МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

ЗБІРНИК НАУКОВИХ ПРАЦЬ

за матеріалами X Всеукраїнської науково-практичної конференції

«ЕЛЕКТРОННІ ТА МЕХАТРОННІ СИСТЕМИ:

ТЕОРІЯ, ІННОВАЦІЇ, ПРАКТИКА»

20 грудня 2024 року

Полтава 2024

3. Контролери заряду з вбудованим захистом

Якщо панель підключена до акумулятора через контролер заряду, треба обирати модель із вбудованим захистом від короткого замикання та перевантажень. Тоді контролери автоматично розривають ланцюг при виявленні аномалій у струмі, забезпечуючи захист системи.

4. Заземлення та моніторинг

Заземлення панелей і всіх металевих елементів конструкції допомагає запобігти накопиченню статичної електрики та забезпечує додатковий захист у випадку короткого замикання. Це важливо для великих установок і систем з високою потужністю. Крім того, необхідно регулярно перевіряти панелі, проводи та з'єднання на предмет пошкоджень, зносу або забруднень.

Комбінація автоматичних вимикачів, діодів і контролерів заряду створює ефективну систему захисту від короткого замикання, підвищуючи надійність роботи сонячної станції і захищаючи панелі від пошкоджень.

ЛІТЕРАТУРА:

1. *Типи сонячних панелей [Електронний ресурс] – режим доступу до ресурсу:* https://www.scribd.com/document/476019352/2nd-half

2. Автоматичні вимикачі [Електронний ресурс] – режим доступу до ресурсу: http://surl.li/edfoti

CONTROL OF SHORT CIRCUIT CURRENTS IN THE SOLAR PANEL

***A. Ivanov**, Master's Student,*
***N. Yermilova**, PhD (Engineering), Associate Professor*
National University "Yuri Kondratyuk Poltava Polytechnic"

УДК 004.77

***О.В. Шефер**, д.т.н., професор,*
***О.Г. Дрючко**, к.х.н., доцент,*
***С.С. Удовик**, студент*
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

З′ЯСУВАННЯ МОЖЛИВОСТЕЙ Й ОБЛАСТЕЙ ЗАСТОСУВАННЯ ТЕХНІЧНИХ РІШЕНЬ ВІДДАЛЕНОГО УПРАВЛІННЯ ВИРОБНИЧИМИ ОБ′ЄКТАМИ

Інноваційні рішення у сучасних системах автоматизації демонструють істотні успіхи у сфері управління виробничими процесами - від складальних ліній, що функціонують з винятковою точністю до інтелектуальних фабрик, керованих штучним інтелектом. Тому сфера промислової автоматизації є показником стрімкості темпу технологічної еволюції. Вплив застосованих інтегрованих фреймворків значно підвищує ефективність виробництва, знижує витрати, мінімізує людські помилки та підвищує загальну продуктивність. А її еволюційний зріст супроводжується новими ключовими тенденціями:

прискореним впровадженням індустріального Інтернету речей (IIoT), доповненою / віртуальною реальністю, інтеграцією штучного інтелекту, більш широким використанням промислової робототехніки, появою автоматизованих складів, різким зростанням попиту на більш досконалі та універсальні системи управління, такі як програмовані логічні контролери (ПЛК) та системи диспетчерського управління та збору даних (SCADA), автоматизацією ланцюжка постачання та керування транспортними засобами.

Сьогодні для побудови локальних мереж Wireless Local Area Network (WLAN) та організації бездротових комунікацій у більшості випадків застосовується технологія Wi-Fi. У даному повідомленні детально розглядаються побудова мереж Wi-Fi, їх принципи роботи, обмеження та питання безпеки.

Основною особливістю WLAN є можливість створити стабільне підключення в місцях, де прокладка кабелів утруднена. Крім того, рішення забезпечує:

• мобільність користувачів. Підключені пристрої легко переміщати в межах покриття бездротової мережі без втрати швидкості та якості передачі даних;

• простоту створення. Побудова Wi-Fi мереж виконується легше та швидше, ніж прокладання проводових рішень;

• можливості підключення сотень користувачів до однієї точки доступу, на відміну від дротових мереж, у яких для підключення кожного пристрою потрібен окремий кабель;

• швидке та легке масштабування або модернізація за допомогою додавання або заміни потрібної кількості мережевих пристроїв;

• енергоефективність, гнучкість та економічність рішення;

• покриття від кількох метрів до кількох кілометрів, залежно від вибраного обладнання та технологій.

Недоліки та обмеження побудови Wi-Fi мережі:

• обмежена дальність передачі сигналу. Ця складність враховується на етапі проектування та вирішується підбором оптимального обладнання та технологій для конкретних завдань замовника;

• можливі перешкоди чи нестабільність з'єднання. Побудова Wi-Fi мережі в будівлі передбачає попередній аналіз таких складнощів та створення оптимальної схеми розміщення обладнання, яка унеможливлює подібні проблеми;

• загрози кібербезпеці, такі як підключення неавторизованих користувачів, кібератаки, підбір ключів, використання фальшивих точок доступу. Для мінімуму таких ризиків підбираються ефективні рішення для захисту бездротових мереж та користувачів.

Залежно від дальності дії, бездротові мережі діляться на 4 типи:

• WPAN або Wireless Personal Area Networks – персональні мережі;

• WLAN або Wireless Local Area Networks — локальні мережі;

• WMAN або Wireless Metropolitan Area Networks – мережі, побудовані в межах міста;

• WWAN або Wireless Wide Area Network – глобальні мережі.

Для побудови бездротових мереж можуть використовуватись такі технології:

• ZigBee (стандарт IEEE 802.15.4). Застосовується при створенні персональних мереж, у тому числі систем «розумний будинок», забезпечує радіус покриття 1-100 м;

• Bluetooth (стандарт IEEE 802.15.1). Невеликий радіус покриття дозволяє створювати персональні мережі, найчастіше, для підключення до ПК бездротових пристроїв;

• Wi-Fi (стандарт IEEE 802.11). Ця технологія сьогодні найчастіше застосовується для створення WLAN;

• WiMAX (стандарт IEEE 802.16). Дозволяє забезпечувати з'єднання на відстані до кількох кілометрів і застосовується для побудови WMAN.

Таблиця 1. Порівняння стандартів Wi-Fi

Стандарт	802.11ac	802.11ax	802.11ax	802.11be
Діапазон	5 ГГц	2,4 ГГц, 5 ГГц	2,4 ГГц, 5 ГГц, 6 ГГц	2,4 ГГц, 5 ГГц, 6 ГГц
Ширина каналу	20 МГц, 40МГц, 80 МГц, опціонально 160 МГц	до 160 МГц	до 160 МГц	до 320 МГц
Максимальна швидкість передачі даних	3,5 Гбіт/с	9,6 Гбіт/с	9,6 Гбіт/с	46 Гбіт/с

Об'єднання Wi-Fi Alliance розробило стандарт безпеки Wi-Fi Protected Access або WPA, який відповідає за надійну автентифікацію користувачів та шифрування трафіку. Завдяки Temporal Key Integrity Protocol ключ у системі динамічно змінюється. Технологія також забезпечує перевірку цілісності повідомлень, що дозволяє виявляти активність кіберзлочинців.

Сьогодні для безпеки бездротових мереж використовуються оновлені протоколи:

• WPA2, який використовує протокол CCMP. В його основі алгоритм розширеного стандарту шифрування (AES), який відповідає за перевірку справжності та цілісності повідомлення. Цей протокол використовується в домашніх мережах та передбачає наявність загального ключа (WPA2-PSK), а також застосовується у корпоративному режимі (WPA2-EAP);

• WPA3, який забезпечує індивідуальне шифрування даних, використовує одночасну автентифікацію рівних або протокол SAE, який передбачає обмін даними між точкою доступу та пристроєм, що підключається. Цей протокол також має підвищений захист від підбору пароля.

Крім того, для підвищення безпеки в бездротових мережах застосовуються механізми контролю доступу, такі як:

• MAC-фільтрація, яка передбачає обмеження доступу до мережі на основі унікальних MAC-адрес мережевих контролерів. Такий метод досить легко обійти, тому він найчастіше використовується як додатковий;

• VPN (Віртуальна приватна мережа), в якій доступ до корпоративної мережі бездротової здійснюється виключно захищеним каналом.

Важливим етапом підтримки високого рівня безпеки корпоративних бездротових мереж є регулярне оновлення програмного забезпечення. Нові версії містять виправлення виявлених уразливостей та дозволяють не тільки отримати новий функціонал, а й підвищити безпеку.

Використання програмного забезпечення для моніторингу мережного трафіку також дає можливість оперативно виявляти аномалії, підозрілу активність та інші проблеми, а також забезпечувати швидке реагування на інциденти.

Грамотно спроектоване та впроваджене рішення має відповідати потребам компанії щодо пропускної спроможності, стабільності підключення та забезпечення покриття всіх необхідних локацій. Побудова Wi-Fi мережі підприємства починається з детального аналізу проекту, в ході якого уточнюються завдання виробництва, запланований бюджет на впровадження та подальше обслуговування, підбирається оптимальне обладнання та технології.

При цьому необхідно враховувати:

• розташування мережевих пристроїв, у тому числі точок доступу. Для досягнення оптимального поширення сигналів та зведення до мінімуму можливих перешкод найчастіше вибирають верхні точки приміщень: стійки, простір під стелею, колони;

• наявність товстих стін, можливі перешкоди від мікрохвильових печей чи Bluetooth-обладнання – все це може вплинути на якість сигналу;

• вибір надійних інструментів кіберзахисту, які відповідають потребам та особливостям роботи підприємства.

Актуальність і значимість таких досліджень і зумовили мету даної роботи.

EXPLANATION OF POSSIBILITIES AND AREAS OF APPLICATION OF TECHNICAL SOLUTIONS FOR REMOTE CONTROL OF PRODUCTION FACILITIES

***O. Shefer**, Doctor of Science, Professor,*
***O. Dryuchko**, PhD, Associate Professor,*
***S. Udovyk**, Student*
National University "Yuri Kondratyuk Poltava Polytechnic"