УДК 621.391:355.4

В. А. Роздільська

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ PLC ДЛЯ ПІДВИЩЕННЯ РАДІОЕЛЕКТРОННОЇ ПРИХОВАНОСТІ ПУНКТІВ УПРАВЛІННЯ В УМОВАХ ІНТЕНСИВНОЇ РОЗВІДКИ ПРОТИВНИКА

Анотація. *Розглянуто можливість застосування технології передавання даних по силових лініях (Power Line Communication, PLC) для організації внутрішніх каналів обміну даними на пунктах управління з метою зниження їх радіоелектронної помітності. Проаналізовано демаскувальні ознаки радіоканалів Wi-Fi та обмеження кабельних мереж Ethernet щодо часу розгортання. Запропоновано принципи побудови PLC-мережі пункту управління та заходи, що обмежують побічне випромінювання і витік сигналу в зовнішню мережу живлення.*

Ключові слова: *пункт управління; PLC; радіоелектронна розвідка; радіоелектронна прихованість; канал обміну даними.*

Abstract. *The possibility of using Power Line Communication (PLC) technology to organize internal data exchange channels at command posts in order to reduce their radio-electronic signature is considered. The revealing features of Wi-Fi radio channels and the deployment-time limitations of wired Ethernet networks are analyzed. Principles for building a command-post PLC network are proposed, together with measures that limit unintended emission and signal leakage into the external power supply network.*

Keywords: *command post; PLC; electronic reconnaissance; radio-electronic covertness; data exchange channel.*

Вступ

Досвід збройної агресії проти України свідчить про те, що пункти управління (ПУ) всіх рівнів є пріоритетними об’єктами розвідки противника. Основним джерелом даних про їх розташування залишається радіоелектронна розвідка (РЕР). Засоби пеленгації дають змогу визначати координати джерел радіовипромінювання за кількома рознесеними пунктами, які визначають напрямки приходу сигналу [1]. Кожен радіоканал, що працює на ПУ, є демаскувальною ознакою, а виявлення ПУ безпосередньо загрожує його ураженням.

Для внутрішнього обміну даними між робочими місцями, серверним обладнанням і засобами зв’язку на ПУ часто застосовують бездротові мережі Wi-Fi, оскільки вони мають достатньо малий час розгортання. Проте точка доступу згідно зі специфікацією IEEE 802.11 періодично передає маякові кадри приблизно кожні 100 мс навіть за відсутності корисного трафіку [2]. Таким чином випромінювання здійснюється безперервно, а його частота, рівень і ідентифікатори чітко фіксуються засобами РЕР. Кабельна мережа Ethernet практично не випромінює, але її розгортання вимагає більшого часу, а при зміні позиції ПУ – повторного прокладання та згортання ліній. Це зумовлює пошук рішення, що поєднує таки переваги як швидкість розгортання для бездротових мереж та низький рівень випромінювання для кабельних мереж.

Метою роботи є обґрунтування можливості застосування технології PLC для побудови внутрішніх каналів обміну даними на ПУ та визначення заходів, що забезпечують її радіоелектронну прихованість.

Результати дослідження

Принцип дії PLC полягає в передаванні інформаційного сигналу провідниками електроживлення, які вже є на ПУ. Широкосмугові системи на основі стандартів IEEE 1901 та ITU-T G.9960 (G.hn) використовують ортогональне частотне мультиплексування (OFDM) у діапазоні від 2 МГц до кількох десятків мегагерц, а сигнал накладається на напругу живлення 230 В/50 Гц через вбудований розв’язувальний фільтр [3, 4]. Вузлом мережі є адаптер, що вмикається в розетку, тому окремий кабель прокладати не потрібно, а розгортання зводиться до підключення пристроїв до наявної електромережі [5, 6]. Стандарти передбачають вбудоване шифрування даних алгоритмом AES-128 [3, 4]. Порівняльну характеристику технологій організації локальної мережі ПУ наведено в таблиці 1.

Таблиця 1 - Порівняльна характеристика технологій організації локальної мережі пункту управління

Показник	Wi-Fi	Ethernet (кабель)	PLC
Радіовипромінювання назовні	Значне, постійне (маякові кадри)	Практично відсутнє (за екранування)	Побічне; потребує обмеження
Час розгортання	Хвилини	Години - доба (прокладання ліній)	Хвилини (наявна мережа живлення)
Окрема кабельна інфраструктура	Не потрібна	Потрібна	Не потрібна
Ризик виявлення засобами РЕР	Високий	Низький	Низький за умови фільтрації
Можливий витік сигналу за межі ПУ	Повітряний, у всіх напрямках	Лише за фізичного доступу до кабелю	Кондуктивний у зовнішню мережу за відсутності фільтрів

Як видно з таблиці 1, PLC за швидкістю розгортання не поступається Wi-Fi, а за відсутністю цілеспрямованого радіовипромінювання наближається до кабельних мереж. Водночас силова проводка не призначена для передавання високочастотних сигналів, оскільки вона не екранована й за певних умов працює як неоптимальна антена, а сигнал може поширюватися кондуктивно по зовнішній мережі живлення за межі ПУ [5, 7]. Тому PLC знижує, але не усуває демаскувальні ознаки, і прихованість забезпечується лише комплексом організаційно-технічних заходів. Крім того, реальна пропускна здатність PLC суттєво залежить від довжини та якості проводки й завад від імпульсних блоків живлення, тож для кожного ПУ її потрібно перевіряти експериментально. Орієнтовно вона достатня для IP-телефонії, обміну формалізованими повідомленнями та картографічними даними, але для великої кількості відеопотоків може бути недостатньою, тому такі потоки доцільно передавати окремими волоконно-оптичними лініями.

З огляду на різні вимоги до швидкості обміну, для ПУ доцільна двоконтурна архітектура: широкосмуговий PLC (IEEE 1901, G.hn) використовують для обміну даними між автоматизованими робочими місцями, серверами та засобами зв’язку, а вузькосмуговий PLC у смузі до 500 кГц (наприклад, G3-PLC за ITU-T G.9903) – для службових і телеметричних даних, зокрема керування живленням і сигналізації, де швидкість обміну не є критичною [5, 8]. Розділення контурів дає змогу значно обмежити спектр і потужність сигналів у більшій частині мережі та спростити її контроль.

Рівень побічного випромінювання PLC-мережі визначається не лише потужністю передавача, а й симетрією та екрануванням проводки: перетворення диференціального сигналу на синфазну складову на відгалуженнях і неоднорідностях ліній збільшує ефективність випромінювання [5, 7]. Тому на практиці екранування, симетрування ліній і фільтрація мають пріоритет над збільшенням потужності передавачів для компенсації загасання. Крім того, сигнал у силовій проводці швидко слабшає з відстанню через загасання та розгалуження, що зменшує дальність його можливого виявлення за межами ПУ за умови виконання наведених нижче заходів.

Пропозиції щодо побудови каналів обміну даними на ПУ на основі PLC:

– створити окрему внутрішню мережу живлення ПУ від автономного джерела (електростанції, акумуляторних батарей), відокремлену від зовнішньої мережі розділовим трансформатором;

– на вводі та вихідних лініях встановити фільтри-загороджувачі, що не пропускають сигнали PLC-діапазону за межі ПУ;

– мінімізувати довжину ліній, застосовувати екрановані кабелі живлення із заземленням екрана та феритові фільтри на відгалуженнях, сегментувати мережу за функціональними контурами;

– обмежувати потужність передавачів до мінімально необхідної та вилучати (режекторувати) частотні смуги, у яких побічне випромінювання найбільш небажане; за орієнтир допустимих рівнів брати вимоги EN 50561-1 [9];

– окрім вбудованого AES-128, використовувати сертифіковані засоби криптографічного захисту інформації на рівні мережевих шлюзів;

– зовнішні напрямки зв'язку організовувати волоконно-оптичними лініями або короткочасними спрямованими сеансами радіозв'язку з винесених за межі ПУ позицій, а перед введенням ПУ в роботу вимірювати рівні побічного випромінювання аналізатором спектра з вимірювальною антеною.

Під час експлуатації також необхідно: розміщувати PLC-адаптери на мінімальній відстані від периметра ПУ; вимикати адаптери, що не використовуються; не живити вузли PLC через подовжувачі, під'єднані до зовнішніх мереж; задавати для кожної мережі окремі ключі шифрування та контролювати перелік підключених пристроїв, оскільки будь-який несанкціонований адаптер у спільній мережі живлення стає потенційною точкою доступу до даних.

Висновки

Технологія PLC дає змогу організувати внутрішні канали обміну даними ПУ без прокладання окремих кабельних ліній і без відкритого радіоінтерфейсу, що зменшує кількість демаскувальних ознак у радіодіапазоні порівняно з Wi-Fi. Прихованість досягається за умов автономного живлення ПУ, фільтрації сигналу на межі, екранування ліній і криптографічного захисту даних.

Подальші дослідження доцільно спрямувати на експериментальне вимірювання рівнів побічного випромінювання PLC-мережі та оцінювання дальності її виявлення засобами РЕР. Результати можуть бути використані під час розроблення вимог до складу, порядку розгортання та експлуатації мереж обміну даними ПУ в умовах інтенсивної розвідки противника.

Список використаних джерел:

1. Poisel R. Electronic Warfare Target Location Methods. 2nd ed. Boston: Artech House, 2012.
2. IEEE Std 802.11-2020. IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. New York: IEEE, 2021.
3. IEEE Std 1901-2010. IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications. New York: IEEE, 2010.
4. ITU-T Recommendation G.9960. Unified high-speed wireline-based home networking transceivers - System architecture and physical layer specification. Geneva: ITU.
5. Ferreira H. C., Lampe L., Newbury J., Swart T. G. (eds.). Power Line Communications: Theory and Applications for Narrowband and Broadband Communications over Power Lines. Chichester: Wiley, 2010.
6. Galli S., Scaglione A., Wang Z. For the Grid and Through the Grid: The Role of Power Line Communications in the Smart Grid // Proceedings of the IEEE. 2011. Vol. 99, No. 6. P. 998-1027.
7. Hrasnica H., Haidine A., Lehnert R. Broadband Powerline Communications: Network Design. Chichester: Wiley, 2004.
8. ITU-T Recommendation G.9903. Narrowband orthogonal frequency division multiplexing power line communication transceivers for G3-PLC networks. Geneva: ITU.
9. EN 50561-1:2013. Power line communication apparatus used in low-voltage installations - Radio disturbance characteristics - Limits and methods of measurement - Part 1: Apparatus for in-home use. Brussels: CENELEC, 2013.

Роздільська Вікторія Андріївна *- курсант 443 навчальної групи, факультету автоматизованих систем управління та наземного забезпечення польотів авіації, Харківський національний університет Повітряних Сил імені Івана Кожедуба, м. Харків, rozdilskaviktoriya@gmail.com*

Rozdilska Viktoriia Andriivna *- cadet of the 443rd study group, Faculty of Automated Control Systems and Aviation Ground Support, Ivan Kozhedub Kharkiv National Air Force University,*
Kharkiv, rozdilskaviktoriya@gmail.com