Угрозы телекоммуникационным сетям в киберфизических системах

А. М. Болдинов
Петербургский государственный университет путей сообщения Императора Александра I
23boldinov98@gmail.com

А. А. Привалов
Петербургский государственный университет путей сообщения Императора Александра I
aprivalov@inbox.ru

Аннотация. **В данной статье рассматриваются транспортные системы, называемые киберфизическими системами (КФС). Описана передача данных в таких системах, приведена сетевая модель для создания протоколов обмена данными. Описана киберфизическая транспортная система (КФТС), которая используется на железнодорожном транспорте. Анализируются угрозы телекоммуникационным сетям в киберфизических системах.**

Ключевые слова: киберфизические системы, киберфизическая транспортная система, GSM-R, телекоммуникационные системы

I. Введение

Развитие транспортных систем, привело к появлению беспилотных транспортных систем, таких систем в которых участие человека не нужно. На основе беспилотных систем появились киберфизические системы. Такие системы все чаще начинают применяться в различных производственных сферах.

Использование беспилотных транспортных систем в различных производственных областях, привело к проблемам в области устойчивого функционирования данных систем, что в свою очередь привело к таким же проблемам в киберфизических транспортных системах. Киберфизичская система – информационно-технологическая концепция, подразумевающая интеграцию вычислительных ресурсов в физические сущности любого вида, включая биологические и рукотворные объекты. В киберфизических системах вычислительная компонента распределена по всей физической системе, которая является её носителем, и синергетически увязана с её составляющими элементами.

Киберфизические системы высокоадаптивны, для их реализации необходимо ставить цели и задачи, которые такая система должна выполнять. Главной целью таких систем является управление сложными процессами, сложными ситуациями. Недостатком таких систем может являться привлечение специалистов в данной области, для того чтобы они создавали и поддерживали такие системы.

II. Передача данных в КФС

Говоря о киберфизических системах, необходимо рассматривать каждый уровень таких систем отдельно. Во-первых, данные системы – это комплексные системы, которые состоят из физических и вычислительных элементов, которые, получая информацию из внешней среды, анализируя ее, применяют ее для дальнейшей оптимизации процессов управления объектом.

Далее, в данных системах происходит интеграция различных вычислительных устройств в физические объекты. Сама вычислительная среда распределяется по всей системе, в которой она располагается.

И наконец, такие системы состоят из внутренних подсистем и управляющих контроллеров или управляющих внутренних подсистем. Также вокруг таких систем находятся внешние системы, которые осуществляют координацию между вычислительными и физическими ресурсами. В киберфизических системах существуют петли управления, это означает что система, может обмениваться с внешними подсистемами в режиме, как прямой, так и обратной связи [1].

Области действия киберфизических систем охватывают различные произоводственные сферы. Создание данных систем основывалось на применении Интернета вещей (Iot), встроенные системы, технологии повсеместного вычисления, системы сетевого обмена. Интернет вещей (Internet of Things – IoT) – технология [2], в которой любой физический объект может быть соединён с любым другим физическим объектом. Если интернет вещей рассматривать, как единую структуру, то данная структура состоит их нескольких сетевых уровней, между которыми происходит межсетевое взаимодействие физических устройств, подсистем обмена информацией, транспортных средств, объектов инфраструктуры. Данная технология позволяет объектам в такой сети производить сбор и обмен данными. Протоколы обмена данными для реализации передачи данных между стационарным оборудованием и оборудованием, находящимся на борту объекта, защиты данных, создаются на базе сетевой модели сетевых протоколов OSI (таблица).

ТАБЛИЦА I Модель OSI

Модель OSI			
№	**Уровень**	**Тип данных**	**Функции**
7	Прикладной	Данные	Доступ к сетевым службам
6	Уровень представления	Поток	Представление и шифрование данных
5	Сеансовый	Сеансы	Управление сеансом связи
4	Транспортный	Сегменты	Прямая связь между конечными пунктами
3	Сетевой	Пакеты/датаграммы	Определение маршрута и логическая адресация
2	Канальный	Кадры	Физическая адресация
1	Физический	Биты	Работа со средой передачи, сигналами и двоичными данными

Когда осуществляется реализация нижних уровней модели существует несколько способов реализации передачи данных: пакетная передача и коммутация каналов.

При пакетной передаче, такой режим коммутации обеспечивает доступ нескольких абонентов к сети. В таком режиме происходит обмен данными с помощью

передачи пакетов небольшого размера, каждый пакет независим друг от друга. Одним из преимуществ данного вида коммутации является возможность передачи данных несколькими абонентами по одной физической линии.

Если используется коммутация каналов, такой вид коммутации обеспечивает отдельное соединение между оборудованием, находящимся на борту объекта киберфизической системы и стационарным оборудованием [3].

Отдельным направлением киберфизических систем, является применение киберфизических систем в виде транспортных систем, иначе такие системы можно назвать киберфизические транспортные системы. У данных систем существует два отдельных типа систем: внутренняя система внутри движущегося объекта и внешняя система, которая объединяет комплекс движущихся объектов. Внешние системы решают задачи по управлению трафиком движения в системе транспортных потоков [4]. Системы первого типа позволяют решить задачи по управлению отдельным объектом в сложных, динамически меняющихся системах [5].

III. Применение киберфизических транспортных систем на железнодорожном транспорте

В качестве таких систем на железнодорожном транспорте применяются системы интервального регулирования движения поездов. Примером таких систем является система интервального регулирования движения поездов, созданная совместно специалистами из России и Италии – ITARUS-ATC. Система позволяет сокращать расходы на управление движением поездов как на обычных, так и на высокоскоростных линиях, повышает безопасность железнодорожного транспорта, пропускную способность магистралей и обеспечивает действие систем непрерывного автоматического ограждения поездов и автоматического управления движением и обеспечения безопасности. Система ITARUS-ATC состоит из нескольких частей: цифровой радиосети GSM-R для обеспечения голосовой связи и обмена данными между бортовым локомотивным устройством и системой управления движением. Основой данной системы является центр радиоблокировки, который с помощью информации от систем сигнализации, централизации, блокировки (СЦБ) и данных от локомотивов, получаемых по радиоканалу, формирует команды на управление движение. выдает разрешения на движение и указывает допустимую скорость.

Система ITARUS-ATC состоит:

- из системы автоблокировки, предназначенной для интервального регулирования движением поездов на перегонах;
- системы электрической централизации станции;
- центра радиоблокировки;
- комплексного локомотивного устройства безопасности КЛУБ-У;
- блока AIRBS для реализации стека протоколов Euroradio;
- сети радиосвязи стандарта GSM-R.

Основная роль в управлении движением в проекте ITARUS-ATC принадлежит центру радиоблокировки:

- контроль проследования составов по сигналам автоблокировки;
- управление обменом информацией с бортовой системой КЛУБ-У по радиосети GSM-R;
- управление интерфейсами, обеспечивающими взаимодействие с системами СЦБ с использованием рабочих станций MMI;
- регистрация основных процессов работы центра.

Соответственно особую роль в киберфизических транспортных системах имеет телекоммуникационная сеть. С ее помощью происходит передача данных, для успешной работы ITARUS-ATC необходимо анализировать угрозы, которые могут подорвать работу системы целиком.

Телекоммуникационная сеть данной системы состоит из бортового локомотивного оборудования, цифровой радиосети и системы управления движения. В качестве локомотивного бортового оборудования используется комплексное локомотивное устройство безопасности (КЛУБ-У), которое собирает сигналы от различных датчиков и устройств, и передает данные в цифровую радиосеть, с помощью которой, происходит обмен данными с системой управления движения.

IV. Анализ угроз телекоммуникационных сетей КФТС

Главной задачей функционирования киберфизических транспортных систем является обеспечение устойчивого функционирования телекоммуникационных сетей. Телекоммуникационные сети обеспечивают обмен данными между движущимися объектами и стационарным оборудованием. Телекоммуникационная сеть состоит из физических каналов связи и коммутационного оборудования, реализующая какой-либо протокол передачи данных.

Соответственно, если не будет происходить анализ угроз для телекоммуникационных сетей, то при совершении атаки на ТКС, функционирование КФТС будет нарушено.

Чтобы рассмотреть все возможные угрозы, необходимо описать классификацию угроз:

- умышленные угрозы – угрозы, которые возникают с какой-то определенной целью, для этого происходит анализ системы целиком, с целью найти уязвимые места или совершение вторжения с использованием данных о системе;
- случайные угрозы – угрозы, которые могут возникнуть вследствие несанкционированного доступа к стационарному оборудованию.

Случайные угрозы могут происходить при выходе из строя части системы, ошибок при администрировании сети или при свободном доступе к оборудованию.

Умышленные угрозы в свою очередь имеют конкретную цель в виде нанесению ущерба сети. Такие угрозы подразделяются на активные и пассивные угрозы. При рассмотрении пассивных угроз, целью является подключение к сети и использование информации в своих интересах. Активные угрозы имеют главную

цель – нарушить устойчивое функционирование КФТС и получить полный доступ к ТКС. Главными целями являются изменение или подмена данных во время передачи данных, разрушение функционирования обмена данных, вывод из строя системы передачи данных.

Злоумышленник может реализовывать угрозу с помощью целого ряда способов, таких как последовательного перебора, перебор с задействованием специально созданных словарей, подмена доверенного объекта в телекоммуникационной сети IP-spoofing и анализ трафика с последующим перехватом циркулирующих пакетов (sniffing) [6]. При проведении атак на сети связи, для совершения успешных атак, проводится сканирование сети. После этого происходит проникновение в сеть связи. После этого субъект, который производит, атаку на сеть связи может получить доступ к оборудованию, которое находится на борту движущегося объекта или к стационарному оборудованию.

При успешном вторжении, атакующий может использовать телекоммуникационную сеть для своих целей. При получении несанкционированного доступа к сети, злоумышленник может реализовать широкий спектр деструктивных воздействий [7], а именно:

- Нарушение конфиденциальности: утечка данных; несанкционированное тиражирование; анализ и перехват трафика в каналах передачи данных; разглашение защищаемых данных.
- Нарушение целостности: воздействие на микропрограммы, данные и драйверы устройств телекоммуникационной сети связи; воздействие на данные и драйверы устройств, обеспечивающих загрузку операционной системы и средств защиты информации (СЗИ) и их функционирование; внедрение вредоносного ПО, программно-аппаратных закладок; воздействие на средства управления конфигурацией телекоммуникационной сети связи, СЗИ.
- Нарушение доступности: нарушение работоспособности и отказы средств обработки, ввода/вывода и хранения данных, аппаратуры и каналов связи, СЗИ.

V. Заключение

Развитие таких систем, как КФС привело к тому, что появились такие системы на транспорте и производстве, в частности на железнодорожном транспорте. Главной задачей устойчивого функционирования КФТС является обеспечение в первую очередь устойчивого функционирования телекоммуникационных сетей. Поэтому анализ угроз в отношении телекоммуникационных сетей в КФС является основным пунктом устойчивого функционирования всей системы целиком.

Список литературы

[1] Горелова Г.В. Киберфизические системы и когнитивное моделирование сложных систем // Проблемы управления безопасностью сложных систем Москва, 18 декабря 2019 года. 299-304 с.

[2] Дешко И.П., Кряженков К.Г., Цветков В.Я. Устройства, модели и архитектуры Интернета вещей. М.: Макс Пресс, 2017. 88 с.

[3] Попов П.А. Совершенствование методов и алгоритмов управления в системах интервального регулирования движения поездов с использованием радиоканала.

[4] Jianjun S.et al.The analysis of traffic control Cyber-physical systems // Procedia-Social and Behavioral Sciences. 2013. Т. 96. С. 2487–2496.

[5] Cartwright R.et al. Cyber-physical challenges in transportation system design // National workshop for research on highconfidence transportation Cyber-physical systems: automotive, aviation & rail. 2008.

[6] Качаев А.Н. Мониторинг событий и обнаружения инцидентов информационной безопасности с использованием SIEM. // Международный студенческий научный вестник, 2015 год, № 3-1, стр. 122-123.

[7] Гречишников Е.В., Добрышин М.М. Оценка эффективности деструктивных программных воздействий на сети связи. // Научный сетевой электронный журнал «Системы управления, связи и безопасности». СПб. №2. 2015.