Internet Engineering Task Force (IETF)
Request for Comments: 7820
Category: Experimental
ISSN: 2070-1721

T. Mizrahi
Marvell

March 2016

UDP Checksum Complement in the One-Way Active Measurement Protocol (OWAMP) and Two-Way Active Measurement Protocol (TWAMP)

Дополнение контрольной суммы UDP в протоколах OWAMP и TWAMP

Аннотация

Протоколы одностороннего активного измерения задержки (One-Way Active Measurement Protocol или OWAMP) и двухстороннего активного измерения задержки (Two-Way Active Measurement Protocol или TWAMP) служат для мониторинга производительности в сетях IP. Измерение задержки в этих протоколах выполняется по тестовым пакетам с временными метками. В некоторых реализациях применяются аппаратные средства создания меток времени, встраивающие точное время передачи в каждый исходящий тестовый пакет OWAMP или TWAMP. Поскольку эти пакеты доставляются по протоколу UDP, поле Checksum обновляется с учётом вставки временной метки. Этот документ предлагает использовать 2 последних октета каждого тестового пакета как дополнение контрольной суммы (Checksum Complement), что позволяет средствам записи временных меток возможность отразить изменение контрольной суммы в этих 2 октетах, а не в поле UDP Checksum. Задаваемое этим документом поведение полностью совместимо с имеющимися реализациями OWAMP и TWAMP.

Статус документа

Документ не относится к категории Internet Standards Track и публикуется лишь для проверки, экспериментальной реализации и оценки.

Документ содержит экспериментальный протокол для сообщества Internet и является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 5741.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке http://www.rfc-editor.org/info/rfc7820.

Оглавление

[1] Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[2] Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

1. Введение

Протоколы OWAMP [OWAMP] и TWAMP [TWAMP] применяются для мониторинга производительности сетей IP.

Задержка и её вариации являются показателями, которые могут измерять OWAMP и TWAMP. Измерение выполняется с использованием временных меток в тестовых пакетах. В некоторых вариантах применения, таких как сети операторов, эти два показателя являются важной частью соглашений об уровне обслуживания (Service Level Agreement или SLA) и поэтому должны измеряться с высокой точностью. Если метки времени включаются в пакеты на аппаратном уровне при выходе пакета с хоста, это может существенно повысить точность по сравнению с метками времени от вышележащих уровней, как описано ниже.

Точность измерения задержки зависит от меток времени и их реализации. Для точной установки меток реализация может использовать аппаратный модуль временных меток (timestamping engine), как показано на рисунке 1. В таких случаях пакеты OWAMP/TWAMP передаются и принимаются на программном уровне, а аппаратный модуль меток меняет каждый исходящий пакет, встраивая точное время передачи в поле пакета Timestamp.

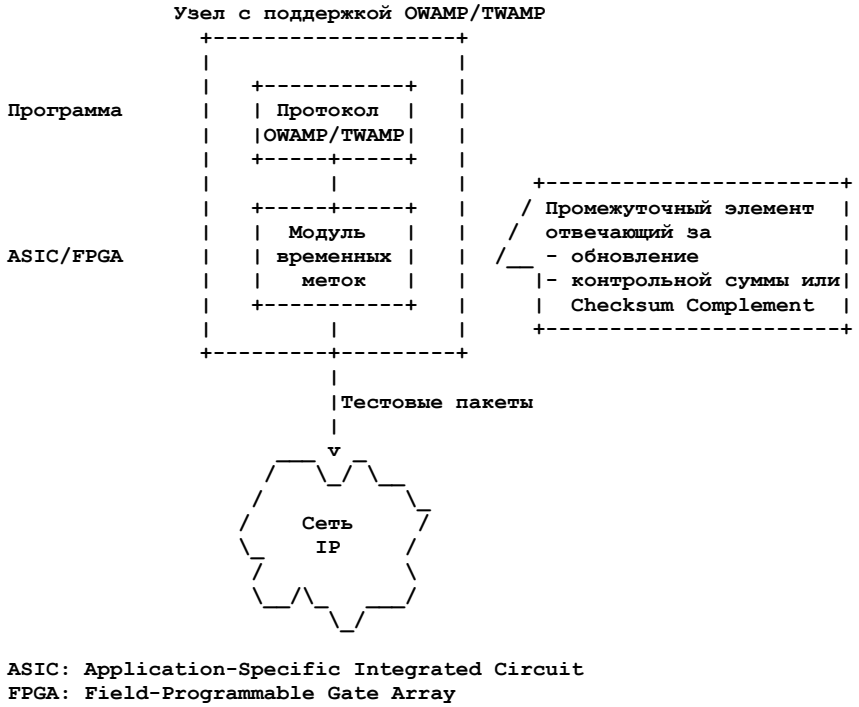

Рисунок 1. Точная установка временных меток в OWAMP и TWAMP.

Тестовые пакеты OWAMP/TWAMP передаются по протоколу UDP. Когда данные UDP (payload) изменяются промежуточным узлом, таким как модуль меток времени, поле UDP Checksum должно соответственно обновляться. При использовании UDP по протоколу IPv4 [UDP] у промежуточного узла, не способного обновить значение UDP Checksum не остаётся вариантов кроме установки значения 0 в поле Checksum, заставляющего получателя игнорировать поле Checksum и, возможно, принимать повреждённые пакеты. UDP по протоколу IPv6, как указано в [IPv6], не разрешает значение 0 для контрольной суммы за исключением особых случаев [ZeroChecksum]. Как отмечено в [ZeroChecksum], использование нулевой контрольной суммы в общем случае не рекомендуется и его следует избегать, когда это возможно.

Поскольку промежуточный элемент меняет лишь конкретное поле пакета (Timestamp), обновление UDP Checksum можно выполнить инкрементно с использованием концепций, представленных в [Checksum].

Аналогичная задача рассматривается в Приложении E к [IEEE1588]. При работе протокола точного времени (Precision Time Protocol или PTP) по протоколу IPv6 добавляются 2 октета в конец данных PTP для обновления UDP Checksum. Значение этих 2 октетов может обновляться промежуточным узлом для сохранения корректности поля UDP Checksum.

Этот документ задаёт похожий подход для протоколов [OWAMP] и [TWAMP], позволяющий промежуточным элементам обновлять тестовые пакеты OWAMP/TWAMP и поддерживать корректность UDP Checksum путём изменения двух последних октетов в пакете.

Термин Checksum Complement (дополнение контрольной суммы) в этом документе относится к 2 октетам в конце данных UDP, используемым для обновления UDP Checksum промежуточными узлами.

Использование Checksum Complement позволяет в некоторых случаях упростить реализацию, поскольку при последовательной обработке данных пакета проще сначала обновить поле Timestamp, а затем - Checksum Complement вместо обновления временной метки и последующего обновления поля UDP Checksum в заголовке UDP.

Механизм Checksum Complement определён также для протокола сетевого времени (Network Time Protocol) в [RFC7821].

2. Используемые соглашения

2.1. Уровни требований

Ключевые слова **должно** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с [KEYWORDS].

2.2. Сокращения

HMAC
Hashed Message Authentication Code - хэшированный код проверки подлинности сообщения.

OWAMP
One-Way Active Measurement Protocol - односторонний протокол активных измерений.

PTP
Precision Time Protocol - протокол точного времени.

TWAMP
Two-Way Active Measurement Protocol - двухсторонний протокол активных измерений.

UDP
User Datagram Protocol - протокол пользовательских дейтаграмм.

3. Применение UDP Checksum Complement в OWAMP и TWAMP

3.1. Обзор

UDP Checksum Complement представляет собой 2-октетное поле, добавляемое в конец тестового пакета. Оно будет занимать 2 последних октета данных UDP (payload).

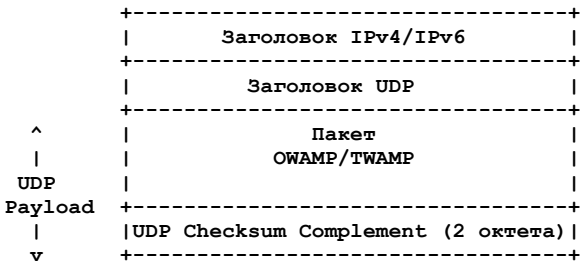

Рисунок 2. Checksum Complement в пакетах OWAMP/TWAMP.

Поле Checksum Complement служит для компенсации изменений, внесённых в пакет промежуточными элементами, как описано в разделе 1. Пример использования Checksum Complement представлен в Приложении A.

3.2. Тестовые пакеты OWAMP и TWAMP с Checksum Complement

Протоколы OWAMP [OWAMP] и TWAMP [TWAMP] используют пакеты с метками времени. Поле Checksum Complement **можно** использовать в следующих случаях:

- в тестовых пакетах OWAMP от отправителя к получателю;
- в тестовых пакетах TWAMP от отправителя к рефлектору;
- в тестовых пакетах TWAMP от рефлектора к отправител.

Тестовые пакеты OWAMP/TWAMP передаются по протоколу UDP с использованием IPv4 или IPv6. Этот документ применим к обоим вариантам использования OWAMP и TWAMP (IPv4 и IPv6).

Тестовые пакеты OWAMP/TWAMP включают поле заполнения Packet Padding. Этот документ предлагает использовать два последних октета поля Packet Padding в качестве Checksum Complement. В этом случае Checksum Complement всегда будет занимать 2 последних октета данных UDP и размещаться со смещением (UDP Length - 2) от начала заголовка UDP.

На рисунке 3 показан тестовый пакет OWAMP с полем UDP Checksum Complement.

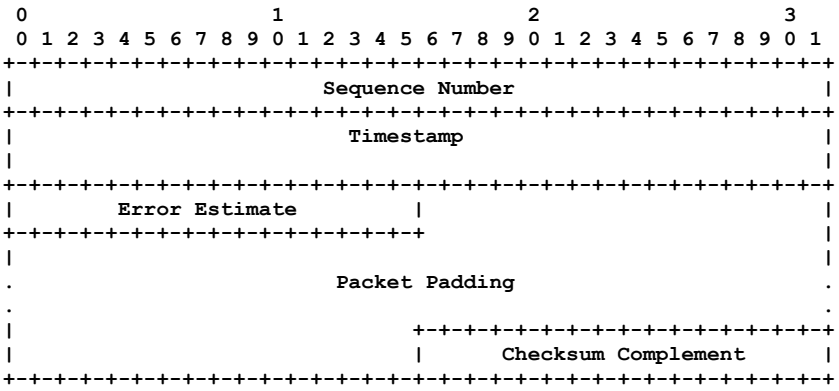

Рисунок 3. Checksum Complement в тестовом пакете OWAMP.

На рисунке 4 показан тестовый пакет TWAMP с полем UDP Checksum Complement (TTL означает Time to Live - время жизни, а MBZ - MUST be zero - должно быть 0 [IPPMIPsec]).

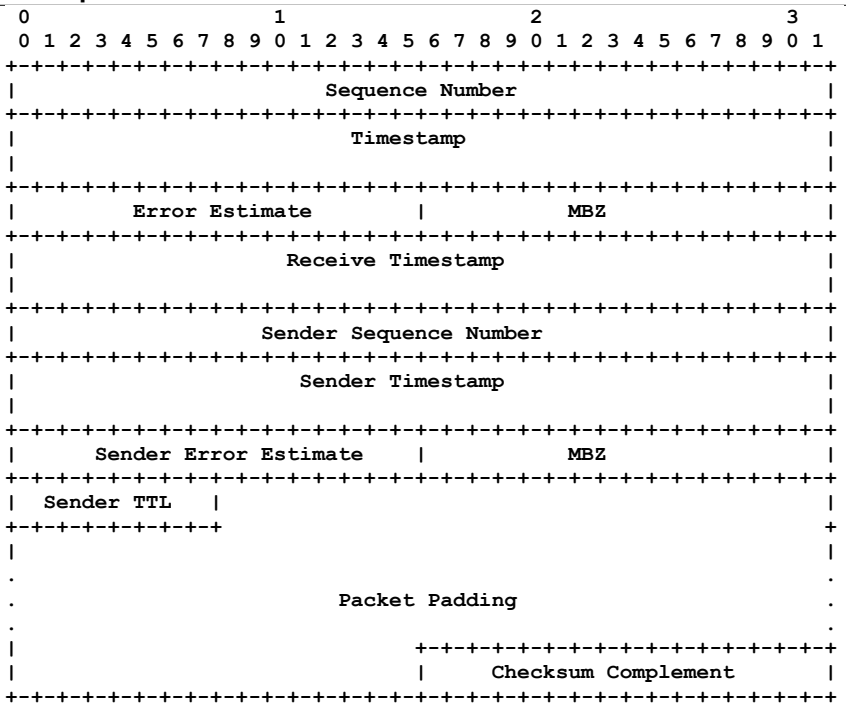

Рисунок 4. Checksum Complement в тестовом пакете TWAMP.

Размер поля Packet Padding в тестовых пакетах анонсируется при организации сессии через поле <Padding Length> в сообщении Request-Session [OWAMP] или Request-TW-Session [TWAMP].

При включении Checksum Complement поле заполнения **должно** быть достаточно большим, чтобы вместить Checksum Complement.

- В OWAMP размер заполнения составляет не менее 2 октетов, что позволяет отправителю внедрить Checksum Complement в последние 2 октета заполнения.
- В TWAMP размер заполнения составляет не менее 29 октетов в режиме без аутентификации и не менее 58 в режиме с аутентификацией. Дополнительное заполнение требуется потому, что заголовок тестовых пакетов рефлектора больше заголовка тестовых пакетов отправителя. Различие размеров этих заголовков составляет 27 октетов в режиме без аутентификации и 56 октетов при использовании аутентификации. Таким образом, заполнение в тестовых пакетах рефлектора короче заполнения в тестовых пакетах отправителя. Использование не менее 29 октетов заполнения (58 в режиме authenticated) в тестовых пакетах отправителя позволяет отправителю и рефлектору использовать 2-октетное поле Checksum Complement. Отметим, что при невыполнении этого требования рефлектор не может использовать Checksum Complement в отражённых тестовых пакетах, но отправителю можно включать Checksum Complement в передаваемые тестовые пакеты.
- В [TWAMP-Reflect] определены два необязательных свойства TWAMP: отражение октетов (octet reflection) и симметричный размер. При включении хотя бы одной из этих возможностей сообщение Request-TW-Session содержит поле <Padding Length>, а также поле <Length of padding to reflect>. В этом случае оба поля должны иметь достаточно большие значения, чтобы использовалось не менее 2 октетов заполнения у отправителя и рефлектора тестовых пакетов. В частности, при включённом отражении октетов должны быть определены два поля Length так, чтобы заполнение занимало хотя бы 2 последних октета после отражённых октетов.

Как указано в разделе 1, описанные в этом документе расширения реализуются на двух логических уровнях - уровне протокола и уровне меток времени. Предполагается, что эти уровни синхронизированы в части включения Checksum Complement. Поскольку оба уровня размещаются в одном сетевом устройстве, предполагается что не нужен протокол для синхронизации этих уровней. Когда применение Checksum Complement разрешено, уровень протокола должен позаботиться о наличии в пакетах требуемого заполнения, избавляя от необходимости проверки этого на уровне меток.

3.2.1. Передача OWAMP/TWAMP с Checksum Complement

Передатчик тестового пакета OWAMP/TWAMP **может** включать поле Checksum Complement в последние 2 октета заполнения.

Передатчик, включающий Checksum Complement в свои исходящие пакеты, **должен** включать в эти пакеты поле Packet Padding, размер которого **должен** позволять включение Checksum Complement. Размер поля Packet Padding согласуется при организации сессии, как указано в параграфе 3.2.

3.2.2. Промежуточное обновление OWAMP/TWAMP с Checksum Complement

Промежуточный элемент, получающий и изменяющий тестовый пакет OWAMP/TWAMP, может изменить поле UDP Checksum или поле Checksum Complement для обеспечения корректности значения UDP Checksum.

3.2.3. Приём OWAMP/TWAMP с Checksum Complement

Этот документ не задаёт дополнительных требований к приёму тестовых пакетов OWAMP/TWAMP.

Уровень UDP на приёмной стороне проверяет значение UDP Checksum в полученных пакетах, а уровню OWAMP/TWAMP следует считать Checksum Complement частью заполнения.

3.3. Совместимость с имеющимися реализациями

Поведение, заданное в этом документе, не вносит дополнительных требований к поведению при получении тестовых пакетов OWAMP/TWAMP. Стек протоколов принимающего хоста выполняет обычную проверку UDP Checksum, т. е. с его точки зрения наличие поля Checksum Complement не заметно. Поэтому функциональность, описанная в этом документе, позволяет взаимодействовать с узлами, соответствующими [OWAMP] или [TWAMP].

3.4. Применение Checksum Complement с аутентификацией и без неё

Протоколы OWAMP и TWAMP могут использовать аутентификацию или шифрование в соответствии с [OWAMP] и [TWAMP].

3.4.1. Checksum Complement в режиме Authenticated Mode

Подлинность тестовых пакетов OWAMP и TWAMP можно проверять с использованием HMAC (Hashed Message Authentication Code). Код HMAC охватывает некоторые поля заголовка тестового пакета, не учитывая поля Timestamp и Packet Padding.

Checksum Complement **можно** использовать при включённой аутентификации. В этом случае промежуточный элемент может внедрить метку времени и обновить поле Checksum Complement без изменения HMAC.

3.4.2. Checksum Complement в режиме Encrypted Mode

При работе OWAMP и TWAMP в режиме шифрования поле Timestamp также шифруется.

Checksum Complement **не следует** применять в режиме с шифрованием. Поле Checksum Complement эффективно в режиме с аутентификацией и без неё, позволяя промежуточному элементу последовательно обрабатывать пакет без его сохранения и пересылки.

В режиме с шифрованием промежуточный элемент, внедряющий метку в тестовый пакет, должен перешифровать пакет должным образом. Для перешифрования промежуточный элемент обычно должен сохранить пакет, перешифровать его и переслать. Таким образом, с точки зрения разработчика Checksum Complement имеет мало смысла в режиме encrypted, поскольку оно не упрощает реализацию.

Примечание. Хотя протоколы [OWAMP] и [TWAMP] имеют встроенные механизмы защиты, они могут использовать дополнительные меры, такие как [IPPMIPsec]. По причинам, указанным выше, применять Checksum Complement в таких случаях **не следует**.

4. Вопросы безопасности

Этот документ описывает использование расширения Checksum Complement для обеспечения корректности UDP Checksum.

Целью этого расширения является упрощение реализации модулей точных временных меток, как показано на рисунке 1. Расширение предназначено для внутреннего использования узлами с поддержкой OWAMP/TWAMP и не рассчитано на промежуточные коммутаторы или маршрутизаторы между отправителем и получателем (рефлектором). Любое изменение тестового пакета промежуточным коммутатором или маршрутизатором следует рассматривать как вредоносную MITM-атаку (man-in-the-middle).

Важно подчеркнуть, что описанная здесь схема не повышает уровень уязвимости протоколов к MITM-атакам. Злоумышленник MITM, злонамеренно изменяющий пакет и Checksum Complement в нем, логически эквивалентен злоумышленнику MITM, который меняет пакет и его поле UDP Checksum.

Описанная в документе концепция предназначена лишь для применения в режиме unauthenticated или authenticated. Как указано в параграфе 3.4.2, Checksum Complement в режиме encrypted не упрощает реализацию по сравнению с использованием традиционных контрольных сумм, поэтому применять Checksum Complement в этом режиме не следует.

5. Литература

5.1. Нормативные документы

[Checksum] Rijsinghani, A., Ed., "Computation of the Internet Checksum via Incremental Update", RFC 1624, DOI 10.17487/RFC1624, May 1994, <http://www.rfc-editor.org/info/rfc1624>.

[IPv6] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, December 1998, <http://www.rfc-editor.org/info/rfc2460>.

[KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[OWAMP] Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)", RFC 4656, DOI 10.17487/RFC4656, September 2006, <http://www.rfc-editor.org/info/rfc4656>.

[TWAMP] Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)", RFC 5357, DOI 10.17487/RFC5357, October 2008, <http://www.rfc-editor.org/info/rfc5357>.

[TWAMP-Reflect] Morton, A. and L. Ciavattone, "Two-Way Active Measurement Protocol (TWAMP) Reflect Octets and Symmetrical Size Features", RFC 6038, DOI 10.17487/RFC6038, October 2010, <http://www.rfc-editor.org/info/rfc6038>.

[UDP] Postel, J., "User Datagram Protocol", STD 6, RFC 768, DOI 10.17487/RFC768, August 1980, <http://www.rfc-editor.org/info/rfc768>.

5.2. Дополнительная литература

[IEEE1588] IEEE, "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems", IEEE Std 1588-2008, DOI 10.1109/IEEESTD.2008.4579760, July 2008.

[IPPMIPsec] Pentikousis, K., Ed., Zhang, E., and Y. Cui, "IKEv2-Derived Shared Secret Key for the One-Way Active Measurement Protocol (OWAMP) and Two-Way Active Measurement Protocol (TWAMP)", RFC 7717, DOI 10.17487/RFC7717, December 2015, <http://www.rfc-editor.org/info/rfc7717>.

[RFC7821] Mizrahi, T., "UDP Checksum Complement in the Network Time Protocol (NTP)", RFC 7821, DOI 10.17487/RFC7821, March 2016, <http://www.rfc-editor.org/info/rfc7821>.

[ZeroChecksum] Fairhurst, G. and M. Westerlund, "Applicability Statement for the Use of IPv6 UDP Datagrams with Zero Checksums", RFC 6936, DOI 10.17487/RFC6936, April 2013, <http://www.rfc-editor.org/info/rfc6936>.

Приложение A. Пример использования Checksum Complement

Рассмотрим сессию между отправителем и получателем OWAMP, где отправитель передаёт тестовые пакеты получателю.

Программный уровень отправителя генерирует тестовый пакет OWAMP с временной меткой T и UDP Checksum = U. Значение U является контрольной суммой заголовка и данных UDP, а также псевдозаголовка. Таким образом,

```
U = Const + checksum(T)                    (1)
```

где Const - контрольная сумма всех охватываемых полей, за исключением T.

Напомним, что программа отправителя выдаёт тестовый пакет с полем Checksum Complement, которое представляет собой просто 2 последних октета заполнения. В этом примере предполагается, что отправитель заполнил эти октеты нулями.

Модуль временных меток отправителя обновляет поле Timestamp точным знасением, меняя T на T', а также обновляет поле Checksum Complement, помещая вместо 0 значение C, так что

```
checksum(C) = checksum(T) - checksum(T')    (2)
```

Когда модуль временных меток отправителя передаёт пакет, значение контрольной суммы U остаётся прежним

```
U = Const + checksum(T) = Const + checksum(T) + checksum(T') -
    checksum(T') = Const + checksum(T') + checksum(C)    (3)
```

Таким образом, после обновления метки времени модулем меток значение U в пакете остаётся корректным.

Когда тестовый пакет приходит к получателю, тот выполняет обычный расчёт UDP Checksum и получает значение U. Поскольку Checksum Complement является частью заполнение, значение checksum(C) «прозрачно» включается в расчёт в соответствии с уравнением (3) без специальных действий получателя.

Благодарности

Автор признателен Al Morton, Greg Mirsky, Steve Baillargeon, Brian Haberman, Spencer Dawkins за полезные замечания.

Адрес автора

Tal Mizrahi
Marvell
6 Hamada St.
Yokneam, 20692
Israel
Email: talmi@marvell.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru