Раздел V. Информационная безопасность телекоммуникационных систем

УДК 631.8

И.А. Калмыков, О.В. Вельц, М.И. Калмыков, Д.О. Науменко

АЛГОРИТМ ИМИТОЗАЩИТЫ ДЛЯ СИСТЕМ УДАЛЕННОГО МОНИТОРИНГА И УПРАВЛЕНИЯ КРИТИЧЕСКИМИ ТЕХНОЛОГИЯМИ

Рассмотрены вопросы обеспечения защиты системы мониторинга, контроля и управления удаленного объекта от навязывания ложного образа сигнала. Отсутствие в составе абонентского терминала, который размещается на удаленном объекте, программно-аппаратного комплекса определения статуса космического аппарата (КА), находящегося в зоне видимости, может привести к нарушению нормальной работы оборудования и увеличению вероятности нанесения ущерба экологии района размещения. Рассмотрены основные виды деструктивных воздействий, которые могут быть применены для нарушения работы системы космической связи, используемой системой мониторинга, контроля и управления операциями в критических сферах деятельности человека. Показано, что наиболее эффективным способом нарушения работы оборудования, которое располагается в труднодоступных и малонаселенных областях Крайнего Севера и районах Арктики, является навязывания ложного образа сигналов, поступающих от КА. Целью работы является разработка системы имитозащиты, позволяющей снизить вероятность навязывания ложной информации. Одним из наиболее эффективных методов борьбы с навязыванием ложных образов является применение запросно-ответной системы опознавания. Приведен алгоритм работы такой системы, использующий протоколы с нулевым разглашением. С помощью алгоритма запросчик, который располагается на стационарном объекте, может в реальном масштабе времени определить статус КА, находящегося в зоне видимости.

Имитозащита данных; навязывание ложных образов; космическая станция; запросно-ответная система опознавания; псевдослучайная функция; протокол доказательства с нулевым разглашением.

I.A. Kalmykov, O.V. Velts, M.I. Kalmykov, D.O. Naumenko

DEVELOPMENT OF AN ALGORITHM IMITATION RESISTANCE FOR OF REMOTE MONITORING AND CONTROL CRITICAL TECHNOLOGIES

The paper discusses the issues of providing protection monitoring, control and management of the remote object from imposing false image signal. Absence in the user terminal, which is located at a remote site, the hardware-software complex definition of the status of the spacecraft (SC), located in the zone of visibility can lead to malfunction of the equipment and increase the likelihood of damage to the ecology deployment area. The basic kinds of destructive effects that can be applied to system malfunction space communications system used for monitoring, control and operations management in critical areas of human activity. It is shown that the most effective way of equipment malfunctions, which is located in the remote and sparsely populated areas of the Far North and Arctic regions, is to impose a false image signals from the spacecraft. The aim is to develop a simulation protection system, which can reduce the probability of false information imposing. One of the most effective methods of imposing false images is the use of challenge-

response system identification. In this paper we developed an algorithm of such a system using zero knowledge protocols. With this algorithm, the interrogator, who is on a stationary object can in real time to determine the status of the spacecraft is in the area of conductivity.

Imitation resistance of data; the imposition of false images; space station ion; challenge-response system identification; pseudo-random function; the protocol zero-knowledge proof.

Экспансия России в Арктике имеет важное геополитическое значение, в частности, стратегическое значение для российской экономики. Глобальное потепление и связанное с этим таяние арктических льдов открывает перед Россией новые экономические перспективы. Они связаны с освоением месторождений нефти и газа на как арктическом шельфе и на прилегающих к Северному Ледовитому океану территориях. Разработка новых месторождений шельфа северных морей призвана компенсировать спад добычи в традиционных нефтегазодобывающих районах.

Характерной чертой систем добычи и транспортировки углеводородных ископаемых является их размещение в труднодоступных и малонаселенных областях Крайнего Севера. Контроль, управление и связь с удаленными объектами становятся критичным элементом в нефтегазовой индустрии, и необходимым для обеспечения безопасности персонала, бесперебойной работы оборудования и повышения эффективности работы.

Для решения данной проблемы государственные и международные компании создают интерактивные системы удаленного мониторинга, контроля и управления операционными процессами. Использование таких центров является основой для оптимизации выполняемых работ с одновременным улучшением безопасности их проведения и уменьшения сопутствующих рисков. Для достижения поставленных задач, компания формирует центры поддержки операций (ЦПО), в которые объединяет высококвалифицированных специалистов, развитые технологические процессы, передовую технологию добычи и транспортировки сырья, испытанное программное обеспечение и системы для обеспечения связи в реальном времени для обмена данными о параметрах выполняемых работ, телеметрического сопровождения и измерений регистрируемых приборами, установленными на удаленном оборудовании.

Для доведения данных в настоящее время используется множество систем, начиная от проводных систем связи и закачивая – беспроводными. Однако, проведенные исследования показали, что наиболее эффективными способом обмена данными между удаленным оборудованием, которое располагается в труднодоступных и малонаселенных областях Крайнего Севера и районах Арктики, и центрами поддержки операций является использование систем космической связи [1].

В этом случае сигнал от многофункционального модуля, размещенного на удаленном оборудовании, передается на космический аппарат (КА), используя соответствующую аппаратуру кодирования. После этого он передается центру управления и контроля состояния оборудования нефтегазовой индустрии, где производится дальнейшая обработка данных и принятие соответствующего управляющего воздействия.

Однако географическое положение многих месторождений за Полярным кругом и на арктическом шельфе приводят к ситуации, когда использование геостационарных орбитальных установок невозможно. Одним из решений вопроса обеспечения интерактивного удаленного мониторинга, контроля и управления является запуск и использования группировки КА на низких околоземных орбитах. Как правило, высота полета такого аппарата не превышает 800 км, период обращения 100 мин. Срок активного существования КА находится в пределе от 3 до 5 лет. В качестве примера можно привести спутник CRyoSat, который осуществляет работу на приполярной орбите [2].

Учитывая заинтересованность многих стран в разработке арктического шельфа, можно сделать вывод о том, что количество орбитальных группировок космических аппаратов будет неизменно расти. Это приведет к ситуации, когда абонентский терминал (АТ), представляющий собой программно-аппаратный комплекс, спроектированный на базе станции спутниковой связи для сбора и обработки навигационных и телеметрических данных на объекте мониторинга, может видеть сразу же несколько КА, принадлежащих различным компаниям и государствам.

Большинство спутниковых систем работают в режиме трансляции сигналов с кодовым разделением каналов. При таком типе разделения каналов сигналы от всех КА орбитальной группировке транслируются в одной полосе частот. В этом случае существует вероятность осуществления попыток злоумышленником нарушения нормальной работы системы космической связи. Дестабилизация работы системы мониторинга, контроля и управления может привести к нарушению функционирования оборудования нефтегазовой индустрии. Кроме того, это может спровоцировать экологическую катастрофу, последствия которой приведет к частичному или полному уничтожению экосистемы Крайнего Севера и Арктики.

Проведенные исследования показали, что в основу дестабилизирующих действий на систему мониторинга, контроля и управления удаленным объектом могут быть положены методы радиоэлектронного подавления сигнала и навязывания ложного базиса сигнала.

Целью радиоэлектронного подавления сигнала КА на низких околоземных орбитах является блокирование передачи сигнала, в результате которого центр поддержки операций утрачивает возможность правильно принимать решение по выбору управляющего воздействия на удаленный объект.

В основу второй группы входят методы подмена базиса ложными сигналами. Основной целью подмены является искажение значений показателей, позволяющих оценить текущее состояние объекта управления, или навязывание некорректного управляющего воздействия, поступающего из центра поддержки операций.

Следует отметить, что, несмотря на многообразие систем способных поставить различные виды радиопомех, данный подход к нарушению работы системы мониторинга, контроля и управления удаленным объектом в условиях Крайнего Севера является неэффективным.

Таким образом, в условиях размещения оборудования в труднодоступных и малозаселенных районах, основным способом негативного воздействия на работу всей системы добычи и транспортировки углеводородов являются методы, образующие вторую группу. При этом подмена подразумевает создание копии базы сигналов и манипулирование его параметрами.

Снизить последствия от навязывания ложных образов возможно за счет повышения структурной скрытности, которая направлена на увеличение априорной неопределенности параметров передаваемых сигналов [3, 4]. Для достижения поставленной цели производится манипулирование основными параметрами сигналов, к которым относятся:

- частота несущего колебания;
- закон модулирования;
- стохастическое использование заранее подготовленных кодовых последовательностей.

Проведенные исследования показали, что реализация данного направления, позволяющего уменьшить последствия от ложного навязывания сигналов, требует значительных аппаратурных и финансовых затрат на свою реализацию.

Одним из перспективных направлений в решении отмеченной выше проблемы является разработка системы, позволяющей оперативно оценить статус спутника, находящегося в зоне видимости абонентского терминала.

В основу такой системы должен быть положен программно-аппаратный комплекс, реализующий процедуру опознавания «свой-чужой». В работе [5] представлен алгоритм работы устройства, используемого для определения статуса летательного аппарата. Основным недостатком запросно-ответной системы является необходимость периодической синхронизации работы запросчика и ответчика. Данная процедура осуществляется на Земле, перед тем как подвижный объект взлетит. Для этого в системе используется устройство синхронизации, в котором выход синхронизатора по фазе запросчика соединяют с помощью проводного канала связи с генератором импульсов, который входит в состав оборудования ответчика. Кроме того при этом синхронизируется работа цифровых счетчиков, расположенных в запросчике и ответчике. Благодаря этому соответствующие разряды счетчиков будут находиться в одинаковых состояниях.

Данного недостатка лишен программно-аппаратный комплекс, использующий протоколы с нулевым разглашением. Такие протоколы, базируясь на алгебраических системах обладающих свойством кольца и поля, нашли широкое применение в системах электронных платежей, которые работают с электронной наличностью [6–10]. Очевидно, что одним из основных свойств любой системы безналичных расчетов является обеспечение безопасности всех ее компонентов на всех этапах функционирования этой системы. При этом покупатель, использующий электронную наличность, продавец, эмитент и эквайер должны быть уверены в защите своих вложений. Использование разработанных протоколов с нулевым разглашением позволяет обеспечить решение такой проблемы, так как данные протоколы обладают хорошей криптографической стойкостью и обеспечивают высокую степень защиты информации от несанкционированного доступа.

Использование протоколов с нулевым разглашением в системах определения «свой-чужой» позволит повысить имитостойкость системы дистанционного контроля и управления удаленными объектами, обеспечивая повышение эффективности их функционирования и снижение рисков связанных с использованием критических технологий. С помощью этих протоколов запросчик, который располагается на стационарном объекте может в реальном масштабе времени определить статус КА, находящегося в зоне видимости. Для физической реализации данных протоколов в виде программно-аппаратного комплекса необходимо выполнение следующего алгоритма обмена данными.

Первый этап. В память вычислительного устройства ответчика, который располагается на борту КА, вводятся числа *U, S, T*. В этом случае число *U* выступает в качестве долгосрочного секретного ключа. Числа *S* и *T* являются базовой основой, с помощью которой производится вычисление сеансовых ключей *S(i)* и *T(i).*

Используя методы системного подхода при проведении исследований основных алгоритмов формирования псевдослучайных функций (ПСФ), была разработана псевдослучайная функция, позволяющая обеспечить случайное значение сеансовых ключей. Согласно работе [9] была разработаная ПСФ, принимающая на входную последовательность $(x_1,...,x_n)$ и ключ $(g,s_1,...,s_n)$, обеспечивает выполнение равенства

$$F((s_1,...,s_n),(g,x_1,...,x_n)) = g^{\left(\frac{1}{\prod_{i=1}^{n}(s_i+x_i)}\right)}, \quad (1)$$

где g – первообразный элемент мультипликативной группы.

Представленные в работе [9] теоремы, позволили показать, что для области определения размером 2^m значение $n = m/\log_2 l$. Вследствие этого при вычислении данной функции требуется в $\log_2 l$ раз меньше умножений. При этом при

сравнении с псевдослучайной функцией Наора-Рейнголда разработанная ПСФ использует меньший объем памяти для вычисления конечного за счет уменьшения в $\log_2 l$ раз размера ключа. Но при этом, стойкость данной ПСФ основывается на доказательстве о сложности решения λ-DDH проблемы.

Тогда имеем

$$S(i) = g^{\frac{1}{S+i+1}} \bmod q, \tag{2}$$

$$T(i) = g^{\frac{1}{T+i+1}} \bmod q, \tag{3}$$

где q – мультипликативная группа; g – первообразный элемент этой группы; i – номер проводимого сеанса.

Второй этап. Используя полученные данные *U, S(i)* и *T(i)* вычислительное устройство ответчика вычисляет истинный статус космического аппарата

$$C(i) = g^U g^{S(i)} g^{T(i)} \bmod q. \tag{4}$$

Вычисленное значение истинного статуса записывается в блок памяти программно-аппаратного комплекса.

Третий этап. Затем в вычислительном комплексе, используя полученные данные U, S(i) и T(i), производится их зашумление

$$U^*(i) = U + \Delta U \bmod q, \tag{5}$$

$$S^*(i) = S(i) + \Delta S \bmod q, \tag{6}$$

$$T^*(i) = T(i) + \Delta T \bmod q, \tag{7}$$

где $\Delta U, \Delta S, \Delta T$ – величины зашумления значений *U, S(i)* и *T(i)* соответственно.

После этого вычислительное устройство ответчика вычисляет зашумленный статус космического аппарата

$$C^*(i) = g^{U^*} g^{S^*(i)} g^{T^*(i)} \bmod q. \tag{8}$$

Вычисленное значение зашумленного статуса записывается в блок памяти программно-аппаратного комплекса.

Четвертый этап. При появлении КА в зоне видимости запросчик, находящийся на абонентском терминале, генерирует «запросное число» *d* и пересылает его космическому аппарату.

Пятый этап. Получив «запросное число» d ответчик производит вычисление ответов

$$r_1 = U^* - dU \bmod \varphi(q); \tag{9}$$

$$r_2 = S(i)^* - dS(i) \bmod \varphi(q); \tag{10}$$

$$r_3 = T(i)^* - dT(i) \bmod \varphi(q). \tag{11}$$

Шестой этап. Окончив выполнение вычислений, ответчик передает запросчику сигнал, который содержит:

- вычисленный истинный статус *C(i)*;
- вычисленный зашумленный статус *C*(i)*;
- ответы на поставленный вопрос r_1, r_2, r_3.

Седьмой этап. Запросчик, получив данный сигнал, вычисляет результат

$$Y(i) = C^d(i) g^{r_1} g^{r_2} g^{r_3} \bmod q. \tag{12}$$

Если вычисленное значение *Y(i)* совпадет со значением зашумленного статуса космического аппарата, $Y(i) = C^*(i)$, то принимается решение, что статус спутника «свой». Между абонентским терминалом, представляющим собой программно-аппаратный комплекс, спроектированный на базе станции спутниковой связи, и

КА производится обмен данными, которые являются результатом обработки навигационных и телеметрических данных на объекте мониторинга, и управляющими воздействиями, передаваемые с центра поддержки операций.

Если вычисленное значение не совпадет со значением зашумленного статуса космического аппарата, $Y(i) \neq C^*(i)$, то принимается решение, что статус спутника «чужой» и обмен информацией между абонентским терминалом и КА не производится.

Выводы. На основе системного подхода определена задача, связанная с обеспечением высокой имитостойкости систем удаленного мониторинга, контроля и управления объектами в условиях размещения объекта управления в Арктике. Показана целесообразность использования в системе определения статуса космического аппарата, находящегося в зоне видимости абонентского терминала, установленного на удаленном объекте управления, протокола с нулевым разглашением. Использование разработанного протокола позволяет на основе обработки «запросного числа» и вычисленного ответа на это число однозначно определить, является ли КА «своим», или он имеет статус «чужой». Применение разработанной псевдослучайной функции в новом протоколе запросно-ответной системы опознавания позволяет защитить оборудование удаленного объект от деструктивных воздействий, повысить эффективность его работы и снизить вероятность выхода из строя.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Центр поддержки операций компании Шлюмберже. http://www.slb.ru/page.php?code=28.
2. http://www.esa.int/Our_Activities/Observing_the_Earth/CryoSat.
3. *Пашинцев В.П., Чипига А.Ф., Галкина В.А., Смирнов А.А.* Решение проблемы обеспечения энергетической скрытности в системах спутниковой связи при близком размещении приемника радиоперехвата // Наукоемкие технологии. – 2012. – Т. 13, № 7. – С. 30-34.
4. *Катков К.А.* Адаптивный алгоритм определения вектора пространственно-временных координат // Известия ОрелГТУ. Информационные системы и технологии. – 2011. – № 1 (63). – С. 5-14.
5. *Моисеев В.Ф., Сивов В.А.* Система опознавания «свой-чужой» // Патент России № 2191403 от 11.12.2001.
6. *Калмыков И.А., Дагаева О.И.* Разработка псевдослучайной функции повышенной эффективности // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 160-169.
7. *Калмыков И.А., Дагаева О.И.* Новые технологии защиты данных в электронных коммерческих системах на основе использования псевдослучайной функции // Известия ЮФУ. Технические науки. – 2012. – 12 (137). – С. 218-224.
8. *Калмыков И.А., Кихтенко О.А., Барильская А.В., Дагаева О.И.* Криптографическая система на базе непозиционных полиномиальных алгебраических структур // Вестник Северо-Кавказского федерального университета. – 2010. – № 2. – С. 51-57.
9. *Калмыков И.А., Дагаева О.И., Науменко Д.О., Вельц О.В.* Системный подход к применению псевдослучайных функций в системах защиты информации // Вестник Северо-Кавказского федерального университета. – 2012. – № 3 (32). – С. 26-34.
10. *Калмыков И.А., Дагаева О.И.* Применение системы остаточных классов для формирования псевдослучайной функции повышенной эффективности// Известия ЮФУ. Технические науки. – 2013. – № 12 (149). – С. 228-234.

Статью рекомендовал к опубликованию д.т.н., профессор О.Б. Макаревич.

Калмыков Игорь Анатольевич – Институт информационных технологий и телекоммуникаций Северо-Кавказского федерального университета, г. Ставрополь; e-mail: kia762@yandex.ru; 355040 г. Ставрополь, ул. Шпаковская, 92, кор. 1, кв. 28; тел.: 88652731380, 89034163533; кафедра информационной безопасность автоматизированных систем; д.т.н.; профессор.

Вельц Оксана Владимировна – e-mail: velts-yatsenco@yandex.ru; 355013, г. Ставрополь, ул. Чехова, 33, кв. 66; тел.: 88652944241; кафедра информатики; старший преподаватель.

Науменко Даниила Олегович – e-mail: dante603@gmail.com; 355040, г. Ставрополь, ул. Семашко, 8, кв. 23; тел.: 89197362888; кафедра информационной безопасности автоматизированных систем; аспирант.

Калмыков Максим Игоревич – e-mail: kmi762@yandex.ru; 355040, г. Ставрополь, пр. Кулакова, 33, кв. 56; тел.: 88652956546; кафедра информационной безопасности автоматизированных систем; аспирант.

Kalmykov Igor Anatolyevich – Institute of Information Technologies and Telecommunications, North-Caucasus Federal University, Stavropol; e-mail: kia762@yandex.ru; 92, Shpakovskaya street, k.1, kv. 28, Stavropol, 355000, Russia; phone: +78652731380, +79034163533; the department of information security of automated systems; dr. of eng. sc.; professor.

Velts Oksana Vladimirovna – e-mail: velts-yatsenco@yandex.ru; 33, Chehova street, kv. 66, Stavropol, 355000, Russia; phone: +78652944241; the department of information science; senior lecturer.

Naumenko Daniil Olegovich – e-mail: dante603@gmail.com; 8, Semashko street, kv. 23, Stavropol, 355000, Russia; phone: +79197362888; the department of information security of automated systems; postgraduate student.

Kalmykov Maksim Igorevich – e-mail: kmi762@yandex.ru; 33, pr. Kulakova, kv. 44, Stavropol, 355040, Russia; phone: +79064710242; the department of information security of automated systems; postgraduate student.

УДК 621.39

С.В. Котенко

ИДЕНТИФИКАЦИОННЫЙ АНАЛИЗ ПРОЦЕССОВ ТЕЛЕКОММУНИКАЦИИ НЕПРЕРЫВНЫХ СООБЩЕНИЙ В ЦИФРОВЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

На фоне значительных достижений в части идентификации пользователей информационно-телекоммуникационных систем в задачах обработки, защиты и передачи информации практически обходится вниманием идентификация (аутентификация) информационно-телекоммуникационных процессов. Следствием этого является отсутствие самого понятия «идентификационный анализ» применительно к информационно-телекоммуникационным системам, не смотря на апробированные результаты продуктивного применения этого понятия к производственным, маркетинговым и педагогическим системам. Критичность сложившейся ситуации заключается в выявленных в последнее время закономерностях, состоящих в значительном и в ряде случаях определяющем влиянии пользовательского уровня на эффективность информационно-телекоммуникационных процессов. Приводится решение задачи теоретического обоснования методики идентификационного анализа процессов телекоммуникации непрерывных сообщений в цифровых информационных системах с позиций подходов и методов теории виртуализации. По результатам полученного решения синтезирована модель идентификационного анализа, включающая канал виртуальной оценки, что обеспечивает потенциально защищенную идентификацию. Отличительную особенность предложенной методики составляет применение в качестве идентификационных признаков адаптивно изменяющихся параметров цифрового представления непрерывных сообщений в цифровых информационных системах.

Идентификация; аутентификация; виртуализация; идентификационный анализ; информационный поток.