УДК 681.511:3

МЕТОД ПРИХОВУВАННЯ ДАНИХ В IP ПАКЕТАХ НА ОСНОВІ ПЕРІОДИЧНОЇ ЗАМІНИ СИГНАТУР

Ралець Д.Р.
Західноукраїнський національний університет
магістрант

I. Вступ

Задача стегоаналізу полягає в виявленні факту інкапсуляції візуально непомітного стеговідомлення або цифрового водяного знака у цифровий контент (зображення, відео, звуковий сигнал і т.п.) та оцінці параметрів вбудованого повідомлення.

Зазвичай в якості моделі стеганографічно прихованої інформації розглядається псевдовипадкова двійкова послідовність. Задачу стегоаналізу можна вирішувати як пряму, де контейнер аналізується з невідомим вмістом, так і як зворотню задачу оцінки прихованості алгоритмів комп'ютерної стеганографії.

Протягом останніх років розвиток стегоаналізу йшов у напрямку використання методів та алгоритмів машинного навчання як універсального та ефективного підходу до розв'язання будь-яких завдань аналізу даних.

Різноманіття використовуваних рішень дуже велике, що потребує систематизованого аналізу відомих результатів в порівнянні з новітніми рішеннями для визначення перспективних напрямків досліджень і розробок. Одним із таких напрямків є використання стеганографії у пакетах протоколів комунікаційних мереж.

II. Мета роботи

Метою даної роботи є розробка методу приховування даних в IP пакетах на основі періодичної заміни сигнатур.

III. Метод приховування даних в IP пакетах на основі періодичної заміни сигнатур

Мережевий канал прихованої передачі даних можна організувати на основі інкапсуляції конфіденційної інформації у поля IP-пакетів.

Основні можливості для приховування даних з використанням IP- пакетів:

- постійні дані: ID пакету, протокол передачі;
- періодично повторювані послідовності символів;
- зарезервовані поля, заповнені нульовими значеннями.

Аналіз розподілу довжин IP пакетів показав, що найбільш часто зустрічаються пакети довжиною: 63, 126, 189 байт - 95% від загального числа пакетів, тому інкапсульовувати конфіденційні дані в пакети іншої довжини недоцільно.

На основі аналізу вимог стандарту H.323, який визначає, що для досягнення середньої якості (MOS 3,5-4.0) передачі мовних сигналів затримка не повинна перевищувати 350 мс, був розроблений метод приховування даних в IP пакетах на основі періодичної заміни сигнатур. Запропонований метод включає кілька етапів, що дозволяють ефективно і безпечно вбудовувати інформацію в мережевий трафік IP-телефонії.

На початкових етапах визначається середня затримка передачі пакету між абонентами, порівнюється з максимально допустимою затримкою та визначається кількість пакетів, яку можна передати, не погіршуючи якість мовного сигналу. Після аналізу IP-пакетів вибираються пакети з довжиною 63, 126, 189 байти. Далі конфіденційна інформація інкапсульовується в ці пакети, здійснюється пошук заданої послідовності символів, таємне повідомлення приховується шляхом заміни сигнатур на маркери із символами секретного повідомлення. Крім того, стегокодер маркує резервні поля пакетів для подальшого розпізнавання таємного повідомлення стегодекодером. Останній етап включає передачу пакетів від абонента А до абонента В.

Блок-схема алгоритму запропонованого методу наведена на рисунку 1.

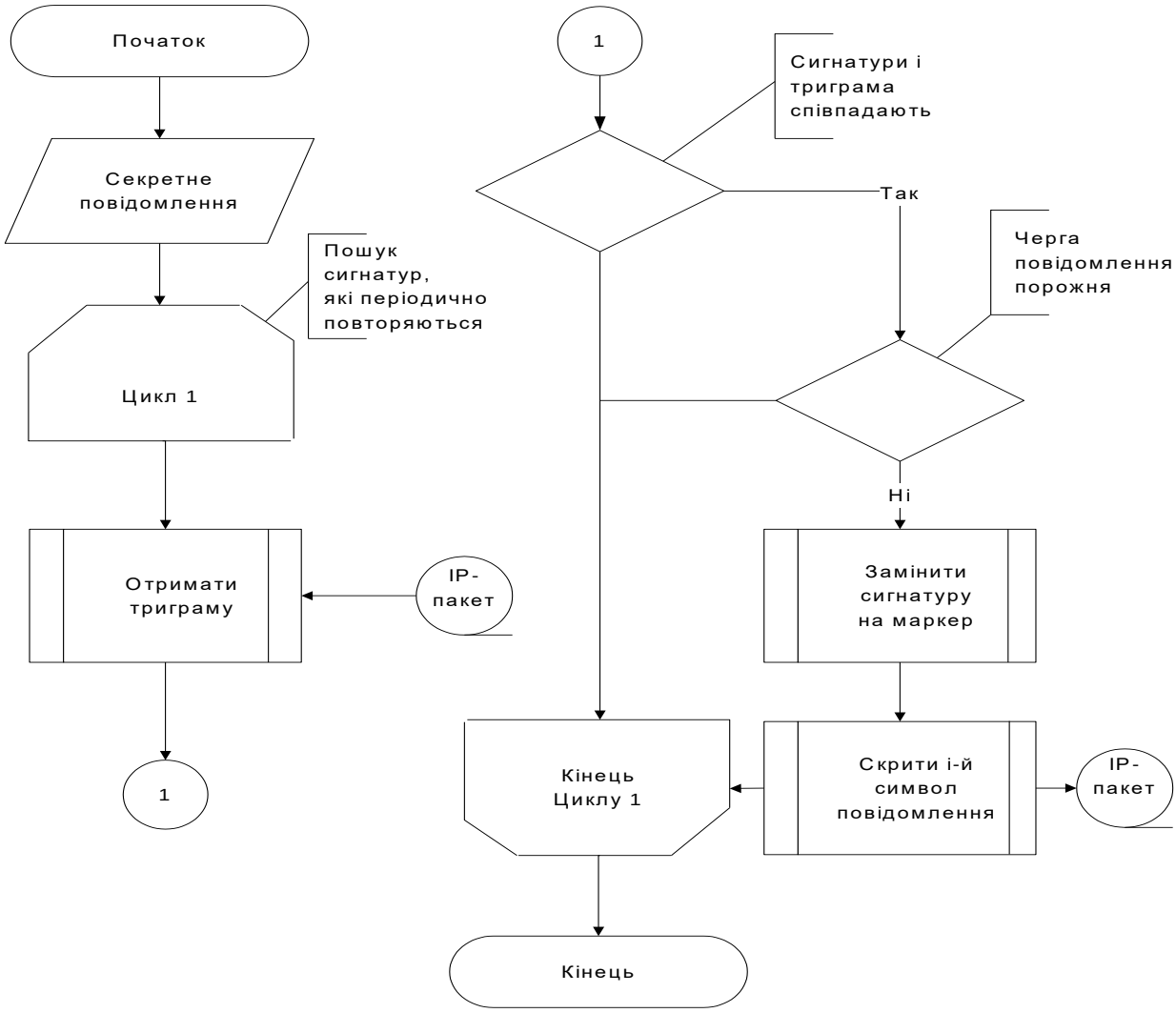

Рисунок 1- Блок-схема алгоритму приховування даних в IP пакетах на основі періодичної заміни сигнатур

Висновок

У роботі запропоновано метод приховування даних в IP пакетах, що базується на періодичній заміні сигнатур. Основними етапами методу є оцінкамережевої затримки, порівняння її з максимально допустимою, визначення кількості пакетів для передачі та етапи аналізу та модифікації IP-пакетів.

Запропонований метод дозволяє ефективно та безпечно вбудовувати інформацію в мережевий трафік IP-телефонії, використовуючи періодичну заміну сигнатур. Практична реалізація методу передбачає використання вибраних довжин IP-пакетів та пошук заданої послідовності символів для виявлення вбудованого повідомлення. Наведено у роботі блок-схема алгоритму надає зрозумілий візуальний огляд запропонованого методу.

Список використаних джерел

1. Naidu, T.R.K.; Kumar, G.P.; Prasad, T.G. Overview of digital audio steganography techniques. Int. J. Emerg. Technol. Eng. 2016, 3, 62–66.
2. Hussain, M.; Wahab, A.W.A.; Javed, N.; Jung, K.H. Hybrid Data Hiding Scheme Using Right-Most Digit Replacement and Adaptive Least Significant Bit for Digital Images. Symmetry 2016, 8, 41.
3. Liu, X.; Tian, H.; Liu, J.; Lu, J. IP voice steganography and steganalysis analysis. J. Chongqing Univ. Posts Telecommun. 2019, 31, 407–419.
4. Deng, S.; Liu, J.; Zhang, W. Scenario of quantitative evaluation for steganalytic algorithms. J. Southeast Univ. 2007, 76–80.
5. Anguraj, S.; Shantharajah, S.; Emilyn, J.J. A steganographic method based on optimized audio embedding technique for secure data communication in the internet of things. Comput. Intell. 2020, 36, 557–573.
6. O. Kovalchuk, M. Karpinski, S. Banakh, M. Kasianchuk, R. Shevchuk and N. Zagorodna, "Prediction Machine Learning Models on Propensity Convicts to Criminal Recidivism", Information, vol. 14, no. 3, pp. 161, 2023.
7. O. Kovalchuk, M. Kasianchuk, M. Karpinskiand R. Shevchuk, "Decision-Making Supporting Models Concerning the Internal Security of the State", INTL Journal of Electronics Telecommunications, vol. 69, no. 2, pp. 301-307, 2023.