УДК 681.322

И.В. КАПГЕР, А.А. ЮЖАКОВ

Пермский государственный технический университет, Россия

ПРИМЕНЕНИЕ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ СООБЩЕНИЙ В ПРОМЫШЛЕННЫХ СЕТЯХ LON ПО ГОСТ 28147-89

Проведен анализ проблем надежности и достоверности передаваемых сообщений промышленных сетей LON, связанных с защитой от несанкционированных действий. Рассмотрена возможность аутентификации отправителя в рамках протокола LonTalk. Приведены методы коммуникации между узлами LonWorks посредством сетевых переменных и явных сообщений. Описаны возможности стандарта шифрования ГОСТ 28147-89, приведены технические требования к ключевой информации. Исследованы возможности применения криптографических преобразований сообщений, передаваемых в промышленных сетях LON, для повышения надежности и достоверности передачи. Предложено применение симметричного шифрования по ГОСТ 28147-89 в рамках протокольных функций LonTalk.

Ключевые слова: *LON, LonWorks, LonTalk, промышленные шины, надежность, достоверность, аутентификация, шифрование, криптография, ГОСТ 28147-89.*

Введение

В настоящее время компьютер и компьютерные сети все чаще применяются для автоматизации производственных процессов. Идея полной автоматизации производства основана на применении промышленных (полевых) шин, так называемых Fieldbus-систем. Fieldbus-системы, которые представляет и LON (Local Operating Network), могут стать существенной составной частью будущих сетей, базисом для разработок, которые в ближайшем будущем приобретут большую значимость. LON предназначена именно для автоматизации производства.

Система LonWorks вызывает огромный интерес во всем мире, который объясняется как техническими, так и экономическими аспектами.

В основе LonWorks лежит прогрессивная концепция, сущность которой состоит в сокращении иерархических уровней децентрализованной системы: отпадает необходимость в главных устройствах (Master), выполняющих функции централизованного управления [1].

Опосредованный обмен информацией при помощи сетевых переменных облегчает задачу программирования. Поддержка коммуникаций осуществляется на аппаратном уровне, пользователю предоставляется микросхема (Neuron Chip), в которой функции обмена информацией являются составной частью системного языка.

Введение в технологию LonWorks, обеспечивающее полное и академичное разъяснение ее фундаментальных концепций, также приведено в [2].

Протокол LON (точнее LonTalk) был разработан американской компанией Echelon Corporation изначально для построения интеллектуальных систем жизнеобеспечения зданий.

1. Постановка проблемы

Суть обсуждаемой задачи состоит в том, что при эксплуатации Fieldbus-сетей имеются проблемы повышения надежности и достоверности передаваемых сообщений, связанных с защитой промышленных сетей от несанкционированных действий [3].

В данной работе рассматривается противодействие следующим угрозам:

- несанкционированное чтение информации из сети LON путем подключения к шине передачи данных;
- внесение изменений в работу системы с нарушением ее работоспособности путем изменения настроек сетевых параметров шины передачи данных сети LON, в том числе перевод контроллеров в неактивное состояние;
- внесение изменений в работу сети LON с целью выполнения необходимых действий без нарушения ее работоспособности путем передачи ложных сообщений.

Ранее [4] было предложено применение методов кодирования (шифрования) и авторизации (аутентификации) в рамках протокольных функций сети LON.

В данной работе рассматривается возможность применения симметричного шифрования в сети LON.

2. Возможности аутентификации LON

К достоинствам LonWorks протокола относится аутентификация отправителя, однако здесь не учитывается угроза прослушивания промышленных сетей с целью получения информации. Так, защищенность сетей LonWorks от несанкционированного доступа и гарантирующего подлинность отправителя, реализована в протоколе LonTalk [1, 2]. LonTalk не использует кодирования в прямом смысле этого слова. Сообщение передается незакодированным, но идентичность отправителя проверяется кодом. Алгоритм кодирования представлен любым 48-битным ключом S (Encrypt Key - ключ кодирования) и случайным 64-битным числом Z, из которых определенным образом вычисляется 64-битное число кодирования V.

Протокол идентификации находится в распоряжении как транспортного, так и сеансового уровней. Идентификация позволяет получателю проверять сообщения идентичного отправителя. Оба участника обозначаются как вызывающий и запрашиваемый. Вызывающий инициирует процесс идентификации посылкой запрашиваемому 64-битного случайного числа Z. Тот отвечает закодированным Vg = Sg(Z) сообщением с использованием личного ключа Sg, а также исходным сообщением Z. Идентичность запрашиваемого проверяется следующим образом: вызывающий проводит кодирование своим собственным ключом Vh = Sh(Z) и сравнивает свой результат Vh с Vg. Если как вызывающий, так и запрашиваемый используют один и тот же ключ Sh = = Sg, протокол идентификации отправляет сигнал успешного завершения, в противном случае - сигнал сбоя. В любом случае сообщение передается дальше на прикладной уровень вместе с информацией об идентификации. Если прикладную задачу при данной транзакции не интересует результат идентификации, она использует полученное сообщение, даже если идентификация транзакции не гарантируется.

Так как сообщения не кодируются, установку нового ключа S посредством команд сетевого менеджмента проводят особым образом. С помощью функции Update_Key можно прибавить некоторую величину (инкремент) к ключу кодирования Encrypt Key, тем самым можно изменить Encrypt Key, без передачи явного ключа по сети.

3. Коммуникация узлов LON

Для каждого чипа изготовителем в EEPROM задается уникальный 48-битный идентификационный номер Neuron ID. Сообщения LonTalk могут использовать Neuron ID для адресации тех узлов, чьи логические сетевые адреса еще не определены.

Коммуникация между узлами выполняется двумя способами. Предпочтительный обмен данными осуществляется посредством сетевых переменных, при котором отсылка и прием выполняются автоматически. Альтернативой является обмен явными сообщениями, при котором процесс коммуникации обрабатывается программой, при этом сообщение должно быть сформировано, отослано, и должен быть принят ответ. Механизм явных сообщений требует меньше места памяти EEPROM, чем механизм обмена сетевыми переменными, однако требует больше места в памяти программы.

Сетевые переменные определяются в прикладной программе и могут быть переменными ввода или вывода. Отсылка значения выполняется автоматически без дополнительного кода в прикладной программе. В одном узле можно определить до 62 сетевых переменных длиной до 31 байта. Если Neuron Chip используется как процессор коммуникации, а вторая система процессоров берет на себя обработку прикладной задачи, то можно реализовать до 4096 сетевых переменных. Для сетевых переменных можно выбрать тип способа передачи Authenticated, при котором значение сетевой переменной может передаваться, только если отправитель и получатель обладают одинаковым ключом Encrypt Key. Добавим, что значение сетевой переменной можно послать с помощью явного сообщения.

В некоторых случаях - когда передаются данные длиной более 31 байта, когда имеющиеся типы сетевых переменных не подходят или требуется передача данных с ответом на них - применения сетевых переменных недостаточно. Дополнительно явное сообщение поддерживает механизм запросов/ответов, позволяющий прикладной задаче одного узла выполнять определенные действия в прикладной задаче другого узла. В результате на свое сообщение (запрос) узел-отправитель получает ответ. С помощью явного сообщения можно передавать данные длиной до 259 байтов. Дополнительно можно выбрать тип способа передачи Authenticated, при котором значение может передаваться, только если отправитель и получатель обладают одинаковым ключом Encrypt Key.

4. Алгоритмы ГОСТ 28147-89

Описание стандарта шифрования содержится в документе «Алгоритм криптографического преобразования данных ГОСТ 28147-89» [5]. В ГОСТе содержится описание алгоритмов нескольких уровней, а также описан построенный на общих принципах с ними алгоритм выработки имитовставки, которая является криптографической контрольной комбина-

цией с целью защиты данных от внесения в них несанкционированных изменений [6, 7, 8]. На самом верхнем находятся практические алгоритмы, которые опираются на три алгоритма низшего уровня, называемые базовыми циклами: цикл зашифрования, цикл расшифрования и цикл выработки имитовставки. В свою очередь, каждый из базовых циклов представляет собой многократное повторение одной процедуры, называемой основным шагом криптопреобразования.

В ГОСТе ключевая информация состоит из двух структур данных: ключа и таблицы замен. Ключ является массивом из восьми 32-битовых элементов кода, элементы ключа используются как 32-разрядные целые числа без знака, размер ключа составляет 32•8 = 256 бит или 32 байта. Таблица замен представлена в виде матрицы размера 8x16, содержащей 4-битовые элементы, которые можно представить в виде целых чисел от 0 до 15. Строки таблицы замен называются узлами замен, они должны содержать различные значения, то есть каждый узел замен должен содержать 16 различных чисел от 0 до 15 в произвольном порядке. Общий объем таблицы замен равен: 8 узлов x 16 элементов/узел x 4 бита/элемент = 512 бит или 64 байта. ГОСТ относится к классу блочных шифров, то есть единицей обработки информации в нем является блок данных.

Основной шаг криптопреобразования является оператором, определяющим преобразование 64-битового блока данных, младшая и старшая части обрабатываются отдельно. Дополнительным параметром этого оператора является 32-битовый блок, в качестве которого используется какой-либо элемент ключа.

Базовые циклы построены из основных шагов криптографического преобразования. В процессе выполнения основного шага используется только один элемент ключа, в то время как ключ ГОСТ содержит восемь таких элементов. Следовательно, чтобы ключ был использован полностью, каждый из базовых циклов должен многократно выполнять основной шаг с различными его элементами. Базовые циклы заключаются в многократном выполнении основного шага с использованием разных элементов ключа и отличаются друг от друга только числом повторения шага и порядком использования ключевых элементов. Цикл расшифрования является обратным циклу зашифрования. Цикл выработки имитовставки вдвое короче циклов шифрования, порядок использования ключевых элементов в нем такой же, как в первых 16 шагах цикла зашифрования.

ГОСТ 28147-89 предусматривает три режима:

- простая замена;
- гаммирование;
- гаммирование с обратной связью;
- выработка имитовставки.

Данные обрабатываются блоками по 64 бита, на которые разбивается массив, подвергаемый криптографическому преобразованию. В режимах гаммирования есть возможность обработки неполного блока данных размером меньше 8 байт.

Зашифрование при простой замене заключается в применении цикла зашифрования к блокам открытых данных. Размер массива данных должен быть кратен 64 битам, после выполнения операции размер массива не изменяется. ГОСТ предписывает использовать режим простой замены для шифрования ключевых данных.

Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, то есть последовательности элементов данных, вырабатываемых с помощью криптографического алгоритма, для получения зашифрованных (открытых) данных. Гамма для этого режима получается с помощью алгоритмического рекуррентного генератора последовательности чисел (РГПЧ), вырабатывающего 64-битовые блоки данных, которые далее преобразовываются по циклу зашифрования в режиме простой замены. Наложение и снятие гаммы осуществляется при помощи операции побитового исключающего «ИЛИ», алгоритмы зашифрования и расшифрования в режиме гаммирования идентичны. РГПЧ для выработки гаммы является рекуррентной функцией с начальным элементом «синхропосылкой», предварительно преобразованной по циклу зашифрования. Последовательность элементов, вырабатываемых РГПЧ, зависит от его начального заполнения и от ключа. Для обратимости процедуры шифрования должна использоваться одна и та же синхропосылка. Синхропосылка для зашифрования должна быть передана для использования при расшифровании. Это достигается хранением или передачей синхропосылки вместе с зашифрованным массивом данных, что приводит к увеличению размера массива данных при зашифровании на размер синхропосылки, то есть на 8 байт, либо использованием предопределенного значения синхропосылки или выработкой ее синхронно источником и приемником по определенному закону, в этом случае изменение размера передаваемого или хранимого массива данных отсутствует. Генерировать синхропосылку синхронно у источника и получателя массива данных не всегда представляется возможным, поскольку требует жесткой привязки к чему-либо в системе.

Режим гаммирования с обратной связью похож на режим гаммирования и отличается от него только способом выработки элементов гаммы – очередной элемент гаммы вырабатывается как результат пре-

образования по циклу зашифрования предыдущего блока зашифрованных данных, а для зашифрования первого блока массива данных элемент гаммы вырабатывается как результат преобразования по тому же циклу синхропосылки. Каждый блок шифртекста в этом режиме зависит от соответствующего и всех предыдущих блоков открытого текста.

Для решения задачи обнаружения искажений в зашифрованном массиве данных в ГОСТе предусмотрен режим выработки имитовставки – контрольной комбинации, зависящей от открытых данных и секретной ключевой информации. Целью использования имитовставки является обнаружение всех случайных или преднамеренных изменений в массиве информации.

5. Применение шифрования в LON

В процессе исследования возможности применения криптографических преобразований (шифрования) для повышения надежности и достоверности передачи сообщений, передаваемых в промышленных Fieldbus -сетях на примере LON, найдено решение, позволяющее применить симметричное шифрование, основанное на блочном шифре по ГОСТ 28147-89.

Предлагается применение специальных методов кодирования (шифрования) в рамках протокольных функций:

- применение симметричного шифрования в пределах всей сети LON или только некоторых узлов;
- применение на каждом узле LON программно-аппаратных средств кодирования (шифрования) с хранением ключей кодирования (шифрования) в памяти аппаратных средств;
- регулярная централизованная смена синхропосылок, используемых для кодирования (шифрования);
- передача критичных или всех данных по сети LON в кодированном (зашифрованном) виде.

Целесообразно для использования функций криптопреобразования по ГОСТу хранить 256-битный ключ и 512-битную таблицы замен в памяти каждого Neuron Chip. В качестве 64-битового блока данных, являющегося синхропосылкой, использовать предопределенное значение синхропосылки, вычисляемое программной Neuron Chip на основании имеющихся в необходимых узлах LON одинаковых 48-битных ключей кодирования Encrypt Key, то есть вырабатывать ее синхронно всеми необходимыми источниками и приемниками по определенному закону. При необходимости смены значения синхропосылки у источников и приемников необходимо с помощью функции Update_Key прибавить некоторую величину (инкремент) к ключу кодирования Encrypt Key, тем самым изменив Encrypt Key и, соответственно, добившись наличия одинаковой синхропосылки у всех необходимых источников и приемников.

В результате применения симметричного шифрования, основанного на блочном шифре по ГОСТ 28147-89 длина сообщения не изменяется, поэтому надежность остается на том же уровне. При этом достоверность сообщений в LON стремится к единице. Стойкость алгоритма шифрования по ГОСТ 28147-89 – это тема отдельного исследования, однако, если принять за аксиому стойкость данного алгоритма, то достоверность сообщений в LON становится равна единице.

Каждый из алгоритмов криптографического преобразования (гаммирование, гаммирование с обратной связью, имитовставка) различается по затратам времени на проведение преобразований. Чем более сложный применяется алгоритм или их комбинация, тем более высокой становится достоверность, и, соответственно, более высоки временные затраты.

Основная задача имитовставки – обнаружить внесение несанкционированных изменений при передаче сообщений. В случае применения имитовставки необходимо учитывать то, что размер исходного сообщения после наложения имитовставки будет увеличен. Но, в любом случае, длина получившегося сообщения в этом случае не может превышать максимальные значения, определенные в LON.

Таким образом, можно зашифровывать и расшифровывать сетевые переменные длиной до 31 байта или явные сообщения длиной до 259 байтов, передаваемые в сети LON (с использованием протокола LonTalk) по ГОСТ 28147-89 в режиме гаммирования с обратной связью или же в режиме обычного гаммирования. Дополнительно для обнаружения всех случайных или преднамеренных изменений в сообщениях LON можно применять имитовставку.

Заключение

Применение симметричного шифрования в промышленных сетях LON позволит исключить несанкционированное чтение информации из сетей LON и исключить возможность использования разрушительных и компрометирующих воздействий на них.

Рекомендуется для криптографических преобразований (шифрования) в промышленных сетях LON использовать симметричное шифрование, основанное на блочном шифре по ГОСТ 28147-89. В качестве перспективы дальнейших исследований в данном направлении может служить применение

асимметричного шифрования с использованием централизованного хранилища открытых ключей, использование стеганографических вставок в сообщениях узлов LON, а также применение фрагментации тела сообщения на произвольное количество сообщений различной длины в соответствии с заранее известным алгоритмом.

Литература

1. Дитмар Д. LON – технология: построение распределенных приложений. Пер. с нем. / Д. Дитмар, Л. Дитмар, Ю.Ш. Ганс; под ред. О. Б. Низамутдинова. – Пермь: Звезда, 1999. – 345 с.

2. Тирш Ф. Введение в технологию LonWorks. Пер. с англ. / Ф. Тирш. - М.; Энергоатомиздат, 2001. – 241с.

3. Латышев Г. Принцип построения безопасных систем автоматизации зданий и сооружений. [Электронный ресурс]. – Режим доступа к ресурсу: http://sga-bms.ru/publications/1082/.

4. Капгер И.В. Повышение надежности и достоверности промышленных Fieldbus-сетей на примере LON / И.В. Капгер, А.А. Южаков // Труды XXXV Международной конференции "Информационные технологии в науке, социологии, экономике и бизнесе IT+SE`2008", Украина, Крым, Ялта – Гурзуф, 30 сентября – 8 октября 2008 г., 2008.

5. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования, Госстандарт СССР, 1990.

6. Яковлев А.В. Криптографическая защита информации / А.В.Яковлев, А.А. Безбогов, В.В. Родин, В.Н. Шамкин. – Тамбов: Изд-во Тамб. гос. техн. ун-та, 2006. – 140 с.

7. Безбогов А.А. Методы и средства защиты компьютерной информации / А.А. Безбогов, А.В. Яковлев, В.Н. Шамкин. – Тамбов: Изд-во Тамб. гос. техн. ун-та, 2006. – 196 с.

8. Винокуров А. Алгоритм шифрования ГОСТ 28147-89, его использование и реализация для компьютеров платформы Intel x86 [Электронный ресурс]. – Режим доступа к ресурсу: http://www.enlight.ru/crypto/articles/vinokurov/gost_i.htm.

Поступила в редакцию 09.02.2009

Рецензент: д-р техн. наук, проф., проф. кафедры автоматики и телемеханики С.Ф. Тюрин, Пермский государственный технический университет, Пермь, Россия.

ВЖИВАННЯ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ПОВІДОМЛЕНЬ В ПРОМИСЛОВИХ МЕРЕЖАХ LON ПО ГОСТ 28147-89

І.В. Капгер, О.А. Южаков

Показані проблеми надійності і достовірності передаваних повідомлень промислових мереж LON, пов'язаних із захистом від несанкціонованих дій. Розглянута можливість аутентифікації відправника в рамках протоколу Lontalk. Приведені методи комунікації між вузлами Lonworks за допомогою мережевих змінних і явних повідомлень. Описані можливості стандарту шифрування ГОСТ 28147-89, приведені технічні вимоги до ключової інформації. Досліджені можливості вживання криптографічних перетворень повідомлень, передаваних в промислових мережах LON, для підвищення надійності і достовірності передачі. Запропоновано вживання симетричного шифрування по ГОСТ 28147-89 в рамках протокольних функцій Lontalk.

Ключові слова: LON, Lonworks, Lontalk, промислові шини, надійність, достовірність, аутентифікація, шифрування, криптографія, ГОСТ 28147-89.

APPLICATION OF CRYPTOGRAPHIC CONVERSIONS OF MESSAGES IN INDUSTRIAL LON NETWORKS UNDER GOST 28147-89

I.V. Kapger, A.A. Yuzhakov

The problems of reliability and authenticity of industrial LON network messages related to the protection from unauthorized actions are shown. The possibility of sender authentication within LonTalk protocol is considered. The communication methods between LonWorks hubs by means of network variable and explicit messages are shown. Possibilities of decryption standard GOST 28147-89 are described, technical requirements to key information are shown. There were studied the possibilities of using cryptographic conversions of massages communicated in industrial LON networks in order to increase the reliability and authenticity of conversion. The use of symmetric encryption under GOST 28147-89 within LonTalk protocol functions is suggested.

Key words: LON, LonWorks, LonTalk, industrial buses, reliability, validity, authenticity, encryption, cryptography, GOST 28147-89.

Капгер Игорь Владимирович – инженер по защите информации Пермской печатной фабрики – филиала ФГУП «Гознак», аспирант кафедры автоматики и телемеханики Пермского государственного технического университета, Пермь, Россия, e-mail: kapger@mail.ru.

Южаков Александр Анатольевич – д-р техн. наук, проф., заведующий кафедрой автоматики и телемеханики Пермского государственного технического университета, Пермь, Россия, e-mail: uz@at.pstu.ac.ru.