УДК 004.056

Аутентификация в сетях сотовой связи: обзор математических моделей

Бойко А. А., Быков М. Ю., Кущев С. С., Перегудов М. А.

Постановка задачи: *в настоящее время актуальной является задача защиты сетей сотовой связи от компьютерных атак, эксплуатирующих уязвимости процедур аутентификации. Ее решение состоит в совершенствовании процедур аутентификации и создании аппаратно-программных средств, способных обнаружить и нейтрализовать компьютерные атаки, эксплуатирующие неустранимые уязвимости. Это решение должно опираться на результаты моделирования.* ***Цель работы:*** *анализ существующих моделей процедур аутентификации в сетях сотовой связи на предмет возможности воспроизведения угроз, обусловленных известными и ранее не исследованными потенциальными уязвимостями.* ***Используемый метод:*** *системный анализ.* ***Новизна:*** *рассмотрение процесса аутентификации в сетях сотовой связи в контексте влияния на него совокупности компьютерных атак, эксплуатирующих известные и ранее не исследованные потенциальные уязвимости.* ***Результат:*** *установлено, что существующие математические модели процесса аутентификации в сетях сотовой связи не взаимосвязаны и ориентированы на производительность или защиту от атак, эксплуатирующих уязвимости, приводящие к вскрытию или модификации данных, вскрытию идентификаторов абонентов, дешифрации информации, рассинхронизации сети или многократному повтору запросов. Выявлена необходимость разработки моделей, воспроизводящих в процессе аутентификации взаимодействие различных подсистем сотовой связи и учитывающих влияние уязвимостей, приводящих к анализу активности абонентов сети, принудительному завершению аутентификации, созданию задержки в процессе передаче информации и переполнению памяти элементов сети.* ***Практическая значимость:*** *результаты исследования могут быть полезны специалистам, отвечающим за защищенность сетей сотовой связи от компьютерных атак.*

Ключевые слова: *сеть сотовой связи, аутентификация, математическая модель, уязвимость, компьютерная атака.*

Актуальность

Настоящая статья продолжает цикл работ авторов, посвященных исследованию эффективности процедур аутентификации в сетях сотовой связи. В статье [1] приведен обзор уязвимостей процедур аутентификации сетей сотовой связи поколений 2G…5G и показаны новые уязвимости, выявленные с использованием метода генерации компьютерных атак (см. [2]), позволяющие:

1) вскрывать обмен данными между абонентом и сетью (в т.ч. о сбоях);
2) вскрывать идентификаторы абонентов;
3) дешифровывать информацию абонентов;
4) проводить анализ интенсивности активности абонентов сети;
5) модифицировать данные в сети;

Библиографическая ссылка на статью:
Бойко А. А., Быков М. Ю., Кущев С. С., Перегудов М. А. Аутентификация в сетях сотовой связи: обзор математических моделей // Системы управления, связи и безопасности. 2025. № 1. С. 187-219. DOI: 10.24412/2410-9916-2025-1-187-219

Reference for citation:
Boyko A. A., Bykov M. Yu., Kuschev S. S., Peregudov M. A. Authentication in Cellular Networks: Overview of Mathematical Models. *Systems of Control, Communication and Security*, 2025, no. 1, pp. 187-219 (in Russian). DOI: 10.24412/2410-9916-2025-1-187-219

6) рассинхронизировать сеть;
7) принудительно завершать аутентификацию и создавать задержки в процессе передаче информации;
8) переполнять память элементов сети;
9) многократно повторять запросы от различных элементов сети.

Результаты анализа известных и вновь выявленных уязвимостей свидетельствуют о необходимости системного подхода к обеспечению безопасности процессов аутентификации в сотовых сетях. Однако, как показано в [1], существующие подходы к аутентификации не являются системными, что снижает эффективность защиты от сложных и многофакторных угроз, нацеленных на обход или нарушение аутентификационных механизмов. Для устранения этого противоречия необходимы математические модели, детально воспроизводящие взаимодействие элементов системы сотовой связи, задействованных в процессе аутентификации. Такие модели должны позволять оценивать эффективность мер защиты в условиях реализации множества взаимосвязанных известных и вновь выявленных уязвимостей в интересах прогнозирования рисков и повышения безопасности сотовой связи.

Цель работы – анализ существующих моделей процедур аутентификации в сетях сотовой связи на предмет возможности воспроизведения угроз, обусловленных известными и ранее не исследованными потенциальными уязвимостями.

Рассматриваемые в статье модели делятся на две группы: аналитико-численные модели процесса аутентификации и средства имитации этого процесса. Каждая модель – это замкнутое представление процесса. Поэтому переменные одной модели не связаны с переменными, имеющими аналогичные обозначения, в других моделях.

1. Обзор аналитико-численных моделей процедуры аутентификации

Модель 1.1. В **2007** году в работе [3] **J. Al-Saraireh** и **S. Yousef** предложили модель процедуры аутентификации для сетей UMTS (Universal Mobile Telecommunications System) с целью снижения трафика и задержек. Она базируется на применении математического аппарата *теории вероятностей* и *комбинаторики*. Идея модели в том, что в центре аутентификации (Authentication Center, AuC) в процессе аутентификации на текущем интервале времени ΔT, который является одинаковым для всех проводимых измерений, для каждой мобильной станции (Mobile Station, MS) формируется не один вектор аутентификации (Authentication Vector, AV), а список из L таких векторов. Это делается для выбора оптимальной длины списка вектора аутентификации L посредством выполнения на AuC следующего алгоритма для значений параметров, полученных на предшествующем интервале времени ΔT [3]:

1) вычисляется интенсивность запросов на аутентификацию λ:

$$\lambda = UAR / \Delta T, \quad (1)$$

где: *UAR* (User Authorization Request) – количество запросов MS на аутентификацию в визитном регистре местоположения (Visitor

Location Register, VLR), поступивших в сеть за рассматриваемый интервал времени ΔT. Здесь и далее курсивом выделяются аббревиатуры, обозначающие численное значение соответствующего показателя;

2) вычисляется среднее количество запросов аутентификации E:

$$E = \left(1 - \frac{\lambda}{\lambda + \mu}\right)^{-L}, \quad (2)$$

где μ – интенсивность ухода MS из VLR за интервал времени ΔT, которая обратно пропорциональна времени пребывания MS в зоне VLR;

3) вычисляется стоимость $C(L)$ для разных длин списка векторов от 1 до L и выбирается AV с минимальной стоимостью. Вычисления оптимальной длины вектора L происходит по следующей формуле расчета стоимости передачи запросов на аутентификацию (Authentication Data Request, ADR):

$$C(L) = E \cdot (L + 2a), \quad (3)$$

где a – параметр задержки передачи данных между узлами сети при заданных сетевых инфраструктуре и технологии.

При малом значении L MS часто запрашивает новые AV, что увеличивает трафик, задержки и энергопотребление. При большом значении L имеет место избыточный трафик, поскольку передается больше информации, чем необходимо. Алгоритм выполняется, пока не найдено такое оптимальное значение L, при котором показатели $C(L)$ и E минимальны.

Модель позволяет сократить сетевой трафик и снизить среднее время задержки аутентификации. Но она не учитывает уязвимости процедуры аутентификации, связанные с вскрытием обмена данными, идентификаторов, дешифровки информации, завершения аутентификации неправильными данными, переполнения памяти и повторных запросов.

Модель 1.2. В **2008** году в работе [4] **W. Liu**, **L. Yang**, **Q. L. Li**, **H. Dai** и **B. Hou** предложили модель для анализа производительности протоколов аутентификации на основе *цепи Маркова*. В ней используются три показателя.

1. Средняя задержка обработки сообщений T_{avg} [4]:

$$T_{\text{avg}} = T_1 + T_2 + T_3 + T_4 + T_5, \quad (4)$$

где: T_1 – время передачи сообщения между пользователем и сервером аутентификации; T_2 – время обработки запроса на сервере; T_3 – время передачи между сервером аутентификации и сервером авторизации; T_4 – время обработки сообщения на сервере авторизации; T_5 – время генерации параметров для сессии.

2. Вероятность потери соединения P_{loss} с использованием распределения вероятностей стационарных состояний [4]:

$$P_{\text{loss}} = \sum_{m=0}^{C_1} \sum_{j=0}^{C_2} \sum_{k=0}^{C_3} \pi_{m,j,k}, \quad (5)$$

где: m – число одновременно обрабатываемых пакетов в очереди на сервере аутентификации; C_1 – максимальная емкость очереди; j – количество пакетов, ожидающих обработку; C_2 – максимальная емкость пула ожидания; k – количество пакетов, находящихся в буфере временного хранения; C_3 – максимальная емкость буфера временного хранения; $\pi_{m,j,k}$ – вероятность нахождения системы

в состоянии, где в очереди m пакетов, в ожидании обработки j пакетов и в буфере k пакетов. Стационарные состояния определяют вероятность нахождения системы в каждом возможном состоянии в долгосрочной перспективе.

Установлено, что увеличение емкости буфера приводит к снижению вероятности потери соединения, а увеличение интенсивности входящих запросов приводит к росту вероятности потери соединения.

3. Оптимальная мягкая временная метка T_S, определяемая как минимум функции затрат аутентификации $C(T)$, которая учитывает риск компрометации и стоимость обработки запросов [4]:

$$C(T) = \sum_{m=0}^{Q_1}\sum_{i=0}^{Q_2}\sum_{j=0}^{Q_3}\sum_{k=0}^{Q_4}(x_{m,i,j,k}\cdot q_{\text{a}} + N\cdot q_{\text{r}}\cdot e^{\beta T}) \ , \quad (6)$$

где: m, i, j, k – индексы состояния системы; Q_1 – максимальное количество пользователей в системе; Q_2 – максимальное количество активных сессий аутентификации; Q_3 – количество запросов в буфере; Q_4 – число возможных состояний сервера; $x_{m,i,j,k}$ – вероятность нахождения системы в m, i, j, k-м состоянии; q_{a} – стоимость обработки одного запроса на аутентификацию; N – общее количество обработанных запросов на аутентификацию; q_{r} – стоимость компенсации рисков, если произошла компрометация безопасности; β – коэффициент скорости роста риска при увеличении времени задержки; T – время ожидания ответа от сервера или время с момента последней аутентификации.

Результаты моделирования показали, что оптимальная мягкая временная метка T_S уменьшается с увеличением скорости роста риска β. При этом среднее время пребывания пользователя в сети оказывает влияние на значение T_S, создавая баланс между уровнем безопасности и нагрузкой на сеть. Эта модель является инструментом оптимизации параметров аутентификационных механизмов на основе компромисса между безопасностью, надежностью и производительностью. Однако она не обеспечивает воспроизведение механизмов защиты от вскрытия обмена данными, идентификаторов, дешифровки информации, модификации данных в сети, рассинхронизации сети, завершения аутентификации неправильными данными, переполнения памяти и повторных запросов.

Модель 1.3. В **2009** году в работе [5] **C. K. Han**, **H. K. Choi**, **J. W. Baek** и **H. W. Lee** предложили модель процедуры аутентификации в сетях LTE. Она базируется на аппарате *теории вероятностей, математической статистики, теории надежности*. В этой модели на текущем интервале времени ΔT, который является одинаковым для всех проводимых измерений на AuC, выполняется следующий алгоритм для численных значений параметров, полученных на предшествующем интервале времени ΔT.

1. Стоимость служебного трафика в зависимости от количества векторов аутентификации $C(K)$:

$$C(K) = ER(K) / EN(K), \quad (7)$$

где: K – количество векторов AV; $ER(K)$ – ожидаемое вознаграждение; $EN(K)$ – ожидаемый интервал восстановления.

Ожидаемое вознаграждение $ER(K)$ равно [5]:

$$ER(K) = C_0 + (K-1)\cdot \sum_{i=1}^{M} p_i \cdot E(y_i) \cdot C_i, \quad (8)$$

где: C_0 – стоимость обработки первого события запроса на аутентификацию; M – количество событий формирования запроса на аутентификацию; p_i – вероятность наступления i-го события; $E(y_i)$ – ожидаемое время наступления i-го события; C_i – стоимость обработки i-го события.

Ожидаемый интервал восстановления $EN(K)$ равен:

$$EN(K) = (K-1)\cdot EY + ED, \quad (9)$$

где: K – количество векторов AV; EY – ожидаемая длительность времени между событиями; ED – среднее время на обработку события.

2. Стоимость сигнализации в зависимости от времени жизни ключа Kasme $C(\Delta T)$ равна [5]:

$$C(\Delta T) = \sum_{i=1}^{M} p_i \cdot \frac{C_0 \cdot T(x_i) + C_i}{\int_0^{\Delta T} (1 - T(x_i))dx_i}, \quad (10)$$

где $T(x_i)$ – вероятность активности ключа x_i в течение интервала времени ΔT.

На рис. 1 показаны повторяющиеся циклы процесса аутентификации со случайными интервалами на примере протокола аутентификации EPS-AKA. События аутентификации показаны как последовательность действий при поддержке модуля управления мобильностью (Mobility Management Entity, MME) и сервера абонентов (Home Subscriber Server, HSS), разделенных случайными промежутками времени. Моменты восстановления отмечают окончание циклов. При каждом новом событии тип запроса выбирается.

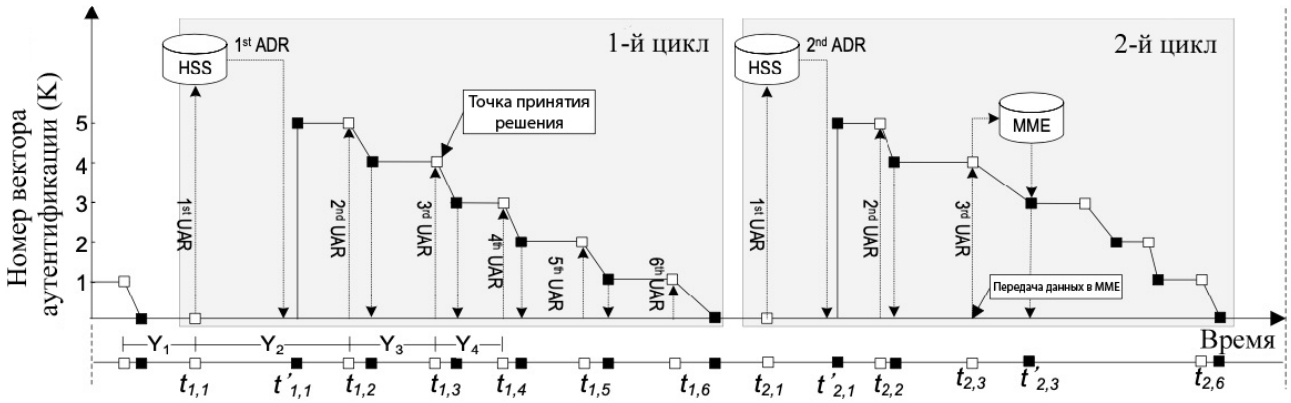

Рис. 1. Временная диаграмма протокола аутентификации EPS-AKA

Результаты моделирования показали, что с ростом интенсивности трафика необходимо увеличивать количество векторов аутентификации K, однако чрезмерное увеличение K приводит к неоправданным временны*ы*м затратам.

Модель учитывает затраты на сигнальную нагрузку при аутентификации, но не воспроизводит аспекты защиты от вскрытия обмена данными, идентификаторов, дешифровки информации, модификации данных в сети, рассинхрони-

зации сети, завершения аутентификации неправильными данными, переполнения памяти и повторных запросов.

Модель 1.4. В **2010** году в работе [6] **А. С. Корсунский** и **О. В. Шейкин** предложили модель процедуры аутентификации в сетях стандарта UMTS, базирующуюся на *теории вероятностей и комбинаторике*. В ней для оценки защищенности от ложных запросов на аутентификацию используется формула для оценки вероятности ошибки при использовании кодового слова помехоустойчивого кода с исправлением ошибок, которая зависит от кратности исправляемых ошибок и количества повторов [6]:

$$P = \frac{n!}{k! \cdot (n-k)!} \cdot \sum_{i=0}^{n} \left(p^i (1-p)^{n-i} \right), \quad (11)$$

где: p – вероятность ошибки на символ; n – длина кодового слова; i – количество ошибок в кодовой последовательности; k – количество ошибок, которые произошли в кодовом слове.

Результаты моделирования показали, что предложенный подход позволяет значительно улучшить точность прогнозирования потенциальных угроз. Однако она фокусируется только на предотвращении ложных запросов и не воспроизводит защиту от вскрытия обмена данными, идентификаторов, дешифровки информации, модификации данных в сети, рассинхронизации сети, переполнения памяти, повторных запросов и анализа активности абонентов.

Модель 1.5. В 2010 году в работе [7] **C. Ntantogian** предложил модель процедуры аутентификации на основе четырехмерной *цепи Маркова* для анализа ложных синхронизаций при переключениях между UMTS и WLAN сетями. В модели для минимизации количества ложных синхронизаций воспроизводится динамика сетевых условий для вычисления показателя Δ – допустимая разность отклонения значения номера последовательности (SQN_{AV}) в сети и значения номера последовательности (SQN_{MS}), хранящегося в MS (такой же показатель используется и далее в модели 1.6 [8]).

Вероятность ложной синхронизации P_{sync}:

$$P_{\text{sync}} = \sum_{\Delta=a+1, W\neq 0} \pi(0,\Delta,U,W) \cdot \frac{\mu_{\text{U}}}{\mu_{\text{U}} + \lambda_{\text{U}}} + \sum_{\Delta=-(a+1), U\neq 0} \pi(1,\Delta,U,W) \cdot \frac{\mu_{\text{W}}}{\mu_{\text{W}} + \lambda_{\text{W}}}, \quad (12)$$

где: π (N, D, U, W) – вероятность нахождения системы в конкретном состоянии (N – состояние сети: $N = 0$ обозначает, что MS находится в сети UMTS, а $N = 1$ – в сети WLAN; D – разность максимального значения номера последовательности (SQN_{AV}) в сети и значения номера последовательности (SQN_{MS}), хранящегося в MS; $U \in [0, L]$ – число сохраненных AV в UMTS, где L – максимально допустимое количество AV; W – количество сохраненных AV в WLAN; μ_{U} – интенсивность пребывания MS в UMTS до переподключения (например, если устройство в среднем проводит 10 минут в UMTS до переподключения, то $\mu_{\text{U}} = 1/10$ мин); λ_{U} – интенсивность запросов на аутентификацию в UMTS; μ_{W} – интенсивность пребывания MS в WLAN до переподключения; λ_{W} – интенсивность запросов на аутентификацию в WLAN.

Если W не равно 0, то MS успешно прошла аутентификацию в сети WLAN и сохранила хотя бы один вектор аутентификации в WLAN.

Установлено, что увеличение интенсивности запросов на аутентификацию в сети UMTS ведет к увеличению среднего числа ложных синхронизаций. Но при достижении оптимального значения показателя Δ дальнейшее увеличение интенсивности запросов не приводит к значительному снижению числа ложных синхронизаций, но негативно влияет на уровень безопасности.

Однако эта модель не воспроизводит процессы вскрытия обмена данными, идентификаторов, дешифровки информации, модификации данных в сети, рассинхронизации сети, завершения аутентификации неправильными данными, переполнения памяти, повторных запросов и анализа активности абонентов.

Модель 1.6. В **2012** году в работе [8] **C. Xenakis**, **C. Ntantogian** и **I. Stavrakakis** предложили модель аутентификации в сетях UMTS. Модель основана на применении *цепей Маркова* и предположении об экспоненциальном распределении времени пребывания мобильного устройства в сетях UMTS и WLAN (Wireless Local Area Network), а также пуассоновского потока запросов на аутентификацию.

Показателем эффективности в этой модели является вероятность рассинхронизации, которая возникает при частой смене доступа между сетями UMTS и WLAN. Эта вероятность P_{sync} равна [8]:

$$P_{\text{sync}} = P_{\text{syncU}} + P_{\text{syncW}}, \tag{13}$$

где P_{syncU} и P_{syncW} – вероятности рассинхронизации при переходе из сети UMTS в WLAN и обратно, соответственно.

Вероятность рассинхронизации P_{syncW} определяется как [8]:

$$P_{\text{syncW}} = \sum_{z>0,\, j=0}^{j=L-1} p_i \cdot \frac{\mu_{\text{U}}}{\mu_{\text{U}} + \lambda_{\text{U}}}, \tag{14}$$

где: p_i – предельная вероятность состояния цепи Маркова; μ_{U} – интенсивность пребывания в UMTS до переподключения; λ_{U} – интенсивность запросов на аутентификацию в UMTS; L – количество AV, генерируемых AuC за сессию.

Вероятность рассинхронизации P_{syncU} определяется как [8]:

$$P_{\text{syncU}} = \sum_{z>0,\, j=0}^{j=L-1} p_i \cdot \frac{\mu_{\text{W}}}{\mu_{\text{W}} + \lambda_{\text{W}}}, \tag{15}$$

где: p_i – предельная вероятность состояния цепи Маркова; μ_{W} – интенсивность пребывания в WLAN до переподключения; λ_{W} – интенсивность запросов на аутентификацию в WLAN.

Условие рассинхронизации [8]:

$$D > \Delta + 1, \tag{16}$$

где: D – разность максимального значения номера последовательности (SQN_{AV}) в сети и значения номера последовательности (SQN_{MS}), хранящегося в MS; Δ – допустимая разность отклонения значения номера последовательности (SQN_{AV}) в сети и значения номера последовательности (SQN_{MS}), хранящегося в MS.

Модель объясняет, почему частые переключения между сетями приводят к расхождению счетчиков последовательностей (SQN) MS и сети, и как этот процесс приводит к рассинхронизациям. На рис. 2 представлена временн*а*я диаграмма, демонстрирующая последовательность обмена сообщениями между AuC и MS через узел обслуживания абонентов пакетной сети передачи данных

(Serving GPRS Support Node, SGSN) и сервер аутентификации, авторизации и управления доступом (Authentication, Authorization and Accounting Server, AAA server). Ось абсцисс отображает время, а вертикальные линии в моменты t_1 ... t_8 обозначают процессы, когда MS либо переключается между сетями, либо запрашивает аутентификацию. При каждом переключении MS выполняет аутентификацию с помощью алгоритма аутентификации UMTS-AKA (Authentication and Key Agreement) в UMTS или алгоритма аутентификации EAP-AKA в WLAN. На этом рисунке показано, как меняются счетчики (черные круги с числами) последовательности на AuC и на MS в процессе аутентификации. В точке t_8 происходит рассинхронизация, когда MS отклоняет действительное значение *AV* из-за того, что разность значений SQN_{HE} и SQN_{MS} превышает Δ.

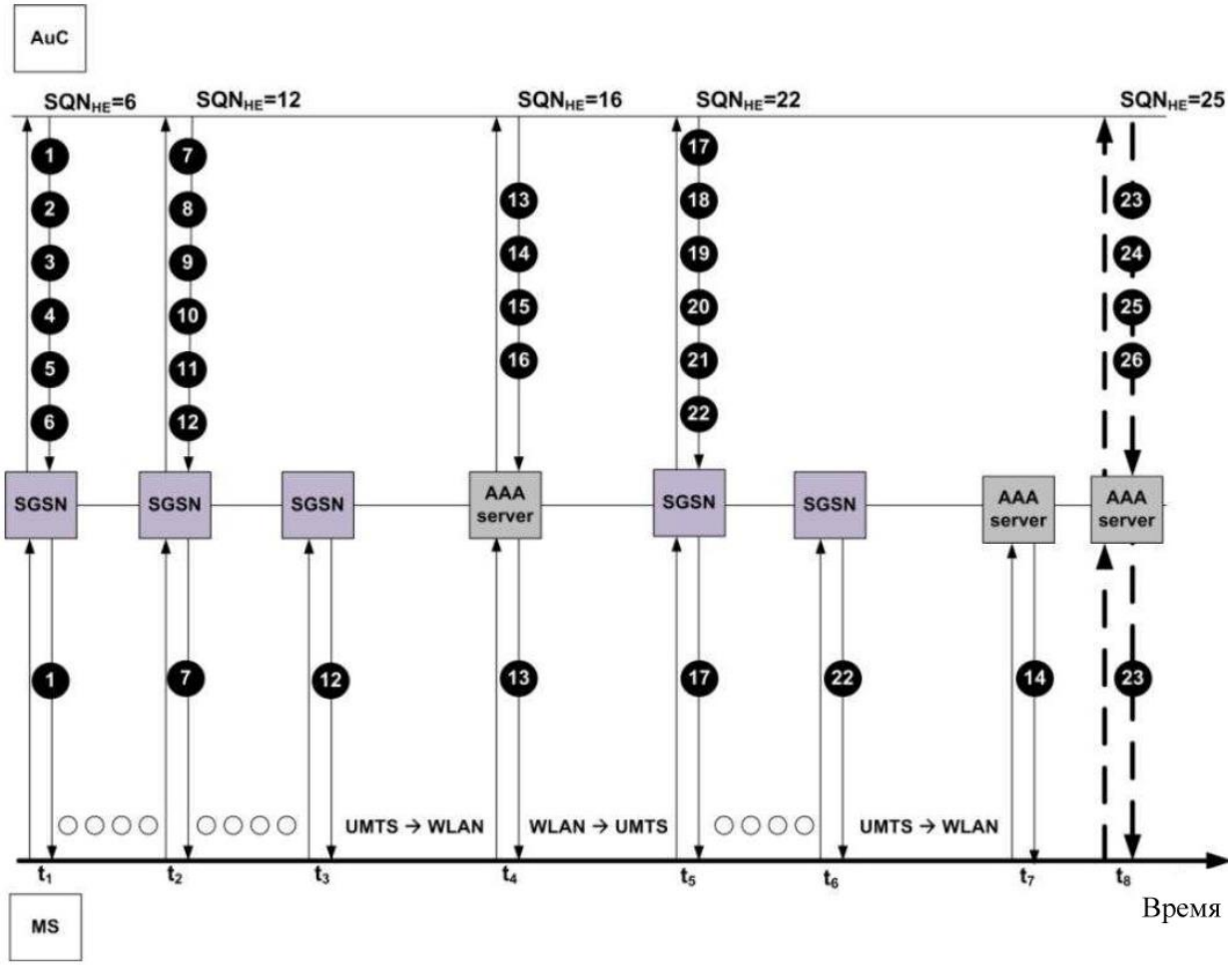

Рис. 2. Пример рассинхронизации в интегрированной сети 3G-WLAN

На рис. 3 показана цепь Маркова для случая, когда MS находится в сети UMTS и выполняет аутентификацию. В этом случае последний полученный SQN_{AV} от UMTS больше, чем последний полученный от WLAN, и MS имеет доступные AV в SGSN.

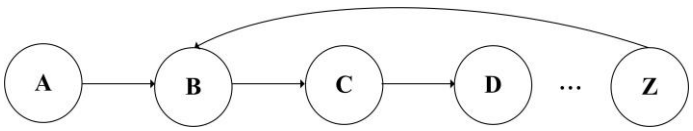

Рис. 3. Цепь Маркова: MS в сети UMTS и выполняет аутентификацию

Состояние A – совокупность состояний цепи Маркова, где MS находится в UMTS, и SGSN имеет доступные AV. Состояние B – совокупность состояний, куда система переходит из состояния A, когда MS производит аутентификацию, используя один из доступных AV, в результате чего в SGSN AV становится на единицу меньше, а разница между SQN_{AV} и SQN_{MS} увеличивается. Состояние C – подготовка к передаче в WLAN, а состояние D – завершение аутентификации перед переподключением. Состояние Z – это ситуация, когда MS находится в UMTS, но в SGSN отсутствуют AV. Переход из A в B обозначает событие аутентификации. Также существует возможность перейти из Z в B при последующей аутентификации, когда в SGSN появляется новый список AV.

На рис. 4 показана цепь Маркова для случая, когда MS переключается из WLAN в UMTS и инициирует процедуру запроса аутентификационных данных ADR для получения новой партии векторов аутентификации AV. В этом случае последний полученный SQN_{AV} от UMTS больше, чем последний полученный от WLAN, и MS переходит из сети WLAN в UMTS. Состояния B…Z – это совокупность состояний, в которых MS находится в сети WLAN с различным количеством AV в AAA сервере. В состояние A система переходит, когда MS переключается в UMTS и получает новую партию AV.

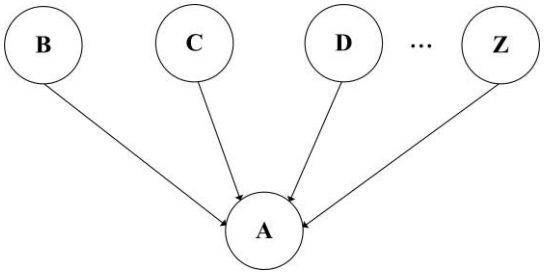

Рис. 4. Цепь Маркова: MS переключается из WLAN в UMTS

Однако эта модель имеет узкую специализацию на проблеме рассинхронизации. Как и предыдущие модели, она не учитывает угрозы вскрытия обмена данными, идентификаторов, дешифровки информации, модификации данных, завершения аутентификации неправильными данными, переполнения памяти, повторных запросов и анализа активности абонентов.

Модель 1.7. В **2013** году в работе [9] **А. Г. Сабанов** предложил модель процесса аутентификации, основанную на разделении его на этапы с различными временными характеристиками. Она базируется на применении теории *систем массового обслуживания* и *цепей Маркова*. Показателями эффективности в этой модели являются вероятность успешной аутентификации и вероятность опасных отказов, приводящих к несанкционированному доступу. Модель воспроизводит систему аутентификации как систему массового обслуживания с интенсивностью входящего пуассоновского потока заявок λ и интенсивностью обработки заявок системой аутентификации μ.

Коэффициент загрузки такой системы равен [9]:

$$\rho = \lambda / \mu . \qquad (17)$$

Если $\rho < 1$, то система работает в стационарном режиме, и переходы системы из одного состояния в другое моделируются с помощью цепи Маркова (см. рис. 5). Модель включает следующие состояния: 1 – абонент отправил запрос на регистрацию; 2 – имеются данные от MS и AuC для проверки пользователя; 3 – имеются данные для проверки валидности MS; 4 – имеются на сервере все данные для начала процесса авторизации.

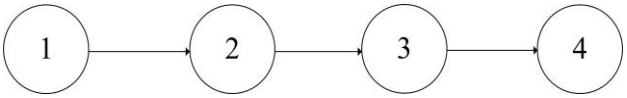

Рис. 5. Цепь Маркова: MS переключается из WLAN в UMTS

Для вычисления стационарных вероятностей системы используется следующий подход. P_1 – это вероятность того, что система находится в начальном состоянии, остальные вероятности выражаются через P_1 с учетом вероятностей переходов [9]:

$$P_2 = P_1 \cdot p_{12}; \quad (18)$$

$$P_3 = P_1 \cdot p_{12} \cdot p_{23}; \quad (19)$$

$$P_4 = P_1 \cdot p_{12} \cdot p_{23} \cdot p_{34}, \quad (20)$$

где p_{ij} – вероятность перехода системы из состояния i в состояние j.

Все вероятности переходов могут быть выражены через вероятность P_1. Для нормировки системы сумма всех вероятностей равна 1.

Рассчитанные стационарные вероятности P_2, P_3, P_4 являются ключевыми для оценки надежности системы аутентификации. Они отражают вероятность нахождения системы в каждом из состояний на длительном интервале времени. Более того, на основе этих вероятностей можно оценить вероятность того, что система не сможет продолжить свою работу из-за сбоя на одном из этапов аутентификации.

Результаты моделирования показывают, что разные этапы аутентификации имеют разную вероятность отказа, и учет этих вероятностей необходим для оценки общей надежности системы. Анализ позволил выявить критические точки процесса, требующие особого внимания при проектировании и эксплуатации. Однако:

1) стационарность нагрузки не позволяет учитывать динамические изменения в работе, когда происходит резкие всплески нагрузки;
2) не рассматриваются процессы вскрытия обмена данными, идентификаторов, дешифровки информации, модификации данных в сети, рассинхронизации сети, завершения аутентификации неправильными данными, переполнения памяти, повторных запросов, выявления активности абонентов.

Модель 1.8. В **2014** году в работе [10] **М. С. Аристов**, **О. И. Шишин**, **А. М. Рапетов**, **А. С. Крымов** и **А. Д. Егоров** предложили модель для оценки уязвимости процедуры аутентификации беспроводных сетей к атакам типа «человек посередине» (англ. Man-In-The-Middle attack, MitM). Модель базируется на применении *исчисления предикатов*. Она включает т.н. «туннельную модель» (формализует условия незащищенности аутентификационных сообще-

ний, возможности их модификации атакующим и отсутствия двусторонней аутентификации) и следующие утверждения, описывающие взаимодействие между участниками сети (абонент, злоумышленник, сервер):

1) утверждение *p*: абонент А и абонент В могут обмениваться сообщениями через радиоканал без защиты, что предоставляет возможность злоумышленнику вмешиваться в процесс;
2) утверждение *q*: сообщения аутентификации передаются без шифрования, что позволяет атакующему перехватывать и изменять их;
3) утверждение *r*: отсутствие двусторонней аутентификации делает систему уязвимой к манипуляциям со стороны злоумышленника.

Модель также содержит следствие *S*: элементы MS, BTS / BSC (Base Transceiver Station / Base Station Subsystem) и MitM удовлетворяют «туннельной модели», что подтверждает уязвимость системы. То есть если утверждения *p*, *q* и *r* истинны, то система подвержена атакам MitM [10]:

$$p \cap q \cap r \Rightarrow S\,. \tag{21}$$

Однако эта модель не воспроизводит аспекты защиты от вскрытия идентификаторов и дешифрования информации, поскольку концентрируется на обмене сообщениями. Кроме того, она не учитывает рассинхронизацию сети, завершение аутентификации неправильными данными, переполнение памяти, повторные запросы, анализ активности абонентов и модификацию данных в сети (хотя атаки MitM используют это). Отсутствие учета вычислительной сложности также является ограничением этой модели.

Модель 1.9. В **2014** году в работе [11] **И. В. Углов** предложил модель функционирования сети сотовой связи с использованием технологии CSFB (Circuit Switched FallBack). Эта модель основана на применении *теории сетей массового обслуживания* и *теории вероятностей*. Она ориентирована на анализ производительности. Показателем эффективности в этой модели является вероятность успешного установления соединения в заданное время. Узлы сети моделируются как системы массового обслуживания с произвольным характером входящих потоков заявок *G*, количеством обслуживающих элементов *m* и ограниченной емкостью очереди *N*.

Для расчета характеристик в модели используются следующие формулы:

1) вероятность успешного установления соединения $P_{\text{усп}}$ равна [11]:

$$P_{\text{усп}} = 1 - P_{\text{отказа}}, \tag{22}$$

где $P_{\text{отказа}}$ – вероятность отказа в обслуживании заявки;

2) среднее время ожидания заявки в очереди W_{q} равно [11]:

$$W_{\text{q}} = p^{m} \cdot \frac{m \cdot P_0}{m! \cdot (1-\rho/m)^2} \cdot \lambda^{-1}, \tag{23}$$

где: m – количество обслуживающих каналов; P_0 – вероятность того, что все обслуживающие каналы свободны; $\rho = \lambda\left(\mu m\right)^{-1}$ – коэффициент загрузки системы; λ – интенсивность входящего потока заявок; μ – интенсивность обслуживания одной заявки; p – вероятность того, что канал занят;

3) среднее время установления соединения T_{conn} равно [11]:

$$T_{\text{conn}} = W_{\text{q}} + \mu^{-1}. \tag{24}$$

Модель позволила обосновать необходимость применения для разных узлов сети разных систем массового обслуживания, учитывающих их архитектурные особенности. Однако в этой модели отсутствует учет реализации компьютерных атак, влияющих на работу сети.

В **2015** году в диссертации [12] **И. В. Углов** предложил усовершенствованную модель, которая подробно воспроизводит архитектуру фрагмента сети MSC/VLR/HLR (Mobile Switching Center/Visitors Location Register/Home Location Register) и учитывает разные классы заявок и вероятностные переходы между элементами. Однако она не воспроизводит какие-либо атаки на сеть.

Модель 1.10. В **2016** году в работе [13] **А. А. Васильченко** и **А. В. Кочуров** предложили модель процедуры аутентификации в стандарте GSM на базе аппарата *марковских процессов* (рис. 6). Описание состояний см. в таблице 1.

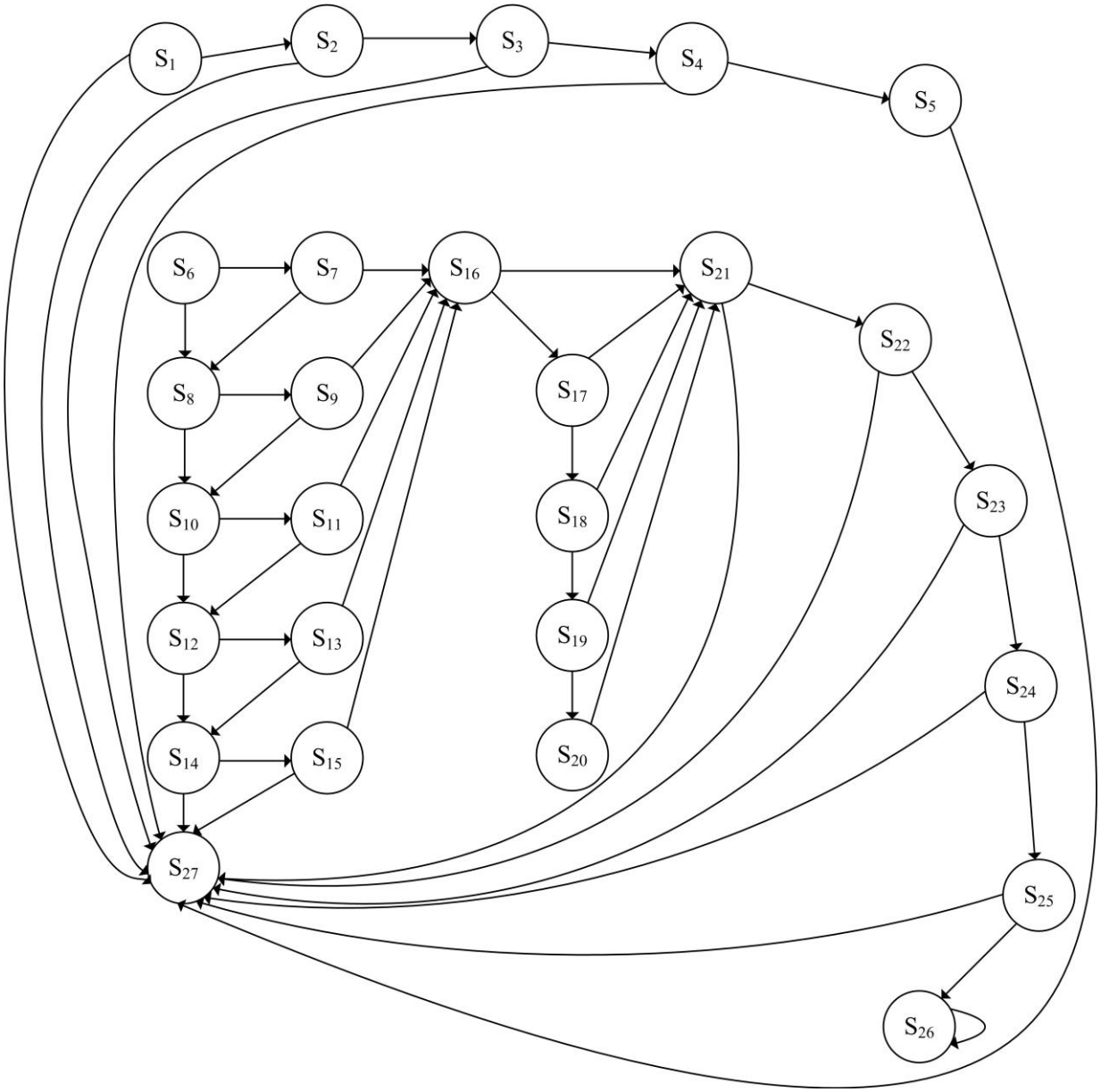

Рис. 6. Цепь Маркова: процедура аутентификации в стандарте GSM

Таблица 1– Описание состояний модели

Узел	Описание
S_1	MS-инициатор шлет сообщение на BS с запросом установления сигнального канала.
S_2	BS приняла сообщение от MS. Если на BS есть свободный сигнальный канал для установления соединения, то BS выделяет сигнальный канал и пересылает данные о нем на MS. Если нет возможности выделить сигнальный канал, то на MS выдается сигнал «Отказ».
S_3	По истечении тайм-аута повторной передачи MS не получила информацию о выделении сигнального канала.
S_4	BS приняла сообщение от MS после повторной передачи. Если на BS есть свободный сигнальный канал, то BS выделяет сигнальный канал и пересылает данные о нем на MS. Если нет возможности выделить сигнальный канал, то на MS выдается сигнал «Отказ».
S_5	По истечении тайм-аута двукратной повторной передачи MS не получила информацию о выделении сигнального канала.
S_6	BS приняла сообщение от MS после 2-кратной повторной передачи. Если на BS есть свободный сигнальный канал, то BS выделяет сигнальный канал и пересылает данные о нем на MS. Если нет возможности выделить сигнальный канал, то на MS выдается сигнал «Отказ».
S_7	По истечении тайм-аута 3-кратной повторной передачи MS не получила информацию о выделении сигнального канала.
S_8	BS приняла сообщение от MS после 3-кратной повторной передачи. Если на BS есть свободный сигнальный канал, то BS выделяет сигнальный канал и пересылает данные о нем на MS. Если нет возможности выделить сигнальный канал, то на MS выдается сигнал «Отказ».
S_9	По истечении тайм-аута 4-кратной повторной передачи MS не получила информацию о выделении сигнального канала.
S_{10}	По истечении тайм-аута 2-кратной передачи BS2 не получила подтверждения об успешном приеме MS и запроса о выделении сигнального канала для MS.
S_{11}	MS приняла сообщение от BS2 после 2-кратной передачи и запрашивает у BS2 выделенный сигнальный канал для продолжения процесса установления соединения.
S_{12}	По истечении тайм-аута 3-кратной передачи BS2 не получила подтверждения об успешном приеме MS и запроса о выделении сигнального канала для MS.
S_{13}	MS приняла сообщение от BS2 после трехкратной передачи и запрашивает у BS2 выделенный сигнальный канал для продолжения процесса установления соединения.
S_{14}	По истечении тайм-аута 4-кратной передачи BS2 не получила подтверждения об успешном приеме MS и запроса о выделении сигнального канала для MS.
S_{15}	MS приняла сообщение от BS2 после 4-кратной передачи и запрашивает у BS2 выделенный сигнальный канал для продолжения процесса установления соединения.
S_{16}	BS2 приняла сообщение от MS. Если на BS2 есть свободный сигнальный канал для установления соединения, то BS2 выделяет сигнальный канал и пересылает данные о нем на MS. Если нет возможности выделить сигнальный канал, то на MS выдается сигнал «Отказ».
S_{17}	По истечении тайм-аута повторной передачи MS не получила информацию о выделении сигнального канала. Если на BS2 есть свободный сигнальный канал для установления соединения, то BS2 повторно выделяет сигнальный канал и пересылает данные о нем на MS. Если нет возможности выделить сигнальный канал отсутствует, то на MS выдается сигнал «Отказ».
S_{18}	По истечении тайм-аута 2-кратной повторной передачи MS не получила информацию о выделении сигнального канала. Если на BS2 есть свободный сигнальный канал для установления соединения, то BS2 повторно выделяет сигнальный канал и пересылает данные о нем на MS. Если нет возможности выделить сигнальный канал, то на MS выдается сигнал «Отказ».
S_{19}	По истечении тайм-аута 3-кратной повторной передачи MS не получила информацию о выделении сигнального канала. Если на BS2 есть свободный сигнальный канал для установления соединения, то BS2 повторно выделяет сигнальный канал и пересылает данные о нем на MS. Если нет возможности выделить сигнальный канал, то на MS выдается сигнал «Отказ».
S_{20}	По истечении тайм-аута 4-кратной повторной передачи MS-ответчик не получил информацию о выделении сигнального канала. Если на BS2 есть свободный сигнальный канал для установления соединения, то BS2 повторно выделяет сигнальный канал и пересылает данные о нем на MS. Если нет возможности выделить сигнальный канал, то на MS выдается сигнал «Отказ».
S_{21}	MS успешно приняла сообщение о выделении сигнального канала от BS2 и по сигнальному каналу запрашивает виртуальный канал на коммутатор MSC2 и далее на VLR2.

Узел	Описание
S_{22}	VLR2 успешно приняла запрос на установление виртуального канала и отправляет на MS *RAND* – случайное число (в рамках процедуры аутентификации).
S_{23}	MS успешно приняла сообщение со случайным числом *RAND*, обрабатывает его, на его основе получает число *SRES* (Signed Response) и передает назад на VLR2.
S_{24}	VLR2 успешно принял сообщение от MS, содержащее *SRES*; VLR2 независимо вычисляет *SRES* и сравнивает с полученным от MS. Если два числа совпадают, то VLR2 шлет сообщение на продолжение установление соединения на BS2. Иначе на MS выдается сигнал «Отказ».
S_{25}	BS2 успешно прияла сообщение с подтверждением дальнейшей возможности установления соединения от MS. Если на BS2 есть свободный трафиковый канал для установления соединения, то BS2 выделяет трафиковый канал и пересылает данные о нем на MS. Если нет возможности выделить трафиковый канал, то на MS выдается сигнал «Отказ»
S_{26}	VLR успешно принял сообщение от MS о запросе начала вызова (состояние соединения).
S_{27}	Состояние «Отказ».

В модели вероятность отказа по причине занятости каналов вычисляется по формуле Эрланга для случая занятости всех имеющихся каналов [13]:

$$P = \frac{(\mu \cdot y)^V}{V!} \cdot \sum_{i=0}^{V-1} \frac{(\mu \cdot y)^i}{i!}, \tag{25}$$

где: μ – интенсивность обслуживания (обратная величина средней длительности телефонного разговора); y – нагрузка на сеть (общая информационная нагрузка от всех абонентов); V – количество каналов на базовой станции.

Модель позволяет прогнозировать эффективность работы сети и оптимизировать ее параметры для минимизации потерь и улучшения качества связи. Однако она, не воспроизводит вскрытие обмена данными, идентификаторов, дешифровку информации, модификацию данных в сети, рассинхронизацию сети, завершение аутентификации неправильными данными, переполнения памяти, повторных запросов и анализа активности абонентов.

Модель 1.11. В **2016** году в работе [14] **M. Khan** и **N. Khan** предложили модель процесса аутентификации стандарта GSM в условиях реализации т.н. атак Сивиллы, когда одно устройство (сибил-узел) модифицирует подписанные ответы *SRES*, выдавая себя за несколько устройств с разными идентификаторами, и жертвы подключаются только к узлам, контролируемым злоумышленником. В основе модели лежит *теория вероятностей и комбинаторика.* Суммарная вероятность успешной атаки $P_{\max}$, учитывающая все случаи от одного до M атакующих узлов, вычисляется по формуле [14]:

$$P_{\max} = \sum_{j=0}^{M} \frac{M!}{j! \cdot (M! - j!)} \cdot \frac{\beta^j}{2^{\alpha M}} \cdot (2^{\alpha} - \beta)^{M-j}, \tag{26}$$

где: M – количество атакующих сибил-узлов; β – размер пула ключей; α – размер ключа аутентификации.

В [14] доказано превосходство предложенного механизма аутентификации над механизмами LwSAD (Lightweight Sybil Attack Detection) и LBAD (Location Based Attack Detection), состоящее в снижении нагрузки на вычислительные средства сети в части трафика и энергозатрат. Однако она, фокусируясь на конкретном типе атак, не воспроизводит иные атаки.

Модель 1.12. В **2017** году в работе [15] **Д. М. Актанбаев** предложил модель для оценки эффективности использования канала передачи данных в сетях сотовой связи. Показателем эффективности в этой модели является средняя вероятность блокировки вызова. Модель основана на применении *цепей Маркова* и *систем массового обслуживания*, предполагая пуассоновский характер потоков заявок и произвольное распределение длительности обслуживания. Качество обслуживания отражено в показателе доли потерянных заявок π_k, представляющей сумму вероятностей всех состояний системы, когда дополнительная заявка не может быть принята из-за нехватки канального ресурса [15]:

$$\pi_k = \sum_{(i_1,i_2,...,i_n)\in U_k} p(i_1,i_2,...,i_n), \tag{27}$$

где U_k – множество состояний, при которых k-я заявка потока теряется, то есть система не может принять заявку из-за недостатка канала.

Средняя вероятность блокировки вызова вычисляется с учетом весовых коэффициентов, отражающих долю каждого класса трафика [15]:

$$P_{cp} = \frac{\sum_{k}^{n}\left(a_k \cdot \pi_k\right)}{\sum_{k}^{n} a_k}, \tag{28}$$

где: a_k – весовой коэффициент для каждого типа трафика (голосовые звонки, видеозвонки, загрузка файлов и веб-страниц), n – количество потоков заявок на выделение канального ресурса.

Применение модели позволило оптимизировать распределение канального ресурса между различными сервисами, минимизируя потери. Однако она не воспроизводит компьютерные атаки.

Модель 1.13. В **2017** году в работе [16] **Э. Р. Зарипова** и **А. Ардила Пинто** предложили модель для оценки времени установления соединения по радиоканалу случайного доступа. Процедура установления соединения воспроизводится *цепью Маркова* с состояниями (n, m, k), где n – число ретрансляций сообщения на этапе, когда устройство абонента пытается инициировать связь с базовой станцией (Msg1), m – число ретрансляций при передаче сообщения HARQ (Hybrid Automatic Repeat reQuest) (Msg3), k – число успешной переданных Msg1, после которых все последующие Msg3 оказались неуспешными. Начальное состояние модели (0, 0, 0). Поглощающие состояния – успешное и неуспешное установление соединения, соответственно. Вероятность успешного установления соединения после состояния (n, m, k) равна [16]:

$$Q(n,m,k) = P(n,m,k)\cdot(1-g)\,p_{\omega}^{-1}, \tag{29}$$

где: $P(n, m, k)$ – вероятность того, что система в процессе выполнения аутентификации находится в состоянии (n, m, k); p_{ω} – вероятность успешного выполнения операции аутентификации; g – вероятность коллизии Msg3.

Вероятность успешной аутентификации равна [16]:

$$p_{\omega} = 1 - \left(p + (1-p) g^{M+1} \right)^{N+1}, \tag{30}$$

где: p – вероятность коллизии преамбулы; g – вероятность коллизии Msg3; M и N – максимальное число ретрансляций Msg3 и Msg1, соответственно.

Время установления соединения для состояния (n, m, k) равно [16]:

$$T(n,m,k) = (n-k)(\triangle_1 + \triangle_2) + k(\triangle_1 + \triangle_3 + M\triangle_4) + \triangle_1 + \triangle_3 + (m+1)\triangle_4, \tag{31}$$

где: Δ_1 – время синхронизации и подготовки к передаче Msg1; Δ_2 – время передачи Msg1 и ожидания; Δ_3 – время обработки успешно принятого Msg2; Δ_4 – время передачи Msg3, получения ответа Msg4 и его обработки.

Среднее время установления соединения D равно [16]:

$$D = \sum_{(n,m,k) \in X} Q(n,m,k) T(n,m,k), \tag{32}$$

где $Q(n, m, k)$ – вероятность завершения соединения в состоянии (n, m, k).

Модель фокусируется исключительно на анализе производительности, игнорируя вопросы безопасности и не учитывая динамические изменения в интенсивности запросов и ошибки во время процедуры соединения.

Модель 1.14. В **2017** году в работе [17] **Т. М. Татарникова** и **Н. В. Яготинцева** предложили модель процедуры аутентификации в инфокоммуникационной сети на основе *теории вероятностей*. Показателем эффективности в модели является вероятность неустановления соединения за время, не превышающее допустимое. Время установления соединения $t_{\text{ус}}$ равно [17]:

$$t_{\text{ус}} = \sum_{i=1}^{n_{\text{п}}} t_{\text{п}i} + \sum_{i=1}^{n_{\text{о.в}}} t_{\text{о.в}i} + n_{\text{р}} \cdot t_{\text{р}}, \tag{33}$$

где: $n_{\text{п}}$ – число путей, пройденных вызовом; $n_{\text{о.в}}$ – число путей, на которые вызов вернулся в режиме «обратной волны»; $n_{\text{р}}$ – число рестартов (не превышающее заданное значение); $t_{\text{п}i}$ – время прохождения i-го пути; $t_{\text{о.в}i}$ – время прохождения в режиме обратной волны; $t_{\text{р}}$ – время выполнения рестарта.

Вероятность неустановления соединения выражается формулой [17]:

$$M_{\xi} = \sum_{c=c_{\min}}^{c_{\max}} \frac{1}{N} \sum_{k=1}^{N} \xi(x_c), \tag{34}$$

где: c – число неработоспособных путей; N – общее количество испытаний; $\xi(x_c)$ – значение случайной величины ξ при k-й реализации; $c_{\min}$ и $c_{\max}$ – минимальное и максимальное число используемых путей, соответственно.

Выражение (34) включает случайную величину $\xi(x_c)$, которая принимает значение 1, если соединение не установлено, и 0, если установлено. Соединение не устанавливается, если время установления $t_{\text{ус}}$ превышает допустимое время $t_{\text{доп}}$ (в статье этот параметр имеет значение 50 мс):

$$\xi(x_c) = \begin{cases} 1, \text{ если } t_{\text{ус}} > t_{\text{доп}}; \\ 0, \text{ если } \le t_{\text{доп}}. \end{cases} \tag{35}$$

В этой работе показано, что при увеличении числа неработоспособных путей вероятность установления соединения снижается. Кроме того, варьируя допустимым временем доставки вызова $t_{\text{доп}}$ и числом альтернативных путей $n_{\text{р}}$,

модель предоставляет возможность находить оптимальные настройки для обеспечения необходимого уровня надежности. Однако эта модель не воспроизводит угрозы вскрытия обмена данными, идентификаторов, дешифровки информации, модификации данных в сети, рассинхронизации сети, завершения аутентификации неправильными данными, переполнения памяти, повторных запросов и анализа активности абонентов.

Модель 1.15. В **2020** году в работе [18] **L. Jiang, X. Chang, J. Bai** и **J. Mišić** предложили модель процедуры аутентификации 5G-AKA. Модель базируется на применении *непрерывных марковких цепей.* Модель воспроизводит переходы состояний системы при отказах и восстановлении. Рассматривается два сценария: основная политика работы системы, когда есть только одна SEAF (The SEcurity Anchor Function), отвечающая за безопасное управление процессами аутентификации и защиты данных, и резервная, когда есть две SEAF, работающие параллельно. Показателями эффективности выступают: дефекты на миллион (Defects Per Million, DPM) и первое время восстановления после сбоя.

На рис. 7 показана модель, построенная с использованием *непрерывных марковких цепей* при основной политике. Состояние 0 соответствует работоспособному SEAF, состояние 1 – отказу SEAF, состояние 2 – началу процесса восстановления. Переходы между состояниями характеризуются показателями: γ (интенсивность отказа), δ (интенсивность обнаружения отказа) и τ (интенсивность восстановления).

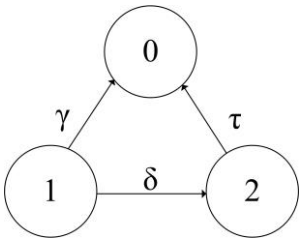

Рис. 7. Цепь Маркова: процесс доступа к SEAF при основной политике

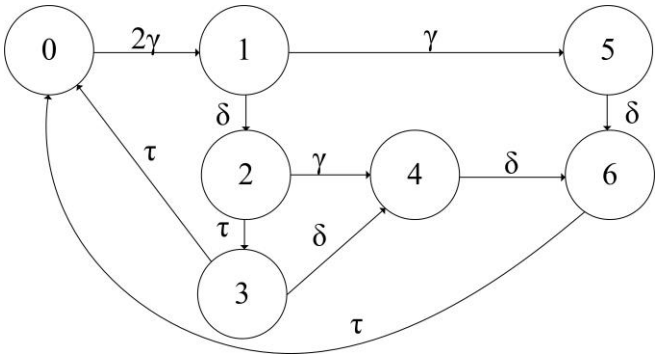

Рис. 8. Цепь Маркова: процесс доступа к SEAF при резервной политике

Показатель DPM для основной политики, показывающий количество неудачных запросов на миллион всех запросов, вычисляется по формуле [18]:

$$DPM = \left(\delta\tau + \tau\gamma + \delta\gamma\right)\gamma^{-2}. \quad (36)$$

На рис. 8 показана модель для резервной политики. Состояние 0 означает, что обе SEAF работают; состояние 1 – отказ одной из SEAF; состояние 2 – обнаружение отказа; состояние 3 – выполнение переключения; состояние 4 – отказ второй SEAF во время переключения; состояние 5 – отказ обеих SEAF; состояние 6 – обнаружение отказов обеих SEAF. Формула для расчета показателя DPM для резервной политики в статье не указана.

Время первого восстановления определяет, как быстро система вернется в рабочее состояние после сбоя, то есть среднее время первого восстановления из состояния 1 в состояние 0 ($t_1 \to 0$) равно [18]:

$$t_1 = 1/\tau. \quad (37)$$

Время первого восстановления для резервной политики равно [18]:

$$t_1 = 1/\tau + 1/\gamma + 1/\delta\ . \quad (38)$$

Также в этой модели используется общая стоимость владения – показатель, суммирующий инфраструктурные затраты, затраты на электроэнергию и охлаждение, эксплуатационные затраты и затраты от простоя.

Модель основана на предположении об экспоненциальном распределении всех временных интервалов, что не в полной мере соответствует реальным условиям работы системы. В ней отсутствует учет восстановления и одновременного отказа нескольких элементов, защиты от вскрытия обмена данными, идентификаторов, дешифровки информации, модификации данных в сети, рассинхронизации сети, завершения аутентификации неправильными данными, переполнения памяти, повторных запросов и анализа активности абонентов.

Модель 1.16. В **2020** году в работе [19] **K. A. Alezabi, F. Hashim** и **S. J. Hashim** предложили модель процесса аутентификации в гетерогенной сети LTE-WiMAX-WLAN, базирующуюся на применении *теории массового обслуживания*. Показателем эффективности в модели является время переключения между сетями, описываемое плотностью распределения задержки переключения $f_{\mathrm{HDA}}(t)$, вычисляемой как [19]:

$$f_{\mathrm{HDA}}(t) = \sum_{m \in MA} P_m \cdot f_{\mathrm{HDA}m}(t), \quad (39)$$

где: MA – множество протоколов в алгоритме; P_m – вероятность использования протокола m; $f_{\mathrm{HDA}m}(t)$ – плотность распределения задержки для протокола m.

Результаты моделирования показали зависимость времени переключения от количества пользователей и количества переходов между базовыми станциями. Также модель объяснила влияние архитектурных решений на производительность системы аутентификации в гетерогенной среде, учитывая стоимость переключения [19]:

$$C_m = C_{m,\mathrm{s}} + C_{m,\mathrm{p}}, \quad (40)$$

где: C_m – общая стоимость метода m; $C_{m,\mathrm{s}}$ – стоимость передачи сигналов; $C_{m,\mathrm{p}}$ – стоимость обработки.

На рис. 9 представлена упрощенная схема гетерогенной сети LTE-WLAN-WiMAX. На ней показана задержка (HD^A) с момента запроса (EAP Request/Identity) до момента подтверждения аутентификации (EAP Success), переменные, используемые для расчета задержки передачи данных (Transmission Delay, TD), и основные компоненты сети:

- пользовательское устройство UE;
- базовая станция BS/eNB (Base Station/eNodeB);
- шлюз ASN-GW/S-GW (Access Service Network Gateway/Serving Gateway);
- сервер PAAAS/WAAAS (Proxy AAA (Authentication, Authorization and Accounting) Server/Wireless AAA Server);
- сервер 3AAAS (3GPP AAA Server).

Однако эта модель не воспроизводит процессы вскрытия обмена данными, идентификаторов, дешифровки информации, модификации данных в сети, рассинхронизации сети, завершения аутентификации неправильными данными, переполнения памяти, повторных запросов и анализа активности абонентов.

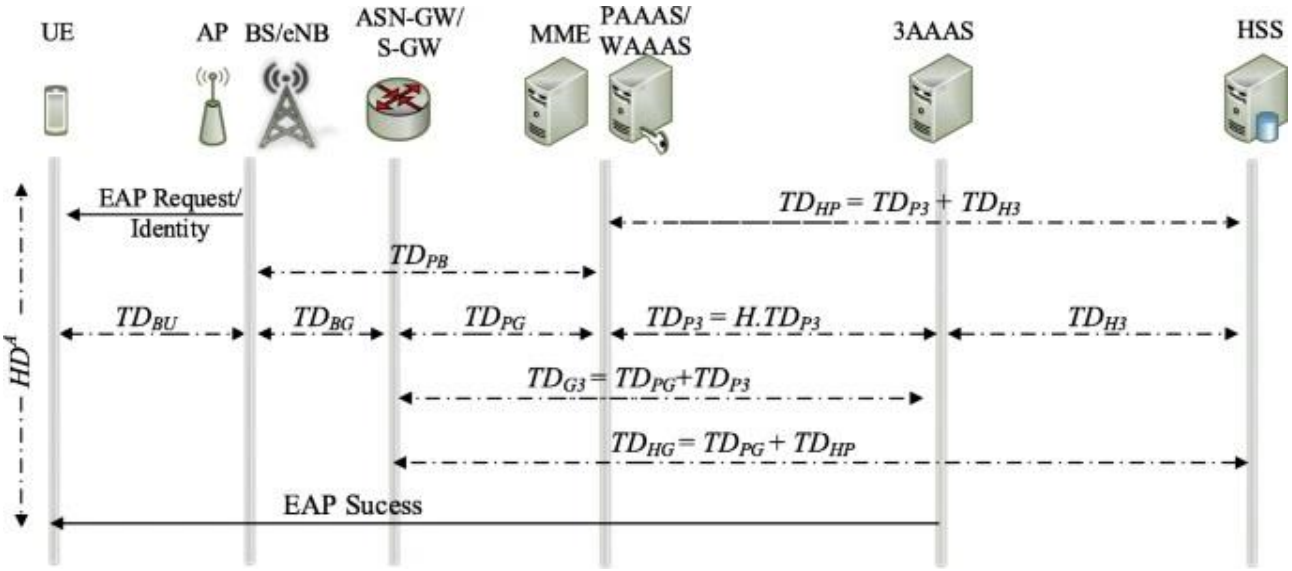

Рис. 9. Упрощенная схема аутентификации в сети LTE-WLAN-WiMAX

Модель 1.17. В **2021** году в работе [20] **S. Nashwan** предложил модель функционирования протокола аутентификации SAK-AKA (Secure Anonymity Key of Authentication and Key Agreement) в сетях 4G/5G. Модель основана на применении *теории массового обслуживания*. Для анализа количества сессий IAPS (Initial Authentication Processes Session) и SAPS (Subsequent Authentication Processes Session) запросы на аутентификацию моделируются пуассоновскими процессами и геометрическим распределением вероятностей. На рис. 10 показан процесс взаимодействия UE, MME и HSS, а также потоки сообщений в сессиях IAPS и SAPS. В IAPS UE отправляет запрос на доступ в MME. MME, в свою очередь, запрашивает аутентификационные векторы у HSS. HSS предоставляет MME набор векторов. MME использует первый из этих векторов (1st-AV) для аутентификации UE. В SAPS UE отправляет запрос на доступ в MME. Однако, MME использует ранее полученные от HSS аутентификационные векторы для аутентификации UE, избегая обращения к HSS. Таким способом SAK-AKA оптимизирует нагрузку на HSS, сокращая количество запросов к HSS при последующих аутентификациях.

Вероятность *n*-го IAPS при условии, что первый SAPS начинается на *m*-ой позиции в ранее полученном пакете AV, вычисляется по формуле [20]:

$$P(n,k,m) = p(1-p)^{n-1} \text{ при } p = 1-\left(\lambda/\left(\lambda+\mu\right)\right)^k, \quad (41)$$

где: p – вероятность успешной сессии; μ – интенсивность ухода AV, то есть частота истечения срока действия AV; m – количество AV, доступных в данный момент для MME; k – количество AV, получаемых MME за раз; λ – интенсивность поступления запросов на аутентификацию.

Ожидаемое количество IAPS сессий вычисляется как [20]:

$$EN = p^{-1} = \left(1-\gamma^{k}\right)^{-1} \text{ при } \gamma = \lambda/\left(\lambda+\mu\right). \quad (42)$$

На рис. 11 показано, как увеличение параметра *k* влияет на *EN*.

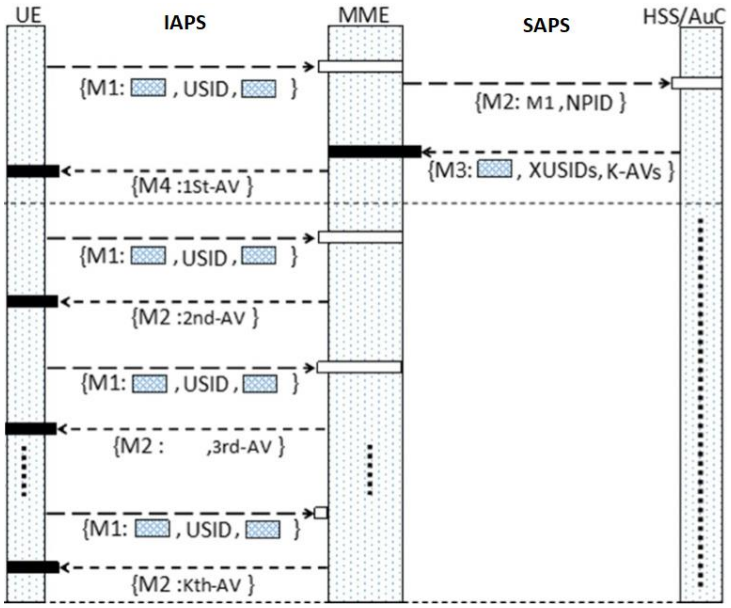

Рис. 10. Потоки трафика при аутентификации

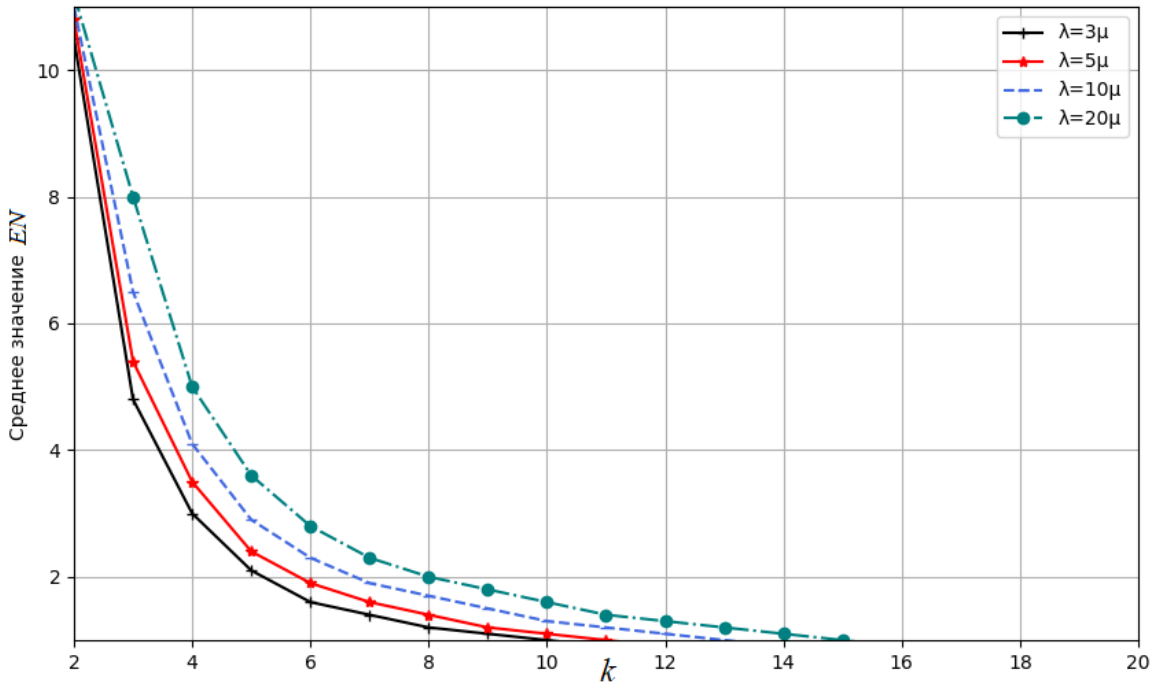

Рис. 11. Зависимость *EN* от параметра *k*

Функция стоимости передачи сообщения $C(k, m)$ для сценария 1, где MME не имеет доступных AV, т.е. m=0, задается формулой [20]:

$$C(k,0) = EN \cdot \left(2\alpha k + 2\beta\right) = \left(1-\gamma^{k}\right)^{-1} \cdot \left(2\alpha k + 2\beta\right), \quad (43)$$

где: α – стоимость обмена сообщениями между UE и MME; β – стоимость обмена сообщениями между MME и HSS.

Функция стоимости в сценарии 2, где у MME m AV и $(1 \le m \le k-1)$ [20]:

$$C(k,m) = \frac{2\alpha k + 2\beta}{1-\gamma^k} - 2(\alpha m + \beta). \quad (44)$$

Результаты моделирования показали, что существует оптимальное значение k, минимизирующее общие затраты.

Также модель объясняет, как динамическое управление параметром k со стороны MME в зависимости от текущей интенсивности запросов аутентификации может снизить накладные расходы и оптимизировать работу протокола SAK-AKA. Для нахождения оптимального k используется метод Ньютона-Рафсона, при котором значение k находится итерационно по формуле [20]:

$$X_{r+1} = X_r - \frac{\alpha + \gamma^{X_r}\left(\ln\gamma\left(\alpha X_r + \beta\right) - \alpha\right)}{\gamma^{X_r}(\ln\gamma)^2\left(\alpha Xr + \beta\right)}, \quad (45)$$

где: X_r – текущее значение k на итерации r; X_{r+1} – следующее значение k на итерации $r+1$.

Однако эта модель не учитывает задержки в передаче сообщений, потери пакетов, существующие угрозы безопасности и возможное изменение стоимости обмена сообщениями в зависимости от нагрузки на сеть. Также использование модели ограничено тем, что все UE одинаковые.

Модель 1.18. В **2023** году в работе [21] **Ю. И. Горбенко** и **И. В. Олешко** предложили модель, позволяющую оценить защищенность механизмов аутентификации. Показателем эффективности является вероятность защиты от несанкционированного доступа. Модель основана на применении *теории вероятностей*. В модели для последовательной, параллельной и комбинированной схемах аутентификации учитываются следующие факторы аутентификации: пароли, биометрические данные и криптографические ключи.

Для комбинированной схемы вероятность успешной аутентификации P_{auth} равна [21]:

$$P_{\text{auth}} = P_1 \cdot P_2 \cdot \ldots \cdot P_n, \quad (46)$$

где $P_1, P_2, \ldots, P_n$ – вероятности успешной аутентификации каждого из n факторов.

Для параллельной схемы P_{auth} используется следующая формула [21]:

$$P_{\text{auth}} = 1 - (1 - P_1) \cdot (1 - P_2) \cdot \ldots \cdot (1 - P_n). \quad (47)$$

Однако эта модель не воспроизводит процессы вскрытия обмена данными, идентификаторов, дешифровки информации, модификации данных в сети, рассинхронизации сети, завершения аутентификации неправильными данными, переполнения памяти, повторных запросов и анализа активности абонентов.

2. Обзор средств имитации процедуры аутентификации

Значительный вклад в исследование аутентификации в сетях сотовой связи внесли программные средства, реализующие имитационные модели соответствующих процессов. Например, ProVerif, CryptoVerif, TAMARIN, Scyther. Они имитируют протоколы аутентификации, показывая их устойчивость к различным атакам, и дают возможность проверять эти протоколы на наличие логических ошибок и корректность обмена сообщениями. Воспроизводимые в этих

средствах модели опираются на логический и символьный анализ. Это позволяет обнаруживать уязвимости, возникающие в процессе программирования.

Модель 2.1. В **2012** году в работе [22] **J. K. Tsay** и **S. Mjølsnes** предложили программное средство для проведения анализа безопасности протоколов аутентификации и соглашения о ключах (AKA) для систем UMTS и LTE. LTE-AKA является усовершенствованной версией протокола UMTS-AKA, который широко используется в 3G-сетях. Авторы провели вычислительный анализ протокола LTE-AKA и формальный анализ протокола UMTS-AKA, который учитывает сообщения, передаваемые в ядре сети, и механизмы защищенного транспорта. В ходе анализа выявлены недостатки в спецификациях протоколов UMTS-AKA и LTE-AKA, а также в спецификациях безопасности ядра сети, которые могут привести к атакам как снаружи, так и внутри сети. В частности, показано, что злоумышленник, находящийся внутри сети, может не только выдать себя за легитимного пользователя, но и пользоваться беспроводными услугами от его имени. Также показано, что в случае использования протоколов Diameter/IPsec или MAP/TCAPsec с длинными идентификаторами сессий протоколы UMTS-AKA и LTE-AKA обеспечивают безопасность аутентификации и секретности ключей при условии, что используемые криптографические примитивы соответствуют стандартным криптографическим требованиям. Однако это средство не воспроизводит защиту от эксплуатации уязвимостей, оставаясь лишь диагностическим инструментом.

Модель 2.2. В **2020** году в работе [23] **E. K. Edris**, **M. Aiash** и **J. K. Loo**, используя инструмент для проверки безопасности протоколов ProVerif, провели систематическую оценку протокола 5G-AKA на основе последних спецификаций 5G. В процессе анализа выявлены недостатки безопасности и предложены рекомендации для их устранения. Эта модель выполняет роль инструмента выявления недостатков безопасности, но не воспроизводит защиту от их эксплуатации, оставаясь диагностическим инструментом.

Модель 2.3. В **2018** году в работе [24] **D. A. Basin**, **J. Dreier** и **L. Hirschi** использовали программное средство TAMARIN для моделирования и анализа 5G-AKA и его варианта EAP-AKA′, который использует схему шифрования на основе эллиптических кривых и скрытность идентификаторов для обеспечения конфиденциальности пользователей. Авторы обнаружили уязвимость в протоколе, связанную с отсутствием защиты целостности идентификаторов сетей, что позволяет злоумышленникам манипулировать этими идентификаторами и выполнять атаки. Предложенный подход увеличивает уровень приватности и защищает от атак, использующих идентификационные данные пользователя. Однако эта модель хотя и учитывает уязвимость, связанную с отсутствием защиты целостности идентификаторов сетей, и воспроизводит подход для повышения приватности и защиты от атак, эксплуатирующих идентификационные данные, не воспроизводит процесс защиты от других типов атак.

Модель 2.4. В **2018** году в работе [25] **P. Panda** и **S. Chattopadhyay** предложили программное средство, имитирующее улучшенную схему аутентификации и согласования ключей (ES-EPS-AKA) для сетей LTE. Эта схема предусматривает применение эллиптической криптографии (Elliptic-Curve

Cryptography, ECC), хеш-функций HMAC (Hash-based Message Authentication Code) и других шифрующих функций для защиты передаваемых сообщений. В частности, модель воспроизводится генерация ключей, используемых для шифрования и аутентификации, и как используется HMAC для проверки подлинности сообщений. Авторы внесли следующие улучшения:

– форвардная секретность – гарантия, что если один ключ будет скомпрометирован, то это не повлияет на безопасность прошлых сеансов;
– защита от атак, позволяющих злоумышленнику манипулировать связью между пользователем и сетью, чтобы выдать себя за другого пользователя и получения доступа к сети.

В таблице 2 показаны результаты сравнения вычислительных затрат протоколов аутентификации EPS-AKA, ES-AKA, EEPS-AKA и ES-EPS-AKA в сетях LTE для пользовательского оборудования (UE), модуля управления мобильностью MME и сервера абонентов HSS, используя обозначения: T_H (хеширование), T_P (умножение точки на эллиптической кривой) и T_M (модульное возведение в степень).

Таблица 2 –Сравнительный анализ вычислительных затрат протоколов

Протокол	UE	MME	HSS	Итого
EPS-AKA	$5T_H$	–	$5T_H$	$10T_H$
ES-AKA	$2T_H+T_P$	$2T_H+T_P$	T_H	$5T_H+T_P$
EEPS-AKA	$2T_M$	$2T_M$	–	$4T_M$
ES-EPS-AKA	$2T_H+3T_P$	T_H+2T_P	T_H	$4T_H+5T_P$

Протокол EPS-AKA использует только T_H, являясь наименее затратным, но и наименее безопасным. ES-AKA и ES-EPS-AKA используют более ресурсоемкие T_P, повышая безопасность. ES-EPS-AKA сочетает T_P и T_H, показывая компромисс между безопасностью и эффективностью. EEPS-AKA использует T_M, не нагружая HSS, но оставаясь со средними показателями. Таблица демонстрирует, что ES-EPS-AKA более ресурсозатратный, чем EPS-AKA, но обеспечивает более высокую безопасность за счет использования ECC. При этом сохраняется более низкая нагрузка на HSS, чем у остальных протоколов.

Эта модель предполагает идеальную синхронизацию между участниками процесса, не рассматривает возможные задержки или сбои в сети и не учитывает уязвимости криптографических протоколов, вопросы ротации и управления долгосрочным ключом.

Модель 2.5. В **2019** году в работе [26] **M. Ouaissa** и **A. Rhattoy** предложили имитационную модель функционирования улучшенного протокола аутентификации и согласования ключей для IoT-систем, использующих мобильные сети LTE и IMS. В модели используется общий идентификатор IMPI (IP Multimedia Private Identity) для аутентификации в сетях LTE и IMS. Это позволяет избежать двойную аутентификацию и повысить безопасность. Показателями эффективности в этой модели являются: энергопотребление при аутентификации и объем памяти, требуемый для хранения ключей и параметров аутентификации. Модель основана на применении эллиптической криптографии и принципах протоколов EPS-AKA и IMS-AKA, определенных 3GPP. Предло-

женный протокол позволяет снизить энергопотребление и объем требуемой памяти в сравнении с протоколами EPS-AKA и IMS-AKA.

Однако результаты моделирования не учитывают влияние пропускной способности сети на энергопотребление и время аутентификации, защиту от вскрытия обмена данными, идентификаторов, дешифровки информации, модификации данных в сети, рассинхронизации сети, завершения аутентификации неправильными данными, переполнения памяти (несмотря на оптимизацию), повторных запросов и анализа активности абонентов.

Модель 2.6. В **2019** году в работе [27] **C. Cremers** и **M. Dehnel-Wild** предложили имитационную модель протокола 5G-AKA, учитывающую «тонкую настройку» пользовательского оборудования, обслуживающей сети и домашней сети. Модель воспроизводит атаку race condition, эксплуатирующую недостатки синхронизации при обработке конкурентных запросов и позволяющую злоумышленнику изменить состояние системы в критический момент. Авторами предложены исправления протокола, которые протестированы и доказаны как эффективные для защиты от такой атаки. Однако эта модель не ориентирована на какие-либо иные атаки.

Модель 2.7. В **2019** году в работе [28] **R. Borgaonkar**, **L. Hirschi**, **S. Park** и **A. Shaik** показали результаты исследования протокола 5G-AKA с точки зрения его конфиденциальности с использованием логики Bana-Comon. Этот метод позволяет формально анализировать безопасность аутентификационных протоколов, выявляя потенциальные утечки данных и уязвимости, связанные с анонимностью пользователей. В ходе исследования выявлена проблема рассинхронизации, несмотря на заявления о безопасности протокола. Рассинхронизация приводит к уязвимостям, которые могут быть использованы злоумышленниками для взлома протокола. Для решения этой проблемы предложено исправление, которое гарантирует сохранение конфиденциальности и предотвращает атаки на протокол. Однако эта модель ограничивается решением конкретной проблемы, не уделяя внимание другим типам уязвимостей.

Модель 2.8. В **2019** году в работе [29] **A. Koutsos** раскрыл логическую уязвимость протокола 5G-AKA в механизме защиты последовательных номеров аутентификации (SQN), который используется для защиты от атак повторного воспроизведения. Проблема состоит в недостаточной случайности и слабой криптографической защите используемого механизма. Другие угрозы эта модель не воспроизводит.

Модель 2.9. В **2019** году в работе [30] **J. Zhang**, **Q. Wang**, **L. Yang** и **T. Fan** показали результаты исследования протокола аутентификации в сетях 5G, который использует взаимные механизмы подтверждения подлинности между клиентом и сервером. Авторы подробно анализируют уязвимости, связанные с механизмами безопасности в протоколах аутентификации, а также с возможностью атак типа «человек посередине» и анализируют, как эти уязвимости могут быть использованы злоумышленниками для доступа к чувствительным данным. В этой работе предложены улучшения, направленные на усиление защиты данных и предотвращение возможных атак. Особое внимание

уделяется новым криптографическим методам, которые могут быть использованы для повышения устойчивости к такому виду угроз.

Модель 2.10. В **2024** году в работе [31] **Y. Ko**, **I. W. A. J. Pawana** и **I. You** предложили усовершенствованную версию протокола 5G-AKA, позволяющую парировать уязвимости, приводящие к нарушению конфиденциальности информации пользователей, за счет использования временных ключей внутри домашней сети. Ее назвали 5G-AKA с прямой секретностью или 5G-AKA-FS. Для воспроизведения использовалась программа ProVerif. Однако несмотря на воспроизведение усиленной защиты конфиденциальности и устойчивости к определенным атакам, модель остается специализированным решением.

В целом следует отметить, что использование специализированных программных средств имитации, таких как ProVerif, CryptoVerif, TAMARIN, Scyther, позволяет весьма качественно осуществить формальный анализ протоколов аутентификации для выявления математических (алгоритмических) причин уязвимостей (подробно об этом см., например, в [2]). Однако с их использованием крайне сложно обнаруживать системные, технологические и эксплуатационные причины уязвимостей.

Выводы

Анализ представленных моделей процедур аутентификации в сетях сотовой связи (см. таблицу 3) показывает, что только 32 % от общего числа моделей воспроизводят от 1 до 3 современных угроз. Эти модели имеют узкий фокус и не отражают динамику взаимодействия различных факторов. Остальные ориентированы на оценку производительности процедур аутентификации.

Также из таблицы 3 следует, что на сегодняшний день отсутствуют модели, воспроизводящие угрозы анализа активности абонентов, принудительного завершения процесса и переполнения памяти элементов сети. Кроме того, существующие модели процедур аутентификации в сетях сотовой связи не способны воспроизвести многоэтапную природу современных кибератак. В частности, многие модели не учитывают взаимодействие между различными протоколами и компонентами сети.

Как следствие, известные математические модели не воспроизводят значительную долю компьютерных атак, эксплуатирующих уязвимости процедур аутентификации сетей сотовой связи стандартов от 2G до 5G. Это подчеркивает необходимость дальнейших исследований по разработке совокупности взаимосвязанных моделей, способных воспроизводить аспекты производительности и современные уязвимости процедур аутентификации сетей сотовой связи.

DOI: 10.24412/2410-9916-2025-1-187-219
URL: https://sccs.intelgr.com/archive/2025-01/08-Boyko.pdf

Таблица 3 – Сравнительный анализ моделей процедур аутентификации

№	Авторы / Основная организация	Годы	Математический аппарат или способ имитации	Источ-ник	Моделируемые угрозы								
					Вскрытие данных	Вскрытие идентификаторов абонентов	Дешифрирование информации	Анализ активности абонентов	Модификация данных в сети	Рассинхронизация сети	Принудительное завершение процесса	Переполнение памяти элементов сети	Многократное повторение запросов
1.1	J. Al-Saraireh, S. Yousef / Princess Sumaya University for Technology (г. Амман, Иордания)	2007	ТВ и комбинаторика	[3]	–	–	–	–	–	–	–	–	–
1.2	W. Liu, L. Yang, Q. L. Li, H. Dai, B. Hou / University of North Carolina (г. Чапел-Хилл, США)	2008	ТМП	[4]	–	–	–	–	–	–	–	–	–
1.3	C. K. Han, H. K. Choi, J. W. Baek, H. Lee / Sungkyunkwan University (г. Сувон, Южная Корея)	2009	ТВ, МС, ТН	[5]	–	–	–	–	–	–	–	–	–
1.4	А. С. Корсунский, О. В. Шейкин / ФНПЦ ОАО «НПО «Марс» (г. Ульяновск, Россия)	2010	ТВ и комбинаторика	[6]	–	–	–	–	–	–	–	–	–
1.5	C. Ntantogian / National and Kapodistrian University of Athens (г. Афины, Греция)	2010	ТМП	[7]	–	–	–	–	–	+	–	–	–
1.6	C. Xenakis, C. Ntantogian, I. Stavrakakis / University of Piraeus (г. Пирей, Греция)	2012		[8]	–	–	–	–	–	+	–	–	–
1.7	А. Г. Сабанов / МГТУ им. Н. Э. Баумана (г. Москва, Россия)	2013	ТМО и ТМП	[9]	–	–	–	–	–	–	–	–	–
1.8	М. С. Аристов, О. И. Шишин, А. М. Рапетов, А. С. Крымов, А. Д. Егоров / НИЯУ МИФИ (г. Москва, Россия)	2014	Исчисление предикатов	[10]	–	–	–	–	–	–	–	–	–
1.9	И. В. Углов / ОАО «Мобильные ТелеСистемы» (г. Москва, Россия)	2015	ТМО и ТВ	[11, 12]	+	–	+	–	–	–	–	–	–
1.10	А. А. Васильченко, А. В. Кочуров / Филиал Военной академии РВСН им. Петра Великого (г. Серпухов, Россия)	2016	ТМП	[13]	–	–	–	–	–	–	–	–	–
1.11	M. Khan, N. Khan / Capital University of Science and Technology (г. Исламабад, Пакистан)	2016	ТВ и комбинаторика	[14]	–	–	–	–	+	–	–	–	–
1.12	Д. М. Актанбаев / Харьковский национальный университет радиоэлектроники (г. Харьков, Украина)	2017	ТМО и ТМП	[15]	–	–	–	–	–	–	–	–	–
1.13	Э. Р. Зарипова, А. Ардила Пинто / Российский университет дружбы народов (г. Москва, Россия)	2017	ТМП	[16]	–	–	–	–	–	–	–	–	–
1.14	Т. М. Татариникова, Н. В. Яготинцева / Санкт-Петербургский государственный экономический университет, (г. Санкт-Петербург, Россия)	2017	ТВ	[17]	–	–	–	–	–	–	–	–	–
1.15	L. Jiang, X. Chang, J. Bai, J. Mišić / Beijing Jiaotong University (г. Пекин, Китай)	2020	ТМП	[18]	–	–	–	–	–	–	–	–	–
1.16	K. A. Alezabi, F. Hashim, S. J. Hashim / Institute of Computer Science and Digital Innovation University (г. Куала-Лумпур, Малайзия)	2020	ТМО	[19]	–	–	–	–	–	–	–	–	–
1.17	S. Nashwan / Al Jouf University (г. Аль-Джауфе, Саудовская Аравия)	2021		[20]	–	–	–	–	–	–	–	–	–
1.18	Ю. И. Горбенко, И. В. Олешко / Харьковский национальный университет радиоэлектроники (г. Харьков, Украина)	2023	ТВ	[21]	–	–	–	–	–	–	–	–	–
2.1	J. K. Tsay, S. Mjolsnes / University of Science and Technology (г. Тронхейм, Норвегия)	2012	Средство CryptoVerif	[22]	–	–	–	–	–	–	–	–	–
2.2	E. K. Edris, M. Aiash, J. K. Loo / Middlesex University (графство Мидлсекс, Великобритания)	2020	Средство ProVerif	[23]	–	–	–	–	–	–	–	–	–
2.3	D. A. Basin, J. Dreier, L. Hirschi / University of Dundee (г. Данди, Шотландия)	2018	Средство TAMARIN	[24]	–	+	–	–	–	–	–	–	–
2.4	P. K. Panda, S. Chattopadhyay / Spark Minda Technical Centre (г. Пуне, Индия)	2018	Имитационная модель	[25]	–	–	–	–	–	–	–	–	–
2.5	M. Ouaissa, A. Rhattoy / Cadi Ayyad University (г. Марракеш, Марокко)	2019		[26]	–	–	–	–	–	–	–	–	–
2.6	C. Cremers, M. Dehnel-Wild / CISPA Helmholtz Center for Information Security (г. Саарбрюккен, Германия)	2019	Средство TAMARIN	[27]	–	–	–	–	–	+	–	–	–
2.7	R. Borgaonkar, L. Hirschi, S. Park, A. Shaik / Высшая техническая школа (г. Берлин, Германия)	2019		[28]	–	–	–	–	–	+	–	–	–
2.8	A. Koutsos / L'université Paris-Saclay (г. Париж, Франция)	2019	Средство Bana-Comon	[29]	–	–	–	–	–	–	–	–	+
2.9	J. Zhang, Q. Wang, L. Yang, T. Fan / Academy of Military Science (г. Пекин, Китай)	2019	Средство Scyther	[30]	+	–	+	–	+	–	–	–	–
2.10	Y. Ko, I. W. A. J. Pawana, I. You / Udayana University (провинция Бали, Индонезия)	2024	Средство ProVerif	[31]	–	–	–	–	–	–	–	–	–

Обозначения: ТВ – теория вероятностей, ТМО – теория массового обслуживания, МП – теория марковских процессов, МС – математическая статистика, ТН – теория надежности.

Заключение

Таким образом, установлено, что существующие математические модели процесса аутентификации в сетях сотовой связи не взаимосвязаны и ориентированы на производительность или защиту от атак, эксплуатирующих уязвимости вскрытия или модификации данных, вскрытия идентификаторов абонентов, дешифрирования информации, рассинхронизации сети или многократного повторения запросов. Выявлена необходимость разработки моделей, воспроизводящих в процессе аутентификации взаимодействие различных подсистем сотовой связи и учитывающих влияние уязвимостей, связанных с анализом активности абонентов сети, принудительным завершением аутентификации, созданием задержки в процессе передаче информации, а также с переполнением памяти элементов сети. Результаты работы могут быть полезны специалистам, отвечающим за защищенность сетей сотовой связи от компьютерных атак.

Литература

1. Бойко А. А., Быков М. Ю., Кущев С. С., Перегудов М. А. Аутентификация в сетях сотовой связи: эволюция, обзор способов защиты и новые уязвимости // Системы управления, связи и безопасности. 2024. № 4. С. 95–144. doi: 10.24412/2410-9916-2024-4-95-144.

2. Бойко А. А. Киберзащита автоматизированных систем воинских формирований. – СПб.: Наукоемкие технологии, 2021. – 300 с.

3. AL-Saraireh J., Sufian Y. Analytical model for authentication transmission overhead between entities in mobile networks // Computer Communications. 2007. № 30. С. 1713–1720. doi: 10.1016/j.comcom.2007.02.001.

4. Liu W., Yang L., Li Q.-L., Dai H., Hou B. Performance Analytic Model for Authentication Mechanism // Proceedings of 2008 IEEE International Conference on Networking, Sensing and Control (ICNSC). 2008. С. 1097–1102. doi: 10.1109/ICNSC.2008.4525380.

5. Han C. K., Choi H. K., Baek J. W., Lee H. W. Evaluation of authentication signaling loads in 3GPP LTE/SAE networks // The 34th Annual IEEE Conference on Local Computer Networks. 2009. С. 20–23. doi: 10.1109/LCN.2009.5355157.

6. Корсунский А. С., Шейкин О. В. Аутентификация корреспондентов в сетях UMTS при использовании псевдослучайных последовательностей Голда и Касами // Автоматизация процессов управления. 2010. № 2. С. 40–47.

7. Ntantogian C. Performance Analysis and Analytical Modeling for the Optimization of the User's Authentication Procedure in 4G Mobile Networks [Электронный ресурс]. – URL: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=eb57efb09fe168318eba7e00c50a881a516705ff (дата обращения: 01.12.2024).

8. Xenakis C. Analysis and Modeling of False Synchronizations in 3G-WLAN Integrated Networks // 27th IFIP International Information Security and Privacy Conference. 2012.

9. Сабанов А. Г. Концепция моделирования процессов аутентификации // Доклады Томского государственного университета систем управления и радиоэлектроники. 2013. № 3 (29). С. 71–75.

10. Аристов М. С., Шишин О. И., Рапетов А. М., Крымов А. С., Егоров А. Д. Обзор и краткий анализ текущего состояния мобильной связи на примере сетей GSM // Спецтехника и связь. 2014. № 1. С. 2–6.

11. Углов И. В. Исследование вероятностно-временных характеристик организации вызовов в конвергентных сетях LTE/GSM с использованием технологии CSFB // T-Comm – Телекоммуникации и Транспорт. 2014. Т. 8. № 5. С. 56–62.

12. Углов И. В. Разработка обобщенных аналитических моделей процессов сигнального обмена в конвергентной сети: дис. ... канд. техн. наук: 05.12.13. – М., 2015. – 155 с.

13. Васильченко А. А., Кочуров А. В. Математическая модель процесса установления соединения в системе сотовой связи типа GSM на "нисходящем" участке // Радиолокация, навигация, связь. XXII международная научно-техническая конференция. 2016. Том 2. С. 643–653.

14. Khan M., Khan N. Low Complexity Signed Response Based Sybil Attack Detection Mechanism in Wireless Sensor Networks // Journal of Sensors. 2016. С. 1–9. doi: 10.1155/2016/9783072.

15. Актанбаев Д. М. ИМС-52 [Электронный ресурс]. – URL: https://studfile.net/hnure/3058/folder:30261/#7403401 (дата обращения: 01.12.2024).

16. Зарипова Э. Р., Ардила Пинто А. Метод оценки времени установления соединения по радиоканалу случайного доступа // Discrete and Continuous Models and Applied Computational Science. 2017. Т. 25. № 1. С. 9–18.

17. Татарникова Т. М., Яготинцева Н. В. Вероятностная модель установления соединения в инфокоммуникационной сети // Известия высших учебных заведений. Приборостроение. 2017. Т. 60. № 2. С. 136–142.

18. Jiang L., Chang X., Bai J., Mišić J., Misic V., Zhi C. Dependability Analysis of 5G-AKA Authentication Service From Server and User Perspectives // IEEE Access. 2020. С. 89562–89574. doi: 10.1109/ACCESS.2020.2993111.

19. Alezabi K. A., Hashim F., Hashim S. J., et al. Efficient authentication and re-authentication protocols for 4G/5G heterogeneous networks // Journal of Wireless Communications and Networking. 2020. № 105. С. 89562–89574. doi: 10.1186/s13638-020-01702-8.

20. Nashwan S., Nashwan I. I. H. Reducing the Overhead Messages Cost of the SAK-AKA Authentication Scheme for 4G/5G Mobile Networks // IEEE Access. 2021. №. 9. С. 97539–97545. doi: 10.1109/ACCESS.2021.3094045.

21. Горбенко Ю. И., Олешко И. В. Модели и методы оценки защищенности механизмов многофакторной аутентификации // Восточно-Европейский журнал передовых технологий. 2023. Т. 6. № 2(66). С. 4–10.

22. Tsay J. K., Mjølsnes S. Computational Security Analysis of the UMTS and LTE Authentication and Key Agreement Protocols // Proceedings of the International Conference on Security and Privacy in Wireless Networks. 2012. С. 123–145.

23. Edris E. K., Aiash M., Loo J. K. Formal Verification and Analysis of Primary Authentication based on 5G-AKA Protocol // Proceedings of the Seventh International Conference on Software Defined Systems (SDS). Paris, France, 2020. С. 256–261. doi: 10.1109/SDS49854.2020.9143899.

24. Basin D. A., Dreier J., Hirschi L., Radomirovic S., Sasse R., Stettler V. A Formal Analysis of 5G Authentication // Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS 2018). 2018. С. 1383–1396.

25. Panda P. K., Chattopadhyay S. An Enhanced Secure Authentication and Key Agreement Scheme for LTE Networks // 2018 3rd International Conference on Contemporary Computing and Informatics (IC3I). 2018. С. 238–243. doi: 10.1109/IC3I44769.2018.9007283.

26. Ouaissa M., Ouaissa M., Rhattoy A. An Efficient and Secure Authentication and Key Agreement Protocol of LTE Mobile Network for an IoT System // International Journal of Intelligent Engineering and Systems. № 4 (12). 2019. С. 212-222. doi: 10.22266/ijies2019.0831.20.

27. Cremers C., Dehnel-Wild M. Component-Based Formal Analysis of 5G-AKA: Channel Assumptions and Session Confusion // Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS 2019). (San-Diego, 24-27 February 2019).

28. Borgaonkar R., Hirschi L., Park S., Shaik A. New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols // Proceedings on Privacy Enhancing Technologies. 2019. С. 108–127.

29. Koutsos A. The 5G-AKA Authentication Protocol Privacy // IEEE European Symposium on Security and Privacy (EuroS&P 2019). Stockholm, Sweden, June 17–19. 2019. С. 464–479.

30. Zhang J., Wang Q., Yang L., Fan T. Formal Verification of 5G-EAP-TLS Authentication Protocol // Proceedings of the Fourth IEEE International Conference on Data Science in Cyberspace (DSC 2019). Hangzhou, China, June 23–25, 2019.

31. Ko Y., Pawana I. W. A. J., You I. Formal Security Reassessment of the 5G-AKA-FS Protocol: Methodological Corrections and Augmented Verification Techniques // Sensors. 2024. № 24. С. 1–26. doi: 10.3390/s24247979.

References

1. Boyko A. A., Bykov M. Yu., Kushev S. S., Peregudov M. A. Authentication in Cellular Networks: Evolution, Review of Security Methods and New Vulnerabilities. *Systems of Control, Communication and Security*, 2024, no. 4, pp. 95–144. doi: 10.24412/2410-9916-2024-4-95-144 (in Russian).

2. Boyko A. A. *Kiberzashchita avtomatizirovannykh sistem voinskikh formirovanii* [Cyberprotection of Automated Systems of Military Formations]. Saint Petersburg, Naukoemkie tekhnologii Publ., 2021. 300 p. (in Russian).

3. AL-Saraireh J., Sufian Y. Analytical model for authentication transmission overhead between entities in mobile networks. *Computer Communications*, 2010, no. 30, pp. 1713–1720. doi:10.1016/j.comcom.2007.02.001.

4. Liu W., Yang L., Li Q. L., Dai H., Hou B. Performance Analytic Model for Authentication Mechanism. *Proceedings of 2008 IEEE International Conference on Networking, Sensing and Control*. 2008. pp. 1097–1102. doi: 10.1109/ICNSC.2008.4525380.

5. Han C. K., Choi H. K., Baek J. W., Lee H. W. Evaluation of authentication signaling loads in 3GPP LTE/SAE networks. *The 34th Annual IEEE Conference on Local Computer Networks*, 2009, pp. 20–23. doi: 10.1109/LCN.2009.5355157.

6. Korunskiy A. S., Sheikin O. V. Autentifikatsiya korrespondentov v setyakh UMTS pri ispol'zovanii psevdosluchaynykh posledovatel'nostey Golda i Kasami [Authentication of Correspondents in UMTS Networks Using Gold and Kasami Pseudorandom Sequences] *Avtomatizatsiya protsessov upravleniya* [Automation of Control Processes], 2010, no. 2, pp. 40–47 (in Russian).

7. Ntantogian C. Performance Analysis and Analytical Modeling for the Optimization of the User's Authentication Procedure in 4G Mobile Networks. Available at: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=eb57efb09fe168318eba7e00c50a881a516705ff (accessed 1 December 2024).

8. Xenakis C. Analysis and Modeling of False Synchronizations in 3G-WLAN Integrated Networks. *27th IFIP International Information Security and Privacy Conference*. 2012.

9. Sabanov A. G. Kontseptsiya modelirovaniya protsessov autentifikatsii [Concept of Modeling Authentication Processes] *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki* [Reports of the Tomsk State University of Control Systems and Radioelectronics], 2013, no. 3 (29), pp. 71–75 (in Russian).

10. Aristov M. S., Shishin O. I., Rapetov A. M., Krymov A. S., Egorov A. D. Obzor i kratkiy analiz tekushchego sostoyaniya mobil'noy svyazi na primere setey GSM [Review and Brief Analysis of the Current State of Mobile Communication Using GSM Networks] *Spetstekhnika i svyaz'* [Specialized Equipment and Communications], 2014, no. 1, pp. 2–6. (in Russian).

11. Uglov I. V. Issledovanie veroyatnostno-vremennykh kharakteristik organizatsii vyzovov v konvergentnykh setyakh LTE/GSM s ispol'zovaniem tekhnologii CSFB [Study of Probabilistic and Temporal Characteristics of Call Setup in LTE/GSM Converged Networks Using CSFB Technology] *T-Comm – Telecommunication and Transport*, 2014, vol. 8, no. 5, pp. 56–62. (in Russian).

12. Uglov I. V. Development of Generalized Analytical Models of Signaling Exchange Processes in Convergent Networks: PhD Thesis in Technical Sciences: 05.12.13. Moscow, 2015. 155 p.

13. Vasil'chenko A. A., Kochurov A. V. Matematicheskaya model' protsessa ustanovleniya soedineniya v sisteme sotovoy svyazi tipa GSM na "niskhodyashchem" uchastke [Mathematical Model of the Call Setup Process in GSM Cellular Networks on the "Downlink" Path] *Radiolokatsiya, navigatsiya, svyaz'* [Radiolocation, Navigation, and Communications]. XXII International Scientific and Technical Conference, 2016, vol. 2, pp. 643–653. (in Russian).

14. Khan M., Khan N. Low Complexity Signed Response Based Sybil Attack Detection Mechanism in Wireless Sensor Networks. *Journal of Sensors*. 2016. pp. 1–9. doi: 10.1155/2016/9783072.

15. Aktanbaev D. M. IMS-52. – Available at: https://studfile.net/hnure/3058/folder:30261/#7403401 (accessed 1 December 2024).

16. Zaripova E. R., Ardila Pinto A. Method for Estimating the Call Setup Time via Random Access Radio Channel [Metod otsenki vremeni ustanovleniya soedineniya po radiokanalu sluchaynogo dostupa] *Discrete and Continuous Models and Applied Computational Science*, 2017, vol. 25, no. 1, pp. 9–18 (in Russian).

17. Tatarnikova T. M., Yagotintseva N. V. Veroyatnostnaya model' ustanovleniya soedineniya v infokommunikatsionnoi seti [Probabilistic Model of Call Setup in an Infocommunication Network] *Izvestiya vysshikh uchebnykh zavedeniy. Priborostroenie* [Proceedings of Higher Educational Institutions. Instrument Engineering], 2017, vol. 60, no. 2, pp. 136–142. (in Russian).

18. Jiang L., Chang X., Bai J., Mišić J., Misic V., Zhi C. Dependability Analysis of 5G-AKA Authentication Service From Server and User Perspectives. *IEEE Access*, 2020, pp. 89562–89574. doi: 10.1109/ACCESS.2020.2993111.

19. Alezabi K. A., Hashim F., Hashim S. J. Efficient authentication and re-authentication protocols for 4G/5G heterogeneous networks // *Journal of Wireless Communications and Networking*, 2020, no. 105, pp. 89562–89574. doi: 10.1186/s13638-020-01702-8.

20. Nashwan S., Nashwan I. I. H. Reducing the Overhead Messages Cost of the SAK-AKA Authentication Scheme for 4G/5G Mobile Networks. *IEEE Access*, no. 9, 2021, pp. 97539–97545. doi: 10.1109/ACCESS.2021.3094045.

21. Gorbenko Yu. I., Oleshko I. V. Modeli i metody otsenki zashchishchennosti mekhanizmov mnogofaktornoy autentifikatsii [Models and Methods for Assessing the Security of Multifactor Authentication Mechanisms] // *Vostochno-Eyropeyskiy zhurnal peredovykh tekhnologiy* [Eastern-European Journal of Advanced Technologies], 2013, vol. 6, no. 2(66). pp. 4–10 (in Russian).

22. Tsay J. K., Mjølsnes S. Computational Security Analysis of the UMTS and LTE Authentication and Key Agreement Protocols. *Proceedings of the International Conference on Security and Privacy in Wireless Networks*, 2012, pp. 123–145.

23. Edris E. K., Aiash M., Loo J. K. Formal Verification and Analysis of Primary Authentication based on 5G-AKA Protocol. *Proceedings of the Seventh International Conference on Software Defined Systems (SDS)*, Paris, France, 2020, pp. 256–261. doi: 10.1109/SDS49854.2020.9143899.

24. Basin D. A., Dreier J., Hirschi L., Radomirovic S., Sasse R., Stettler V. A Formal Analysis of 5G Authentication. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS 2018)*, 2018, pp. 1383–1396.

25. Panda P. K., Chattopadhyay S. An Enhanced Secure Authentication and Key Agreement Scheme for LTE Networks. *3rd International Conference on Contemporary Computing and Informatics*, 2018, pp. 238–243. doi: 10.1109/IC3I44769.2018.9007283.

26. Ouaissa M., Ouaissa M., Rhattoy A. An Efficient and Secure Authentication and Key Agreement Protocol of LTE Mobile Network for an IoT System. *International Journal of Intelligent Engineering and Systems*. vol. 4(12). 2019. p. 212-222. doi: 10.22266/ijies2019.0831.20.

27. Cremers C., Dehnel-Wild M. Component-Based Formal Analysis of 5G-AKA: Channel Assumptions and Session Confusion. *Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS 2019)*, San Diego, California, USA, February 24–27, 2019.

28. Borgaonkar R., Hirschi L., Park S., Shaik A. New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols. *Proceedings on Privacy Enhancing Technologies*, 2019, pp. 108–127.

29. Koutsos A. The 5G-AKA Authentication Protocol Privacy. *IEEE European Symposium on Security and Privacy (EuroS&P 2019)*, Stockholm, Sweden, June 17–19, 2019, pp. 464–479.

30. Zhang J., Wang Q., Yang L., Fan T. Formal Verification of 5G-EAP-TLS Authentication Protocol. *Proceedings of the Fourth IEEE International Conference on Data Science in Cyberspace (DSC 2019)*, Hangzhou, China, June 23–25, 2019.

31. Ko Y., Pawana I. W. A. J., You I. Formal Security Reassessment of the 5G-AKA-FS Protocol: Methodological Corrections and Augmented Verification Techniques. *Sensors*, 2024, vol. 24, pp. 1–26. doi: 10.3390/s24247979.

Статья поступила 14 марта 2025 г.

Информация об авторах

Бойко Алексей Александрович – доктор технических наук, доцент. Преподаватель. Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж). Область научных интересов: методы и системы защиты информации, методы оценки эффективности сложных систем. E–mail: albo@list.ru

Быков Михаил Юрьевич – адъюнкт. Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж). Область научных интересов: информационная безопасность систем сотовой связи. E–mail: bykovmu@ya.ru

Кущев Сергей Сергеевич – кандидат технических наук, начальник кафедры. Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж). Область научных интересов: методы и системы защиты информации. E–mail: serkser@list.ru

Перегудов Максим Анатольевич – кандидат технических наук. Докторант. Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж). Область научных интересов: защита информации, моделирование сетей связи. E–mail: maxaperegudov@mail.ru

Адрес: 394064, Россия, г. Воронеж, ул. Ст. Большевиков, д. 54А.

Authentication in Cellular Networks: Overview of Mathematical Models

A. A. Boyko, M. Yu. Bykov, S. S. Kushev, M. A. Peregudov

Task Statement*: Currently, the urgent task is to protect cellular networks from computer attacks that exploit the vulnerabilities of authentication procedures. Its solution is to improve authentication procedures and create hardware and software tools capable of detecting and neutralizing computer attacks that exploit intractable vulnerabilities. This decision should be based on the modeling results.* ***Objective****: Analysis of existing models of authentication procedures in cellular networks for the possibility of reproducing threats caused by known and previously unexplored potential vulnerabilities.* ***Methods used****: Systems analysis.* ***Novelty****: consideration of the authentication process in cellular networks in the context of the impact of a combination of computer attacks exploiting known and previously unexplored potential vulnerabilities.* ***Result****: It has been established that the existing mathematical models of the authentication process in cellular networks are not interconnected and are focused on performance or protection against attacks exploiting vulnerabilities that lead to the opening or modification of data, the opening of subscriber IDs, decryption of information, network desynchronization or repeated requests. The necessity of developing models reproducing the interaction of various cellular communication subsystems during authentication and taking into account the impact of vulnerabilities leading to the analysis of network subscribers' activity, forced termination of authentication, creating delays in the transmission of information and overflowing the memory of network elements has been identified.* ***Practical significance****: The results of the study may be useful to specialists responsible for protecting cellular networks from computer attacks.*

Key words: *cellular network, authentication, mathematical model, vulnerability, computer attack.*

Information about Authors

Aleksey Aleksandrovich Boyko – Doctor of Engineering Sciences, Associate Professor. Lecturer. Zhukovsky and Gagarin Military Aviation Academy. Field of research: methods and systems of information protection, methods of assessing the effectiveness of complex systems. E–mail: albo@list.ru

Mikhail Yuryevich Bykov – Postgraduate. Zhukovsky and Gagarin Military Aviation Academy. Field of research: information security of cellular communication systems. E-mail: bykovmu@ya.ru

Sergey Sergeyevich Kushev – Ph.D. of Engineering Sciences. Head of the Department. Zhukovsky and Gagarin Military Aviation Academy. Field of research: methods and systems of information protection. E-mail: serkser@list.ru

Maxim Anatol'evich Peregudov – Ph.D. of Engineering Sciences. Doctoral Candidate. Zhukovsky and Gagarin Military Aviation Academy. Field of research: information security, modeling of radio network. E-mail: maxaperegudov@mail.ru

Address: Russia, 394064, Voronezh, Old Bolsheviks Street, 54A.