Д.В. Мишин
Научный руководитель: А. В. Провоторов
Муромский институт (филиал) ФГБОУВПО Владимирский Государственный Университет имени Александра Григорьевича и Николая Григорьевича Столетовых
Россия, 062264, Владимирская область, г. Муром, ул. Орловская, д.23
matthewbgr@gmail.com

Легковесный защищенный протокол передачи данных для систем интернета вещей

С развитием интернета распространяется автоматизация многих процессов нашей жизнедеятельности. Управление производством, автоматизация сельскохозяйственных процессов, мониторинг различного рода систем и показателей. Все эти важные задачи мы с каждым днем, шаг за шагом, все в большей степени возлагаем на плечи компьютеров. Однако, какой бы радужной не казалась перспектива переложить всю рутинную работу на автоматизированные вычислительные системы, все еще остаются проблемы, которые отодвигают ее вариации от идеала. Одной из таких проблем является безопасность передачи данных.

Защищенный протокол передачи данных позволит решить ряд проблем с безопасностью при передачи данных между устройствами системы интернета вещей. Так как одной из целей автоматизации является сокращение расходов на оборудования, за частую, в силу масштабов автоматизации, то одним из условий для разработки протокола было – легковесность криптографических методов, используемых в нем, что позволит снизить нагрузку на вычислительные мощности, а в следствии и стоимость оборудования.

Важными этапами работы протокола будут:

- Процессы работы с ключами шифрования – учитывая простые, но эффективные решения, разработанные алгоритмы работы с ключами позволят избежать ряд проблем с безопасностью;
- Гибкость протокола для пользовательских настроек – в зависимости от задач и возможностей, пользователь может настроить протокол в зависимости от потребностей.
- Фильтрация данных – так же является одной из ключевых особенностей работы протокола. Данный процесс позволит отбросить поврежденные либо не несущие доверия входные данные.

Задачи защищенного протокола передачи данных представлены следующим списком.

1. Задача обеспечения конфиденциальности данных. «Интернет вещей» - это расширение механизмов сбора, хранения и анализа данных. К Интернету подключается все больше и больше устройств, а также требуется больше элементов, которые требуют защиты: само устройство, сеть, приложение или платформа, которую оно использует.
2. Шифрование данных: передача данных незашифрованными средствами представляет собой серьезную проблему безопасности. Учитывайте также важность сетевой безопасности, поскольку интернет обычно ориентирован на мобильные устройства различных типов и преимущественно беспроводные сети.
3. Защита от несанкционированной подписки - злоумышленник, подключенный к той же сетевой инфраструктуре, может наблюдать за сетевыми пакетами. В ситуациях, когда пользователи общаются по многоадресной рассылке, злоумышленник может просто подписаться на один и тот же адрес многоадресной рассылки.
4. Защита от несанкционированной публикации - злоумышленник подключен к той же сетевой инфраструктуре и может вводить сетевые пакеты с любым содержимым данных, заголовками и адресатом, который она пожелает.
5. Защита от фальсификации и воспроизведения – злоумышленник может использовать общий секретный ключ для создания сообщений в сети и притворяться, что это пришло от другого пользователя.

Так как выше представленный протокол ориентируется на передачу данных между устройствами интернета вещей, то остается незащищенный канал передачи данных между локальной частью системы интернета вещей и пользователем. Безопасную, удаленную передачу данных можно организовать через надежных посредников, таких как сервера производителей подобных систем, а также использование прикладных интерфейсов надежных посредников.