УДК 004.056

С.О. Родін
Національний університет “Львівська політехніка”,
кафедра захисту інформації

ТЕХНОЛОГІЇ ЗВ’ЯЗКУ В СИСТЕМАХ ОХОРОНИ. ВИДИ ТА ОСОБЛИВОСТІ ЗАСТОСУВАННЯ

Проаналізовано сучасні технології зв’язку в системах охорони, переваги та недоліки різних сучасних технологій зв’язку. Визначено найперспективнішу технологію зв’язку для систем охорони.

Ключові слова: zigbee, системи охорони, канал зв’язку, діапазон, частоти.

The paper overviews and analyzes modern communication technologies applied in security systems. The advantages and disadvantages of different communication technologies are presented. The most promising communication technology for security systems was singled out.

Key words: Zigbee, security systems, communication channel, range, frequencies.

Вступ

Канали зв’язку є важливим компонентом систем охорони, оскільки безпосередньо впливають на надійність таких систем. За їх участі передаються сигнали на пульти централізованого спостереження.

Залежно від фізичної природи ліній зв’язку, способу передавання і технологій каналоутворення можна виділити кілька різновидностей каналів зв’язку, що застосовуються у сучасних системах охорони. У статті проаналізовано ключові особливості їх застосування та технологічні інновації.

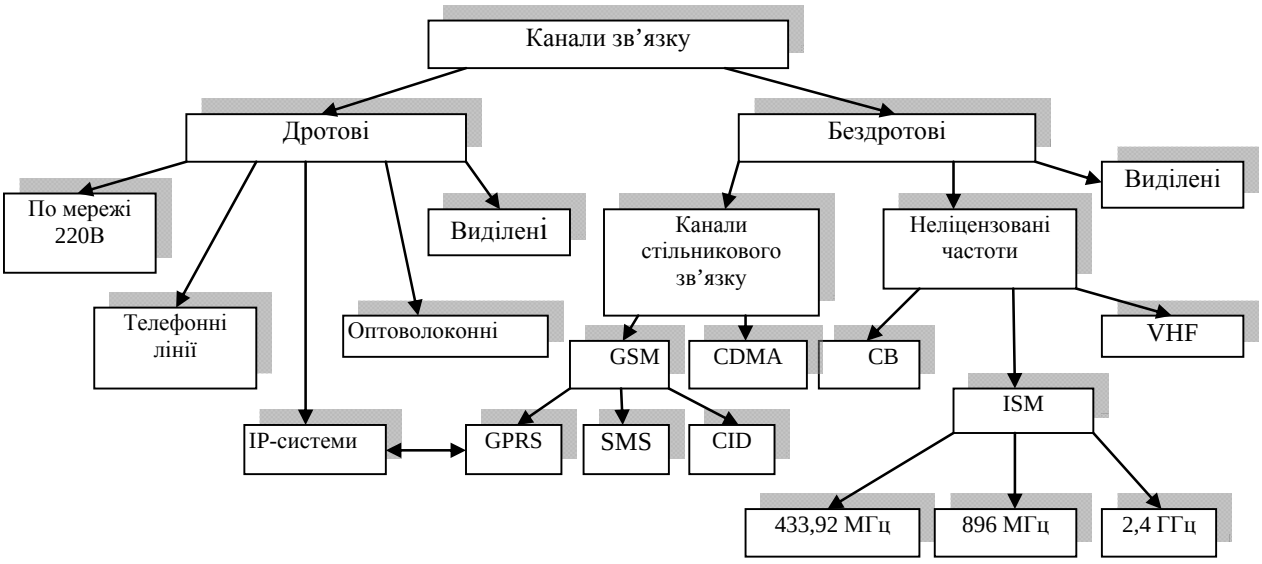

Рис. 1. Класифікація систем зв’язку для систем охорони

Дротові системи

Історично першими були дротові системи.

Передавання сигналу мережею 220 В

Найменш поширені системи, які передають сигнал мережею 220 В і використовують різні технології, зокрема PLC (Power Line Communication). Використання вже прокладених комунікацій є безумовною перевагою, проте недоліками є: обмежена відстань, можливі частотні колізії з іншими системами, що не дає поки можливості ширше розвивати ці систем [1].

Телефонні лінії

Найпоширеніші серед дротових систем є системи з додзвоном, які використовують загальносвітові протоколи, такі як Contact ID та ін. Очевидними недоліками цих рішень є відсутність постійного моніторингу мережі та незадовільний стан телефонних ліній.

Оптоволоконні системи

Оптоволоконні системи рідко застосовують як самостійні при охороні об'єктів, а побудовані на їх основі системи з протоколом TCP / IP набагато поширеніші. До недоліків оптоволоконного кабелю, що впливає на безпеку систем охорони, належать менша механічна міцність і менша довговічність, ніж електричного кабелю. Тому ці системи переважно застосовують для передавання сигналу комунікаційними магістралями разом з іншими системами.

Виділені лінії

Системи, побудовані на виділених лініях, передбачають постійний моніторинг, але вимагають обов'язкової установки ретрансляторів на АТС. Це особливо проблематично при переході на нові технології (зокрема оптоволокно).

IP-системи

Інтернет-системи працюють як з використанням дротових ліній (на базі технологій типу ADSL або оптоволокна), так і разом із радіоканальними GSM-і GPRS-системами і основним протоколом TCP/IP. Цей вид систем найпоширеніший і продовжує розвиватися та інтегруватися із системами відеоспостереження, контролю доступу.

Бездротові системи

У роботі [2] проведено порівняльний аналіз дротових і бездротових каналів зв’язку, а також визначено основні фактори, що сприяють поступовому поширенню бездротових технологій.

Канали стільникового зв’язку

Сьогодні понад 90 % – це стандарт GSM, рідше CDMA.

Основними перевагами охоронних GSM-рішень є:

- використання вже збудованих мереж;
- зростаючі зона покриття і стійкість мереж;
- спадна вартість трафіку і обладнання за рахунок розвитку технологій виробництва;
- можливість роботи з декількома операторами – резервування;
- різні способи доставки – SMS, CSD, а також GPRS – симбіоз з IP. Проста інтеграція на програмному рівні з іншими системами.

Існують і очевидні недоліки:

- залежність від операторів, їх доступність та ціни за трафік;
- за стійкість і своєчасність роботи мереж оператори не несуть відповідальності: під час великих свят або при надзвичайних ситуаціях;
- маса доступних “глушилок”, від яких не врятують ні дві, ні три SIM-карти.

Неліцензовані частоти

Ключовими перевагами використання неліцензованих частот можна вважати два:

- відсутність необхідності придбання частотних діапазонів і реєстрації засобів зв’язку;
- невисока вартість за рахунок розвитку технологій виробництва чипів – практично готових приймально-передавальних пристроїв.

Це найпоширеніший у світі безліцензійний ISM-діапазон (Industrial, Scientific and Medical – 433,92 МГц) [3]. Відрізняється дуже дешевою елементною базою (чип – передавач), процесором з хорошою "пробивною" здатністю в густо забудованих районах, меншими габаритами антен.

Однак цей діапазон найбільш "засмічений" з-поміж усіх інших: автосигналізації, іграшки, системи керування тощо. А мала дозволена потужність (10 мВт) [4] забезпечує більшу дальність при використанні спрямованих виносних антен тільки в прямій видимості.

Загальносвітовий діапазон 868 МГц призначений як для сповіщувачів, так і для моніторингу. Відрізняється мініатюрнішими і ефективнішими антенно-фідерними пристроями (АФП), сучасною елементною базою із "розумним" програмним використанням спектра аналогічно ZigBee, менш "засміченим" порівняно з ISM-діапазоном, проте малою дозволеною потужністю – 10 мВт [3] та невизначеністю даного діапазону для використання в системах охорони на території України.

Радіоканали з виділеними частотами в VHF / UHF-діапазонах

Можна виділити два основні недоліки радіоканалу в діапазонах VHF / UHF:

- обов'язкове оформлення з фіксацією території частотного ресурсу, з подальшою обов'язковою реєстрацією засобів зв'язку та плати за використання частот;
- необхідність побудови (на відміну від GSM) власної мережі з використанням ретрансляторів при її розширенні.

Але переваги вельми істотні:

- максимальна дозволена потужність;
- незалежність від операторів і стану їх мереж;
- можливість використання внутрішніх антен на об'єктах, що охороняються при великих відстанях;
- частоти видані і контролюються державними органами та видаються тільки конкретним користувачам або структурам.

Як результат – чільне використання цих систем в збройних силах, ВМФ, МВС, МНС, СБУ, авіації, космонавтиці та в інших галузях.

Технологія – ZigBee

ZigBee – це нова технологія побудови бездротових мереж передавання даних у сімействі IEE 802.15 Low Rate Wireless Personal Area Network (LR-WPAN – бездротові персональні обчислювальні мережі).

У мережі ZigBee пристрої при вмиканні живлення завдяки вбудованому програмному забезпеченню можуть самоорганізовуватися і формувати мережу, а в разі пошкодження чи недоступності одного з вузлів здатні встановлювати нові маршрути для передавання повідомлень. Технологія ZigBee застосовна як для реалізації простих з'єднань "точка-точка" і "зірка", так і для утворення складних мереж з топологіями "кластерне дерево" і "стільникова мережа".

Стандарт ZigBee передбачає використання частотних каналів у діапазонах 868 МГц, 915 МГц і 2,4 ГГц. Найбільшої швидкості передавання даних і найвищої завадостійкості досягають у діапазоні 2,4 ГГц. Тому більшість виробників мікросхем випускають приймачі саме для цього діапазону.

Радіосигнали використовують широкосмугову модуляцію з прямим розширенням спектра, яка керується цифровим потоком у модуляторі. Двійкова фазова маніпуляція використовується на смугах в 868 і 915 МГц, а квадратурна фазова маніпуляція зі зміщенням, яка передає по 2 біти в символі, використовується на смузі 2,4 ГГц. У чистому вигляді, під час передавання через повітря швидкість передавання даних становить 250 кбіт/с для кожного каналу в діапазоні 2.4 ГГц, 40 кбіт/с для кожного каналу в діапазоні 915 МГц і 20 кбіт/с в діапазоні 868 МГц. Відстань передавання від 10 до 75 метрів при роботі в середині приміщень і понад 1500 метрів при роботі на відкритому повітрі, хоча вона сильно залежить від виду обладнання. За рахунок ретрансляції зона покриття мережі може значно збільшуватися.

ZigBee-модулі самостійно утворюють мережу і підтримують ретрансляцію повідомлень. Модулі ZigBee не вимагають конфігурації і містять вбудований протокол пакетного передавання даних з перевіркою цілісності передаваних даних.

Характеристики ZigBee:

- частотний діапазон – 2,4 ГГц, 16 частот з шириною 5 МГц;
- DS-SS – пряме розширення спектра сигналу;
- O-QPSK – квадратурна фазова маніпуляція зі зміщенням;
- автоматичне регулювання вихідної потужності в широких межах задля забезпечення енергоефективності;
- дозволена потужність – 100 мВт;
- оцінка рівня потужності сигналу в ефірі – RSSI та підтвердження про успішну доставку для кожного пакета даних;
- Mesh – мережева технологія, забезпечує самоорганізацію та самовідновлення радіомережі, надійність та гнучкість маршрутизації;
- до 65536 вузлів (модемів) у мережі;
- механізм множинного доступу в ефір із контролем несучої та запобіганням колізіям – CSMA (Carrier Sense, Multiple Access);
- 128-бітне шифрування даних за алгоритмом AES;
- швидкість передавання даних включно зі службовою інформацією – до 250 кбіт/с.

Рис. 2. Приймально-передавальний пристрій ZigBee

Висновок

Стандарт ZigBee є оптимальним для побудови великих мереж різноманітних пристроїв у масштабах підприємств і офісних будівель, а також локально розподілених об'єктів: заміські селища, спорткомплекси, склади, бази, ринки і т.д. Завдяки низці переваг стандарт ZigBee придатний для забезпечення зв’язку в системах охорони, а саме: за методом прямого розширення спектра (DS-SS) можна досягти хорошої електромагнітної сумісності з іншими пристроями та практично повної невразливості до випадкових електромагнітних завад, а також енергетичної прихованості завдяки низькому рівню спектральної густини, енергоефективності та захищеності передавання даних [5]. Використання потужного сигналу, складної модуляції, розділення каналів, динамічної маршрутизації та засобів перевірки цілісності даних забезпечує надійне передавання сигналу між вузлами. Можливість застосування алгоритму шифрування AES-128 забезпечує обмеження доступу в мережі та захисту передаваної інформації. Важливою перевагою, безумовно, є простота в експлуатації, налаштуванні та встановленні.

Однак тільки комплексне використання різних рішень з урахуванням особливостей конкретного об'єкта може стати оптимальним вибором. А взаємний моніторинг комплексно використовуваних технологій (дублювання) є запорукою успіху у вирішенні питання безпеки.

1. Журнал “Системы безопасности”. – 2012. – № 1. – М.: ООО “Гротек”, 2012. 2. Князєв Д. // Вдосконалення систем захисту інформації, що використовують канали GSM // Матеріали V Міжнародної конференції молодих вчених CSE-2011. – Львів: Видавництво Львівської політехніки, 2011. – С. 308–311. 3. Закон України “Про радіочастотний ресурс України”. 4. Постанова Кабінету Міністрів України № 815 від 9 червня 2006 р. “Про затвердження Плану використання радіочастотного ресурсу України”. 5. Скляр Б. // Цифровая связь. Теоретические основы и практическое применение. 2-е изд., испр. – М.: Издательский дом “Вильямс”, 2003. – 1104 с.