УДК 004.056

МЕТОДИ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ ПОТОКІВ ІЗ ЗАСТОСУВАННЯМ ХЕШУВАННЯ

А. В. Ярмілко, І. О. Розломій, Г. В. Косенюк
Черкаський національний університет імені Богдана Хмельницького, Україна

Сучасні виробничі системи поєднують в одному комплексі людей і технічні пристрої, в тому числі – роботизовані модулі різного рівня інтелектуальності та автономності, що передбачає їхню кооперацію в процесі виконання прикладних завдань. Нового рівня складності функціонування таких систем набуває при виконанні завдань у відкритому виробничому просторі, який не забезпечує ізоляцію такого кооперативного утворення від сторонніх виробничих та невиробничих факторів. З розвитком виробничих систем спостерігаємо зникнення фізичних бар'єрів між людьми та роботами у процесі їхньої спільної виробничої діяльності, а також перехід кооперації у співробітництво. Однак існує проблема, пов'язана з відсутністю належної довіри до дій робота при співробітництві. У взаємодії людей всі аспекти цього процесу розгортаються відносно легко та без особливих зусиль, і здебільшого це відбувається підсвідомо завдяки розумовій здатності. Досягнення подібної двосторонньої та безперебійної взаємодії між людьми та роботами, що працюють разом, – це нове велике завдання [1]. Воно безпосередньо пов'язане із забезпеченням гарантоздатності утвореної системи компонентів з природним та штучним інтелектом. Одною з актуальних задач у цьому контексті є захист внутрісистемних комунікацій як один з кроків на шляху досягнення вищого рівня довіри у людино-машинній системі за рахунок достовірності інформації.

У кооперативних виробничих системах з гібридним (людино-машинним) інтелектом при використанні їх у відкритому просторі можлива дія завад, в тому числі – в комунікаційних процесах. Також можлива внутрішня кластеризація системи, яка відбивається на комунікаційній структурі. При цьому метою утворення комунікаційних кластерів, крім суто функціональних аспектів, було б недопущення (чи мінімізація) стороннього втручання (умисного чи випадкового) в канали інформаційного обміну виробничих підсистем. Це найбільше стосується саме машинних компонентів, оскільки їхній інтелект не завжди здатен розпізнати джерело надходження даних, внаслідок чого можуть бути запущені хибні сценарії їхнього функціонування з негативними наслідками різного ступеня тяжкості.

Таким чином, технологічно необхідним є виконання аналізу інформаційних повідомлень між компонентами кластеру. Проте нас може цікавити не тільки виявлення помилок, але й виявлення відмінностей двох інформаційних фрагментів або їх примірників. Природа відмінностей може бути різною, а їхня оцінка – залежною від мети аналізу інформації. Якщо метою буде контроль збереження інформації в комунікаційному процесі, то відмінність трактуватиметься як помилка з усіма можливими наслідками реагування на неї. Якщо ж нас цікавитиме структура чи динаміка змін інформаційних фрагментів, то відмінності свідчитимуть про факт та локалізацію динамічних процесів, інші супутні параметри.

У загальному випадку повідомлення, якими обмінюються компоненти ситуативного кластера, являють собою блоки інформації, складені з автентифікаційної та інформаційної складової. У процесі ідентифікації користувача модуль-приймач порівнює автентифікаційні дані повідомлення, отриманого від модуля-передавача, з даними, які зберігаються в доступній у межах комунікаційного кластера базі даних. Після встановлення достовірності автентифікатора, необхідно перевірити відсутність фальсифікацій у інформаційній частині надісланого повідомлення, а в разі їхнього виявлення – виконати відновлення дійсної інформації.

Аналіз змісту інформаційної частини повідомлення також частково або повністю може бути виконаний криптографічними методами. Оскільки окремим випадком такого аналізу може бути встановлення факту та області локалізації зміни у блоці даних, необхідною є розробка методів, які дозволяють виявити декілька змін у окремому блоці інформації та встановити їх координати з метою ідентифікації та формування відповіді. Нами для аналізу спільно використовуваних інформаційних ресурсів були запропоновані методи, які поєднують принципи організації парольної автентифікації та ідентифікації з методами хешування. Було розроблено методи виявлення однократних та багатократних помилок у блоках інформації, а також метод виявлення областей локалізації таких помилок та відновлення цілісності первинних повідомлень. Зважаючи на однотипність задач виявлення фальсифікацій у кожній зі складових повідомлення, вони розглядалися як блоки даних.

Для виявлення однократних помилок у повідомленні запропоновано метод, базований на обчисленні хеш-функції. Застосування алгоритмів хешування з такою метою є відомою практикою. Однак, у загальному випадку, обчислення та подальший аналіз хеш-функції повністю всього інформаційного повідомлення

дозволяє перевірити його достовірність, але не дає можливості виявити, в яких саме фрагментах інформації відбулися порушення цілісності. Тому запропонований метод виявлення фальсифікацій передбачає обчислення хеш-функції в кожному блоці чи навіть в кожному записі надісланого повідомлення. Обчислення хеш-функцій для кожного запису в блоці інформації дозволяє визначити запис, в якому відбулися зміни, але його недоліком є висока надлишковість при контролі цілісності послідовності записів невеликого розміру. Для схеми обрахунку, яка передбачає обчислення хеш-функції для блоку даних, характерна невисока надлишковість, проте суттєвим недоліком є неможливості виявлення фальсифікацій в окремому записі.

Оскільки розглянуті методи хешування з метою виявлення фальсифікацій у повідомленні виявилися функціонально неповними стосовно задачі локалізації пошкоджень інформації, було запропоновано новий метод, який отримав назву методу перехресного хешування. Суть запропонованого методу полягає в обчисленні хеш-функції повідомлення для блоку даних за схемою, яка поєднує хешування для блоку даних як у горизонтальному, так і у вертикальному напрямах. Це дає змогу, застосовуючи перевірку значень хеш-функції за предикатом, виявити порушення цілісності в горизонтальному та вертикальному блоці [2]. Визначивши рядок (горизонтальний блок даних) та стовпець (вертикальний блок даних), у яких відбулися зміни, на їх перетині можна виявити фальсифікований фрагмент повідомлення.

При виявленні порушень цілісності повідомлення воно розбивається на блоки інформації, для кожного з них обчислюється значення хеш-функції за аналогією з обчисленням хеш-функції всього повідомлення. Далі необхідно перевірити достовірність їхніх значень за предикатом. Порушення цілісності повідомлення визначається за зміною значень хеш-функцій окремих блоків інформації. Цей метод дозволяє виявляти однократні помилки у повідомленнях.

Для виявлення та виправлення багатократних помилок використано коригуючі можливості кодів Гемінга [3]. Проте для криптографічних цілей здатність коду Гемінга виявити двократну помилку та виправити однократну помилку в двійковому коді є недостатньою. Тому доречною є побудова кодів, які дозволяють виявити більшу кількість помилок, шляхом введення надлишкової інформації. Оцінка коригуючої можливості таких кодів може бути виконана за допомогою параметрів «кодова відстань» та «мінімальна кодова відстань». Гемінгом було показано їх залежність від довжини коду та введеної надлишковості [4].

Код Гемінга в загальному вигляді може бути заданий породжуючою матрицею, яка складається з одиничної матриці $k \times k$ та приписаної матриці перевірочних елементів $k \times r$. Тут k – кількість рядків породжуючої матриці, r – кількість стовпців породжуючої матриці. Величини k і r мають задовольняти двом умовам: по-перше, отримання породжуючої матриці максимально малого розміру та, по-друге, забезпечення мінімальної кодової відстані, необхідної для виявлення заданої кількості помилок. Для визначення значень перевірочних елементів матриці необхідно виходити з основних властивостей коригуючих кодів.

Крім принципів надлишкового кодування, іншою складовою метода гарантованого виявлення фальсифікацій є методи хешування, які забезпечують відносно невисоку надлишковість, невелику кількість криптографічних перетворень та можливість контролювати довжину хеш-коду. Для контролю цілісності інформації використовується поняття «синдром» з теорії лінійних кодів як сукупність ознак, характерних та достатніх для розпізнавання помилок. Отриманий метод має потенціал забезпечення гарантованого виправлення помилок будь-якої кратності.

Таким чином, застосування технології хешування забезпечує як швидку автентифікацію в багатоагентному середовищі, так і можливість швидкого аналізу структури та змісту надісланих повідомлень. Запропоновані методи забезпечують виявлення однократних і багатократних помилок та гарантоване виправлення заданої кількості фальсифікованих фрагментів у повідомленні шляхом введення контрольних блоків інформації та виконання перехресного хешування. Розроблені методи можуть стати одним з кроків на шляху досягнення належного рівня достовірності інформації у комунікаційній системі та підвищення довіри у співробітництві або співпраці людей та роботів.

Литература

1.Kolbeinsson A., Lagerstedt E., Lindblom J. Foundation for a classification of collaboration levels for human-robot cooperation in manufacturing // Production & Manufacturing Research, vol. 7, no. 1, 2019. – P. 448-471.

2.Розломій І.О., Косенюк Г.В. Виявлення порушень цілісності електронного документу шляхом перехресного хешування // Вісник ХНУ. Радіотехніка, електроніка та телекомунікації. 2018. №5 (265). – С. 32–35.

3.Cao Z., Yin Zh., Hu H., Gao X., Wang L. High capacity data hiding scheme based on (7, 4) Hamming code // Springerplus, vol. 5, 2016. – P.175.

4.Ma Z., Li F., Zhang X. Data hiding in halftone images based on hamming code and slave pixels // J Shanghai Univ (Nat Sci), vol. 19, no. 2. 2013. – P. 111–115.