ПРОТОКОЛ ВЗАИМНОЙ АУТЕНТИФИКАЦИИ ГРУППЫ ОБЪЕКТОВ С ДИНАМИЧЕСКОЙ ТОПОЛОГИЕЙ

Басан А.С.[1], Басан Е.С.[2], Ищукова Е.А.[3], Корнилов А.П.[4]

Цель: *Цель работы заключается в разработке протокола взаимной аутентификации для группы объектов с динамической топологией (например, для роя беспилотных летательных аппаратов (БПЛА)), которые совместно выполняют общее задание. При этом важно учитывать, что каждый отдельный объект группы обладает ограниченным запасом энергии. Необходимо учитывать тот факт, что объект может выключаться из сети, а затем заново подключаться к ней, поэтому протокол должен предусматривать способ повторной взаимной аутентификации объектов группы. Также объекты должны иметь возможность передавать данные на управляющий узел, который называется базовая станция (БС). При проектировании протокола важно учесть, что риски вскрытия переданной информации должны быть минимизированы в случае, если злоумышленник получит физический доступ к памяти объекта группы.*

Методы исследования: *Метод основывается на использовании математического аппарата теории вероятностей, математической статистики, теории информации, криптографии. В качестве криптографических примитивов используются генератор псевдослучайных последовательностей, функции хеширования, симметричное шифрование, а также физически неклонируемая функция.*

Результаты: *Выполнен анализ существующих подходов к взаимной аутентификации и передаче данных в группе объектов с динамической топологией. Предложен протокол взаимной аутентификации БПЛА, который решает ряд важных задач, таких как: динамическое изменение ключа шифрования, отсутствие высоконагруженных вычислений для динамических элементов сети, масштабируемость, возможность обмена данными между участниками сети. Разработанный протокол основывается на использовании нескольких базовых алгоритмов: алгоритма построения остовного дерева, алгоритма выполнения взаимной аутентификации БПЛА и организации передачи данных, а также алгоритма выполнения аутентификации БПЛА перед БС. Предоставлен имитационный пример для иллюстрации разработанного решения с выделенными фазами и анализ передачи в нем сообщений в рамках двух БПЛА.*

Научная новизна *прежде всего состоит в том, что в разработанном протоколе аутентификации особое внимание уделено задаче устойчивости схемы аутентификации и реконфигурации сети БПЛА, а также учтена проблема малых вычислительных мощностей, большая часть высоконагруженных расчетов, занимающих процессор, передана на БС – самый мощный вычислительный элемент сети. Приведенное решение обеспечивает смену сессионного ключа с наличием минимума заранее установленной информации и постоянное обновление ключа между элементами сети.*

Вклад каждого соавтора: *Басан Е.С. — общее руководство проектом, разработка технического задания на разработку протокола взаимной аутентификации для групп объектов с динамической топологией, разработка алгоритма выполнения аутентификации БПЛАП перед базовой станцией; Басан А.С. — проведение анализа существующих методов взаимной аутентификации для группы объектов с динамической топологией; Ищукова Е.А. – разработка алгоритма выполнения взаимной аутентификации БПЛА и организации передачи данных; Корнилов А.П. – разработка алгоритма построения остовного дерева, проведение моделирования, анализ результатов.*

Ключевые слова: *беспилотный летательный аппарат, базовая станция, аутентификация, криптография, шифрование, псевдослучайное число, остовное дерево, сеть, хэш функция, временная метка, запрос, ответ, масштабируемость, отказоустойчивость.*

DOI:10.21681/2311-3456-2023-4-41-52

1 Басан Александр Сергеевич, кандидат технических наук, доцент кафедры Безопасности информационных технологий Института компьютерных технологий и информационной безопасности Южного Федерального Университета «ЮФУ», г. Таганрог, Россия. E-mail: asbasan@sfedu.ru.

2 Басан Елена Сергеевна, кандидат технических наук, доцент кафедры Безопасности информационных технологий Института компьютерных технологий и информационной безопасности Южного Федерального Университета «ЮФУ», г. Таганрог, Россия. E-mail: ebasan@sfedu.ru, ORCID 0000-0001-6127-4484.

3 Ищукова Евгения Александровна, кандидат технических наук, доцент кафедры Безопасности информационных технологий Института компьютерных технологий и информационной безопасности Южного Федерального Университета «ЮФУ», г. Таганрог, Россия. E-mail: uaishukova@sfedu.ru, ORCID 0000-0002-6818-1608.

4 Корнилов Александр Петрович, студент кафедры Безопасности информационных технологий Института компьютерных технологий и информационной безопасности Южного Федерального Университета «ЮФУ», г. Таганрог, Россия. E-mail: akornilov@sfedu.ru.

Введение

В современном быстроменяющемся мире проблема проверки подлинности пользователя и программы в автоматизированном виде актуальна как никогда раньше. Процесс предоставления защищенного доступа и установления доверительных отношений между автоматизированной системой и другой стороной является основой аутентификации как проверки, действительно ли собеседник тот, за кого себя выдает. В связи с точностью и механичностью аутентификации и идентификации создаются реализации автоматических средств, предназначенных для проведения данных действий в рамках компьютерного процесса, то есть делегирование этих полномочий базовому вычислительному устройству по заранее заданному алгоритму. Особенно остро проблема аутентификации в условиях ограниченности ресурсов стоит в сетях БПЛА, что породило целый ряд работ, посвященных данной проблеме, причем создатели протоколов делают упор на различные аспекты при самой реализации своего решения. Большая часть работ подразумевает наличие пользователя в системе, представляемого программной сущностью с минимально возможными вычислительными возможностями, и процесс аутентификации включает в себя дополнительную третью сторону как активного участника. Существующие классические решения, связанные с центрами сертификации и сертификатом открытого ключа, не подходят в связи с тем, что не решают проблему аутентификации элементов сети перед базовой станцией.

В работе [1] представлена модель шифрования в сети БПЛА в гетерогенной сети. Для защиты данных при общении БПЛА в сети используется техника функционального шифрования. Данная техника позволяет знать пользователям только определенную информацию во всем сообщении. Весь процесс разделен на две фазы: общение между устройством пользователя и БС и общение между БС и устройством пользователя через БПЛА. Данный протокол был проверен при помощи инструмента AVISPA, что дает достаточный уровень безопасности коммуникации в подобной сети. В работе [2] представлена система обнаружения вторжений в сети БПЛА. БПЛА в сети подвержены большому количеству атак, которые позволяют предотвращать и обнаруживать вторжения. В частности, в статье были классифицированы существующие механизмы обнаружения вторжений по способу сбора ресурсов, стратегии размещения, состоянию обнаружения и типу вторжений. В статье [3] представлена схема шифрования данных на основе уникальности в гетерогенных сетях БПЛА. Данное исследование показывает способ безопасного общения в гетерогенных сетях БПЛА при помощи шифрования, основанного на уникальности, что также предотвращает сеть от нарушителей и вторжения. В [4] представлен надежный протокол аутентификации дронов в сети БПЛА на основе индивидуальных характеристик из сигнала электроэнцефалограммы (ЭЭГ). В качестве источника выработки производного ключа используется ЭЭГ оператора в биометрической системе для шифрования между БПЛА и базовой станцией (БС). Представлены сценарии коммуникаций в сети в случае атаки, что позволяет добраться БПЛА до безопасной локации в целости и сохранности. В работе [5] представлена стратегия взаимодействия БПЛА в гетерогенных сетях с коммуникацией на радиоволнах миллиметровой длины. Дано описание подобных коммуникаций в сетях, сформулированы их проблемы в графоподобных сетях, разработана стратегия уменьшения задержки при передаче данных в кооперативной сети и представлены задачи на будущее развитие для разработанной стратегии. В [6] представлен легковесный механизм аутентификации для БПЛА по легковесной анонимной схеме аутентификации. Оригинальный протокол достаточно не масштабируемый, легко отслеживаемый и уязвим к основным сетевым атакам, поэтому была предложена схема легковесных симметричных ключей и временных секретных данных в Улучшенной версии данного протокола. В работах [7, 8] представлен процесс аутентификации на основанной на уникальности подписи-шифрования в сети LoRaWan (широкодоступные сети с большим радиусом действия). Подобная схема смешивает подпись и шифрование на публичном ключе в одну процедуру. Отличие предложенных решений заключается в том, что в [8] используются временные учетные данные. Согласно [9] предложена схема, в которой аутентификация пользователей заменена на аутентификацию устройств, в связи с тем, что БПЛА взаимодействуют без человеческого вмешательства. Представлена схема прямого анонимного подтверждения как элегантное средство баланса между анонимностью и аутентичностью, также предложена схема взаимной аутентификации на ассиметричных парах ключей, доверенном платформенном модуле. В работе [10] представлен алгоритм аутентификации на основе различных криптографических механизмов, таких как криптография на эллиптических кривых, цифровая подпись, хэш-функция. Данные криптографические сервисы обеспечивают целостность, конфиденциальность, анонимность, до-

ступность, приватность, неотрицание и защиту от атаки отказ в обслуживании. Дополнительно проанализированы затраты по памяти используемых сообщений в сети. В работе [11] представлен протокол на основе блокчейн-технологии. БПЛА в сети могут общаться как узлы в блокчейн сети. Предложенная техника ассиметричного шифрования позволяет определить неверную информацию при физическом похищении БПЛА. Около 90% БПЛА способны взаимодействовать друг с другом в то время как поддельные БПЛА не могут распространять поддельную информацию в сети. В [12] для LoRaWan (широкодоступные сети с большим радиусом действия) представлены криптографические механизмы для реализации безопасности в сетях БПЛА. В статье [13] представлена схема валидации через часть пароля, что не позволяет атакующему заполучить полный пароль за одну попытку. Реализация данного механизма осуществляется через проблему декомпозиции вектора, что позволяет пользователю создавать пароль из обычных символов, вводимых в случайном порядке в двумерном пространстве. В работе [14] рассмотрен протокол аутентификации пользователей с БПЛА на основе секретного сеансового ключа с использованием временных учетных данных.

Облегченный протокол аутентификации для сетей БПЛА на основе безопасности и оптимизации вычислительных ресурсов [15] был предложен группой ученых из Китайской народной республики в 2021 году. Данная схема предполагает наличие Сервера, являющегося самым мощным вычислительным элементом сети, точки доступа, через которую происходит подключение к серверу, самого БПЛА и сенсора, который является самым ограниченным по вычислительным мощностям устройством, ассоциирован с человеком. Предполагается наличие только одного сервера в сети и связь элементов сети с сервером через точку доступа. Ключевая проблема данного протокола заключается в отсутствии описания использования параметров, подтверждающих аутентичность устройства. Ключевым преимуществом является выработка одинакового ключа у сенсора, связанного с ним БПЛА и сервера. Также данный протокол является легковесным – основные вычисления переносятся на сервер, вычисления производятся за ограниченное время и с временными метками, чтобы противостоять атаке повтором, и также малое количество информации, требующейся для аутентификации.

Из криптографических примитивов требуются модули:

— генератор псевдослучайных чисел (ГПСЧ);
— функция свертки (хэш-функция);
— модулярная арифметика на больших числах;
— алгоритм симметричного шифрования;
— физически неклонируемая функция (ФНФ) – программная реализация на псевдослучайных числах;
— функции работы со временем – получение текущего системного времени и анализ разницы временных меток.

Данный протокол не подходит в изначальном своем варианте из-за отсутствия в нем механизма взаимной аутентификации участников сети – БПЛА. Также предполагается аутентификация пользователя через маломощный сенсор, что неактуально для задачи.

Усовершенствованный протокол аутентификации для связи дронов в сетях 5G [16] также представленный китайскими учеными в конце 2021 года предполагает наличие в системе пользователей, БПЛА и сервер аутентификации. Пользователь ассоциируется с мобильным устройством и сначала получает доступ к нему, после этого появляется возможность взаимодействовать с сетью. Пользователь нужен для наблюдения за информацией о БПЛА и формирования полетной миссии. Протокол является легковесным, так как на самих дронах и мобильных устройствах используются малоресурсные и облегченные криптографические операции. Для конкретной тройки пользователь (мобильное устройство), БПЛА, сервер генерируется одинаковый сессионный ключ. Также для противостояния атаке повтором используются временные метки. Большая часть информации в протоколе передается в хэшированном виде, что затрудняет подделку сообщения и позволяет не передавать в открытом виде идентифицирующую информацию.

Из криптографических примитивов требуются модули:

— ГПСЧ;
— функция свертки (хэш-функция);
— биометрическая функция (как один из факторов аутентичности);
— алгоритм симметричного шифрования;
— функции работы со временем – получение текущего системного времени и анализ разницы временных меток.

Усовершенствованный протокол аутентификации для связи дронов в сетях 5G уязвим к атаке, направленной на физический захват дрона, что неминуемо приведет к раскрытию сессионного ключа и как следствие возможность отправлять ложные сообщения с использованием оригинальных ключей БПЛА.

Масштабируемый протокол взаимной аутентификации S-MAPS для динамических групп БПЛА [17] представлен в начале 2022 года учеными из Сингапура. Протокол предполагает связь между БПЛА и базовой станцией через остовное дерево. Предполагается наличие полной связи между всеми элементами сети (БПЛА) и базовой станцией для построения дерева и наличия на устройстве физически неклонируемой функции для создания пар запрос-ответ. Данный протокол работает и для изменяемой сети путем перестроения дерева и внесения информации о паре запрос-ответ на базовую станцию. Для обеспечения уверенности в аутентичности устройства возможно провести несколько итераций протокола. Шифрование информации цифровым отпечатком устройства при передаче защищает протокол при прослушке открытого канала. При генерации остовного дерева с случайной точки возможность блокирования одним БПЛА коммуникации в сети очень мала, также используемые временные метки позволяют избегать атаку повтором.

Из криптографических примитивов требуются модули:

— ГПСЧ;
— функция свертки (хэш-функция);
— алгоритм симметричного шифрования;
— физически неклонируемая функция;
— функции работы со временем– получение текущего системного времени и анализ разницы временных меток.

Данный протокол не подходит в изначальном своем варианте из-за отсутствия в нем механизма взаимной аутентификации участников сети – БПЛА.

Способ построения системы опознавания свой-чужой на основе протокола с нулевым разглашением [18] представлен российскими учеными в 2014 году. Данная схема позволяет только определять в системе путем запросов и ответов кто владеет секретными значениями, а кто нет, не раскрывая их. Для начала работы протокола необходима инициализация проверяемых значений с последующей перепроверкой. Ключевым плюсом данной системы является отсутствие разглашения информации и определение того, кто является своим, а кто чужим в сети. Данный протокол не позволяет выработать сеансовый ключ, он позволяет только идентифицировать участника протокола. В основе данной системы опознавания свой-чужой на основе протокола с нулевым разглашением лежит модулярная арифметика в поле больших чисел.

В 2019 году группой российских ученых получен патент на способ, систему и устройство криптографической защиты [19]. В патенте описан способ криптографической защиты каналов связи между БПЛА и базовой станцией, основанный на использовании симметричной и асимметричной криптографии. Указанный пакет описывает принцип выработки и передачи ключей между БПЛА и базовой станцией, но не обеспечивает динамическую смену ключа. Также наличие патента накладывает ограничения на его использование.

1. Постановка задачи

В настоящий момент не существует универсальных протоколов аутентификации, которые бы подходили для всех задач БПЛА. Более того, большинство протоколов БПЛА ориентированы на использование зарубежной криптографии — как в области симметричного шифрования, так и в области асимметричного. Необходимо разработать протокол аутентификации для роя БПЛА, которые совместно выполняют общее задание. При этом необходимо предусмотреть тот факт, что БПЛА обладает ограниченным запасом энергии, а соответственно может выключаться из сети, а затем заново подключаться к ней. В этих случаях протокол должен предусматривать способ повторной аутентификации БПЛА. Также при выполнении задания роем БПЛА каждый отдельный БПЛА должен иметь возможность передавать конфиденциальные данные БС. Важно учесть, что риски вскрытия переданной информации должны быть минимизированы в случае, если злоумышленник получит физический доступ к памяти БПЛА.

Основные задачи, решаемые протоколом, должны включать в себя:

— возможную смену ключа (его динамическое изменение);
— отсутствие привязки к конкретному значению (зашитые в железо значения ключей);
— легковесность для элементов сети (отсутствие высоконагруженных вычислений для каждого элемента сети);
— легкая масштабируемость и отсутствие больших объемов данных, передаваемых в сети;
— отказоустойчивость с учетом наличия в сети злоумышленников и реконфигурации в сети.

При разработке необходимо сделать основной упор на использование отечественной криптографии, учесть возможное частое включение выключение устройств, а также малый вычислительный ресурс устройств.

2. Протокол взаимной аутентификации группы объектов с динамической топологией

Для решения поставленной задачи предлагается взять схему взаимодействия БПЛА с базовой станцией по принципу использования остовного дерева, как это описано в работе [3]. При этом весь математический аппарат будет основан на отечественной криптографии. Предполагается, что для обмена данными между БПЛА и БС будет использоваться симметричное шифрование на основе стандартов ГОСТ Р34.12-2015 [6] и ГОСТ Р34.13-2018 [7]. В качестве алгоритма шифрования предполагается использовать симметричный блочный шифр Кузнечик, обрабатывающий 128-битный блок данных на секретном ключе длиной 256 бит. В качестве режимов шифрования используется режим простой замены с зацеплением (CBC). Генерация псевдослучайных последовательностей будет выполняться на основе стандарта ГОСТ Р ИСО 28640-2012 [8]. В качестве функции хэширования выбран отечественный алгоритм хэширования «Стрибог», описанный в стандарте ГОСТ Р 34.11-2012 [9] длиной 256 бит. В качестве физически неклонируемой функции предлагается использовать программную реализацию на основе подхода, описанного в работе [10]. Использование данной функции позволяет сформировать уникальный цифровой слепок устройства на основе аппаратных данных устройства.

Работа протокола состоит из двух фаз: подготовительной и основной. В рамках подготовительной фазы происходит регистрация БПЛА в реестре БС. При этом формируется ключ симметричного шифрования, общий для данного БПЛА и БС, который предполагается использовать для шифрования данных журнала логирования БПЛА, а также для передачи первичных значений, по которым строится остовное дерево. Ключ генерируется на основе рекомендаций по стандартизации Р 1323565.1.022–2018 [11]. На следующем шаге строится остовное дерево в виде графа, вершинами которого являются элементы сети (подразумевается, что граф связный). Остовное дерево и все его возможные пути от базовой станции доступны всем участникам сети для выполнения протокола аутентификации. Путь представляет собой последовательность связанных, неповторяющихся вершин до вершины со степенью 1. Во время подготовительной фазы выполняется регистрация БПЛА. Для этого базовая станция собирает данные от каждого устройства БПЛА с помощью протокола запрос-ответ. При этом передаваемые данные формируются на основе физически неклонируемой функции, как цифрового отпечатка системы и доказательства аутентичности.

Используемые обозначения:

n – количество БПЛА в сети;

m – устройство под номером m из n БПЛА в сети;

ρ – количество всех возможных путей остового дерева;

i – i-ый путь из ρ путей;

k_i – количество узлов в i пути;

j – j-ый путь из k_i элементов i-ого пути;

PUF(X) – значение физически неклонируемой функции от аргумента X;

ID_m : – идентификатор $БПЛА_m$;

MK_m : – мастер-ключ $БПЛА_m$;;

БС – базовая станция;

$БПЛА_{ij}$ – БПЛА, находящийся на i пути j позиции;

$E(X)_K$ – зашифрование сообщения X на ключе K;

$D(X)_K$ – расшифрование сообщения X на ключе K;

C_{ij} , R_{ij} – пара запрос-ответ для $БПЛА_{ij}$;

AK – единый ключ аутентификации (authentication key);

T_0 – временная метка;

t – текущее время;

S_{Kij} – Сессионный ключ $БПЛА_{ij}$ с БС;

$N_{\pm}$ – случайное значение (nonce), сгенерированное БС;

N_{ij} – случайное значение (nonce), сгенерированное $БПЛА_{ij}$;

M_i – запрос, сформированный БС для i пути;

M_{ij} – запрос, сформированный БС для $БПЛА_{ij}$;

T_{ij} – ответ $БПЛА_{ij}$ для БС;

T_i – ответ по i пути для БС;

X||Y – конкатенация значений X и Y;

X/Y – убрать значение X из Y;

X←Y: Z передача значения Z от устройства Y устройству X.

Для описания инфраструктурных решений, используемых в дальнейшем моделировании протокола, опишем 3 вспомогательных алгоритма, используемые в разработанном протоколе – алгоритм построения остового дерева, алгоритм передачи и выполнения процесса аутентификации на устройстве и алгоритм выполнения аутентификации на БС.

Алгоритм 1. Построение остовного дерева.

1. Получение списка ребер N, состоящего из элементов (u, v), где u и v это элемент сети – БС или БПЛА.

2. Инициализация результирующего списка ребер остовного дерева ST = $\varnothing$.

3. Пока |ST| < |N|-1 переходить на шаг 4 иначе конец алгоритма, вернуть ST.

4. Получение очередного ребра (u, v) из списка N.

5. Если множество всех соединенных вершин с u не равно множеству всех соединенных вершин с v, то переход на шаг 6 иначе на шаг 3.

6. Добавляем в список ST ребро (u, v).

Алгоритм 2. Выполнение взаимной аутентификации БПЛА и организации передачи данных.

1. Если j=1, то $БПЛА_{ij} \leftarrow$ БС: $M_i = M_i / M_{ij}$, иначе $БПЛА_{ij} \leftarrow БПЛА_{i(j-1)}$: $M_i = M_i / M_{ij}$. Обработка выполняется для всех значений i от 1 до ρ и для всех j от 1 до k_i.

2. $БПЛА_{ij}$: $D\left(E\left(N_\alpha, T_0, R_{ij}\right)_{R_{ij}}\right)$Если не проходят условият $- T_0 \geq \Delta T$, PUF(C_{ij}) = R_{ij}, $T_0 = T_0^{872;}$, то происходит ошибка аутентификации БС, устанавливается $T_{ij}^{"}$ = "" и процесс аутентификации для данного БПЛА заканчивается с ошибкой. Обработка выполняется для всех значений i от 1 до ρ и для всех j от 1 до k_i.

3. $БПЛА_{ij}$: N_{Cij}, S_{Kij}=$C_{ij} \oplus N_{\pm} \oplus N_{C_{ij}}$, $C_{ij}^{'}$, $R_{ij}^{'}$ = PUF($C_{ij}^{'}$), $T_{ij}^{"}$=$E(N_{C_{ij}}, T_0, C_{ij}^{'}, R_{ij}, R_{ij})_{R_{ij}}$. Обработка выполняется для всех значений i от 1 до ρ и для всех j от 1 до k_i.

Алгоритм 3. Выполнение аутентификации БПЛА перед БС.

1. БС, генерирует АК.

2. БС: $D(E(N_{C_{ij}}, T_0, C_{ij}^{'}, R_{ij}^{'}, R_{ij})_{R_{ij}})_{R_{ij}}$, если не $t - T_0 \geq \Delta T$, то ошибка аутентификации $БПЛА_{ij}$ и переход к следующему j, S_{Kij}=$C_{ij} \oplus N_{\pm} \oplus N_{C_{ij}}$, $C_{ij}^{'}$, $R_{ij}^{'}$, $E(AK)_{S_{Kij}}$, начальное значение Q_i = "", $Q_i = Q_i \,||\, E(AK)_{S_{Kij}}$. Обработка выполняется для всех значений i от 1 до ρ и для всех j от 1 до k_i.

Для демонстрации принципов работы приведено формальное описание протокола.

Протокол взаимной аутентификации БПЛА.

1. БС$\leftarrow БПЛА_m$: ID_m, MK_m, $E(ID_m, C_m, C_m)_{MK_m}$ Обработка выполняется для всех устройств под номером m из n БПЛА, ID_m, MK_m передаются в закрытом виде.

2. БС: Выполнение *Алгоритма 1*, N_α, T_0.

3. БС: Начальное значение при j=1 M_i="", $M_{ij} = C_{ij}, T_0, j, E(N_{\pm}, T_0, R_{ij})_{R_{ij}}$, $M_i = M_i \,||\, M_{ij}$. Обработка выполняется для всех значений i от 1 до ρ и для всех j от 1 до k_i.

4. Выполнение *Алгоритма 2.*

5. Если j=1, то БС $\leftarrow БПЛА_{ij}$: $T_i^{"} = T_{ij} \,||\, T_i$ иначе $БПЛА_{i(j-1)} \leftarrow БПЛА_{ij}$: T_i=$T_{ij} \,||\, T_i$. Обработка выполняется для всех значений i от 1 до ρ и для всех j от 1 до k_i.

6. Выполнение *Алгоритма 3*.

7. Если j=1, то $БПЛА_{ij} \leftarrow$ БС: $Q_i = Q_i / E(T, AK)_{S_{Kij}}$ иначе $БПЛА_{ij} \leftarrow БПЛА_{i(j-1)}$: $Q_i = Q_i / E(T, AK)_{S_{Kij}}$, $D(E(T, AK)_{S_{Kij}})_{S_{Kij}}$. Обработка выполняется для всех значений i от 1 до ρ и для всех j от 1 до k_i.

В основную фазу работы происходит построение матрицы с запросами – ответами по всем маршрутам, которые присутствуют в остовном дереве. На основании матрицы путей строится матрица с запросами и ответами, где каждый элемент соответственно равен аргументу и значению PUF, а на ее основе матрица сообщений. Сообщения M_i конкатенируются и отправляются нужному устройству. В процессе передачи сообщения от одного БПЛА к другому устройства по очереди вычленяют свою часть сообщения и производят процесс аутентификации. При этом в процессе аутентификации происходит формирование ответа текущего БПЛА и ожидание ответов аутентификации от остальных БПЛА пути (потомков). Обратный ответ в сторону базовой станции складывается из всех ответов БПЛА, принадлежащих одному пути.

Каждый БПЛА, выполняет после получения своей части сообщения проверку временного диапазона, расчет ответа, расшифровку зашифрованной части, сверку значений ответа и временной метки.

Если на этом этапе выявляется ошибка, то процесс аутентификации на устройстве завершается, иначе извлеченное случайное число сохраняется и генерируются собственное случайное число и новая пара запрос-ответ $(C_{ij}^{'}, R_{ij}^{'})$. Формируется сессионный ключ $S_{k_{ij}}$. После этого ответ передается родительскому узлу. При наличии дочерних узлов он дополняется ответами от этих дочерних узлов.

Сервер после получения ответа расшифровывает значения, проверяет временную метку, обновляет значения запрос-ответ и формирует сессионный ключ из полученных значений. После запускается процесс обновления пары запрос-ответ.

По завершении данного процесса устанавливается сессионный ключ для каждого БПЛА с БС. После этого формируется единый ключ аутентификации (authentication key АК), который будет использован всеми БПЛА для взаимной аутентификации. Данный ключ генерируется на основе рекомендаций по стандартизации Р 1323565.1.022–2018 [11]. Сгенерированный АК передается каждому БПЛА в зашифрованном виде, для шифрования используется сессионный ключ. Его распространение по сети БПЛА происходит в соответствии с описанным выше алгоритмом взаимодействия по островному дереву. Смена АК происходит единовременно для всех БПЛА.

Максимальное количество путей в остовном дереве с N узлами может составлять N-1. Данный факт накладывает ограничения на количество возможных и используемых соединений, то есть в сети на N элементов должно быть у каждого как минимум N соединений и граф должен быть полносвязным.

Размерность сообщения. В рамках передачи пакетов между БПЛА по принципу использования остовного дерева одним из ключевых моментов является определение нагрузки на сеть. Рассмотрим, какие объемы данных будут передаваться между узлами сети в случае использования предложенной схемы. Для этого определим размерность каждого параметра в передаваемом пакете.

Параметры R, C, N представляют собой случайные числа, каждое из которых имеет размерность 256 бит.

Параметр T является временной меткой и занимает разное количество памяти и имеет размерность 64 бит в случае представления в виде числа и 96 или 256 бит в случае представления в виде объекта внутри языка программирования. Для упрощения разбития текста на блоки при шифровании рассматривается реализация с 256-битной длиной.

Параметр номера пути является обычным целым неотрицательным числом и занимает 32 бит.

Зашифрованная часть входного сообщения, состоящая из параметров T, N и R будет занимать 768 бит или 96 байт, округление в большую сторону идет в связи с блочным алгоритмом шифрования, который принимает на вход блоки, кратные 256 битам. Часть, которая остается незашифрованной – параметры j, T, C будут занимать 352 бита – 44 байта. Итоговый размер сообщения будет суммой размера зашифрованной и незашифрованной частей и будет равен 1120 битам – 140 байт.

Выходное сообщение состоит из параметров N, T, C', R' и R, которые будут занимать 1280 бит – 160 байт.

Максимальный размер входного сообщения для пути N*1120, выходного N*1280, где N количество узлов в сети, где сеть состоит из одного пути и все узлы в него входят. Входное и выходное сообщения рассматриваются для основного этапа протокола шагов 4 и 5.

3. Эмуляция работы предложенной схемы на малых числах

Рассмотрим схему для взаимодействия 3 узлов (БПЛА) с базовой станцией. В качестве схемы расположения узлов сети рассмотрим топологию, представленную на рис. 1.

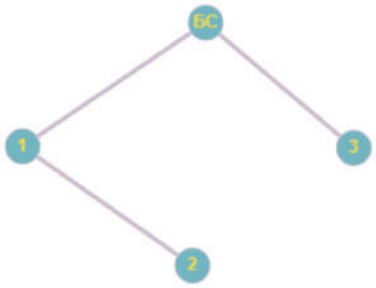

Рис. 1. Остовное дерево сети для примера

Полный процесс взаимодействия БС и БПЛА представлен на рис. 2. Рассмотрим по шагам численный пример взаимодействия БС и БПЛА.

Шаг 1. БС сохраняет ID каждого БПЛА с их мастер-ключами МК – (ID1, 70, $E(40,10)_{70}$), (ID2, 32, $E(38,26)_{32}$), (ID3, 70, $E(64,37)_{45}$), МК и ID передаются в закрытом виде.

Представим запись в базе данных базовой станции о стартовых значениях запрос-ответ для аутентификации в виде, представленном в табл. 1.

Табл. 1

Стартовые значения запрос-ответ

ID	C	R	MK
ID1	40	10	70
ID2	38	26	32
ID3	64	37	45

Шаг 2. БС выполняет *Алгоритм 1* и строит остовное дерево из всех элементов, распространяет его и генерирует значения T_0=234, $N_\alpha = 148$. Матрица путей остовного дерева:

$$\begin{matrix} 1 & 2 \\ 3 & - \end{matrix}.$$

Шаг 3. После составления матрицы путей начинается процесс аутентификации, для этого составляется матрица запросов C и матрица ответов R:

$$C=\begin{matrix} 40 & 38 \\ 64 & - \end{matrix},$$

$$R=\begin{matrix} 10 & 26 \\ 37 & - \end{matrix}.$$

Дальше строится матрица сообщений, рассылаемых по сети, выглядит она следующим образом

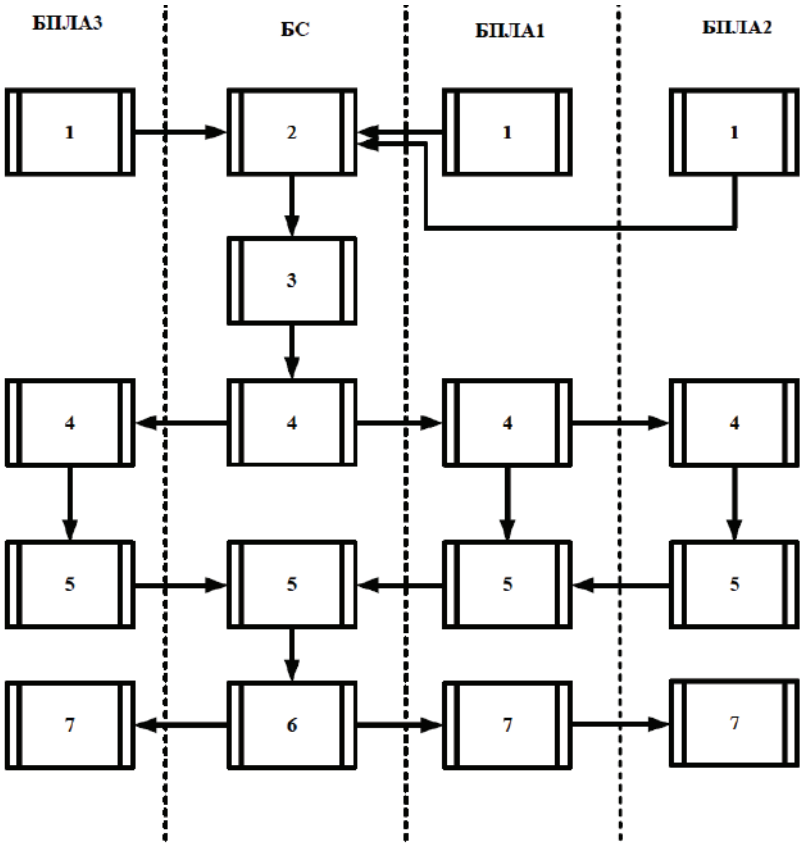

Рис. 2. Модель взаимодействия трех БПЛА и БС

$$M= \begin{matrix} 40,234,1,E(148,234,10)_{10} & 38,234,1, E(148,234,26)_{26} \\ 64,234,2, E(148,234,37)_{37} & - \end{matrix}.$$

БС генерирует для каждого пути сообщение

$$M_1 = 40,234,1,E\left(148,234,10\right)_{10} \|$$

$$\| \ 38,234,1, E\left(148,234,26\right)_{26}$$

$$M_2 = 64,234,2, E(148,234,37)_{37}$$

Шаг 4 для БПЛА1. БПЛА1 выполняет *Алгоритм 2*, получает от БС M_1 выделяет свою часть на анализ $M_{11} = 40,234,1, E\left(148,234,10\right)_{10}$ и пересылает оставшуюся часть дочернему узлу $M_{12} = 38,234,1, E\left(148,234,26\right)_{26}$.

Осуществляется проверка $t - T_0 < \Delta T$, идет расшифровка полученных данных и проверка на равенство времени и ответа устройства 234=$234^{\text{извл}}$, $10^{\text{извл}}$ = $PUF\left(40\right)$. В случае ошибки проверки процесс аутентификации для данного устройства прекращается. Устройство генерирует случайное число $N_{11} = 100$ и новые пары запрос-ответ $C_{11}{}' = 11, R_{11}{}' = 42$. Затем идет расчет значения сессионного ключа $S_{k_{11}} = 40 \oplus 148 \oplus 100 = 216$. Формируется пересылаемый дальше ответ $T_{11}{}'' = E\left(100,234,11,42,10\right)_{10}$.

Шаг 4 для БПЛА3. БПЛА3 выполняет *Алгоритм 2*, получает от БС M_2 и выделяет свою часть на анализ $M_{21} = 64,234,2, E(148,234,37)_{37}$.

Осуществляется проверка $t - T_0 < \Delta T$, идет расшифровка полученных данных и проверка на равенство времени и ответа устройства 234=$234^{\text{извл}}$, $37^{\text{извл}}$ = $PUF\left(64\right)$. В случае ошибки проверки процесс аутентификации для данного устройства прекращается. Устройство генерирует случайное число $N_{21} = 451$ и новые пары запрос-ответ $C_{21}{}' = 5, R_{21}{}' = 59$. Затем идет расчет значения сессионного ключа $S_{K_{21}} = 37 \oplus 148 \oplus 451 = 370$. Формируется пересылаемый дальше ответ $T_{21}{}'' = E\left(451,234,5,59,37\right)_{37}$.

Шаг 4 для БПЛА2. БПЛА2 выполняет *Алгоритм 2*, выделяет свою часть на анализ $M_{12} = 38,234,1, E\left(148,234,26\right)_{26}$.

Осуществляется проверка $t - T_0 < \Delta T$, идет расшифровка полученных данных, и проверка на равенство времени и ответа устройства 234=$234^{872;}$ $26^{872;}$= = $PUF\left(38\right)$. В случае ошибки проверки процесс аутентификации для данного устройства прекращается. Устройство генерирует случайное число $N_{11} = 228$

и новые пары запрос-ответ $C_{12}'=64, R_{12}'=28$. Затем идет расчет значения сессионного ключа $S_{K_{12}}=26\oplus148\oplus228=106$. Формируется пересылаемый дальше ответ $T_{12}''=E(228,234,64,28,26)_{26}$.

Шаг 5 для БПЛА2. Формируется T_1'', $T_1''=T_{12}''=E(228,234,64,28,26)_{26}$ и пересылается БПЛА1.

Шаг 5 для БПЛА3. Формируется T_2'', $T_2=T_{21}''=E(451,234,5,59,37)_{37}$ и пересылается БС.

Шаг 5 для БПЛА1. Дополняется T_1'', $T_1''=T_{11}''\,||\,T_1''=E(100,234,11,42,10)_{10}\,||E(228,234,64,28,26)_{26}$ и пересылается БС.

Шаг 6. БС выполняет *Алгоритм 3*, генерирует значение АК = 27 взаимного ключа аутентификации. Затем БС обрабатывает полученные значения из сети расшифровывает их и проверяет $t-T_0<\Delta T$, после этого вычисляет $S_{K_{11}}=216$, $S_{K_{12}}=106$, $S_{K_{21}}=370$ и сохраняет новые значения к себе в память $C_{11}'=11, R_{11}'=42$. $C_{12}'=64, R_{12}'=28, C_{21}'=5, R_{21}'=59$.

После этого БС зашифровывает t и АК на для каждого устройства на своем S_K – $Q_1=E(250,27)_{216}\,||E(250,27)_{106}$ $Q_2=E(250,27)_{370}$и пересылает их в сеть.

Шаг 7 для БПЛА1. БПЛА1 получает значение $E(250,27)_{216}||E(250,27)_{106}$и выделяет свою часть $E(250,27,)_{216}$ и пересылает $E(250,27)_{106}$ БПЛА1, расшифровывает , проверяет временную метку и получает значение АК.

Шаг 7 для БПЛА3. БПЛА3 получает значение $E(250,27)_{370}$ расшифровывает, проверяет временную метку и получает значение АК=27.

Шаг 7 для БПЛА2. БПЛА2 получает значение $E(250,27)_{106}$ расшифровывает, проверяет временную метку и получает значение АК=27.

Выводы

В данной статье обсуждались вопросы создания универсального протокола взаимной аутентификации для группы объектов с динамической топологией (например, для роя беспилотных летательных аппаратов (БПЛА)), которые совместно выполняют общее задание. Обзор аналогов показал, что существующие методы и подходы в области аутентификации объектов в сети с динамической топологией далеко не всегда могут решить поставленные задачи. Как правило, авторы сосредотачиваются на решении одной задачи: аутентификация или передача данных. При этом переконфигурация сети, добавление или исключение новых объектов в сети влекут за собой появление возможных уязвимостей и необходимость внесения изменений в используемые протоколы. Важно отметить, что все рассмотренные подходы в области протоколов аутентификации БПЛА используют импортные алгоритмы криптографии. В то время как сегодня как никогда остро стоит вопрос импортозамещения и необходимость создания протоколов, основанных на использовании отечественной криптографии.

Данное исследование было сосредоточено на разработке алгоритма взаимной аутентификации и передачи данных для групп БПЛА с учетом следующих требований. Каждый отдельный объект группы обладает ограниченным запасом энергии. Объект может выключаться из сети, а затем заново подключаться к ней, поэтому протокол должен предусматривать способ повторной взаимной аутентификации объектов группы. Объекты должны иметь возможность передавать данные на управляющий узел, который называется базовая станция (БС). При проектировании протокола важно учесть, что риски вскрытия переданной информации должны быть минимизированы в случае, если злоумышленник получит физический доступ к памяти объекта группы.

В результате проделанной работы был проведен анализ существующих зарубежных протоколов аутентификации БПЛА, были выделены их преимущества, недостатки и необходимые функциональные компоненты. После анализа существующих протоколов был разработан протокол аутентификации для роя БПЛА, ориентированный на использование отечественных стандартов шифрования и генерации псевдослучайных чисел. Разработанный протокол позволяет аутентифицировать БПЛА и БС, после чего БПЛА могут производить взаимную аутентификацию.

Практическое подтверждение/достоверность предлагаемых научных решений подтверждается экспериментальными подтверждения на основе программных реализаций разработанных протоколов с использованием языка программирования C++.

Научная новизна данного исследования прежде всего состоит в том, что впервые разработан протокол, комплексно решающий вопрос взаимной аутентификации и передачи данных для динамической структуры сети, в которой не только изменяется конфигурация сети, но также меняется количество активных участников сети. Несомненным достоинством разработанного протокола является его ориентированность на использование отечественных алгоритмов шифрования.

Работа выполнена при поддержке гранта Российского научного фонда No 22-11-00184, https://rscf.ru/project/22-11-00184/

Литература

1. Diwankshi Sharma, Aabid Rashid, Sumeet Gupta, Sachin Kr. Gupta A Functional Encryption Technique in UAV Integrated HetNet: A Proposed Model // International Journal of Simulation: Systems, Science & Technology. March 2019. DOI 10.5013/IJSSST.a.20.S1.07.-7.1-7.7 https://ijssst.info/Vol-20/No-S1/paper7.pdf
2. G. Choudhary, V. Sharma, I. You, K. Yim, I.-R. Chen, and J.-H. Cho, “Intrusion Detection Systems for Networked Unmanned Aerial Vehicles: A Survey,” 14th IEEE International Wireless Communications & Mobile Computing Conference, Limassol, Cyprus, pp. 560-565, June 2018.
3. Aabid Rashid, Diwankshi Sharma, Tufail A. Lone, Sumeet Gupta, Sachin Kr. Gupta Identity-Based Encryption in UAV Assisted HetNets: A Survey. 10th ICCCNT 2019 July 6-8, 2019, IIT – Kanpur Kanpur, India-IEEE – 45670.
4. Ashutosh Singandhupe, Hung Manh La, David Feil-Seifer Reliable Security Algorithm for Drones Using Individual Characteristics From an EEG Signal. DOI 10.1109/ACCESS.2018.2827362, IEEE Access April 2018.
5. Guang Yang, Ming Xiao, Muhammad Alam, Yongming Huang “Low-Latency Heterogeneous Networks Millimeter-Wave Communications,” IEEE Communication Magazine, Vol.56, pp. 124-129, January 2018. doi:10.1109/MCOM.2018.1700874
6. Z. Ali, S. A. Chaudhry, M. S. Ramzan, And F. Al-Turjman, ”Securing Smart City Surveillance: A Lightweight Authentication Mechanism for Unmanned Vehicles”, Human-driven Edge Computing (HEC) , IEEE Access, Volume: 8, pp 43711 — 43724, 2020.
7. Sana Benzarti, Bayrem Triki, and Ouajdi Korbaa Drone authentication using ID-Based Signcryption in LoRaWAN network.- December 2019.- Conference: International Conference on Intelligent Systems Design and Applications (ISDA)At: South Africa, PretoriaVolume: https://link.springer.com/chapter/10.1007/978-3-030-49342-4_20
8. Sana Benzarti, Bayrem Triki, and Ouajdi Korbaa Drone partial temporary authentication in Journal of Information Assurance and Security. ISSN 1554-1010 Volume 15 (2020) pp. 126-135.
9. Chen, L.; Qian, S.; Lim, M.; Wang, S. An enhanced direct anonymous attestation scheme with mutual authentication for network-connected UAV communication systems. China Commun. 2018, 15, 61–76.
10. Chin-Ling Chen, Yong-Yuan Deng, Wei Weng, Chi-Hua Chen, Yi-Jui Chiu and Chih-Ming Wu A Traceable and Privacy-Preserving Authentication for UAV Communication Control System.- Received: 15 November 2019; Accepted: 20 December 2019; Published: 1 January 2020.-Electronics 2020, 9, 62; doi:10.3390/electronics9010062
11. García-Magariño, I.; Lacuesta, R.; Rajarajan, M.; Lloret, J. Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain. Ad Hoc Netw. 2019, 86, 72–82.
12. Gemalto, Actility AND Semtech, ”LoRaWA SECURITY A WHITE PAPER PREPARED FOR THE LoRa ALLIANCE”, [Online]. Available: https://loraalliance.org/sites/default/files/2018- 04/lora alliance security whitepaper.pdf, (2019, Ferbruary).
13. I. Praveen, M. Sethumadhavan, ”Partial Password Authentication using Vector Decomposition”, International Journal of Pure and Applied Mathematics, volume 118, Number 7 Special Issue, pp. 381-385, 2018.
14. J. Srinivas, A. K. Das, N. Kumar, and J.J. P. C.Rodrigues, ”TCALAS: Temporal Credential Based Anonymous Lightweight Authentication Scheme for Internet of Drones Environment”, IEEE Transactions on Vehicular Technology, Volume: 68 , Issue: 7, pp. 6903 — 6916, July 2019.
15. A Lightweight Authentication Protocol for UAV Networks Based on Security and Computational Resource Optimization / Yuan Lei, Lining Zeng, Yan-Xing Li et al.
16. Amassing the Security: An Enhanced Authentication Protocol for Drone Communications over 5G Networks / Tsuyang Wu, Xinglan Guo, Yehcheng Chen, Saru Kumari and Chienming Chen // Drones 2022– 6.– 10.
17. Gaurang Bansal, S-MAPS: Scalable Mutual Authentication Protocol for Dynamic UAV Swarms / Gaurang Bansal, Biplab Sikdar.
18. Способ построения системы опознавания свой-чужой на основе протокола с нулевым разглашением / Калмыков И. А., Саркисов А. Б., Калмыков М. И. и др. // https://patents.google.com/patent/RU2570700C1/ru
19. Борисов К.В., Любушкина И.Е., Панасенко С.П. и др. Способ, система и устройство криптографической защиты каналов связи беспилотных авиационных комплексов // Патент №2704268, опубликован 25.10.2019 — https://i.moscow/patents/ru2704268c1_20191025

PROTOCOL FOR MUTUAL AUTHENTICATION OF AN OBJECT'S GROUP WITH DYNAMIC TOPOLOGY

Basan A.S.[5], Basan E.S.[6], Ishchukova E.A.[7], Kornilov A.P.[8]

Purpose: *The aim of the work is to develop a mutual authentication protocol for a group of objects with a dynamic topology (for example, for a swarm of unmanned aerial vehicles (UAVs)), which jointly perform a common task. It is important to take into account that each individual object of the group has a limited energy reserve. It is necessary to take into account the fact that an object can be disconnected from the network and then reconnected to it, so the protocol must provide a way to re-authenticate the objects of the group mutually. Also, objects must be able to transmit data to the control node, which is called the base station (BS). When designing a protocol, it is important to take into account that the risks of opening the transmitted information should be minimized if an attacker gains physical access to the group object's memory.*

Method: *The method is based on the use of the mathematical apparatus of probability theory, mathematical statistics, information theory, cryptography. As cryptographic primitives, a pseudo-random sequence generator, hash functions, symmetric encryption, and a physically non-cloneable function are used.*

Results: *The analysis of existing approaches to mutual authentication and data transfer in a group of objects with dynamic topology is carried out. A UAV mutual authentication protocol is proposed, which solves a number of important tasks, such as: dynamic change of the encryption key, absence of highly loaded calculations for dynamic network elements, scalability, and the possibility of data exchange between network participants. The developed protocol is based on the use of several basic algorithms: an algorithm for constructing a spanning tree, an algorithm for performing UAV mutual authentication and organizing data transfer, and an algorithm for performing UAV authentication in front of the BS. A simulation example is provided to illustrate the developed solution with dedicated phases and analyze the transmission of messages in it within two UAVs.*

The scientific novelty *primarily lies in the fact that in the developed authentication protocol, special attention is paid to the problem of stability of the authentication scheme and reconfiguration of the UAV network, and also takes into account the problem of low computing power, most of the highly loaded calculations that occupy the processor are transferred to the BS — the most powerful computing element of the network . The above solution ensures the change of the session key with the presence of a minimum of pre-established information and the constant updating of the key between network elements.*

Keywords: *unmanned aerial vehicle, base station, authentication, cryptography, encryption, pseudo-random number, spanning tree, network, hash function, timestamp, request, response, scalability, fault tolerance.*

References

1. Diwankshi Sharma, Aabid Rashid, Sumeet Gupta, Sachin Kr. Gupta A Functional Encryption Technique in UAV Integrated HetNet: A Proposed Model // International Journal of Simulation: Systems, Science & Technology. March 2019. DOI 10.5013/IJSSST.a.20.S1.07.-7.1-7.7 https://ijssst.info/Vol-20/No-S1/paper7.pdf
2. G. Choudhary, V. Sharma, I. You, K. Yim, I.-R. Chen, and J.-H. Cho, "Intrusion Detection Systems for Networked Unmanned Aerial Vehicles: A Survey," 14th IEEE International Wireless Communications & Mobile Computing Conference, Limassol, Cyprus, pp. 560-565, June 2018.

5 Alexandr S. Basan, Ph.D. (of Tech.), Associate Professor of the Department of Information Technology Security, Institute of Computer Technologies and Information Security, Southern Federal University "SFedU", Taganrog, Russia. E-mail: asbasan@sfedu.ru.

6 Elena S. Basan, Ph.D. (of Tech.), Associate Professor of the Department of Information Technology Security, Institute of Computer Technologies and Information Security, Southern Federal University "SFedU", Taganrog, Russia. E-mail: ebasan@sfedu.ru, ORCID 0000-0001-6127-4484.

7 Evgeniya A. Ishchukova, Ph.D. (of Tech.), Associate Professor of the Department of Information Technology Security, Institute of Computer Technologies and Information Security, Southern Federal University «SFedU», Taganrog, Russia. E-mail: uaishukova@sfedu.ru , ORCID 0000-0002-6818-1608.

8 Alexandr P. Kornilov, student of the Department of Information Technology Security, Institute of Computer Technologies and Information Security, Southern Federal University «SFedU», Taganrog, Russia. E-mail: akornilov @sfedu.ru.

3. Aabid Rashid, Diwankshi Sharma, Tufail A. Lone, Sumeet Gupta, Sachin Kr. Gupta Identity-Based Encryption in UAV Assisted HetNets: A Survey. 10th ICCCNT 2019 July 6-8, 2019, IIT – Kanpur Kanpur, India-IEEE – 45670.
4. Ashutosh Singandhupe, Hung Manh La, David Feil-Seifer Reliable Security Algorithm for Drones Using Individual Characteristics From an EEG Signal. DOI 10.1109/ACCESS.2018.2827362, IEEE Access April 2018.
5. Guang Yang, Ming Xiao, Muhammad Alam, Yongming Huang "Low-Latency Heterogeneous Networks Millimeter-Wave Communications," IEEE Communication Magazine, Vol.56, pp. 124-129, January 2018. doi:10.1109/MCOM.2018.1700874
6. Z. Ali, S. A. Chaudhry, M. S. Ramzan, And F. Al-Turjman, "Securing Smart City Surveillance: A Lightweight Authentication Mechanism for Unmanned Vehicles", Human-driven Edge Computing (HEC), IEEE Access, Volume: 8, pp 43711 — 43724, 2020.
7. Sana Benzarti, Bayrem Triki, and Ouajdi Korbaa Drone authentication using ID-Based Signcryption in LoRaWAN network.- December 2019.- Conference: International Conference on Intelligent Systems Design and Applications (ISDA)At: South Africa, PretoriaVolume: https://link.springer.com/chapter/10.1007/978-3-030-49342-4_20
8. Sana Benzarti, Bayrem Triki, and Ouajdi Korbaa Drone partial temporary authentication in Journal of Information Assurance and Security. ISSN 1554-1010 Volume 15 (2020) pp. 126-135.
9. Chen, L.; Qian, S.; Lim, M.; Wang, S. An enhanced direct anonymous attestation scheme with mutual authentication for network-connected UAV communication systems. China Commun. 2018, 15, 61–76.
10. Chin-Ling Chen, Yong-Yuan Deng, Wei Weng, Chi-Hua Chen, Yi-Jui Chiu and Chih-Ming Wu A Traceable and Privacy-Preserving Authentication for UAV Communication Control System.- Received: 15 November 2019; Accepted: 20 December 2019; Published: 1 January 2020.-Electronics 2020, 9, 62; doi:10.3390/electronics9010062
11. García-Magariño, I.; Lacuesta, R.; Rajarajan, M.; Lloret, J. Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain. Ad Hoc Netw. 2019, 86, 72–82.
12. Gemalto, Actility AND Semtech, "LoRaWA SECURITY A WHITE PAPER PREPARED FOR THE LoRa ALLIANCE", [Online]. Available: https://loraalliance.org/sites/default/files/2018- 04/lora alliance security whitepaper.pdf, (2019, Ferbruary).
13. I. Praveen, M. Sethumadhavan, "Partial Password Authentication using Vector Decomposition", International Journal of Pure and Applied Mathematics, volume 118, Number 7 Special Issue, pp. 381-385, 2018.
14. J. Srinivas, A. K. Das, N. Kumar, and J.J. P. C.Rodrigues, "TCALAS: Temporal Credential Based Anonymous Lightweight Authentication Scheme for Internet of Drones Environment", IEEE Transactions on Vehicular Technology, Volume: 68 , Issue: 7, pp. 6903 — 6916, July 2019.
15. A Lightweight Authentication Protocol for UAV Networks Based on Security and Computational Resource Optimization / Yuan Lei, Lining Zeng, Yan-Xing Li et al.
16. Amassing the Security: An Enhanced Authentication Protocol for Drone Communications over 5G Networks / Tsuyang Wu, Xinglan Guo, Yehcheng Chen, Saru Kumari and Chienming Chen // Drones 2022– 6.– 10.
17. Gaurang Bansal, S-MAPS: Scalable Mutual Authentication Protocol for Dynamic UAV Swarms / Gaurang Bansal, Biplab Sikdar.
18. Sposob postroenija sistemy opoznavanija svoj-chuzhoj na osnove protokola s nulevym razglasheniem / Kalmykov I. A., Sarkisov A. B., Kalmykov M. I. i dr. // https://patents.google.com/patent/RU2570700C1/ru
19. Borisov K.V., Ljubushkina I.E., Panasenko S.P. i dr. Sposob, sistema i ustrojstvo kriptograficheskoj zashhity kanalov svjazi bespilotnyh aviacionnyh kompleksov // Patent №2704268, opublikovan 25.10.2019 — https://i.moscow/patents/ru2704268c1_20191025