Труды МАИ. 2021. № 121
Trudy MAI, 2021, no. 121

Научная статья

УДК 621.396

DOI:10.34759/trd-2021-121-12

ОСОБЕННОСТИ КЛАССИФИКАЦИИ И ФИЛЬТРАЦИИ ТРАФИКА СЕТИ ПЕРЕДАЧИ ДАННЫХ 6G

Игорь Геннадьевич Бужин[1]✉, Вероника Михайловна Антонова[2], Юрий Борисович Миронов[3], Варвара Александровна Антонова[4], Алла Сергеевна Корчагина[5], Маргарита Геннадьевна Канищева[6]

[1,2,3,4,5,6]Московский технический университет связи и информатики, МТУСИ, Москва, Россия

[2] Институт радиотехники и электроники им. В.А. Котельникова РАН, Москва, Россия

[1]i.g.buzhin@mtuci.ru✉

[2]xarti@mail.ru

[3]i.b.mironov@mtuci.ru

[4]varvara_zi@mail.ru

[5]alla-97@inbox.ru

[6]margo.kan@list.ru

Аннотация. В статье рассмотрены особенности функционирования системы мониторинга угроз информационной безопасности транспортной сети передачи данных 6G. В частности, проведен анализ логической структуры типовой системы мониторинга. Предложены основные принципы организации функционирования системы классификации и фильтрации трафика транспортной сети передачи данных

6G при применении технологии SDN. Кроме того, авторами представлены пути решения задачи фильтрации и мониторинга на основе сформулированных принципов. Описаны пути устранения опасной уязвимости CVD-2021-0047.

***Ключевые слова*:** нарезка сети, фильтрация трафика, программно-определяемая сеть (SDN), сети передачи данных 6G

Для цитирования: Бужин И.Г., Антонова В.М., Миронов Ю.Б., Антонова В.А., Корчагина А.С, Канищева М.Г. Особенности классификации и фильтрации трафика сети передачи данных 6G // Труды МАИ. 2021. № 121. DOI: 10.34759/trd-2021-121-12

FEATURES OF CLASSIFICATION AND FILTERING OF DATA TRAFFIC IN 6G NETWORK

Igor G. Buzhin[1]✉, Veronika M. Antonova[2],
Yuri B. Mironov[3], Varvara A. Antonova[4],
Alla S. Korchagina[5], Margarita G. Kanishcheva[6]

[1,2,3,4,5,6]Moscow technical university of communications and informatics,
Moscow, Russia

[2] Kotel'nikov institute of radio engineering and electronics of RAS,
Moscow, Russia

[1]i.g.buzhin@mtuci.ru✉

[2]xarti@mail.ru

[3]i.b.mironov@mtuci.ru

[4]varvara_zi@mail.ru

[5]alla-97@inbox.ru

[6]margo.kan@list.ru

Abstract. AdaptiveMobile has identified a vulnerability in the of the Network Slicing mechanism implementation, which could disclose information about arbitrary network segments or cause a denial of service. The vulnerability was assigned the CVD-2021-0047 number. Federal Service for Technology and Export Control (FSTEC of Russia) introduced vulnerability to the bank of threats and determined the level of danger as medium. One of the trends for this vulnerability elimination in the 6G networks is formulation of the classification principles and filtering of the 6G transport network traffic for effective application of the Network Slicing mechanism.

The basic principles of collecting, filtering and traffic classification of the data transmission network are as follows:

- Traffic filtering and classification is based on the analysis of the header fields of the data protocol units of L2 - L4 levels;
- Each consumer and operator data protocol unit (PDU) should be subjected to filtering and classification;
- The filter along with the the classifier represent a combination of certain fields of the header of the L2-L4 level PDU with ranges indication of their possible values;
- The class may include the PDU that meets the criteria of different filters. The PDU satisfying one and the same filter may correspond to different classes. In the latter case, such PDU should be copied to the storage corresponding to the different classes;
- PDU of different classes should be stored separately in data processing and storage centers;

- Filtering policy forming, i.e. a specific set of filters and class attributes, corresponds to the function of the SDN controller applications, which can act as external applications for the SDN transport network controller;
- Filtering and Classification policies delivery is being performed in the in_band mode in the transport network via VPN channels;
- Regional (border) data processing and storage centers may add filtering rules to the filters of their domain, with the permission of the main data processing and storage center,;
- The PDU network users gathering should be performed covertly for them;
- The network services consumers should not receive any information about the monitoring system, which includes the traffic classification and filtering system by means of their data transmission network;
- Filtering and classification policies may be dynamically changed, if necessary, by the monitoring system administrator in each of the regions, provided that the consistency of classifiers in different regions is maintained.

The proposed principles and ways of solving the filtering and monitoring problem are aimed at eliminating the dangerous CVD-2021-0047 vulnerability.

Keywords: Network Slicing, traffic filtering, Software Defined Networking (SDN), 6G data transmission networks

For citation: Buzhin I.G., Antonova V.M., Mironov Yu.B., Antonova V.A., Korchagina A.S., Konishcheva M.G. Features of classification and filtering of data traffic in 6G network. *Trudy MAI*, 2021, no.121. DOI: 10.34759/trd-2021-121-12

Введение

Мобильная связь за 40 лет полностью изменила мир. Сегодня мы сильно зависим от беспроводной связи как в работе, так и в жизни; она стала ключевым фактором цифровой трансформации каждого бизнеса. Сети связи 5G призваны сделать беспроводными все каналы связи – как высоконагруженные, так и сверхвысоконадежные, в конечном итоге соединяя все услуги и сервисы. Опираясь на фундамент 5G, беспроводная сеть 6G поставила своей целью повсеместную интеллектуальную революцию. Фактически 6G будет служить нейронной сетью в масштабе человечества и связующим звеном между двумя мирами, физическим и цифровым. Искусственный интеллект (ИИ), основанный на машинном обучении, станет основой 6G, и в этой сфере наше общество полностью перейдет от подключенных людей и подключенных вещей к подключенному интеллекту (connected intelligence). Система 6G будет генерировать огромное количество данных, связанных с работой сети и управлением сетью, с деятельностью пользователей, сканированием окружающей среды и работой оконечных устройств. Поскольку эти данные будут поступать из совершенно разных областей, актуальные задачи проектирования новой системы 6G включают в себя эффективную организацию данных и управление ими с учетом защиты конфиденциальности.

Постановка задачи

Транспортная сеть 5G представляет собой сеть передачи данных и включает в себя сети радиодоступа, сети агрегации и ядро транспортной сети, которое состоит из магистральных сетей, создаваемых в городах, и сетей, обеспечивающих междугородную связь. Такая транспортная сеть строится преимущественно, где это

возможно, с использованием оптического волокна и протоколов IPv4 или IPv6. В транспортной сети 5G выделяют сеть радиодоступа 5G (5G RAN) и опорная сеть 5G (5G core network, 5G CN). Принцип построения транспортной сети 6G останется аналогичным по сравнению с 5G. Транспортная сеть 6G должна на всем своем протяжении, включая RAN и CN, должна обеспечивать передачу трафика множества разнообразных услуг с требуемым качеством обслуживания и уровнем обеспечения информационной безопасности, что достигается путем логического разделения транспортной сети на слои (slices). Такая нарезка сети позволит на одной физической сетевой инфраструктуре организовывать несколько логических слоев (slices) (виртуальных сетей), которые будут отличаться между собой ключевыми характеристиками, такими как тип оказываемых услуг, скорость передачи, объем трафика, величина задержки передачи, задержка отклика сети, требования к тарификации и др. Реализация таких сетевых слоев (Network Slicing) опирается на максимальное, где это возможно, использование программного обеспечения вместо аппаратных средств связи (программируемость сети), а также на внедрение технологий программно-конфигурируемых сетей (Software Defined Networking, SDN), виртуализации сетевых функций (Network Functions Virtualization, NFV) и технологий периферийных вычислений (Mobile Edge Computing, MEC). Компанией AdaptiveMobile была выявлена уязвимость [1] реализации механизма Network Slicing, которая может раскрыть информацию о произвольных сегментах сети или вызвать отказ в обслуживании. Уязвимости был присвоен номер CVD-2021-0047. ФСТЭК России внес уязвимость в банк угроз и определил уровень опасности: средний. Одним из направлений для устранения данной уязвимости в сетях 6G является

формулирование принципов классификации и фильтрации трафика транспортной сети 6G для эффективного применения механизма Network Slicing.

Система мониторинга трафика транспортной сети

Система мониторинга имеет распределенную модульную архитектуру. На рис. 1 представлена типовая логическая схема системы мониторинга.

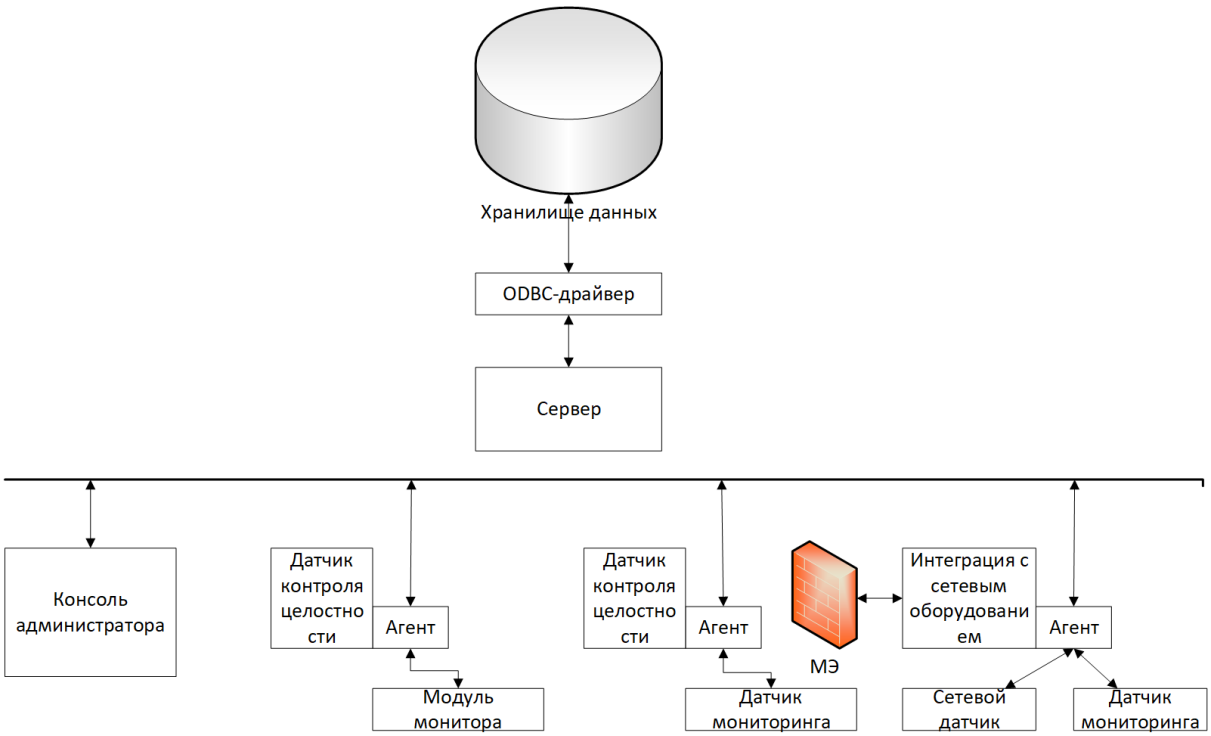

Рис. 1 - Логическая структура типовой системы мониторинга

Хранилище данных обеспечивает централизованное хранение событий системы. Сервер является связующим звеном между модулями системы, обеспечивает передачу информации между ними, выполняет функции контроля работоспособности компонентов. ODBC-драйвер обеспечивает защищенный информационный обмен (шифрование) между информационным фондом и компонентами системы, которые к нему подключаются. Консоль администратора (клиент) обеспечивает пользовательский интерфейс системы. Агент выполняет функции управления датчиками, а также функции передачи информации между

датчиками и сервером. К одному агенту может быть подключены несколько разнородных по функциям датчиков. Агент также обеспечивает контроль доступности узла, на котором он установлен и передачу администратору данных об этом узле: имя, IP-адрес, используемая операционная система, текущий активный пользователь и другая служебная информация. Сетевой датчик осуществляет предварительный анализ и сбор поступающего трафика. Датчик контроля целостности производит контроль целостности компонентов, устанавливаемых на узлы сети, а также исполняемых конфигурационных файлов и иных параметров и ресурсов, на которых он установлен. Монитор доступности сканирует контролируемые сегменты сети, а также сетевые узлы на предмет их доступности с использованием протокола ICMP. Хостовой датчик осуществляет мониторинг состояния программно-технических средств, на которых он установлен и сбор информации.

Компонент интеграции с сетевым оборудованием состоит из модуля управления сетевым оборудованием (предоставляет возможность посылать команды сетевому оборудованию (коммутаторам, межсетевым экранам и др.) напрямую, либо, на основе шаблонов, например, с целью блокирования компьютерной атаки в стадии ее развития) и модуля приема сообщений от сетевых устройств (предоставляет возможность приема SNMP и syslog-сообщений от различных узлов сети (коммутаторы, межсетевые экраны и др.) с последующей их обработкой и выводом в понятном для пользователя виде).

Для работы компонента Сервер необходимо наличие хранилища данных. Для использования криптоалгоритмов, на все узлы, на которые установлены компоненты

системы, устанавливаются компоненты внешнего крипропровайдера. Для обеспечения криптографически защищенного информационного обмена между компонентами, а также для обеспечения работы функции контроля целостности ресурсов, требуется доступ к услугам удостоверяющего центра.

Таким образом, основные задачи системы мониторинга:

- сбор информации о функционировании комплекса технических средств защищаемой СПД и о событиях безопасности в ней, в том числе от датчиков;
- комплексная обработка и анализ информации о различных событиях в защищаемой системе, отображение информации с использованием принципов вложенности информации и построения мнемосхем (по принципу "событие" - когда и где оно произошло);
- подготовка и выгрузка информации о событиях в иерархически организованные информационные системы.

Реализация функций мониторинга осуществляется путем использования программного хостового датчика, который устанавливается на узлы, подвергаемые мониторингу.

Основные принципы организации функционирования системы классификации и фильтрации трафика при применении технологии SDN

Основными принципами сбора, фильтрации и классификации трафика сети передачи данных являются:

- фильтрация и классификация трафика основана на анализе полей заголовков протокольных единиц данных уровней L2 – L4;

- фильтрации и классификации должен подвергаться каждая протокольная единица данных (ПЕД) потребителей и оператора;
- фильтр, равно как и классификатор, представляют комбинацию определенных полей заголовка ПЕД уровня L2-L4 с указанием диапазонов их возможных значений;
- класс может включать ПЕД, удовлетворяющих признакам разных фильтров. ПЕД, удовлетворяющие одному и тому же фильтру, могут соответствовать разным классам. В последнем случае такая ПЕД должна быть скопирована в хранилище, соответствующее разным классам;
- ПЕД разных классов в должны храниться раздельно в центрах обработки и хранения данных (ЦОХД);
- формирование политики фильтрации, т.е. конкретного множества фильтров и признаков классов, соответствует функции приложений контроллера SDN, которые могут выступать в роли внешних приложений для контроллера транспортной SDN сети;
- доставка политик фильтрации и классификации осуществляется в режиме in_band в транспортной сети по каналам VPN;
- районные (граничные) ЦОХД могут с разрешения главного ЦОХД добавлять в фильтры своего домена правила фильтрации;
- сбор ПЕД пользователей сети должен осуществлять скрытно для них;

- потребители услуг сети не должны получать никакой информации о системе мониторинга, в которую входит система классификации и фильтрации трафика) средствами своей сети передачи данных;
- политики фильтрации и классификации могут динамически меняться при необходимости администратором системы мониторинга в каждом из регионов при условии сохранения согласованности классификаторов в разных регионах.

При использовании технологии SDN политики фильтрации и классификации реализуются в виде загружаемых правил (как правило, на основании работы протокола OpenFlow) в коммутаторы сенсоров и входные шлюзы районных ЦОХД и главных ЦОХД. Основная идея использования коммутатора SDN в качестве сенсора заключается в использовании возможностей этого устройства, которые допускаются стандартом OpenFlow, а именно использование в любой комбинации поля заголовка.

Коммутатор является системой, управляемой потоком событий, реализующей обработку битовых векторов ограниченной длины – фрагментов сетевого обмена. Передача битового вектора в коммутатор является событием, а коммутатор реализует формирование реакции на событие. При этом по источнику возникновения потоков событий и по их свойствам потоки могут быть разделены на два основных класса:

- поток данных для фильтрации с последующими классификацией и хранением - контур данных;
- поток данных управления – контур управления.

Обработка потоков данных конура данных в рамках коммутатора сводится к последовательной обработке каждого отдельного фрагмента данных – кадра Ethernet согласно заложенной в коммутатор логике. Основная логика коммутатора SDN

реализует обработку пакетов, которые проходят через него. Обработка кадров в коммутаторе описывается как суперпозиция отображений, каждое из которых отвечает отдельному требованию спецификации. При этом аргументом функции максимального уровня вложенности всегда является множество транзитных пакетов, равно как и значение функции минимального уровня вложенности также принадлежит этому множеству.

В соответствии с принципами фильтрации и классификации, сформулированными выше, классификация потоков должна осуществляться для каждого отдельно взятого пакета. Классификация осуществляется на базе значений фиксированного набора полей заголовка протокольной единицы данных (ПЕД) и заданной политики классификации, заданной в виде набора масок.

Предлагаемый способ обладает широкими возможностями по классификации потока. Наиболее логичным принципом классификации представляется по номерам или меткам правил фильтрации, загружаемых в сенсоры, выполненные на основе коммутаторов SDN. В соответствие с этими метками, система мониторинга, пользуясь возможностями автоматической коммутации потоков в технологии SDN, в состоянии направить отфильтрованную и классифицированную информацию на хранение в предназначенные для этого хранилища и сегменты системы мониторинга, в соответствии с реализованной информационной моделью хранения отфильтрованных данных. В зависимости от информационной модели, передача на хранение данных может быть выполнена с заполнением соответствующих полей значением метки, отвечающей определенной классификации потока.

Поток может маркироваться либо за счет опциональных полей заголовка, либо за счет использования адреса в формате IPv6 для дальнейшего анализа и упаковываться в транспортный туннель (например, GRE и т.п.). Обычно использование опциональных полей заголовка нежелательно, т.к. такие поля часто обрезают промежуточные коммутаторы или маршрутизаторы, но в случае использования механизма туннелирования потока это ограничение является несущественным.

Частным случаем решения задачи фильтрации и мониторинга на основе принципов, которые описаны выше, являются методы сигнатурного анализа трафика, широко используемые в различных IDS\IPS, системах DPI и межсетевых экранах.

Методы сигнатурного анализа трафика используют в процессе сетевого мониторинга предварительно накопленные сведения об облике событий сетевой безопасности, поэтому процедуры сигнатурного контроля требуют ресурсных затрат (прежде всего, памяти) для доступа к накопленным сведениям. Это ограничивает реализацию таких процедур, например, непосредственно в точке маршрутизации, не обладающей соответствующими ресурсами. В то же время, эти, методы свободны от ограничений, связанных с признаками, характеризующими сетевые пакеты и соединения. Строго говоря, в качестве сигнатур могут выступать произвольные двоичные комбинации, их сочетания и условия появления в потоке данных. Но сетевая сигнатура - это не просто набор данных, появление которых в трафике, ассоциируется с событием безопасности. Если не рассматривать DPI-системы, то сигнатурные методы сетевого мониторинга игнорируют содержание пакетов и контролируют значения полей заголовка или комбинацию таких значений.

В самом простом, но, тем не менее, обязательном случае сигнатуры, анализирующие значение полей заголовка, должны проверять соблюдение соглашений соответствующих RFC. Например, TCP-пакет с одновременным набором флагов SYN и FIN это явное нарушение RFC 793 (которым определяется стандартный протокол TCP), что и используется в инструментальных средствах атак. Кроме того, многие вредоносные эксплойты включают значения заголовка, преднамеренно нарушающее соглашение RFC, так как коды многих операционных систем и приложений написаны в предположении, что соглашения RFC соблюдаются, и поэтому эти коды не предусматривают надлежащей обработки ошибок трафика. Также, некоторые программные средства могут содержать ошибки кодирования, и сетевые пакеты, произведенные ими, содержат значения заголовков, нарушающих соглашения RFC.

С другой стороны, развиваются и стандарты, и в них появляются новые соглашения, что позволяет допустить действия по формированию трафика, которые ранее были запрещены. Во всех таких случаях, особенно при несинхронном развитии RFC и практики применения сетевых протоколов сигнатурные методы, использующие устаревшие соглашения RFC, могут порождать множество сигналов ложной тревоги. Тем не менее, соответствующие RFC могут являться базисом для развития сигнатур, потому что множество событий безопасности соответствуют каким-то нарушениям RFC. Особенно это справедливо при условии, что существующие сигнатуры периодически пересматриваются и модифицируются в соответствии с обновлением соглашений RFC.

Контроль выполнения соглашений RFC дополняется признаками, которые хотя и могут присутствовать и в нормальном трафике, но условия их появления являются нетипичными, и обнаружение их в составе заголовка контролируемого пакета снижает уровень доверия к легитимности трафика. Например, это могут быть необычные рефлексивные порты (если это не NetBIOS), небольшой размер TCP window size, неизменность значения IP identification number и т.д. Эти значения не являются запрещенными, это может быть совпадением, но, когда накапливается несколько таких признаков, уровень доверия становится недопустимо низким.

Поэтому наряду с некорректными значениями заголовка, которые являются основными признаками события безопасности, разрешенные, но подозрительные значения заголовка так же целесообразно включать в состав сигнатур. Например, попытка определения готовности к подключениям к номерам портов, обычно связываемых с распространением вредоносного кода, может служить быстрым путем идентификации атаки. Но часть безопасного трафика тоже может использовать те же самые порты, поэтому без более детальной сигнатуры, включающей другие характеристики трафика, нельзя точно определить природу этого трафика. Подозрительные, но законные значения заголовков лучшие проверять в комбинации с другими характеристиками, что приводит к выводу о необходимости использования комплексных (составных) сигнатур.

Рассматривая несколько потенциальных элементов события безопасности, можно составлять множество различных вариантов для разработки сигнатуры на основе заголовка, так как контроль может включать любой выбранный элемент или их комбинацию. Простая сигнатура (например, контроль одновременного набора

SYN и FIN флагов), являясь индикатором вероятного злонамеренного действия, не позволяют судить о происхождении этого действия. Флаги SYN и FIN используются вместе, чтобы обойти сетевые защитные устройства, но их присутствие может означать, что проводится просто сканирование защиты, идет сбор информации или атака уже проводится. Поэтому сигнатура, ограничивающаяся только контролем одновременности флагов SYN и FIN, слишком проста, чтобы быть действительно полезной в широком смысле.

С другой стороны, сигнатура, основанная на многочисленных подозрительных характеристиках, должна быть более определенной. Она обеспечивает более точной информацией об источнике нападения, но будет менее эффективной с точки зрения ошибочности, нежели сигнатура, 231 проверяющая только одно значение заголовка. Как правило, простые сигнатуры более склонны к ложным тревогам из-за своей прямолинейности. В то же время, сложные сигнатуры чаще могут устаревать и становиться склонными к ошибкам, из-за того, что какая-то одна из характеристик инструмента или методологии может измениться со временем. Развитые сигнатуры – это всегда компромисс между эффективностью и точностью. Относительно просто создать сигнатуру, соответствующую специфическому типу трафика, гораздо труднее предусмотреть в ней минимизацию ложных сигналов тревоги и пропуска действительно вредных (неотфильтрованных) пакетов.

Основой создания большинства сигнатур служат идентифицированные черты пакетов, которые были необычны или подозрительны, или нарушают существующие стандарты, и определение, какие из этих характеристик эффективны, устойчивы и

точны, т.е. годятся для создания сигнатуры. Наиболее часто используемые элементы сигнатуры это:

- IP-адреса (типовые для резервирования, без маршрутизации, предназначенные для трансляции);
- номера портов, которые не должны быть использованы (известные порты для специфических протоколов);
- необычная фрагментация пакетов;
- специфические комбинации TCP флагов;
- типы/коды ICMP, которые обычно не применяются.

В принципе, любые значения заголовков могут использоваться в сигнатурах, но приведенные параметры, как правило, всегда присутствуют в составе многих других характеристик пакетов.

В ряде случаев существует потребность прояснять методы и направления атаки. Если реагировать готовностью защитных средств на весь аномальной трафик, то атака будет отражена, но направленность действий атакующего скорее всего не будет определена. Базируя же сигнатуры на исследовании потенциальных нападений и уязвимостей, развитии наборов сигнатур, объединении общих и специфических сигнатур, можно идентифицировать вероятный источник угрозы, механизм действий атакующего и его цели.

Таким образом, развитие и доработка сигнатур может заключаться в двух подходах: добавление определенных сигнатур на конкретные инструменты нападения или специфические эксплоиты, или создание общей сигнатуры, которые

просто ищет различные аномалии в трафике – подобная система способна отражать и ранее неизвестные типы нападений. Конкретный вид сигнатуры будет зависеть от используемого метода и определяемых значений.

Заключение

В данной работе рассмотрены принципы функционирования системы мониторинга угроз информационной безопасности транспортной сети передачи данных 6G, предложены основные принципы организации функционирования системы классификации и фильтрации трафика транспортной сети передачи данных 6G при применении технологии SDN, предложены пути решения задачи фильтрации и мониторинга на основе сформулированных принципов. Предложенные принципы и пути решения задачи фильтрации и мониторинга направлены на устранение опасной уязвимости CVD-2021-0047.

Список источников

1. 5G Network Slicing Security in 5G Core Networks. URL: https://info.adaptivemobile.com/5g-network-slicing-security#hs_cos_wrapper_dnd__form-module-2

2. Samouylov K.E., Shalimov I.A., Buzhin I.G., Mironov Y.B. Model of functioning of telecommunication equipment for software-configurated networks // Modern Information Technologies and IT-Education, 2018, vol. 14, no. 1. DOI:10.25559/SITITO.14.201801.013-026

3. Tsvetkov V.K., Oreshkin V.I., Buzhin I.G., Mironov Y.B. Model of Restoration of the Communication Network Using the Technology of Software Defined Networks // 2019

IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ELCONRUS, 2019, pp. 1559-1563. DOI: 10.1109/EIConRus.2019.8656723

4. Buzhin I.G., Mironov Y.B. Evaluation of telecommunication equipment Delays in Software Defined Networks // Systems of Signals Generating and Processing in the Field of on Board Communications, 2019, pp. 8706825. DOI: 10.1109/SOSG.2019.8706825

5. ONF TR-502: SDN Architecture. URL: https://www.opennetworking.org/images/stories/downloads/sdn-resources /technical-reports/TR_SDN_ARCH_1.0_06062014.pdf

6. Методика моделирования угроз безопасности информации (проект), Федеральная служба по техническому и экспортному контролю (ФСТЭК России), 2020 г. URL: https://fstec.ru/component/attachments/download/2727

7. Концепция создания и развития сетей 5G/IMT-2020 в Российской Федерации, утверждена приказом Минкомсвязи России № 923 от 27.12.2019 г. URL: https://digital.gov.ru/uploaded/files/kontseptsiya-sozdaniya-i-razvitiya-setej-5g-imt-2020.pdf

8. Spyros Denazis, Evangelos Haleplidis, Kostas Pentikousis, Jamal Hadi Salim. RFC 7426: Software-Defined Networking (SDN): Layers and Architecture Terminology, 2015, 35 pp. URL: https://www.researchgate.net/publication/280554784_RFC_7426_Software-Defined_Networking_SDN_Layers_and_Architecture_Terminology

9. Technical Specification SDN Security Considerations in the Data Center. ONF Solution Brief, 2013, URL: https://opennetworking.org/wp-content/uploads/2013/05/sb-security-data-center.pdf

10. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию, утвержден приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. N 374-ст. URL: https://docs.cntd.ru/document/1200057516

11. Threat Analysis for the SDN Architecture 1.0 Technical Specification, Open Networking Foundation, 2016, URL: https://opennetworking.org/wp-content/uploads/2014/10/Threat_Analysis_for_the_SDN_Architecture.pdf

12. Mahmoud Said Elsayed, Nhien-An Le-Khac, Soumyabrata Dev, Anca Delia Jurcut. Machine-Learning Techniques for detecting Attacks in SDN, arXiv:1910.00817v1 [cs.CR], 2 Oct 2019, URL: https://arxiv.org/pdf/1910.00817.pdf

13. Волков С.С., Курочкин И.И., Применение методов машинного обучения в SDN в задачах обнаружения вторжений // International journal of open information technologies. 2019. Т. 7. № 11 С. 49-58.

14. 3GPP, System architecture for the 5G system, 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 23.501, Aug. 2020, v 16.5.1. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144

15. 3GPP, «Common API Framework for 3GPP northbound APIs», 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 23.222, July 2020, v 17.1.0. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3337

16. 3GPP, Architecture enhancements for 5G System (5GS) to support network data analytics services, 3rd Generation Partnership Project (3GPP), Technical Specification (TS)

23.288, July 2020, v 16.4.0. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3579

17. Антонова В.М., Кондрашова Д.А., Сухорукова Н.А. Угрозы безопасности сетей 5G // Colloquium-journal. 2021. № 1-1 (88). С. 57-60. DOI: 10.24412/2520-2480-2021-188-57-60

18. Антонова В.М., Богомолова Н.Е., Кузичев Д.М. Моделирование процессов организации соединений в системе мобильной связи пятого поколения в среде MATLAB, - М.: МГТУ им. Н.Э. Баумана, 2021. – 48 с.

19. Антонова В.М., Захир Б.М., Кузнецов Н.А. Моделирование графов с различными видами достижимости с помощью языка Python // Информационные процессы. 2019. Т. 19. № 2. С. 159-169.

20. Казак П.Г., Шевцов В.А. Принципы построения энергоэффективной системы сотовой связи и беспроводного широкополосного доступа в Интернет для Арктики // Труды МАИ. 2021. № 118. URL: http://trudymai.ru/published.php?ID=158239. DOI: 10.34759/trd-2021-118-06

21. Бородин В.В., Петраков А.М., Шевцов В.А. Моделирование служебного канала передачи маршрутной информации адаптивной летающей сети связи // Электросвязь. 2016. № 11. С. 41-45.

22. Волков А.С., Баскаков А.Е. Разработка процедуры двунаправленного поиска для решения задачи маршрутизации в транспортных программно-конфигурируемых сетей // Труды МАИ. 2021. № 118. http://trudymai.ru/published.php?ID=158240. DOI: 10.34759/trd-2021-118-07

References

1. *5G Network Slicing Security in 5G Core Networks*. URL: https://info.adaptivemobile.com/5g-network-slicing-securityhs_cos_wrapper_dnd__form-module-2

2. Samouylov K.E., Shalimov I.A., Buzhin I.G., Mironov Y.B. Model of functioning of telecommunication equipment for software-configurated networks, *Modern Information Technologies and IT-Education*, 2018, vol. 14, no. 1. DOI:10.25559/SITITO.14.201801.013-026

3. Tsvetkov V.K., Oreshkin V.I., Buzhin I.G.,. Mironov Y.B. Model of Restoration of the Communication Network Using the Technology of Software Defined Networks, *2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering*, *ELCONRUS*, 2019, pp. 1559-1563. DOI: 10.1109/EIConRus.2019.8656723

4. Buzhin I.G., Mironov Y.B. Evaluation of telecommunication equipment Delays in Software Defined Networks, *Systems of Signals Generating and Processing in the Field of on Board Communications*, 2019, pp. 8706825. DOI: 10.1109/SOSG.2019.8706825

5. *ONF TR-502: SDN Architecture*. URL: https://www.opennetworking.org/images/stories/downloads/sdn-resources /technical-reports/TR_SDN_ARCH_1.0_06062014.pdf

6. *Metodika modelirovaniya ugroz bezopasnosti informatsii (proekt), Federal'naya sluzhba po tekhnicheskomu i eksportnomu kontrolyu (FSTEK Rossii), 2020 g.* URL: https://fstec.ru/component/attachments/download/2727

7. *Kontseptsiya sozdaniya i razvitiya setei 5G/IMT-2020 v Rossiiskoi Federatsii, utverzhdena prikazom Minkomsvyazi Rossii № 923 ot 27.12.2019 g.* URL:

https://digital.gov.ru/uploaded/files/kontseptsiya-sozdaniya-i-razvitiya-setej-5g-imt-2020.pdf

8. Spyros Denazis, Evangelos Haleplidis, Kostas Pentikousis, Jamal Hadi Salim. *RFC 7426: Software-Defined Networking (SDN): Layers and Architecture Terminology*, 2015, 35 pp. URL: https://www.researchgate.net/publication/280554784_RFC_7426_Software-Defined_Networking_SDN_Layers_and_Architecture_Terminology

9. *Technical Specification SDN Security Considerations in the Data Center. ONF Solution Brief*, 2013, URL: https://opennetworking.org/wp-content/uploads/2013/05/sb-security-data-center.pdf

10. *GOST R 51275-2006. Zashchita informatsii. Ob"ekt informatizatsii. Faktory, vozdeistvuyushchie na informatsiyu, utverzhden prikazom Federal'nogo agentstva po tekhnicheskomu regulirovaniyu i metrologii* (GOST R 51275 Information security. Object of informatization. Factors affecting information. General Provisions), 2006, no. 374-st. URL: https://docs.cntd.ru/document/1200057516

11. *Threat Analysis for the SDN Architecture 1.0 Technical Specification, Open Networking Foundation*, 2016, URL: https://opennetworking.org/wp-content/uploads/2014/10/Threat_Analysis_for_the_SDN_Architecture.pdf

12. Mahmoud Said Elsayed, Nhien-An Le-Khac, Soumyabrata Dev, Anca Delia Jurcut. *Machine-Learning Techniques for detecting Attacks in SDN, arXiv:1910.00817v1 [cs.CR],* 2 Oct 2019. URL: https://arxiv.org/pdf/1910.00817.pdf

13. Volkov S.S., Kurochkin I.I. *International Journal of Open Information Technologies*, 2019, vol. 7, no. 11, pp 49-58.

14. *3GPP, System architecture for the 5G system, 3rd Generation Partnership Project (3GPP),* Technical Specification (TS) 23.501, Aug. 2020, v 16.5.1. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144

15. *3GPP, «Common API Framework for 3GPP northbound APIs», 3rd Generation Partnership Project (3GPP),* Technical Specification (TS) 23.222, July 2020, v 17.1.0. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3337

16. *3GPP, Architecture enhancements for 5G System (5GS) to support network data analytics services, 3rd Generation Partnership Project (3GPP)*, Technical Specification (TS) 23.288, July 2020, v 16.4.0. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3579

17. Antonova V.M., Kondrashova D.A., Sukhorukova N.A. // Solloquium-journal, 2021, no. 1-1(88), pp. 57-60. DOI: 10.24412/2520-2480-2021-188-57-60

18. Antonova V.M., Bogomolova N.E., Kuzichev D.M. *Modelirovanie protsessov organizatsii soedinenii v sisteme mobil'noi svyazi pyatogo pokoleniya v srede MATLAB* (Modeling of connection organization processes in the fifth-generation mobile communication system in the MATLAB environment), Moscow, MGTU im. N.E. Baumana, 2021, 48 p.

19. Antonova V.M., Zakhir B.M., Kuznetsov N.A. Modelirovanie grafov s razlichnymi vidami dostizhimosti s pomoshch'yu yazyka Python // Informatsionnye protsessy. 2019. T.

19. № 2. С. 159-169.

20. Kazak P.G., Shevtsov V.A. *Trudy MAI*, 2021, no. 118. URL: http://trudymai.ru/eng/published.php?ID=158239. DOI: 10.34759/trd-2021-118-06

21. Borodin V.V., Petrakov A.M., Shevtsov V.A. *Elektrosvyaz'*, 2016, no. 11, pp. 41-45.

22. Volkov A.S., Baskakov A.E. *Trudy MAI,* 2021, no. 118. http://trudymai.ru/eng/published.php?ID=158240. DOI: 10.34759/trd-2021-118-07

Статья поступила в редакцию 16.11.2021; одобрена после рецензирования 27.11.2021; принята к публикации 21.12.2021

The article was submitted on 16.11.2021; approved after reviewing on 27.11.2021; accepted for publication on 21.12.2021.