Известия Гомельского государственного университета
имени Ф. Скорины, № 6 (111), 2018

Информатика

УДК 004.777

Программируемое управление доступом к сети с адаптивной настройкой физических интерфейсов

А.И. Чернышев[1], И.О. Демиденко[1], А.В. Воруев[1], С.Ю. Михневич[2]

Представлены результаты исследований в рамках проекта AgronomiX. Рассматривается структура облачных сред и применение туманных вычислений. Использованы методы анализа трафика на транспортном уровне. Высказываются предложения по настройке контроллеров облачной туманности.
Ключевые слова: облачная сетевая среда, туманные вычисления, телекоммуникационные сети, информационные технологии.

Results of researches within the AgronomiX project are presented. The structure of cloud environments and application of foggy calculations are considered. Methods of the analysis of traffic at the transport level are used. Suggestions for configuring cloud nebula controllers are expressed.
Keywords: cloud network environment, foggy calculations, telecommunication networks, information technologies.

Введение. Прогнозируется, что к 2020 г. Интернет соединит 50 миллиардов устройств. Среди этих устройств большая часть будет охватывать датчики и устройства первичного сбора данных, которые будут генерировать потоки информации, необходимые для оценки состояния окружающей среды или объектов, информация о состоянии которых интересует исследователя. Примером таких устройств являются IoT-системы.

Уровень активной нагрузки на устройство первичного сбора данных исключает возможность преобразования информационного потока в сетевой трафик, отвечающий всем условиям информационной безопасности.

Один из подходов, предлагающий возможность использования устройств IoT и соблюдения требований к информационной безопасности, реализуется в рамках концепции «туманных вычислений» (fog computing).

1. Структура сетевой среды туманных вычислений. Туманные вычисления - эта сетевая модель IoT определяет инфраструктуру распределенных вычислений, расположенную ближе к периметру сети. Она позволяет устройствам на периметре локально проводить замеры, выполнять приложения и принимать немедленные решения. Данные не нужно отправлять по сетевым соединениям в режиме online. Предусмотрена возможность их промежуточного накопления и первичной обработки. Повышается отказоустойчивость, позволяя устройствам IoT работать, когда сетевые соединения теряются. Повышается уровень безопасности благодаря хранению чувствительных данных в пределах границы, где они необходимы (рисунок 1).

Для обеспечения работоспособности системы необходимо использование компонентов платформы поддержки приложений, которые реализуют инфраструктуру для размещения приложений, банков первичного размещения данных и обеспечения мобильности приложений между средами облачных и туманных вычислений.

В качестве таких устройств естественным посредником являются устройства, обеспечивающие подключение (кабельное или беспроводное) к сетевой среде IoT-устройств.

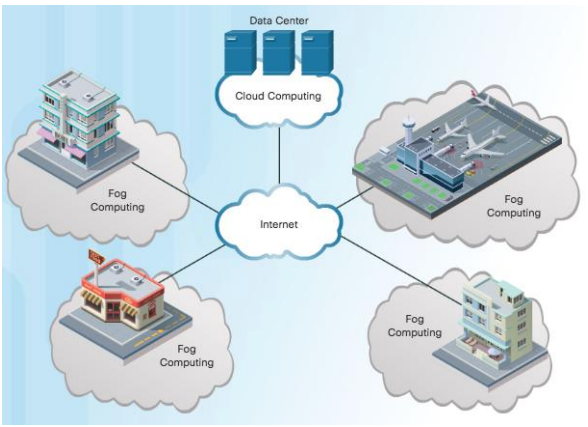

Рисунок 1 – Сетевая модель «туманных вычислений» (Fog Computing)

Операционная система такого сетевого устройства должна обладать большим уровнем универсальности, поскольку его вычислительная мощность будет обеспечивать замену функционала, вынесенного за границу IoT-устройств. Например, Cisco IOx – это программное решение компании Cisco для своих устройств, которое сочетает функционал Cisco IOS и Linux, что позволяет маршрутизаторам размещать приложения вблизи объектов, которыми эти приложения управляют и которые необходимо контролировать, анализировать и оптимизировать (рисунок 2).

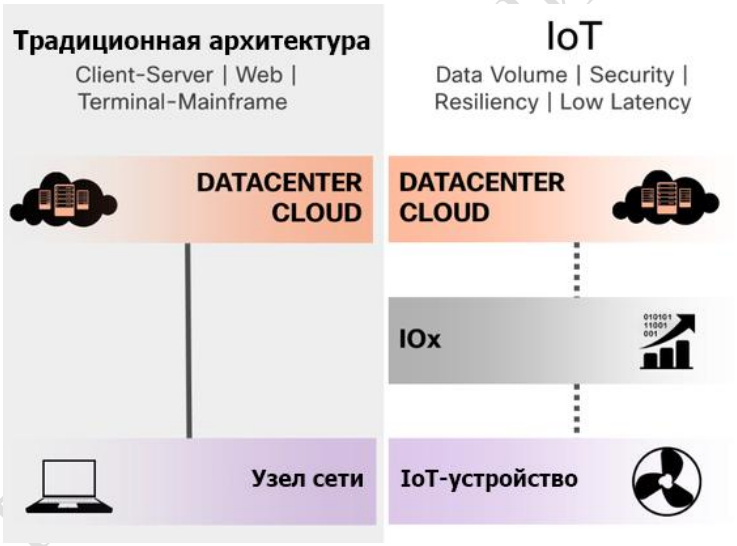

Рисунок 2 – Сетевая модель «туманных вычислений» (Fog Computing)

2. Программируемая сетевая архитектура. Программируемая сетевая архитектура (Программно-конфигурируемая сеть, Программно-определяемая сеть, Software-defined Networking, SDN) – это сеть передачи данных, в которой уровень управления сетью отделён от устройств передачи данных и реализуется программно. Формально это один из способов виртуализации вычислительных ресурсов, позволяющий более гибко решить вопрос ограничения доступа к физической среде передачи данных.

Централизованное управление множеством сетевых устройств снижает вероятность ошибки в назначении доступа и сокращает время обслуживания сети в случае изменения в политиках безопасности или протоколах связи.

Архитектура SDN разграничивает целевые и управляющие потоки данных, которые возникают на уровне передачи данных, уровне управления и уровне приложений (рисунок 3).

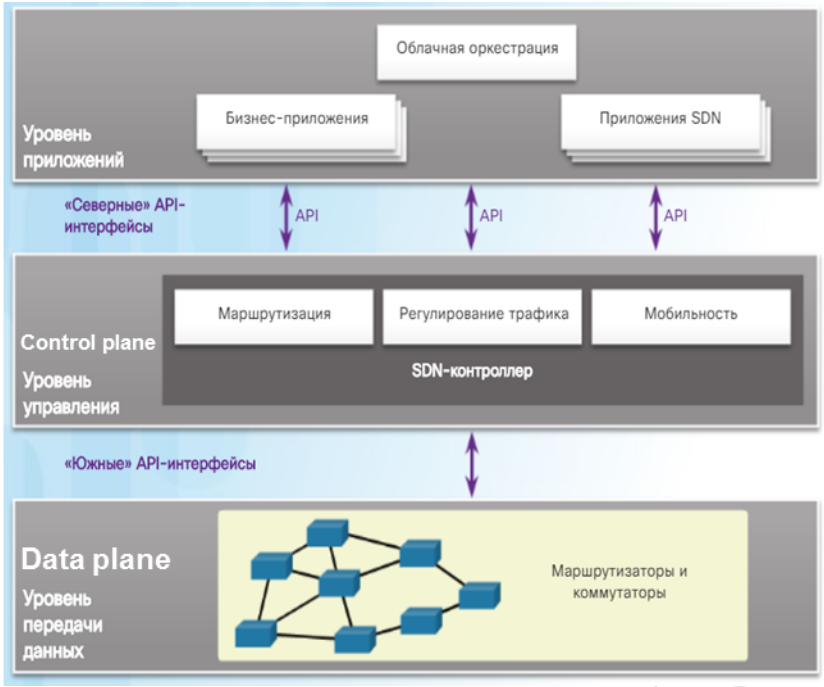

Рисунок 3 – Трехуровневая модель архитектуры SND

Таким образом, точка принятия решений об авторизации доступа оконечного оборудования к физическому интерфейсу и назначения характеристики организуемого канала связи переносится на сторону сервера.

3. Управление сетевым интерфейсом для доступа к сети. Управление доступом к сети на основе портов использует характеристики физического доступа к инфраструктуре IEEE 802 LAN, чтобы обеспечить средства аутентификации и авторизации устройств, подключенных к порту. Порт в этом контексте является единственной точкой привязки к инфраструктуре ЛВС. Примерами портов, в которых может быть желательно использование аутентификации, являются порты коммутаторов и мостов (как указано в IEEE 802.1D), порты, используемые для присоединения серверов или маршрутизаторов к инфраструктуре ЛВС, а также ассоциации между станциями и точками доступа в IEEE 802.11 Wireless LANs. Стандарт IEEE 802.1X определяет общую архитектуру, функциональные элементы и протоколы, которые поддерживают взаимную аутентификацию между клиентами портов, подключенных в границах одной локальной сети.

Операция процесса аутентификации использует протокол Extensible Authentication Protocol (EAP, указанный в IETF RFC 2284) в качестве средства передачи информации для аутентификации между узлом и сервером аутентификации. С помощью EAP может быть добавлена поддержка нескольких схем аутентификации, включая смарт-карты, Kerberos, шифрование с открытым ключом, одноразовые пароли и прочее.

Аутентификатор PAE (Port Access Entity) отвечает за обеспечение аутентификации узла-клиента или другого присоединяемого к сети устройства, которые подключаются к контролируемому порту и для контроля состояния авторизации управляемого порта соответственно (рисунок 4).

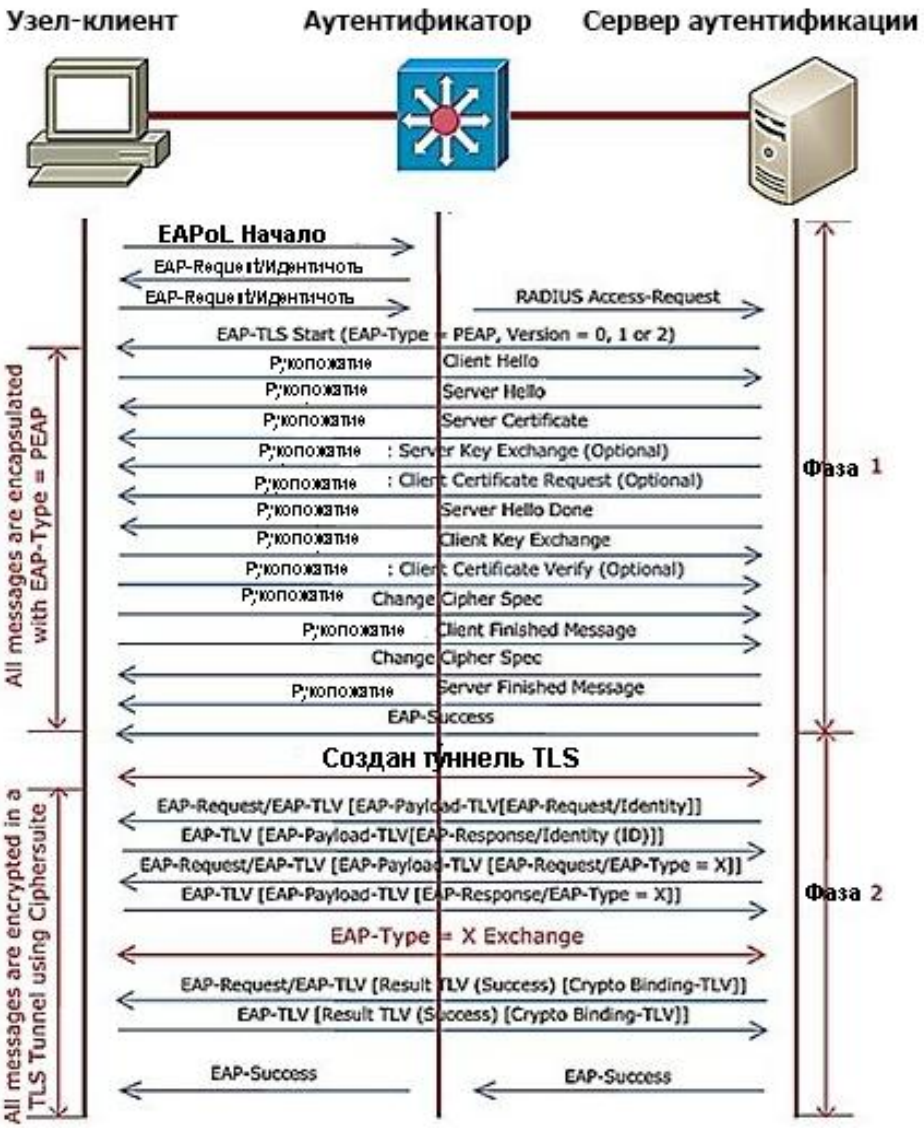

Рисунок 4 – Процедура аутентификации EAP-PEAP и обмен сообщениями

Сервер аутентификации либо размещен в той же локальной сети, что и аутентификатор PAE, либо он может находиться в другой сети. Важное требование, чтобы в момент проведения процедуры аутентификации сервер был доступен.

4. Определение границ действия облачной среды. Иерархическая архитектура обслуживания приложений позволяет сочетать аппаратные решения, программные интерфейсы обслуживания клиентов (приложения) и программно-реализованные (виртуализированные) сетевые сервисы для повышения эффективности обслуживания конечного оборудования.

На рисунке 5 представлена архитектура, состоящая из контроллера облачной туманности (Control Plane, уровень 1) и многоуровневых туманных узлов (Control Plane, уровни 2, 3 и 4), которые работают совместно, чтобы включить миграцию служб для распределения видео с поддержкой QoE.

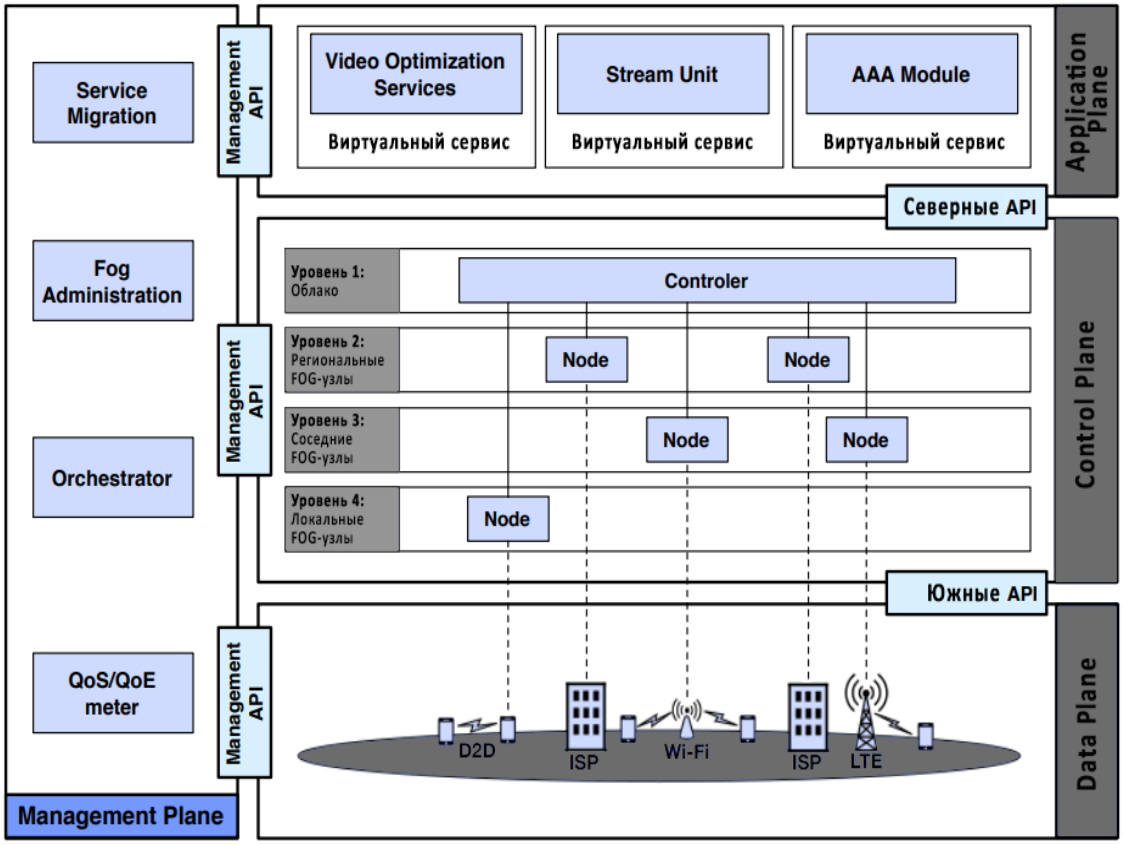

Рисунок 5 – Многоуровневая архитектура FOG-Computing

В такой архитектуре мы рассматриваем полностью подключенный и полностью туманный сценарий, где туманные узлы иерархически организованы для предоставления видеоуслуг для конечных пользователей.

Могут быть использованы широко распространенные локальные туманные узлы, например, мобильные устройства (Control Plane, уровень 4), где такой туманный узел (FOG-узел) передает видеоконтент через беспроводную связь с устройства на устройство (межмашинный интерфейс, M2M) для мобильных устройств с аналогичными требованиями к трафику друг с другом, чтобы создать сеть M2M.

Соседний Fog-узел, например, базовая станция (BS) или точка доступа (AP) (Control Plane, уровень 3), поддерживает от несколько десятков до нескольких сотен локальных FOG-узлов. Над ними должен быть региональный Fog-узел, например, блок базовой полосы (BBU) или поставщик интернет-услуг (ISP) (Control Plane, уровень 2), управляющий координацией по всему городу. Вершиной такой многоуровневой архитектуры является облако или связь с ним (Control Plane, уровень 1).

Произведем оценку проекта с четко определенными границами, метриками и включенными устройствами. На рисунке 6 представлена топология сети, включающей в себя все необходимые устройства для анализа разработанной fog computing framework, используемой для проведения экспериментов.

Топология состоит из четырех различных устройств, промежуточного программного обеспечения облачной туманности, узлов управления туманностью, ячеек туманности и датчиков. Среднее промежуточное ПО облачной туманности создает верхний уровень топологии и выполняется на Macbook Pro, подключенном к облачной среде OpenStack, и используется для загрузки и решения задач. Остальные компоненты, включенные в настройку, развернуты на Potatoes Pis.

Кроме того, узел Fog Control Node 1 (FCN 1) напрямую связан с облачой туманностью (CFM) и используется как контроллер, то есть узел управления облачной туманностью для подсоединенных туманных устройств. Туманность, контролируемая и организованная

FCN 1, состоит из FCN 2 и FCN 3. Оба, FCN 2 и FCN 3, контролируют подключенные туманные ячейки, которые обрабатывают данные с подключенных устройств IoT.

В этой установке подключенные устройства IoT представляют собой сенсорные модули, состоящие из датчика температуры и влажности. Эти сенсорные модули подключены к соответствующему участку с помощью сенсорных модулей.

Топология сети настроена как сеть беспроводной локальной сети точкой доступа Linksys. Эта точка доступа подключена к Интернету и работает как шлюз подключения каждого Potatoes Pi к Интернету.

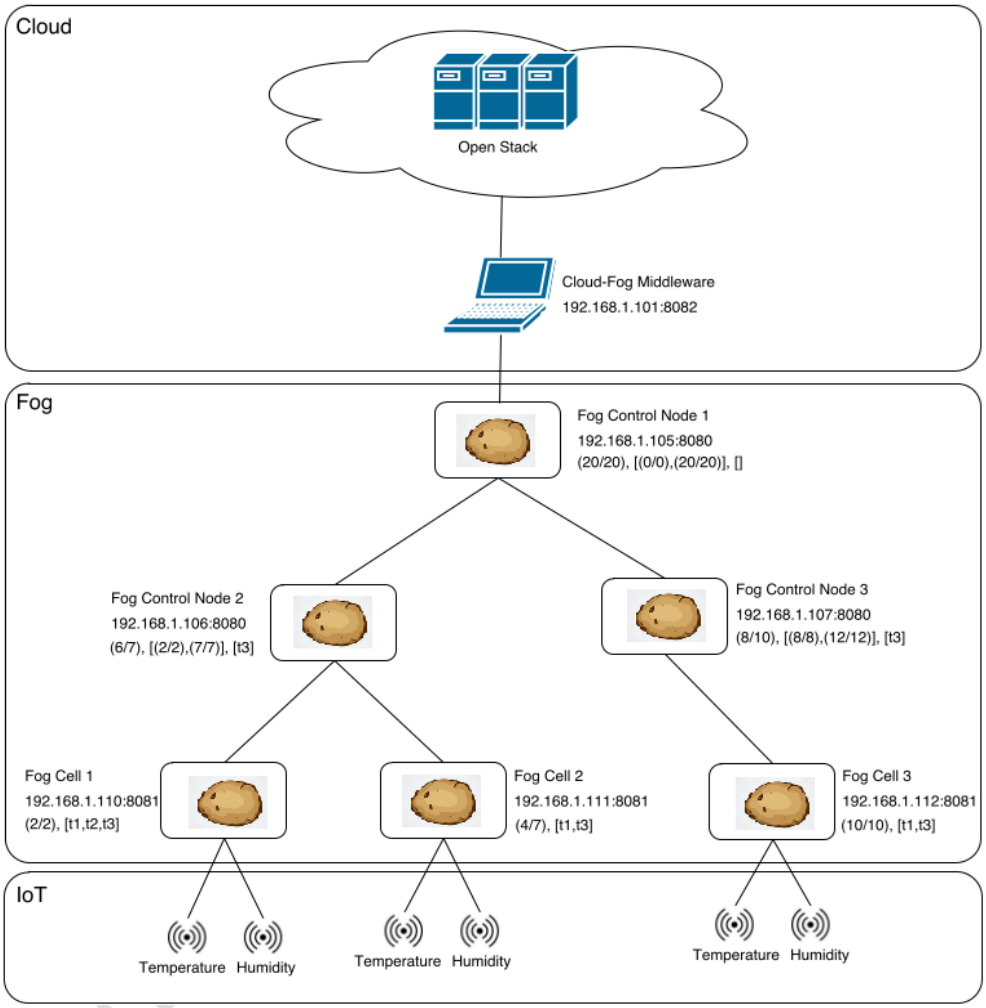

Рисунок 6 – Логические связи в топологии

В разработанном испытательном проекте каждый компонент должен быть подключен к Интернету, поскольку туманные службы требуют возможности загрузки данных Docker Image для создания и развертывания динамических служб.

В топологии сети для оценки каждое устройство в слое туманности содержит различную информацию (сверху вниз):

- имя устройства;
- IP-адрес и порт;
- местоположение устройства;
- диапазон местоположения и список типов услуг, которые устройство может обрабатывать.

Последняя строка информации устройства может отличаться в зависимости от типа устройства, например, только узлы управления туманом имеют диапазон местоположения. Расположение устройства и его местоположение необходимы для оценки ответственного «родителя» для нового соединения устройств туманности. Параметр диапазона местополо-

жения определяет географическую область, за которую отвечает узел управления туманностью. Следовательно, каждое устройство, запрашивающее «родителя» с его собственным местоположением устройства, получает возвращаемого «родителя», который покрывает область, в которой находится запрашивающее устройство. На рисунке 7 представлена сетка размещения настройки оценки.

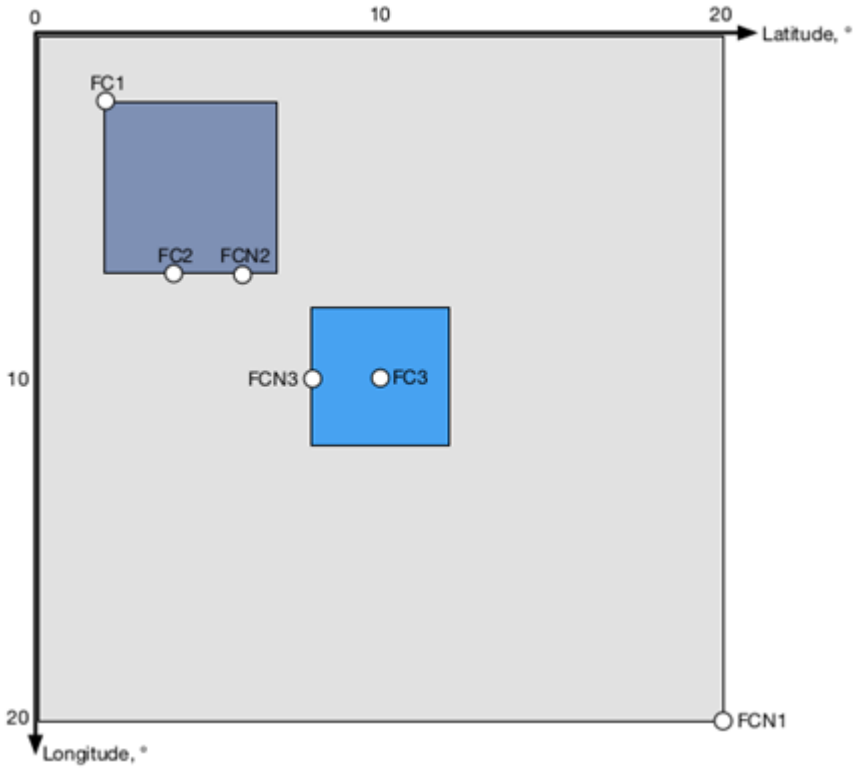

Рисунок 7 – Расположение устройств

Чтобы была возможность дать оценку, надо определить запросы приложения, состоящие из набора задач и продолжительности приложения, которые будут запрашиваться при управлении FCN и развернуто в системе.

Выбранные приложения предназначены для отображения реализованных функциональностей и механизмов, а также для оценки системы с отношением к метрикам. Приложение запрашивает отправлять в систему данные, соответствующие следующим условиям:

– запрошенные типы обслуживания туманности должны соответствовать типам услуг устройств туманности;

– запрашиваемые облачные службы должны быть перенаправлены в репозиторий Docker Hub с префиксом «fogframe /» перед запросом;

– все поля приложения должны быть заполнены в соответствии с примерным сценарием.

Даже если выполнение приложения соответствует указанным условиям, приложение может выйти из строя.

Возможные причины: (1) перегружена облачная среда OpenStack, (2) исчерпаны плавающие IP-адреса, (3) туманность перегружена. Число развертываемых облачных виртуальных машин теоретически неограничено, однако на практике он ограничен доступными облачными ресурсами и ограничением плавающих IP-адресов.

Конкретные приложения, которые могут использоваться при оптимизации оценки, следующие:

1. Приложение для обработки данных с показаниями датчиков (application1).

Задачи:

– (Service Key: temp-hum, Service Type: t1, Amount: 5);

– (Service Key: busy-image, Service Type: t2, Amount: 8);
– (Service Key: busy-image, Service Type: t3, Amount: 26).
Продолжительность: 5минут.
2. Приложение обработки данных (application2).
Задачи:
– (Service Key: busy-image, Service Type: t3, Amount: 5 to 80).
Продолжительность: 5 минут.
3. Приложение для обработки данных Cloud-Fog (application3).
Задачи:
– (Service Key: busy-image, Service Type: t3, Amount: 15);
– (Service Key: cloud-service, Service Type: t4, Amount: 15).
Продолжительность:1 минута.
4. Изменение данных, обрабатываемых приложением (application4).
Задачи:
– (Service Key: busy-image, Service Type: t1;
– Amount: according to input function);
– (Service Key: busy-image, Service Type: t3;
– Amount: according to input function).
Продолжительность: между 1 и 5 минутами.

Заключение. В современной сетевой среде при реализации процедур масштабирования необходимо проводить большое число операций по изменению настройки сетевых устройств. Планирование данных операций должно учитывать взаимные зависимости между узлами сети, аппаратными и программными ограничениями устройств коммутации и маршрутизации, особенности внутрисетевых политик информационной безопасности. Статическое решение данной задачи создает условия, когда сеть может выйти из рабочего состояния или появится уязвимость в ее инфраструктуре при минимальном изменении состава оборудования.

В условиях использования IoT-устройств в сети будет постоянно происходить подключение новых устройств и отключение старых. Обеспечение информационной безопасности в динамически изменяемых сетевых средах может быть обеспечено с использованием технологий, описанных в данной статье.

Литература

1. Воруев, А.В. Изменение подходов к безопасной загрузке операционных систем / А.В. Воруев, В.И. Рагин, А.И. Кучеров, В.Д. Левчук // Известия Гомельского государственного университета имени Ф. Скорины. – 2015. – № 6 (93). – С. 53–59.

2. Колаиб, С.М. Помехи и потери сигнала в оптоволоконной среде / С.М. Колаиб, А.В. Воруев // Актуальные вопросы физики и техники : материалы VII Республиканской научной конференции студентов, магистрантов и аспирантов, Гомель, 25 апреля 2018 г. : в 3-х ч. / Гомельский государственный университет им. Ф. Скорины ; редкол. : Д.Л. Коваленко (гл. ред.) [и др.]. – Гомель : ГГУ им. Ф. Скорины, 2016. – Ч. 2. – С. 70.

3. Репозиторий учебных материалов Cisco Netacad. CCNA Routing and Switching [Электронный ресурс]. – Режим доступа : https://www.netacad.com/. – Дата доступа : 01.10.2018.

[1]Гомельский государственный
университет им. Ф. Скорины

[2]Белорусский государственный университет
информатики и радиоэлектроники

Поступила в редакцию 09.11.2018