В.А. Рындюк, В.А. Козлов

Гибридная распределенная модель системы кодирования управляющих воздействий

В настоящее время все более актуальными становятся вопросы использования беспилотных объектов, применяемых для выполнения различного рода автономных задач. Управление такими объектами осуществляется дистанционно по беспроводному каналу связи. К данной ка-

тегории объектов дистанционного управления принадлежат, к примеру:

– системы бесконтактной передачи управляющего воздействия на различного рода механизмы в рамках единого устройства (например, автомобиля), работающего в режиме непосредственного цифрового управления (НЦУ);

– автоматизированные системы контроля и доступа (например, автотранспорта на охраняемую территорию), системы управления ячейками камеры хранения или депозитария;

– системы управления беспилотными, перемещающимися в пространстве устройствами (роботами, автомобилями, летательными аппаратами и т.д.).

Сложность и значимость задач, выполняемых такими устройствами, как в гражданской сфере общества, так и в военных целях, обусловливает необходимость их надежного и бесперебойного использования. Поэтому важнейшей задачей является обеспечение защиты таких устройств от возможных незаконных управляющих воздействий извне по беспроводным каналам связи в режиме реального времени.

Это и определило **цели** настоящего исследования: разработка модели криптографических преобразований системы кодирования управляющих воздействий, которые передаются по незащищенным каналам связи.

Алгоритмы беспилотного управления можно успешно применять, к примеру, при перевозке беспилотным летательным аппаратом (БПЛА) денежных средств.

Системы дистанционного беспилотного управления должны обладать как минимум двумя распределенными пунктами формирования управляющих воздействий (отправителя и получателя).

Дистанционное управление объектом в режиме онлайн по беспроводному каналу связи имеет ряд специфических особенностей. Эти проблемы, в первую очередь, связаны с тем, что коды управляющих воздействий на объект могут быть перехвачены злоумышленниками.

Существуют два возможных способа защиты от такого рода атак: физический (путем изменения различных характеристик, например, частотных, передаваемого сигнала по неизвестным для злоумышленника правилам), и криптографический (путем шифрации кодов управляющих воздействий).

Каждый из этих вариантов защиты имеет свои преимущества и недостатки. Наиболее эффективным способом защиты считается одновременное использование обоих вариантов. В нашей статье мы ограничимся исследованием второго, криптографического способа защиты.

Как известно, традиционные способы шифрации кодов управляющих воздействий не всегда эффективны даже при использовании криптографически стойких систем шифрации. Дело в том, что хакеру совсем не обязательно заниматься дешифрацией перехваченных им шифр-кодов управляющих воздействий. Ему, для внесения хаоса в процесс дистанционного управления объектом, достаточно просто посылать на этот объект перехваченные им раннее шифр-коды управляющих воздействий.

Вторая, не менее важная проблема для таких систем дистанционного управления, связана с защитой от DDoS-атак. При DDoS-атаке на объект управления (в состав которого входит компьютерное устройство), этот объект перестает реагировать на запросы законной системы управления.

В данной работе описаны модели и методы построения системы дистанционного управления, обеспечивающей решение этих двух взаимосвязанных проблем защиты: от DDoS-атак и от хакера, перехватывающего шифр-коды управляющих воздействий с целью воздействия на процесс дистанционного управления объектом по незащищенному каналу связи.

Система управления беспилотным объектом включает в себя два самостоятельных, но взаимосвязанных режима управления: автономный и внешний.

Автономный – характеризуется априори выбранной и заложенной в программу автономного устройства специальной программой управления, например, в виде конкретного маршрута передвижения БПЛА.

Внешний режим управления предполагает формирование так называемых корректирующих управляющих воздействий, изменяющих саму программу режима автономного управления. Например, воздействий, связанных с внештатной коррекцией программы полета БПЛА или с изменением режима работы какого-либо механизма объекта, работающего в режиме НЦУ.

Дистанционное управление автономным объектом осуществляется с использованием беспроводных сетевых Wi-Fi технологий и, так как беспроводная связь характеризуется большим радиусом доступности, значит у злоумышленника есть возможности для перехвата и анализа управляющей информации.

В связи с этим модель дистанционного управления по открытому каналу связи должна обладать дополнительными возможностями, не позволяющими злоумышленнику (даже при наличии у него больших объемов ранее перехваченной им информации, связанной с дистанцион-

ным управлением именно этим объектом) получить полезную для него информацию.

Во-первых, это так называемая сеансовая аутентификация, отличающаяся тем, что для каждого очередного сеанса связи генерируется новый сеансовый ключ аутентификации. И, во-вторых, это применение шифр-кодов управляющих воздействий, которые каждый сеанс связи шифруются с использованием новых одноразовых (сеансовых) ключей шифрации.

Выполнение этих двух условий гарантированно отсекает возможность воздействия хакера на процесс дистанционного управления объектом, так как при хаотичном вбрасывании перехваченных им раннее шифр-кодов управляющих воздействий, они, во-первых, не пройдут процесс сеансовой аутентификации, а во-вторых, их дешифрация с использованием текущего сеансового ключа связи не даст ожидаемых злоумышленником результатов, поскольку их шифрация производилась не текущим, а перехваченным ранее сеансовым ключом.

Для реализации этих дополнительных условий мы предлагаем использовать гибридную вероятностную модель криптографических преобразований. Классический вариант такой модели шифрации включает в себя две системы шифрации: симметричную и асимметричную, существенно различающихся, в том числе по быстродействию выполнения процедур шифрации и дешифрации (симметричная система выполняет данные процедуры на порядок быстрее).

В гибридной вероятностной модели криптографических преобразований при помощи симметричного блока выполняется шифрация исходного текста сеансовым (одноразовым) ключом, а сам ключ, имеющий небольшую размерность, шифруется асимметричным блоком гибридной модели с использованием открытого ключа вашего партнера.

Такой подход позволяет добиться приемлемой скорости процедур шифрации и дешифрации и не требует передачи секретной информации (сеансового симметричного ключа) партнеру по защищенному каналу связи.

Особенностью вероятностных гибридных моделей является то, что они, в отличие от классических гибридных моделей, используют в качестве дополнительного параметра вектор инициализации (комбинацию случайных чисел), и это позволяет при многократной шифрации одного и того же исходника получать разные по содержанию шифрограммы. В процессе организации очередного сеанса связи соединение сеансового ключа и вектора инициализации шифруется асимметричным блоком вероятностной гибридной модели с использованием открытого ключа получателя.

Рассмотрим более подробно основные этапы функционирования вероятностной гибридной модели. На первом этапе отправитель формирует случайный сеансовый ключ связи – вектор инициализации (сокращенно In.Vect).

На втором этапе исходник шифруется симметричным алгоритмом, используя в качестве ключа шифрации In.Vect (вектор инициализации). На этом этапе производится шифрация In.Vect с использованием алгоритма асимметричных криптопреобразований (АКП), при этом ключом шифрации является открытый ключ асимметричной системы криптопреобразований получателя.

На третьем этапе симметричный шифр исходника и АКП-шифр In.Vect передаются получателю по открытому каналу связи.

Получатель сначала расшифровывает своим закрытым асимметричным ключом сеансовый симметричный ключ (In.Vect), а затем расшифровывает с его помощью полученный им шифр исходного текста.

Такую технологию связи по незащищенному беспроводному каналу связи, построенную на базе вероятностной гибридной модели, часто называют технологией *digital envelope* (*цифрового конверта*). В рамках этой технологии сеансовый ключ действителен только для одного сеанса связи, что и служит гарантией более высокого уровня защиты.

Таким образом, для защиты от DDos-атак использован оригинальный алгоритм анализа принятой приемником шифрограммы. Алгоритм используется для нахождения кода аутентификации отправителя, встроенного в текст шифрограммы. Ключом этого алгоритма является In.Vect предыдущего сеанса связи, переданный получателю в зашифрованном виде.

Такой подход обеспечивает эффективную защиту от DDos-атак, которые пресекаются практически мгновенно, еще до начала обработки пакета путем его дешифрации.

Таким образом, нами предложен эффективный алгоритм распределенного управления объектом по беспроводному каналу связи, который можно успешно использовать, например, при перевозке денежных средств БПЛА в больших городах с интенсивным движением транспортных средств. Практическая реализация таких перевозок одобрена руководством Сбербанка РФ [5; 6].

Библиографический список

1. Козлов В.А., Рындюк В.А., Воробьев Г.А., Чернышев А.Б. Модели и методы защиты от атак «Man in the middle» (MITM) // Современные фундаментальные и прикладные исследования. 2017. № 1 (24). С. 27-35.
2. Козлов В.А., Рындюк В.А. Система дистанционного управления объектом

по незащищенным каналам связи на базе системы диалогового кодирования и вероятностной модели криптографических преобразований // Вестник Ессентукского института управления, бизнеса и права. Ессентуки. 2015. № 11. С. 260-264.
3. Козлов В.А., Рындюк В.А. Система управления депозитарными банковскими ячейками на базе вероятностной модели электронной цифровой подписи // Труды Международной научно-практической конференции «Транспорт-2015», Ростов-на-Дону, апрель 2015 г. Часть 2. Технические науки. Ростов-на-Дону, 2015. С. 66-69.
4. Козлов В.А., Чернышев А.Б., Калиберда И.В., Оршанский А.Ю. Вероятностная модель системы асимметричных криптографических преобразований // Научное обозрение. 2015. № 7. С. 261-266.
5. Козлов В.А., Чернышев А.Б., Рындюк В.А., Оршанский А.Ю. Вероятностная модель системы симметричных криптографических преобразований для дистанционного управления объектами по открытым каналам связи // Современные фундаментальные и прикладные исследования. Кисловодск. 2016. № 2 (21). С. 43-48.
6. «Сбербанк» проведет испытания беспилотника для перевозки наличных. [Электронный ресурс]. Режим доступа: http://ruvsa.com/news/unmanned_systems_development/sberbank%2c+ispitania%2c+drones%2c+perevoski.
7. ЦБ РФ инициировал правовую основу для доставки наличности беспилотниками [Электронный ресурс]. Режим доступа: http://ruvsa.com/news/unmanned_systems_development/Russia%2C+drones%2C+law%2C+money
8. Ferguson N., Schneier B., & Kohno T. (2010). Cryptography Engineering: Design Principles and Practical Applications. New York: John Wiley & Sons.
9. Gary C. Kessler. An Overview of Cryptography. © 1998-2016 – A much shorter, edited version of this paper appears in the 1999 Edition of Handbook on Local Area Networks, published by Auerbach in September 1998 [Электронный ресурс]. Режим доступа: http://www.garykessler.net/library/ crypto. html#fig02.
10. Mao W. Modern Cryptography: Theory & Practice. Upper Saddle River, NJ: Prentice Hall Professional Technical Reference, 2004.
11. Vorobyev G.A., Ryndjuk V.A., Kozlov V.A., Makarov A.M. Probabilistic models of cryptographic systems and their applications // 3rd International Conference on Digital Information Processing, Data Mining, and Wireless Communications, DIPDMWC. 2016. № 3. С. 160-163.