УДК 621.396.1

ДОСЛІДЖЕННЯ МЕТОДІВ МОНІТОРИНГУ ТРАФІКУ ДЛЯ ПРОТИДІЇ ФРОДУ В IP-ТЕЛЕФОНІЇ

Карпишин Н.Я., Кравчук С.О.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: nazar.karpishin@gmail.com

RESEARCH OF TRAFFIC MONITORING METHODS TO ANTI-FRAUD IN IP-TELEPHONY

Currently, IP telephony technology has become quite widespread, as it provides many advantages of using Internet protocols for voice transmission compared to traditional circuit-switched systems.

На даний час технологія IP-телефонії набула досить велике поширення, оскільки вона надає багато переваг застосування Інтернет-протоколів для передачі голосу порівняно з традиційними системами з комутацією каналів.

Рис. 1. Залежність прогнозу збільшення капіталу VOIP ринку від часу, в роках (Джерело: ZionResearchAnalysis 2016 р.)

Зростання частки IP-телефонії з роками демонструє рис. 1, де наведено зростання капіталу ринку технології передачі медіа-даних у реальному часі за допомогою сімейства протоколів TCP/IP (VoIP, голос через IP (voice over IP).

Технологія 5G (П’яте покоління мобільних мереж) може відіграти важливу роль у розвитку Voice over Internet Protocol (VoIP), тобто телефонії через Інтернет.

5G має значно більшу пропускну здатність та швидкість передачі даних порівняно з попередніми версіями мобільних мереж, що може забезпечити високоякісну передачу голосу в реальному часі з мінімальним затримкою. Це може бути особливо корисно для VoIP, де якість зв'язку має велике значення.

Завдяки 5G мережі, користувачі VoIP можуть відчувати більш стабільне та

якісне з'єднання, яке забезпечує більшу якість передачі голосу та зменшення затримки. Крім того, зв'язок через 5G мережу може бути більш безпечним та захищеним, що дозволяє користувачам відчувати себе більш упевненими у тому, що їхні особисті дані захищені.

Стрімкий ріст цікавості до технологій штучного інтелекту не був проігнорований і в сфері VOIP. Штучний інтелект та машинне навчання вже можуть розпізнавати мову та аналізувати дані дзвінків. І з розвитком цієї галузі очікується автоматична відправка кореспонденції та доставка. Крім того, штучний інтелект зможе виявляти та реагувати на помилки та несправності.

Також розвиток штучного інтелекту може суттєво допомогти в протидії шахрайству в IP телефонії. Серед варіантів - моніторинг трафіку. Завдяки машинному навчанню, система може навчитись розпізнавати ненормальні патерни в трафіку, що можуть свідчити про спроби шахрайства. Наприклад, якщо виявлено, що дзвінки з одного номера здійснюються до багатьох різних номерів одночасно, це може свідчити про автоматизований шахрайський процес.

ШІ може використовуватись для автоматичного виявлення підозрілих транзакцій та підозрілих дзвінків на основі аналізу поведінки користувачів, історії транзакцій та інших факторів. Таким чином, штучний інтелект може допомогти виявляти шахраїв, які використовують телефонні мережі для здійснення шахрайства та інших злочинних дій. Крім того, штучний інтелект може допомогти вдосконалити систему авторизації та ідентифікації користувачів, забезпечуючи високий рівень безпеки та захисту від несанкціонованого доступу до системи. Він також може допомогти управляти ризиками та покращити ефективність боротьби з фродом у мережі IP телефонії.

В цілому, застосування штучного інтелекту в моніторингу трафіку для протидії фроду в IP телефонії може допомогти забезпечити високий рівень безпеки та ефективності мережі, зменшити ризики від шахраїв та інших злочинців, а також підвищити рівень задоволення користувачів.

Мета роботи полягає в тому, щоб шляхом дослідження доступних методів моніторингу трафіку розробити нові та/або удосконалити наявні, для оптимізації протидії шахрайству в IP телефонії. Це дозволить зменшити фінансові та репутаційні ризики, як для компаній провайдерів, так і для їх клієнтів.

Фрод (англ. fraud) - це шахрайство або обман, який зазвичай виконується з метою отримання незаконної вигоди, часто фінансової. Фрод в IP-телефонії є серйозною проблемою в сучасному світі. IP-телефонія, як технологія передачі голосу через Інтернет, стала дуже популярною в останні роки, із зростанням популярності вона стала більш вразлива на шахрайство.В свою чергу можна виділити деякі з найпоширеніших видів порушень: tollfraud , рефайл, злом провайдерського або клієнтського обладнання. (АТС, IPPBX).

Серед найбільш дієвих методів протидії фроду слід виділити моніторинг трафіку в мережі, який дозволяє ефективно протидіяти порушенням. Також слід виділити саме методи моніторингу трафіку серед яких:

1. Packet Sniffing: цей метод забезпечує збір даних, які передаються через

мережу IP телефонії. Цей метод можна виконати за допомогою програмного забезпечення, такого як Wireshark, і дозволяє перевіряти вміст кожного пакету.

2. Deep Packet Inspection (DPI): цей метод забезпечує збір додаткових даних з кожного пакету, таких як IP-адреси та номери телефонів. DPI дозволяє здійснювати детальний аналіз трафіку, виявляти шкідливі програми та виявляти аномальну активність.

3. NetFlow Analysis: цей метод дозволяє збирати дані про трафік та аналізувати його. Інформація про трафік, що передається через IP телефонію, записується в форматі NetFlow та може бути аналізована, щоб виявити аномальну активність.

4. Call Detail Record (CDR) Analysis: цей метод забезпечує збір даних про кожен телефонний дзвінок, включаючи час дзвінка, тривалість та номери, що беруть участь. Ці дані можуть бути аналізовані для виявлення незвичайної активності та шахрайства.

5. Real-time Monitoring: цей метод забезпечує моніторинг мережі IP телефонії в режимі реального часу. Це дозволяє виявляти проблеми в мережі та шкідливі дії в момент їх виникнення.

Комбінування різних методів моніторингу трафіку, таких як аналіз поведінки користувачів, виявлення аномального трафіку та використання сигнатур для ідентифікації фроду, дозволяє створити більш комплексну систему захисту від шахрайства в ip-телефонії.

Така комбінація методів моніторингу трафіку дозволяє збільшити точність виявлення фроду та знизити кількість помилкових спрацювань системи захисту. Наприклад, виявлення аномального трафіку може доповнюватись аналізом поведінки користувачів, що дозволить виявляти зловмисну діяльність на основі характеристик використовуваного трафіку та взаємодії з мережею.

Крім того, використання сигнатур для ідентифікації фроду допомагає виявляти вже відомі методи атак, тоді як аналіз поведінки користувачів та виявлення аномального трафіку дозволяють виявляти нові та невідомі методи атак.

Таким чином, комбінація різних методів моніторингу трафіку є дієвим інструментом для захисту від фроду в ip-телефонії, що забезпечує більш точний та комплексний аналіз трафіку та дозволяє виявляти як відомі, так і нові методи атак.

Література

1. https://financesonline.com/voip-software-statistics
2. https://cfca.org/
3. https://cfca.org/wp-content/uploads/2021/12/CFCA-Fraud-Loss-Survey-2021-2.pdf
4. https://www.vyopta.com/blog/business-collaboration/telecommunications-security-vulnerabilties/
5. https://www.allot.com/resources/Covid-19-Impact-Asia.pdf
6. https://www.ringcentral.com/us/en/blog/the-growing-popularity-of-voip-and-emerging-trends-in-the-market/
7. https://www.statista.com/statistics/691602/global-mobile-voip-market-size-by-region/
8. https://www.acrobits.net/blog/5g/5g-voip-global-standard/