УДК: 004.056 DOI: 10.53816/23061456_2021_11–12_65

СПОСОБ ДЕЦЕНТРАЛИЗОВАННОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕВОЙ ИНФОРМАЦИИ В ГРУППАХ РОБОТОТЕХНИЧЕСКИХ КОМПЛЕКСОВ ВОЕННОГО НАЗНАЧЕНИЯ

METHOD FOR DECENTRALIZED DISTRIBUTION OF KEY INFORMATION IN GROUPS OF MILITARY ROBOTIC SYSTEMS

А.В. Решотка, Н.И. Елисеев, А.Д. Ваничкин

A.V. Reshotka, N.I. Eliseev, A.D. Vanichkin

КВВУ им. С.М. Штеменко

Переход от одиночного применения робототехнических комплексов военного назначения (РТК ВН) к групповому порождает ряд проблем, таких как необходимость одновременного управления отдельными объектами и группой в целом, а также обеспечение взаимодействия между группами. Это, в свою очередь, повышает уровень требований к информационной безопасности связи между узлами сети. Необходимо чтобы каждый узел проходил авторизацию при добавлении в сеть, а сеть обеспечивала прямую и обратную секретность. Кроме того, повышение сложности применяемых алгоритмов защиты и организации сети не должно вызывать инерционности управления объектами. Для решения перечисленных проблем в работе рассматривается разработанный способ распределения ключевой информации, применимый для групп РТК ВН.
Ключевые слова: распределение ключевой информации, угрозы безопасности информации, робототехнический комплекс, группа РТК ВН.

The transition from a single use of robotic sistem for military purposes to a group one gives rise to a number of problems, such as the need for simultaneous control of individual objects and the group as a whole, as well as ensuring interaction between groups. This, in turn, raises the level of requirements for information security of communication between network nodes. It is required that each node is authorized when added to the network, and the network provides forward and backward secrecy. In addition, an increase in the complexity of the applied algorithms for protection and network organization should not cause inertia in object management. To solve the listed problems, the work considers the developed method for the distribution of key information applicable to the groups of robotic sistem for military purposes.
Keywords: distribution of key information, threats to information security, robotic complex, robotic sistem for military purposes group.

В группе РТК ВН взаимодействие между узлами сети осуществляется с помощью беспроводных каналов связи, что является одним из наиболее уязвимых мест системы, следовательно, необходимо применение шифрования и обеспечение высокой криптостойкости и имитостойкости. Помимо всего остаются вопросы о скрытых и помехозащищенных режимах работы [1–5].

Для решения представленных проблем предлагается применение децентрализованного распределения ключевой информации. Способы распределения ключевой информации представляют собой условные последовательности действий участников связи по созданию защищенного канала, путем формирования общего ключа шифрования с учетом требуемого уровня идентификации РТК ВН в сети, что достигается доверенной аутентификацией [6, 11–13].

В описываемом способе распределения ключевой информации, иерархия отдельных узлов сети имеет следующий вид. Все участники общей группы делятся на некоторое число отдельных подгрупп в зависимости от общего количества участников и их распределения в пространстве. Каждая подгруппа управляется контроллером подгруппы (КП). Совокупность всех участников и КП формируют группу участников и контроллеров (ГУК). Совокупность всех КП формирует группу контроллеров подгрупп (ГКП).

На всех КП находится система «создания группы» (СГ). Система СГ отвечает за:

1) распространение сертификатов среди всех участников взаимодействующих с данным КП;

2) настройку групповых политик и выбор параметров шифрования;

3) объявление о групповом шировещательном сеансе с помощью протоколов объявления и описания сеансов;

4) доступность сервисов;

5) идентификацию, аутентификацию и авторизацию участников сети.

Структура заявленного способа представлена на рис. 1.

Изменение количества участников в подгруппе.

При изменении количества участников в подгруппе сети, происходит следующий порядок действий. КП генерирует новый групповой ключ, шифрует его ГУК ключом и отправляет его другим КП для согласования. ГУК ключ защищает связь в группе ГКП и используется всеми КП в сеансе. ГУК ключ действителен в течение короткого периода времени, называемого временем жизни (life time — L). КП генерирует новый ключ подгруппы и ГУК ключ.

После согласования нового группового ключа, этот ключ зашифровывается новым ключом подгруппы и КП отправляет его всем участникам подгруппы. Ключ подгруппы защищает групповой ключ. Каждая подгруппа имеет собственный ключ подгруппы. Для того чтобы участники подгруппы смогли расшифровать полученное сообщение, они должны узнать новый ключ подгруппы. Алгоритм действий при изменении количества участников представлен на рис. 2.

Для получения нового ключа подгруппы применяется атрибутное шифрование с правилом доступа на основе шифротекста (далее — CP-ABE). КП формирует сообщение для участников подгруппы. Это сообщение представляет собой зашифрованный закрытым ключом на основе атрибутов ключ подгруппы. Информация, зашифрованная в сообщении, описывается набором атрибутов, а правило доступа к данным содержится в самих шифрованных данных (шифротексте). Секретный ключ участника в то же время соответствует собственному набору атрибутов участника. Участник может расшифровать

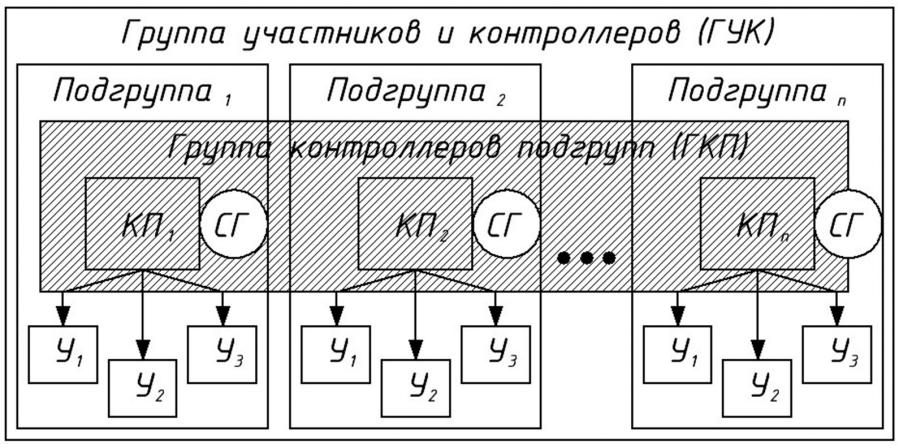

Рис. 1. Структура заявленного способа

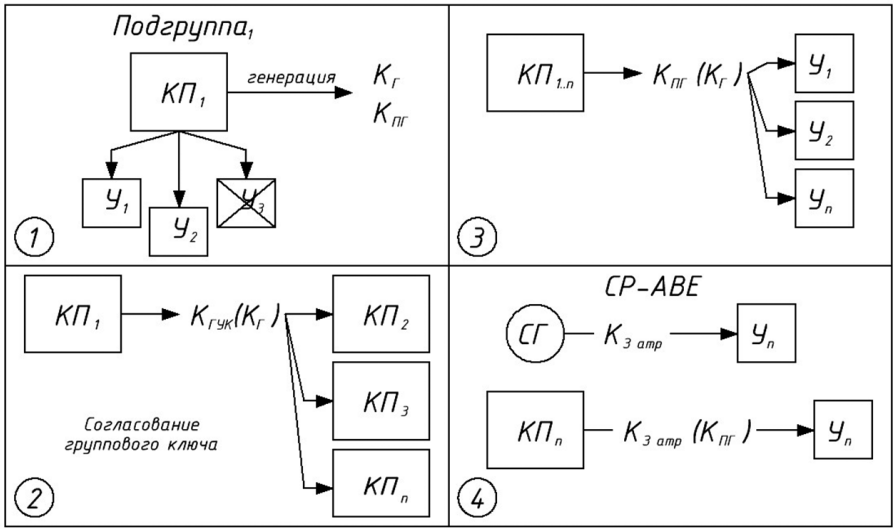

Рис. 2. Алгоритм действий при изменении количества участников подгруппы

данные при помощи своего закрытого ключа, полученного от (СГ) доверенного центра. В роли доверенного центра, в этом способе выступает система «создания группы».

Расшифровав сообщение закрытым ключом, участник получает ключ подгруппы. Ключом подгруппы участник расшифровывает ключ группы. Получив ключ группы, участники могут принимать и отсылать данные с остальными узлами сети по защищенному каналу.

Изменение количества участников в группе ГКП.

Во время работы сети возможны ситуации, при которых КП оказывается отключенным. Причиной отключения КП может стать частичное или полное уничтожение условного объекта, выполняющего роль КП. Участники, связанные с отключенным КП, могут присоединиться к ближайшим КП выполнив действия, предписанные протоколом расширенного поискового кольца. КП в группе ГКП выявив изменение членства группы, создают и распространяют новый групповой и ГУК ключ.

При добавлении нового КП в сеть, присоединяющийся КП запрашивает текущие ГУК ключ и групповой ключ у других КП. Новый КП отправляет запрос на добавление в ГКП вместе со своим сертификатом. КП уже состоящий в ГКП, отправляет новому КП групповой ключ, зашифрованный ключом ГУК и ГУК ключ, зашифрованный закрытым ключом на основе атрибутов. Новый КП может расшифровать данные при помощи собственного закрытого ключа, основанного на атрибутах, который он получает от доверенного центра (СГ). Алгоритм действий при изменении количества КП представлен на рис. 3.

Время жизни ГУК ключа определяется параметром life time. Когда приходит время менять ключ, один из КП много адресно рассылает сообщение с новым групповым и ГУК ключом, зашифрованным закрытым ключом атрибутов, всем остальным участникам ГКП.

Аутентификация.

Описываемый способ распределения использует уникальную инфраструктуру проверки открытых ключей (PKI) для аутентификации всех сторон в системе. Корневым центром сертификации является система СГ. «Сертификат системы СГ является корнем иерархии. Система СГ поддерживает три сертификата. Первый из них используется для идентификации КП для системы СГ, называется сертификат контроллеров подгруппы. Второй — авторизация сеанса — используется для идентификации КП для других КП и участников группы. Третий — содержит сертификаты участников, используются для аутентификации участников в КП и авторизации их для участия в безопасной группе» [7–8].

На рис. 4 показана взаимосвязь протоколов, из которых состоит способ распределения ключей. Система СГ объявляет о начале группового сеанса посредством протоколов объявления (SAP) и описания сеанса (SDP). КП слушает адрес SAP для объявления новой подгруппы. Когда объяв-

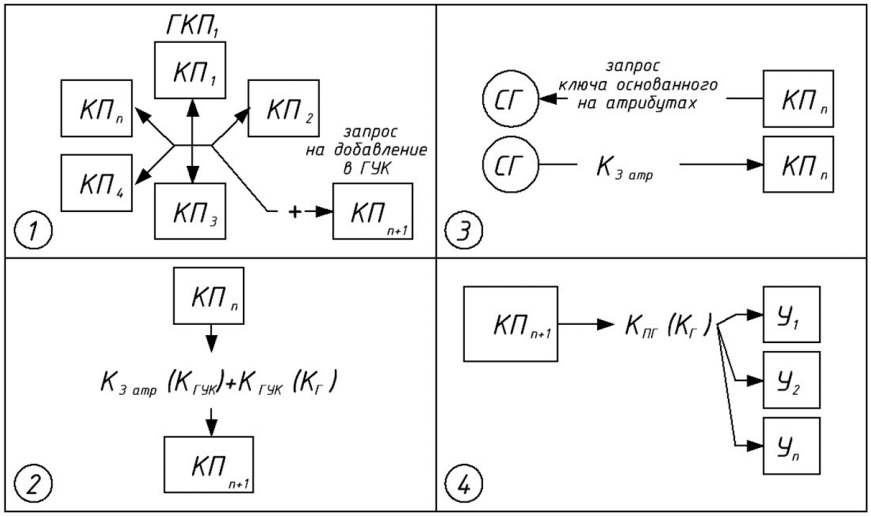

Рис. 3. Алгоритм действий при изменении количества КП в ГКП

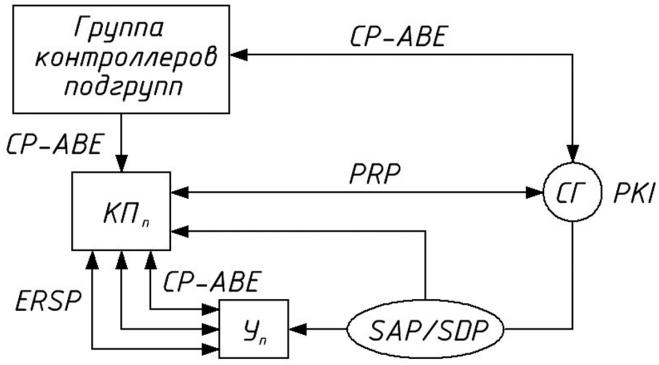

Рис. 4. Взаимосвязь протоколов в способе распределения ключей

ляется новая подгруппа, КП запрашивает разрешение на управление этой подгруппой у СГ, используя протокол запроса разрешений (PRP).

Участники сети постоянно слушают адрес SAP и, когда сеанс им интересен, они связываются с ближайшим КП для предоставления им группового ключа. Участники сети используют протокол Expand searching Ring Protocol (ERSP) для поиска КП.

CP-ABE.

Атрибутное шифрование с правилом доступа на основе шифротекста (CP-ABE) [9–10] применяется в данном способе для распространения ГУК ключа в группе ГКП и распространения ключа подгруппы в подгруппе.

Для хранения атрибутов используется метод плоской таблицы. В данном методе каждому участнику присваивается уникальный идентификатор и набор атрибутов. Пример 3-х битного ID и его набора атрибутов приведен далее. Пусть A1, A2, A3, B1, B2, B3 — это шесть атрибутов, определенных в системе. На рис. 5 представлена таблица для этого случая.

Идентификатор формируется в зависимости от атрибутов. Если участнику соответствует атрибут из набора A, то битовое значение равно 0, а если из набора B, то единица. Таким образом, участник с битом ID 001 имеет атрибуты A1, A2 и B3. Когда участник подгруппы выходит из неё, необходимо обновить ключ группы, ключ подгруппы и закрытый ключ на основе атрибутов всех текущих пользователей. Для этого необходим обратный битовый идентификатор (побитовое НЕ) покидающего участника. Новое правило доступа к данным будет иметь вид: B1^B2^A3. То есть доступ к данным будет только у тех пользователей, которым соответствует как минимум один атрибут из обратного идентификатора уходящего участника. Доступ к данным будет закрыт для участника с идентификатором: 001.

Значение	1-й бит	2-й бит	3-й бит
0	A1	A2	A3
1	B1	B2	B3

ID Бит	Атрибут
000	A1 A2 A3
001	A1 A2 B3
010	A1 B2 A3
011	A1 B2 B3
100	B1 A2 A3
101	B1 A2 B3
110	B1 B2 A3
111	B1 B2 B3

Рис. 5. Плоская таблица для восьми участников

Для количества участников n, потребуется всего лишь $2\log(n)$ атрибутов, то есть для 1024 участников необходимо 20 атрибутов.

Вывод

Благодаря использованию атрибутного шифрования и регулярному обновлению ключей, описанный способ распределения ключевой информации обладает прямой и обратной секретностью. Метод плоской таблицы позволяет сократить необходимый объём памяти, что позволяет использовать данный способ на платформах с низкими вычислительными способностями. Кроме этого, атрибутное шифрование позволяет избавится от сертификации открытых ключей на некоторых этапах работы способа распределения ключей.

Литература

1. Буренок В.М., Ивлев А.А., Корчак В.Ю. Развитие военных технологий XXI века: проблемы планирование, реализация. — Тверь: Издательство ООО «КУПОЛ». 2009. 624 с.

2. Басан А.С., Басан Е.С., Макаревич О.Б. Анализ и разработка средств обеспечения безопасности для систем группового управления автономными мобильными роботами // Вопросы кибербезопасности. № 5 (24). 2017. С. 42–49.

3. Помазуев О.Н. Основные направления деятельности по совершенствованию работы в области роботизации Вооруженных Сил Российской Федерации // II Военно-научная конференция «Роботизация Вооруженных Сил Российской Федерации». — М.: сборник трудов — М.: ГНИИ ЦР МО РФ. 2017. С. 12–17.

4. Ермолов И.Л. Актуальные вопросы группового применения РТК ВН // II Военно-научная конференция «Роботизация Вооруженный Сил Российской Федерации»: сборник трудов. — М.: ГНИИ ЦР МО РФ. 2017. С. 44–49.

5. Хрипунов С.П., Благодарящев И.В. Групповое применение робототехнических комплексов военного назначения: проблемы и пути решения // II Военно-научная конференция «Роботизация Вооруженный Сил Российской Федерации»: сборник трудов. — М.: ГНИИ ЦР МО РФ. 2017. С. 534–536.

6. Гудков М.А., Дворников А.С., Сорокин К.Н. Применение когнитивных радиосистем для обеспечения связи с роботизированными платформами военного назначения // II Военно-научная конференция «Роботизация Вооруженный Сил Российской Федерации»: сборник трудов. — М.: ГНИИ ЦР МО РФ. 2017. С. 440–444.

7. Патент РФ № 2019117686, 06.03.2020. Решотка А.В., Чижиков В.И., Сабин В.О. Способ децентрализованного распределения ключевой информации // Патент России № 2716207 C1. 2020. Бюл. № 33.

8. НИР (шифр «Облик-РТК»). Отчет о выполнении этапа НИР (промежуточное). — Краснодар: КВВУ. 2015. 271 с. Инв. № Н258.

9. Душкин А.В. Анализ шифрования данных в информационной системе с использованием схемы Ciphtertext policy attribute-based encryption / А.В. Душкин, Ю.В. Щербакова. Воронежский институт ФСИН России // Вестник Воронежского института ФСИН России. — Воронеж. 2014. С. 24–27.

10. Душкин А.В. Анализ подходов применения схемы шифрования данных CB-ABE для облачных технологий / А.В. Душкин, Ю.В. Щербакова, Т.С. Буряк. НАУКА И АСУ 2014 // Наукоемкие технологии в космических исследованиях земли. Выпуск 4. 2014. С. 64–67.

11. Макаренко С.И. Робототехнические комплексы военного назначения — современное состояние и перспективы развития // Системы управления, связи и безопасности. 2016. № 2. С. 73–122.

12. Русинов В. Состояние и планы развития наземных робототехнических комплексов США [Электронный ресурс] // Зарубежное военное обозрение: информационно-аналитический иллюстрированный журнал Министерства обороны России. 2013. № 3. С. 44–56.

13. Кравченко А.Ю. Проблемы и перспективы создания робототехнических комплексов военного назначения / А.Ю. Кравченко, Ю.Е. Стукало (ФГКУ «46 ЦНИИ» Минобороны России, г. Москва) // «Перспективные системы и задачи управления»: сб. материалов восьмой всероссийской научно-практической конф. — Таганрог: Изд-во ТТИ ЮФУ. 2013. С. 22–28.

References

1. Burenok V.M., Ivlev A.A., Korchak V.U. Development of military technologies of the XXI century: problems of planning, implementation. — Tver: Publishing house of OOO KUPOL. 2009. 624 p.

2. Basan A.S., Basan E.S., Makarevich O.B. Analysis and development of security tools for group control systems for autonomous mobile robots // Cybersecurity. Issues № 5 (24). 2017. P. 42–49.

3. Pomazuev O.N. The main directions of activities to improve work in the field of robotization of the Armed Forces of the Russian Federation // II Military Scientific Conference «Robotization of the Armed Forces of the Russian Federation». 2017. P. 12–17.

4. Ermolov I.L. Topical issues of group application of RTK VN // II Military scientific conference «Robotization of the Armed Forces of the Russian Federation»: collection of works. — M.: GNII TsR Ministry of Defense of the Russian Federation. 2017. P. 44–49.

5. Khripunov S.P., Blagodashchev I.V. Group application of military-purpose robotic systems: problems and solutions // II Military scientific conference «Robotization of the Armed Forces of the Russian Federation»: collection of works. — M.: GNII CR Ministry of Defense of the Russian Federation. 2017. P. 534–536.

6. Gudkov M.A., Dvornikov A.S., Sorokin K.N. Application of cognitive radio systems to provide communication with robotic platforms for military purposes // II Military scientific conference «Robotization of the Armed Forces of the Russian Federation»: collection of works. — M.: GNII TsR MO RF. 2017. P. 440–444.

7. RF patent № 2019117686, 06.03.2020. Reshotka A.V., Chizhikov V.I., Sabin V.O. A way of decentralized distribution of key information // Patent of Russia № 2716207 C1. 2020. Bul. № 33.

8. Research work (code «Oblik-RTK») Report on the implementation of the research stage (intermediate). — Krasnodar: KVVU. 2015. 271 p. Inv. № H258.

9. Dushkin A.V. Analysis of data encryption in an information system using the Ciphtertext policy attribute-based encryption scheme / A.V. Dushkin, Yu.V. Shcherbakova. Voronezh Institute of the Federal Penitentiary Service of Russia // Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia. — Voronezh. 2014. P. 24–27.

10. Dushkin A.V. Analysis of approaches to the application of the CB-ABE data encryption scheme for cloud technologies / A.V. Dushkin, Yu.V. Shcherbakova, T.S. Buryak, SCIENCE AND ACS 2014 // Science-Intensive Technologies in Space Research of the Earth. Issue 4. 2014. P. 64–67.

11. Makarenko S.I. Robotic complexes for military purposes - the current state and development prospects // Control systems, communications and security. 2016. № 2. P. 73–122.

12. Rusinov V. State and development plans of ground-based robotic systems in the United States [Electronic resource] // Foreign military review: information-analytical illustrated magazine of the Ministry of Defense of Russia. 2013. № 3. P. 44–56.

13. Kravchenko A.Yu. Problems and prospects of creating robotic military complexes / A.Yu. Kravchenko, Yu.E. Stukalo (FGKU «46 Central Research Institute» of the Ministry of Defense of Russia, Moscow) // «Perspective systems and management tasks»: collection of articles. materials of the eighth all-Russian scientific and practical conference. — Taganrog: Publishing house of TTI SFU. 2013. P. 22–28.