УДК 004.052

РАЗРАБОТКА ОТКАЗОУСТОЙЧИВОЙ ЗАПРОСНО-ОТВЕТНОЙ СИСТЕМЫ АУТЕНТИФИКАЦИИ СПУТНИКА, ФУНКЦИОНИРУЮЩЕЙ В МОДУЛЯРНЫХ КОДАХ

Калмыков М.И., Зеленский М.Д., Денисенко В.В., Калмыков И.А., Алиев Г.С., Ефременков И.Д.

ФГАОУ ВО «Северо-Кавказский федеральный университет», Ставрополь, e-mail: kia762@yandex.ru

Для обеспечения эффективной работы системы мониторинга, контроля и управления удаленными экологически опасными объектами в настоящее время широко используются системы спутниковой связи. Введение в состав абонентского терминала управления удаленным объектом запросно-ответной системы опознавания спутника позволит программно-аппаратному комплексу перед организацией информационного обмена произвести определение статуса космического аппарата, который находится в зоне видимости. В этом случае использование системы определения «свой-чужой» позволит снизить вероятность отказов и сбоев в процессе функционирования оборудования экологически опасных технологий из-за навязывания ложных управляющих команд, поступающих от чужих космических аппаратов. Однако в процессе работы такой системы могут возникнуть сбои и отказы, что приводит к появлению ошибок в проводимых вычислениях. Устранить данный недостаток можно за счет обеспечения отказоустойчивости запросно-ответной системы на основе использования корректирующих модулярных кодов.

Ключевые слова: система опознавания «свой-чужой», протокол доказательства с нулевым разглашением, отказоустойчивость, корректирующие модулярные коды

DEVELOPMENT OF FAULT-TOLERANT REQUEST-RESPONSE AUTHENTICATION SYSTEM OF THE SATELLITE, OPERATING IN MODULAR CODES

Kalmykov M.I., Zelenskiy M.D., Denisenko V.V., Kalmykov I.A., Aliev G.S., Efremenkov I.D.

North-Caucasus Federal University, Stavropol, e-mail: kia762@yandex.ru

To ensure effective monitoring, control and management of remote ecologically dangerous objects currently widely used satellite communications system. The introduction of the subscriber terminal to control a remote object's request-response identification system of the satellite will allow appliance to the organization of information exchange to make a determination of the status of the spacecraft, which is in sight. In this case, the use of the definition of «friend or foe» will reduce the probability of faults and failures in the operation of the equipment environmentally-dangerous technologies due to the imposition of false control commands received from foreign space vehicles. However, in the process of work of such system failures could occur and failures, which leads to errors in the calculations. To eliminate this disadvantage by providing a failover request-response system based on the use of corrective modular codes.

Keywords: system identification «friend or foe», the report of the proof with zero disclosure, fault-tolerance, the corrective modular codes

Использование системы опознавания «свой-чужой» в низкоорбитальных системах спутниковой связи (ССС) позволяет повысить информационную скрытность данной системы связи. Применение протокола типа «запрос-ответ», основанного на доказательстве с нулевым разглашением данных, позволяет однозначно аутентифицировать космический аппарат (КА). При этом для обеспечения требуемого уровня криптозащиты в данной системе будет использоваться достаточно большой модуль p, который применяется в процессе вычислений. Такая одномодульная структура характеризуется значительными схемными затратами, что приводит к увеличению вероятности возникновения сбоев и отказов в работе системы.

Поэтому придание запросно-ответной системе, используемой для аутентификации КА, свойства отказоустойчивости является актуальной задачей.

Цель исследования. Возрастание требований к технико-экономическим характеристикам современных систем спутниковой связи, а также обеспечение требуемого уровня их имитостойкости привели к необходимости использования запросно-ответных систем, позволяющих определить статус КА. Для обеспечения требуемого уровня имитостойкости таких систем опознавания «свой-чужой» в работах [1,2] предлагается использовать протокол, основанный на доказательстве с нулевым разглашением знаний. Данный протокол обладает достаточно высокой криптостойкостью.

Однако в процессе работы запросно-ответной системы могут возникнуть сбои и отказы, которые приведут к искажению результатов вычислений. Для устранения таких последствий необходимо, чтобы система опознавания обладала свойством устойчивости к отказам. Эффективные результаты можно получить с помощью использования модулярных кодов. В данных кодах вычисления производятся параллельно и по независимым вычислительным каналам. Это свойство модулярных кодов можно использовать при разработке отказоустойчивой системы опознавания статуса КА.

Поэтому целью данной работы является повышение отказоустойчивости запросно-ответной системы, применяемой в низкоорбитальных системах спутниковой связи, на основе использования непозиционных модулярных кодов, которые способны осуществлять поиск и коррекцию ошибок, вызванных сбоями и отказами оборудования.

Материалы и методы исследования

В процессе использования низкоорбитальных систем спутниковой связи широкое внимание уделяется вопросам обеспечения высокой надежности работы бортовых комплексов. Введение в состав космического аппарата системы опознавания «свой-чужой» приводит к увеличению схемных затрат. Поэтому при разработке структуры запросно-ответной системы особое внимание уделяется вопросам обеспечения отказоустойчивости работы такой системы. Так как обеспечение масса-габаритных показателей для оборудования КА является достаточно жестким, то для обеспечения устойчивости к отказам и сбоям, которые могут возникнуть в процессе работы системы опознавания, целесообразно использовать алгебраические системы, обладающие свойством кольца и поля.

Особое место среди таких алгебраических систем занимают модулярные коды. В настоящее время среди непозиционных модулярных кодов можно выделить две большие группы. Основу первой группы составляют непозиционные коды системы остаточных классов (СОК). При построении таких кодов классов вычетов в качестве оснований применяются взаимно простые числа [4, 6, 7]. Благодаря этому любой позиционный код можно представить в виде набора остатков, полученных при делении этого числа на числа-основания:

$$A = (\alpha_1, \alpha_2, ..., \alpha_k), \qquad (1)$$

где $\alpha_i \equiv A \bmod p_i$; $i = 1, ..., k$.

Основу второй группы непозиционных кодов составляют модулярные полиномиальные коды, в частности, коды полиномиальной системы классов вычетов (ПСКВ) [5, 8]. При построении таких кодов классов вычетов в качестве оснований применяются неприводимые полиномы. Благодаря этому любой позиционный код представляется в самом начале в полиномиальной форме, а затем полученному полиному в соответствие ставится набор остатков, полученных при делении этого числа на модули:

$$A(z) = (\alpha_1(z), \alpha_2(z), ..., \alpha_k(z)), \qquad (2)$$

где $\alpha_i(z) \equiv A(z) \bmod p_i(z)$; $i = 1, ..., k$.

Несмотря на различия, данные модулярные коды имеют много общего. Данные коды, за счет параллельной и независимой обработки вычетов, позволяют повысить скорость выполнения следующих модульных операций:

$$\left| A \otimes B \right|_{p_i}^{+} = \left| \alpha_i \otimes \beta_i \right|_{p_i}^{+}, \qquad (3)$$

где $A = (\alpha_1, \alpha_2, ..., \alpha_n)$ и $B = (\beta_1, \beta_2, ..., \beta_n)$ – модулярный код в кольце вычетов; $\alpha_i \equiv A \bmod p_i$; $\beta_i \equiv \hat{A} \bmod p_i$; $\otimes$ – операции сложения, вычитания и умножения по модулю основания кода СОК p_i; $i = 1, \ldots, k$.

В работах [2, 3] представлен протокол аутентификации космического аппарата, использующий доказательство с нулевым разглашением данных. Данный протокол применяется при определении статуса КА, который попадается в зону видимости станции спутниковой связи, расположенной на необслуживаемом объекте. С целью повышения его эффективности был разработан протокол, использующий модулярные коды.

Для организации процесса работы системы опознавания используется секретный ключ U. При этом открытый ключ спутника, который используется при решении уравнения двойного использования сеансового ключа $S(i)$, определяется

$$K_U = g^U \bmod q, \qquad (4)$$

где q – простое число; g – первообразный элемент, порождающий группу q.

Чтобы выполнить протокол аутентификации КА с помощью модулярных кодов, необходимо выбирать основания $p_1, \ldots, p_k$, так, чтобы диапазон P кода СОК удовлетворял

$$P = \prod_{i=1}^{k} p_i > q, \qquad (5)$$

где p_i – простые числа, в которых g – первообразный элемент.

Затем вычисляем значение истинного статуса КА в системе остаточных классов:

$$\begin{aligned} C_1 &= g^{U_1} g^{S_1} g^{T_1} \bmod p_1 \\ &\vdots \\ C_k &= g^{U_k} g^{S_k} g^{T_k} \bmod p_k, \end{aligned} \qquad (6)$$

где $C_i \equiv C \bmod p_i$; $K_i \equiv K \bmod p_i$; $S_i \equiv S \bmod p_i$; $T_i \equiv T \bmod p_i$; C – статус КА; S – параметр, который используется для вычисления сеансового секретного ключа; T – параметр, который используется для обнаружения двойного применения сеансового ключа.

Данное значение истинного статуса КА в виде кода СОК ($C_1, C_2, \ldots, C_L$) заносится в блок памяти ответчика, который располагается на борту спутника. Затем пользователь проводит «зашумление» своих секретных данных. При этом используются случайные значения $\Delta U(j), \Delta S(j), \Delta T(j)$, где j – номер сеанса связи:

$$U_i^*(j) = (U + \Delta U_i(j)) \bmod p_i$$
$$S_i^*(j) = (S(j) + \Delta S(j)) \bmod p_i$$
$$T_i^*(j) = (T(j) + \Delta T(j)) \bmod p_i. \quad (7)$$

В результате получаются значения

$$U^* \neq U, S^*(j) \neq S, T^*(j) \neq T.$$

После этого система вычисляет новый «зашумленный статус КА» согласно

$$C_1^* = g^{U_1^*} g^{S_1^*} g^{T_1^*} \bmod p_1$$
$$\vdots$$
$$C_k^* = g^{K_k^*} g^{S_k^*} g^{T_k^*} \bmod p_k \quad (8)$$

где C^* – зашумленный статус спутника; $C_i^* \equiv C^* \bmod p_i$.

На следующем этапе запросчик пересылает пользователю число $d \in Z_q$. Ответчик приступает к вычислению ответа на вопрос d.

$$r_i(1) = (U_i^* - dU_i) \bmod \varphi(p_i),$$
$$r_i(2) = (S_i^* - SK_i) \bmod \varphi(p_i),$$
$$r_i(3) = (T_i^* - dT_i) \bmod \varphi(p_i). \quad (9)$$

Полученные ответы на поставленный вопрос d передаются запросчику. Затем запросчик приступает к проверке доказательства истинности пользователя:

$$A_1 = (C_1^d g^{r_1(1)} g^{r_1(2)} g^{r_1(3)}) \bmod p_1$$
$$\vdots$$
$$A_k = (C_k^d g^{r_k(1)} g^{r_k(2)} g^{r_k(3)}) \bmod p_k. \quad (10)$$

Если космический аппарат является своим, то справедливо равенство

$$A_i = C_i^* \bmod p_i. \quad (11)$$

Представленный выше алгоритм работы запросно-ответной системы в модулярных кодах можно аналогичным образом реализовать с использованием полиномиальной системы классов вычетов. Рассмотрим разработанный алгоритм коррекции ошибок с использованием минимальной избыточности. Для этого в систему оснований $p_1(z),..., p_k(z)$, с рабочим диапазоном

$$P_{раб}(z) = \prod_{i=1}^{k} p_i(z),$$

введем одно основание $p_{n+1}(z)$, которое удовлетворяет условию

$$\deg p_{n+1}(z) \geq \deg p_k(z). \quad (12)$$

Тогда в избыточном коде полиномиальной системе классов вычетов полином $A(z)$ представляется как набор остатков

$$A(z) = (\alpha_1(z), \alpha_2(z),..., \alpha_n(z), \alpha_{n+1}(z)), \quad (13)$$

где $\alpha_i(z) \equiv A(z) \bmod p_i(z)$ $p_i(z)$ – минимальный многочлен, определяемый в расширенном поле Галуа GF (2^v).

Для определения ошибок в коде ПСКВ используется полиномиальная форма позиционной характеристики интервала, которая определяется

$$S(z) = \left[A(z) / P_{раб}(z) \right]. \quad (14)$$

Используя модульные операции, определим значение интервал-кода:

$$S(z) = \left\| \left[\frac{\sum_{i=1}^{n} \alpha_i(z) B_i^*(z)}{P_{раб}(z)} \right] + \sum_{i=1}^{n+1} \alpha_i(z) R_i(z) \right|_{p_{n+1}(z)}^{+} =$$
$$= \left| K^A(z) + \sum_{i=1}^{n+1} \alpha_i(z) R_i(z) \right|_{p_{n+1}(z)}^{+}, \quad (15)$$

где $B_i(z) = R_i(z) P_{раб}(z) + B_i^*(z)$ – ортогональный базис полной, состоящей из n+1 оснований, ПСКВ; $R_i(z) = \left[B_i(z) / P_{раб}(z) \right]$; $B_i^*(z) = rest\left(B_i(z) / P_{раб}(z) \right)$ – ортогональный базис системы с основаниями $p_1(z)$, $p_2(z)$,..., $p_n(z)$; $K^A(z) = \left[\sum_{i=1}^{n} \alpha_i(z) B_i^*(z) \Big/ P_{раб}(z) \right]$ – количество переходов за величину рабочего диапазона $P_{раб}(z)$.

Значит, значение $K^A(z)$ будет определяться только значениями произведений $\alpha_i(z) B_i^*(z)$, i=1,..., n. Тогда выражение (15) можно представить в виде

$$S(z) = \left| K^A(z) + \sum_{i=1}^{n+1} \alpha_i(z) R_i(z) \right|_{p_{n+1}(z)}^{+} =$$
$$= \left| \sum_{i=1}^{n} \alpha_i(z) R_i^*(z) + \alpha_{n+1}(z) R_{n+1}(z) \right|_{p_{n+1}(z)}^{+}, \quad (16)$$

где

$$\alpha_i(z) R_i^*(z) = \alpha_i(z) R_i(z) + K_i^A(z);$$
$$K_i^A(z) = \left[\alpha_i(z) B_i^*(z) / P_{раб}(z) \right] -$$

количество переходов за рабочий диапазон $P_{раб}(z)$, которое возникнет при значении остатка $\alpha_i(z)$; i =1,..., n.

Результаты исследования и их обсуждение

Рассмотрим работу разработанного протокола с использованием кода СОК. Пусть выбраны основания p_1 =11, p_2 = 13, p_3 = 19. Тогда диапазон СОК будет равен P = 2717. В качестве первообразного элемента данной группы возьмем g = 2. Пусть значение секретного ключа равно U = 3. Пусть значения S = 5 и T = 5. Представим данные параметры в СОК:

K = (3, 3, 3), S = (5, 5, 5), T = (5, 5, 5).

Используем (6) для вычисления представления:

$$C_1 = g^{U_1} g^{S_1} g^{T_1} \bmod p_1 = 8;$$
$$C_2 = g^{U_2} g^{S_2} g^{T_2} \bmod p_2 = 2;$$
$$C_3 = g^{U_3} g^{S_3} g^{T_3} \bmod p_3 = 3.$$

Полученный истинный статус спутника $C = (8, 2,3)$ записывается в память ответчика.

Затем проводится «зашумление» секретных данных. При этом используются значения $\Delta K = 2, \Delta S = 2, \Delta T = 2$. Тогда зашумленные значения $U^* = (5, 5, 5)$, $S = (7, 7, 7)$ и $T = (7, 7, 7)$.

После пользователь вычисляет «зашумленное вручение» согласно (8)

$$C_1^* = g^{U_1^*} g^{S_1^*} g^{T_1^*} \bmod 11 = 5;$$
$$C_2^* = g^{U_2^*} g^{S_2^*} g^{T_2^*} \bmod 13 = 11;$$
$$C_3^* = g^{U_3^*} g^{S_3^*} g^{T_3^*} \bmod 19 = 2.$$

Пусть запросчик пересылает спутнику число $d = 10$.

Ответчик вычисляет ответы на вопрос $d = 10$. Первый ответ в коде СОК равен

$$r_1(1) = \left(U_1^* - dU_1\right) \bmod \varphi(11) = 5;$$
$$r_2(1) = \left(U_2^* - dU_2\right) \bmod \varphi(13) = 11;$$
$$r_3(1) = \left(U_3^* - dU_3\right) \bmod \varphi(19) = 11.$$

Второй ответ в коде СОК равен

$$r_1(2) = \left(S_1^* - dS_1\right) \bmod \varphi(11) = 7;$$
$$r_2(2) = \left(S_2^* - dS_2\right) \bmod \varphi(13) = 5;$$
$$r_3(2) = \left(S_3^* - dS_3\right) \bmod \varphi(19) = 11.$$

Третий ответ в коде СОК равен

$$r_1(3) = \left(T_1^* - dT_1\right) \bmod \varphi(11) = 7;$$
$$r_2(3) = \left(T_2^* - dT_2\right) \bmod \varphi(13) = 5;$$
$$r_3(3) = \left(T_3^* - dT_3\right) \bmod \varphi(19) = 11.$$

Полученные ответы (5, 11, 11), (7, 5, 11), (7, 5, 11) передаются запросчику, который приступает к проверке доказательства истинности пользователя. Для этого вычисляется

$$A_1 = \left| C_1^d g^{r(1)_1} g^{r(2)_1} g^{r(3)_1} \right|_{11}^{+} = 5;$$
$$A_2 = \left| C_2^d g^{r(1)_2} g^{r(2)_2} g^{r(3)_2} \right|_{13}^{+} = 11;$$
$$A_3^* = \left| C_3^d g^{r(1)_3} g^{r(2)_3} g^{r(3)_3} \right|_{19}^{+} = 2.$$

Так как

$$A_1 = C_1^* \bmod p_1 = 5;$$
$$A_2 = C_2^* \bmod p_2 = 11;$$
$$S_3 = C_3^* \bmod p_3 = 2,$$

то статус КА «свой» и запросчик разрешает начать сеанс связи.

Рассмотрим разработанный алгоритм коррекции ошибок с помощью модулярного кода. Пусть $p_1(z)=z+1$, $p_2(z)=z^3+z^2+1$, $p_3(z)=z^3+z+1$. В качестве контрольного основания используем $p_3(z)$. Тогда

$$P_{раб}(z) = p_1(z) p_2(z) =$$
$$= z^4 + z^2 + z + 1.$$

Вычислим ортогональные базисы ПСКВ:

$$B_1(z)=z^6+ z^5+ z^4+ z^3+ z^2+z+1;$$
$$B_2(z)=z^6+z^5+z^3+1;$$
$$B_3(z)=z^4+z^2+z+1.$$

Представим ортогональные базисы в виде

$$B_1(z)=R_1 P_{раб}(z)+B_1{}^*=(z^2+z);$$
$$P_{раб}(z)+(z^3+z^2+1);$$
$$B_2(z)=R_2 P_{раб}(z)+B_2{}^*=(z^2+z+1);$$
$$P_{раб}(z)+(z^3+z^2);\ B_3(z)=R_3 P_{раб}(z)= 1\ P_{раб}(z).$$

Получаем систему безызбыточных оснований $p_1(z)=z+1$, $p_2(z)=z^3+z^2+1$, в которой определены ортогональные базисы

$$B_1{}^*(z)= z^3+z^2+1,$$
$$B_2{}^*(z)= z^3+z^2.$$

Пусть $\alpha_2(z) = z$. Вычислим значение $\alpha_i(z) R_i^*(z) \bmod p_3(z)$. Тогда получаем

$$\alpha_2(z) R_2^*(z) =$$
$$= (\alpha_2(z) R_2(z) + K_i^A(z)) \bmod p_3(z) =$$
$$= (z(z^2 + z + 1) + 1) \bmod z^3 + z + 1 =$$
$$= (z^3 + z^2 + z + 1) \bmod z^3 + z + 1 = z^2.$$

Возьмем полином $A(z)= z^3+z^2+z+1$, который принадлежит $P_{раб}(z)$. В ПСКВ данный полином имеет вид $A(z)=(0, z, z^2)$. Определим значение интервала $S(z)$ согласно (16)

$$S(z) = \left| 0 \cdot R_1^*(z) + z \cdot R_2^*(z) + z^2 \cdot R_3 \right|_{z3+z+1}^{+} =$$
$$= \left| 0 + z^2 + z^2 \right|_{z3+z+1}^{+} = 0.$$

Так как интервал $S(z) = 0$, то код ПСКВ не содержит ошибки.

Пусть ошибка произошла по первому основанию. Тогда $A(z)=(1, z, z^2)$. Определим значение $S(z)$, используя выражение (16). Получаем

$$S(z) = \left|R_1^*(z) + zR_2^*(z) + z^2R_3\right|^+_{z3+z+1} =$$

$$= \left|z^2 + z + z^2 + z^2\right|^+_{z3+z+1} = z^2 + z = 110.$$

Так как значение полиномиальной формы позиционной характеристики интервала $S(z) \neq 0$, то код ПСКВ содержит ошибку. Произведем ее исправление. Преобразователь кода ПСКВ в позиционный код определяет значение

$$A^*(z)=(\alpha_1(z)B_1(z)+$$
$$+\alpha_2(z)B_2(z)\ \alpha_3(z)B_3(z))\text{mod}\ z^7+1 =$$
$$= ((z^6+ z^5+ z^4+ z^3+ z^2+z+1)+z(z^6+z^5+z^3+1)+$$
$$z^2(z^4+z^2+z+1))\text{mod}\ z^7+1 =$$
$$= (z^7+z^6+z^5+z^4+1)\ \text{mod}\ z^7+1= z^6+z^5+z^4.$$

Тогда для исправления ошибки вычисляем

$$\text{A}(z)=\text{A}^*(z)+ \Delta A_j(z) =$$
$$(z^6+z^5+z^4)+(z^6+z^5+z^4+z^3+z^2+z+1)=$$
$$=z^3+z^2+z+1.$$

Заключение

В работе показана целесообразность использования модулярных кодов при построении отказоустойчивой системы опознавания «свой-чужой». Представлен алгоритм работы запросно-ответной системы, которая использует коды СОК. Проведенные исследования показали, что применение модулярного кода позволяет не только повысить скорость реализации данной информационной технологии за счет параллельных вычислений по основаниям, но и корректировать ошибки, которые возникают из-за сбоев и отказов в процессе работы. Представлены примеры выполнения протокола аутентификации КА и обнаружения и коррекции ошибок, возникающих в работе системы опознавания «свой-чужой», функционирующей в модулярных кодах.

Список литературы

1. Гостев Д.В. Разработка протокола снятия со счета электронных денежных средств // Проблемы автоматизации. Региональное управление. Связь и автоматика. – ПАРУСА-2015*: Сборник трудов IV Всероссийской научной конференции молодых ученых, аспирантов и студентов, г. Геленджик, 29–30 октября 2015 г. – С. 137–140.

2. Калмыков И.А., Ляхов А.В., Пашинцев В.П. Применение помехоустойчивого протокола аутентификации космического аппарата для низкоорбитальной системы спутниковой связи // Инфокоммуникационные технологии. – 2015. – Т. 13; № 2. – С. 183–190.

3. Калмыков И.А., Вельц О.В., Калмыков М.И. Алгоритм имитозащиты для системы удаленного мониторинга и управления критическими технологиями // Известия ЮФУ. Технические науки. – Таганрог: ТРТУ, 2014. – №2 (151). – С. 181–187.

4. Ananda Mohan Residue Number Systems. Theory and Applications. Springer International Publishing Switzerland, 2016.

5. Chu, J., & Benaissa, M. Polynomial Residue Number System GF(2m) Multiplier Using Trinomials. In 17th European Signal Processing Conference, August 24–28, 2009, Glasgow, Scotland, pp. 958–962.

6. Mohan P.V. Residue Number Systems. Algorithms and Architectures. Springer, 2002.

7. Omondi A. and Premkumar B. Residue Number Systems: Theory and Implementation. Imperial College Press. UK, 2007.

8. Stepanova E.P., Toporkova E.V., Kalmykov M.I., Katkov R.A., Rezenkov D.N. Application of the codes of a polynomial residue number system, aimed at reducing the effects of failures in the AES cipher // Journal of Digital Information Management. – 2016. – Vol. 14, N.2. – PP. 114–123.