Modbus до іншого мережного пакета, на прикладному рівні у який додається заголовок із перевіркою цілісності всіх полів Modbus (в тому числі, сформованих на прикладному рівні). Переваги: повнота контролю цілісності, унеможливлення порушень автентичності відправника; Недоліки: зменшення швидкодії, можливість перевищення максимальних розмірів пакета, необхідність використання додаткового програмного шлюза.
3) Варіант 3. Поле даних Modbus шифрується/дешифрується, додається нове поле=ЕЦП (поле даних Modbus). Переваги: забезпечення конфіденційності, забезпечення автентифікації відправника. Недоліки: зменшення швидкодії (при використанні асиметричного шифрування); необхідність обміну таємним ключем між приймачем та одержувачем (при симетричному шифруванні).

Для реалізації доцільно обрати варіанти 1 та 3, для чого розробити програмний застосунок із реалізацію криптографічних функцій на основі бібліотеки OpenSSL.

Також ефективно буде використати інфраструктуру відкритого ключа: Враховуючи особливості процесу обміну даними в промисловому Інтернеті речей пропонується надавати сертифікати кожному застосунку, який відповідає за обмін даними із відповідним пристроєм на низькому рівні. Таємне значення ключа пропонується зберігати у захищеній області пам'яті (якщо застосунок мобільний), чи забороняти доступ до нього засобами операційної системи. Таємне значення ключа сервера, що виконує функції центра сертифікації ключів, пропонується зберігати на пристрої, який забезпечує всебічний захист від несанкціонованого доступу (наприклад, засоби типу Гряда). Для контролю актуальності сертифікатів варто використовувати принцип швидкого застарівання сертифікатів, впровадження якого не потребує щоразового звертання до центра сертифікації для контролю актуальності та статусу сертифікату. Однак, списки відкликаних сертифікатів все одно рекомендовано вести на сервері, де зберігаються сертифікати відкритого ключа. Внаслідок стабільних інформаційних потоків та сталих зв'язків між промисловими пристроями дані про відкриті ключі абонентів можуть а) одержуватись шляхом звертання до серверу відповідних сертифікатів відкритого ключа (для зовнішніх систем та пристроїв) б) тимчасово зберігатись у кеш-пам'яті (для внутрішніх систем та пристроїв) (однак, це потребує унеможливлення доступу до кеша сторонніми засобами).

Застосунок має наступну структуру:

- Модуль аналізу пакету (встановлення зміщень полів, звертання до даних);
- Модуль ЕЦП (використовуються функції OpenSSL (на основі RSA чи еліптичних кривих));

Schneider-electric » Modbus Firmware : **Security Vulnerabilities**

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

| # | CVE ID | CWE ID | # of Exploits | Vulnerability Type(s) | Publish Date | Update Date | Score | Gained Access Level | Access | Complexity | Authentication | Conf. | Integ. | Avail. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | CVE-2017-6034 | 287 | | Bypass | 2017-06-29 | 2017-07-06 | 7.5 | None | Remote | Low | Not required | Partial | Partial | Partial |

An Authentication Bypass by Capture-Replay issue was discovered in Schneider Electric Modicon Modbus Protocol. Sensitive information is transmitted in cleartext in the Modicon Modbus protocol, which may allow an attacker to replay the following commands: run, stop, upload, and download.

| 2 | CVE-2017-6032 | 358 | | | 2017-06-29 | 2017-07-06 | 5.0 | None | Remote | Low | Not required | Partial | None | None |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

A Violation of Secure Design Principles issue was discovered in Schneider Electric Modicon Modbus Protocol. The Modicon Modbus protocol has a session-related weakness making it susceptible to brute-force attacks.

Total number of vulnerabilities : 2 Page : 1 (This Page)

Рис. 2. Типові вразливості протоколу Modbus

| 2 байти | 2 байти | 2 байти | 1 байт | 1 байт | до 252 байт |
|---|---|---|---|---|---|
| ID транзакції | ID протоколу | довжина пакету | адреса підлеглого пристрою | код функції | дані (інформаційне поле) |

Рис. 3. Структура пакета Modbus TCP

- Модуль шифрування (за вимогою, можна встановити індикатор чи треба шифрувати дані всередині пакета).

Мова написання застосунку: C++ або Java.

## Висновки

Систематизовано інформацію по використанню спеціальних мережних протоколів в області промислового Інтернету речей, запропоновано модель загроз. Досліджено властивості популярного протоколу Modbus TCP, встановлено причини його потенційної небезпечності. Запропоновано покращення даного протоколу із використанням ЕЦП та шифрування.

## Перелік використаних джерел


1. Интернет вещей. — 2017. — Режим доступа `https://iot.ru/wiki/internet-veshchey`.
2. Industrial Internet of Things — IIoT Промышленный интернет вещей. — 2018. — Режим доступа: http://www.tadviser.ru/index.php/Статья:IIoT_-_Industrial_Internet_of_Things_(Промышленный_интернет_вещей).
3. CVE Details – The ultimate security vulnerability datasource. — 2017. — Access mode: `https://www.cvedetails.com`.
4. Отчет X-Force об уязвимостях CVE-2017-6032. — Режим доступа: `https://exchange.xforce.ibmcloud.com/vulnerabilities/124447`.
5. Отчет X-Force об уязвимостях CVE-2017-6034. — Режим доступа: `https://exchange.xforce.ibmcloud.com/vulnerabilities/124448`.
6. Aamir Shahzad, Malrey Lee, Young-Keun Lee, Suntae Kim, Naixue Xiong, Jae-Young Choi, Younghwa Cho Real Time MODBUS Transmissions and Cryptography Security Designs and Enhancements of Protocol Sensitive Information. — Symmetry 2015, 7, 1176-1210; doi:10.3390/sym7031176. — С. 1–35 с.