Метод обеспечения анонимности в сетях с использованием сетевого кодирования

Сергеев Михаил Алексеевич S.MementoMori@gmail.com
Московский Физико Технический Институт

Введение. В этой статье мы рассмотрим схему, позволяющую обеспечить анонимности в сети с использованием сетевого кодирования. В качестве основы взят известный метод COPE, который обычно используется для повышения эффективности передачи данных. Данный метод был подвергнут модификации для достижения анонимности контрагентов при передаче сообщений.

1 Введение

Основным отличием беспроводных сетей от проводных является то, что среда передачи данных совершенна открыта любому желающему, поэтому заинтересованному злоумышленнику ничего не стоит получать необходимую информацию, получив доступ к среде. Для обеспечения безопасности передачи было придумано много подходов. Одним из самых известных сейчас, например, является протокол WPA2, позволяющий не допускать злоумышленника в Wi-Fi сеть путём создания секретного пароля и распространением его между легитимными пользователями сети. Однако в случае, когда злоумышленник завладел этим секретным ключом, безопасность передачи остаётся под угрозой. Далее будем рассматривать более узкую задачу - не секретность передачи информации в целом, а лишь обеспечение анонимности передачи.

Существует несколько задач, объединяемых общим названием «обеспечением анонимности», среди них выделяют: [**?**]

- Обеспечение анонимности отправителя и получателя
- Сокрытие маршрута передачи
- Сокрытие факта передачи

Мы сосредоточимся на первом типе задач. Для этого рассмотрим метод COPE, основной частью которого является разбиение передаваемого пакета на части и передача его по частям через промежуточные узлы. Таким образом достигается более плотное использование полосы пропускания. Однако мы можем воспользоваться этим подходом, сделав недоступной одну из частей пакета никому, кроме адресата. В этом случае сторонний наблюдатель (в том числе и злоумышленник) не сможет получить доступ к полному пакету, а значит, и к указанию на то, кому предназначался пакет.

Дальше в статье мы сначала рассмотрим механизм работы оригинального COPE, а затем познакомимся с предлагаемыми изменениями.

2 Общие слова о COPE

По своей сути, COPE является архитектурой, в рамках которой, во-первых, передаваемые пакеты разделяются на части, а во-вторых, каждая часть передаётся независимо. Для этого используется три механизма [**?**]:

- **Opportunistic Listening**, сохраняющий все принятые пакеты в специальный буфер,
- **Opportunistic Coding**, объединяющий разные пакеты одного сообщения в линейную комбинацию и передающий её широковещательно для повышения эффективности использования пропускной способности,
- **Learning Neighbour State**, позволяющий использовать предыдущий пункт - механизм определения списка частей пакетов, уже сохранённых на соседних узлах, чтобы иметь возможность передавать им только недостающие части.

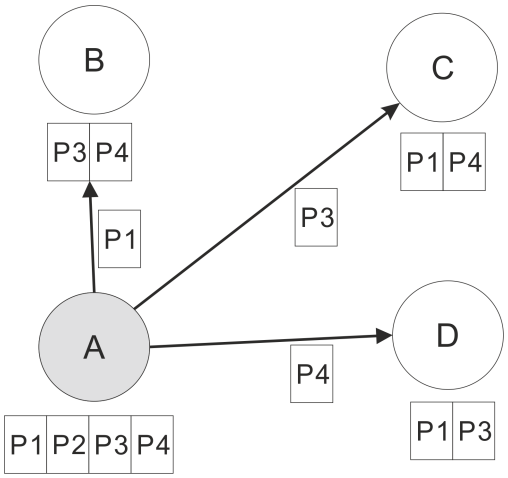

Рис. 1: Иллюстрация передачи пакетов по методу COPE

Для лучшего понимания рассмотрим пример, изображенный на Figure 1. Допустим, что узел A имеет в буфере сообщение **P**, разбитое на четыре пакета - $P1$, $P2$, $P3$ и $P4$, при этом $P1 \oplus P2 \oplus P3 \oplus P4 = \mathbf{P}$. Посредством

механизма LNS он узнаёт, какие пакеты есть на соседних узлах (содержимое буфера указано рядом с каждым узлом). После этого он решает послать пакет $P1$ узлу B, пакеты $P2$ и $P3$ - узлу C, а пакет $P4$ - узлу D. В этом случае у него есть несколько вариантов линейной комбинации пакетов, часть из которых приводят к более эффективным вариантам передачи, часть - к менее эффективным. В частности, если передать комбинацию пакетов $P1$ и $P2$, узел C сможет принять свой пакет $P2$, однако у B будет недостаточно данных для того, чтобы выделить $P1$ из комбинации. Если же передать комбинацию $P1 \oplus P3 \oplus P4$, все три узла смогут выделить предназначенное им сообщение из передачи. В дальнейшем, узел C может передать пакет $P2$ узлам D и B. Формальный признак Opportunistic Coding звучит как [?]

> Для передачи n пакетов, $p_1, ..., p_n$, n узлам, $r_1, ..., r_n$, отправитель может сложить по модулю 2 эти n пакетов в том случае, если любой узел r_i владеет $n-1$ пакетами p_j, где $j \neq i$.

3 Предлагаемые изменения

Рассмотрев структуру COPE, мы можем перейти к изменениям, которые предлагается внести, чтобы реализовать обеспечение анонимности первого типа. Для этого обратимся к центральной части этого подхода - к разбиению сообщения на части и составлению линейных комбинаций. Понятно, что при разбиении сообщения на n частей, узел должен получить не менее n независимых линейных комбинаций, чтобы иметь возможность принять исходное сообщение. Предлагаемая идея состоит в том, чтобы, разбив сообщение на n частей, не использовать одну из них(допустим, первую) при составлении линейных комбинаций. В этом случае в сети будут передаваться пакеты, перехватив которые, злоумышленник не сможет получить исходный пакет, в котором указан адрес получателя.

Для того, чтобы получатель смог получить и прочитать исходное сообщение, исключаемый пакет выбирается не случайным образом, а создаётся по определённому алгоритму. Для этого у всех узлов существует общая односторонняя функция $F(addr_s, addr_d, counter)$, которая позволяет создать пакет фиксированной длины в зависимости от адреса отправителя, адреса получателя и некоторого счётчика. Примером такой функции может служить функция нахождения MD5 хэша от достаточно большого файла, к которому приписаны указанные выше параметры функции. Также возможно использование proof-of-work алгоритмов [?].

Узел-отправитель составляет секретный пакет, а использованное значение счётчика помещает в заголовок пакетов.

При получении сообщения узел-приёмник сохраняет принятые комбинации пакетов в буфер и, как только понимает, что линейных комбинаций достаточно и не хватает только исключённого пакета, производит ту же опе-

рацию, получая секретный пакет, с помощью которого может восстановить исходное сообщение.

Злоумышленник же, в свою очередь, не зная адреса получателя, не может воспользоваться этой функцией для восстановления исходного сообщения.

4 Альтернативный подход

Рассмотрим также случай, когда сообщение $\mathbf{P}$ можно представить в виде вектора в F_p^n. Представим сообщение в виде транспонированной матрицы в F_p

$$P = \begin{bmatrix} p_1^1 & p_2^1 & \cdots & p_k^1 \\ \vdots & \vdots & \ddots & \vdots \\ p_1^n & p_2^n & \cdots & p_k^n \end{bmatrix}$$

В качестве сообщений при этом будем использовать p_i, сформированый следующим образом. ($p_0 = \varphi(\cdot)$)

$$p_i^T = \begin{bmatrix} p_i^1 & \cdots & p_i^i + p_0^i & \cdots & p_i^n \end{bmatrix}$$

При этом $\varphi(\cdot)$ строится следующим образом - отправитель берёт адрес получателя, дополняет его случайным зерном и кодирует кодом Рида-Соломона. Затем в полученный вектор вносятся ошибки и результат используется в качестве секретного пакета.

Получатель при получении n столбцов матрицы, может, зная свой адрес, декодировать секретный пакет и восстановить исходное сообщение. А поскольку злоумышленник не знает адреса, попытки декодирования будут провалены из-за вставленных ошибок, из-за чего ему потребуется делать полный перебор всех возможных вариантов адреса.

5 Заключение

Был рассмотрен метод, позволяющий обеспечить анонимность получателя в открытой беспроводной сети со множественным доступом.

Список литературы

[1] Katti Sachin, et al. *XORs in the air: practical wireless network coding,* IEEE/ACM Transactions on Networking (TON), 16.3 (2008): 497-510

[2] Zhu Xiaoyan et al. *A batched network coding scheme for wireless networks,* Wireless Networks, 15.8 (2009): 1152-1164.

[3] Coelho Fabien *Exponential Memory-Bound Functions for Proof of Work Protocols,* IACR Cryptology ePrint Archive 2005 (2005): 356.

[4] Kang Ruogu Stephanie Brown and Sara Kiesler. *Why do people seek anonymity on the internet?: informing policy and design.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2013.