УНИВЕРСИТЕТ ИТМО
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
январь–февраль 2017 Том 17 № 1 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
January–February 2017 Vol. 17 No 1 ISSN 2226-1494 http://ntv.ifmo.ru/en

УДК 621.391

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЯМЫХ СОЕДИНЕНИЙ 5G ПРИ ИЗМЕНЕНИИ СКОРОСТИ ДВИЖЕНИЯ АБОНЕНТОВ И НАЛИЧИИ СОТОВОГО СОДЕЙСТВИЯ

А.Я. Омётов[a], С.Д. Андреев[b], А.Б. Левина[c], С.В. Беззатеев[d], А. Орсино[e]

[a] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193382, Российская Федерация
[b] Российский университет дружбы народов, Москва, 117198, Российская Федерация
[c] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
[d] Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, 190000, Российская Федерация
[e] Технологический Университет Тампере, Тампере, 33720, Финляндия
Адрес для переписки: alla_levina@mail.ru

Информация о статье
Поступила в редакцию 01.12.16, принята к печати 29.12.16
doi: 10.17586/2226-1494-2017-17-1-100-109
Язык статьи – русский

Ссылка для цитирования: Омётов А.Я., Андреев С.Д., Левина А.Б., Беззатеев С.В., Орсино А. Обеспечение информационной безопасности прямых соединений 5G при изменении скорости движения абонентов и наличии сотового содействия // Научно-технический вестник информационных технологий, механики и оптики. 2017. Т. 17. № 1. С. 100–109. doi: 10.17586/2226-1494-2017-17-1-100-109

Аннотация
Исследованы проблемы пиринговых систем типа «устройство–устройство» (D2D), функционирующих в условиях сотового содействия сетей 5G. Проанализирована задача обеспечения защищенных прямых соединений между мобильными пользователями с помощью разработанного симулятора. Приведены результаты имитационного моделирования динамической кластеризации пользователей, находящихся в географической близости при обмене пакетными данными и использовании модели мобильности Леви. Результаты исследования позволяют определить преимущества интеграции технологии в сеть 3GPP LTE с точки зрения пропускной способности. Показано, что имплементация технологии позволяет получить прирост пропускной способности системы до 30% при незначительном увеличении временных затрат на инициализацию прямых соединений. Полученные результаты могут быть полезны исследователям и сотрудникам организаций, работающих в области телекоммуникационных систем и информационной безопасности.

Ключевые слова
информационная безопасность, 5G, D2D

ON INFORMATION SECURITY SOLUTIONS APPLICABLE TO D2D COMMUNICATIONS WITHIN THE 5G DOMAIN: ANALYZING THE INFLUENCE OF USER MOBILITY

A.Ya. Ometov[a], S.D. Andreev[b], A.B. Levina[c], S.V. Bezzateev[d], A. Orsino[e]

[a] Bonch-Bruevich Saint Petersburg State University of Telecommunications, Saint Petersburg, 193382, Russian Federation
[b] RUDN University, Moscow, 117198, Russian Federation
[c] ITMO University, Saint Petersburg, 197101, Russian Federation
[d] Saint Petersburg State University of Aerospace Instrumentation, Saint Petersburg, 190000, Russian Federation
[e] Tampere University of Technology, Tampere, 33720, Finland
Corresponding author: alla_levina@mail.ru

Article info
Received 01.12.16, accepted 29.12.16
doi: 10.17586/2226-1494-2017-17-1-100-109
Article in Russian

For citation: Ometov A.Ya., Andreev S.D., Levina A.B., Bezzateev S.V., Orsino A. On information security solutions applicable to D2D communications within the 5G domain: analyzing the influence of user mobility. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2017, vol. 17, no. 1, pp. 100–109. doi: 10.17586/2226-1494-2017-17-1-100-109

Abstract
The paper deals with the problems of peer-to-peer systems such as Device-to-Device (D2D) operating in 5G networks. First, we consider the task of ensuring secure, direct connections between mobile users by utilizing the developed simulator. We

present results of the dynamic user clustering in geographical proximity exchanging packet data and Levy flight mobility model. The study results give the possibility to determine benefits of the technology integration in the 3GPP LTE network in terms of throughput. We have shown that technology implementation provides a system capacity increase up to 30% with a slight growth in the time required for the initialization of direct connections. The results may be useful for the academy and industrial experts working in the field of telecommunication systems and information security.

Keywords
information security, 5G, D2D

Введение

В последнее время все более усиливается влияние беспроводных технологий на современное общество, что, в свою очередь, предвещает рост научного интереса к тематике информационной безопасности беспроводных технологий связи. Как результат, это влечет за собой потенциальную возможность установления беспроводного соединения в любом месте и в любое время [1]. Данная возможность является весьма привлекательной для внедрения в ближайшем будущем концепции «Интернета вещей» (Internet of Things, IoT) [2]. При интеграции IoT с сетями будущего поколения 5G [3] многие устройства могут быть оборудованы сенсорами и дополнительными модулями, с помощью которых появляется возможность обрабатывать и передавать полезную информацию без непосредственного вмешательства человека. Особый интерес с недавнего времени представляют сети, построенные по архитектуре Long Term Evolution (LTE). Данные беспроводные технологии открывают возможность для создания широкого спектра сервисов, начиная с удаленного наблюдения и заканчивая здравоохранением. Они также предполагают прямое взаимодействие устройств между собой и, с другой стороны, возможность их непосредственного подключения к сети Интернет.

Сотовые сети, которые известны сегодня, разрабатывались для голосовой связи, т.е. для использования их людьми. Для адаптации таких сетей под большое количество IoT-устройств необходима значительная модификация их работы [4]. Основными требованиями к таким технологиям остаются низкая сложность обработки данных, дешевизна в производстве, приемлемая зона покрытия сети и высокая энергетическая эффективность. Некоторые специфические технологии, такие как ZigBee и радиочастотная идентификация (Radio Frequency IDentification, RFID), изначально разрабатывались с учетом этих требований. С другой стороны, некоторые повсеместно используемые беспроводные технологии также могут быть использованы для таких целей [5].

В частности, беспроводные локальные сети (Wireless Local Area Network, WLAN), построенные на основе стандарта IEEE 802.11 (также широко известные под коммерческим названием Wireless Fidelity (Wi-Fi), являются одним из самых распространенных технических решений для организации беспроводного доступа в домах и на предприятиях. Благодаря их высокой пропускной способности, относительно низкой стоимости и широкой распространенности использование Wi-Fi для сценариев IoT становится все более привлекательным [6]. В настоящей работе производится исследование принципиальной возможности использования современной технологии Wi-Fi, с учетом ее технических характеристик, для типовых сценариев прямых D2D-соединений.

Основной целью настоящего исследования является изучение влияния скорости движения абонентов, использующих прямые соединения в условиях сотового содействия. Рассматривается функционирование системы при применении известных примитивов информационной безопасности, потенциально пригодных к разработке системы связи, использующей подходящие IoT-технологии для реализации защищенного подключения и обслуживания множества разнородных устройств IoT.

Обзор текущих решений

Ключевые требования к системам без постоянного централизованного управления могут быть определены следующим образом [7]: надежный алгоритм контроля связи; адаптивный механизм для быстрого реагирования на изменения топологии и отказы отдельных узлов сети; возможность беспроводной релейной связи; возможность непрерывной защищенной связи даже в случае недоступности инфраструктурной сети.

Особое внимание в настоящей работе сосредоточено на задачах обеспечения информационной безопасности с точки зрения установления защищенной связи между «незнакомыми» или «недоверенными» устройствами. Несмотря на инновационную постановку задачи, обусловленную развивающейся пиринговой технологией связи «устройство–устройство» в условиях сотового содействия, история вопроса достаточно обширна и частично рассмотрена в работах [8–10]. Например, известный алгоритм обмена ключами Диффи–Хеллмана [11] обеспечивает свойство нулевого разглашения для каждой стороны, однако требует надежного канала для его успешного применения. Принимая во внимание более поздние разработки, на сегодняшний день уже традиционно инфраструктура открытых ключей (ИОК) используется в качестве центра доверия (т.е. представителя сертификации) для распределения публичных ключей и обеспечения связи конечных устройств [12]. Упрощенная схема ИОК представлена на рис. 1.

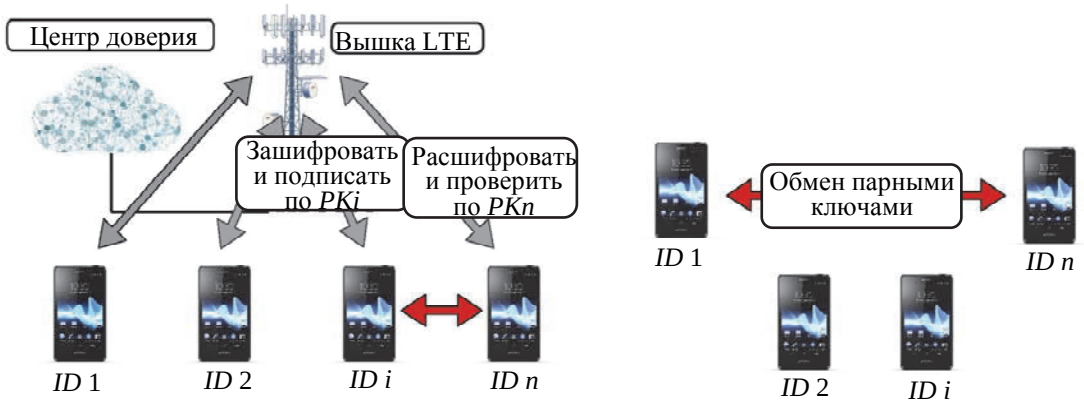

Рис. 1. Защищенная передача данных при наличии/отсутствии инфраструктуры открытых ключей: *PKi*, *PKn* – публичные ключи, *ID* – уникальный идентификатор устройства, *i*, *n* – порядковые номера устройств

Если рассматриваемая сеть не предусматривает централизованного управляющего устройства, для установления прямого соединения может быть использован парный ключ [13]. Важно отметить, что при использовании этого метода устройства не смогут получать информацию о своих парных устройствах помимо их идентификатора. Следовательно, будет необходимо использовать криптографию, основанную лишь на публичных идентификаторах [14, 15], и проверять подпись устройства, основанную на уникальном идентификаторе. Однако в таком случае для дешифрования необходим персональный секретный ключ. Соответствующая служба может быть реализована с помощью использования генератора закрытых ключей (ГЗК), который будет использоваться только в случае его доступности в системе.

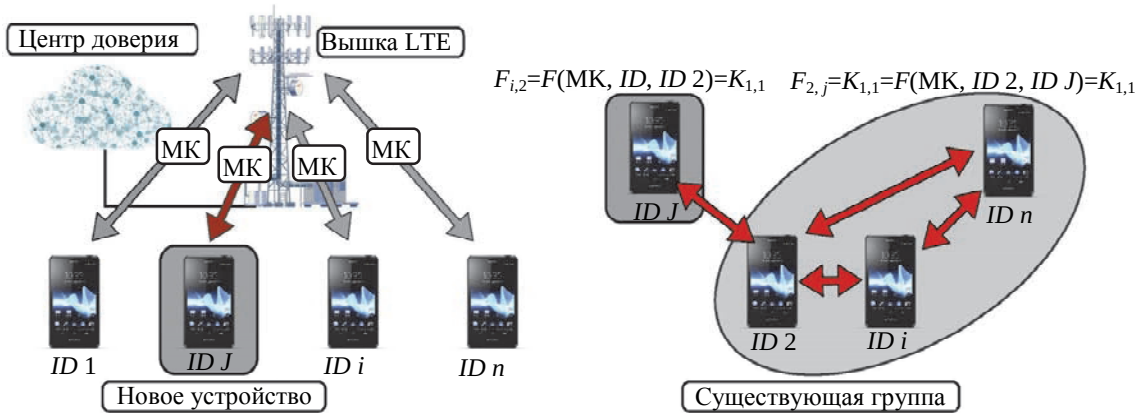

Рис. 2. Распределение ключей, где МК – мастер-ключ, а *J* – порядковый номер нового устройства

Отметим также, что в случае временной недоступности ГЗК группа пользователей, подключенных к ГЗК ранее, может сформировать (или использовать существующий) мастер-ключ (МК) [16, 17]. Соответственно, новое устройство может получить доступ к сети, как показано на рис. 2. Новый парный ключ может быть сгенерирован как функция от МК и множества идентификаторов ($\mathbf{F_{i,j}} = F(MK, ID_i, ID_j)$) и получен следующим образом:

$\mathbf{F_{i,1}} = F(MK, ID_i, ID_1)$

$\mathbf{F_{i,2}} = F(MK, ID_i, ID_2)$

…

$\mathbf{F_{i,i}} = F(MK, ID_i, ID_i)$

$\mathbf{F_{i,n}} = F(MK, ID_i, ID_n)$.

В сенсорных сетях устройства обычно не используют МК после генерации парного ключа [18], т.е. МК является одноразовым. Такой подход используется в основном в силу статической топологии большинства сетей этого типа. В рассмотренной архитектуре «устройство–устройство» МК продолжает использоваться с целью обеспечения непрерывной возможности подключения новых устройств к пиринговой сети даже в случае отсутствия подключения к сотовой сети. Помимо этого, новый МК может быть сгенерирован в случае восстановления связи с базовой станцией.

Примечательно, что устройство может хранить парный ключ $\mathbf{F_{i,i}}$ с самим собой. Это делается в основном для случаев, когда новый пользователь оказывается поблизости, т.е. когда целевое устройство подключено к сотовой сети и запрашивает МК напрямую у координатора сети с целью получения нового ключа и подключения к соседствующему устройству $K_{i,j} = K_{1,1} = F(MK, ID_1, ID_1)$.

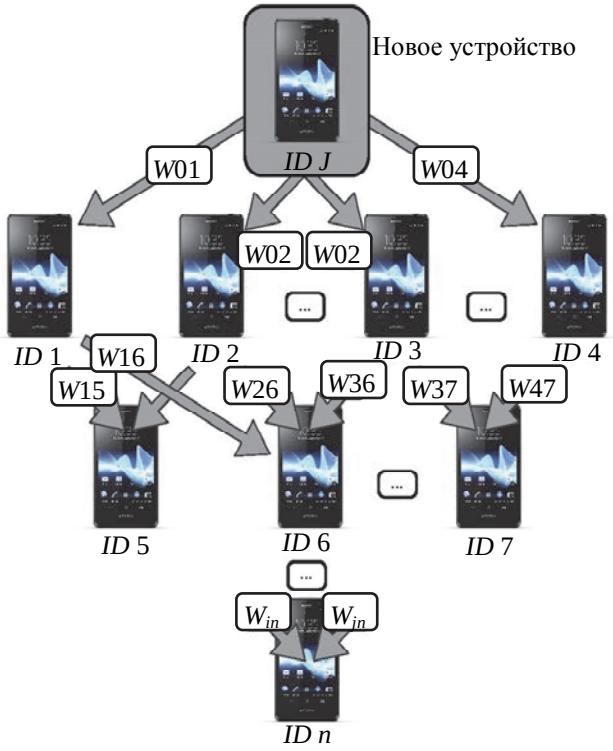

Рис. 3. Политика доверия, основанная на Pretty Good Privacy: *Wij* – уровень доверия между узлами *i* и *j*

Другой важной проблемой в пиринговых сетях с сотовым содействием, основанных на географической близости, является вопрос доверия. Например, рассмотрим популярное решение, основанное на системе доверия Pretty Good Privacy (PGP) [19]. Уровень доверия может принимать значения от нуля до единицы и определяется как сумма произведений уровней доверия уже известных пользователей $t = w_{01}w_{11} + w_{02}w_{12}$, как представлено на рис. 3. Если результат функции доверия близок к или равен 1, то можно принять решение о доверии пользователю. В противном случае пользователю может быть отказано в подключении.

Классические решения в пиринговых сетях

Вторая часть данного исследования рассматривает классические проблемы в самоорганизующихся сетях [20], т.е. основанные на географической близости подключения/отключения устройств в сети при отсутствии подключения к централизованной инфраструктуре. Важно отметить, что такой сценарий связан с дополнительными трудностями, такими как распределение ключей для сопоставления устройств.

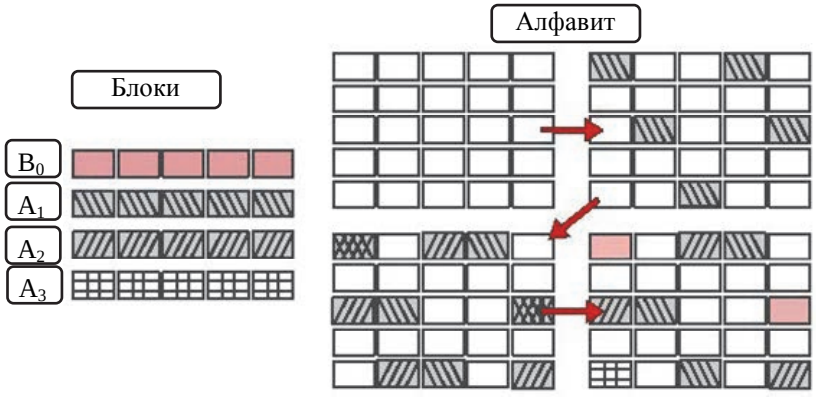

Рис. 4. Cover-Free Family для $r = 2$, $n = 5$

Последнее может быть достигнуто с помощью протокола широковещательного шифрования [21], который предполагает использование определенного числа множеств пользовательских ключей $\mathbf{K} = K_1, K_2, \ldots, K_n$, где $|K_i| \geq 1, \cup K_i = \mathbf{K}, |K_i \cap K_j| \geq 1$. В свою очередь, для создания ключа может быть использована система Cover Free Families (CFF), включающая алфавит из элементов X и множество подмножеств (блоков) $F(X)$. Пример CFF показан на рис. 4. Способ формирования CFF с использованием кодов, исправляющих ошибки, предлагался в работах [22, 23]. Соответственно, система может быть оп-

ределена как CFF, если для любого блока $B_0 \in \mathbf{B}$ и любых других r блоков $A_1; \ldots; A_n \in \mathbf{B}$ может быть рассчитано как

$$B_0 \nsubseteq \bigcup_{j=1}^{r} A_j,$$

где $|X| = T$ – размер алфавита; $|B_0| = N$ – число блоков; r – число блоков, которые не покрывают ни один другой блок; n – длина блока.

Так как все пользователи должны обладать возможностью получения своего ключа, может возникнуть ситуация, когда малая группа пользователей может воспроизвести ключ. Таким образом, атака может быть осуществлена определенной группой устройств. С другой стороны, использование такого подхода гарантирует, что если число устройств меньше или равно минимальному числу, необходимому для восстановления ключа I, то группа не будет покрывать ключ любого другого устройства. Для рассмотренной задачи могут быть использованы системы распределения ключей, основанные на известных решениях, таких как китайская теорема об остатках [24], полином Лагранжа [25] и коды, исправляющие ошибки (Рида–Соломона) [26].

Обеспечение непрерывной защищенной связи с использованием вышеуказанных решений должно стать значительным шагом для систем типа «устройство–устройство» с сотовым содействием. В данной ситуации свойства полинома Лагранжа оказываются предпочтительнее в силу относительной простоты вычисления. Это становится одним из ключевых факторов для современных устройств IoT, являющихся энергозависимыми. Классическая формулировка подразумевает, что каждое устройство связи (представляющее своего пользователя) имеет такой же «вес» при голосовании, как и все остальные в общем дереве доверия. Однако может возникнуть ситуация, когда существует необходимость использования различных «весов» для воздействия на решение при обеспечении доверия в более сложных системах. Следовательно, возникнет необходимость добавления подписи к данным до их передачи, а также встает задача использования моделей управления ключами, которые распределяют части ключа между устройствами. В списке ниже рассмотрены доступные на данный момент «демократические» решения [27].

1. Схема (1, N) – каждое устройство может восстановить секретный ключ (рис. 5, а).
2. Схема (N, N) – секретный ключ может быть восстановлен только с использованием всех N частей (рис. 5, б).
3. Схема (K, N) – секретный ключ может быть восстановлен с использованием K частей, где $K < N$ (рис. 5, в). Эта схема используется в решении, рассмотренном далее.
4. Схема (K, N) с весами – участники с суммой весов, большей или равной K, могут восстановить ключ. Значения весовых коэффициентов могут отличаться в зависимости от уровня доверия (рис. 5, г).

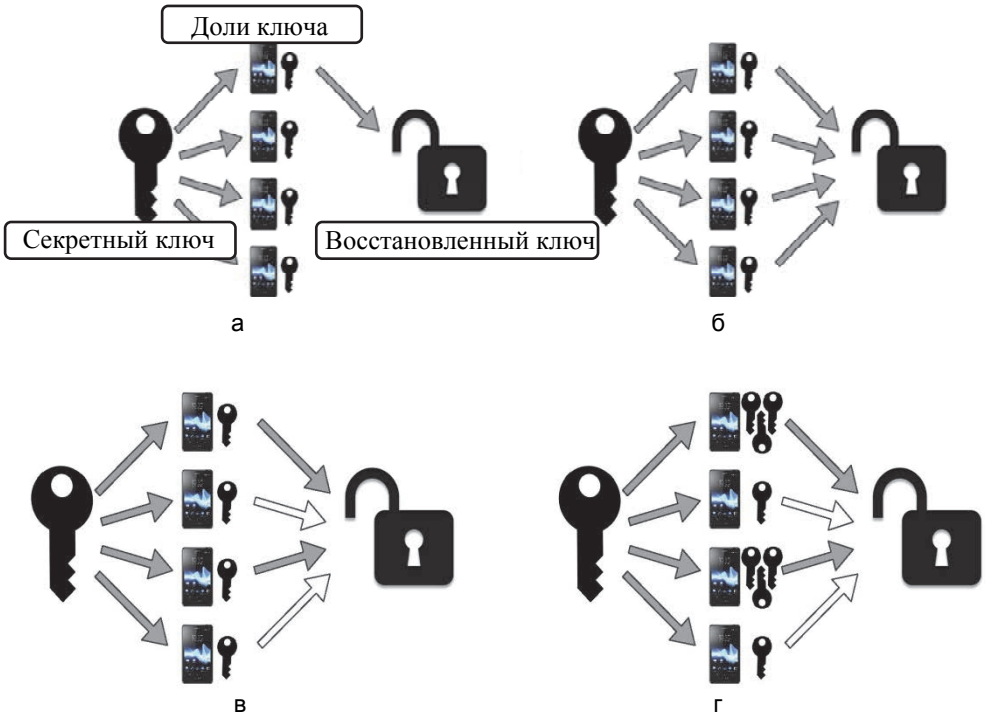

Рис. 5. Примеры схем распределения ключей (а–г)

Помимо вышеуказанных, интересно также рассмотреть известные «диктаторские» решения [28]. Основное отличие заключается в том, что одно или более «важных» устройств должно участвовать в восстановлении ключа, и если ни одно из таких устройств не принимает участия в процессе, ключ не может быть восстановлен. В частности, предполагается, что секретный ключ – это пароль a в, например, Web

Host Manager (WHM) [29, 30], зашифрованный ключ – это $b = a + e$, а части ключа являются значениями и позициями возможных систематических ошибок. Таким образом, процесс восстановления ключа, по сути, представляет собой исправление ошибок в известных битах b. Если взвешенная сумма неисправленных ошибок меньше, чем пороговое значение t, то ключ может быть восстановлен с помощью процедуры декодирования.

При более детальном рассмотрении реализации систем «устройство–устройство» может возникнуть ситуация, при которой пользователи подключены к центру доверия через инфраструктурную сотовую сеть. В таком случае функционал управления многоуровневым доступом и иерархией может быть изменен на основании технологии уровней доступа [31], которые принимают во внимания следующие требования информационной безопасности:

– безопасность – только авторизованные пользователи могут получить доступ к информации;
– анонимность – внутренняя иерархия должна быть скрыта;
– адаптивность – структура сети часто изменяется и должна быть динамической;
– простота – устройства IoT критически ограничены в своих ресурсах.

Более того, основанные на географической близости системы «устройство-устройство» могут быть усовершенствованы за счет использования криптосистемы Мак-Элиса, использующей коды, исправляющие ошибки [32]. Таким образом, каждое устройство имеет свой собственный закрытый ключ и не передает никакой дополнительной информации о себе в зашифрованном сообщении. Важно отметить, что существует возможность обмена сообщениями на всех уровнях иерархии.

Для предотвращения неавторизованного использования данных предлагается использование технологии стеганографии и, в частности, стеганографического метода F5 [33]. По сути, за счет изменения одного бита данных в сообщении можно передать другое сообщение, содержащее новые данные $(0, n-1)$. Таким образом, редактируя менее важные части передаваемой информации, можно получить существенное улучшение уровня информационной безопасности. При этом открытым остается вопрос корректного выбора данных для модификации, а также понимания того, как определенные модификации повлияют на процесс декодирования. Потенциальное решение этого вопроса – модель взвешенного контейнера (например, взвешенная метрика Хэмминга) [34–36]. Здесь для подсчета числа добавленных ошибок и определения веса искажения можно использовать штрафную функцию [34]:

$$F = \sum_{i=1}^{l} \eta_i v_i ,$$

где η_i – среднее число ошибок, а v_i – уровень важности в зоне I_i.

Потенциальные улучшения за счет наличия прямых соединений

В предыдущей работе авторов [37] был представлен алгоритм кластеризации мобильных станций, использующих безопасные соединения в случаях, когда географическая близость позволяет достигать преимуществ по сравнению с использованием инфраструктурных соединений. Были использованы криптопримитивы, рассмотренные в предыдущих разделах данной работы, и показаны реальные затраты времени на создание защищенных групп. Данное исследование проводилось при поддержке Технологического университета города Брно, Чешская Республика.

Поскольку число устройств, задействованных в измерениях, было достаточно малым в силу ограничений в наличии оборудования, было принято решение исследовать влияние мобильности (скорости движения абонентов) и их количества на задержки в беспроводном канале связи и максимально достижимую пропускную способность системы. Для анализа была разработана система имитационного моделирования на языке Python. Результаты измерений времени генерации примитивов отображены в таблице. Для получения данных было произведено взвешенное усреднение по результатам 10000 измерений.

Криптопримитив	Сервер	Устройство
RSA 512 Публичный ключ	7,29	109,33
RSA 512 Секретный ключ	99,96	1157,81
RSA 1024 Публичный ключ	19,43	304,12
RSA 1024 Секретный ключ	352,12	5887,1
RSA 2048 Публичный ключ	66,21	951,54
RSA 2048 Секретный ключ	2132,9	35981,32
Время генерации случайной величины	7,24	25,12

Таблица. Время генерации на серверной/клиентской сторонах, мкс

Для моделирования одной соты 3GPP LTE были использованы следующие параметры системы. Радиус покрытия eNodeB был выбран равным 100 м^2. Максимальная дальность (радиус) соединения по

технологии ближнего действия (D2D) составила 30 м. Максимальное количество пользователей – 20; максимальные скорости передачи в системах дальнего и ближнего радиусов действия – 10 и 40 Мбит/с соответственно. Время на установление соединения по технологии Wi-Fi Direct принято равным 1 с. Для моделирования движения абонентов использована «модель полета Леви» (с параметром 1,5), соответствующая случайному блужданию пользователей. Выбор данной модели обусловлен недавними исследованиями, подтверждающими, что перемещение людей может быть адекватно описано процессом, где многочисленные короткие изменения дальности и направления движения чередуются с более длительными переходами [38, 39].

При инициализации разработанной имитационной программы 20 пользователей равномерно размещены в зоне покрытия базовой станции. Скорость каждого из них распределена в пределах [0,2; 2] м/с. Пример траектории движения дан на рис. 6. Таким образом, моделирование позволяет имитировать передвижение абонента согласно спецификации 3GPP TS 36.304. Для учета трафика был использован тип мультимедийного контента с интервалом генерации 100 мс и размером пакета 100 кБ. Количество проведенных экспериментов задано равным 1000, длительность эксперимента – 15 минут реального времени функционирования системы, а представленный доверительный уровень равен 90%.

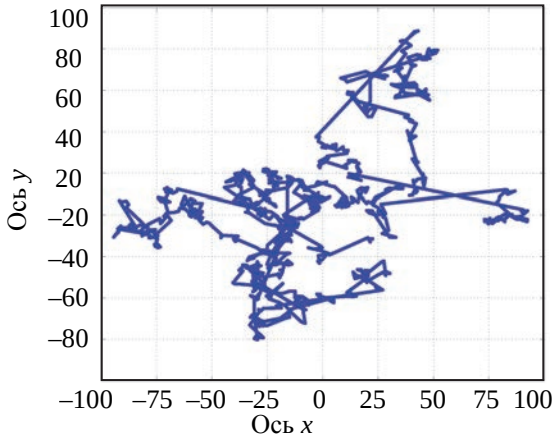

Рис. 6. Пример движения отдельного пользователя в системе

Для анализа системы были выбраны известные метрики – задержка на стороне пользовательской станции (время запроса на загрузку мультимедийного контента с учетом подтверждения) и средняя пропускная способность на пользователя (усредненная по обоим каналам распространения).

Рассмотрим вначале влияние мобильности абонентских станций на задержку. Результаты представлены на рис. 7. Как видно из результатов моделирования, график задержки линейно убывает с ростом скорости движения пользователей. Это обусловлено возрастанием числа потенциальных взаимодействующих пар с увеличением скорости. Таким образом, пользователи получают возможность использовать прямое соединение значительно более существенную часть времени, нежели инфраструктурное соединение. Однако результаты для задержек при использовании сотового содействия на более чем 30% выше. Это обусловлено дополнительными временными затратами на инициализацию прямых соединений.

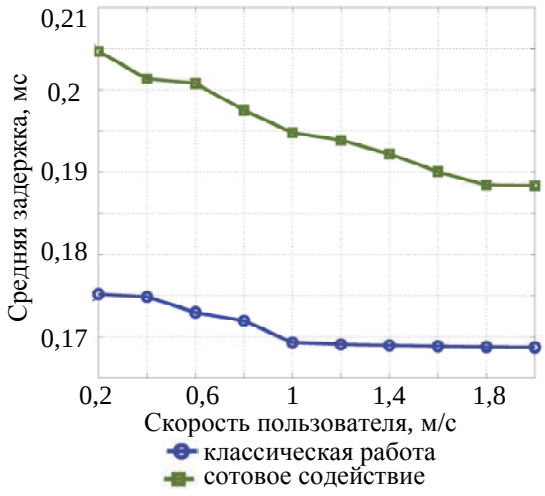

Рис. 7. Зависимость задержки от скорости пользователя

С другой стороны и согласно данным на рис. 8, средняя пропускная способность возрастает с повышением скорости движения пользователей, а анализируемая система показывает предпочтительные результаты в сравнении с классической. Это связано с потенциальной возможностью установления соединений даже за пределами сотового покрытия. В этом случае прирост пропускной способности достигается за счет дополнительных соединений, зависящих, в том числе, от используемых примитивов информационной безопасности.

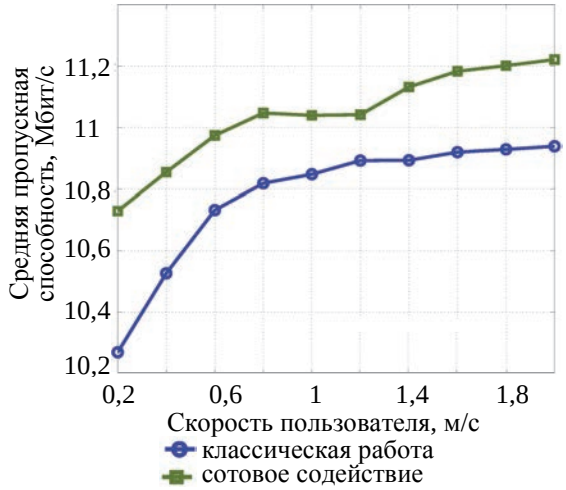

Рис. 8. Зависимость пропускной способности от скорости пользователя

Подводя итог, важно отметить, что даже в современных сотовых сетях могут возникать ситуации, когда соединение с централизованным узлом управления оказывается недоступным. Применение решений типа «устройство–устройство», основанных на принципах сотового содействия, может обеспечить пользователей приемлемым уровнем связи даже вне сотового покрытия, но ценой дополнительных задержек.

Заключение

Функционирование рассмотренных систем «устройство-устройство» сходно с работой самоорганизующихся сетей, но обладает ключевым отличием – в случае систем «устройство-устройство» все устройства связи (были) ассоциированы с сотовой базовой станцией, по крайней мере, на какое-то время, чего достаточно для распределения исходной информации, относящейся к безопасности (мастер-ключи, сертификаты и т.д.). Следовательно, классические распределенные решения безопасности (для, например, сенсорных сетей) могут быть значительно усовершенствованы в случае связи «устройство-устройство» за счет использования возможности (периодического) доступа к доверенной сотовой инфраструктуре. В работе был проведен обзор существующих решений, рекомендуемых к использованию в системах прямых соединений в условиях сотового содействия сетей следующего поколения. Показано, что существующие протоколы информационной безопасности могут быть применены в сетях рассматриваемого типа при специфической группировке. Также рассмотрены потенциальные преимущества и недостатки при интеграции подобных решений в современные сотовые системы.

Литература

1. Adams C., Lloyd S. Understanding PKI: Concepts, Standards, and Deployment Considerations. 2nd ed. Addison-Wesley Professional, 2003. 322 p.
2. Боронин П.Н., Кучерявый А.Е. Интернет вещей как новая концепция развития сетей связи // Информационные технологии и телекоммуникации. 2014. №3(7). С. 7–30.
3. Haas Z.J., Deng J., Liang B., Papadimitratos P., Sajama S. Wireless Ad Hoc Networks. Encyclopedia of Telecommunications. John Wiley and Sons, 2002.
4. Мутханна А.С., Кучерявый А.Е. D2D-коммуникации в сетях мобильной связи пятого поколения 5G // Информационные технологии и телекоммуникации. 2014. №4 (8). С. 51–63.
5. Khalili A., Katz J., Arbaugh W.A. Toward secure key distribution in truly ad-hoc networks // Proc. Symposium on Applications and the Internet Workshops. 2003. P. 342–346. doi: 10.1109/saintw.2003.1210183
6. Yi X., Willemson J., Nait-Abdesselam F. Privacy-preserving

References

1. Adams C., Lloyd S. *Understanding PKI: Concepts, Standards, and Deployment Considerations*. 2nd ed. Addison-Wesley Professional, 2003, 322 p.
2. Boronin P.N., Kucheryavy A.E. Internet of Things as a new concept of the telecommunication networks development. *Informatsionnye Tekhnologii i Telekommunikatsii*, 2014, no. 3, pp. 7–30. (In Russian)
3. Haas Z.J., Deng J., Liang B., Papadimitratos P., Sajama S. *Wireless Ad Hoc Networks. Encyclopedia of Telecommunications*. John Wiley and Sons, 2002.
4. Muthanna S., Kucheryavy A.E. D2D-communication in the 5G mobile networks. *Informatsionnye Tekhnologii i Telekommunikatsii*, 2014, no. 4, pp. 51–63. (In Russian)
5. Khalili A., Katz J., Arbaugh W.A. Toward secure key distribution in truly ad-hoc networks. *Proc. Symposium on Applications and the Internet Workshops*, 2003, pp. 342–346. doi: 10.1109/saintw.2003.1210183
6. Yi X., Willemson J., Nait-Abdesselam F. Privacy-preserving

wireless medical sensor network // Proc. 12th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications (TrustCom). 2013. P. 118–125. doi: 10.1109/trustcom.2013.19
7. Омётов А.Я., Кучерявый Е.А., Андреев С.Д. О роли беспроводных технологий связи в развитии "Интернета Вещей" // Информационные технологии и телекоммуникации. 2014. № 3(7). С. 31–40.
8. Lu Q., Miao Q., Fodor G., Brahmi N. Clustering schemes for D2D communications under partial/no network coverage // IEEE 79th Vehicular Technology Conference (VTC Spring). 2014. P. 1–5. doi: 10.1109/vtcspring.2014.7022860
9. Perrig A., Stankovic J., Wagner D. Security in wireless sensor networks // Communications of the ACM. 2004. V. 47. N 6. P. 53–57. doi: 10.1145/990680.990707
10. McDaniel P., McLaughin S. Security and privacy challenges in the smart grid // IEEE Security & Privacy Magazine. 2009. V. 7. N 3. P. 75–77. doi: 10.1109/msp.2009.76
11. Hubaux J.-P., Capkun S., Luo J. The security and privacy of smart vehicles // IEEE Security & Privacy Magazine, 2004. V. 2. N 3. P. 49–55. doi: 10.1109/msp.2004.26
12. Diffie W., Hellman M.E. New directions in cryptography // IEEE Transactions on Information Theory. 1976. V. 22. N 6. P. 644–654. doi: 10.1109/tit.1976.1055638
13. Liu D., Ning P., Li R., Establishing pairwise keys in distributed sensor networks // ACM Transactions on Information and System Security (TISSEC). 2005. V. 8. N 1. P. 41–77. doi: 10.1145/1053283.1053287
14. Shamir A. How to share a secret // Communications of the ACM. 1979. V. 22. N 11. P. 612–613. doi: 10.1145/359168.359176
15. Shamir A. Identity-based cryptosystems and signature schemes // Lecture Notes in Computer Science. 1985. V. 196. P. 47–53. doi: 10.1007/3-540-39568-7_5
16. Perrig A., Szewczyk R., Tygar J., Wen V., Culler D.E. SPINS: security protocols for sensor networks // Wireless Networks. 2002. V. 8. N 5. P. 521–534. doi: 10.1023/a:1016598314198
17. Du W., Deng J., Han Y.S., Varshney P.K., Katz J., Khalili A. A pairwise key predistribution scheme for wireless sensor networks // ACM Transactions on Information and System Security (TISSEC). 2005. V. 8. N 2. P. 228–258. doi: 10.1145/1065545.1065548
18. Zhu S., Setia S., Jajodia S. LEAP+: efficient security mechanisms for large-scale distributed sensor networks // ACM Transactions on Sensor Networks. 2006. V. 2. N 4. P. 500–528. doi: 10.1145/1218556.1218559
19. Zimmermann P. Why I wrote PGP // Part of the Original PGP User's Guide. 1991.
20. Zhou L., Haas Z.J. Securing ad hoc networks // IEEE Network. 1999. V. 13. N 6. P. 24–30. doi: 10.1109/65.806983
21. Беззатеев С.В., Степанов М.В. Множества, свободные от покрытий, построенные с помощью эллиптических кодов // Научный вестник норильского индустриального института. 2007. №1. С. 74–75.
22. Bezzateev S., Stepanov M. Algebraic-geometry codes on Griesmer bound // Proc. Algebraic and Combinatorial Coding Theory, ACCT-10. Zvenigorod, Russia, 2006. P. 256–258.
23. Du X., Wang Y., Ge J., Wang Y. An ID-based broadcast encryption scheme for key distribution // IEEE Transactions on Broadcasting. 2005. V. 51. N 2. P. 264–266. doi: 10.1109/tbc.2005.847600
24. Chiou G.-H., Chen W.-T. Secure broadcasting using the secure lock // IEEE Transactions on Software Engineering. 1989. V. 15. N 8. P. 929–934. doi: 10.1109/32.31350
25. Jakobsen T., Knudsen L.R. The interpolation attack on block ciphers // Lecture Notes in Computer Science. 1997. P. 28–40. doi: 10.1007/bfb0052332
26. McEliece R.J., Sarwate D.V. On sharing secrets and reed-solomon codes // Communications of the ACM. 1981. V. 24. N 9. P. 583– 584. doi: 10.1145/358746.358762
27. Man C.W., Safavi-Naini R. Democratic key escrow scheme // Lecture Notes in Computer Science. 1997. V. 1270. P. 249–260. doi: 10.1007/bfb0027932
28. Yuan J., Ding C. Secret sharing schemes from three classes of linear codes // IEEE Transactions on Information Theory. 2006. V. 52. N 1. P. 206–212. doi: 10.1109/tit.2005.860412
29. Massey J.L. Minimal codewords and secret sharing // Proc. 6th wireless medical sensor network. *Proc. 12th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2013, pp. 118–125. doi: 10.1109/trustcom.2013.19
7. Omjotov A.Ya., Kucheryavy A.E., Andreev S.D. About the wireless technology role for the development of ”Internet of Things”. *Informatsionnye Tekhnologii i Telekommunikatsii*, 2014, no. 3, pp. 31–40. (In Russian)
8. Lu Q., Miao Q., Fodor G., Brahmi N. Clustering schemes for D2D communications under partial/no network coverage. *IEEE 79th Vehicular Technology Conference (VTC Spring)*, 2014, pp. 1–5.
9. Perrig A., Stankovic J., Wagner D. Security in wireless sensor networks. *Communications of the ACM*, 2004, vol. 47, no. 6, pp. 53–57. doi: 10.1145/990680.990707
10. McDaniel P., McLaughin S. Security and privacy challenges in the smart grid. *IEEE Security &Privacy Magazine*, 2009. vol. 7, no. 3, pp. 75–77. doi: 10.1109/msp.2009.76
11. Hubaux J.-P., Capkun S., Luo J. The security and privacy of smart vehicles. *IEEE Security & Privacy Magazine*, 2004, vol. 2, no. 3, pp. 49–55. doi: 10.1109/msp.2004.26
12. Diffie W., Hellman M.E. New directions in cryptography. *IEEE Transactions on Information Theory*, 1976, vol. 22, no. 6, pp. 644–654. doi: 10.1109/tit.1976.1055638
13. Liu D., Ning P., Li R., Establishing pairwise keys in distributed sensor networks. *ACM Transactions on Information and System Security*, 2005, vol. 8, no. 1, pp. 41–77. doi: 10.1145/1053283.1053287
14. Shamir A. How to share a secret. *Communications of the ACM*, 1979, vol. 22, no. 11, pp. 612–613. doi: 10.1145/359168.359176
15. Shamir A. Identity-based cryptosystems and signature schemes. *Lecture Notes in Computer Science*, 1985, vol. 196, pp. 47–53. doi: 10.1007/3-540-39568-7_5
16. Perrig A., Szewczyk R., Tygar J., Wen V., Culler D.E. SPINS: Security protocols for sensor networks. *Wireless Networks*, 2002, vol. 8, no. 5, pp. 521–534. doi: 10.1023/a:1016598314198
17. Du W., Deng J., Han Y.S., Varshney P.K., Katz J., Khalili A. A pairwise key predistribution scheme for wireless sensor networks. *ACM Transactions on Information and System Security*, 2005, vol. 8, no. 2, pp. 228–258. doi: 10.1145/1065545.1065548
18. Zhu S., Setia S., Jajodia S. LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. *ACM Transactions on Sensor Networks*, 2006. vol. 2, no. 4, pp. 500–528. doi: 10.1145/1218556.1218559
19. Zimmermann P. Why I wrote PGP. *Part of the Original PGP User's Guide*, 1991.
20. Zhou L., Haas Z.J. Securing ad hoc networks. *IEEE Network*, 1999, vol. 13, no. 6, pp. 24–30. doi: 10.1109/65.806983
21. Bezzateev S.V., Stepanov M.V. Sets, free of coatings, constructed using elliptic codes. *Nauchnyi Vestnik Noril'skogo Industrial'nogo Instituta*, 2007, no. 1, pp. 74–75. (In Russian).
22. Bezzateev S., Stepanov M. Algebraic-geometry codes on Griesmer bound. *Proc. of Algebraic and Combinatorial Coding Theory, ACCT-10*. Zvenigorod, Russia, 2006, pp. 256–258.
23. Du X., Wang Y., Ge J., Wang Y. An ID-based broadcast encryption scheme for key distribution. *IEEE Transactions on Broadcasting*, 2005, vol. 51, no. 2, pp. 264–266. doi: 10.1109/tbc.2005.847600
24. Chiou G.-H., Chen W.-T. Secure broadcasting using the secure lock. *IEEE Transactions on Software Engineering*, 1989, vol. 15, no. 8, pp. 929–934. doi: 10.1109/32.31350
25. Jakobsen T., Knudsen L.R. The interpolation attack on block ciphers. *Lecture Notes in Computer Science*, 1997, pp. 28–40. doi: 10.1007/bfb0052332
26. McEliece R.J., Sarwate D.V. On sharing secrets and reed-solomon codes. *Communications of the ACM*, 1981, vol. 24, no. 9, pp. 583–584. doi: 10.1145/358746.358762
27. Man C.W., Safavi-Naini R. Democratic key escrow scheme. *Lecture Notes in Computer Science*, 1997, vol. 1270, pp. 249–260. doi: 10.1007/bfb0027932
28. Yuan J., Ding C. Secret sharing schemes from three classes of linear codes. *IEEE Transactions on Information Theory*, 2006, vol. 52, no. 1, pp. 206–212. doi: 10.1109/tit.2005.860412
29. Massey J.L. Minimal codewords and secret sharing. *Proc. 6th Joint Swedish-Russian International Workshop on Information Theory*. Citeseer, 1993, pp. 276–279.

Joint Swedish-Russian International Workshop on Information Theory. Citeseer, 1993. P. 276–279,
30. Lee K.H., Jung T., Krouk E., Bezzateev S., Linsky E. Weighted Secret Sharing and Reconstructing Method. Patent US 7551740. 2009.
31. Denning D.E. A lattice model of secure information flow // Communications of the ACM. 1976. V. 19. N5. P. 236–243. doi: 10.1145/360051.360056
32. McEliece R. A public-key cryptosystem based on algebraic coding theory // DSN Progress Report. 1978. P. 42–44.
33. Westfeld A. F5—A steganographic algorithm // Lecture Notes in Computer Science. 2001. P. 289–302. doi: 10.1007/3-540-45496-9_21
34. Bezzateev S., Voloshina N., Zhidanov K. Multi-level significant bit (MLSB) embedding based on weighted container model and weighted F5 concept // Proc. 2nd Int. Afro-European Conference for Industrial Advancement AECIA. 2015. P. 293–303. doi: 10.1007/978-3-319-29504-6_29
35. Bezzateev S., Voloshina N. The digital fingerprinting method for state images based on weighted Hamming metric and on weighted container model // Journal of Computer and Communications. 2014. V. 2. N 9. P. 121–126. doi: 10.4236/jcc.2014.29016
36. Voloshina N., Zhidanov K., Bezzateev S. Optimal weighted watermarking for still images // Proc. XIV Int. Symposium on Problems of Redundancy in Information and Control Systems. St. Petersburg, 2014. P. 98–102.
37. Ometov A., Olshannikova E., Masek P., Olsson T., Hosek J., Andreev S., Koucheryavy Y. Dynamic trust associations over socially-aware D2D technology: a practical implementation perspective // IEEE Access. 2016. V. 4. P. 7692–7702. doi: 10.1109/access.2016.2617207
38. Brockmann D., Hufnagel L., Geisel T. The scaling laws of human travel // Nature. 2006. V. 439. N 7075. P. 462–467. doi: 10.1038/nature04292
39. Rhee I., Shin M., Hong S., Lee K., Kim S.J., Chong S. On the Levy-walk nature of human mobility // Proc. IEEE INFOCOM 2008 - The 27th Conference on Computer Communications. 2011. V. 19. N3. P. 30–43. doi: 10.1109/infocom.2008.145

30. Lee K.H., Jung T., Krouk E., Bezzateev S., Linsky E. *Weighted Secret Sharing and Reconstructing Method*. Patent US 7551740, 2009.
31. Denning D.E. A lattice model of secure information flow. *Communications of the ACM*, 1976, vol. 19, no. 5, pp. 236–243. doi: 10.1145/360051.360056
32. McEliece R. A public-key cryptosystem based on algebraic coding theory. *DSN Progress Report*, 1978, pp. 42–44.
33. Westfeld A. F5—A steganographic algorithm. *Lecture Notes in Computer Science*, 2001, pp. 289–302. doi: 10.1007/3-540-45496-9_21
34. Bezzateev S., Voloshina N., Zhidanov K. Multi-level significant bit (MLSB) embedding based on weighted container model and weighted F5 concept. *Proc. 2nd Int. Afro-European Conference for Industrial Advancement AECIA*, 2015, pp. 293–303. doi: 10.1007/978-3-319-29504-6_29
35. Bezzateev S., Voloshina N. The digital fingerprinting method for state images based on weighted Hamming metric and on weighted container model. *Journal of Computer and Communications*, 2014, vol. 2, no. 9, pp. 121–126. doi: 10.4236/jcc.2014.29016
36. Voloshina N., Zhidanov K., Bezzateev S. Optimal weighted watermarking for still images. *Proc. XIV Int. Symposium on Problems of Redundancy in Information and Control Systems*. St. Petersburg, 2014, pp. 98–102.
37. Ometov A., Olshannikova E., Masek P., Olsson T., Hosek J., Andreev S., Koucheryavy Y. Dynamic trust associations over socially-aware D2D technology: a practical implementation perspective. *IEEE Access*, 2016, vol. 4, pp. 7692–7702. doi: 10.1109/access.2016.2617207
38. Brockmann D., Hufnagel L., Geisel T. The scaling laws of human travel. *Nature*, 2006, vol. 439, no. 7075, pp. 462–467. doi: 10.1038/nature04292
39. Rhee I., Shin M., Hong S., Lee K., Kim S.J., Chong S. On the Levy-walk nature of human mobility. *Proc. IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, 2011, vol. 19, no. 3, pp. 30–43. doi: 10.1109/infocom.2008.145

Авторы

Омётов Александр Ярославич – аспирант, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193382, Российская Федерация, Alexander.ometov@gmail.com

Андреев Сергей Дмитриевич – кандидат технических наук, доцент, Российский университет дружбы народов, Москва, 117198, Российская Федерация, Serge.andreev@gmail.com

Левина Алла Борисовна – кандидат физико-математических наук, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, alla_levina@mail.ru

Беззатеев Сергей Валентинович – доктор технических наук, заведующий кафедрой, профессор, Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, 190000, Российская Федерация, bsv@aanet.ru

Орсино Антонино – аспирант, Технологический Университет Тампере, Тампере, 33720, Финляндия, antonino.orsino@tut.fi

Authors

Alexander Ya. Ometov – postgraduate, Bonch-Bruevich Saint Petersburg State University of Telecommunications, Saint Petersburg, 193382, Russian Federation, Alexander.ometov@gmail.com

Sergey D. Andreev – PhD, Associate professor, RUDN University, Moscow, 117198, Russian Federation, Serge.andreev@gmail.com

Alla B. Levina – PhD, Associate professor, ITMO University, Saint Petersburg, 197101, Russian Federation, alla_levina@mail.ru

Sergey V. Bezzateev – D.Sc., Head of Chair, Professor, Saint Petersburg State University of Aerospace Instrumentation, Saint Petersburg, 190000, Russian Federation, bsv@aanet.ru

Antonino Orsino – postgraduate, Tampere University of Technology, Tampere, 33720, Finland, antonino.orsino@tut.fi