УДК. 004.722

А. И. Куликов, Я. А. Бекенёва
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Среда имитационного моделирования систем мониторинга для анализа объема передаваемого трафика

В последние годы резко возрастают объемы трафика, передаваемого в компьютерных сетях. Не стали исключением и системы, предназначенные для мониторинга различных процессов, так как подобные системы все более усложняются по структуре и содержат большое количество устройств, в том числе генерирующих мультимедийные данные. Разработанная среда предназначена для создания моделей систем мониторинга в виде компьютерной сети. Основная ее цель – оценить потоки данных, нагрузку на каналы связи, их пропускную способность и выявить узкие места. Различные устройства, используемые в системах мониторинга, генерируют разный объем данных и передают их с разной частотой. Элементы модели системы мониторинга были проверены на реальных устройствах, когда пользователь может изменять настройки трафика в соответствии со своими потребностями. Такая среда может использоваться как для изучения каналов связи в существующих системах мониторинга, так и для проектирования новых архитектур с целью оптимизации трафика.

Сеть, симуляция, траффик, cisco, пропускная способность

Системы мониторинга, используемые для наблюдения за ходом различных процессов на предприятиях, имеют сложную структуру и включают в себя большое количество разных устройств контроля. Каждое устройство регистрирует определенные параметры процесса в заданные моменты времени или непрерывно и передает данные на центральный узел. Разные типы устройств генерируют различные объемы данных.

Системы видеонаблюдения устанавливаются для визуального контроля обстановки на объекте. На сегодняшний день они – это обязательная, а в некоторых случаях – главная составляющая любой системы безопасности. Организация видеонаблюдения на объекте в несколько раз увеличивает шансы предотвратить несанкционированное проникновение на него. В общем виде система видеонаблюдения состоит из видеокамер, устройств записи и воспроизведения. При помощи системы видеонаблюдения можно обезопасить практически любой объект. Объем непрерывно генерируемых устройствами видеонаблюдения данных весьма велик, рост количества используемых камер пропорционально увеличивает нагрузку как на каналы связи, так и на устройство, обрабатывающее изображения. Хранение, структурирование, а в случае создания распределенной системы еще и нагрузка на сеть требуют большого количества расчетов и ресурсов.

В последние годы в разных системах все чаще используются распределенные вычисления. При разработке новых методов обработки данных в системах мониторинга, в том числе распределенных, особенно важна оценка объема передаваемого трафика. Для проведения экспериментов по оценке трафика при разных предлагаемых подходах к обработке можно как использовать математические расчеты, так и создать среду для моделирования потоков данных. В данной статье представлена среда, позволяющая создавать разнообразные сценарии передачи данных и оценивать их объем в разных сегментах сети в заданные моменты времени.

Моделирование систем, в том числе систем мониторинга, представляет собой достаточно часто встречаемую задачу в различных областях исследований, например в здравоохранении. Как правило, в таких исследованиях основной задачей становится изучение возможностей работы проектируемой системы с целью корректировки ее функционала. Задача моделирования системы с точки зрения структуры вычислительной сети значительно менее распространена.

Гораздо чаще встречается задача моделирования компьютерных сетей [1]–[3]. В настоящее время на рынке доступны разнообразные программные продукты, предназначенные для моделирования компьютерных сетей. Такие продукты позволяют имитировать сети, имеющие различную топологию и включающие в себя стандартные устройства: персональные компьютеры, маршрутизаторы, коммутаторы, шлюзы, серверы и пр. Включение в состав сети дополнительных устройств требует либо подключения соответствующих библиотек, либо внедрения собственных разработок.

Задача моделирования системы мониторинга в виде компьютерной сети может быть реализована на основе существующего симулятора при наличии нескольких возможностей:

1) реализации различных сценариев передачи данных разными устройствами мониторинга;

2) учета объема передаваемых данных при разном количестве зафиксированных событий;

3) реализации моделирования непрерывной передачи потоков данных, имеющих объем, равный объему видеоданных.

Для реализации проекта необходимо было выбрать подходящий симулятор сети. На данный момент существует два лидера в этой области:

1) Cisco Packet Tracer (CPT) [4], [5];

2) OMNeT++ [6].

В результате изучения возможностей средств моделирования сетей был сделан вывод, что они имеют схожий функционал, и, не смотря на то, что OMNeT++ имеет немного более гибкие механизмы настройки, выбор для реализации экспериментов был сделан в пользу Cisco Packet Tracer по следующим причинам:

1) более дружелюбный интерфейс;

2) наличие режима симуляции, позволяющего наглядно видеть перемещение пакетов, а также анализировать пакеты на предмет нахождения на том или ином уровне модели OSI;

3) готовые решения из раздела IoT, удобные для реализации проекта по выбранной теме;

4) возможность тонкой настройки работы каждого устройства средствами языка программирования;

5) большое количество учебных материалов на русском языке, что делает освоение этой среды проще по сравнению с аналогами.

Перед построением сетей и проведением экспериментов необходимо было построить простую сеть, а также провести ее верификацию на реальном оборудовании для применения полученных данных в проведении дальнейшего исследования.

В рабочую область программы CPT были добавлены следующие компоненты:

1) маршрутизатор, выполняющий функцию интернет-соединения;

2) коммутатор;

3) компьютер;

4) камера наблюдения.

Сеть в симуляторе была успешно построена, однако для дальнейшей работы и моделирования более сложной сети, на основании которой можно будет делать выводы о проделанной работе, а также давать рекомендации для создания систем видеонаблюдения, необходимо было узнать, какой трафик передают камеры видеонаблюдения (до этого использовалась примерное значение, взятое из открытых интернет-источников).

Для получения данных о том, какое количество трафика передает за сутки среднестатистическая камера, было решено провести эксперимент с реальным оборудованием. IP-камера была подключена к персональному компьютеру посредством маршрутизатора, при этом на протяжении всего эксперимента велся учет трафика, поступающего с камеры.

Из проведенного исследования был сделан следующий вывод: камера с разрешением 976 × 582 пикс. за сутки использования записывает 19.8 Гбайт информации. Для удобства дальнейших подсчетов это число было округлено до 20 Гбайт. Далее были подсчитаны оптимальные установки для пакетов в CPT – 2500 байт в 0.01 с.

Основной задачей исследования было оценить трафик в системах мониторинга при различных вариантах архитектур и различных устройствах, используемых для мониторинга процесса перемещения объектов. Для сравнения были рассмотрены три варианта архитектур систем мониторинга в точках наблюдения, которые отличаются друг от друга составом и количеством устройств:

1) минимальный;

2) базовый;

3) расширенный.

Рассмотрим подробнее каждый из них[1].

Минимальный вариант содержит три контрольно-пропускных пункта, на каждом из которых присутствует по две камеры слежения для

[1] Все описанные эксперименты проводились в среде Cisco Packet Tracer.

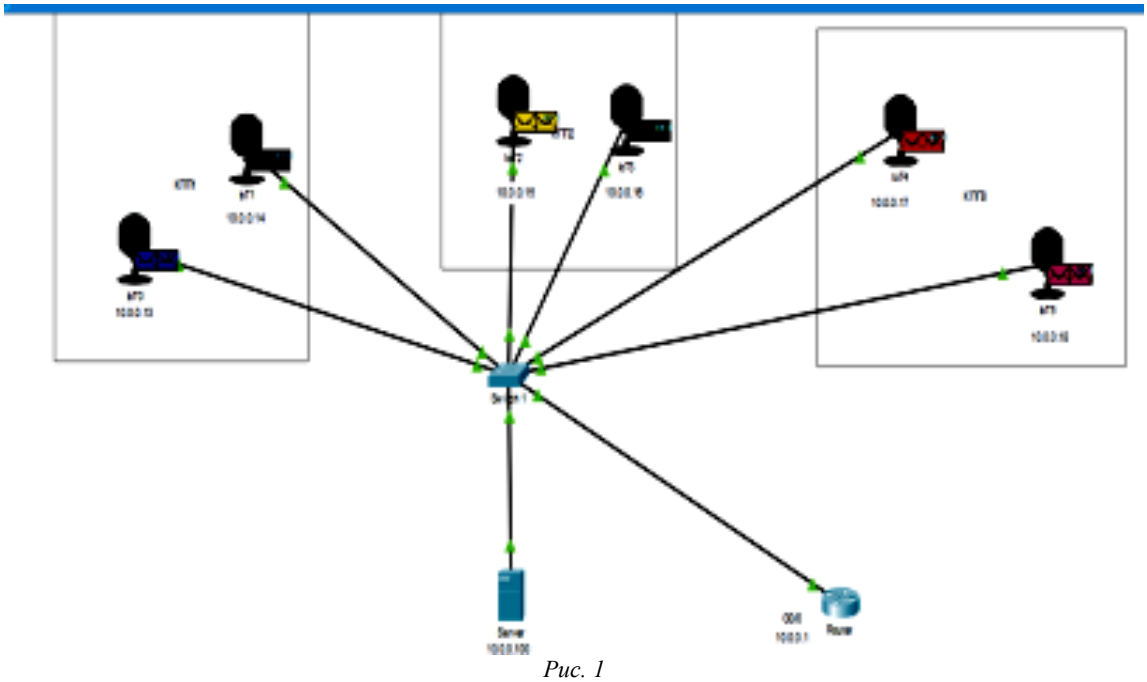

Рис. 1

контроля ситуации на въезде и на выезде (рис. 1). Все камеры передают записываемые данные на один и тот же сервер, который используется в качества узла сбора и обработки данных. При инициации эксперимента были указаны настройки передаваемого объема данных от каждой камеры в соответствии с полученными ранее результатами для реальной камеры – 2500 байт каждую сотую секунды.

Для наглядного показа объема трафика, передаваемого с каждого устройства, было решено использовать встроенный в CPT анализатор трафика для компьютерных сетей – Netflow Collector, доступный на всех интегрированных серверах и персональных компьютерах в окне «Desktop». Анализатор работает в связке с установленным и настроенным маршрутизатором, на который и будут отправляться пакеты трафика, в то время как сервер при помощи описанной утилиты будет составлять диаграмму всего переданного трафика.

Данный эксперимент был проведен 144 раза для получения данных за сутки модельного времени. Проведенные эксперименты показали отсутствие потерь при передаче данных.

В базовом варианте сети (рис. 2), к камерам добавлены другие устройства для отслеживания обстановки на объекте: датчик движения 1, датчик задымления 2, считыватель магнитных карт 3. Для этих устройств были использованы типовые значения объема генерируемых сообщений, взятые из спецификаций.

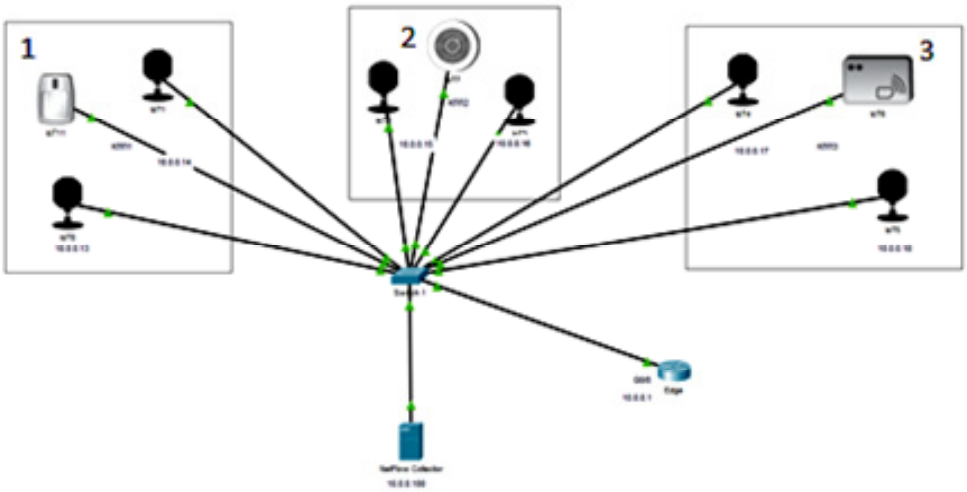

Рис. 2

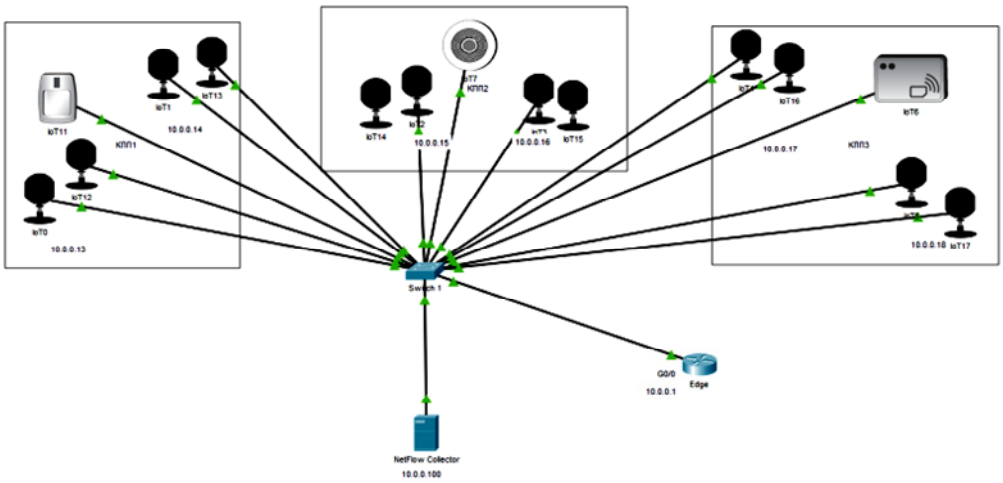

Рис. 3

Проведенная серия испытаний для базового варианта архитектуры тоже насчитывает 144 эксперимента. В результате получилось, что и в базовом варианте архитектуры не был потерян ни один пакет. Дополнительные устройства также обошлись без потерь во время передачи, у датчика задымления и считывателя магнитных карт равные доли трафика. Датчик движения, в свою очередь, передает почти в два раза меньше трафика, чем датчик задымления и считыватель магнитных карт.

В расширенном варианте сети (рис. 3) помимо уже имеющихся и перекочевавших из базового варианта датчиков слежения добавлены по одной дополнительной камере к каждой имеющейся и привязаны к тому же IP-адресу, что в теории должно обеспечить бесперебойный поток данных в случае потерь на одной из камер. Аналогично предыдущим вариантам, запуск симуляции был произведен 144 раза.

В результате эксперимента утилита NetFlow Collector показала, что в расширенном варианте сети уже начала происходить потеря данных, о чем свидетельствует небольшое различие в долях каждой из пар камер, хотя визуально на диаграмме, скриншот которой представлен на рис. 4, это незаметно.

Также о потере данных сигнализирует надпись в окне настройки пакетов «Failed» – это значит, что пакет потерялся в процессе транспортировки.

Файлы проектов сохранены в формате .pkt, доступны для открытия, редактирования и проведения экспериментов.

Из трех рассмотренных вариантов сетей для установки на реальном объекте можно порекомендовать базовый вариант как самый надежный по соотношению нагрузки на сеть и количества оборудования, обеспечивающего безопасность.

Данные, полученные в результирующей таблице, говорят о том, что хотя дополнительные камеры и будут компенсировать потерю пакетов, однако установка расширенного варианта сети нецелесообразна как технически (и до установки

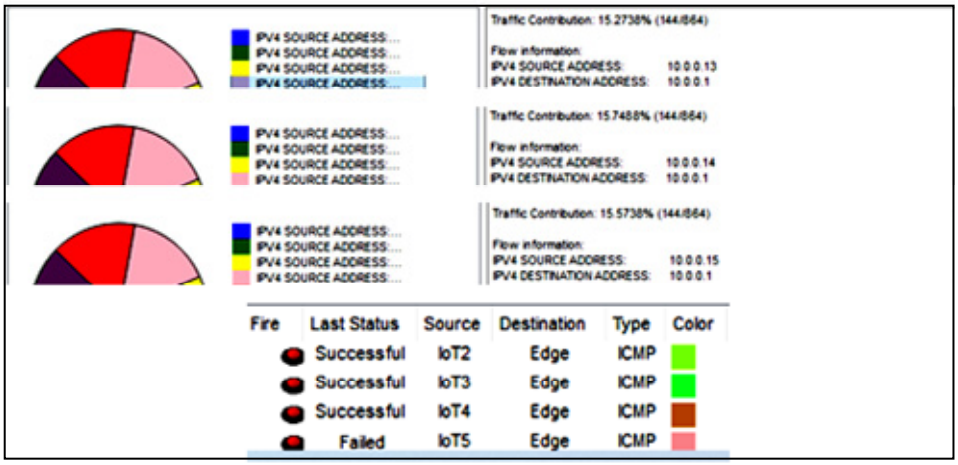

Рис. 4

дополнительных камер сеть без проблем справлялась с нагрузкой), так и финансово (нет смысла в закупке дополнительного дорогостоящего оборудования, если сеть с меньшим количеством оборудования, меньшими затратами на его закупку и обслуживание справляется лучше перегруженной).

Параметры сети	Минимальный	Базовый	Расширенный
Кол-во устройств	6	9	15
Кол-во камер	6	6	12
Объем трафика КПП 1, Гбайт	40	40.08	80.08
Объем трафика КПП 2, Гбайт	40	40.17	80.17
Объем трафика КПП 3, Гбайт	40	40.17	80.17
Объем потерь, Гбайт	120	120.42	240.42

В результате проведенных экспериментов с разными вариантами сетей можно сделать следующие выводы:

1. Выбранный симулятор сетей и реализованные в нем модели полностью удовлетворяют целям работы, в результате проведения экспериментов удалось получить наглядные данные, опираясь на которые, можно проектировать сети на реальном предприятии.

2. Система получилась гибко настраиваемой, в нее в любой момент можно добавить новые или убрать лишние устройства, причем это не только камеры наблюдения, но и другие полезные устройства слежения, широко применяемые на практике.

3. Система позволяет анализировать как общий трафик, так и трафик, поступающий с отдельных устройств и узлов, что может быть крайне полезно для глубокого анализа построенной сети на предмет возникновения потери данных и устранения подобных проблем.

Изучение систем распределенного видеонаблюдения показывает важность грамотного подхода к их проектированию. Предложенная среда моделирования сетей позволяет исследовать объемы трафика и нагрузку на каналы связи и узлы сбора данных для любой структуры системы мониторинга и любого состава устройств. Полученные результаты позволят оценить вероятность перегрузки или выхода из строя отдельно взятых узлов, а также определить требования к каналам связи и вычислительным мощностям узлов, собирающих и обрабатывающих данные. Таким образом могут быть оценены различные характеристики системы мониторинга с точки зрения передачи данных на ранних этапах проектирования.

Предложенные в данной статье сценарии построения сети на примере контрольно-пропускных пунктов, а также предложения по оптимальному варианту выбора такой сети могут быть использованы на реальных объектах с целью повышения их безопасности.

Сценарии универсальны. В реальной практике могут применяться и другие датчики отслеживания обстановки, при необходимости их легко интегрировать в готовые схемы сети и проверить работоспособность, сэкономив большое количество времени и финансов.

Развитием данной работы может стать изучение разных сценариев и составов систем мониторинга для поиска так называемых узких мест, т. е. могут быть реализованы сценарии, где осуществляется перегрузка каналов связи или определенных узлов трафиком от камер до такой степени, чтобы они вышли из строя, а также изучение вопроса и формирование рекомендаций, как избежать подобных ситуаций или устранить их последствия.

Работа выполнена при финансовой поддержке Стипендии Президента Российской Федерации СП-2581.2019.5.

СПИСОК ЛИТЕРАТУРЫ

1. Netsquid, a network simulator for quantum information using discrete events / T. Coopmans, R. Knegjens, A. Dahlberg, D. Maier, L. Nijsten, J. de Oliveira Filho, S. Wehner // Communications Phys. 2021. Vol. 4, № 1. P. 1–15.

2. Simblock: A blockchain network simulator / Y. Aoki, K. Otsuki, T. Kaneko, R. Banno, K. Shudo // IEEE INFOCOM 2019-IEEE Conf. on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 2019. P. 325–329. URL: https://ieeexplore.ieee.org/document/8845253 (дата обращения: 01.10.2021).

3. Baidya S., Shaikh Z., Levorato M. FlyNetSim: An open source synchronized UAV network simulator based on ns-3 and ardupilot // Proc. of the 21st ACM Intern. Conf. on Modeling, Analysis and Simulation of Wireless and Mobile Systems. Montreal: Association for Computing Machinery, 2018. P. 37–45.

4. Компания Cisco System, URL: https://www.cisco.com/c/dam/global/ru_ua/training-events/events/pdf/videosurveillance-amarchen.pdf (дата обращения: 01.10.2021).

5. Основы Cisco Packet Tracer. URL: http://just-networks.ru/articles/osnovy-raboty-s-cisco-packet-tracer (дата обращения: 01.10.2021).

6. Хабаров С. П. Основы моделирования беспроводных сетей. Среда OMNeT++: учеб. пособие. СПб.: Лань, 2019.

A. I. Kulikov, Ya. A. Bekeneva
Saint Petersburg Electrotechnical University

AN ENVIRONMENT FOR SIMULATION MODELING OF MONITORING SYSTEMS FOR ANALYZING THE VOLUME OF TRANSMITTED TRAFFIC

In recent years, the volume of traffic transmitted in computer networks has been increasing. Systems designed to monitor various processes are no exception, since such systems are becoming more and more complex in structure and contain a large number of devices, including those that generate multimedia data. The developed environment is designed to create models of monitoring systems in the form of a computer network. The main goal is to assess data flows, load on communication channels, estimate bandwidth and identify bottlenecks. Different devices used in monitoring systems generate different amounts of data and transmit them at different frequencies. Elements of the monitoring system model have been tested on real devices, but the user can change the traffic settings according to his needs. Such an environment can be used both for studying communication channels in existing monitoring systems and for designing new architectures in order to optimize traffic.

Network, simulation, traffic, cisco, bandwidth