УДК 004.056

ПОДХОД К УПРАВЛЕНИЮ МАРШРУТИЗАЦИЕЙ В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ ЦИФРОВОГО ПРОИЗВОДСТВА

А.Д. Дахнович
Санкт-Петербургский политехнический университет Петра Великого
Россия, 194064, Санкт-Петербург, ул. Политехническая, 29
E-mail: add@ibks.spbstu.ru

Д.А. Москвин
Санкт-Петербургский политехнический университет Петра Великого
Россия, 194064, Санкт-Петербург, ул. Политехническая, 29
E-mail: moskvin@ibks.spbstu.ru

Ключевые слова: киберугрозы, киберфизические системы, информационная безопасность, промышленный интернет вещей, автоматизированные системы управления технологическим процессов, индустрия 4.0.

Аннотация: Применение технологий цифровизации производства меняет не только процессы обработки данных и принятия решений, но и непосредственный процесс управления киберфизическими системами, применяемых для реализации технологических процессов. Вместе с тем появляются новые угрозы кибербезопасности, нарушающие устойчивость управления технологическим процессом. Данные угрозы ранее не были актуальны или устранялись средствами функциональной безопасности, таким образом, необходима адаптация существующих механизмов управления для устранения новых угроз. В статье приводятся основные угрозы нарушения устойчивой маршрутизации на производственном уровне, а также приводится метод управления маршрутизацией в киберфизических системах цифрового производства на основе одноранговых сетей с использованием принципов чесночной маршрутизации, удовлетворяющая требования кибербезопасности.

1. Введение

Существующие автоматизированные системы управления технологическим процессом (АСУ ТП) строятся в основном по принципу эшелонированной защиты, что отмечается в таких руководящих документах и стандартах, как NIST SP 800-82, SANS, US CERT, а также приказе ФСТЭК № 31. Данный подход заключается в организации многоуровневой защиты сети предприятия посредством ее сегментирования на зоны, а также выстраиванию отношений между данными зонами. В зависимости от назначения системы количество уровней меняется, однако принцип защиты остается прежним.

Непосредственная функция маршрутизации, т.е. отправки управляющих информационных сигналов, влияющих на физические процессы и состояние системы, выполняются на трех нижних уровнях архитектуры: человеко-машинных интерфейсов, программируемых логических контроллеров и конечных устройств. Основными угрозами в подобных сетях АСУ ТП являются угрозы функциональный безопасности, которые

устраняются такими подходами, как резервирование, внедрение цикла безопасной разработки и пр. Данные подходы указаны в семействе стандартов ISA/IEC 6244.

2. Угрозы нарушения устойчивости управления

Системы Цифрового Производства (ЦП) представляют из себя совокупность киберфизических систем (КФС), таких как «Интернет Вещей», технологий сбора, обработки, хранения данных и управления технологическим процессом. Особенности подобных систем, отмеченных в статье[1], обусловлены подходом к построению систем ЦП. Наиболее распространенной архитектурой является предложенная консорциумом Промышленного Интернета Вещей[2].

Основным отличием от классических систем АСУ ТП является реализация полевого сегмента, реализующего технологические процессы и отвечающего за физическое состояние системы. В [7] данным сегментов является промышленный «Интернет Вещей». Стандарт IIC не специфицирует структуру граничного сегмента и взаимодействий между ними, так как его топология и управление взаимодействие между устройствами будет зависеть от особенностей местности, требований и возможностей.

Сегодня для построения сегмента КФС ЦП чаще применяется топология Mesh, т.е. взаимодействие между устройствами строится на основе одноранговых связей между устройствами. Об этом может свидетельствовать множество разрабатываемых для «Интернета Вещей» протоколов, такие как ZigBee, Thread, ZWave, 6LoWPAN, DALI и прочие. Подобная топология позволяет добиться масштабируемости при большом количестве устройств, работающих в единой информационной среде.

Особенность построения сетей ЦП заключается в гетерогенности и связности устройств [1]. Для реализации сегмента КФС применяются технологии, существующие в информационных системах корпоративных сегментов сети. Объектом защиты в данных системах является информации, что требует обеспечение ее конфиденциальности, целостности и доступности. Однако перенос КФС в среду IP-сетей ведет к появлению новых угроз и возможностей нарушителя, так как основной целью нарушителя является не владение информацией, а перехват управления системой и/или нарушение ее устойчивости. Таким образом, устойчивостью системы является ее способность выполнять целевые функции в условиях внешних воздействий[3].

Модель нарушителя при этом меняется, так как стирается четкая грань между возможностью внутреннего и внешнего нарушителей. Подобное обусловлено тем, что системы становится потенциально доступны из сети Интернет или по беспроводному каналу связи. Наиболее полно угрозы промышленного ИВ, применяемого в критической информационной инфраструктуре, перечислены в руководящем документе европейского института ENISA[4]. Сетевые угрозы относятся 3 группы:

- вредоносная деятельность (подмена устройств, DDoS-атаки);
- сетевые атаки (сбор информации по сети, перехват и подмена сообщений, переотправка сообщений);
- отказ в обслуживании сети.

Вектора данных групп угроз отмечены на рис. 1. Нарушение устойчивости функций управление может быть реализовано вследствие реализации хотя бы одной из приведенных угроз кибербезопасности.

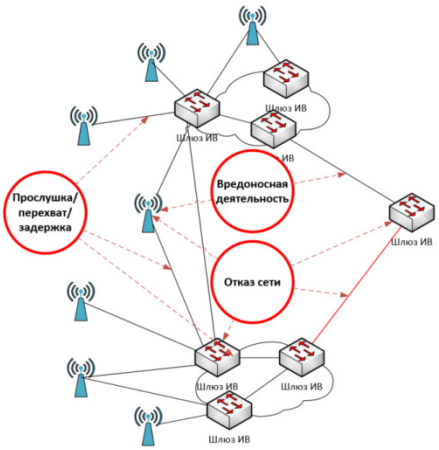

Рис. 1. Угрозы промышленного Интернета Вещей.

Реализация хотя бы одной из приведенных угроз нарушает устойчивость управления КФС.

3. Разработанный подход к управлению маршрутизацией

Для обеспечение устойчивого функционирования КФС, такой как промышленный «Интернет Вещей», предлагается применить подход к управлению маршрутизацией в peer-to-peer сетях с применением принципов чесночной маршрутизации.

3.1. Терминология чесночной маршрутизации

Чесночная маршрутизация оперирует понятиями сообщения, пакета и роутера. Пакет состоит из множества сообщений единого размера, по аналогии с тем, как чеснок состоит из долек. Пакеты пересылаются специализированными маршрутизаторами, называемыми узлами. Для определения того, что сообщение из пакета адресовано именно данному узлу, узел расшифровывает его заголовки. Абстрактный процесс маршрутизации на основе данного подхода изображен на рис. 2.

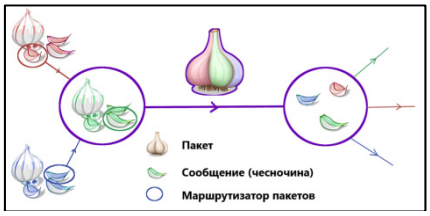

Рис. 2. Концепция чесночной маршрутизации.

Основное применение данная технология получила в рамках реализации анонимной сети I2P для защиты от временного анализа трафика. В I2P защита данных обеспечивается следующими методами:

- применение криптографии с открытым ключом для установки ключа шифрования и подписи данных (у каждого узла есть две пары собственных открытых и закрытых ключей);
- шифрование сообщений на ключе адресата, так что только он сможет прочитать его;

- для входящих и исходящих сообщений используются различные каналы, которые строятся через несколько узлов, подобно анонимной сети TOR;
- каждый пакет, пересылаемый между узлами, состоит из множества зашифрованных сообщений, что не позволяет просматривать трафик остальным участникам и анализировать внутреннюю инфраструктуру.

3.2. Разработанный подход

Методы обеспечения информационной безопасности, применяемые в сети I2P, могут быть применены в управлении потоками данных при организации маршрутизации между узлами P2P-сети КФС. Для этого необходимо модернизировать систему в соответствии со спецификой ИВ.

Рассмотрим пример маршрутизации между узлами двух сегментов K и L. Сегментами в данном случае являются группы равноправных устройств, организованных в одноранговую сеть и использующих единую таблицу маршрутизации. Каждый сегмент K должен содержать две таблицы для каждого удаленного сегмента L:

- таблица исходящих подключений $OutBound_{KL}$ – список адресов удаленных узлов сегмента L, к которым могут подключаться устройства сегмента K. Данная таблица должна быть синхронизирована с соответствующей таблицей входящих подключений в сегменте L;
- таблица входящих подключений $InBound_{KL}$ – список адресов локальных узлов сегмента K, к которым могут подключаться устройства удаленного сегмента L. Данная таблица должна быть синхронизирована с соответствующей таблицей исходящих подключений в сегменте L.

Адресом в данном случае будет являться сопоставление сетевого адреса ухла (например, IP) и двух публичных ключей. Если узел $k \in K$ должен уметь общаться с узлом $l \in L$, то в таблица маршрутизации сегмента K будет содержать напротив адреса узла l два публичных ключа PK_l и PK_k. Ключ PK_l – это открытый ключ шифрования узла l, необходимый для шифрования данных, отправляемых только данному узлу. Ключ PK_k – это открытый ключ узла k, необходимый для цифровой подписи пересылаемых данных. Таким образом, таблица исходящих подключений будет содержать запись вида:

$$RA_{kl} = (PK_l, PK_k), RA_{kl} \in OutBound_{KL}$$

Аналогичным образом будут выглядеть записи в таблице маршрутизации входящих подключений. Сообщение, посылаемое узлом k, шифруется на открытом ключе удаленного узла l и упаковывается в пакет, после чего пересылается следующему узлу.

Для выбора узлов, маршрутизирующих сообщения, предлагается использовать подход, применяемый в сетях I2P: каждый узел публикует во временную сетевую базу под названием LeaseSet, адреса двух узлов, по которым к данному узлу могут поступать пакеты [5].

Управление маршрутизацией заключается в распространении соответствующих таблиц маршрутизации между сегментами КФС. Предлагается использовать подход одноранговых сетей ZigBee и Thread. В данных сетях используется подход, когда существует мастер-узел для распространения таблицы маршрутизации. Далее данные таблицы распространяются среди узлов для последующей маршрутизации и построения временных каналов. Схематично процесс маршрутизации на основе разработанного подхода представлен на рис. 3.

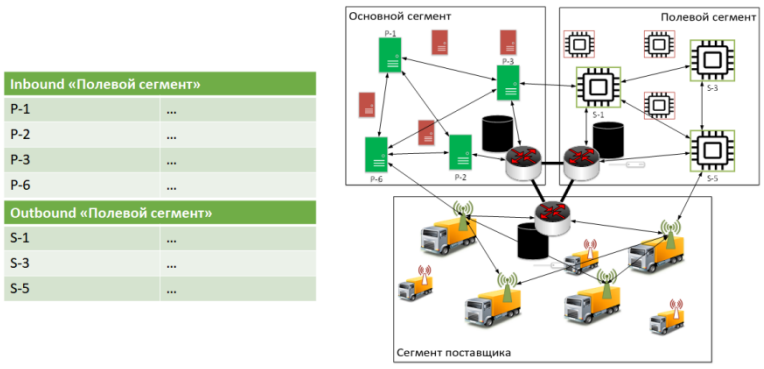

Рис. 3. Управление маршрутизацией между сегментами. Таблицы маршрутизации.

4. Заключение

Данный подход обеспечивает единовременную защиту сетей КФС, организованных по принципу одноранговых Mesh-сетей, от перечисленных угроз безопасности. В таблице 1 перечислены угрозы и методы защиты подхода, которые обеспечивают их устранение.

Таблица 1. Методы обеспечения безопасности КФС разработанного подхода.

Угрозы	Метод защиты
Подмена устройств	Аутентификация с помощью таблиц маршрутизации
DDoS	Одноранговая архитектура обеспечивает балансировку нагрузки
Разведка сети и сбор информации	Сквозное шифрование данных; изоляция каналов передачи данных между конечными узлами; фиксированный размер пакетов;
Перехват и подмена данных	Подпись данных
Переотправка сообщений	Контроль статуса доставки сообщений, отправляемого по отличному от канала приема каналу
Отказ доступа сети	Одноранговая архитектура обеспечивает резервирование каналов

Исследование выполнено в рамках гранта Президента РФ для государственной поддержки ведущих научных школ Российской Федерации НШ-2992.2018.9 (соглашение 075-02-2018-504).

Список литературы

1. Зегжда Д.П., Москвин Д.А., Дахнович А.Д. Анализ угроз информационной безопасности в сетях цифрового производства // Проблемы информационной безопасности. Компьютерные системы. 2017. № 4. С. 41-46.
2. The Industrial Internet of Things Volume G1: Reference Architecture. https://www.iiconsortium.org/IIC_PUB_G1_V1.80_2017-01-31.pdf.
3. Zeghzda D. Sustainability as a criterion for information security in cyber-physical systems. // Automatic Control and Computer Sciences. 2016. Vol. 50. P. 13-18.
4. Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport.
5. Niedermayer H. Architecture and Components of secure and anonymous Peer-to-Peer Systems. 2010. 188 p.