

УДК 504.054

Безопасный алгоритм интеллектуальной транспортной системы для полнодуплексного и неортогонального множественного доступа

Хан Р.

Национальный исследовательский Томский политехнический университет,
Томск, 634050, Российская Федерация

В работе предлагается новый алгоритм для полнодуплексного неортогонального множественного доступа на основе модуляции (FD-MNOMA). Предлагаемый алгоритм предотвращает угрозу безопасности в полнодуплексном режиме в кооперативной системе связи. В целях повышения безопасности в сигнал добавляется искусственный шум и реализуется соответствующий алгоритм неортогонального множественного доступа FA-MNOMA. Для предлагаемого алгоритма представлено уравнение пропускной способности секретности. Оценка эффективности показывает, что FA-MNOMA и FD-MNOMA превосходят традиционный неортогональный множественный доступ. Мощность секретности FA-MNOMA дополнительно оптимизируется с помощью генетического алгоритма машинного обучения. В работе также показана реализация FA-MNOMA в интеллектуальной транспортной системе в качестве одного из ее приложений.

Ключевые слова: неортогональный множественный доступ (NOMA), искусственный шум (AN), алгоритм Component-Forward (CF), генетический алгоритм, 5G

Введение

Электромагнитный спектр – это природный ресурс, его бережное использование поможет повысить спектральную эффективность. Полнодуплексный режим связи (FD) и неортогональный множественный доступ (NOMA) направлены на эффективное использование спектра [1, 2]. При полнодуплексной передаче ближайший пользователь с двумя антеннами помогает удаленному пользователю получить сигнал более высокого качества. Когда ближайший пользователь передает и принимает сигналы в одно и то же время и на одной и той же частоте, он сталкивается с большим количеством помех, что вызывает проблемы с безопасностью [3].

Используя NOMA, передатчик пользователя *Alice* распределяет различную мощность для каждого пользователя в зависимости от его расстояния или канала. *Alice* передает сигналы сообщений после объединения всех сигналов с помощью суперпозиционного кодирования. Каждый пользователь получает свой сигнал с высокими помехами от других пользователей, поскольку не было разделения

Библиографическая ссылка на статью:

Хан Р. Безопасный алгоритм интеллектуальной транспортной системы для полнодуплексного и неортогонального множественного доступа // Информационные технологии и телекоммуникации. 2023. Т. 11. № 2. С. 25–34. DOI: 10.31854/2307-1303-2023-11-2-25-34

Reference for citation:

Khan R. An Algorithm Design for a Secure Full Duplex Non-Orthogonal Multiple Access in Wireless Communication System // Telecom IT. 2023. Vol. 11. Iss. 2. PP. 25–34. DOI: 10.31854/2307-1303-2023-11-2-25-34

между сигналами разных пользователей с точки зрения времени и частоты. Следовательно, каждый пользователь должен выполнить последовательное подавление помех (SIC) перед декодированием своего сигнала. Чтобы снизить уровень помех, авторы в [4] предложили новый алгоритм неортогонального множественного доступа на основе модуляции сигнала M-NOMA для полудуплексного режима связи (HD), которая отделяет половину пользователей друг от друга. В M-NOMA Alice модулирует половину сигналов сообщений на синфазной составляющей, а оставшуюся половину – на квадратурной составляющей 4-х квадратурной амплитудной модуляции (4-QAM), чтобы отделить половину пользователей с точки зрения модуляции и уменьшить помехи. Анализ источников показывает, что полнодуплексный режим NOMA (FD-NOMA) сталкивается в основном с помехами в совместном канале [5–7]. В интересах повышения безопасности при передаче сигнала был разработан алгоритм Component-Forward (CF) для FD-NOMA (далее – FD-MNOMA). В сигнал был добавлен искусственный шум (AN) для повышения секретности [8] (далее – FA-MNOMA), а в целях ее оптимизации был использован генетического алгоритма машинного обучения (MLGA).

Модель системы

Алгоритм Component-Forward (CF) обеспечивает пользователю полнодуплексный режим для пересылки сообщения. Он отличается от существующего типа связи с декодированием и пересылкой (DF), где во время FD-режима возникают помехи. На рисунке 1 показана модель FD-системы FA-MNOMA с CF для связи между устройствами по нисходящей линии (DL) [9]. Интеллектуальная транспортная система (ИТС) на рисунке 1 рассматривается как одно из приложений для FA-MNOMA и представляет собой передатчик (Alice), четыре транспортных средства ($Bob_1, Bob_2, Bob_3, Bob_4$) и подслушиватель (Eve).

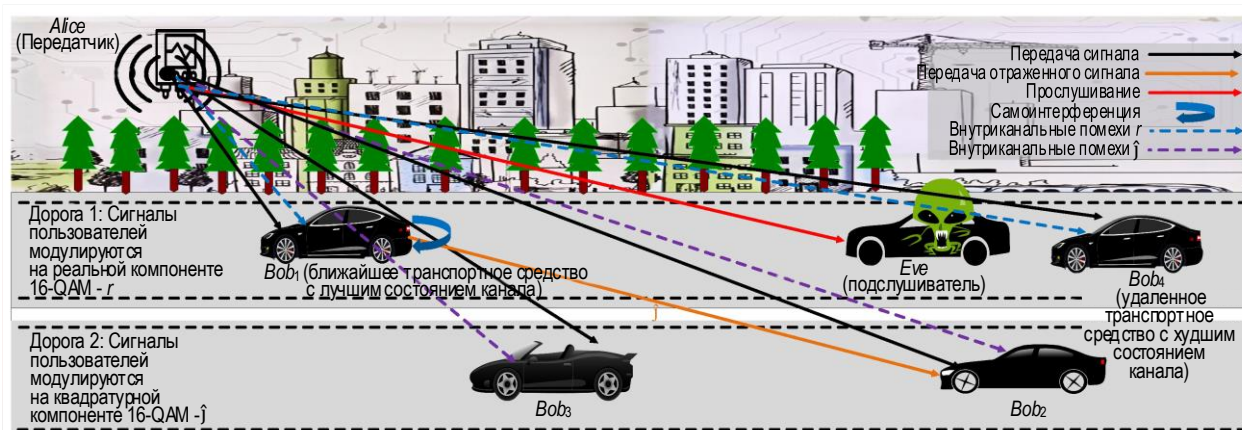


Рис. 1. Модель интеллектуальной транспортной системы

Сигнал каждого транспортного средства модулируется с помощью M-NOMA, чтобы уменьшить помехи NOMA. Bob_1 «помогает» с помощью FD-режима Bob_3 , используя алгоритм CF. Эта система включает в себя собственные и совместные помехи. Считается, что два ближайших транспортных средства

(Vob_1 и Vob_3) и два удаленных (Vob_2 и Vob_4) имеют аналогичное состояние канала. Передатчик и приемники содержат одну антенну, кроме Vob_1 .

Пусть P_T – это общая мощность передачи сигнала. Для каждой передачи мощность будет разделена между пользователями с использованием коэффициентов распределения мощности NOMA α_1 , α_2 , α_3 и α_4 , где $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 1$.

Коэффициенты мощности распределяются относительно расстояний $d_1 < d_2 < d_3 < d_4$ и условий канала $g_4 \approx g_3 < g_2 \approx g_1$ каждого транспортного средства от $Alice$, статистически и с помощью многоуровневого генетического алгоритма (MLGA). Каждое транспортное средство сталкивается с каналом с рэлеевским замиранием, и считается, что информации о состоянии канала (CSI) известна $Alice$ и транспортному средству Vob_1 , а Eve не имеет такой информации. Канал Eve хуже, чем каналы двух соседних пользователей, поэтому Eve не может обнаружить их сигналы. Следовательно, Eve способна обнаружить только сигнал транспортных средств Vob_2 и Vob_4 . В передачу включены и другие каналы: g_{13} и g_{11} для совместной передачи CF в FD-режиме от Vob_1 к Vob_2 , канал самоинтерференции от Vob_1 к самому себе.

$Alice$ использует M-NOMA [3] для наложения сигналов транспортных средств, так как этот алгоритм более эффективно предотвращает помехи сигнала по сравнению с NOMA из-за его ортогональной природы модулированных сигналов:

$$x[t] = (\sqrt{\alpha_1}x_1[t] + \sqrt{\alpha_4}x_4[t])\sqrt{P_T} + j(\sqrt{\alpha_2}x_2[t] + \sqrt{\alpha_3}x_3[t])\sqrt{P_T}.$$

Для четырех транспортных средств помехи в M-NOMA вдвое меньше, чем в NOMA, потому что транспортные средства на дороге 1 (Vob_1 и Vob_4) модулируются на синфазной составляющей, а на дороге 2 (Vob_2 и Vob_3) модулируются на квадратурных составляющих модуляции. Таким образом, оба пользователя дороги 1 сталкиваются только с помехами в совместном канале друг с другом. В лучшем случае нет никаких помех между пользователями разных дорог. Один ближайший и один удаленный пользователь модулируются на одном и том же компоненте созвездия 4-QAM. Это делается для того, чтобы избежать помех между двумя мощными сигналами (удаленные узлы Vob_2 и Vob_4). Таким образом, удаленные пользователи в идеальных условиях не мешают друг другу, а сталкиваются только с незначительными помехами из-за сигнала очень низкой мощности, которые можно рассматривать как шум. В соответствии с системной моделью, транспортное средство Vob_1 , функционирующее в FD-режиме, получает сигнал высокой мощности Vob_2 от $Alice$, поэтому он может помочь удаленному пользователю Vob_2 , используя CF. Чтобы декодировать собственный сигнал, Vob_1 выполняет SIC, декодируя сигнал Vob_4 и удаляя объединенный искусственный шум A_1 из Vob_2 и Vob_4 , а затем вычитая его из общего принятого сигнала. Vob_1 декодирует свой собственный сигнал из общего принятого сигнала и добавляет искусственный шум A_2 , нулевое пространство g_{12} , а затем передает сигнал транспортным

средствам Vob_2 и Vob_3 без его декодирования, используя CF-алгоритм как отражатель для помощи Vob_2 . Vob_3 не может декодировать сигнал, полученный от транспортного средства Vob_1 из-за добавления A_2 . Для пересылки сигнала Vob_1 использует мощность P_c – модулирует синфазной составляющей и передает сигнал мнимой составляющей без его декодирования. В FD-режиме существует самоинтерференция между комплексным сигналом принятого и переданного транспортным средством Vob_1 .

Искусственный шум (AN) является достаточным способом для защиты сигналов передачи от Eve и других пользователей. Конструкция системы AN зависит от канала приемника, но не зависит от канала Eve . AN генерируется перед передачей сигнала $Alice$ и транспортным средством Vob_1 для деградации канала Eve . Оба сигнала x и A_n имеют комплексную гауссову природу. В случае фиксированного AN значение $\|g_e A_n\|$ может быть меньше. Чтобы избежать этой ситуации, значение AN рассматривается как гауссовская случайная величина в нулевом пространстве (g_n) каналов Vob , соответственно, так что $g_n A_n = 0$ [10]. Наложённый $Alice$ сигнал для широкополосной передачи может быть задан как:

$$s[t] = s_1[t] + s_2[t],$$

где

$$s_1[t] = \sqrt{P_T}(\sqrt{\alpha_1}x_1[t] + \hat{j}\sqrt{\alpha_2}x_2[t]) + A_1,$$

$$s_2[t] = \sqrt{P_T}(\sqrt{\alpha_3}x_3[t] + \hat{j}\sqrt{\alpha_4}x_4[t]) + A_2.$$

Согласно M-NOMA сигнал каждого пользователя в отдельности не является комплексным. Однако он комбинируется с сигналом другого пользователя или AN для создания общего комплексного сигнала. Кроме того, в рамках данного исследования предполагается, что два пользователя имеют одинаковые условия канала, поэтому один и тот же AN может быть добавлен к комбинированному сигналу двух разных пользователей. Это экономит полосу пропускания, а скорость передачи данных останется выше, поскольку можно ограничить выделение AN каждому пользователю отдельно.

Транспортные средства Vob_2 и Vob_4 обычно декодируют сигнал, как пользователи M-NOMA. Vob_2 не может декодировать сигнал, полученный от Vob_1 , так как последний добавил A_2 , то есть нулевое пространство канала g_{13} только для Vob_3 . Сигнал M-NOMA, принимаемый Vob_1 , также включает в себя помехи для его передачи по совместному каналу, и он задается как [8]:

$$y_1[t] = K_1 d_0^\gamma d_1^{-\gamma} [\sqrt{g_1 P_T}(\sqrt{\alpha_1}x_1[t] + \hat{j}\sqrt{\alpha_2}x_2[t]) + \sqrt{g_1 P_T}(\sqrt{\alpha_4}x_4[t] + \hat{j}\sqrt{\alpha_3}x_3[t])] + \sqrt{g_{11}[t]P_1}s[t] + w_1[t], \quad (1)$$

где $w_n \sim CN(0, \sigma^2)$ – это аддитивный белый гауссовский шум; $s[t]$ – сигнал, переданный Vob_1 (принятый вместе с предыдущей передачей) на Vob_2 .

Скорость передачи данных для Vob_2 , полученных от Vob_1 , задается как:

$$R_{12} = \log_2 \left(1 + \frac{G_1 P_T \alpha_3}{G_1 \alpha_2 P_T + 1} \right),$$

где $G_n = K_n d_0^\gamma d_n^{-\gamma} g_n / \sigma^2$ и второй член скорости передачи данных является SINR.

Скорость передачи данных Vob_1 для обнаружения собственного сигнала задается как:

$$R_1 = \log_2 \left(1 + \frac{G_1 P_T \alpha_1}{G_1 \alpha_4 P_T + 1} \right).$$

Аналогично может быть получена скорость передачи данных для Vob_4 , принимаемых Vob_2 , и скорость передачи данных в Vob_2 его собственного сигнала. Совместная FD-связь используется только для приоритетного пользователя Vob_3 , поэтому без потери общности была введена задержка τ .

Общий сигнал DL, полученный транспортным средством Vob_3 от *Alice* и Vob_1 , задается как [4]:

$$y_3[t] = \sqrt{g_3 P_T} (\sqrt{\alpha_1} x_1[t] + j \sqrt{\alpha_2} x_2[t]) + \sqrt{g_3 P_T} (\sqrt{\alpha_3} x_3[t] + j \sqrt{\alpha_4} x_4[t]) + \sqrt{g_{13} P_c} j (x_2 + x_3)[t - \tau] + w_3[t]. \quad (2)$$

В (2) сигнал, полученный от Vob_1 , содержит только мнимую часть, как $g_{13} A_2 = 0$.

Принятый сигнал *Eve* может быть определен путем добавления [10] A_1 во втором и A_2 в третьем члене (2). *Eve* принимает сигнал с высокими помехами из-за отсутствия информации об AN и M-NOMA, несущих символы в действительной и мнимой компонентах для декодирования. Таким образом, используя (2), сравним FA-MNOMA; M-NOMA с AN (AN-MNOMA) и FD-NOMA по выражению:

$$y_e[t] = K_e d_0^\gamma d_e^{-\gamma} [g_e (\sqrt{P_T} (\sqrt{\alpha_1} x_1[t] + j \sqrt{\alpha_2} x_2[t])) + g_e (\sqrt{P_T} (\sqrt{\alpha_4} x_4[t] + j \sqrt{\alpha_3} x_3[t]) + A_1)] + K_{1e} d_0^\gamma d_{1e}^{-\gamma} g_{1e}[t] (\sqrt{P_c} (x_2 + x_3)[t - \tau] j + A_2) + w_e[t]. \quad (3)$$

Задачи оптимизации суммарной секретности

Для оптимизации суммарной секретности с использованием MLGA выбранные случайно сгенерированные параметры используются в интересах получения функции пригодности. «Способность к секретности» используется в этой статье в качестве функции приспособленности. Если она не достигает требуемого максимально возможного значения, то алгоритм выбирает случайно сгенерированные параметры, отвечающие за текущую функцию

приспособленности. Выбранные параметры смешиваются вместе и используются для получения лучших параметров с помощью кроссовера. Новые параметры мутируют с некоторыми из старых, чтобы получить наилучшую возможную функцию пригодности. Процесс продолжается до тех пор, пока эта задача не будет выполнена.

MLGA – это подходящий метод машинного обучения для задач оптимизации. Он использует естественный принцип выживания наиболее приспособленных, чтобы максимизировать функцию пригодности [5]. В данном исследовании способность к секретности используется в качестве функции пригодности. Чтобы повысить секретность, оптимизируем скорость передачи данных и коэффициенты мощности системы с помощью MLGA. Формулировка задачи для максимизации секретности приведена в виде:

$$P1: \max: S_T = (R_{Bob_3} - R_{Eve}) + (R_{Bob_4} - R_{Eve}), \quad (4)$$

где ограничения на коэффициент мощности следующие:

$$C1: A(\alpha_1, \dots, \alpha_4) = \sum_{n=1}^4 \alpha_n = 1,$$

$$C2: \alpha_n > 0, n = \{1, \dots, 4\},$$

и SINR:

$$C3: \zeta_n > \zeta_T, n = \{1, \dots, 4\},$$

где ζ_T – пороговое значение для принятого SINR.

В левой части приведенного выше уравнения есть две скобки – первая содержит емкость секретности Bob_3 с разницей между емкостью Bob_3 и Eve , а вторая содержит емкость секретности для Bob_4 .

$$G_n = \frac{K_n d_0^\gamma d_n^{-\gamma} g_n}{\sigma_n^2},$$

где K_n – константа потерь на пути; d_0 – опорное расстояние; d_n – соответствующее расстояние между узлом Bob и передатчиком; σ_n^2 – дисперсия шума; g_n – коэффициент усиления канала между узлами.

Оценка эффективности

В интересах оценки производительности предлагаемой системы проведем моделирование: используется 16-QAM модуляция и канал рэлеевского замирания. Общая мощность составляет $P_T = 1$ Вт. Базовыми сравнительными схемами являются AN-MOMA, которая является дополнением AN к существующим M-NOMA, FD-MNOMA. Предлагаемая система была смоделирована с учетом связи DL с 16-QAM. Система включает в себя четыре транспортных средства с известными условиями канала на узле $Alice$ и узле приемника Bob .

На рисунке 2 показан результат моделирования для секретности с системой из четырех пользователей и пассивным сигналом *Eve*. Сравнение между FA-MNOMA, AN-MNOMA, M-NOMA, FD-NOMA и NOMA показывает, что предлагаемая FA-MNOMA превосходит все другие варианты реализации. Это связано с тем (3), что *Eve* сталкивается с большим количеством помех из-за добавления AN, отсутствия информации CSI о *Bob* и желаемого компонента M-NOMA конкретного *Bob*. Следовательно, это приводит к значительному увеличению FA-MNOMA.

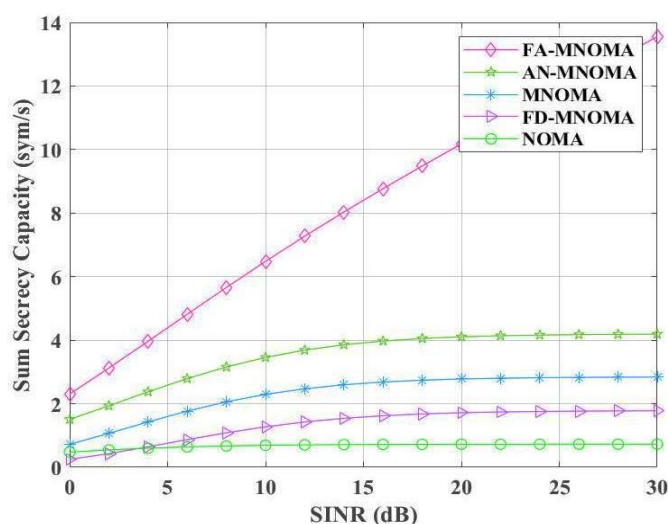


Рис.2. Сравнение суммарной секретности для предлагаемого FD с AN и M-NOMA, AN с M-NOMA, FD с M-NOMA, M-NOMA и NOMA

На рисунке 3 показан результат моделирования FA-MNOMA с MLGA и без него. Для MLGA коэффициенты мощности генерируются случайным образом. Для каждого Bob_i были сгенерированы четыре случайных числа в качестве инициализированной совокупности по отношению к расстоянию и с суммой коэффициентов распределения мощности, равных 1.

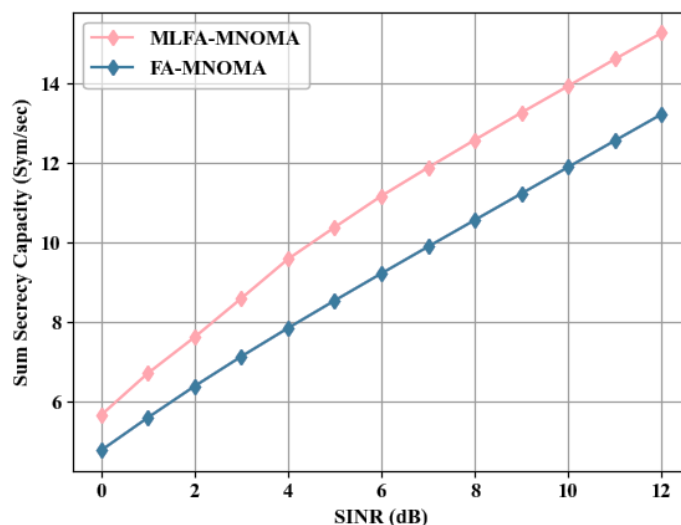


Рис. 3. Сумма сравнения емкости секретности для предлагаемого FD AN M-NOMA с MLGA и без него

Способность к секретности используется в качестве функции пригодности MLGA. Оптимизированная секретность была представлена с использованием метода MLGA. Результат показывает, что MLGA дополнительно повышает производительность FA-MNOMA благодаря параметрам, соответствующим оптимизированному уровню секретности FA-MNOMA. Таким образом, использование MLGA делает систему эффективной с точки зрения секретности. Для ограниченного числа транспортных средств, выбранных в данной работе, легко измерить параметры системы статистически. Однако в системе с большим количеством транспортных средств в ИТС необходим ML [5].

Заключение

В исследовании предложен новый метод (FA-MNOMA), предназначенный для предотвращения угрозы безопасности в системе беспроводной связи. Разработанный алгоритм отделяет один сигнал сообщения от другого, модулируя их на разных компонентах созвездия 4-QAM. Это предотвращает помехи в режиме FD-передачи, когда пользователь помогает другому пользователю, принимая сигнал от источника и передавая сигнал пользователям в то же время и на той же частоте, применяя разработанный алгоритм CF. Оценка производительности показывает, что FA-MNOMA превосходит другие методы, а секретность FA-MNOMA может быть дополнительно оптимизирована с использованием MLGA. FA-MNOMA возможно применить в любой системе беспроводной связи. В данной работе он реализован для ИТС.

Литература

1. Yue X., Liu Y., Kang S., Nallanathan A., Ding Z. Exploiting Full/Half-Duplex User Relaying in NOMA Systems // *IEEE Transactions on Communications*. 2018. Vol. 66. Iss. 2. PP. 560–575. DOI: 10.1109/TCOMM.2017.2749400
2. Yin L., Chengong W., Kai M., Kuanxin B., Haowei B. A NOMA Power Allocation Strategy Based on Genetic Algorithm // *Proceedings of the 8th International Conference in Communications, Signal Processing, and Systems (CSPS 2019)*. Lecture Notes in Electrical Engineering. Singapore: Springer, 2019. Vol. 571. PP. 2182–2190. DOI:10.1007/978-981-13-9409-6_265
3. Khan R., Kumar P., Jayakody D. N. K., Liyanage M. A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions // *IEEE Communications Surveys & Tutorials*. 2020. Vol. 22. Iss. 1. PP. 196–248. DOI: 10.1109/COMST.2019.2933899
4. Xu D., Ren P., Lin H. Combat Hybrid Eavesdropping in Power-Domain NOMA: Joint Design of Timing Channel and Symbol Transformation // *IEEE Transactions on Vehicular Technology*. 2018. Vol. 67. Iss. 6. PP. 4998–5012. DOI: 10.1109/TVT.2018.2802915
5. Chen X., Liu G., Ma Z., Zhang X., Fan P., et al. When Full Duplex Wireless Meets Non-Orthogonal Multiple Access: Opportunities and Challenges // *IEEE Wireless Communications*. 2019. Vol. 26. Iss. 4. PP. 148–155. DOI: 10.1109/MWC.2019.1800369

6. Mohammadi M., Shi X., Chalise B. K., Ding Z., Suraweera H. A., et al. Full-Duplex Non-Orthogonal Multiple Access for Next Generation Wireless Systems // IEEE Communications Magazine. 2019. Vol. 57. Iss. 5. PP. 110–116. DOI: 10.1109/MCOM.2019.1800578

7. Khan R., Jayakody D. N. K. Full Duplex Component-Forward Cooperative Communication for a Secure Wireless Communication System // Electronics. 2020. Vol. 9. Iss. 12. P. 2102. DOI: 10.3390/electronics9122102

8. Goel S., Negi R. Guaranteeing Secrecy using Artificial Noise // IEEE Transactions on Wireless Communications. 2008. Vol. 7. Iss. 6. PP. 2180–2189. DOI: 10.1109/TWC.2008.060848

9. Zhang Z., Ma Z., Xiao M., Ding Z., Fan P. Full-Duplex Device-to-Device-Aided Cooperative Nonorthogonal Multiple Access // IEEE Transactions on Vehicular Technology. 2016. Vol. 66. Iss. 5. PP. 4467–4471. DOI: 10.1109/TVT.2016.2600102

10. Khan R., Jayakody D. N. K., Pervaiz H., Tafazolli R. Modulation Based Non-Orthogonal Multiple Access for 5G Resilient Networks // Proceedings of the IEEE Globecom Workshops (GC Wkshps. IEEE, 2018. DOI: 10.1109/GLOCOMW.2018.8644085

Статья поступила 11 мая 2023 г.

Одобрена после рецензирования 30 ноября 2023 г.

Принята к публикации 04 декабря 2023 г.

Информация об авторе

Хан Рабиа – аспирант Инженерной школы информационных технологий и робототехники Национального исследовательского Томского политехнического университета. E-mail: rabi.khan14@gmail.com

An Algorithm Design for a Secure Full Duplex Non-Orthogonal Multiple Access in Wireless Communication System

R. Khan

National Research Tomsk Polytechnic University,
Tomsk, 634050, Russian Federation

In this article, a new Component-Forward (CF) cooperative communication algorithm is proposed for Full Duplex Modulation-based Non-Orthogonal Multiple Access and is referred as FD-MNOMA. The FD-MNOMA prevents security issues in the FD mode of a cooperative communication system, where a near user assists a far user to receive a better quality of signal. For further improving the security issues, Artificial Noise (AN) is also added to the signal and called it FA-MNOMA. In this article, the secrecy capacity equation is derived for the FA-MNOMA algorithm. Performance evaluation shows that FA-MNOMA and FD-MNOMA outperforms the traditional NOMA. The secrecy capacity of FA-MNOMA is further optimized using Machine Learning Genetic Algorithm (MLGA). This article also shows the implementation of FA-MNOMA in the Intelligent Transportation System (ITS) as one of its applications.

Key words: 5G, AN, component-forward (CF), FA-MNOMA, FD, NOMA, MLGA, secrecy capacity

Information about Author

Rabia Khan – Ph.D. student, National Research Tomsk Polytechnic University.
E-mail: rabi.khan14@gmail.com