УДК 004.056.53

ЕЛЕКТРОМАГНІТНА АТАКА НА ПОСЛІДОВНІ ІНТЕРФЕЙСИ ЗВ'ЯЗКУ ТА ПРОТИДІЯ ЇЙ

В. М. Вдовенко[1], В. М. Степаненко[1]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

У роботі досліджено один з видів електромагнітних атак на системи послідовної асинхронної передачі даних. Атака з заміною бітів дозволяє порушнику побітово перехоплювати та змінювати інформацію, тим самий порушуючи її цілісність. Запропоновано декілька методів протидії подібним атакам для запобігання несанкціонованого збору і спотворення інформації.

Ключові слова: SPI, UART, I^2C, електромагнітна атака.

Вступ

Кібернетичні системи залежать від цілісності даних, що передаються між давачами, механізмами та контролерами. Актуальність даної роботи поянюється широким використанням дротового послідовного цифрового зв'язку для вказаної передачі даних. Він менш вразливий до електромагнітних перешкод, ніж бездротовий зв'язок. На відміну від паралельного зв'язку, послідовний спосіб передачі даних вимагає менше проводів. Стандарти послідовного зв'язку, такі як SPI, UART і I^2C, використовують для підключення контролерів до безлічі давачів і навіть приймачів GPS. Зловмисник, який має можливість маніпулювати бітами, що передаються давачами, може здійснити атаку з ін'єкцією помилкових даних. Наприклад, якщо він отримає змогу маніпулювати даними про місцезнаходження або швидкість, отриманими за допомогою бортового GPS безпілотного літального апарата, або показами давачів швидкості швидкості колеса транспортного засобу, то такі системи можуть вийти з ладу.

1. Модель загрози

В даній роботі досліджено можливість того, що зловмисник може змінити цифрову інформацію (тобто біти) за допомогою аналогових засобів. Маніпулювання цифровими даними суттєво відрізняється від подібних атак з використанням електромагнітної індукції на аналогові пристрої. По-перше, зловмиснику необхідно індукувати напругу, що відповідає з логічним рівнем передавача (наприклад, $3,3/5$ В для CMOS/TTL). По-друге, зловмисник повинен визначити, коли дані передаються, і синхронізувати своє обладнання з цільовою системою. Синхронізація вимагає, щоб зловмисник отримав часові характеристики системи жертви. Наприклад, щоб перетворити нуль на одиницю (припускаючи логіку CMOS), зловмисник повинен замінити сигнал з 0 В на $3,3$ В у той момент, коли приймач жертви аналізує сигнал. Додаткова складність отримання необхідної інформації про часові характеристики полягає в тому, що дротовий зв'язок значно складніше прослухати, ніж бездротовий (незважаючи на технології формування променю та вузьконаправлені антени).

Зловмисник намагається змінити дані, націлюючись на виходи периферійних пристроїв послідовного зв'язку, що працюють на логічних рівнях CMOS/TTL (тобто $3,3/5$ В). Послідовний зв'язок, який використовує сигналізацію фізичного рівня з вищою напругою (наприклад, RS-232) або диференціальну сигналізацію (наприклад, RS-422), все ще вразливий до обраної атаки, оскільки такі системи зазвичай реалізуються за допомогою, наприклад, периферійного пристрою UART, який перетворює вихідні сигнали CMOS/TTL периферійного пристрою на необхідні лінійні напруги.

Система зловмисника не має фізичного зв'язку з апаратним забезпеченням жертви, а сигналами зв'язку маніпулюють виключно за допомогою навмисного електромагнітного впливу. Зловмисник знаходиться поблизу жертви та використовує не заборонене комерційне апаратне забезпечення (наприклад, генератор сигналів довільної форми, підсилювач, фільтр низьких частот, підсилювач із низьким рівнем шуму та зонд магнітного поля). Він вводить дані за допомогою вузькосмугового сигналу. Передбачається, що зловмиснику заздалегідь відома номінальна тривалість бітів (тобто швидкість передачі) послідовних кадрів (і що тривалість є постійною в межах кадру), а також відома довжина кадрів (також постійна), яка практично реалізовано в більшості послідовних протоколів. Зловмисник може отримати ці параметри (тривалість бітів і довжину кадру) шляхом підслуховування комунікацій перед тим, як почати атаку.

Приймач системи послідовного зв'язку відбирає вхідні дані в центрі часового проміжку передачі кожного біта даних. Зловмисник, маючи інформацію

про час дискретизації жертви, може генерувати певну форму сигналу, щоб збільшити або зменшити напругу жертви в моменти дискретизації, щоб змінити біти контрольованим способом. Згаданий вище вузькосмуговий сигнал розроблений таким чином, що напруга жертви збільшується або зменшується під час дискретизації для перевертання бітів. Нарешті, передбачається, що зловмисник використовує взаємоіндукцію у малому радіусі, щоб зробити атаку ефективною за наявності радіочастотного екранування. Необхідні структури для створення та спрямування таких полів включають вузькосмугові петльові антени, соленоїди та тороїди.

Процес проведення атаки можна умовно поділити на три етапи:

1. Етап виявлення – порушник відстежує побічне електромагнітне випромінювання від комунікацій жертви.
2. Етап обробки сигналу – порушник аналізує отриманий сигнал для синхронізації свого обладнання з темпом передачі даних жертви.
3. Етап впливу – порушник генерує електромагнітний сигнал для впливу на обладнання жертви, змінюючи інформацію на потрібну йому.

1.1. Характеристика жертви

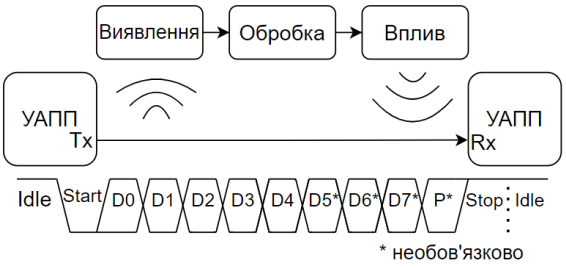

Рис. 1. Схематичне зображення атаки

В якості цілі можливої атаки взято універсальний асинхронний приймач/передавач (УАПП). Типовий пристрій УАПП має два порти, Tx і Rx , для передачі та отримання даних відповідно (рис. 1). Він також відповідає за перетворення паралельних даних у послідовні для Tx або навпаки для Rx. Передача даних є асинхронною, що означає, що немає головного тактового сигналу для синхронізації Tx і Rx, і передача даних починається, коли в каналі є дані (тобто ініціюється переходом від високого до низького вольтажу для початкового біта) [1]. Кадр даних УАПП завжди починається з нульового біта, що призводить до переходу високого рівня сигналу в низький, оскільки канал має високий рівень у режимі очікування, тобто в режимі відсутності даних. Цей перехід від високого рівня напруги до низького на початку кадру даних ініціює операцію отримання, і порт Rx починає вибірку даних кілька разів (наприклад, 16 разів) із швидкості передачі (наприклад, $9,6$ кбіт/с). Кадр даних УАПП включає стартовий біт, від 5 до 8 бітів даних, один біт контролю парності (необов'язковий) і 1, $1,5$ або 2 стоп-біта. Атаки будуть показані на кадрах з 8-бітовими даними та одним стоп-бітом без перевірки парності.

Модуль приймача відбирає вхідні дані в центрі кожного біта даних. Поширеним методом є налаштування тактової частоти приймача на 16-кратну швидкість передачі (baud rate). Після переходу від високого до низького початкового біта, перша вибірка виконується в середині початкового біта (тобто на 8-му такті), щоб гарантувати, що в каналі є дані, і виявлений перехід від високого до низького не через шум. Потім для виявлення даних виконується вибірка кожні 16 тактів, які знаходяться в середині сигналу бітів даних.

1.2. Етап виявлення

На етапі виявлення зловмисник пасивно прослуховує витік електромагнітного випромінювання в схемі жертви. Коли починається передача даних, висока напруга в неактивному каналі УАПП стає рівною 0 В для молодшого початкового біта, а невеликий, але помітний змінний у часі струм жертви i_v, який випромінює магнітне поле $\boldsymbol{B}_v$, циркулює в схемі УАПП. $\boldsymbol{B}_v$ уловлюється давачем поля.

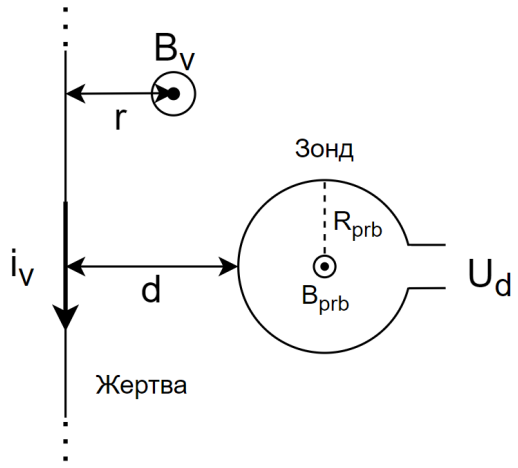

Рис. 2. Детектування побічного випромінювання жертви

Закон Фарадея стверджує, що змінне в часі магнітне поле, нормальне до петлі провідника, призводить до виникнення електрорушійної сили (ЕРС) на вільних електронах провідника та породжує різницю потенціалів між кінцями провідника. Для визначення зв'язку між струмом жертви, i_v, і виявленою напругою від зонда поля, $\boldsymbol{U}_d$, використовується модель на рисунку 2. Зонд кругового поля розташований на відстані d від сигнальної лінії жертви. Струм жертви, i_v, вважається нескінченно довгим, що справедливо для сигнальних ліній з набагато більшою довжиною, ніж радіус зонда, $\boldsymbol{R}_{prb}$.

$$\boldsymbol{B}_v = \frac{\mu_0 i_v}{2\pi r} \tag{1}$$

де μ_0 – магнітна проникність вільного простору, r – відстань від провідника.

Індукована напруга, U_d, на затискачах давача поля є похідною за часом потоку, захопленого нормально до поверхні давача поля.

$$U_d = -\frac{\mathrm{d}}{\mathrm{dt}} \iint_{S_{prb}} B_v \cdot dS = -\mu_0 \frac{\mathrm{d}}{\mathrm{dt}} \iint_{S_{prb}} \frac{i_v}{2\pi r} \cdot dS \quad (2)$$

Якщо радіус зонда досить малий порівняно з відстанню прослуховування, електромагнітний витік жертви, B_v, на поверхні зонда є приблизно рівномірним і дорівнює полю в центрі зонда ($r = R_{prb} + d$).

$$B_v = \frac{\mu_0 i_v}{2\pi(d + R_{prb})} \quad (3)$$

З формул (2) і (3) виводимо детектовану напругу:

$$U_d = -\mu_0 \frac{R_{prb}^2}{2(d + R_{prb})} \frac{\mathrm{d}}{\mathrm{d}t} i_v \quad (4)$$

1.3. Етап обробки сигналу

На етапі обробки сигналу аналоговий витік оцифровується і з нього виділяються піки напруги. Процес обробки сигналу повинен мати низьку затримку, щоб гарантувати, що навіть перший біт після початкового біта, наприклад, D0 у кадрі УАПП (рис. 1), може бути змінений за допомогою електромагнітної індукції після виявлення. Наприклад, хвиля атаки повинна передаватися за 156,25 мкс, що є тривалістю 1,5 біта, для перевертання D0 у системі УАПП 9,6 Кбіт/с [2]. Максимально допустима затримка стає суворішою зі збільшенням швидкості передачі даних.

Для обробки сигналу можна використовувати різні процесори, такі як Software-defined radio (SDR), програмовані вентильні матриці (FPGA) або цифрові процесори обробки сигналів (DSP). Завдяки простоті розробки програми та портативності, SDR є життєздатним варіантом для обробки сигналів. Проте SDR, як відомо, мають високу затримку [3], оскільки радіоінтерфейс і комп'ютер загального призначення, на якому виконується більша частина обробки сигналів, спілкуються через інтерфейси, такі як Ethernet, USB або PCIe. Затримка USRP X300 із з'єднанням PCIe становить від 8 до 15 мс. Мінімальна затримка SDR навіть із високоякісними USRP, такими як X300, і швидкими інтерфейсами, такими як PCIe, становить принаймні 8 мс, що значно перевищує максимально допустиму затримку (156,25 мкс) для системи УАПП 9,6 Кбіт/с.

Цифрові осцилографи з частотою дискретизації до 5 Gsps можуть бути використані для оцифровки витоку електромагнітного струму жертви та ініціювання сигналу атаки [2]. Затримка цифрового осцилографа визначається як час затримки між надходженням сигналу на вхід осцилографа і передачею сигналу тригера з виходу осцилографа. Вихід тригера осцилографа посилає сигнал від низького до високого, коли осцилограф виявляє пік вище певного порогу, який регулюється вручну під час атак. Відомо показники затримки для двох цифрових осцилографів, а саме Keysight DSOX3024T і Tektronix MDO4104C, і вони становлять 24 нс і 40 нс для моделей Tektronix і Keysight відповідно. Як висновок, затримка кожного осцилографа значно нижча за необхідну затримку (наприклад, 156,25 мкс для жертви зі швидкістю передачі даних 9,6 кбіт/с). Крім того, затримки осцилографа дуже послідовні, на відміну від затримок SDR. Як тільки осцилограф виявляє пік напруги (наприклад, пік через початковий біт кадру даних УАПП) у зібраному електромагнітному витоку жертви, тригерний сигнал осцилографа надсилається до генератора сигналу, щоб розпочати ін'єкцію сигналу атаки. Затримка генератора сигналу, яка є часовою затримкою між прийомом тригерного сигналу (від осцилографа) і передачею сигналу атаки, також додається до загальної затримки етапу обробки сигналу. Відомо, що затримка, наприклад, Agilent 33600A є постійною і становить 150 нс. Незважаючи на те, що затримка генератора сигналу вища, ніж затримка вказаних вище цифрових осцилографів, вона все ще значно нижча від необхідної затримки. Це показує, що осцилограф і генератор сигналу із загальною затримкою приблизно 200 нс можна використовувати як процесор для обробки сигналу на цьому етапі атаки.

1.4. Етап впливу

Як тільки дані жертви виявлені, починається етап впливу. Вона полягає в випромінюванні хвилі спеціальної форми до схеми жертви. Зловмисник використовує випромінювач магнітного поля, наприклад тороїд, соленоїд або рамкову антену, щоб ефективно генерувати магнітне поле та індукувати напругу в схемі жертви.

Нехай зловмисник використовує соленоїд із зовнішнім магнітним полем, щоб маніпулювати бітами на відстані. Тоді, магнітне поле осі z, B_z, соленоїда [4]:

$$B_z = \frac{\mu N i_a}{2} \left(\frac{\frac{L}{2} - z}{L\sqrt{R^2 + (\frac{L}{2} - z)^2}} + \frac{\frac{L}{2} + z}{L\sqrt{R^2 + (\frac{L}{2} + z)^2}} \right) \quad (5)$$

де μ – магнітна проникність середовища, тобто повітря, N – кількість витків, L – довжина соленоїда, z – відстань по осі z.

Зафіксований магнітний потік визначається аналітично, а U_{ind} визначається за допомогою похідної за часом. Оскільки U_{ind} лінійно пропорційне частоті атаки в безперервній формі сигналу (тобто, похідна за часом від синусоїди), низькочастотні атаки страждають від низької ефективності зв'язку. Щоб подолати це, можна використовувати форми струму з різкими змінами та великими похідними за часом, такі як пилкоподібна хвиля. Іншим варіантом є генератори імпульсного струму, які генерують високий струм протягом дуже короткого проміжку часу, як

практикується в методі транскраніальної магнітної стимуляції (TMS).

2. Потенційні методи захисту

Одним з методів запобігання впливу зовнішніх електромагнітних полів на передачу інформації є використання оптоволоконних систем передачі даних. Оптоволоконний зв'язок є надійним способом передачі даних у насиченому електромагнітними полями середовищі, оскільки дані надсилаються у вигляді світла через волоконний кабель, у якому немає вільних електронів, на відміну від звичайних способів передачі (наприклад, кабелів, провідних доріжок друкованих плат). Недоліком є вища складність і вартість таких систем у порівнянні зі звичайними електронними.

Ще одним методом захисту може слугувати екранування. Екранування полягає в захисному покритті чутливих до електромагнітного випромінювання компонентів екрануючою оболонкою. Екран може бути виконаний у вигляді фольги або металевої сітки, яка ефективно розсіює електромагнітні поля та запобігає їх проникненню до проводів. Екран також може бути заземлений, що допомагає виводити будь-яке випромінювання з пристрою.

Скручені кабелі, в яких два або більше кабелів переплетені між собою, використовуються для мінімізації електромагнітного випромінювання один від одного, однак вони також стійкі до електромагнітних перешкод від зовнішніх джерел [5]. Скручений кабель являє собою ланцюжок невеликих петель жертви з протилежними нормалями до поверхні. Це означає, що навіть якщо зловмисник індукує напругу в одній петлі, у наступній петлі, припускаючи, що величина магнітного поля не зміниться суттєво, та сама напруга індукується з протилежним знаком, що скасовує індуковану напругу в попередньому контурі.

Висновки

У роботі досліджено механізм підміни даних, що передаються через послідовний цифровий дротовий канал зв'язку. Показано, що вони можуть бути змінені контрольованим чином за допомогою впливу генерованих ззовні електромагнітних полів, що призводить до порушення цілісності інформації і збоїв в роботі системи, в якій вона циркулює (наприклад, втрата орієнтації безпілотного апарата). Визначено алгоритм дій, який повинен здійснити порушник для реалізації атаки. Надано рекомендації щодо запобігання подібним атакам, а саме: заміна електронних комунікацій оптоволоконними, використання дротів з екрануючим покриттям, використання скручених дротів.

Перелік використаних джерел

1. *Laddha M. R.*, *Thakare A. P.* A Review on Serial Communication by UART // International Journal of Advanced Research in Computer Science and Software Engineering. — 2013. — Т. 3. — URL: https://www.academia.edu/download/35186800/V3I1-0220.pdf.
2. *Dayanıklı G. Y.* Electromagnetic Interference Attacks on Cyber–Physical Systems: Theory, Demonstration, and Defense. — 2021. — 193 с. — URL: https://vtechworks.lib.vt.edu/bitstream/handle/10919/104862/Dayanikli_G_D_2021.pdf.
3. *Schmid T.*, *Sekkat O.*, *Srivastava M. B.* An Experimental Study of Network Performance Impact of Increased Latency in Software Defined Radios // Proceedings of the Second ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization. — Montreal, Quebec, Canada : Association for Computing Machinery, 2007. — С. 59—66. — (WinTECH '07). — ISBN 9781595937384. — DOI: 10.1145/1287767.1287779. — URL: https://doi.org/10.1145/1287767.1287779.
4. *Callaghan E. E.*, *Maslen S. H.* The magnetic field of a Finite solenoid. // Technical Report D465, NASA Lewis Research Center. — 1960. — URL: https://ntrs.nasa.gov/api/citations/19980227402/downloads/19980227402.pdf.
5. *Barnett D.*, *Groth D.*, *McBee J.* Cabling: The Complete Guide to Network Wiring, Third Edition. — 2006. — 720 с. — URL: https://www.academia.edu/17984876/Cabling_The_Complete_Guide_to_Network_Wiring_Third_Edition.