УДК 62.519

БЕЗДРОТОВА СИСТЕМА ЗВ'ЯЗКУ ДАВАЧІВ ПЕРИМЕТРАЛЬНОЇ СИСТЕМИ ОХОРОНИ НА ОСНОВІ ПРОТОКОЛУ LORAWAN

М. М. Копанєв[1, a], Д. О. Прогонов[1]

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

Анотація

Забезпечення раннього виявлення порушників контрольованої зони є важливою задачею. Вирішення даної задачі потребує розробки комплексної системи периметрального захисту об'єкту інформаційної діяльності. Особлива увага при створенні даної системи приділяється побудові захищених каналів передачі від давачів системи захисту. В роботі запропоновано використовувати протокол передачі LORAWAN для швидкої та надійної передачі інформації від давачів до центру обробки. Розроблено програмний додаток для аналізу, дешифрування і протидії підміни даних. За результатами порівняльного аналізу існуючих систем зв'язку давачів та розробленого прототипу показано переваги використання протоколу LORAWAN, зокрема підвищення захищеності каналів зв'язку до підмині даних.

Ключові слова: периметральна система захисту, Інтернет речей, протокол LoRaWAN, фізичні давачі

Вступ

Периметральна система захисту (СЗ) є комплексом фізико-технічних засобів для протидії несанкціонованих проникнень на територію об'єкта інформаційної діяльності [1]. Забезпечення раннього виявлення порушників контрольованої зони (КЗ) потребує використання фізичних давачів і системи збору та аналізу їх показів. Дана система повинна забезпечувати задану ймовірність виявлення порушення периметру при мінімальних затримках передачі даних від сенсорів. Зважаючи на необхідність швидкого і безпечного транспортування інформації каналом зв'язку, становить інтерес побудова захищеної системи передачі показів давачів до центру обробки з використанням спеціалізованих протоколів зокрема, LoRaWAN (Long Range Wide Area Network).

1. Постановка задачі

Переважна більшість проблем безпеки даних у існуючих СЗ створюються на етапі проектування [3]. Незважаючи на науково–технічний розвиток, СЗ продовжують розробляти на поширених протоколах зв'язку, зокрема TCP/IP які не захищають канал передачі інформації від активних (підміна даних) та пасивних (прослуховування каналу) атак. Тому актуальною та важливою задачею є розробка новітніх систем зв'язку елементів СЗ, що дозволить ефективно протидіяти активним та пасивним атакам. Становить інтерес застосування малопотужних захищених систем зв'язку для Інтернету речей (англ. IoT), зокрема заснованих на протоколі LoRaWAN. Метою дослідження є визначення структури побудови та необхідних компонент системи збору, моніторингу і аналізу даних в режимі реального часу для об'єкту із попередньо встановленою системою захисту з використанням протоколу LoRaWAN.

2. Пропонований аналог

В роботі розглянуто випадок захисту прототипу СЗ, що включає декілька рубежів охорони об'єкту. Перший рубіж представлений цегляним парканом висотою 2 метри. На другому рубіжі (внутрішніх сторонах паркану) розташовані двосторонні активні інфрачервоні детектори. Вібраційний кабель (ВК) заведено у земляний покрив біля паркану із дотиком до огородження. ВК застосовується для виявлення зловмисника, що оминув інфрачервоні сенсори, зокрема для фіксування підкопів, стрибків через огородження, тощо. Третій рубіж виявлення порушника складають радіохвильові (РХ) випромінювачі, розташовані на відстані одного метру від паркану. РХ–випромінювачі формують еліпсоподібне поле висотою 3 метри и шириною до 5 метрів.

В роботі пропонується підключення давачів до мережі збору і обробки інформації з використанням бездротового протоколу зв'язку LoRaWAN, що забезпечує захищену від прослуховування передачу інформації до центру обробки. Ієрархія вузлів зв'язку складається з давача (сенсора), Шлюзу обміну повідомленнями, Мережевого серверу і Серверу додатків [4]. Датчик поєднується із модулем прийому–передачі даних, що формує пакет даних, оброблює (шифрує) і надсилає до Шлюзу. Послідовне подвійне шифрування даних, зроблене на рівні давачів, дозволяє Шлюзу перетворювати радіосигнал на цифровий і безпечно передавати дані до Мережевого сервера. Сервер регулює взаємодію датчиків і Шлюзів, зокрема їх своєчасне опитування. На наступному

[a] morbiyccc@gmail.com

кроці Сервером додатків проводиться декодування інформації. Також Сервер додатків застосовується для сортування, зберігання і візуалізації даних.

3. Результати

В ході дослідження із використанням середовища програмування NI LabVIEW розроблено прототип СЗ, що модулює приймання інформації з давачів. Розроблений додаток (рис. 1) дозволяє імітувати послідовну підміну даних під час вимірювання чи передачі інформації, і попереджувати про це оператора, слідкувати за цілісністю захисту у режимі реального часу і презентувати інформацію у зручному вигляді. Додаток забезпечує виявлення порушника, інформування про порушення встановлених цільових показників, декодування зашифрованих даних, зберігання інформації (наприклад, у файли, локальні і хмарні бази даних), ведення журналу прийнятих запитів, графічне і аналітичне представлення відомостей та інструменти швидкого налаштування параметрів сигналізації.

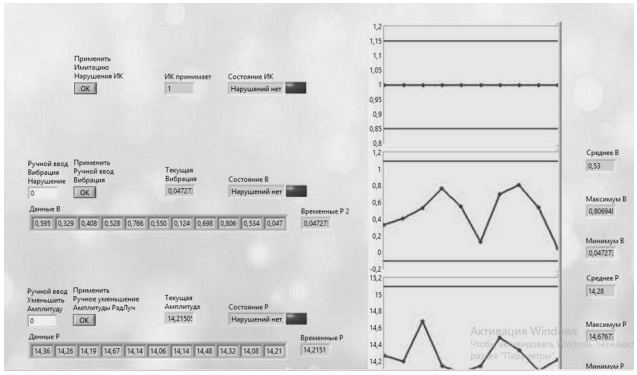

Рис. 1. Розроблений у середовищі NI LabView додаток

Одним із типових представників СЗ є комплекс, заснований на кабельній структурі зв'язку із давачами, зокрема система швидкого розгортання СЗ периметру об'єкта «Гербіцид». Прикладом бездротової радіохвильової СЗ швидкого розгортання є «FORTEZA–12» [5].

Для порівняння існуючих систем та запропонованого прототипу були обрані наступні показники: радіус опитування, кількість давачів, можливість швидкого розгортання СЗ в умовах нестачі часу, наявність первинної обробки даних у мікроконтролері давача, безпечна автентифікація сенсорів при з'єднанні зі Шлюзом, регулярне оновлення аутентифікації датчиків, шифрування первинних даних перед передачею, ймовірність підміни первинних даних, степінь захищеності каналу зв'язку від прослуховування, ймовірність атаки повторення на давач і відмова пристрою в обслуговуванні. Результати порівняння наведені у таблиці 1.

Запропонований прототип на основі протоколу LoRaWAN дозволяє суттєво підвищити радіус опитування давачів і чисельність підключених сенсорів у порівнянні з існуючими аналогами (таблиця 1). Забезпечення безпечної аутентифікації датчиків та подвійне шифрування даних для протоколу LORAWAN суттєво ускладнює прослуховування каналу зв'язку та зменшує можливості атаки повторення і відмови в обслуговуванні. Необхідність використання декількох Шлюзів/Серверів для надійної обробки даних зі значної кількості давачів ускладнює швидке розгортання системи. Крім того, через малий розмір пакету даних у протоколі LoRaWAN відсутня первинна обробки даних. Для подолання даного обмеження в роботі запропоновано використання функцій обробки за допомогою розробленого програмного модулю.

Табл. 1. Порівняння типових існуючих на ринку СЗ із запропонованим аналогом

Характеристика	Системи захисту		
	На основі протоколу LoRaWAN	«FORTEZA-12»	«Гербіцид»
Радіус опитування у місті, м	~1.300	~500	~200
Кількість давачів	до 60.000	до 48	До 1.000
Швидке розгортання СЗ	ні	так	так
Первинна обробка даних	ні	так	ні
Безпечна автентифікація давачів	так	ні	ні
Оновлення автентифікації давачів	так	ні	Лише за участі оператора
Шифрування первинних даних	Так, подвійне	ні	ні
Можливість фальсифікації первинних даних	Дуже мала	мала	істотна
Прослуховування каналу зв'язку	Сильно ускладнене	так	так
Атака повторення	неможлива	можлива	можлива
Відмова в обслуговуванні	Сильно ускладнене	ускладнене	можливе

Висновки

В роботі запропонована побудова СЗ із використанням протоколу LoRaWAN для зв'язку між давачами периметральної системи захисту об'єкта інформаційної діяльності. Розроблено програму диспетчерського контролю за показами фізичних давачів. Показано здатність розробленої програми адаптуватися у режимі реального часу для детектування підміни даних, проникнення зловмисника на територію, здатність інформувати оператора як індикацією, так і через електронну поштову скриньку.

Перелік використаних джерел

1. Arata, M. (2005). Perimeter Security
2. National Instruments (March 19, 2019) (//www.ni.com/white-paper/53954/en/)
3. Humayed, A. Lin, J., Li, F., Luohttps, B.(2017). Cyber-Physical Systems Security. Cornell University (//arxiv.org/pdf/1701.04525.pdf).
4. LoRa Alliance (//lora-alliance.org/about-lorawan).
5. Іванов І. (2000). Охрана периметров: ПАРИТЕТ ГРАФ, Москва