АНАЛІЗ КІБЕРЗАГРОЗ ТА ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ 5G-МЕРЕЖ У СИСТЕМАХ УПРАВЛІННЯ АВТОНОМНИМИ КОМПЛЕКСАМИ

Зозуля М.В., В'юхін Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Впровадження мереж п'ятого покоління (5G) у контури керування автономними комплексами – безпілотними літальними апаратами та наземними роботизованими платформами – забезпечує передавання телеметрії та відео високої чіткості в реальному часі; специфікація URLLC визначає цільову надійність $1-10^{-5}$ для пакета обсягом 32 байти за затримки user plane 1 мс, причому 3GPP встановлює суворіший орієнтир 0,5 мс окремо для кожного напрямку передавання. Оскільки порушення цілісності каналу керування (C2) означає для такої платформи не втрату даних, а втрату керованості фізичним об'єктом, у роботі розглянуто механізм атак типу Man-in-the-Middle (MitM) у радіоканалі 5G, застосовному саме до такого контуру керування. Показано, що вразливість зумовлена двома архітектурними факторами: незахищеним цілісністю вікном до автентифікації UE та політиковою, фактично опціональною, активацією захисту цілісності user plane (UPIP).

Мета роботи розглянути можливість проведення успішної атаки типу MitM у 5G-контурах керування автономними комплексами та оцінити достатність передбачених стандартом контрмір. Основна теза: таке втручання можливе не через слабкі криптографічні примітиви, а через два архітектурні фактори – вікно до автентифікації та фактично опціональну активацію захисту цілісності user plane.

Перший фактор. У термінології 3GPP кінцевий пристрій, що підключається до мережі, називають UE (User Equipment); для автономного комплексу в ролі UE виступає саме бортовий 5G-модем дрона чи робота — той самий вузол, який приймає команди керування та передає телеметрію, тобто атака на UE є атакою безпосередньо на контур C2. Повідомлення RRC та NAS, передані до процедури Security Mode Command, не мають захисту цілісності, а широкомовні блоки MIB/SIB не захищені в жодній із генерацій. Початкові фази входу в мережу, які відбуваються до застосування механізмів безпеки 5G, є найуразливішими, а проблема фальшивих базових станцій досі має статус дослідження (3GPP TR 33.809) і не закрита нормативно.

Другий фактор. У LTE протокол PDCP забезпечує для control plane і шифрування, і захист цілісності, тоді як для user plane — лише шифрування без захисту цілісності, що породжує malleable encryption і безпосередньо уможливлює підміну корисного навантаження. У 5G підтримка захисту цілісності user plane (UPIP) обов'язкова для gNB, проте активація виконується для кожного радіоносія окремо згідно з політикою, а гранична швидкість для UPIP узгоджується під час встановлення PDU-сесії; через накладні витрати на розмір пакета функція на практиці часто не використовується. NSA-фаза 5G

успадковує відсутність захисту цілісності user plane повністю, тоді як у SA-фазі атака блокується лише за умови фактичного ввімкнення UPIP; окремо відзначено підвищений ризик для високоцінних IoT- та IIoT-пристроїв, тобто саме для класу бортових контролерів [1].

Розрив між специфікацією та практикою підтверджено інструментальними замірами сигналізації у двох операторів, присутніх приблизно у 70 % країн ЄС: зафіксовано повну відсутність SA-розгортань, передавання постійних ідентифікаторів IMSI та IMEI у відкритому вигляді, а також те, що захист конфіденційності увімкнено в більшості мереж, тоді як захист цілісності відсутній. Саме ця відсутність дозволяє противнику виконувати маніпуляцію даними та імперсонацію, тобто MitM, навіть за активного шифрування [2].

Зіставлення механізмів захисту радіоінтерфейсу наведено в табл. 1.

Таблиця 1 – Зіставлення механізмів захисту радіоінтерфейсу 4G та 5G SA

Механізм	**4G (LTE)**	**5G SA**
Постійний ідентифікатор абонента	IMSI передається відкритим текстом	SUCI — закриття SUPI асиметричною криптографією
Цілісність user plane	Відсутня (лише шифрування)	Підтримка обов'язкова, активація за політикою (per-DRB)
Радіоможливості UE	Передаються до активації безпеки (bidding down)	Передаються після Security Mode Command
Пейджинг	Нагода виводиться з IMSI	Нагода виводиться з 5G-S-TMSI
Широкомовні MIB/SIB	Без захисту цілісності	Без захисту цілісності (3GPP TR 33.809)

Атаки типу «людина посередині» вже давно становлять серйозну загрозу для телекомунікаційних мереж, дозволяючи зловмисникам перехоплювати, змінювати та перенаправляти легітимні повідомлення [3].

Прихід нового класу загроз не є головною відмінністю від попереднього покоління; ключовим фактором є саме зниження порогу входу для нападника. Атака SigOver на LTE вимагала переваги в потужності близько 40 дБ , тоді як сучасні реалізації для 5G задовольняються незначним перевищенням; послідовність SigOver → aLTEr → IMP4GT → Sni5Gect → 5Gone демонструє перехід від лабораторних умов до публічних мереж і від спеціалізованого обладнання до звичайної обчислювальної платформи.

Атака SigOver, вперше продемонстрована на LTE, полягала в overshadowing: зловмисник передавав власний сигнал одночасно з легітимною базовою станцією, перебиваючи широкомовні повідомлення на користь підробленого пакета, але для цього була потрібна перевага в потужності приблизно 40 дБ над сигналом справжньої макровежі. Пряме перенесення цього принципу в 5G змінює саму фізику атаки, оскільки радіодоступ 5G

будується не на поодиноких потужних вежах, а на щільній сітці малих сот, зокрема в міліметровому діапазоні, де кожна станція обслуговує значно меншу територію, ніж макростанція LTE.

Через коротшу відстань між UE і власною станцією рівень легітимного сигналу, який потрібно перебити, у 5G здебільшого нижчий, ніж у зоні покриття LTE-вежі, тож для придушення вже достатньо незначного перевищення потужності в тих самих часо-частотних ресурсах — саме такий принцип демонструє 5Gone, перевірений на комерційних сотах шириною 100 МГц із наскрізною затримкою менш ніж 500 мкс. Водночас дистанція, на якій може діяти зловмисник відносно однієї станції, скорочується разом з радіусом соти, проте кількість самих сот на тому самому маршруті польоту дрона в рази зростає, тож зона, де можливе перехоплення каналу керування, не звужується, а фактично розширюється; це підтверджують і дослідження на рівні реалізацій, які фіксують успішне приєднання до фальшивої станції та пониження з'єднання без істотної переваги в потужності. Попри сильнішу криптографію 5G, нижчий поріг для атак overshadowing та нові точки вразливості лише підвищили ризики для контуру керування C2 порівняно з LTE.

Отже, шифрування каналу керування без обов'язкового захисту цілісності user plane і без заборони пониження генерації не забезпечує стійкості автономного комплексу до атак MitM, а фаза до автентифікації, яку регулює 3GPP TR 33.809, і досі залишається незакритою. Тому для контуру C2 потрібні конкретніші кроки, а не просто «увімкнути шифрування». По-перше, для телеметрії та команд захист цілісності (UPIP) має бути обов'язковим («Required»), тоді як відео можна передавати окремим потоком без цієї вимоги. По-друге, на бортовому обладнанні варто заборонити пониження до 4G і дозволити роботу лише в 5G SA, що прибирає останній крок більшості описаних атак. По-третє, оскільки MAVLink не має власного захисту, поверх нього потрібне шифрування з перевіркою автентичності та захистом від повторного відтворення команд. По-четверте, телеметрію варто звіряти з інерціальними датчиками та камерою – розбіжність цих даних вказує на підміну каналу.

Список літератури

1. Rupprecht D., Kohls K., Holz T., Pöpper C. IMP4GT: IMPersonation Attacks in 4G NeTworks. Network and Distributed System Security Symposium (NDSS 2020). Reston : Internet Society, 2020. DOI: https://doi.org/10.14722/ndss.2020.24283

2. Lasierra O., Garcia-Aviles G., Municio E., Skarmeta A., Costa-Pérez X. European 5G Security in the Wild: Reality versus Expectations. Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '23). New York : ACM, 2023. URL: https://arxiv.org/abs/2305.08635

3. Kotukh Y. V. Evolution of Man-in-the-Middle attacks in 5G telecommunication systems / Y. V. Kotukh, G. Z. Khalimov, I. Y. Dzhura // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2025. – №222. – P. 98–107. – DOI: 10.30837/rt.2025.3.222.09.