DOI: 10.18372/2410-7840.22.14659
УДК 621.396.4 (043.2)

СИСТЕМА МОНІТОРИНГУ ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ З ВИКОРИСТАННЯМ ПЛАТФОРМИ QIVICON

Анна Романова, Георгій Конахович

Пояснено, як віддалено може бути введено шкідливий сигнал у сенсорну систему. Детально представлено, як працює запропонований метод захисту та проаналізовано його безпеку. Показано, як зберігати певну гарантію безпеки. Запропоновано новий метод захисту для виявлення нападу, який засновано на ідеї, що коли у датчику вимикається живлення, вихід сенсору повинен бути «спокійним». Якщо сигнал атаки зловмисно індуктується в систему датчиків під час «спокійного» періоду, мікроконтролер може це виявити. Представлено детальний опис методу виявлення ЕМЗ (електромагнітних завад) та доведено гарантію їх виявлення в контексті сильної моделі зловмисника. Такий підхід для виявлення загальних сигналів ЕМЗ може існувати як в мікрофонній системі, так і в системі датчиків температури, чи інших сенсорів. Доведено, що механізм виявлення є і ефективним, і надійним. Зосереджено увагу на атаках з потужними ЕМЗ, в яких зловмисник маніпулює датчиками користувача, щоб внести саме ті значення, які бажає.

Ключові слова: *електромагнітні завади, сенсорний датчик, «розумний будинок», система моніторингу, сигнал атаки.*

ВСТУП

Одна з найбільш суттєвих проблем впровадження Інтернету речей (IoT) є забезпечення кібербезпеки. Особливо небезпечні випадки перехоплення управління IoT зловмисниками, які можуть заблокувати дверні замки та вимагати за розблокування викуп. На ринку в сфері «розумних будинків» представлено широкий вибір готових рішень з різними наборами апаратно-програмних складових від зарубіжних і вітчизняних виробників. Але установка такого комплексу коштує відносно дорого і, як правило, вимагає професійного інженерного планування на етапі будівництва будинку або ремонту квартири.

Потік інформації, що надходить з датчиків температури, тиску, світла і подібних до них, дуже великий, особливо, якщо потрібен безперервний моніторинг обраних параметрів і аналіз статистики за тривалий проміжок часу. Відповідно, для зберігання такого обсягу інформації потрібно велике сховище. Розміщення на фізичних носіях в домашніх умовах потребує грошових витрат і додаткових налаштувань, тому найчастіше використовуються «хмарні» сервіси.

Метою даної статті є проектування та дослідження адаптивної системи моніторингу електромагнітних завад в сенсорній мережі домашнього контролю на основі сучасної платформи QIVICON, що в подальшому дозволить своєчасно виявити та нейтралізувати кібер загрозу.

Спроектована система моніторингу побічних електромагнітних випромінювань може бути реалізована на практиці для готової платформи «розумного будинку» для типового користувача.

ПОСТАНОВКА ПРОБЛЕМИ

Отже великою проблемою, як готових рішень, так і самостійно розроблених систем з підключенням хмарних сервісів, є кібербезпека. Інформація, що надходить з пристроїв в мережу, а потім і в Інтернет, є конфіденційною і при передачі вимагає більше особливих заходів з безпеки, ніж виробники систем та її компонентів на даному етапі розвитку Інтернету речей можуть надати через відсутність стандартів.

Платформа QIVICON (рис. 1) є високозахищеною системою, однак, «лазівки» є в будь-якій електронній установці. В даній статті покращено метод виявлення електромагнітного атакуючого сигналу під час штатної роботи усієї системи, з використанням платформи QIVICON.

QIVICON було обрано за основу системи, зважаючи на те, що платформа QIVICON основана на відкритому програмному забезпеченні, що є досить цікавим та перспективним фактором, її було обрано за основу для даної роботи [1].

Сенсорні системи (рис. 2) використовуються щоразу, коли мікроконтролеру необхідно взаємодіяти з фізичним світом. Їх є багато в домашній автоматизації, заводських системах управління, критичних інфраструктурах, транспортній системі та в іншому. В сенсорній системі датчик перетворює фізичну величину в аналоговий сигнал, який надсилається на АЦП та мікроконтролер для оцифрування та подальшої обробки. Після вимірювання в цифровому вигляді мікроконтролер може виконувати завдання відповідно до вимірювання. Електромагнітні завади (ЕМЗ) можуть впливати на вимірювання, так як вони передаються в мікроконтролер.

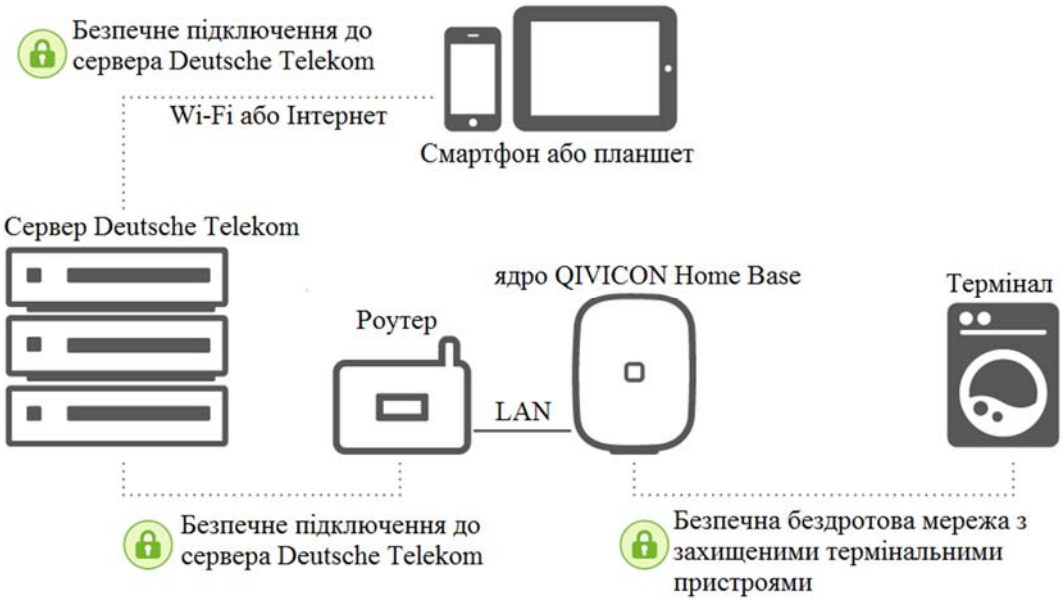

Рис. 1. Передача інформації в системі платформи QIVICON

Зловмисник може маніпулювати вихідним датчиком, навмисно індукуючи ЕМЗ в проводії між датчиком і мікроконтролером. Характер аналогового каналу між датчиком і мікроконтролером такий, що мікроконтролер не може аутентифікувати, чи вимірювання надходять від датчика або зловмисника. Якщо мікроконтролер містить невірні вимірювання у своїх контрольних рішеннях щодо управління, це може мати катастрофічні наслідки.

Наукова новизна даної статті полягає в обґрунтуванні ефективної (за критерієм надійності, гнучкості та економічності) системи моніторингу побічних електромагнітних завад в сенсорній мережі для інтелектуальних домашніх систем на платформі QIVICON.

ПОТУЖНІ АТАКУЮЧІ ЕЛЕКТРОМАГНІТНІ ЗАВАДИ

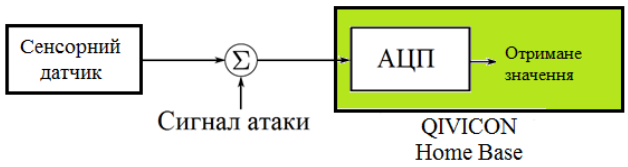

Рис. 2. Сенсорна система

Як показано на рис. 2, сенсорна система складається з двох основних модулів: датчика та мікроконтролера. Датчик виводить вимірювання на мікроконтролер через провід. Зловмисник може перешкоджати виходу датчика, вводячи атакуючий сигнал у сенсорну систему. Коли атакуючий сигнал надходить у сенсорну систему, він накладається на вихід датчика. Вихід атакованого датчика оцифровується за допомогою аналого-цифрового перетворювача в мікроконтролері і, нарешті, цей сигнал обробляється мікроконтролером.

Атаки ЕМЗ можна поділити на два типи: потужні ЕМЗ-атаки та ЕМЗ-атаки низької потужності. Атаки потужних ЕМЗ призводять до заклинювання, спалювання та повного збою системи користувача.

У цій роботі було зосереджено увагу на атаках з потужними ЕМЗ, в яких зловмисник маніпулює датчиками користувача, щоб внести саме ті значення, які бажає.

Для успішної зміни показань датчика зловмисник покладається на дві особливості сенсорної системи: одна полягає в тому, що провід, що з'єднує датчик і мікроконтролер, виконує роль антени; інший - нелінійність електронних компонентів або субдискретизація (заниження долі окремих складових) з АЦП.

Завданням нападника є додавання шкідливого сигналу до виходу датчика. Зловмисник генерує атакуючий сигнал, модулюючи сигнал високочастотної несучої. Цей сигнал потрапляє у провід, що підключає датчик до мікроконтролера, і змушує мікроконтролер зчитати помилкове значення. Також використовують нелінійність електронних компонентів для введення довільних даних у датчики. Ці дані можуть бути амплітудно, частотно або фазово-модульовані на носії. Вводячи сигнал з частотою, що перевищує частоту дискретизації АЦП, АЦП буде поміщати вибірку атакуючого сигналу на визначений інтервал і пропускати високочастотні коливання. Як результат, шкідливий сигнал накладається на звичайний сигнал з виходу датчика.

РАНДОМІЗОВНИЙ ВИХІД ДАТЧИКА

Система датчиків складається з двох основних модулів: датчика та мікроконтролера. Показання датчика передаються на мікроконтролер через провід, що з'єднує вихід датчика і вхід мікроконтролера. На жаль, провід чутливий до електромагнітних завад і ЕМЗ можуть впливати на сенсорну систему, індукціюючи напругу на проводі. Зловмисник може використовувати провід для введення атакуючого сигналу у вихід датчика для зміни його показань.

Проведемо вмикання та вимикання датчику. Увімкнення означає, що датчик зміщений при високій напрузі; вимкнення означає, що датчик зміщений при 0 В (або іншому відомому рівню напруги). Коли датчик увімкнено, він вимірює фізичну величину та вихід датчика несе інформацію про фізичну величину. Коли датчик вимкнений, вихід датчика стає постійним сигналом на певному рівні напруги. Припустимо, що зловмисник вводить атакуючий сигнал у систему, коли датчик вимкнено, на кінцевому виході датчика з'явиться порушення. Мікроконтролер може легко виявити подібні порушення, а значить, виявляється атакуючий сигнал. Якщо сенсорна система може випадково вимкнути датчик, зловмисник повинен здогадатися, коли датчик вимкнений, щоб вона могла уникнути надсилання атакуючого сигналу до сенсорної системи; в іншому випадку помилка спричинення нерівномірного виходу датчика, коли датчик вимкнений, безпосередньо розкриє атакуючого в сенсорній системі.

Ми вимагаємо, щоб мікроконтролер виміряв фізичну величину та моніторив атакуючий сигнал включеннями, а значить, датчик повинен перемикатися між станами увімкнення та вимкнення.

Будемо використовувати манчестерський код як напругу зміщення для датчика, оскільки манчестерський код перемикається між високим рівнем напруги та 0 В у середині точки кожного тактового циклу (рис. 3).

Манчестерське кодування – це двухфазне, полярне кодування, яке само синхронізується. Біжучий біт визначається по зміні стану в середині бітового інтервалу. Це кодування використовується в Ethernet. Зміна від -В до +В > «1»; від +В до –В > «0» [2].

У цьому випадку манчестерський код створюється з n-бітної рандомізованої секретної послідовності нулів та одиниць. Оскільки секретна послідовність є рандомною, датчик вмикається і вимикається випадковим чином, то і вихідний датчик має рандомну схему увімкнення та вимикання. В даному підході припущено, що фізична величина є постійною. Оскільки фізична величина є постійною, то форма хвилі виходу датчика аналогічна закодованому манчестерському коду.

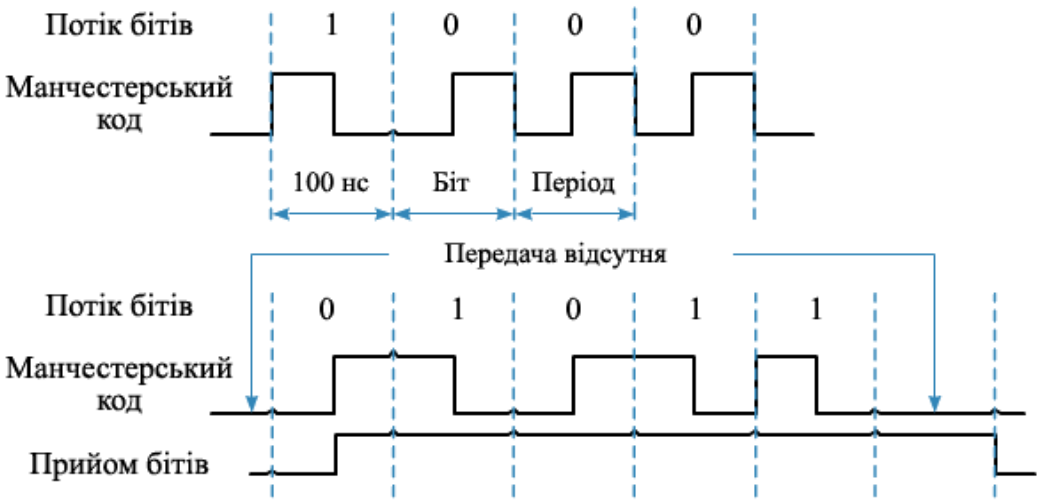

Рис. 3. Приклад кодування з використанням манчестерського коду

Вбудований АЦП оцифровує вихід датчика й мікроконтролер вирішує чи відбувається атака, перевіряючи оцифрований вихід датчика. Як показано на рис. 3, секретна послідовність має n біт і, таким чином, манчестерський код має n тактових циклів. Відповідно, вихідний датчик має n тактових циклів. Ми визначаємо кожен тактовий цикл виходу датчика як підвимір, і всі n підвимірів утворюють цілісне вимірювання.

Крім того, кожний підвимір цифровим чином поділяється за допомогою АЦП на два зразки: один відбирається коли датчик зміщується при високій напрузі, а значення вибірки - не нульовий вольт; інший зразок оцифровується коли датчик зміщений у 0 В, а значення вибірки – 0 В. Мікроконтролер може точно вирівняти оцифрований сигнал із секретною послідовністю, а значить, аналізуючи будь-який зразок, мікроконтролер знає,

чи повинен він бути нульовим або ненульовим. Згодом, виходячи зі знань мікроконтролера про таємну послідовність, зразок, який повинен бути не нульовим, умовно називається "ненульовим зразком", а зразок, який повинен бути нульовим, називається "нульовим зразком".

Під час вторгнення на атакуючий сигнал може впливати або нульова, або ненульова вибірка з підвиміру. Якщо зловмисник змінює нульовий зразок, мікроконтролер може негайно помітити атаку, оскільки рівень напруги нульового зразка не становить 0 В. І навпаки, якщо зловмисник змінить ненульовий зразок, вона також буде швидко виявлена. Це тому, що фізична величина повинна залишатися незмінною під час вимірювання, а всі ненульові зразки повинні бути рівними; однак змінений ненульовий зразок має інший рівень напруги від інших ненульових зразків, а значить, атака виявляється за рахунок відхилення.

МОДЕЛЬ СЕНСОРНОЇ СИСТЕМИ ПО ДАНОМУ МЕТОДУ

На рис. 4 представлена модель сенсорної системи, яка працює з наведеним методом виявлення ЕМЗ. Модель системи складається з датчика та мікроконтролера. Датчик приводиться в дію напругою зміщення, яка контролюється мікроконтролером.

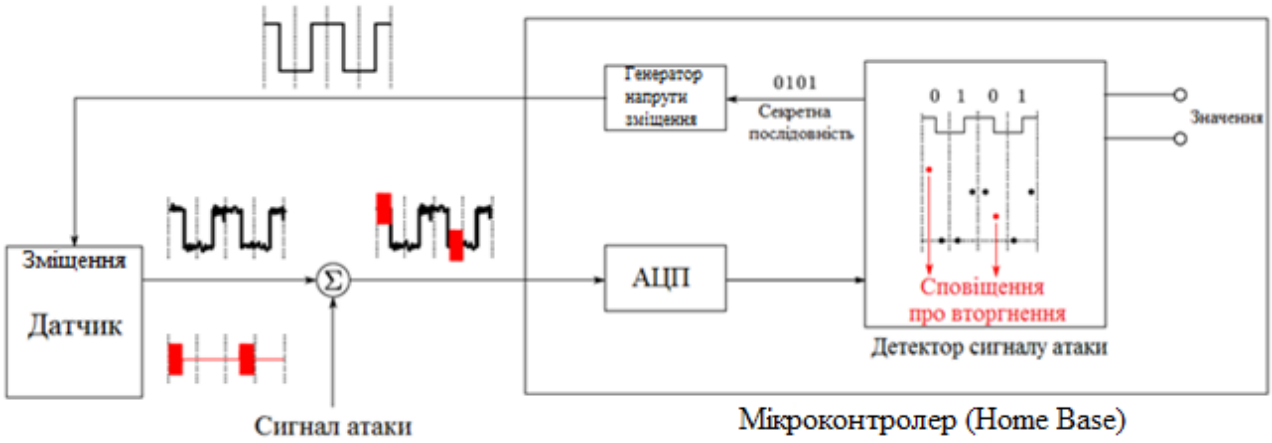

Рис. 4. Система датчиків, яка оснащена представленим методом виявлення ЕМЗ

Вихід датчика використовується для надсилання вимірювань на мікроконтролер, який перевіряє наявність атакуючих сигналів та відображає фізичну величину через вимірювання.

В цьому випадку всі дані з датчиків обробляються в центральній базі Home Base. Мікроконтролер має три блоки, включаючи генератор напруги зміщення, АЦП та детектор сигналу атаки. Генератор напруги зміщення кодує n-бітну секретну послідовність манчестерським кодом, що є напругою зміщення для датчика. АЦП оцифровує вихідний датчик і передає оцифровані дані в детектор сигналу атаки, щоб перевірити, чи існує атакуючий сигнал. Детектор сигналу атаки має два виходи: одне значення являє собою вимірювання фізичної величини; інше («дійсне») вказує, чи готове значення для читання. Якщо не виявлено атакуючого сигналу, вимірюванню присвоюється «дійсне» значення, при цьому встановлюється значення «вірно». Отже, сенсорна система знає, що значення дійсне для подальшої обробки. Однак, якщо в результаті вимірювання виявляється атакуючий сигнал, для цього вимірювання встановлено значення «невірно», це означає, що значення недійсне для зчитування. Після такого розвитку подій мікроконтролер попередить власника сенсорної системи, що вона знаходиться під атакою. Про шляхи попередження буде пояснено в роботі згодом.

У даній системній моделі припускається, що фізична величина залишається незмінною при вимірюванні. Незважаючи на те, що фізична величина змінюється, якщо тривалість вимірювання досить коротка, ми також можемо вважати фізичну величину постійною. Прикладом постійної фізичної величини є кімнатна температура. Температура змінюється повільно протягом тривалого періоду. Однак за короткий час, наприклад 0,01 с, температура не змінюється.

Для кожного вимірювання мікроконтролер генерує n-бітну таємну послідовність, і відповідно манчестерський код має n тактових циклів. Два зразки оцифровуються з кожного тактового циклу чи підвиміру, тому частота дискретизації АЦП в два рази перевищує тактову частоту манчестерського коду. На практиці частота дискретизації АЦП має верхню межу. Таким чином, тактова частота манчестерського коду також має максима-

льне значення, що становить половину найшвидшого показника вибірки. Найменша тривалість n тактових циклів визначається найбільшою швидкістю вибірки АЦП. Щоб застосувати такий метод виявлення, важливо переконатися, що фізична величина не змінюється протягом n циклів годин.

Завданням зловмисника є маніпулювання формою хвилі виходу датчика без виявлення сенсорною системою. Ми припускаємо, що зловмисник не може отримати доступ до сенсорної системи фізично. Крім того, ми припускаємо, що зловмисник не має інформації про n-бітну таємну послідовність. Беручи до уваги будь-який підвимір, ми припускаємо, що зловмисник знає рівні напруги, але не знає, чи переходить рівень напруги від високої напруги до 0 В або від 0 В до високої напруги в середині точки підміру (рис. 3). Таким чином, зловмисник повинен вгадувати напрямок переходу рівня напруги в кожному підвиміру. Більше того, зловмисник може навмисно вводити заздалегідь продуманий і складений сигнал у сенсорну систему, а отже, зловмисник може змінювати форму хвилі виходу датчика за своїм бажанням. Крім того, зловмисник знає, коли модуль датчика починає і перестає передавати вимірювання, і він може точно вирівняти створений ним сигнал з виходом датчика.

ВИЗНАЧЕННЯ АТАКИ НА СИСТЕМУ

Після отримання оцифрованого виходу датчика детектор сигналу атаки вирівнює його з відповідною секретною послідовністю. Як показано на рис. 5, кожна цифра в секретній послідовності відповідає двом зразкам на оцифрованому виході датчика. Цифра 1 означає, що відповідні два зразки є нульовими та ненульовими в послідовному порядку; цифра 0 вказує на ненульову та нульову вибірку в послідовному порядку. Таким чином, мікроконтролер знає порядок всіх зразків. Коли сигналу атаки немає, оцифрований вихід датчика задовольняє двом вимогам:

1) Усі ненульові зразки рівні;

2) Усі нульові зразки дорівнюють нулю.

Як тільки відбувається атака, будь-яку вибірку в підвимірі можна змінити. Детектор сигналу атаки спочатку перевіряє ненульові зразки. Як показано на рис. 5, якщо зловмисник змінює лише кілька ненульових зразків при вимірюванні, сигнал, сформований усіма нульовими пробами, стає непостійним.

Нерівні ненульові зразки означають, що відбувається атака. Щоб обійти виявлення, зловмисник змушений збільшувати або зменшувати всі ненульові зразки до одного рівня напруги. Можливо, зловмисник помилився і змінив нульовий зразок. Як тільки випадковий зразок буде змінений зловмисником, атака буде виявлена.

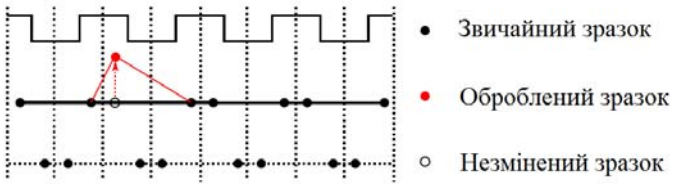

Рис. 5. Вихід датчика постійної фізичної величини

Після перевірки оцифрованого виходу датчика, якщо виявлена атака, вимірювання скасовується. На відміну від цього, якщо не виявлено атакуючого сигналу, можна отримати кількісне визначення фізичної величини. Кількісне визначення - це значення ненульових зразків. Однак на практиці, враховуючи наявність шуму, його можна обчислити шляхом усередкування всіх ненульових зразків.

Розумний зловмисник повинен здогадатися: зразок нульовий чи ненульовий. Щоб уникнути виявлення, зловмисник не повинен впливати на жоден нульовий зразок і він повинен змінювати всі ненульові зразки так, щоб зберегти їх однаковими. На рис. 5 представлено приклад виявлення атакуючого сигналу в сенсорній системі. Зловмисник має на меті змінити перший і третій підвимір виходу датчика. У першому підвимірі зловмисник робить правильну здогадку, і до ненульового півциклу додається високочастотний сигнал. Однак у третьому підвимірі зловмисник робить неправильну здогадку і додає високочастотний сигнал до нульового півциклу. Після оцифрування два зразки зміщуються вгору: ненульовий зразок у першому підвимірі та нульовий зразок у третьому. Порівняно з іншими ненульовими зразками, ненульовий зразок у першому підмірі має інше значення і детектор сигналу атаки може виявити атаку негайно. У третьому підмірі другий зразок повинен був дорівнювати нулю, однак він зміщується на ненульове значення і мікроконтролер може помітити зміни. В результаті може бути виявлений атакуючий сигнал.

ІМПЛЕМЕНТАЦІЯ СПЕЦІАЛЬНОГО МЕТОДУ В МІКРОФОННІЙ СИСТЕМІ

Мікрофон може перетворити звук в електричний сигнал. В даний час мікрофони можна знайти на багатьох різних пристроях, таких як смартфони, навушники та ноутбуки. У мікрофонній системі використовується провід для підключення мікрофонного модуля та мікроконтролера, а отже, зловмисник може використовувати провід

для введення атакуючого сигналу в мікрофонну систему. Наприклад, зловмисник може вводити голосові команди в смартфон через ЕМЗ, а систему голосового помічника можна попросити виконувати шкідливі чи небезпечні завдання в смартфоні. Отже, людина не може чути жодну ЕМЗ, а значить, користувач не може помітити атакуючий сигнал.

Один сигнал 1 кГц - це звук, а інший 1 кГц сигнал - від зловмисника, який вводить шкідливий сигнал 1 кГц в мікрофонну систему ЕМЗ. Схожість цих двох сигналів вище 0,93.

Без спеціального методу виявлення мікрофонна система не може визначити, яким є сигнал: нормальним чи шкідливим. До того ж, зловмисник може віддалено вводити в мікрофонну систему шкідливий сигнал, схожий на звуковий. Генератор сигналів виконаний з можливістю виводити постійний сигнал 300 мВ, таким чином, мікрофон зміщується на 300 мВ. Спочатку відтворюємо аудіосигнал 1 кГц через динамік мобільного телефону на максимальній гучності. Далі вимкнемо динамік і атакуючий сигнал, який промодульований шкідливим сигналом 1 кГц на несучому сигналі 144 МГц випромінюється через антену на 5 дБм. Атакуючий сигнал демодулюється нелінійними електронними компонентами (наприклад, підсилювачами та АЦП) в мікрофонній системі та з'являється оцифрований шкідливий сигнал 1 кГц.

Отже, існує два сигнали 1 кГц, які реконструюються комп'ютером: один - сигнал від динаміка, інший - викликається зловмисником. Без даного способу виявлення важко сказати, чи приймається сигнал від динаміка чи зловмисника: й звуковий, й сигнал зловмисника мають 1 кГц, і вони мають схожі амплітуди. Відомо, що коефіцієнт кореляції Пірсона може бути використаний для вимірювання лінійної кореляції двох сигналів, а цей коефіцієнт є відповідною метрикою для показу схожості двох сигналів у наших експериментах. Коефіцієнт кореляції Пірсона аудіосигналу 1 кГц і шкідливого сигналу 1 кГц вище 0,93, що означає, що ці два сигнали мають високу схожість.

Перш за все, зловмисник може контролювати вихід мікрофонної системи та обманювати мікроконтролер.

З наведених вище експериментальних результатів система мікрофона може вважати шкідливий сигнал нормальним звуковим сигналом. Далі буде показано, як розгорнути цей метод виявлення до мікрофонної системи для виявлення атакуючого сигналу.

Коли метод виявлення застосовується до мікрофонної системи, комп'ютер кілька разів передає секретну послідовність 1100 генератору сигналів, а генератор сигналів кодує секретну послідовність манчестерським кодом з тактовою частотою 40 кГц. Манчестерський кодований код перемикається між 0 мВ і 300 мВ. Зазначимо, що напруга зміщення є для мікрофона, а не для підсилювача. На рис. 6, без жодного аудіосигналу чи атакуючого сигналу, представлено вихід мікрофонного модуля, який фіксується цифровим осцилографом RIGOL DS2302A, що має частоту дискретизації 2 ГГц.

Коли комп'ютер отримує оцифрований сигнал від Arduino DUE, перед тим, як перевірити наявність атаки, необхідно розглянути три практичні проблеми в системі мікрофонів. Перша - це синхронізація оцифрованого сигналу із секретною послідовністю. Кожна цифра в секретній послідовності відповідає одному підвиміру і значення цифри визначає напрямок переходу рівня напруги в середині точки підвиміру. Тільки якщо оцифрований сигнал точно вирівняний із секретною послідовністю, комп'ютер буде знати, чи є конкретний зразок нульовим чи ненульовим.

На практиці потрібно налаштувати генератор сигналів так, щоб на початку першого підвиміру завжди був перехід рівня напруги від високого до низького, щоб можна було ідентифікувати початкову точку оцифрованого сигналу. Далі легко вирівняти оцифрований сигнал із секретною послідовністю.

Інше практичне питання: як обробляти зразки, що піднімаються або падаючих країв виходу модуля мікрофона. Зразки з краю можуть призвести до помилкового позитивного сповіщення про атаку або до неточного вимірювання фізичної кількості. Як показано на рис. 5, час фронту імпульса сигналу дорівнює τ = 2:45 мкс і помітно, що не більше двох зразків виходять з краю сигналу. Також, враховуючи частоту вибірки та тактову частоту, ми можемо виявити, що в кожному під вимірі є 16 зразків. Таким чином, щоб усунути негативні впливи крайніх зразків, ми видаляємо перший і останній зразки за кожен півцикл.

Третє практичне завдання - визначення рівня напруги нульових зразків. Оскільки вихід модуля мікрофона зосереджений на рівні 1,65 В, нульові зразки зміщуються на ненульовий рівень. Як показано на рис. 6, середнє значення нульових зразків становить 1,15 В. Однак можна помітити, що нульові зразки коливаються навколо 1,15 В, а діапазон коливань - ΔВ = 0,04 В. Зауважимо, що ΔВ -

також стійкість до шуму нульових зразків. Коли немає атакуючого сигналу, нульові зразки знаходяться в межах [1,15 В – 1/2 ΔВ; 1,15 В + 1/2 ΔВ] = [1,13; 1,17] В. Якщо нульовий зразок знаходиться назовні [1,13; 1,17] В, система мікрофона буде оповіщена про атаку.

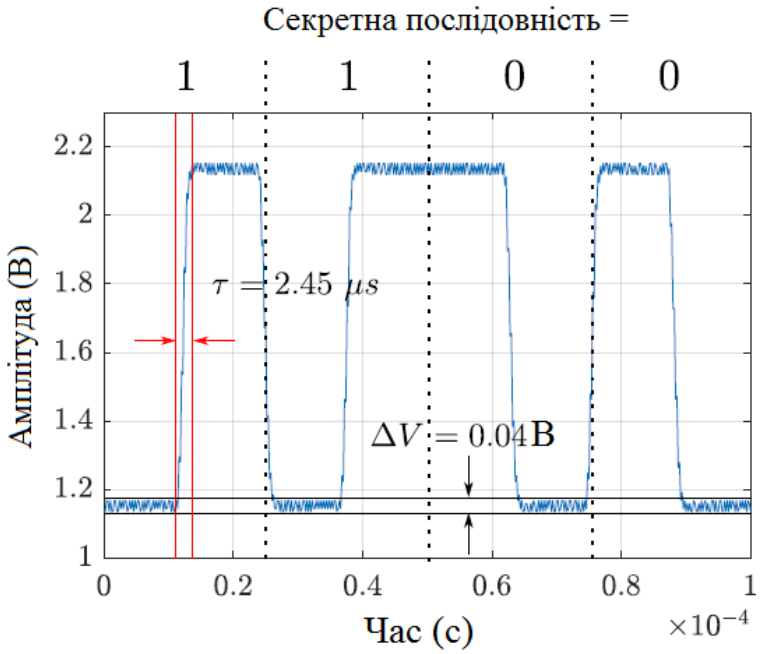

Рис. 6. Вихід мікрофонного модуля, який фіксується цифровим осцилографом

Після отримання вимірювань з модуля мікрофона комп'ютер синхронізує відповідну секретну послідовність з вимірюванням і видаляє зразки з «країв». За межами нульових зразків, що становить [1,13; 1,17] В, комп'ютер може визначити, чи відбувається атака при вимірюванні. Для оцінки ефективності даного методу виявлення розглянемо наступні три випадки:

Випадок 1. Аудіосигнал частотою 1 кГц відтворюється з динаміка на максимальному рівні гучності й немає сигналу атаки. На рис. 7 амплітудна оболонка, що утворена ненульовими зразками оцифрованої послідовності, являє собою компонент 1 кГц. Оскільки сигналу про атаку не існує, цей випадок є посиланням на наступні два випадки.

Випадок 2. Вимикаємо динамік і зловмисник передає сигнал атаки на 5 дБм. Для введення сигналу 1 кГц в систему мікрофона атакуючий сигнал генерується модуляцією сигналу 1 кГц на носії 144 МГц. Як показано на рис. 8, можна помітити, що як нульові, так і ненульові вибірки несуть інформацію сигналу 1 кГц.

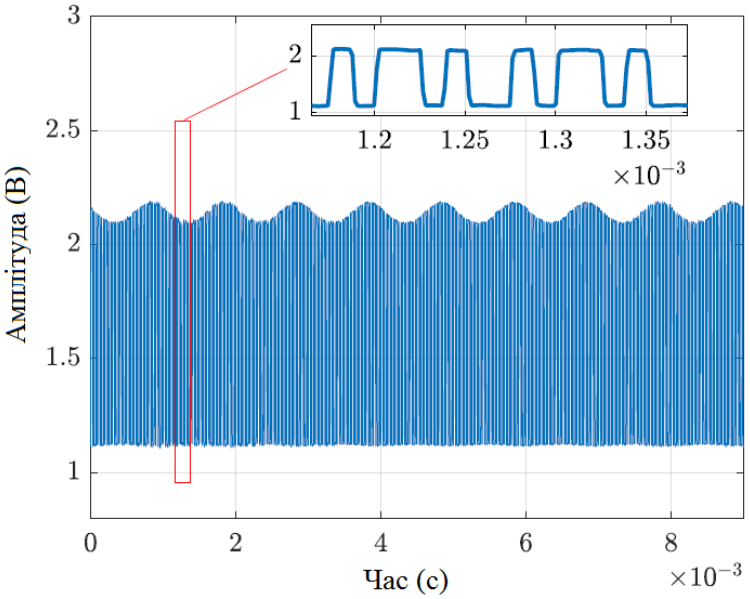

Рис. 7. Демонстрація першого випадку на графіку

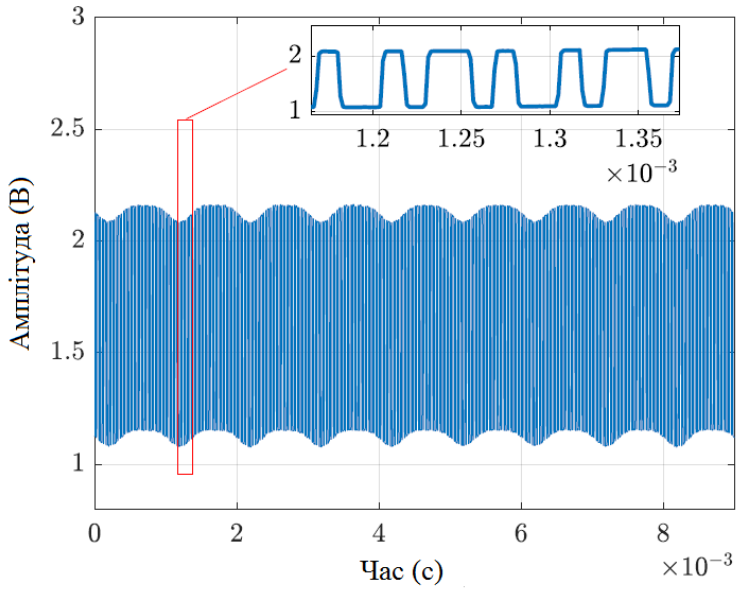

Рис. 8. Демонстрація другого випадку на графіку

Випадок 3. Вмикаємо динамік і зловмисник випромінює сигнал атаки в цей самий час. Частота звукового сигналу все ще становить 1 кГц, а гучність не змінюється. Щоб вставити в систему сигнал 5 кГц, зловмисник модулює сигнал 5 кГц на носії 144 МГц, а потужність передачі атакуючого сигналу становить 0 дБм. Як показано на рис. 9, сигнал 5 кГц домінує як у нульових, так і ненульових зразках.

У кожному випадку фіксується 100 вимірювань. Оскільки фізична величина в вимірюванні не є постійною, використовуємо наші критерії виявлення непостійної фізичної величини, щоб перевірити, чи існує атакуючий сигнал у кожному вимірюванні.

Відповідно, у випадку 2 та випадку 3 ми можемо обчислити дійсну позитивну швидкість виявлення атакуючого сигналу. Результати виявлення представлені в таблиці 1. У випадку 2 та випадку 3 комп'ютер виявляє, що деякі нульові зразки знаходяться поза межами й таким чином сигнал атаки може бути виявлений. Істинно-позитивні показники виявлення нападу становлять 100% як у випадку 2, так і у випадку 3. Результати означають, що сигнали атаки існують у кожному вимірі у цих двох випадках.

Експерименти також показують, що коли немає сигналу атаки (випадок 1), всі нульові зразки знаходяться в межах, а представлений метод виявлення не дає жодної помилкової позитивної тривоги атаки.

Як тільки зловмисник випадково збільшує або зменшує значення нульової вибірки до значення, яке знаходиться за межами меж (наприклад, випадки 2 та 3), атака виявляється негайно.

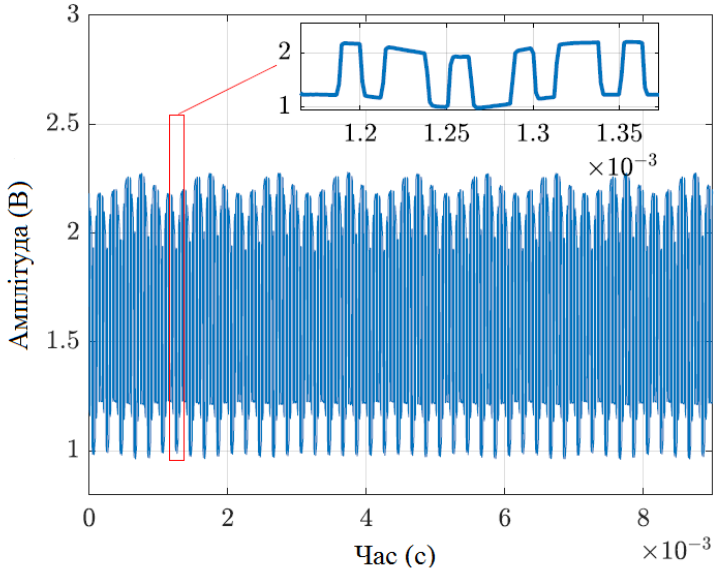

Рис. 9. Демонстрація третього випадку на графіку

Таблиця 1

Показники виявлення

Номер випадку	Звук	Сигнал атаки (модулюючий сигнал, несучий)	Позитивний показник виявлення
2	-	(1 кГц, 144 МГц)	100%
3	1 кГц	(5 кГц, 144 МГц)	100%

Слід звернути увагу, що у випадках 2 та 3 зловмисник ініціює «сліпі» атаки, що означає, що зловмисник не здогадується, коли датчик увімкнений чи вимкнений. Іншими словами, «сліпий» атакуючий сигнал впливає на кожен зразок вимірювання. Це є причиною того, що справжня позитивна ймовірність для цих двох випадків становить 100%.

ВИСНОВКИ

В статті показано загальну модель сенсорних систем і пояснено як потрапляє атакуючий сигнал в сенсорну систему дистанційно. Зловмисники можуть використовувати електромагнітні завади для зміни показань датчиків, а такі атаки можуть загрожувати конфіденційності та безпеці користувацької інформації.

В якості побічного ефекту число потенційних загроз і можливих атак на безпеку або конфіденційність пристроїв або цілих систем різко зросла. На жаль, в області IoT ще не приділяється достатньо великої уваги питанню безпеки [3].

Виявлення існування сигналів або протоколів може поставити під загрозу безпеку користувача, наприклад, якщо у користувача є дуже дорогий пристрій. Більш того, такий тип атаки може привести до серйозної проблеми конфіденційності в різних системах [4].

В даній роботі було зосереджено увагу на атаках з потужними ЕМЗ, в яких зловмисник маніпулює датчиками користувача, щоб внести саме ті значення, які бажає. Перш за все, зловмисник може контролювати вихід сенсорної системи та обманювати мікроконтролер.

Для успішної зміни показань датчика зловмисник покладається на дві особливості сенсорної системи: одна полягає в тому, що провід, що з'єднує датчик і мікроконтролер, виконує роль антени; інший - нелінійність електронних компонентів або субдискретизація (заниження долі окремих складових) з АЦП.

З наведених експериментальних результатів видно, що система може вважати шкідливий сигнал нормальним сигналом. Далі, показано як розгорнути метод виявлення до будь-якої сенсорної системи для виявлення та знешкодження дії атакуючого сигналу.

Метод демонструє, що коли зловмисник ініціює «сліпі» атаки, тобто, не здогадується, коли датчик увімкнений чи вимкнений, він не може обійти систему виявлення та здійснити успішну атаку. Іншими словами, «сліпий» атакуючий сигнал впливає на кожен зразок вимірювання. Це є причиною того, що справжня позитивна ймовірність для цих двох випадків становить 100%.

На практиці важко проводити «розумні» атаки, які дозволяють зловмиснику вгадувати і вирівнювати атакуючий сигнал з датчиком виходу. Отже, представлена система моніторингу побічних атакуючих електромагнітних випромінювань має високий ступінь гарантії виявлення. Ймовірність того, що зловмиснику вдасться обманути систему є дуже низькою.

ЛІТЕРАТУРА

[1]. QIVICON [Електронний ресурс]. Режим доступу: https://en.wikipedia.org/wiki/QIVICON.

[2]. Кодування і передача даних з допомогою адаптера [Електронний ресурс]. Режим доступу: https://studopedia.su/3_27863_koduvannya-signaliv.html.

[3]. L. Atzori, A. Iera,G. Morabito, "The Internet of Things: A survey", *Computer Networks*, iss.15, pp. 87-96, 2010.

[4]. Д. Ляхов, А. Стрелкина, Д. Узун, "Анализ методов и средств оценивания и обеспечения кибербезопасности IoT системы", *Открытые информационные и компьютерные интегрированные технологии*, №80, С. 182-193, 2018.

СИСТЕМА МОНИТОРИНГА ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ С ИСПОЛЬЗОВАНИЕМ ПЛАТФОРМЫ QIVICON

Показано, как отдаленно может быть введён сигнал от злоумышленника в сенсорную систему. Объяснено, как работает представленный датчик при наличии сигнала атаки. Подробно показано, как работает предложенный метод защиты и проанализирована его безопасность. Показано, как сохранять определенную гарантию безопасности. Предложен новый метод защиты для выявления нападения, основанный на идее,

что когда у датчика выключается питание, выход сенсора должен быть «спокойным». Если сигнал атаки злонамеренно индуктируется в систему датчиков во время «спокойного» периода, микроконтроллер может это обнаружить. Представлено детальное описание метода выявления ЭМП (электромагнитных помех) и доказано гарантию их выявления в контексте сильной модели злоумышленника. Такой подход для выявления общих сигналов ЭМП может существовать как в микрофонной системе, так и в системе датчиков температуры, или других сенсоров. Объяснено, что такое манчестерское кодирование и продемонстрировано на графике, как и для чего оно применяется в данной работе. Показано, как детали и составляющие сенсорных систем уязвимы к атакам. Доказано, что представленный в работе механизм обнаружения является и эффективным, и надежным. Доводы основаны только на теоретических расчетах, однако, они включают в себя все возможные отклонения. Сосредоточено внимание на атаках с мощными ЭМП, в которых злоумышленник манипулирует датчиками пользователя, чтобы внести именно те значения, которые желает.

Ключевые слова: электромагнитные помехи, сенсорный датчик, «умный дом», система мониторинга, сигнал атаки.

ELECTROMAGNETIC ADVERSE RADIATION MONITORING SYSTEM USING THE QIVICON PLATFORM

In this article it was explained how a harmful signal could be intruded into the sensor system remotely. The structure of the sensor, which was considered vulnerable to electromagnetic interference, has been presented. Demonstrated the way of how the microcontroller and other components of the sensor work. The exact explanation was given to determine exact ways how the proposed sensor works in the presence of an attack signal. Examples were given of how the attack detection system changes with respect to the type of physical quantity measured by the sensor. It was presented in detail how the proposed method of protection works and its safety was analyzed. Hereby shown how to keep a certain security guarantee. A new method of protection for attack detection has been proposed, which is based on the idea that when the sensor is turned off, the sensor output should be "quiet". If the attack signal is maliciously induced into the sensor system during the "quiet" period, the microcontroller can detect it. A detailed description of the method of detecting EMC (electromagnetic interference) is presented and the guarantee of their detection in the context of a strong model of an attacker is proved. Such approach for detecting common EMF signals can exist both in a microphone system and in a system of temperature sensors or other sensors. It was explained what Manchester coding is and was shown in the graph, how and why it was used in this work. It shows which parts and components of the sensor systems were vulnerable to attacks and explains how these components could have been protected in the near future. It has been proven that the detection mechanism presented in the paper is both effective and reliable. The proofs were based only on theoretical calculations; however, they include all possible deviations. The subject focus was concentrated on the attacks with powerful EMCs, in which an attacker manipulates the user's sensors to enter exactly the values he wants.

Keywords: electromagnetic interference, touch sensor, smart home, monitoring system, attack signal.

Романова Анна Віталіївна, випускниця Національного авіаційного університету, магістр за спеціальністю "Телекомунікації та радіотехніка".
E-mail: annieromanova22@gmail.com.
Orcid ID: 0000-0001-7642-9346.
Романова Анна Витальевна, выпускница Национального авиационного университета, магистр по специальности "Телекоммуникации и радиотехника".
Romanova Anna, National Aviation University graduate, Master in Telecommunications and Radio Engineering.

Конахович Георгій Филимонович, доктор технічних наук, професор, завідувач кафедри телекомунікаційних та радіоелектронних систем Національного авіаційного університету.
E-mail: tks@nau.edu.ua.
Orcid ID: 0000-0002-6636-542X.
Конахович Георгий Филимонович, доктор технических наук, профессор, заведующий кафедрой телекоммуникационных и радиоэлектронных систем Национального авиационного университета.
Konakhovych Heorhiy, Doctor of Technical Sciences, Professor, Head of the Department of Telecommunication and Radio-Electronic Systems of the National Aviation University.