КРИПТОГРАФІЧНЕ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ПОВІДОМЛЕНЬ В КІБЕРФІЗИЧНИХ СИСТЕМАХ

Караман Д.Г., Комаров Г.А.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

Сучасний розвиток кіберфізичних систем (КФС) демонструє стрімке зростання інтеграції фізичних процесів та цифрових обчислень у єдині розподілені системи [1]. Такі системи дедалі частіше використовуються в критичних галузях: промисловій автоматизації, енергетиці, транспорті, охоронних системах, медичних пристроях. Враховуючи високі вимоги до безпеки та стабільності функціонування, однією з ключових проблем КФС стає забезпечення цілісності переданих даних.

Цілісність повідомлень у КФС безпосередньо впливає на достовірність рішень, які приймаються системою в реальному часі. Збій або навмисна модифікація даних через атаку може призвести до фізичних наслідків – аварій, відмов обладнання, загрози життю людей. Це робить питання забезпечення цілісності не лише технічним, а й стратегічним завданням для розробників та операторів КФС.

Традиційні методи захисту, засновані лише на перевірці коректності даних на прикладному рівні, не забезпечують належного рівня стійкості до атак на цілісність [2]. Тому доцільним є використання криптографічних механізмів, зокрема: кодів аутентифікації повідомлень (MAC), криптографічних хеш-функцій (SHA-3, BLAKE2), цифрових підписів та захищених протоколів передачі даних. Їх використання дозволяє захистити як прості IoT-пристрої, так і складні мікроконтролерні комплекси від атак на цілісність.

Розроблено програмний модуль для перевірки цілісності повідомлень в КФС. Він призначений для інтеграції у мережеву взаємодію мікроконтролерів, IoT-пристроїв та серверів. Модуль повинен враховувати обмеження ресурсів, забезпечувати захист від типових атак на цілісність – зокрема від підміни повідомлень, модифікації трафіку та атак типу *man-in-the-middle*.

Проаналізовано сучасні криптографічні методи забезпечення цілісності: MAC-коди, SHA-3, BLAKE2, цифрові підписи (ECDSA, Ed25519) та протоколи TLS, DTLS, MQTT з автентифікацією. Систематизовано основні загрози та атаки, що порушують цілісність даних у КФС, обґрунтовано вибір оптимального методу для програмної реалізації. Розроблено структуру програмного модуля забезпечення цілісності для мікроконтролерів, IoT-пристроїв та серверів.

Література:

1. Karaman D. G., Dzevochko O. M., Olshevskii O. M. Automated monitoring of high-speed processes in cyber-physical systems. Автоматизація, електроніка, інформаційно-вимірювальні технології: освіта, наука, практика: матеріали IV Міжнарод. наук.-техн. конфер., (28-29 листопада 2024 р.) Харків: НТУ «ХПІ». 2024. 305 с. (с.17-18) ISBN 978-617-05-0519-4

2. Zuev A., Karaman D., Olshevskiy A. «Wireless sensor synchronization method for monitoring short-term events.» Advanced Information Systems, Vol. 7(4). 2023. pp. 33–40.