АНАЛИЗ ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ В СЕТЯХ 4G/LTE

ANALYSIS OF THE ORGANIZATION OF INFORMATION PROTECTION IN 4G/LTE NETWORKS

УДК 621.396.1, 004.056

Шелашников Олег Алексеевич, бакалавр, Поволжский государственный университет телекоммуникаций и информатики, г. Самара

Муртазин Марсель Маратович, бакалавр, Поволжский государственный университет телекоммуникаций и информатики, г. Самара

Shelashnikov O.A. oselasnikov@gmail.com

Murtazin M.M. murtazin998@gmail.com

Аннотация

Технология беспроводной широкополосной мобильной связи четвертого поколения есть стандарт мобильной связи, который с 2010 года постоянно совершенствовался. Развивались технические решения, которые предусматривали расширение полосы пропускания, агрегацию частот и имеет расширенные возможности многолучевой передачи с поддержкой ретрансляции сигнала. С каждым годом количество четвертого поколения подключений увеличивается, а это означает, что возрастает риск кибератак на пользовательское и операторское оборудование. В статье была рассмотрена инфраструктура сети четвертого поколения, компоненты архитектуры безопасности и их взаимосвязь. Проведен анализ организационных и

технических мер обеспечения защиты информации. Система защиты информации основана на общепризнанных стандартах безопасности сетей четвертого поколения. Изложены основные требования по безопасности в сетях четвертого поколения, включая их компоненты при условии их взаимодействия. Рассмотрены основные меры противодействия деструктивному воздействию на объекты защиты в сетях четвертого поколения.

Annotation

Fourth-generation wireless broadband mobile technology is a mobile communications standard that has been continuously improved since 2010. Technical solutions have evolved to include bandwidth expansion, frequency aggregation and has advanced multipath capabilities with support for signal retransmission. Every year the number of fourth-generation user connections increases, which means that the risk of cyber-attacks on user and operator equipment increases. The paper considered the infrastructure of the fourth-generation network with components of security architecture and their relationships. An analysis of organizational and technical measures to ensure information protection was carried out. Information protection system is based on generally recognized security standards of the fourth generation networks. The basic security requirements in the networks of the fourth generation, including their components subject to their interaction. The main measures to counteract the destructive impact on the objects of protection in the networks of the fourth generation are considered.

Ключевые слова: мобильные сети четвертого поколения, требования безопасности, защита информации, LTE, 4G.

Keywords: Fourth-generation mobile networks, security requirements, information security, LTE, 4G.

Инфраструктура сетей четвертого поколения с 4G/LTE с точки зрения безопасности представляет собой комбинацию нескольких защищаемых компонентов и взаимосвязей между ними [1; 2]. Защищаемое пользовательское оборудование (UE) предоставляет доверенные приложения и услуги пользователю и отвечает за передачу данных в сеть и из сети. Оборудование UE содержит аппаратно и программно защищенный универсальный модуль идентификации абонента (USIM), который хранит международный идентификатор абонента мобильной связи (IMSI), однозначно идентифицирующий каждого пользователя. Кроме того, в USIM хранится секретный ключ K для получения дополнительных ключей, используемых во время процедуры аутентификации в сети LTE.

Защищаемые базовые станции, которые реализуют точки доступа на уровне радиоканала к сетям 4G/LTE, называются eNB или eNodeB, причем каждая eNB участвует в процессе шифрования и защиты целостности данных управления радиосвязью, а также шифрования пользовательских данных.

Защищаемый узел управления мобильностью (MME) в сетях 4G обрабатывает установление новых подключений и проводит процесс аутентификации. Он предназначен для управления мобильными данными, где применяется шифрование и защита целостности.

Защищаемый сервер хранения абонентских данных (HSS) хранит аутентификационную информацию мобильных абонентов. Таким образом, он играет центральную роль во время начальной процедуры аутентификации несвязанного UE, предоставляя MME пользовательскую информацию, связанную с информационной безопасностью.

Общая схема, включающая взаимосвязи отдельных защищаемых компонентов сети 4G, показана на рис. 1.

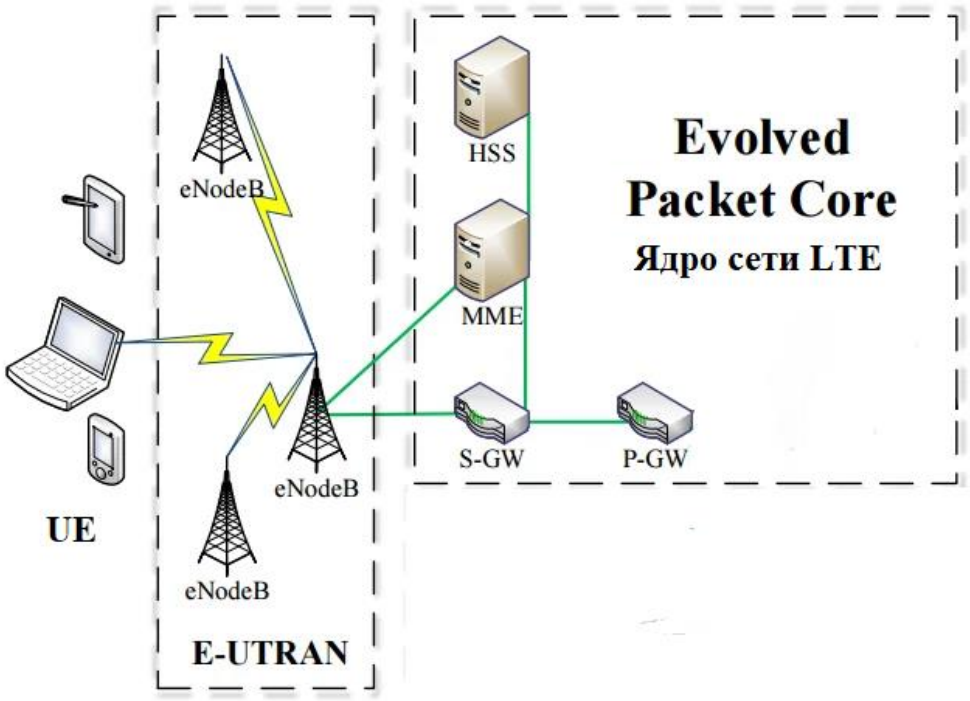

Рис.1 – Архитектура защищаемых компонентов 4G/LTE

При сравнении с глобальной системой мобильной связи (GSM) и с универсальной системой мобильной связи (UMTS), сеть 4G/LTE обладает более развитыми средствами безопасности, например используя взаимную аутентификацию, применяя более длинные ключи шифрования и расширенные иерархии ключей, используемые в алгоритмах шифрования.

Построение сетей 4G/LTE имеет множество отличий от схем, используемых в 3G. Эти отличия позволят добиваться лучшего, либо не уступающего предыдущим стандартам, уровня безопасности. Основные положения для достижения новых требований к безопасности 4G/LTE можно сформулировать следующим образом [3;4]:

– критически важная защищаемая инфраструктура строится иерархическим образом – для каждой операции обработки информации будут использованы различные секретные ключи;

– разделены механизмы безопасности для слоев с доступом и без доступа;

– обеспечивается превентивная защищенность всех уязвимых элементов для уменьшения возможного ущерба при доступе злоумышленника к ключам;

– добавлены специальные механизмы безопасности для взаимодействия между сетями 4G/LTE и 3G.

Существует несколько основных требований к мерам безопасности в сетях 4G, а именно:

– безопасность не ниже уровня сетей типа 3G, без проблем при переключении для пользователя;

– защищенность от атак через интернет;

– беспрепятственный переход от стандарта 3G к стандарту 4G, при создании механизмов защиты для 4G/LTE.

Последнее требование выполняется при использовании механизма аутентификации 3GPP AKA. Требованиями к компоненту EPC, т.е. к ядру сети 4G/LTE выполняются при помощи использования технологии безопасной доменной зоны (NDS), как это описано в стандарте 3GPP TS 33.210.

Поскольку для технологии 4G/LTE схема построения защищенной сети отличается от 3G, некоторые решения безопасности 3G не могут быть полностью использоваться в сетях 4-го поколения. Например, ключи шифрования, с помощью которых защищается текущее соединение при получении управляющих сообщений, не могут храниться в памяти при отсутствии связи с мобильным терминалом. Так же базовая станция eNB не может устанавливаться в незащищенной локации для покрытия внутренних помещений, поскольку при этом многократно возрастает риск несанкционированного доступа к ней [5].

Специально для этого были созданы следующие меры противодействия.

– использование ключа безопасности и иерархии соединений, а именно в 4G/LTE есть пять главных правил построения соединений;

– управление ключами, где выделяют три главные функции в управлении ключами – создание, распространение и генерация;

– использование аутентификации, шифрования и защиты целостности с учетом частого обновления процесса аутентификации, происходящего при обмене порядковых номеров в сообщениях механизмов безопасности;

– использование уникальных идентификаторов пользователей, причем в 4G существует некоторое количество механизмов идентификаторов пользователей, а именно: международный идентификатор мобильного оборудования (IMEI) – уникальный для каждой мобильной станции; M-TMSI – временный идентификатор для пользовательского устройства в узле MME; временный идентификатор сотовой радиосети (C-RNTI), он является временным и уникальным для пользовательского устройства UE [6].

В целом защищаемый трафик 4G/LTE можно разделить на два типа: пользовательские данные и данные управления. Особое внимание уделяется шифрованию пользовательских данных. Шифрование активируется командой RRC «Режим безопасности», которая определяет алгоритм шифрования сообщений. Оператор связи так же может выбрать, какой алгоритм целостности будет использоваться при передаче сообщений.

Для установления защищенного канала связи с сетью 4G/LTE используется взаимная аутентификация между UE и сети, которая является обязательным требованием стандарта безопасности. Без аутентификации ни одна из частей ссылки не может полностью доверять другой стороне.

Несмотря на то, что 4G/LTE продолжает улучшаться, существует несколько проблем безопасности. Это прежде всего недостаточная гибкость и масштабируемость архитектуры 4G/LTE из-за чего и появляются уязвимости и лазейки в сетях. Также затруднено обнаружение и эффектное противодействии DoS-атакам, которые нарушают IP-доступ через беспроводные сети, при этом злоумышленники постоянно создают новые варианты атак на базовые станции eNB, в том числе через пользовательское оборудование UE. Противодействие этим и иным деструктивным воздействиям представляет собой направление дальнейших исследований.

Литература

1. Угрозы безопасности ядра пакетной сети 4G [Электронный ресурс] / Компания «Positive Technologies». – Электрон. текстовые дан. и граф. дан. – М.: офиц. сайт, 2017. - Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/epc-2017/?sphrase_id=74511, свободный. – Загл. с экрана.

2. Белянков, Д.А., Цветков В.Ю. Безопасность и конфиденциальность в сетях 4G/4G/LTE [Текст]/ Д.А. Белянков, В.Ю. Цветков – 56-я науч. конф. аспирантов, магистрантов и студентов БГУИР: тр. конф. – Минск, 2020. – С. 122–124.

3. Анализ защищенности системы безопасности 4G/LTE-A от направленного воздействия DOS-атак [Электронный ресурс]/ Н.В Кормильцев, А.Д. Уваров, И.И. Хаматнуров, М.В. Тумбинская. – Электрон. текстовые дан. и граф. дан. – М.: офиц. сайт, 2019. - Режим доступа: https://www.fin-izdat.com/journal/national/detail.php?ID=74026, свободный. – Загл. с экрана.

4. 4G/LTE и 5G с точки зрения криптографии [Электронный ресурс] / Компания «АО «НПК «Криптонит»». – Электрон. текстовые дан. и граф. дан. – М.: офиц. сайт, 2021. - Режим доступа: https://kryptonite.ru/revolte, свободный. – Загл. с экрана.

5. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses (Release 16) [Electronic resource] / Sofiya, 2019.– Access mode: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2297

6. Высоцкая, В.В., Лыньков, Л. М. Безопасность и конфиденциальность в сетях 4G/4G/LTE [Текст]/ В.В. Высоцкая, Л.М. Лыньков. – 54-я Науч. конф. аспирантов, магистрантов и студентов БГУИР: тр. конф. – Минск, 2018. – С. 74–75.

Literature

1. Threats to the security of the core of the 4G packet network [Electronic resource] / Positive Technologies Company. – Electron. text data. and count. dan. – M.: ofits. website, 2017. - Access mode: https://www.ptsecurity.com/ru-ru/research/analytics/epc-2017/?sphrase_id=74511 , free. – Blank from the screen.

2. Belyankov, D.A., Tsvetkov V.Yu. Security and privacy in 4G/4G/LTE networks [Text]/ D.A. Belyankov, V.Yu. Tsvetkov – 56th scientific conference. postgraduates, undergraduates and students of BSUIR: tr. conf. – Minsk, 2020. – pp. 122-124.

3. Analysis of the security of the 4G/LTE-A security system from the directed impact of DOS attacks [Electronic resource]/ N.V. Kormiltsev, A.D. Uvarov, I.I. Hamatnurov, M.V. Tumbinskaya. – Electron. text data. and count. dan. – M.: ofits. website, 2019. - Access mode: https://www.fin-izdat.com/journal/national/detail.php?ID=74026 , free. – Blank from the screen.

4. 4G/LTE and 5G from the point of view of cryptography [Electronic resource] / The company "JSC "NPC "Kryptonite"". – Electron. text data. and count. dan. – M.: ofits. website, 2021. - Access mode: https://kryptonite.ru/revolte , free. – Blank from the screen.

5. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses (Release 16) [Electronic resource] / Sofiya, 2019.– Access mode: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2297

6. Vysotskaya, V.V., Lynkov, L. M. Security and privacy in 4G/4G/LTE networks [Text]/ V.V. Vysotskaya, L.M. Lynkov. – 54th Scientific Conference. postgraduates, undergraduates and students of BSUIR: tr. conf. – Minsk, 2018. – pp. 74-75.