УДК 621.396.41

М.М. Антонов, А.А. Конев, Д.С. Никифоров, С.А. Черепанов

Организация защищенной гетерогенной сети в автоматизированных системах коммерческого учета энергоресурсов

Создание автоматизированной системы для ЖКХ является сложной задачей. Такая система размещается на большой территории и должна отвечать высоким требованиям по надежности работы. Одной из проблем является обеспечение безопасности информации, обрабатываемой системой. В данной статье описываются подходы к решению задач, связанных с реализацией протоколов передачи данных между гетерогенными узлами автоматизированной системе коммерческого учета энергоресурсов, аутентификации и добавления в базу этих узлов.
Ключевые слова: маршрутизация, аутентификация, автоматизированная система коммерческого учета энергоресурсов, базы данных, гетерогенные сети, eap-psk.
doi: 10.21293/1818-0442-2016-19-3-107-110

В настоящее время существует потребность в недорогой, простой в обслуживании, надежной и функциональной автоматизированной системе коммерческого учета энергоресурсов (АСКУЭ) для бытовых потребителей. Создание аппаратно-программного комплекса (АПК) сбора данных о потребляемых энергоресурсах с приборов учета на базе российских электронных компонентов позволит решить проблему комплексного импортозамещения. Гетерогенная организация сети позволит многократно увеличить достоверность передачи данных. Задача создания такой АСКУЭ осложняется двумя факторами – большим количеством узлов учета конечных потребителей и рассредоточением их на значительной территории, что существенно затрудняет доступ к ним через ставшие традиционными каналы передачи данных типа витая пара и интерфейс RS-485.

Проблема гетерогенности каналов связи

Для связи устройств учета энергоресурсов (УУЭ) с устройством сбора и передачи данных (УСПД) используются PLC- и RF-каналы связи (рис. 1). Полученная в итоге сеть является сетью с гетерогенными каналами связи и различными по своему типу узлами. В частности, узлами могут являться устройства учета таких энергоресурсов, как электроэнергия, горячая и холодная вода, тепло и т.п. К данной сети предъявлены следующие требования:

1) в сети может быть до 512 устройств. Это позволяет использовать УСПД как для обслуживания подъезда, так и для целого дома в зависимости от количества квартир;

2) сеть должна быть немобильной, т.к. УУЭ являются стационарными устройствами;

3) каналы связи должны быть гетерогенными (гетерогенными являются каналы, которые могут передавать данные по одной из нескольких доступных на выбор физических сред);

4) должна быть обеспечена гарантия доставки данных, т.к. данные, передающиеся по сети, являются коммерчески важными;

5) устройства в сети должны взаимодействовать по протоколу 6LoWPAN [1], т.к. это увеличит совместимость системы с УУЭ сторонних производителей;

6) должна быть возможность быстрого добавления новых типов устройств.

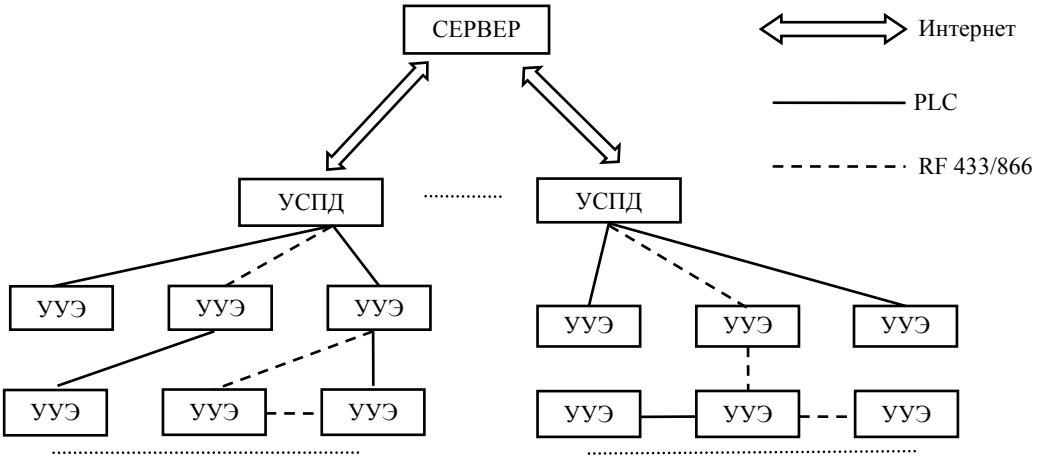

Рис. 1. Система с гетерогенными каналами связи

В ходе реализации задачи создания защищенной гетерогенной сети в АСКУЭ было проведено тестирование прототипа. Нами были выявлены следующие недостатки:

– низкая надежность доставки данных между узлами системы, расстояние между которыми превышает 15 м;

– проблема обеспечения информационной безопасности;

– проблема добавления в систему узлов новых типов.

Для решения данных проблем были поставлены задачи:

– разработка протокола маршрутизации данных в сети с гетерогенными каналами связи;

– разработка протокола аутентификации устройств внутри сети с гетерогенными каналами связи;

– разработка гибкого механизма добавления новых типов устройств в сеть с гетерогенными каналами связи.

Для обеспечения надежной доставки передаваемой информации необходима быстрая и надежная маршрутизация данных. Стандартные протоколы, как дистанционно-векторные (например, RIP, EIGRP), так и протоколы состояния канала связи (например, OSPF, IS-IS), не справляются с задачей, т.к. генерируют чрезмерное количество служебного трафика [2].

При этом некоторые протоколы маршрутизации, такие как Better Approach To Mobile Ad hoc Networking (B.A.T.M.A.N.), Optimized Link State Routing Protocol (OLSR), Babel и Dynamic Source Routing (DSR), могут частично решить вышеописанную задачу.

В таблице представлена степень удовлетворения рассмотренными протоколами ограничений, налагаемых требуемым типом сети. Если протокол удовлетворяет условию, в соответствующей ячейке ставится знак «+», иначе – знак «–».

Соответствие протоколов условиям сети

Протокол	Ограничения					
	1	2	3	4	5	6
BATMAN	+	+	–	+	–	–
OLSR	+	+	–	+	–	–
Babel	+	+	+	+	–	–
DSR	+	+	–	–	+	–

Таким образом, можно сделать выводы о необходимости разработки нового протокола маршрутизации.

В процессе работы был создан протокол маршрутизации в сетях с гетерогенными каналами связи «MI-LAN». Протокол поддерживает возможность передачи данных через промежуточные узлы как ретрансляторы [3], что позволяет надежно передавать данные на расстояния, большие, чем доступны при передаче данных от узла к узлу напрямую.

Моделирование показало, что сеть «MI-LAN» обеспечивает надежную передачу данных от узла к узлу на расстоянии до 500 м.

Обеспечение безопасности передаваемой информации

Для обеспечения безопасности информации, обрабатываемой системой, необходимо предусмотреть процедуры идентификации и аутентификации для всех устройств сети. АСКУЭ является распределенной системой, компоненты которой включают в себя устройства сбора и передачи данных (УСПД) и устройства учета энергоресурсов (УУЭ). Данные устройства устанавливаются на объектах, которые необходимо контролировать. Такими объектами могут быть как промышленные предприятия, использующие АСКУЭ для контроля технических процессов, так и жилые дома, в которых необходимо рассчитать стоимость жилищно-коммунальных услуг. И если в первом случае АСКУЭ устанавливается в пределах контролируемой зоны, то во втором система распространяется на целые городские кварталы, используя существующую инфраструктуру для связи компонентов. В данном случае нет возможности контролировать все линии связи и устройства, которые используются в системе. УСПД передает данные на центральный сервер по существующим каналам связи. Для связи УУЭ с УСПД используется сеть с гетерогенными каналами связи «MI-LAN».

Проблема заключается в том, что устройства никак не контролируют ту информацию, которую получают. Таким образом, гарантировать достоверность информации, получаемой от УУЭ, невозможно. Более того, невозможно даже гарантировать того, что информация получена именно от УУЭ, а не от какого-либо несанкционированного устройства. Это позволяет искажать показания УУЭ, выводить из строя сеть «MI-LAN» либо привести к полному отказу работы системы и, как следствие, является серьезной проблемой.

Чтобы обеспечить должный уровень безопасности, необходимо предусмотреть процедуру аутентификации устройств в АСКУЭ, то есть создать перечень устройств, используемых в системе, и обеспечить процедуру идентификации и аутентификации этих устройств [4]. Внутри сети «MI-LAN» необходимо обеспечить процедуру шифрования всего трафика, необходимо обеспечить аутентификацию УСПД на серверах АСКУЭ.

Для идентификации и аутентификации устройств разрабатывается протокол аутентификации на базе EAP-PSK. Данный протокол использует предустановленный 128-битный ключ PSK в качестве секрета. Время жизни данного ключа считается неограниченным ввиду специфики его использования. Во время работы протокола происходит процедура взаимной аутентификации [5] сторон и установления между ними защищенного канала, обеспечивающего контроль целостности и конфиденциальность [6] передаваемой по нему информации. Процедура аутентификации EAP-PSK состоит из 2 раундов обмена сообщениями (рис. 2).

Протокол EAP-PSK можно использовать для взаимной аутентификации двух устройств, соеди-

ненных между собой напрямую, либо через другие устройства (в таком случае промежуточные устройства используются как ретрансляторы). Также для снятия нагрузки с устройств функции аутентифицирующей стороны можно вынести на отдельный сервер аутентификации.

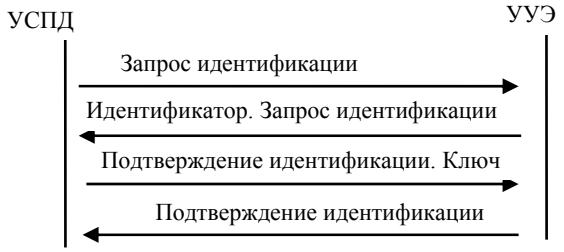

Рис 2. Раунды обмена сообщениями во время процедуры аутентификации EAP-PSK

Отличие разрабатываемого протокола от оригинального EAP-PSK состоит в том, что протокол может работать поверх различных типов каналов связи (что позволяет использовать его в сети «MI-LAN») и с различными типами устройств.

По защищенному каналу, установленному во время аутентификации устройств, производится передача ключа шифрования, общего для всех устройств внутри сети «MI-LAN». На этом ключе производится шифрование всего трафика внутри сети. Срок жизни данного ключа составляет 30 дней. Генерация и распределение новых ключей происходит автоматически.

Такой подход позволит предотвратить внедрение в систему неавторизованных устройств, «прослушивание» сети «MI-LAN», подделку пакетов сети.

Гетерогенность данных

Проблема добавления новых узлов в сеть заключается в том, что гетерогенность в системе представлена не только организацией сети, но и типом собираемых, хранимых и обрабатываемых данных [7].

Для решения данной проблемы необходимо спроектировать базу данных, которая будет учитывать особенности сбора и хранения разнородных данных. Также такая база данных должна быть масштабируемой и расширяемой.

Спроектированная база данных должна удовлетворять требованиям, предъявляемым к центральному серверу, на котором она будет располагаться.

Исходя из требований к аппаратной части центрального сервера и требований в обслуживании 10000 УСПД и 255 счетчиков на каждый УСПД, в минимальной конфигурации сервера, объем дискового пространства, занимаемого базой данных, не должен превышать 500 Гб.

На основе проведенного исследования и поставленных требований была создана модель базы данных центрального сервера (рис. 3) [8].

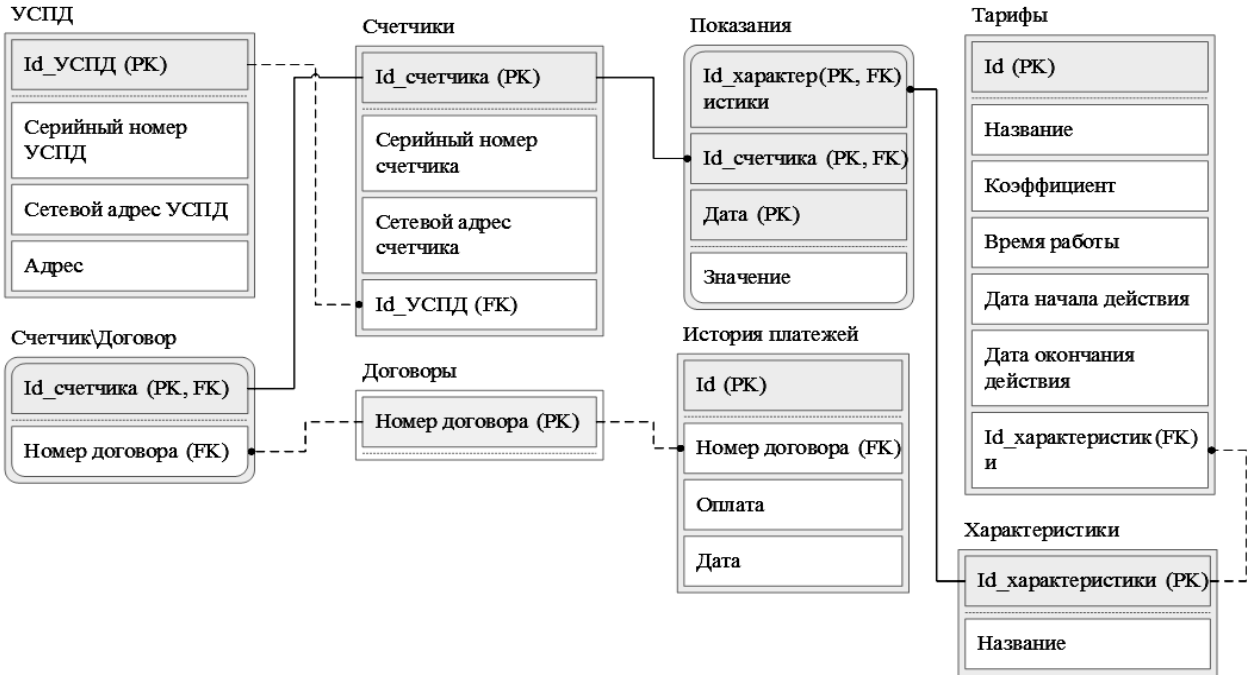

Рис. 3. Модель базы данных

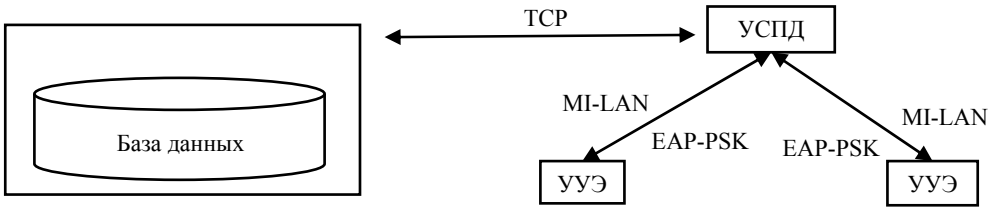

Рис. 4. Структура системы после внедрения сети «MI-LAN»

Одним из решений при проектировании БД является разделение таблиц показаний и типов показаний; таким образом, можно записывать и хранить показания, не привязываясь к их типу. Это позволяет добавлять или убирать из системы обработку любых типов собираемых данных.

Следующим решением в БД является отсутствие прямой привязки УУЭ к такой характеристике, как тип учитываемых ресурсов. Они привязаны только к договору, а уже договор учитывает тип ресурсов и всю остальную информацию, необходимую для дальнейшей обработки данных в системе.

Заключение

Структура системы с учетом доработок представлена на рис. 4.

В ходе работы были разработаны протоколы маршрутизации и аутентификации для сети с гетерогенными каналами связи «MI-LAN».

Сеть «MI-LAN» используется для связи УСПД и УУЭ. Помимо протоколов маршрутизации MI-LAN и аутентификации устройств, сеть «MI-LAN» включает в себя базу данных, позволяющую при необходимости добавлять правила взаимодействия с устройствами новых типов. Протокол маршрутизации «MI-LAN» обеспечивает надежную передачу данных между узлами сети, расположенными на расстоянии до 500 м друг от друга. Протокол аутентификации устройств обеспечивает надежную аутентификацию всех устройств в сети «MI-LAN», а также предоставляет защищенный канал связи во время аутентификации устройств, по которому передается общий для всей сети ключ шифрования.

Прототип данной системы внедрен и успешно эксплуатируется в жилом доме.

Работа выполнена при финансовой поддержке Минобрнауки РФ по контракту № 02.G25.31.0107 от 14 августа 2014 г.

Литература

1. Recommendation ITU-T G.9903: Narrowband orthogonal frequency division multiplexing power line communication transceivers for G3-PLC networks [Электронный ресурс]. – Режим доступа: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-G.9903-201402-I!!PDF-E&type=items (дата обращения: 09.03.2016).

2. Murray D. An experimental comparison of routing protocols in multihop ad hoc networks / D. Murray, M. Dixon, T. Koziniec // Australasian Telecommunication Networks and Applications Conference. – Australasia: IEEE, 2010. – P. 159–164.

3. Маршрутизация в беспроводных мобильных ad hoc-сетях / В.М. Винокуров, А.В. Пуговкин, А.А. Пшеников и др. // Доклады Том. гос. ун-та систем управления и радиоэлектроники. – 2010. – № 2 (22), ч. 1. – С. 288–292.

4. Шелупанов А.А. Требования к системам аутентификации по уровням строгости / А.Г. Сабанов, А.А. Шелупанов, Р.В. Мещеряков // Ползуновский вестник. – 2012. № 2–1. – С. 61–67.

5. Никифоров Д.С. Механизм защищенного взаимодействия устройства сбора и передачи данных с сервером сбора данных в автоматизированной системе коммерческого учета энергоресурсов // Электронные средства и системы управления. – 2015. – № 1, ч. 2. – С. 180–184.

6. Конев А.А. Оценка качества защищенности компьютерных сетей / А.А. Конев, А.К. Новохрестов // Динамика систем, механизмов и машин. – 2014. – №4. – С. 85–87.

7. Атре Ш. Структурный подход к организации баз данных – М.: Финансы и статистика, 1983. – 317 с.

8. Дейт К. Дж. Введение в системы баз данных. – М.: Вильямс, 2001. – 1072 с.

Антонов Максим Михайлович
Аспирант каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа
Тел.: +7-999-620-15-23
Эл. почта: amm@csp.tusur.ru

Конев Антон Александрович
Канд. техн. наук, доцент каф. КИБЭВС
Тел.: (382-2) 70-15-29, доб. 2980
Эл. почта: kaa1@keva.tusur.ru

Никифоров Дмитрий Сергеевич
Аспирант каф. КИБЭВС
Тел.: +7-999-620-20-64
Эл. почта: nds@csp.tusur.ru

Черепанов Сергей Андреевич
Аспирант каф. КИБЭВС
Тел.: +7-923-424-59-74
Эл. почта: sivkinpunk@gmail.com

Antonov M.M., Konev A.A.,
Nikiforov D.S., Cherepanov S.A.

Development of a protected network for an automated system of energy control and accounting

Creation of automated systems for housing and communal services is a challenge. Such a system is located in a large area, and must meet high reliability standards. One of the problems is the security of information processed by the system. This article explains the approaches to problem solving, when creating such a network.

Keywords: routing, authentication, ASCAE, databases, heterogeneous networks, eap-psk.