Защита интернета вещей на примере умного дома

Выбор типа связи между устройствами

Для связи между устройствами был выбран радио сигнал…
Тут должно быть краткое описание проблемы, но будем писать его мы в самом конце

Наш протокол передачи данных

Примечания:

1. При передачи все сообщения шифруются алгоритмом XXTEA
2. Передаваемое сообщение содержит само сообщение и его контрольную сумму для проверки целостности и валидности принятого сообщения

Алгоритм передачи данных:

1. Устройство-отправитель посылает запрос устройству-получателю на получение временного ключа
2. Устройство-получатель генерирует случайный временный ключ и отправляет его устройству-отправителю
3. Устройство-отправитель XOR-ит временный ключ с сообщением(сообщение + его контрольная сумма) и отправляет его устройству-получателю
4. Устройство-получатель принимает сообщение, XOR-ит его с временным ключом и путем сравнения контрольной суммы, вложенной в сообщение, с вычисленной контрольной суммой сообщения, сообщение проверяется на потерю данных и на то, был ли пакет зашифрован правильным внешним ключом

Вывод

- Разработанный протокол позволяет передавать данные без потерь(хзхз)
- Защита от спама командами(однотипные команды зашифрованы временным ключом и каждый раз имеют разное тело сообщения)
- …