УДК 004.056: 061.068

ШИФРОВАНИЕ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ХАОТИЧЕСКОЙ ДИНАМИКИ В СЕНСОРНОЙ СЕТИ

А.В. СИДОРЕНКО, К.С. МУЛЯРЧИК

Белорусский государственный университет
Независимости, 4, 220050, Минск, Беларусь

Поступила в редакцию 10 марта 2015

Приводится структурная схема передачи зашифрованной информации в беспроводной сенсорной сети. Алгоритм шифрования основан на схеме блочного симметричного алгоритма и использует хаотические системы и отображения. Алгоритм шифрования на динамическом хаосе имеет преимущества: увеличение степени защиты информации о маршрутизации, надежности и пропускной способности передачи данных, что расширяет функциональные возможности в решении криптографических задач. Аппаратно-программное обеспечение реализуется в сверхширокополосных приемопередатчиках типа ППС-40А. Особенности программной и аппаратной реализации алгоритма приводятся. Выполнена инсталляция программного обеспечения в микроконтроллеры приемопередатчиков ППС-40А. Приводятся характеристики программного кода микроконтроллера приемопередатчика до и после реализации функции шифрования.

Ключевые слова: шифрование, информация, алгоритм, хаотическая динамика.

Введение

В настоящее время интенсивное развитие получает «концепция Интернет-вещей» – концепция вычислительной сети физических объектов («вещей»), оснащенных встроенными технологиями для взаимодействия друг с другом или с внешней средой. При этом организация таких сетей возможна как в области экономики, так и в развитии общественных отношений.

В рамках данной концепции можно выделить особый класс сетей – беспроводные сенсорные сети, которые используются преимущественно для решения широкого круга задач мониторинга и управления [1, 2]. Эти сети являются распределенными и самоорганизующимися и состоят из множества миниатюрных узлов (сенсоров). Основным требованием, предъявляемым к узлам такой сети, является длительное время их автономной работы, что приводит к использованию в них элементов с малыми вычислительными возможностями и режимов работы с низким энергопотреблением. Так, объем памяти микроконтроллера, используемого в таких устройствах, как правило, находится в пределах 1–4 Кбайт, а частота его работы составляет 8–20 МГц [3].

Наиболее важной задачей защиты информации при разработке систем передачи на базе беспроводных сенсорных сетей является обеспечение конфиденциальности передаваемых данных. В отсутствие данной возможности, злоумышленник может перехватывать и обрабатывать передаваемые по сети пакеты с целью извлечения такой информации, как идентификаторы узлов или непосредственно передаваемые данные, что возможно в силу широковещательной природы беспроводных сенсорных сетей [4].

Зашифрованная передача информации в сенсорной сети

Задача обеспечения конфиденциальности передаваемых по сети данных решается внедрением функций шифрования непосредственно в приемопередатчики, что позволяет

установить безопасное соединение между отдельными приемопередатчиками и передавать друг другу информацию, которая не может быть перехвачена «внешними наблюдателями».

Типичный пример взаимодействия устройств в беспроводной сенсорной сети включает в себя следующую последовательность действий (рис. 1).

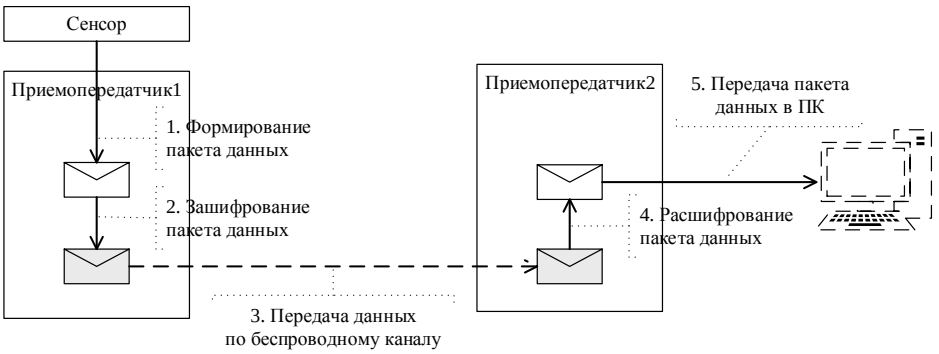


Рис. 1. Схема зашифрованной передачи информации в сенсорной сети

Приемопередатчик 1 производит снятие текущих показателей с сенсора и формирует информационный пакет для отправки в эфир, зашифровывает его, используя текущие в узле настройки шифрования, и отправляет в эфир. Приемопередатчик 2 принимает пакет из эфира, расшифровывает его, используя текущие в узле настройки шифрования, и осуществляет его дальнейшую обработку: передачу в компьютер или дальнейшую ретрансляцию в эфир.

Следует отметить, что функция шифрования данных в приемопередатчике осуществляет шифрование всего тела пакета данных целиком, не затрагивая при этом заголовок пакета и байты контрольной суммы. Выбор такой схемы преобразования продиктован необходимостью защиты информации о маршрутизации, поскольку одной из целей пассивного прослушивания является извлечение идентификаторов узлов, что позволит построить схему маршрутизации и выявить расположение узлов в сети.

Таким образом, шифрование на физическом уровне позволяет осуществлять безопасную передачу информации между узлами сети, устраняя возможность пассивного прослушивания и связанных с ним атак.

Установлено, что для обеспечения функции шифрования в приемопередатчиках сенсорных сетей следует использовать блочный симметричный алгоритм шифрования, с одной стороны, требующий для своей реализации не более 25 % доступного объема оперативной памяти микроконтроллера, а с другой стороны, позволяющий легко изменять длину блока текста, что будет способствовать повышению надежности передачи и увеличению полезной пропускной способности канала связи при передаче зашифрованной информации. Дополнительным требованием является предельный объем программного кода – 10 % от доступной памяти для хранения программ.

Существующие алгоритмы шифрования, такие как СТБ 34.101.31-2007 (BelT), AES, ГОСТ 28147-89, DES и другие, обладая известными достоинствами, не соответствуют описанным выше требованиям и не подходят для реализации в беспроводных сенсорных сетях. Основными причинами тому являются отсутствие в приемопередатчиках достаточного объема памяти для функционирования алгоритма шифрования, низкая вычислительная мощность устройства, при которой временная продолжительность процесса шифрования оказывается достаточно высокой, ограниченные коммуникационные возможности. Так, примерный объем оперативной памяти микроконтроллера, необходимый для реализации алгоритма BelT, составляет от 544 до 1152 байт.

Алгоритм шифрования на основе хаотической динамики

Для обеспечения функции шифрования данных в приемопередатчиках, с учетом вышеизложенного, разработан новый алгоритм шифрования, использующий в своей основе принципы динамического хаоса, а именно – хаотические отображения. Так, хаотические отображения являются «дешевыми» с точки зрения потребности в вычислительных ресурсах. В силу своей нелинейности такие отображения являются хорошими кандидатами на

использование вместо таблиц подстановки (в традиционных алгоритмах), что значительно снижает требования к объему оперативной памяти. Кроме этого, выражение для вычисления хаотического отображения инвариантно по отношению к множеству, на котором определены его аргументы, что позволяет использовать одну и ту же структуру отображения для реализации различных его вариантов в зависимости от доступности ресурсов. А это приводит к возможности изменять длину блока в алгоритме шифрования.

В основу структуры разработанного блочного симметричного алгоритма шифрования с использованием хаотической динамики (рис. 2) положена итеративная схема Шеннона, в которой в качестве базового преобразования использована сеть Фейстеля.

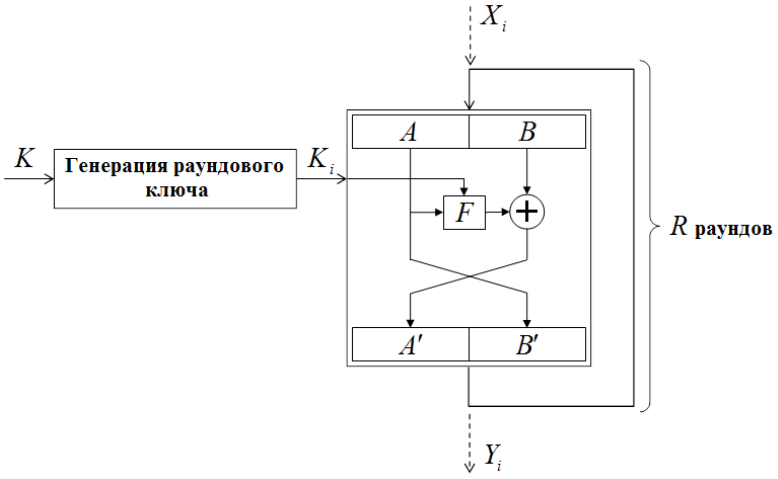


Рис. 2. Схема алгоритма шифрования на основе динамического хаоса с использованием сети Фейстеля

Принципиальным отличием разработанного алгоритма от известных, основанных на сети Фейстеля, является использование в качестве нелинейного блока F дискретного хаотического отображения – преобразования, заданного на конечном целочисленном множестве мощностью M, обладающего хаотической динамикой и управляемого параметром (раундовым ключем) K_i:

$$F = F(A, K_i, M), \quad (1)$$

где A – входное значение отображения (левый входной подблок в сети Фейстеля); K_i – управляющий параметр отображения; M – мощность множества, на котором определено отображение.

Можно выделить следующие преимущества использования дискретных хаотических отображений вместо таблиц подстановки в алгоритмах шифрования, ориентированных на применение в устройствах с ограниченными ресурсами.

1. Уменьшение объема оперативной памяти, требуемой для реализации алгоритма шифрования ввиду отсутствия необходимости хранения таблиц подстановки. В современных традиционных алгоритмах шифрования размер таблиц подстановки достигает 70 % всего объема памяти, необходимой для реализации алгоритма шифрования.

2. Возможность менять мощность множества, на котором определено нелинейное преобразование (дискретное хаотическое отображение), что влечет за собой возможность устанавливать необходимую длину ключа и длину обрабатываемого блока текста, например, 32 бита, 64 бита и т.д.

Другими словами, дискретное хаотическое отображение можно представить как совокупность множества различных таблиц подстановки, причем выбор и использование конкретной таблицы зависит от значения управляющего параметра.

Также отметим, что, поскольку раундовый ключ непосредственно является неотъемлемой частью нелинейного преобразования (дискретного хаотического отображения), а не складывается побитно с блоком текста, дифференциальный криптоанализ такого преобразования затрудняется. Кроме этого, конкретный вид нелинейного преобразования, реализуемого дискретным хаотическим отображением, определяется значением раундового ключа на каждом раунде базового преобразования. Все это в целом способствует повышению криптостойкости разработанного алгоритма шифрования.

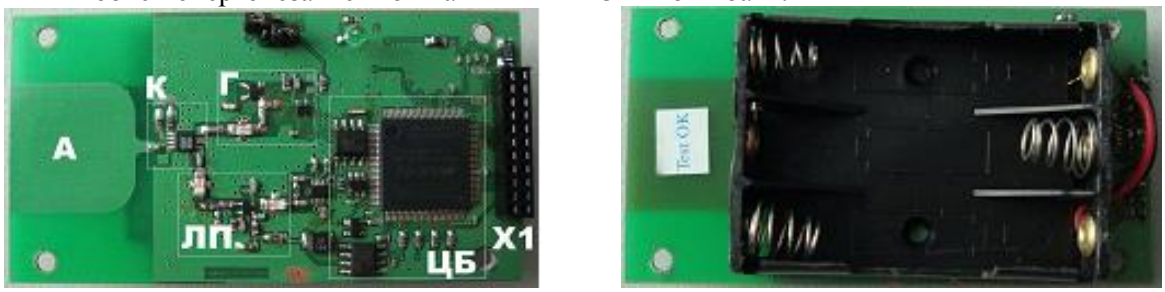
Совместное использование в разработанном алгоритме шифрования таких структурных элементов, как итеративная схема Шеннона, сеть Фейстеля и дискретное хаотическое отображение, делает возможным выбор и установление требуемой длины ключа шифрования и длины блока обрабатываемого текста, при этом длина блока текста должна быть кратна двум. Это является существенным преимуществом разработанного алгоритма при его использовании в узлах беспроводной сенсорной сети, поскольку в зависимости от характера передаваемой информации (размера пакета), а также условий передачи (например, зашумленность канала, вероятность возникновения ошибки при передаче) может выбираться та или иная длина блока текста [5, 6].

Аппаратно-программная реализация алгоритма шифрования

Аппаратно-программная реализация предложенного алгоритма шифрования была выполнена на базе сверхширокополосных прямохаотических приемопередатчиков серии ППС-40А, используемых в качестве узлов при построении беспроводных сенсорных сетей. Внешний вид и структурная схема приемопередатчика серии ППС-40А представлены на рис. 3 и 4 соответственно, а технические характеристики приведены в табл. 1.

Центральным узлом цифрового блока является микроконтроллер Atmel ATmega 168, обладающий следующими характеристиками:

– 8-разрядная архитектура;
– тактовая частота – до 20 МГц;
– объем памяти для хранения данных (RAM) – 1 Кбайт;
– объем памяти для хранения программного кода (ROM) – 16 Кбайт;
– объем энергонезависимой памяти EEPROM – 512 байт.



а *б*

Рис. 3. Приемопередатчик для беспроводных сенсорных сетей: *а* – вид сверху; *б* – вид снизу

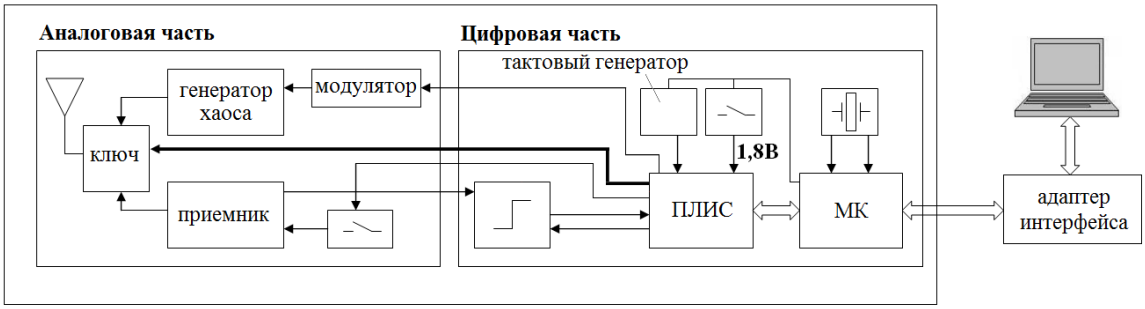


Рис. 4. Структурная схема приемопередатчика серии ППС-40А

Таблица 1. **Технические характеристики приемопередатчика**

Наименование характеристики	Значение
Полоса выходного сигнала	3,1–5,1 ГГц
Средняя мощность излучаемого сигнала (скорость 2,5 Мбит/с)	–10 дБм
Средняя мощность излучаемого сигнала (скорость 0,1 Мбит/с)	–21 дБм
Дальность приема	до 20 м
Физическая скорость передачи/приема данных	2,5/2,5 Мбит/с
Интерфейс сопряжения с ПК и датчиками	UART
Напряжение питания	4,5 В

На основании анализа приведенных характеристик можно заключить, что приемопередатчик серии ППС-40А относится к классу устройств с ограниченными ресурсами и коммуникационными возможностями, а, следовательно, для обеспечения в нем функций шифрования требуется использовать специально предназначенные для этого алгоритмы, к числу которых относится разработанный алгоритм шифрования.

Для проверки работоспособности алгоритма, а также получения его количественных характеристик было проведено компьютерное моделирование реализации разработанного алгоритма шифрования для 8-разрядных микроконтроллеров Atmel. Результаты исследования количественных характеристик данной реализации разработанного алгоритма шифрования в зависимости от размера блока текста приведены в таблицах 2, 3.

Таблица 2. **Характеристики реализации алгоритма шифрования в режиме работы CFB на эмуляторе 8-разрядных микроконтроллеров Atmel**

Размер блока текста, байт	Объем памяти для хранения данных, байт		Количество тактов микроконтроллера для зашифрования блока текста	
	суммарный	на один байт блока текста	суммарное	на один байт блока текста
4	223	56	12911	3228
8	241	30	14167	1771
12	259	22	15423	1285
16	277	17	16679	1042
20	295	15	17935	897
24	313	13	19191	800
28	331	12	20447	730
32	349	11	21703	678

Таблица 3. **Максимальная скорость обработки данных алгоритмом шифрования в зависимости от тактовой частоты микроконтроллера и размера блока текста**

Размер блока текста, байт	Максимальная скорость обработки данных алгоритмом шифрования (Кбит/с) при частоте микроконтроллера			
	5 МГц	10 МГц	15 МГц	20 МГц
4	12,1	24,2	36,3	48,4
8	22,1	44,1	66,2	88,2
12	30,4	60,8	91,2	121,6
16	37,5	74,9	112,4	149,9
20	43,6	87,1	130,7	174,2
24	48,9	97,7	146,6	195,4
28	53,5	107,0	160,5	214,0
32	57,6	115,2	172,8	230,4

Объем памяти для хранения программного кода не изменяется в зависимости от размера блока текста и равен 762 байтам. В целом приведенные скоростные характеристики соответствуют типичным скоростным характеристикам беспроводных сенсорных сетей, в которых «брутто» скорость (включая служебную информацию) составляет порядка 250 Кбит/с, а средняя скорость передачи полезных данных, в зависимости от загрузки сети и числа ретрансляций, составляет от 5 до 40 Кбит/с. Использование предложенной реализации разработанного алгоритма шифрования обеспечивает уменьшение требуемого для реализации алгоритма объема памяти в микроконтроллере как минимум в два раза по сравнению с алгоритмом шифрования BelT, в 3,5 раза по сравнению с алгоритмом AES и в 4,9 раз по сравнению с алгоритмом ГОСТ 28147-89.

Аппаратно-программная реализация алгоритма шифрования

Для экспериментального исследования реализуемых средств защиты была построена опытная беспроводная сенсорная сеть, использующая в качестве узлов приемопередатчики серии ППС-40А. Обобщенная структура такой сети представлена на рис. 5. Сеть организована таким образом, что в ней осуществляется однонаправленная передача данных от сенсорных узлов к координатору сети (базовой станции) напрямую либо через промежуточные узлы – ретрансляторы [7].

В ходе экспериментальной проверки разработанной аппаратно-программной реализации алгоритма шифрования была выполнена инсталляция (прошивка) разработанного программного обеспечения в микроконтроллеры приемопередатчиков серии ППС-40А. Было проанализировано изменение характеристик программного кода микроконтроллера приемопередатчика до и после реализации функции шифрования. Результаты анализа представлены в табл. 4.

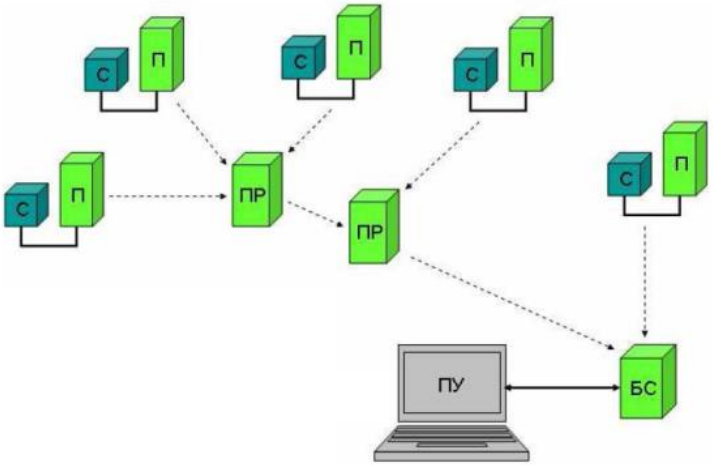


Рис. 5. Структура беспроводной сенсорной сети

Таблица 4. **Характеристики реализации функции шифрования в микроконтроллере приемопередатчика**

Объем памяти для хранения:	До реализации	После реализации	Изменение (увеличение)
– программного кода, байт	3194	4190	996
– данных в RAM, байт	427	476	49
– данных в EEPROM, байт	20	28	8

Заключение

Результаты выполнения работы сводятся к следующему/

1. Приведена структурная схема передачи зашифрованной информации в сенсорной сети. В указанной схеме обеспечивается защита передаваемой информации о маршрутизации, повышении надежности передачи и увеличение полезной пропускной способности данных.

2. Предложен блочный симметричный алгоритм шифрования на основе динамического хаоса, в котором обоснованно используется сеть Фейстеля в качестве базового преобразования.

3. Аппаратно-программная реализация алгоритма шифрования осуществляется на базе сверхширокополосных приемопередатчиков серии ППС-40А. Выполнена инсталляция разработанного программного обеспечения в микроконтроллеры приемопередатчиков. Приведены характеристики программного кода микроконтроллера приемопередатчика до и после реализации функции шифрования.

DATA ENCRYPTION USING THE CHAOTIC DYNAMICS IN WIRELESS SENSOR NETWORKS

A.V. SIDORENKO, K.S. MULYARCHIK

Abstract

The block-diagram for transmission of the encrypted information in wireless sensor networks is presented. For the encryption algorithm based on the symmetric algorithmic diagram the chaotic systems and maps are used. The dynamic chaos based encryption algorithm features the advantages (higher level of defense of the information about the routing; better reliability and data carrying capacity) which extend the scope of the cryptographic problems solved. The hardware and the software are realized with an ultra wideband transmitter- receiver of the PPS-40A type. Installation of

the software in microcontroller of the PPS-40A type transmitter-receiver is illustrated. The characteristics of the transmitter-receiver microcontroller code before and after the encryption function realization are given. The peculiarities in implementation of the hard- and software for the encryption algorithm are considered.

Список литературы

1. *Панасенко С., Смагин С.* // Мир ПК. 2011. № 7. С. 50–52.
2. *Сидоренко А.В., Мулярчик К.С., Ходасевич А.И. и др.* // Матер. 7-й Междунар. науч.-техн. конф. «Приборостроение –2014». Минск, 19–21 ноября 2014. С. 379–380.
3. *Yick J., Mukherjee B., Ghosal D.* // Computer Networks. 2008. № 52. P. 2292–2330.
4. *Алферов А.П.* Основы криптографии. М., 2002.
5. *Сидоренко А.В., Мулярчик К.С.* // Докл. БГУИР. 2013. № 1. С. 62–67.
6. *Дмитриев А.С., Сидоренко А.В., Андреев Ю.В. и др.* // Электроника инфо. № 6. 2013. С. 36–37.
7. *Дмитриев А.С., Ефремова Е.В., Клецов А.В. и др.* // Радиотехника и электроника. 2008. № 53 (10). С. 1278–1289.