Independent Submission
Request for Comments: 9564
Category: Informational
ISSN: 2070-1721

M. Blanchet
Viagenie

1 April 2024

Faster Than Light Speed Protocol (FLIP)

Протокол FLIP

Аннотация

Последние достижения в сфере искусственного интеллекта (artificial intelligence или AI), такие как большие языковые модели позволяют разработать для Internet протокол, работающий быстрее скорости света (Faster than LIght speed Protocol или FLIP). FLIP позволяет избежать перегрузок, повысить безопасность и ускорить доставку пакетов в Internet с использованием AI для предсказания будущих пакетов на приёмной стороне до их прибытия. Документ описывает протокол, его различные инкапсуляции и некоторые эксплуатационные соображения.

Оглавление

1. Введение

Представление ChatGPT широкой публике состоялось 30 ноября 2022 г. [CHATGPT]. С тех пор большие языковые модели (large language model или LLM) используются в самых разных приложениях. Они демонстрируют мощные способности генерировать точные результаты на основе входных данных и соответствующего обучения LLM. Данная спецификация протокола использует эту способность для предсказания будущих рпкетов до их прибытия к принимающему партнёру, что позволяет достичь скорости доставки, превышающей световую, поэтому протокол получи название «Быстрее скорости света» (Faster than LIght speed Protocol или FLIP).

Поскольку FLIP может предсказывать пакеты, кадры или потоки байтов, он может применяться на любом уровне стека протоколов IP. Более того, при должном обучении FLIP может также предсказывать будущие шифрованные пакеты, поскольку шифрование - это просто строки байтов. Данная спецификация показывает FLIP как промежуточный (shim) заголовок канального (L2) и транспортного уровня. Поскольку FLIP можно применять на любом уровне, предполагается разработка дополнительных спецификаций, таких как предсказание запросов и откликов HTTP, содержимого электронной почты и т. д.

Поскольку скорость связи в дальнем космосе, к сожалению, ограничена скоростью света, а расстояния между космическими аппаратами и Землёй очень велики, возникают очень большие задержки при связи. Обеспечивая доставку быстрее скорости света (faster-than-light-speed), FLIP является ключевым дополнением для сетей IP в дальнем космосе [IP-DEEP-SPACE].

2. Подготовка партнёров по протоколу

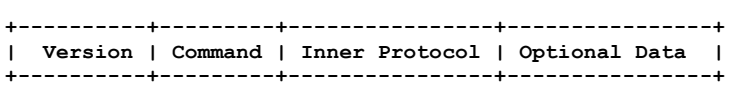
Для успешного достижения скорости, превышающей световую, партнёры на любом протокольном уровне, используемом FLIP, должны подготовить свою сторону соединения с помощью правильной модели, обученной для конкретного случая. Этот документ не задаёт конкретную LLM, поскольку реализации могут самостоятельно выбрать

наиболее подходящую для них модель и обучить её должным образом. Как и с любой LLM, очень важно использовать большой объем обучающих данных, таких как собранные пакеты, в разных условиях для получения хорошо обученной модели. Во избежание проблем с безопасностью, приватностью и правовыми вопросами специфика применяемой LLM, способы обучения и используемые при этом данные не следует публиковать или раскрывать в протоколе.

Например, реализация может взять большое число файлов с собранными пакетами (Packet Capture или PCAP) от tcpdump в разных точках Internet. То, что трафик может оказаться зашифрованным, не имеет значения, поскольку хорошо обученная LLM способна предсказать зашифрованных трафик так же хорошо, как открытый.

3. Заголовок FLIP

При любом использовании FLIP (выше или ниже IP или иного транспорта, а также на любом прикладном уровне) внедряется промежуточный заголовок FLIP, показанный ниже.



Version - версия

Это поле переменного и незаданного размера содержит хэш-значение SHA-256 для модели, используемое в качестве версии, как описано в разделе 5.

Command - команда

Код (codepoint), указывающий операцию данного кадра FLIP. Команды описаны в разделе 4, а исходный список действительных команд FLIP приведён в таблице 1.

Размер списка возможных команд не ограничен, поскольку партнёры с искусственным интеллектом могут поддерживать бесконечное число команд, просто обновляя свои модели без необходимости обновлять реализацию протокола.

Таблица 1.

Команда	***Код***	***Документ***
model	0x01	RFC 9564
data	0x02	RFC 9564

Inner Protocol - внутренний протокол

Поскольку заголовок FLIP является промежуточным (shim), в этом поле указывается внутренний (вложенный) протокол. Например, промежуточный заголовок FLIP может помещаться между заголовками IP и TCP, а пакет IP будет содержать код FLIP в качестве транспортного протокола. Тогда поле внутреннего протокола FLIP будет содержать код TCP, который иначе размещался бы в заголовке пакета IP.

Optional Data - необязательные данные

Некоторые команды имеют дополнительные данные, размещаемые вслед за полем Command.

Размер заголовка является переменным и зависит от используемой команды. С учётом применения искусственного интеллекта в реализации этого протокола, фактический размер заголовка и каждого из его полей не указывается в заголовке. Вместо этого предполагается, что соответствующая нейронная сеть на стороне получателя способна найти фактическое завершение заголовка, что позволяет сэкономить занимаемые заголовком биты.

Для подобающей сигнализации вышележащему уровню о наличии заголовка FLIP резервируется определённый код (codepoint) на уровне ниже FLIP. В разделе 7 указаны такие регистрации для IP и транспортных кодов.

4. Работа протокола

Перед отправкой первого пакета с использованием FLIP отправителю и получателю следует настроить подходящую модель, как отмечено выше. Выбор подобающей LLM и набора данных для обучения остаётся за реализацией.

Команды протокола описаны ниже.

Model (codepoint 0x01) - модель

Эта команда предоставляет партнёрам возможность передать свою модель по основному каналу (in-band) протокола FLIP. Сама модель передаётся в поле Optional Data заголовка FLIP. Перед фактическими данными модели помещается заголовок MIME с подходящим типом носителя. Если типа носителя для модели не существует, его следует зарегистрировать в реестре IANA Media Type.

Data (codepoint 0x02) - данные

Эта команда говорит принимающему партнёру, что следующие за ней данные могут быть предсказаны, благодаря чему достигается производительность выше скорости света (faster-than-light-speed).

Передачу модели партнёру по основному каналу (in-band) следует выполнять редко, поскольку размер моделей может быть большим. Кроме того, такая передача фактически раскрывает модель для прослушивающего линии злоумышленника. Разработчики могут предусмотреть использование пост-квантового криптографического алгоритма, который устойчив к предсказаниям AI, т. е. постквантового криптографического алгоритма с искусственным интеллектом (post-Quantum-AI cryptographic algorithm).

5. Версия протокола

Как описано в [RFC6709], большинство протоколов должно разрабатываться с возможностью будущих улучшений, например, предоставляя способ указать новую версию протокола. В случае FLIP обученные модели всегда будут улучшаться в результате нового обучения. В качестве номера версии применяется хэш-значение SHA-256 [RFC6234] обученной модели, чтобы каждый партнёр знал используемую версию FLIP. Значение SHA-256 помещается в поле Version заголовка FLIP, как описано выше. С учётом того, что новые значения SHA-256 являются не последовательными, а полностью случайными, это предотвращает атаки с повторным использованием (replay) предсказаний будущего.

6. Продолжение работы

Этот новый протокол может революционизировать разработку протоколов Internet и пути использования Internet. Например, предполагается, что протокол можно будет использовать для потокового видео, дополненной и виртуальной

реальности, пост-квантовой криптографии и т. п. Предсказывая будущие пакеты, все эти протоколы и приложения смогут получить выгоду от использования FLIP.

7. Взаимодействие с IANA

Коды для FLIP могут регистрироваться в реестрах IANA:

- Protocol Numbers [IANA-PN]: 345, FLIP, Faster than LIght speed Protocol, RFC 9564;
- Service Name and Transport Protocol Port Number Registry [IANA-SN]: FLIP, 68534, udp and tcp, RFC 9564

8. Вопросы безопасности

Способность предсказывать будущие пакеты на основе LLM может использоваться злоумышленниками, прослушивающими трафик путём его перехвата. Если у них есть доступ к той же модели, которую использует целевой партнёр, можно предсказать следующие пакеты и начать различные атаки, включая такие новые атаки, как «воспроизведение будущего» (futureplay attack). По сравнению с типичными replay-атаками в этом случае злоумышленник может предсказать будущие пакеты и заранее отправить их получателю. Хотя сейчас это может показаться неочевидным, эти новые атаки следует изучить, пока они не стали проблемой. Поэтому предлагается продолжить исследования в этом направлении.

Способность партнёра предсказывать будущие пакеты повышает общий уровень безопасности Internet, поскольку злоумышленники не смогут внедря в соединения плохие пакеты, так как получатель всегда может сравнить принятый пакет с пресказанным и легко обнаружить и отвергнуть плохие пакеты.

9. Литература

[CHATGPT] Wikipedia, "ChatGPT", 20 March 2024, <https://en.wikipedia.org/w/index.php?title=ChatGPT&oldid=1214732037>.

[IANA-PN] IANA, "Protocol Numbers", <https://www.iana.org/assignments/protocol-numbers/>.

[IANA-SN] IANA, "Service Name and Transport Protocol Port Number Registry", <https://www.iana.org/assignments/service-names-port-numbers/>.

[IP-DEEP-SPACE] Blanchet, M., Huitema, C., and D. Bogdanović, "Revisiting the Use of the IP Protocol Stack in Deep Space: Assessment and Possible Solutions", Work in Progress, Internet-Draft, draft-many-deepspace-ip-assessment-01, 4 March 2024, <https://datatracker.ietf.org/doc/html/draft-many-deepspace-ip-assessment-01>.

[RFC6234] Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, DOI 10.17487/RFC6234, May 2011, <https://www.rfc-editor.org/info/rfc6234>.

[RFC6709] Carpenter, B., Aboba, B., Ed., and S. Cheshire, "Design Considerations for Protocol Extensions", RFC 6709, DOI 10.17487/RFC6709, September 2012, <https://www.rfc-editor.org/info/rfc6709>.

Благодарности

Поскольку в этой спецификации протокола применяется искусственный интеллект и большие языковые модели, было решено, что тупым людям недопустимо рецензировать эту спецификацию. Вместо этого спецификация была представлена нескольким чат-сервисам LLM и улучшена в соответствии с их комментариями и предложениями, что и отмечено здесь. Фактически эта спецификация могла быть полностью создана чат-службами LLM. Более того, с учётом того, что создаваемые IETF спецификации полагаются на человеческий интеллект, следует предусмотреть также возможность использования LLM для подготовки спецификаций. Наконец, учитывая трудности с подбором экспертов на руководящие позиции (например, в IESG или IAB), следует рассмотреть использование LLM для замещения этих позиций. К сожалению, из соображений приватности, безопасности и законодательства использованные для этой работы чат-службы LLM не могут быть названы здесь.

Адрес автора

Marc Blanchet
Viagenie
Email: marc.blanchet@viagenie.ca

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru