УДК [004.384:004.722.4:004.773].056.55:004.052.42

И.В. КАПГЕР, Ал-р А. ЮЖАКОВ, Ал-й А. ЮЖАКОВ

Пермский государственный технический университет, Россия

РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ СООБЩЕНИЙ В СИСТЕМАХ УПРАВЛЕНИЯ ПРОМЫШЛЕННЫХ СЕТЕЙ LON ИНТЕЛЛЕКТУАЛЬНЫХ ЗДАНИЙ

Исследованы проблемы промышленных сетей LON, используемых для построения интеллектуальных систем жизнеобеспечения зданий, связанные с защитой от несанкционированных действий. Рассмотрены возможности повышения надежности и достоверности сообщений, передаваемых в промышленных сетях LON, включая методы аутентификации узлов, шифрования сообщений, использования стеганографических вставок. Предложены реализации алгоритмов шифрования и стеганографии в рамках протокола LonTalk. Достигнутые результаты позволяют исключить несанкционированное чтение информации из промышленных сетей LON и исключить возможность использования разрушительных и компрометирующих воздействий на них.

Ключевые слова: *интеллектуальное здание, LON, LonWorks, LonTalk, промышленные шины, надежность, достоверность, аутентификация, шифрование, стеганография.*

Введение

В настоящее время компьютерные сети все чаще применяются для автоматизации производственных процессов, построения интеллектуальных систем жизнеобеспечения зданий. Идея полной автоматизации производства основана на применении промышленных (полевых) шин, так называемых Fieldbus-систем, которые представляет и LON (Local Operating Network) [1]. В основе LonWorks лежит прогрессивная концепция, сущность которой состоит в сокращении иерархических уровней децентрализованной системы: отпадает необходимость в главных устройствах, выполняющих функции централизованного управления. 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. Протокол LonTalk был разработан компанией Echelon Corporation изначально для построения интеллектуальных систем жизнеобеспечения зданий.

1. Постановка проблемы

Суть проблемы состоит в том, что при эксплуатации сетей LON имеются проблемы повышения надежности и достоверности передаваемых сообщений, связанных с защитой промышленных сетей от несанкционированных действий [2]. При этом должно быть обеспечено противодействие несанкционированному чтению информации из сети LON путем подключения к шине. Ранее было предложено применение методов кодирования (шифрования) и авторизации (аутентификации) в рамках протокольных функций сети LON, были рассмотрены возможности применения различных алгоритмов для криптографического преобразования сообщений, передаваемых в промышленных сетях LON. Так, рассматривались возможности применения симметричного шифрования, основанного на блочном шифре по ГОСТ 28147-89 [3], применения стеганографических вставок [4], применение нового алгоритма шифрования [5]. Наиболее простым примером, в котором необходимо использование шифрования, служит процесс обмена сообщениями между узлами LON при осуществлении идентификации и аутентификации пользователей в системах контроля и управления доступом интеллектуальных зданий. В данной работе мы будем рассматривать варианты реализации применения симметричного шифрования, основанного на блочном шифре по ГОСТ 28147-89 [6], применения нового алгоритма шифрования [7, 8] и использования стеганографических вставок [9] в прошивках (firmware) узлов LON, построенных на микросхеме Neuron Chip, с применением языка программирования Neuron C. В литературе встречаются аналогичные попытки встроить функции алгоритмов криптографических преобразований в специализированный кристалл. Так, например, исследовались алгоритмы криптографических преобразований по стандартам ГОСТ 28147-89, ГОСТ Р 34.10-94 и

© И.В. Капгер, Ал-р А Южаков, Ал-й А Южаков

ГОСТ Р 34.11-94 и предлагалось для ускорения работы использование специализированных жестких кристаллов, реализующие функции, используемые в данных алгоритмах [10].

2. Узлы LON

Узлы LON – объекты, которые взаимодействуют с физически подключенными устройствами ввода-вывода и соединяются с другими узлами в сети, используя протокол LonTalk. Каждый узел имеет Neuron-чип, интерфейсы ввода-вывода и приемопередающее устройство для подключения к сети. Поведение узла определяется конфигурацией узла и программой, содержащейся в его памяти. Конфигурирование, настройка узла и сети LON, а также загрузка программ в память узла обычно осуществляется специализированным программным обеспечением, например, LonMaker [11]. Для большинства узлов Neuron-чип содержит прикладную программу узла и обеспечивает протокол LonTalk. В узлах, которые используются для управления или контроля сети, прикладная программа может выполняться на персональном компьютере или микропроцессоре. Здесь мы будем рассматривать программирование приложения на языке Neuron C [12] только для узлов с Neuron-чипами версии 3150, используя программное обеспечение LonMaker, NodeBuilder [13] и специализированный стенд Mini Evaluation Kit [14]. В стенде Mini Evaluation Kit, который состоит из одного узла с Neuron-чипом версии 3150 и одного – версии 3120, узел 3120 исключен по причине малого объема памяти и заменен на аналогичный 3150.

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. LonTalk не использует кодирования в прямом смысле этого слова. Сообщение передается незакодированным, но идентичность отправителя проверяется кодом. Алгоритм кодирования представлен любым 48-битным ключом аутентификации и случайным 64-битным числом, из которых динамически вычисляется 64-битное число кодирования. Так как сообщения не кодируются, установку нового ключа аутентификации посредством команд сетевого менеджмента проводят с помощью особой функции путем прибавления некоторой величины (инкремента) к ключу аутентификации, тем самым, изменяя его без передачи явного ключа по сети. Коммуникация между узлами выполняется как посредством сетевых переменных, размером не более 31 байта, так и путем обмена явными сообщениями размером до 259 байтов. Для обмена можно выбрать тип способа передачи, при котором данные могут передаваться, если отправитель и получатель обладают одинаковым ключом аутентификации.

3. Криптографические преобразования

Первый из рассматриваемых вариантов – применение криптографического преобразования сообщений по ГОСТ 28147-89 89 [6]. В ГОСТе ключевая информация состоит из ключа размером 256 бит и таблицы замен размером 512 бит. Для применения блочного шифра к потоку информации в сети LON возможно использовать только режим гаммирования. Гаммирование – это наложение (снятие) при помощи операции побитового исключающего «ИЛИ» на открытые (зашифрованные) данные криптографической гаммы, то есть последовательности элементов данных, вырабатываемых с помощью алгоритма. Для выработки гаммы необходим начальный элемент – синхропосылка, для обратимости процедуры шифрования должна использоваться одна и та же синхропосылка, что достигается использованием предопределенного значения синхропосылки или выработкой ее синхронно источником и приемником по определенному закону. При необходимости смены значения синхропосылки у источников и приемников необходимо с помощью встроенной функции прибавить некоторую величину (инкремент) к ключу аутентификации, тем самым, изменив его и, соответственно, добившись наличия одинаковой синхропосылки у всех необходимых источников и приемников. Как вариант можно использовать генерацию случайных чисел узлом-передатчиком и безопасную отправку значения синхропосылки приемнику, зашифрованную в режиме простой замены. Аналогично можно использовать генерацию случайных чисел передатчиком для формирования сессионных ключей с последующим их шифрованием на долгосрочных ключах в режиме простой замены и безопасной их отправкой приемнику.

Второй из рассматриваемых вариантов – применение криптографического преобразования сообщений по новому алгоритму шифрования [8], который отличается от остальных тем, что вычисления производятся с определённой точностью, на основе тригонометрических функций. Особенность состоит в том, что при увеличении точности вычислений период гаммирования может достигнуть сколь угодно большого значения. Алгоритм реализован путем использования периодических функций косинуса. Вычисление тригонометрической функции относительно открытого (или зашифрованного) зна-

чения, используя ключевые параметры, фактически является гаммой, с которой осуществляется сложение исходного значения. Вычисление гаммы проводится по формулам вычисления рядов по причине отсутствия в языке встроенных тригонометрических функций.

Третий из рассматриваемых – применение алгоритмов стеганографии [9] для скрытой передачи данных. Скрываемое сообщение встраивается в потоковый контейнер в те отсчеты, искажение которых не приводит к существенным искажениям контейнера, который затем открыто, транспортируется адресату. Для уменьшения погрешности исходной открытой последовательности целесообразно искажать только ее младшие биты. В узле-получателе сети LON восстанавливается как открытая, так и скрываемая информация из передаваемой последовательности, причем открытая информация имеет определенную заранее погрешность. В литературе встречаются рекомендации по, например, шифрованию сообщения, дроблению зашифрованного сообщения на возможно мелкие части и распылению частей в пространстве по большому числу контейнеров. Повысить криптостойкость можно за счет использования пустых контейнеров, а также ложных контейнеров, в которых содержится шум [15].

Реализация указанных алгоритмов осуществляется путем внедрения специфичных функций в тело основной программы прошивки на этапе проектирования и подготовки к программированию Neuron Chip. В вариантах программы на языке Neuron C реализованы все комбинации использования ключевых данных, в том числе генерация случайных чисел, использование секретных значений ключей аутентификации, определенных в узле-приемнике и узле-передатчике на стадии проектирования, а также функции безопасного обмена ключами. В литературе при исследовании потоковых алгоритмов криптографических преобразований, при которых сообщения кодируются побайтово и без внесения избыточности, имеются рекомендации для целей защиты от накопления статистики осуществлять динамическую смену вектора инициализации потокового алгоритма. С этой целью, как вариант, после передачи каждых, например, N бит информации от источника происходит передача служебного сообщения, содержащего вектор инициализации длиной M бит [16]. Периодическая передача векторов инициализации обусловлена необходимостью защиты потокового алгоритма от сбоев синхронизации работы отправителя и получателя и от накопления статистики. В нашей реализации предусмотрена смена ключевого материала и вектора инициализации указанных алгоритмов с безопасной передачей их между узлами LON по сети.

При реализации указанных алгоритмов использовалось, для примера, зашифрование выходной сетевой переменной nvoLuxLevel из функционального профиля LightSensor [17], передача сетевой переменной по сети и последующее расшифрование входной сетевой переменной nviLuxLevel, полученной узлом-приемником из сети. Правильность реализации шифрования по ГОСТ 28147-89 в режиме простой замены проверялась на примере, приведенном в Приложении А из ГОСТ Р 34.11-94 [18]. Программные реализации указанных алгоритмов в настоящее время зарегистрированы в Федеральном институте промышленной собственности России в качестве программ для ЭВМ [19, 20, 21].

4. Анализ преобразований

Поточные шифры для генерации псевдослучайной последовательности (ПСП) – гаммы или ключевого потока – используют ключ. Такая ПСП должна быть неотличимой от истинно случайной. Существует множество статистических тестов, позволяющих обнаружить различные типы неслучайности, которые могут существовать в ПСП. Например, частотный тест определяет, является ли число единиц и нулей в двоичной ПСП приблизительно таким же, как в истинно случайной последовательности, т.е. количество единиц и нулей должно быть примерно одинаковым. Фундаментальный статистический анализ ПСП неоднократно проводился, например, в диссертационных работах [22, 23] и изданиях [24]. Программное обеспечение, ссылка на которое приведена в [24] и которое предоставлено для проведения тестирования его автором, позволяет проводить как графические, так и оценочные тесты. В отличие от графических тестов, где результаты интерпретируются пользователями, вследствие чего возможны различия в трактовке результатов, оценочные тесты характеризуются тем, что они выдают численную характеристику, которая позволяет однозначно сказать, пройден тест или нет. Набор тестов, представленных в указанном программном обеспечении, базируется на статистических тестах Д. Кнута, Diehard и NIST.

Для сбора статистики и последующего проведения тестов использовался специализированный стенд Mini Evaluation Kit [14], реализующий криптографическое преобразование сообщений с нулевым значением и их последующую передачу с темпом одно 16-битное сообщение за две секунды, а также программное обеспечение LonScanner [25], обеспечивающее перехват пакетов сети LON и их последующее сохранение в течение 12 часов, в результате чего получены несколько зашифрованных последовательностей размером 43 килобайта, по ГОСТ

28147-89 и по новому алгоритму шифрования.

Из 18 оценочных тестов наша реализация алгоритма шифрования ГОСТ 28147-89 успешно прошла 16, реализация нового алгоритма шифрования – 17. Графические тесты оказались положительными для обоих вариантов.

Заключение

При реализации алгоритмов криптографических преобразований сообщений, передаваемых в сетях LON найдено решение, позволяющее использовать указанные алгоритмы в рамках LonTalk:

- применение криптографических преобразований сообщений в сети LON;
- применение стеганографических вставок для передачи скрытой информации в LON;
- хранение долговременных ключей в памяти узлов;
- регулярная смена сессионных ключей.

Целесообразно в качестве основных секретных ключевых параметров использовать имеющиеся в узлах LON одинаковые 48-битные ключи аутентификации, а также хранить долговременный ключевой материал в памяти каждого узла. При необходимости смены значения секретных ключевых параметров у источников и приемников с помощью функции протокола LonTalk прибавляется некоторая величина к ключу аутентификации, чем обеспечивается наличие одинаковых секретных ключевых параметров у всех необходимых источников и приемников. При необходимости передачи сессионного ключевого материала по сети использовать его шифрование.

Предложенная программная реализация указанных алгоритмов криптографических преобразований в прошивках узлов LON, построенных на Neuron Chip, обеспечивает защищенную передачу, в том числе скрытую, любых значений, передаваемых в сети LON. В результате применения криптографических преобразований длина сообщений не изменяется. 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. Применение криптографических преобразований позволит исключить несанкционированное чтение информации из сетей LON и исключить возможность использования разрушительных и компрометирующих воздействий на них.

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

3. Капгер И.В. Применение криптографического преобразования сообщений в промышленных сетях LON по ГОСТ 28147-89 / И.В. Капгер, А.А. Южаков // Радіо¬електронні і комп'ютерні системи. – 2009. –7 (41). – С. 106-110.

4. Капгер И.В. Применение стеганографических вставок при передаче сообщений в промышленных сетях LON / И.В. Капгер, А.А. Южаков // Труды Международной научно-технической конференции «Информационные технологии и информационная безопасность в науке, технике и образовании "ИН-ФОТЕХ - 2009"», Севастополь, Украина, 07-12 сентября 2009 г., 2009.

5. Капгер И.В. Применение криптографических алгоритмов в сетях LON / И.В. Капгер, В.П. Сизов, А.А. Южаков // Системы мониторинга и управления: сб. науч. тр./ Перм. гос. тех. ун-т.– Пермь, 2009.

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

7. Устройство для шифрования В.П. Сизова. Патент №2331116 Россия.

8. Сизов В.П. Новый алгоритм шифрования // Вопросы защиты информации. – 2008. – № 2.

9. Грибунин В.Г. Цифровая стеганография. / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев // М.: Солон-Пресс, 2002. – 265 с.

10. Терехов А.Н. Предложение по реализации основных криптографических алгоритмов в заказных кристаллах / А.Н. Терехов, В.Л. Богданов // Проблемы информационной безопасности. Компьютерные системы. 1999. – № 1. – С. 88–94.

11. LonMaker User's Guide. Release 3.1 Revision 2, Echelon Corporation, 2003, 302 p.

12. NEURON C: Руководство для программиста. Пер. с англ. / Рус.-австр. центр FIELDBUS технологий. – Пермь: Изд-во ПГТУ, 1999. – 340 с.

13. NodeBuilder® User's Guide. Release 3.1 Revision 3, Echelon Corporation, 2003, 378 p.

14. Mini EVK User's Guide. Revision 3, Echelon Corporation, 2006. – 96 p.

15. Алексеев А.П. Сокрытие сообщений путем их распыления в пространстве. / А.П. Алексеев, В.В. Орлов // «Инфокоммуникационные технологии». – 2008. – Т. 6. – № 3. – С. 52–56.

16. Никитин В.Н. Влияние механизмов защиты на пропускную способность каналов с ошибками / В.Н. Никитин, Д.В. Юркин // Защита информации. Inside, – 2009, №3.

17. LONMARK® Functional Profile: Light Sensor. Version 1.1, LONMARK Interoperability Association, 1997. – 9 p.

18. ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования. – М.: Госстандарт России, 1994. – 16 с.

19. Программа «Реализация криптографического преобразования сообщений, передаваемых в промышленных сетях LON, по ГОСТ 28147-89». Свидетельство о государственной регистрации программы для ЭВМ №2009616305, опубл. 13.11.2009.

20. Программа «Реализация криптографического преобразования сообщений, передаваемых в промышленных сетях LON, по алгоритму шифрования В.П. Сизова». Свидетельство о государственной регистрации программы для ЭВМ №2010610256, опубл. 11.01.2010.

21. Программа «Реализация применения стеганографических вставок в сообщениях, передаваемых в промышленных сетях LON». Свидетельство о государственной регистрации программы для ЭВМ №2010610255, опубл. 11.01.2010.

22. Фионов А.Н. Эффективные методы построения идеальных криптографических систем защиты информации: Дис. ... доктора техн. наук: 05.12.13. – Новосибирск, 2005. – 241 с. РГБ ОД, 71 06-5/403.

23. Чугунков И.В. Разработка и исследование алгоритмов генерации псевдослучайных последовательностей для компьютерных систем ответственного назначения: Дис. ... канд. техн. наук: 05.13.11, 05.13.19 : – Москва, 2003. – 184 с. РГБ ОД, 61:04-5/2070.

24. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.

25. LonScanner Protocol Analyzer User's Guide, Echelon Corporation, 2005. – 78 p.

Поступила в редакцию 25.02.2010

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

РЕАЛІЗАЦІЯ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ ПОВІДОМЛЕНЬ В СИСТЕМАХ УПРАВЛІННЯ ПРОМИСЛОВИХ МЕРЕЖ LON ІНТЕЛЕКТУАЛЬНИХ БУДІВЕЛЬ

І.В. Капгер, Ол-р А. Южаков, Ол-й О. Южаков

Досліджені проблеми промислових мереж LON, використовуваних для побудови інтелектуальних систем життєзабезпечення будівель, пов'язане із захистом від несанкціонованих дій. Розглянуті можливості підвищення надійності і достовірності повідомлень, передаваних в промислових мережах LON, включаючи методи аутентифікації вузлів, шифрування повідомлень, використання стеганографіческих вставок. Запропоновані реалізації алгоритмів шифрування і стеганографії в рамках протоколу Lontalk. Досягнуті результати дозволяють виключити несанкціоноване читання інформації з промислових мереж LON і унеможливити використання руйнівних і компрометуючих дій на них.

Ключові слова: інтелектуальна будівля, LON, Lonworks, Lontalk, промислові шини, надійність, достовірність, аутентифікація, шифрування, стеганографія.

IMPLEMENTATION OF CRYPTOGRAPHIC CONVERSIONS OF THE MESSAGES IN CONTROL SYSTEMS OF INDUSTRIAL LON NETWORKS OF INTELLECTUAL BUILDINGS

I.V. Kapger, Al-r A. Yuzhakov, Al-y A. Yuzhakov

The problems of the industrial LON network used for construction of intellectual life-support systems of buildings, related to the protection from unauthorized actions were re-searched. Possibilities of increasing reliability and authenticity of the messages transferred in industrial networks LON, including methods of authentification of sites, enciphering of messages, usages steganographic insertions are considered. Implementations of algorithms of enciphering and steganography within the limits of LonTalk protocol are offered. The reached results allow to eliminate unapproved reading of the information from industrial networks LON and to eliminate possibility of usage of destructive and compromising effects on them.

Key words: intellectual building, LON, LonWorks, LonTalk, industrial buses, reliability, validity, authenticity, encryption, steganography.

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.

Южаков Алексей Александрович – аспирант кафедры автоматики и телемеханики Пермского государственного технического университета, Пермь, Россия, e-mail:uzalex84@mail.ru.