Система защищенной корпоративной связи для металлургического предприятия

УДК 654

А. Б. Маховиков,
*декан факультета фундаментальных и гуманитарных дисциплин,
доцент,
канд. техн. наук,
эл. почта: amakhovikov@spmi.ru*

С. Б. Крыльцов,
*ассистент кафедры информационных систем и вычислительной техники,
эл. почта: kryltsov_sb@pers.spmi.ru*

К. В. Матрохина,
*аспирант кафедры информационных систем и вычислительной техники,
эл. почта: matrokhina_kv@pers.spmi.ru*

В. Я. Трофимец, *профессор кафедры информационных систем и вычислительной техники,
докт. техн. наук,
профессор,
эл. почта: trofimets_VYa@pers.spmi.ru*

*Санкт-Петербургский горный университет,
Санкт-Петербург, Россия*

Рассмотрено применение систем видео-конференц-связи для управления промышленными предприятиями, в том числе металлургическими. Эти системы позволяют существенно снизить затраты на проведение совещаний, связанные с командированием сотрудников. Их особенно активно начали использовать в период пандемии Covid-19. Однако все существующие системы не учитывают особенности корпоративной сетевой инфраструктуры. Сложные системы связи, состоящие из различных сегментов, а также симметричных и асимметричных каналов с множеством параметров, которые могут неоднократно варьироваться, создают проблемы для построения эффективных VoIP-решений, особенно при развитии услуг видео-конференц-связи. Поскольку типичный подход к обеспечению конфиденциальности передачи голосовых и видеоданных по сетям связи заключается в том, что каждый маршрут между отправляющей и принимающей сторонами считается общедоступным, он теряет преимущества управления топологией сети в корпоративном секторе. В то же время типичная клиент-серверная архитектура коммуникаций по корпоративным IP-сетям показывает меньшую эффективность по сравнению с одноранговыми коммуникациями из-за меньшего использования знаний сетевой инфраструктуры. Авторы предлагают новый подход к построению систем защищенной корпоративной связи, в основе которого не клиент-серверная архитектура, а архитектура p2p , что позволяет учитывать структуру корпоративной сети предприятия, в том числе металлургического, разгрузить внешний и внутренние каналы связи и снизить вычислительные затраты на уровне хостов.

Ключевые слова: *коммуникационные системы, IP-телефония, распределенные коммуникации, p2p-сети, моделирование, видеоконференция.*

DOI: *10.17580/tsm.2023.04.01*

Введение

До недавнего времени существовали значительные трудности с внедрением информационных технологий в металлургическую отрасль, что было обусловлено рядом причин: недостаточным финансированием, недооцениванием роли информационных технологий (основные средства, как правило, вкладывали в технологическое производство), масштабом предприятия, бюрократическими проволочками.

Однако в настоящее время металлургическая отрасль достаточно активно запускает проекты, связанные с внедрением новых информационных технологий в производство. Прежде всего это связано с наметившимся подъемом в реальном секторе отечественной экономики, в том числе в металлургии. Так, например, ПАО «ГМК «Норильский никель», завершило внедрение информационной системы SAP Audit Management в главном офисе, после чего приступило к применению этой системы в семи подразделениях внутреннего контроля и аудита компаний Норникеля [1]. Все чаще специалисты, отвечающие за внутренний аудит, при проведении проверок уделяют особое внимание использованию инструментов data-аналитики.

В рамках процесса внедрения цифровых технологий металлургическая компания ПАО «Полюс» на таких объектах добычи, как месторождения Олимпиадинское, Наталкинское, создает инфраструктуру беспроводной широкополосной связи, что позволяет обеспечить надежную передачу данных с эксплуатируемых активов компании в систему управления на диспетчерских пунктах. Расширяется дистанционное управление работой добывающего оборудования. Оператор диспетчерской может руководить самоуправляемыми транспортными средствами и оборудованием, в том числе грузовиками, экскаваторами и буровыми установками [2]. Для решения задачи автоматического управления подвижными объектами необходимо совершенствовать математический аппарат систем управления, в частности калмановскую фильтрацию [3], и развивать методы имитационного моделирования [4].

Для эффективной работы и выполнения программы по производству цветных металлов компании внедряют автоматизированные системы контроля технологических параметров работы оборудования и применяют современные инженерные средства контроля [5, 6]. Например, компания «РУСАЛ» в рамках цифровой трансформации систем управления провела испытания и внедрила следующие инструменты автоматизированного управления технологией: автономная система управления параметрами на основе BigData, динамический цифровой двойник процесса (виртуальный электролизер) [7].

ПАО «Полюс» подошла к вопросу цифровизации системно. В 2022 г. была создана цифровая компания «Полюс Диджитал», основной деятельностью которой является разработка, внедрение и адаптация цифровых ИТ-решений — от мобильных приложений для производственных задач до информационных систем, помогающих принимать управленческие решения.

Пандемия Covid-19, начавшаяся в 2020 г., нанесла урон минерально-сырьевому комплексу в целом, в том числе и сегменту подготовки специалистов. Эффективным средством борьбы с возникшими неопределенностями стало внедрение и расширение применения цифровых технологий в различных сферах [8]. Так, пандемия обусловила необходимость значительных изменений в организации производственного процесса на всех предприятиях минерально-сырьевого комплекса [9, 10], в том числе и на металлургических [11], выразившихся в существенном расширении использования информационных систем. Например, если ранее к системам видео-конференц-связи обращались изредка, в частности для снижения командировочных расходов при управлении филиалами, то теперь предприятия вынуждены были их использовать постоянно и повсеместно, так как от очного формата проведения совещаний в условиях пандемии пришлось оказаться.

Несмотря на то что системы для проведения видеоконференций достаточно давно широко применяют в различных отраслях, многие металлургические компании до начала 2020 г. не внедряли их. Основная причина — высокие материальные затраты и устойчивая традиция проводить совещания в очном формате. Сегодня видеоконференции стали привычным атрибутом работы филиалов металлургических предприятий.

Таким образом, в настоящее время одной из актуальных задач является снижение командировочных расходов сотрудников за счет активного применения в филиалах металлургических предприятий систем видео-конференц-связи.

Также в условиях пандемии Covid-19 возникла необходимость усиления мер по обеспечению информационной безопасности. Ужесточились требования безопасности по использованию удаленных компьютеров и устройств при проведении аудио- и видеоконференций, а также контроль в этой сфере. В компании «Норникель» продолжается реализация запланированных мероприятий и программ по защите корпоративных информационных систем и автоматизированных систем управления технологическими процессами. ПАО «Полюс» для снижения рисков нарушения информационной безопасности совершенствует системы контроля подключений к корпоративной сетевой инфраструктуре, повышая осведомленность работников и подрядчиков в части информационной безопасности.

Ряд компаний в связи с ограничениями, исключающими возможность очного обучения, начали активно использовать дистанционные формы обучения персонала. В частности, ПАО «ГМК «Норильский никель» запустило более 150 различных образовательных курсов на платформе «Академия Норникель». В 2021 г. компанией был разработан курс «Основы цветной металлургии», который успешно прошли более 700 непрофильных специалистов. Все это стало возможным благодаря активному применению цифровых технологий и дистанционной форме обучения (всего в онлайн-мероприятиях приняли участие более 75 тыс. человек) [1].

Все системы видео-конференц-связи построены по одному принципу, являются универсальными и не учитывают особенности корпоративной сетевой среды. Передача голосовых сообщений по интернет-протоколу (VoIP)[1] в настоящее время организована в соответствии с установленной системой стандартов, разработанных как международными организациями, так и частными компаниями. Несмотря на название, текущие стандарты VoIP также охватывают потоковые видеосообщения, файлы и текстовые сообщения. Развитие интернета делает интернет-протокол (IP, Internet Protocol) фактически стандартным для маршрутизации между компьютерами, подключенными как к локальным, так и к глобальным сетям [12]. Публичный обмен мгновенными сообщениями и вызовы VoIP имеют несколько отличительных особенностей: они доставляются по небезопасным сетям, поддерживаются через серверы поставщиков.

Эти особенности обусловливают необходимость защиты данных, передаваемых по маршруту точка – точка, в целях обеспечения конфиденциальности, поскольку предполагается, что соединения поддерживаются по небезопасным каналам [13–15]. Надежность системы связи VoIP зависит от многих факторов и должна обеспечивать индивидуальную связь между участниками [16–18]. В коммуникационных приложениях, особенно при реализации в сотовых сетях, обеспечение надежности становится серьезной проблемой, так как надежность передачи пакетов в сотовых сетях существенно зависит от мощности сигнала и загруженности станции, пропускной способности канала и т. д. [19–21]. Таким образом, наличие надежного алгоритма

[1] VoIP — Voice over Internet Protocol, передача голосовых сообщений по интернет-протоколам.

передачи данных по сотовым сетям следует рассматривать как характеристику системы связи [22–24]. Можно перечислить несколько аспектов обеспечения безопасной и надежной связи между абонентами:

- надежный сквозной алгоритм шифрования [25, 26];
- кроссплатформенность (включая мобильные платформы);
- контроль обработки данных каждым узлом системы, участвующим в VoIP-трафике;
- простота применения для пользователей и системных администраторов [27];
- надежные протоколы передачи данных, адаптированные к сетям с нестабильным качеством связи [28, 29].

Настоящее исследование выполнено в целях разработки и моделирования новой структуры системы видео-конференц-связи для использования корпоративными клиентами, в том числе металлургическими предприятиями России.

Существенной проблемой при реализации современных систем VoIP является обеспечение конфиденциальности при передаче мультимедийного трафика: голосовых, видео- и текстовых данных. Пакеты VoIP часто передают по сетям общего назначения, таким как магистрали провайдеров, беспроводные локальные сети, сети LTE[2] операторов мобильной связи [30, 31].

Пакеты данных в таких сетях могут быть перехвачены на любом промежуточном узле локальной и глобальной сети, что обуславливает необходимость использования шифрования для обеспечения требований конфиденциальности сеансов связи [32]. Кроме того, инфраструктура Ethernet (семейство проводных компьютерных сетевых технологий) подвержена атакам, направленным на отказ в обслуживании промежуточного сетевого или абонентского оборудования. Дополнительной проблемой при обеспечении защиты VoIP-трафика является необходимость обеспечения минимальной задержки при передаче потоковой аудио- и видеоинформации [33].

Технологии качества обслуживания являются неотъемлемой частью сетей VoIP. Ограничение частоты дискретизации аудиопотока, а также битрейта (скорости потоковой передачи данных) при сжатии видеоданных [34, 35] на уровне протокола позволяет стандартизировать требования к полосе пропускания, однако потери пакетов и задержки доставки пакетов оказывают существенное влияние на качество сеанс связи [36, 37]. Задержку между приемом и доставкой пакетов вызывают шифрование трафика, длина маршрута между терминалами, нестабильность соединения и загруженность линий передачи данных [38, 39].

В последних двух случаях типичной проблемой становится джиттер (от англ. jitter — дрожание) — изменение качества воспроизводимого на устройстве получателя аудио- и/или видеопотока из-за изменения времени доставки пакета [40, 41]. Для работы в условиях джиттера на уровне стека (комбинации) протоколов VoIP можно изменять маршрут доставки пакетов или ограничивать размер передаваемых данных с предсказуемым ухудшением качества связи [42].

В настоящей статье основное внимание уделено разработке модели системы аудио- и видеосвязи, которая настраивает существующую корпоративную сетевую инфраструктуру для обеспечения распределенной связи между одноранговыми узлами за счет использования свойств сетевой функциональности.

Материалы и методы исследования

Корпоративная сетевая инфраструктура

Поскольку интернет работает как огромная IP-сеть и, следовательно, все промежуточное сетевое оборудование маршрутизирует IP-сети, IPv4 и IPv6 (4-я и 6-я версии интернет-протоколов соответственно) фактически являются стандартами для организации связи [43, 44]. Некоторая свобода в построении голосовой и видеосвязи появляется на транспортном уровне модели OSI[3] [45, 46].

Протоколы TCP[4] и UDP[5] являются хорошо известными стандартами для передачи пакетов данных, позволяя хосту с определенным IP-адресом поддерживать отдельные подключения к различным приложениям на основе номера порта приложения. Хотя TCP поддерживает гарантированную передачу пакетов, эти механизмы связаны с огромными накладными расходами, особенно в сотовых сетях, и поэтому не подходят для передачи голоса и видеоданных в реальном времени [47].

Напротив, UDP указывает только исходные и конечные порты и данные для проверки целостности дейтаграммы, поэтому не гарантирует получения дейтаграмм или их серии в нужном порядке. Благодаря простоте дейтаграммы UDP она подходит в качестве идеального строительного блока для поддержки аудио- и видеопотоков без накладных расходов на транспортном уровне, в то время как восстановление фактических данных из дейтаграмм может быть перенесено на прикладной уровень.

Предлагаемая модель описана на примере сетевой инфраструктуры, представленной на **рис. 1**.

Она включает следующие компоненты: промежуточное сетевое оборудование: *1* — пограничный маршрутизатор (ER, Edge Router); *2* — маршрутизатор отдела

[2] LTE, Long-Term Evolution — стандарт беспроводной высокоскоростной передачи данных для мобильных телефонов и др.

[3] OSI — Open System Interconnection, модель взаимосвязи открытых систем.

[4] TCP — Transmission Control Protocol, протокол управления передачей; обеспечивает виртуальные соединения между пользовательскими приложениями и гарантирует точную доставку данных.

[5] UDP — User Datagram Protocol, протокол передачи дейтаграмм пользователя; служит для быстрого обмена специальными сообщениями (дейтаграммами) без гарантии доставки.

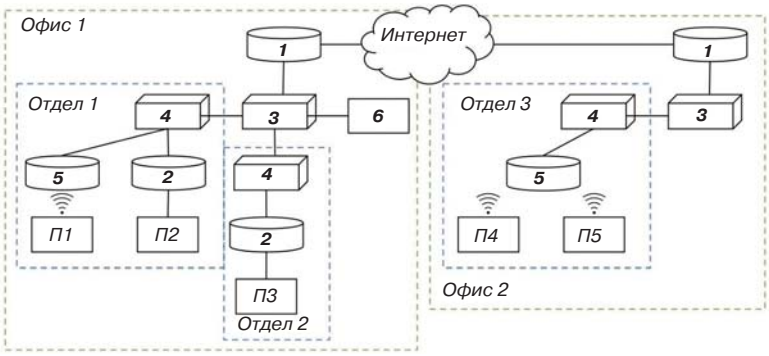

Рис. 1. Рассматриваемая инфраструктура корпоративной телекоммуникационной сети

(DR, Designated Router); *3* — пограничный коммутатор (ESW, Edge Switch); *4* — коммутатор отдела (DSW, Distribution Switch); *5* — беспроводная точка доступа (DAP-5); *6* — административная единица (AU, Administrative Unit), которая может быть аналогом равноправного устройства или выделенного сервера; П1– П5 — устройства ПИР (пассивный инфракрасный датчик, Peer Devices).

Фрагментированное окно

Фрагменты аудио- и видеопотока могут появляться на приемнике в различном порядке, а некоторые фрагменты вовсе могут отсутствовать. На это влияют множество факторов, в том числе:

- динамическая маршрутизация промежуточного сетевого оборудования приводит к тому, что части сегментов передаются по разным маршрутам [48–50];
- мгновенное переключение на другой тип сети является причиной того, что части сегмента выбирают разные маршруты к приемнику, например переключение между сотовой сетью и сетью Wi-Fi [51];
- переполнение буфера промежуточного сетевого оборудования может привести к отсутствию пакетов;
- сбои в сети могут вызвать потерю пакетов [52, 53].

Для решения указанных проблем необходимо, чтобы приложение VoIP поддерживало правильный порядок фрагментов данных, обеспечивая при этом непрерывный поток данных. Самый простой способ поддерживать правильный порядок дейтаграмм — добавить поле последовательности к полезной нагрузке дейтаграммы [54]. Поскольку задержка дейтаграмм может варьироваться или некоторые дейтаграммы могут отсутствовать из-за указанных проблем, упорядочивание и ожидание фрагментов данных становится проблемой баланса, которая обычно решается с помощью окна данных.

Принимающая сторона поддерживает окно данных определенной длины, в течение которой она ожидает возможного поступления дейтаграмм с данными. Как правило, если какие-то аудиофрагменты отсутствуют, они опускаются при восстановлении сигнала, однако в зависимости от соотношения между размером окна и средней задержкой дейтаграммы можно запросить отсутствующие дейтаграммы у их отправителя.

Минимальное условие того, чтобы такой подход был выгодным, — длина окна более чем в 2 раза превышает среднюю задержку дейтаграммы. Основным триггером для запроса отсутствующих дейтаграмм является получение дейтаграмм в неправильном порядке. В зависимости от фиксированного размера полезной нагрузки дейтаграммы и размера окна счетчик циклической последовательности может быть уменьшен до 1 для 2 байтов.

Поведение окна может быть последовательным: окно применяется к входным данным пошагово и поэтому представляет собой самоочищающийся или скользящий буфер, что соответствует циклическому буферу. Последнее позволяет захватывать больше дейтаграмм, так как пропуск недостающих фрагментов происходит только в конце окна. Окно вносит постоянную задержку в связь VoIP, и его размер должен быть минимизирован в зависимости от распределения задержки дейтаграмм.

Политики выборочного маршрута

К корпоративной коммуникационной сети могут быть подключены все участники внутри одного здания, где традиционный подход к медиакоммуникациям в режиме реального времени имеет наибольшее число недостатков и предполагается, что каналы между участниками являются общедоступными и, следовательно, небезопасными. Однако распространенным случаем является сеть связи, объединяющая несколько ответвлений, как это было описано в разд. «Корпоративная сетевая инфраструктура».

В таком случае наиболее выгодным способом является использование свойств маршрута для повышения качества передачи аудио- и видеоданных. Маршруты между одноранговыми узлами могут различаться по пропускной способности, задержке, типу соединения и уровню безопасности. В современных протоколах маршрутизации пропускная способность и задержка используются для расчета так называемого расстояния между маршрутизаторами, что позволяет ранжировать разные маршруты к одному и тому же хосту и выбирать маршрут с наименьшим расстоянием.

Этот подход эффективен в отношении магистральных сетей поставщиков телекоммуникационных услуг, но плохо масштабируется для гораздо меньших сетей филиалов, где типы соединений более разнообразны. Например, такие протоколы не учитывают беспроводные соединения, так как их качество существенно зависит от расстояния и наличия препятствий между сетью и оборудованием партнера.

Поэтому предлагается ввести политики выборочного маршрута, применяемые к каждому маршруту между одноранговыми узлами. Такой маршрут характеризуется рядом параметров, включая тип соединения, пропускную способность, задержку и безопасность. Часть

параметров предполагается устанавливать административно, например параметры безопасности. Опишем политики маршрутизации, применяемые к сети, рассмотренной на **рис. 2**.

Топология сети филиала заносится сетевыми администраторами в блок 6 (AU). ПИР 3 (П3) активно передает информацию о задержке маршрутов каждому ПИР в блок 6(AU), который, в свою очередь, генерирует управляющие сигналы для одноранговых узлов в зависимости от топологии сети и данных измерений задержки.

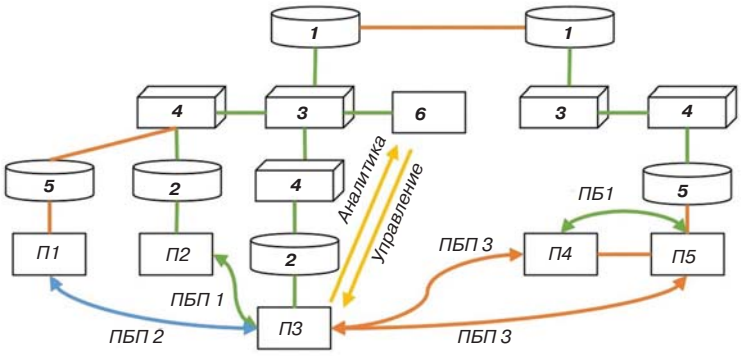

Рис. 2. Политики выборочного маршрута, применяемые ко всем маршрутам ПИР 3:
зеленые — безопасные, оранжевые — небезопасные (обозначения см. рис. 1)

Как видно, П2 подключен к П3 через проводное сетевое оборудование, и этот маршрут рассматривается администраторами как безопасный, что гарантируют правильно настроенные маршрутизаторы и параметры коммутатора, например управления портами, привязки MAC ACL (Access Control Lists, списки контроля доступа), а также физически закрепленного оборудования. Для таких случаев была введена Политика 1 (см. рис. 2), включающая параметры для полного отключения защиты видео- и аудиоданных. Это позволяет снизить расходы, связанные с шифрованием дейтаграмм. При этом пропускная способность каналов фиксирована за счет прямого проводного соединения, а значит с учетом измерений латентности позволяет уменьшить размер окна фрагментации.

П1 подключается к П3 через проводное и беспроводное сетевое оборудование, при этом все оборудование контролируется сетевыми администраторами филиала. Поэтому его политика отличается от Политики 1 типом соединения и параметрами безопасности, которые зависят от уровня безопасности беспроводного соединения между П1 и точкой доступа. Например, если точка доступа защищена с помощью технологии WPA2 (Wi-Fi Protected Access[6]), трафик между точкой доступа и каждым клиентом также защищен, поэтому дополнительная защита не требуется. Однако если точка доступа предполагает гостевую сеть, шифрование дейтаграмм должно происходить на стороне одноранговых узлов. Знание типа беспроводного соединения позволяет учитывать показатели качества беспроводного соединения для изменения размера окна с обеих сторон.

П4 и П5 расположены в разных филиалах и поэтому подключены через интернет к П1. Маршрут считается незащищенным, поэтому все меры безопасности применяются в соответствии с Политикой 3. При этом канал между П4 и П5 является локальным, и, следовательно, потоки аудио- и видеоданных между ними передаются в соответствии с Политикой 1.

[6]WPA — стандарт безопасности для вычислительных устройств с беспроводным подключением к интернету.

Результаты исследований

Мультиплексирование видеоданных

Реализация p2p-взаимодействия (от англ peer-to-peer networking, равный к равному) в корпоративных VoIP-системах сопряжена с рядом проблем. Для примера структура сложного p2p-кейса показана на рис. 1. В таких системах каждый участник сети отправляет на сервер поток данных, поступивший с видеокамеры или рабочего стола/окна работающего приложения. Аудио- и видеопотоки мультиплексируются на сервере. Мультиплексированный видеопоток — высококачественный видеопоток от активного докладчика, смешанный с набором низкокачественных сжатых видеопотоков с устройств других участников. Затем мультиплексированный поток направляется каждому участнику видеоконференции.

В условиях p2p-архитектуры для формирования видеопоследовательности, включающей как основного выступающего, так и всех участников видеоконференции, каждый пользователь должен передавать свой видеопоток всем остальным пользователям. Таким образом, при участии в видеоконференции N сотрудников клиент формирует N-1 исходящих потоков аудио- и видеоданных и получает N-1 предоставленных потоков. Даже при условии сжатия видеопотоков на устройстве клиента, который на данный момент не является активным, уже при 10 одновременных подключениях такой подход создает значительную нагрузку как на корпоративную сеть, так и на устройства участников.

По результатам теоретического анализа предполагается возможность организации p2p-взаимодействия пользователей. В процессе апробации сформулированной гипотезы был предложен новый подход к построению системы p2p VoIP, основанный на организации пользователей системы в сети со смешанной топологией. Согласно этому подходу, каждый участник сети выполняет двунаправленное мультиплексирование аудио- и видеопотоков, формируя исходящий поток данных для входящего потока данных и добавляя аудио- и видеопоток, захваченный с устройства участника.

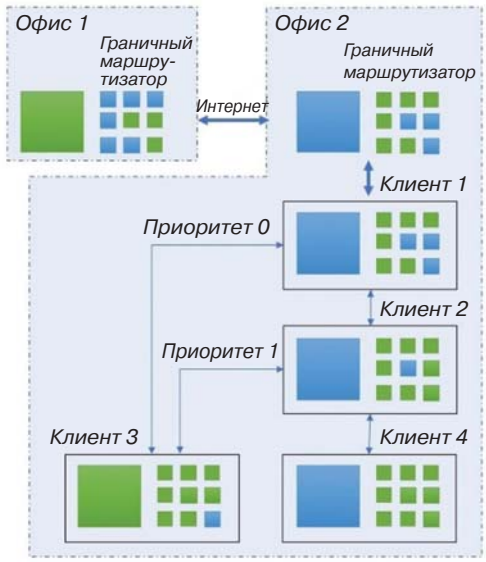

Рис. 3. Схема формирования видеоряда

Схема формирования видеоряда в соответствии с этим подходом представлена на **рис. 3**.

В системе, разработанной в соответствии с предложенным подходом, каждый участник сети транслирует и принимает видеопоток только от соседних участников системы. Таким образом, структура сети позволяет сократить объем входящего и исходящего потоков видеоданных у каждого участника до двух. Возможность уменьшения числа узлов системы диктуется сетевой инфраструктурой компании. В ходе исследования было выявлено, что в реальных условиях полная линеаризация структуры сети возможна только при малом числе участников, и, несмотря на существующие конфигурации p2p-сетей, минимизировать число взаимосвязанных узлов можно с помощью информации о сетевой инфраструктуре.

По результатам теоретических исследований были сформулированы два подхода к построению логических маршрутов между участниками сети. Первый заключается в использовании сетевой инфраструктуры для оптимизации маршрутов между участниками. Для реализации такого подхода сеть должна включать административную единицу, содержащую графический интерфейс, позволяющий описать оборудование, топологию сети (параметры соединений между узлами сети), а также параметры сети, передающей трафик ее участников. По сформированному описанию решается задача линеаризации графа связей для известных узлов сети, что позволяет им составить карту логических маршрутов, уменьшающую число соседних участников сети, и определить их приоритетность.

Второй подход заключается в формировании набора инструментов для настройки изменений в структуре сети и адаптации к ним (включая подключение и отключение пользовательских устройств), что в целом характерно для p2p-сетей. В рамках этого подхода выделяются основные метрики, такие как качество и пропускная способность соединения между соседними узлами, аппаратные параметры устройств участников, использующиеся для своевременной реорганизации топологии и назначения точек мультиплексирования видеоданных в случае их изменения.

Моделирование политик маршрутизации и эффективности размера входного окна

Пошаговое моделирование проводили в компьютерной модели сети (см. рис. 1), построенной с помощью языка Python. Модель использовали для доказательства возможности применения правильной маршрутизации, оптимизации политик маршрутизации и проверки расчетов размера окна фрагментации.

В компьютерной модели для имитации поведения реальной сети применяли методы теории графов. Ребра графа содержат настраиваемые параметры связи между узлами сети в зависимости от типа связи. Каждое соединение вносит задержку в зависимости от использования его пропускной способности и случайности, генерируемой нормальным распределением с контролируемыми значениями.

Узлы графа, включая сетевое оборудование, представляют собой хосты[7]. В модели хосты вводят задержку только при применении преобразования данных, такого как шифрование дейтаграмм и кодирование/декодирование аудио- и видеоинформации. Предполагается, что сетевое оборудование не вносит никаких задержек в доставку данных, так как оно уже учтено при расчете ребер графа. ПИР также имеют настраиваемые параметры окна фрагментации, которые рассчитываются административной единицей (см. разд. «Фрагментированное окно»).

Параметры моделирования для узлов и маршрутов приведены в **таблице**.

Моделирование проводили с учетом двунаправленного видеопотока между каждым из трех маршрутов. Потоковые битрейты для П1, П2, П3, П5 составляли 5, 5, 3, 3 Мбит/с соответственно. С учетом параметров моделирования были получены следующие результаты.

Маршрут 1. Средняя потеря пакетов 0,15 %, общая задержка 2,04 мс, расчетный размер окна 20 мс, недоставленные кадры 0 %. Поскольку Маршрут 1 следует Политике 1, трафик передается в незашифрованном виде, а задержка полностью вызвана кодированием видеопотока и сетевым оборудованием. Общая задержка меньше, чем время между двумя видеокадрами, поэтому предполагаемый размер окна не вносит дополнительной задержки, но способен компенсировать потерю пакетов на маршруте.

Маршрут 2. Средняя потеря пакетов 1,58 %, общая задержка 5,51 мс, расчетный размер окна 20 мс, недоставленные кадры 0,021 %. Маршрут 2 вводит шифрование трафика и нестабильность беспроводного

[7] Хост — от англ. host, устройство, узел сети, работающей по принципу клиент – сервер.

Параметры моделирования для распределенной сети связи

Маршрутизатор 1 – Политика 1					Маршрутизатор 2 – Политика 2					Маршрутизатор 3 – Политика 3				
№ п/п	У/М	ВЛ	СПП	ПС	№ п/п	У/М	ВЛ	СПП	ПС	№ п/п	У/М	ВЛ	СПП	ПС
1	П3	15	–	–	1	КО – БТД	–	0,01	1	1	ПК – ПМ	–	0	1
2	П3 – МО	–	0,01	1	2	БТД	1	–	–	2	ПМ	1	–	–
3	МО	1	–	–	3	БТД – П1	–	3	0,15	3	ПМ – ПМ	–	1,5	0,02
4	МО – КО	–	0,01	1	4	П1	10	–	–	4	ПМ	1	–	–
5	ПК (М3)	1	–	–	5	–	–	–	–	5	ПМ – ПК	–	0	1
6	ПК – КО	–	0,01	1	6	–	–	–	–	6	ПК	1	–	–
7	КО (М2)	1	–	–	7	–	–	–	–	7	ПК – КО	–	–	1
8	КО – МО	–	0,01	1	8	–	–	–	–	8	КО	1	–	–
9	МО	1	–	–	9	–	–	–	–	9	КО – БТД	–	0,01	1
10	МО – П2	–	0,01	1	10	–	–	–	–	10	БТД	1	–	–
11	П2	15	–	–	11	–	–	–	–	11	БТД – П5	–	0,01	0,05
12	–	–	–	–	–	–	–	–	–	12	П5	25	–	–

Примечание. У/М — узел/маршрут; ВЛ — вычислительная латентность, мкс; СПП — средняя потеря пакетов, %; ПС — пропускная способность, Гбит; ПМ — пограничный маршрутизатор; МО — маршрутизатор отдела; ПК — пограничный коммутатор; КО — коммутатор отдела; БТД — беспроводная точка доступа; М — маршрутизатор.

соединения между П1 и точкой доступа. Это, в свою очередь, увеличивает общую задержку маршрута, а также увеличивает потери пакетов. Однако также применяется окно минимального размера, которое компенсирует почти все потери пакетов.

Маршрут 3. Средняя потеря пакетов 2,77 %, общая задержка 101,27 мс, расчетный размер окна 350 мс, недоставленные кадры 0,078 %. Маршрут 3 учитывает нестабильное интернет-соединение между офисами. Значительная часть латентности вызвана потоком через оборудование провайдера. Увеличенный размер окна компенсирует большую часть потерь пакетов, внося при этом дополнительную задержку.

Предложенная модель может быть использована для дальнейшего формирования набора протоколов распределенного обмена аудио- и видеоданными в целях применения в корпоративных сетях. Опуская вопросы кодирования, можно считать, что модель подходит для определения параметров маршрутизации и безопасности одноранговой связи по существующей сетевой инфраструктуре интернет-протокола.

Оценка экономической эффективности

Экономический эффект от применения систем, основанных на предлагаемом подходе, заключается в существенной разгрузке внешнего интернет-канала предприятия. Так, например, при использовании любой из существующих систем видео-конференц-связи, построенных на клиент-серверной архитектуре, и при нахождении сервера в публичной части сети Интернет исходящий поток данных составляет $N{\cdot}M$, где N — число клиентов в сети предприятия, а M — поток от каждого клиента. При применении предлагаемого подхода, если совещание проводится между филиалами, выступающий находится внутри сети данного филиала и в ней имеется хотя бы один слушатель, поток составляет $2{\cdot}M$, а если вне — M. Таким образом, выигрыш по загрузке канала равен $N/2$ или N раз и тем существеннее, чем больше пользователей участвуют в конференции. Можно отметить, что если совещание проводится между подразделениями данного филиала, то при использовании рассмотренной архитектуры внешний канал не задействуется.

Кроме того, если при традиционном подходе на каждом хосте необходимо декодировать и воспроизводить N потоков данных, то при предлагаемом — максимум 2. Это снижает требования к производительности компьютерной техники, используемой для проведения совещаний, что особенно актуально в настоящее время, когда введенные против России санкции вызывают сложности с закупками новой компьютерной техники.

Косвенной характеристикой эффективности предлагаемого подхода к построению систем защищенной корпоративной связи является их независимость от возможного отключения из-за введенных санкций, как это случилось с Cisco Webex и Zoom, а также устойчивость к хакерским атакам из-за отсутствия в архитектуре центрального сервера.

Заключение

В статье рассмотрено применение систем защищенной корпоративной связи для управления металлургическими предприятиями и показана острая необходимость расширения их применения, что обусловлено как невозможностью организации очных совещаний в условиях пандемии Covid-19, так и значительным снижением затрат на командирование сотрудников для участия в очных совещаниях. Также предложен новый подход к построению корпоративных VoIP-систем. Подчеркивается, что, хотя ИТ-индустрия переходит на распределенные системы, все еще существуют проблемы при организации видеоконференций p2p из-за

значительных накладных расходов, связанных с несколькими одновременными видеопотоками, передаваемыми по корпоративной сети.

Предлагаемый подход заключается в линеаризации соединений между одноранговыми узлами, что ограничивает число одновременно обрабатываемых видеопотоков и, следовательно, снижает вычислительные затраты и накладные расходы на передачу как для сети, так и для пользовательских устройств.

Этот подход позволяет использовать преимущества систем p2p и, по крайней мере, частичное знание сетевой инфраструктуры для повышения качества обслуживания систем VoIP, что снижает требования как к каналам связи, так и к производительности пользовательских устройств. Моделирование для проверки эффективности таких улучшений проводили на примере регулируемого размера буфера на клиентских устройствах. Предоставленные данные моделирования показывают сходимость результатов с утверждениями, сформулированными в разд. «Материалы и методы исследования». Сочетание регулируемого скользящего окна с политиками выборочной маршрутизации позволяет уменьшить задержку потоковой видеоинформации по стабильным каналам, обеспечивая при этом необходимую безопасность и стабильность частоты кадров по нестабильным каналам.

Дальнейшие исследования будут направлены на реализацию более конкретного моделирования, которое позволит детально оценить накладные расходы на уровне каждого узла корпоративной сетевой инфраструктуры, включая потерянные фрагменты потока на клиентских и сетевых устройствах. Также предполагается на основе описанного подхода разработать прототип системы корпоративной защищенной видеоконференц-связи и организовать его пробную эксплуатацию на одном из металлургических предприятий России.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

См. англ. блок

ЦМ

Tsvetnye Metally. 2023. No. 4. pp. 5–13
DOI: 10.17580/tsm.2023.04.01

SECURED COMMUNICATION SYSTEM FOR A METALLURGICAL COMPANY

Information about authors
A. B. Makhovikov, Dean of the Faculty for Basic Sciences and the Humanities[1], Associate Professor, Candidate of Technical Sciences,
e-mail: amakhovikov@spmi.ru
S. B. Kryltsov, Assistant Lecturer at the Department of Information Systems and Computers[1], e-mail: kryltsov_sb@pers.spmi.ru
K. V. Matrokhina, Postgraduate Student at the Department of Information Systems and Computers[1], e-mail: matrokhina_kv@pers.spmi.ru
V. Ya. Trofimets, Professor at the Department of Information Systems and Computers[1], Doctor of Technical Sciences, Professor
e-mail: trofimets_VYa@pers.spmi.ru

[1]Saint Petersburg Mining University, Saint Petersburg, Russia.

Abstract
This paper examines the use of videoconferencing systems for production (metallurgical) site management. Such systems help achieve a significant reduction in costs associated with meetings and related business trips. Application of such systems was especially wide-spread during the Covid-19 pandemic. However, none of the existing systems takes into account certain features typical of the corporate network infrastructure. Sophisticated communication systems consisting of various segments, as well as of symmetric and asymmetric channels with multiple parameters, which may vary numerous times, make it more difficult to build efficient VoIP solutions, especially when growing videoconferencing services. As the typical approach to securing confidentiality when transmitting voice and video data across communication networks implies that every sender-receiver route is considered public, it loses the benefits of network topology control in the corporate sector. At the same time, the typical client-server architecture across corporate IP networks demonstrates lower performance when compared with peer-to-peer networking because of lesser use of network infrastructure knowledge. The authors propose a new approach to building secured corporate communication systems, which does not have at its basis the client-server architecture but rather a p2p architecture. The latter enables to take into account the existing corporate network structure (including that of a metallurgical company), unload external and internal communication channels and reduce the computing costs at the host level.
Key words: communication systems, VoIP, distributed communications, p2p networks, modelling, videoconference.

References
1. Yearly report. Nornickel. Paving the way to carbon-free future. Moscow, 2021. 181 p.
2. Yearly report. Polyus PJSC. Moscow, 2021. 52 p.
3. Brigadnov I., Lutonin A., Bogdanova K. Error State Extended Kalman Filter Localization for Underground Mining Environments. *Symmetry*. 2023. Vol. 15, No. 2. p. 344. DOI: 10.3390/sym15020344.
4. Voronin V. A., Nepsha F. S. Simulation of the electric drive of the shearer to assess the energy efficiency indicators of the power supply system. *Journal of Mining Institute*. 2020. Vol. 246. pp. 633–639. DOI: 10.31897/PMI.2020.6.5.
5. Cabascango V. E. Q., Bazhin V. Y., Martynov S. A., Pardo F. R. O. Automatic Control System for Thermal State of Reverberatory Furnaces in Production of Nickel Alloys. *Metallurgist*. 2022. Vol. 66. pp. 104–116.
6. Martynov S. A., Bazhin V. Yu., Petrov P. A. A digital control system designed for ore thermal furnaces producing metallurgical silicon. *Tsvetnye Metally*. 2021. No. 1. pp. 70–76. DOI: 10.17580/tsm.2021.01.08.
7. Yearly report. RUSAL. Moscow, 2021. 271 p.
8. Gerasimova I. G., Pushmina S. A., Carter E. V. A fresh look at blended learning: boosting motivation and language acquisition in an ESP course for engineering students. *Global Journal of Engineering Education*. 2022. Vol. 24, No 1. pp. 52–58.
9. Litvinenko V. S. Digital economy as a factor in the technological development of the mineral sector. *Natural Resources Research*. 2020. Vol. 29. pp. 1521–1541.
10. Razmanova S. V., Andrukhova O. V. Oilfield service companies as part of economy digitalization: assessment of the prospects for innovative development. *Journal of Mining Institute*. 2020. Vol. 244. pp. 482–492. DOI: 10.31897/pmi.2020.4.11.
11. Boikov A., Payor V. The Present Issues of Control Automation for Levitation Metal Melting. *Symmetry*. 2022. Vol. 14, No. 10. 1968. DOI: 10.3390/sym14101968.
12. Barry M. A., Tamgno J. K., Lishou C., Ciss M. B. QoS impact on multimedia traffic load (IPTV, RoIP, VoIP) in best effort mode. *20th International Conference on Advanced Communication Technology (ICACT)*. 2018, February. pp. 694–700.
13. He W., Golla M., Padhi R., Ofek J., D rmuth M. et al. Rethinking access control and authentication for the home internet of things (IoT). *27th Security Symposium (Security 18)*. 2018. pp. 255–272.
14. Jiang Y., Tang S. An efficient and secure VoIP communication system with chaotic mapping and message digest. *Multimedia Systems*. 2018. Vol. 24, No. 3. pp. 355–363.
15. Nu o P., Su rez C., Su rez E., Bulnes F. G., delaCalle F. J. et al. A diagnosis and hardening platform for an asterisk VoIP PBX. *Security and Communication Networks*. 2020. DOI: 10.1155/2020/8853625.

16. Nazih W., Elkilani W. S., Dhahri H., Abdelkader T. Survey of countering DoS/DDoS attacks on SIP based VoIP networks. *Electronics*. 2020. Vol. 9, No. 11. 1827. DOI: 10.3390/electronics9111827.
17. Neves F., Soares S., Assuncao P. A. A. Optimal voice packet classification for enhanced VoIP over priority-enabled networks. *Journal of Communications and Networks*. 2018. Vol. 20, No. 6. pp. 554–564.
18. Politis A. C., Hilas C. S. CTS-to-self as a Protection Mechanism for the No Acknowledgment Protocol in VoIP WLANs. *Contemporary Engineering Sciences*. 2018. Vol. 11, No. 29. pp. 1421–1435.
19. Shpenst V. A. Complexation of telecommunications and electrical systems in mines and underground facilities. *Journal of Mining Institute*. 2019. Vol. 235. pp. 78–87.
20. Terleev A. V., Khalturin A. A., Shpenst V. A. LoRaWAN gateway coverage evaluation for smart city applications. *Proceedings of the 3rd 2021 International Youth Conference on Radio Electronics, Electrical and Power Engineering, REEPE 2021*. 9388004. DOI: 10.1109/REEPE51337.2021.9388004.
21. TADVISER. Industrial Internet of Things of Russia. Research of Tadviser and Kostec Group Available online. Available at: http://tadviser.com/index.php/Article:IIoT_2018:_The_market_of_industrial_Internet_of_Things_in_Russia (Accessed : 10.03.2023).
22. Di Mauro M., Liotta A. An experimental evaluation and characterization of VoIP over an LTE-A network. *IEEE Transactions on Network and Service Management*. 2020. Vol. 17, No. 3. pp. 1626–1639.
23. Ravanbakhsh N., Mohammadi M., Nikooghadam M. Perfect forward secrecy in VoIP networks through design a lightweight and secure authenticated communication scheme. *Multimedia Tools and Applications*. 2019. Vol. 78, No. 9. pp. 11129–11153.
24. Elnawawy T., Ishkewy H., Harb H. Design a distributed adaptive VoIP load balancing (DA – VOIP – LB) over cloud. *The 1st International Conference on Information Technology IEEE/ITMUSTCONF*. 2019, April. pp. 29–30.
25. Saenger J., Mazurczyk W., Keller J., Caviglione L. VoIP network covert channels to enhance privacy and information sharing. *Future Generation Computer Systems*. 2020. Vol. 111. pp. 96–106.
26. Shukur H., Zeebaree S. R., Ahmed A. J., Zebari R. R., Ahmed O. et al. A state of art survey for concurrent computation and clustering of parallel computing for distributed systems. *Journal of Applied Science and Technology Trends*. 2020. Vol. 1, No. 4. pp. 148–154.
27. Khalifa O. O., Roslin R. J. B., Bhuiyan S. S. N. Improved voice quality with the combination of transport layer & audio codec for wireless devices. *Bulletin of Electrical Engineering and Informatics*. 2019. Vol. 8, No. 2. pp. 665–673.
28. Fouladi S., Emmons J., Orbay E., Wu C., Wahby R. S. Salsify: Low-latency network video through tighter integration between a video codec and a transport protocol. *15th Symposium on Networked Systems Design and Implementation (NSDI-18)*. 2018. pp. 267–282.
29. He J., Tang Z., Fan Z., Zhang J. Enhanced collision avoidance for distributed LTE vehicle to vehicle broadcast communications. *IEEE Communications Letters*. 2018. Vol. 22. pp. 630–633.
30. Maesa D. D. F., Mori P., Ricci L. A blockchain based approach for the definition of auditable access control systems. *Computers & Security*. 2019. Vol. 84. pp. 93–119.
31. Newton P. C., Ramkumar K., Rio R. N. CBT-VOIP: codec based technique to reduce VoIP transmission delay in mobile AD-HOC networks. *International Journal of Advanced Research in Computer Science*. 2017. Vol. 8, No. 7. pp. 998–1001. DOI: 10.26483/ijarcs.v8i7.4543.
32. Zhukovskiy Y., Batueva D., Buldysko A. et al. Motivation towards energy saving by means of IoT personal energy manager platform. *Journal of Physics: Conference Series*. 2019. Vol. 1333, Iss. 6. p. 062033. DOI: 10.1088/1742-6596/1333/6/062033.
33. Deng Y., Deng Y. Design and Implementation of Distributed Call-Center Based on Soft-Switch. *Journal of Physics: Conference Series*. 2021. Vol. 1883, No. 1. p. 012084.
34. Wieckowski A., Heg G., Bartnik C., Lehmann C., Stoffers C. et al. Towards a live software decoder implementation for the upcoming versatile video coding (VVC) codec. *IEEE International Conference on Image Processing (ICIP). 2020. 25–26 October*. pp. 3124–3128.
35. Vu T. L., Zeng Z., Xu H., Chng E. S. Audio codec simulation based data augmentation for telephony speech recognition. *Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC). 2019. 18–21 November*. pp. 198–203.
36. Ergen T., Kozat S. S. Online training of LSTM networks in distributed systems for variable length data sequences. *IEEE Transactions on Neural Networks and Learning Systems*. 2017. Vol. 29, No 10. pp. 5159–5165.
37. Wang H., Yang Z., Hu Y., Yang Z., Huang Y. Fast detection of heterogeneous parallel steganography for streaming voice. *Proceedings of the 2021 ACM Workshop on Information Hiding and Multimedia Security. 2021. 21 June*. pp. 137–142.
38. Kassim M., Rahman R. A., Aziz M. A. A., Idris A., Yusof M. I. Performance analysis of VoIP over 3G and 4G LTE network. *2017 International Conference on Electrical, Electronics and System Engineering (ICEESE)*. 2017. 9–10 November. pp. 37–41.
39. Zhou A., Zhang H., Su G., Wu L., Ma R. et al. Learning to coordinate video codec with transport protocol for mobile video telephony. *The 25th Annual International Conference on Mobile Computing and Networking*. 2019. 21–25 October. p. 29.
40. Lin Z., Lu J., Qiu X. An effective hybrid low delay packet loss concealment algorithm for MDCT-based audio codec. *Applied Acoustics*. 2019. Vol. 154. pp. 170–175.
41. Zhukovskiy Y. L., Starshaia V. V., Batueva D. E., Buldysko A. D. Analysis of technological changes in inte-grated intelligent power supply systems. Innovation-Based Development of the Mineral Resources Sector: Challenges and Prospects. 2019. pp. 249–258.
42. Abualhaj M. M., Al-Tahrawi M. M., Al-Khatib S. N. A new method to improve Voice over IP (VoIP) bandwidth utilization over Internet Telephony Transport Protocol (ITTP). *Proceedings of the 8th International Conference on Software and Information Engineering. 2019, April*. pp. 192–195.
43. Al-Najjar A., Layeghy S., Portmann M., Indulska J. Enhancing quality of experience of VoIP traffic in SDN based end-hosts. *28th International Telecommunication Networks and Applications Conference (ITNAC)*. 2018. 21–23 November. 183 95 300.
44. Kim W., Song T., Kim T., Park H., Pack S. VoIP capacity analysis in full duplex WLANs. *IEEE Transactions on Vehicular Technology*. 2017. Vol. 66, Iss. 12. pp. 11419–11424.
45. Peng J., Tang S. Covert communication over VoIP streaming media with dynamic key distribution and authentication. *IEEE Transactions on Industrial Electronics*. 2020. Vol. 68, Iss. 4. pp. 3619–3628.
46. Uhl T. QoS by VoIP under use different audio codecs. *2018 Joint Conference-Acoustics. 2018, 11–14 September*. 181 968 63.
47. Shukur H., Zeebaree S., Zebari R., Ahmed O., Haji L. et al. Cache coherence protocols in distributed systems. *Journal of Applied Science and Technology Trends*. 2020. Vol. 1, Iss. 3. pp. 92–97.
48. Dhillon P. K., Kalra S. Secure and efficient ECC based SIP authentication scheme for VoIP communications in internet of things. *Multimedia Tools and Applications*. 2019. Vol. 78, Iss. pp. 22199–22222.
49. Dominic S., Jacob L. Distributed resource allocation for D2D communications underlaying cellular networks in time-varying environment. *IEEE Communications Letters*. 2017. Vol. 22, Iss. 2. pp. 388–391.
50. Yang Y., Wang X. Compression Techniques for VoIP Transport over Wireless Interfaces. *VoIP Handbook*. 2018. pp. 99–116.
51. Safiullin R. N., Afanasyev A. S., Reznichenko V. V. The concept of development of monitoring systems and management of intelligent technical complexes. *Journal of Mining Institute*. 2019. Vol. 237. pp. 322–330. DOI: 10.31897/pmi.2019.3.322.
52. Mukherjee S., Ravindran R., Raychaudhuri D. A distributed core network architecture for 5G systems and beyond. *Proceedings of the 2018 Workshop on Networking for Emerging Applications and Technologies. 2018, 20 August*. pp. 33–38.
53. Miraz M. H., Molvi S. A., Ganie M. A., Ali M., Hussein A. H. Simulation and analysis of quality of service (QoS) parameters of voice over IP (VoIP) traffic through heterogeneous networks. 2017. DOI: 10.48550/arXiv.1708.01572.
54. Araneo A., Gamess E., Urribarri D. A set of policies and guidelines for deploying safer VoIP solutions. *International Journal of Computer Theory and Engineering*. 2018. Vol. 10, No. 2. DOI: 10.7763/IJCTE.2018.V10.1197.