Projeto de Iniciação Científica:
Mecanismos e políticas de segurança para Internet das Coisas

Aluno: Bruno Maciel Rotondaro[1]
Orientador: Prof. Dr. Arlindo F. da Conceição

[1]Bacharelado em Ciência e Tecnologia
Universidade Federal de São Paulo (UNIFESP)
Campus São José dos Campos

Abstract. *The Internet of Things era brings many security challenges, because from the moment when all devices are connected to the Internet, they are susceptible to cyberattacks. This project aims to develop a cybersecurity tool for long distance communication systems using LoRaWAN and MQTT technologies. A test environment will be created consisting of a prototype of a sensor network and a server, based on InterSCity platform. The security tests will be conducted to verify the security mechanisms provided by the tools. It is also intended to propose improved end-to-end security mechanisms.*

Resumo. *A era da internet das coisas traz muitos desafios de segurança, pois a partir do momento que um dispositivo é conectado à Internet ele está sujeito à ataques cibernéticos. Este projeto visa avaliar a segurança cibernética em sistemas de comunicação sem fio de longa distância, que utilizam as tecnologias LoRaWAN e MQTT. Será criado um ambiente de testes, composto por uma rede de sensores e um servidor baseado na plataforma InterSCity. Os testes de penetração serão feitos para verificar os mecanismos de segurança fornecidos pelas ferramentas. Pretende-se ainda propor mecanismos aprimorados de segurança fim a fim.*

1. Introdução

Com o avanço da tecnologia, conectar tudo à internet para a criação de Objetos Inteligentes ficou cada vez mais relevante. Desse modo, a Internet das Coisas surgiu a fim de conectar objetos do dia-a-dia à internet [14].

Keyur K. Patel define IoT [10] como: *"Em um mundo onde bilhões de objetos podem sentir, se comunicar e compartilhar informação, todos conectados através da internet. Esses objetos interconectados tem seus dados regularmente coletados, analisados e usados para iniciar ações providenciando uma riqueza de inteligência, para planejamento, administração e tomada de decisão. Este é o mundo da Internet das Coisas."*

Neste Cenário, a prática de defender computadores de ataques cibernéticos, cibersegurança [3], é essencial para Internet das Coisas, pois, as informações na rede podem estar vulneráveis. Dessa forma, é preciso a melhoria de protocolos de segurança na Internet. De modo que, ataques como o que usou câmeras conectadas à internet para fazer um ataque DDoS (Distributed Denial of Service) no Twitter em 2016 [8], sejam evitados.

Deste modo, este projeto de Iniciação Científica visa investigar as vulnerabilidades de segurança em comunicações em longa distância, particularmente em aplicações IoT baseadas nas tecnologias LoRa e MQTT. Para isso, um ambiente de testes de rede de sensores sem fio será desenvolvido e um servidor será criado. E testes de ataques cibernéticos serão realizados para verificar a robustez dos mecanismos de segurança. Pretende-se propor melhorias nesses ambientes.

2. Fundamentação teórica

Este projeto, utilizará as seguintes tecnologias: a plataforma InterSCity [2], que será usada no servidor, e as tecnologias de LoRaWAN [4] e MQTT [7], que serão usadas para os sensores se comunicarem entre si e com o servidor, como ilustrado na Figura 2. A seguir apresenta-se um resumo dessas tecnologias.

2.1. InterSCity

O InterSCity [2] é um projeto colaborativo de pesquisa que abrange 9 instituições nacionais e parceiros internacionais. Ele é focado em pesquisas em 3 frentes: rede e computação distribuída de alto desempenho, engenharia de software, análise e modelagem matemática para a Internet do futuro e cidades inteligentes. Nesse projeto, foi desenvolvida a plataforma InterSCity que foi criada para dar suporte a projetos de Internet das Coisas, Big Data e Computação em Nuvem. Em seu site [2], a plataforma é descrita como: *"O principal objetivo da plataforma InterSCity é fornecer serviços e APIs de alto nível para apoiar o desenvolvimento de novos serviços para as cidades, reunindo tecnologias, como IoT, Big Data e Cloud Computing. A plataforma adota uma arquitetura de micro serviço, projetada para suportar adequadamente a integração de uma grande quantidade de dispositivos e dados e fornecer serviços de qualidade em escala de cidade."*

2.2. Message Queue Telemetry Transport (MQTT)

O MQTT [7] é um protocolo de conexão Máquina-à-Máquina, desenvolvido para ser leve, rápido e sem perdas. Muito eficiente para conexões com dispositivos em lugares remotos que demandam um código pequeno e com conexão restrita. É ideal para aplicações de Internet das Coisas devido ao seu tamanho e baixo uso de energia e conexão. Para que

esse protocolo funcione são necessários Clientes e um Broker. Os clientes podem se inscrever ou publicar em um tópico e o Broker é quem gerencia as mensagens e quem está inscrito nos tópicos. Essas mensagens são assíncronas e possuem um QoS (Qualidade de Serviço), ou seja, uma prioridade de chegada da mensagem. Para publicar uma mensagem o Cliente escolhe o QoS, um QoS de 0 significa que a mensagem será entregue no máximo uma vez, o de 1 significa que a mensagem vai ser entregue pelo menos uma vez e o de 2 significa que a mensagem será entregue exatamente uma vez. O MQTT utiliza a porta 1883 e o protocolo TCP/IP para a comunicação do Broker com os clientes.
Para proteger as informações transmitidas podem ser usadas medidas de segurança, a mais importante é a utilização de TLS (Transport Layer Security) [3] em conjunto com o MQTT para ter uma conexão segura entre o Cliente e o Broker. O TLS utiliza a porta 8883 e vai criptografar, autenticar e verificar a integridade das mensagens enviadas.

2.3. LoRaWAN

LoRa (Long Range) [4] é uma tecnologia para transmissão de dados por rádio frequência, ela usa a modulação *chirp spread spectrum* para reduzir Interferências e, deste modo, atingir um baixo consumo de energia mesmo em comunicação de longa distância. Essa tecnologia utiliza frequências de rádio não licenciadas para comunicação, as quais variam de região a região. LoRaWAN (Long Range Wide Area Network) é um padrão da indústria que define a estrutura de um pacote de dados e como os pacotes são processados e criptografados. A rede LoRaWAN é recomendada para dispositivos IoT, pelo seu baixo custo de recursos computacionais e pela baixa utilização de energia. Assim, os dispositivos podem ficar em lugares de difícil acesso e requerer baixa manutenção.

2.4. Criptografia com Curvas Elípticas

A criptografia baseada em curvas elípticas [3] é um algoritmo de chave assimétrica que foi criado em 1985 por Neal Koblitz e Victor Miller, porém começou a ser mais utilizado no começo dos anos 2000. Esse algoritmo oferece o mesmo nível de segurança que o RSA, que é baseado na fatoração do produto de dois números primos [3]. Essa criptografia com chaves menores de aproximadamente 256 bits consegue a mesma proteção que uma de 3072 bits em RSA como representado na tabela 1.

A fórmula matemática de curvas elípticas é: $y^2 = x^2 + ax + b \; mod \; p$, onde p é um número primo e a e b pertencem aos primos inteiros. Essa formula é usada para fazer o gráfico, como demonstrado na Figura 1

As operações principais usadas pelo algoritmo são a duplicação de pontos e adição de pontos da curva. A base dessa criptografia é um problema logarítmico discreto (EC-DLP) [13], ou seja, em um problema como, $q = dp$, um ponto d não pode ser calculado mesmo sabendo os pontos q e p, porém é fácil encontrar q com os pontos d e p.

Tabela 1. Comparação de tamanho de chaves em Bits [15].

Symmetric Algorithm	ECC	RSA
80	163	1024
112	233	2240
128	289	3072
192	409	7680
256	571	15360

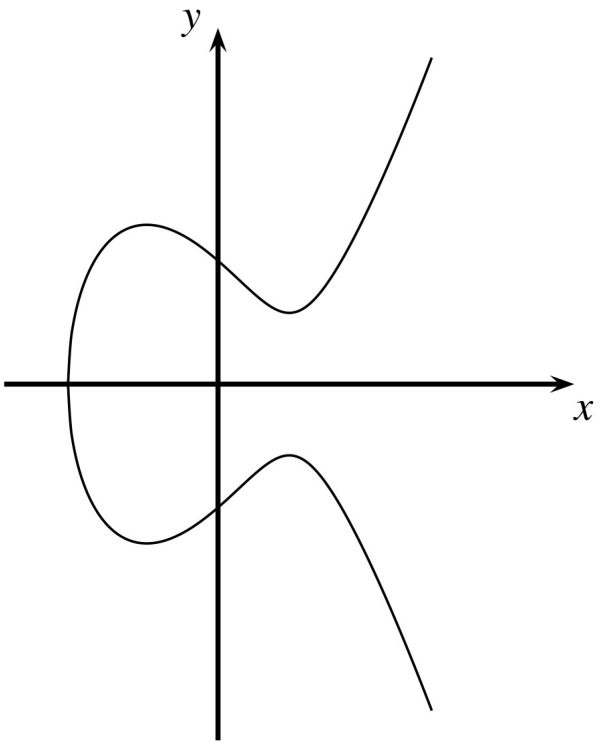

Figura 1. $y^2 = x^3 - 3x + 3$ em $\mathbb{R}$

Para criar a chave privada e pública, o ponto inicial p da curva e os seus coeficientes são pré configurados no cliente e no servidor, após isso, ocorrem d duplicações ou adição de pontos e chegamos em um ponto q. Assim, d é a chave privada e q a chave pública [9].

3. Arquitetura do Ambiente de Testes

O ambiente de testes será composto de: Nós sensores, um *gateway*, um servidor no The Things Network para processar os dados em LoRaWAN e mandar como MQTT e um servidor com InterSCity para armazenar os dados e manipulá-los, como representado na

Figura 2.

- Os nós sensores serão compostos por um Arduino Uno com um shield LoRaWAN da Radioenge, eles irão ter um sensor ultrassônico HC-SR04 para medir o nível de uma lixeira. Eles mandarão a informação do sensor para o *gateway* usando a rede LoRaWAN utilizando rádio frequência LoRa.
- O *gateway* será um Raspberry pi 3 com um kit para LoRaWAN da Radioenge, ele receberá as informações do sensor por rádio frequência e transmitirá para o The Things Network por TCP/IP com TLS.
- O The Things Network irá processar os dados recebidos em LoRaWAN e irá mandar para o InterSCity por MQTT com TLS para armazenar e manipular os dados.

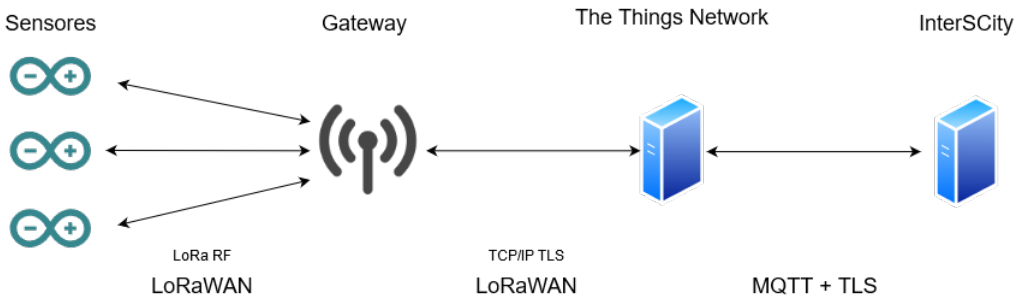

Figura 2. Arquitetura do ambiente de testes

4. Trabalhos Relacionados

A criptografia com Curvas Elípticas tem sido estudada em outros trabalhos em junção com LoRaWAN e MQTT. Porém, em nenhum trabalho as três tecnologias foram integradas.

- Em Raad Et al. [12]. Eles analisam a segurança do LoRaWAN contra ataques ”Bit-Flipping”. O objetivo do artigo é adicionar uma camada extra de criptografia com assinatura digital utilizando curvas elípticas. Eles atingem esse objetivo utilizando o Método Adaptativo de Criptografia com Curvas Elípticas e o Algoritmo de Assinatura Digital com Curvas Elípticas. E o trabalho concluiu que o método proposto foi muito efetivo contra o ataque.
- Em Routo Terada [16]. Foi criado um método de *Authenticated Key Agreement* (AKA) sem a necessidade de uma *Public Key Infrastructure* e seguro pelo *Random Oracle Model*. Neste projeto, os protocolos de AKA são baseados no problema Diffie-Hellman, Curvas Elípticas e funções de Emparelhamento Bilinear. Esse artigo contém um protocolo de interesse para utilizar na criptografia do *payload* no projeto.
- Em Mektoubi Et al. [5]. Eles propuseram uma nova abordagem para trocas de informação utilizando MQTT e as criptografias RSA e AES, também fizeram uma

comparação da criptografia RSA com Curvas Elípticas. O objetivo deles é melhorar a segurança do MQTT e para conseguirem utilizaram um agente de cetificação para gerar dois tipos de certificado, um para o cliente e um para o tópico. Com isso, chegaram a conclusão que as chaves feitas por curvas elípticas são mais curtas e que para cada operação que fizeram, existia um algoritmo e para cada algoritmo uma chave diferente, o que não acontece no RSA onde uma única chave pode ser usada em todo o processo e como varias chaves eram geradas no algoritmo de curvas elípticas, consumia mais banda,no projeto deles. Então fizeram uma solução híbrida entre curvas elípticas e RSA.

- Em Bardram Et al. [1], LoRaWAN e MQTT foram usados para monitorar a capacidade de um porto na Dinamarca. A plataforma The Things Network é usada como intermediária para o LoRaWAN. Sua comunicação com o *gateway* e o servidor é por MQTT. O artigo conclui que o LoRaWAN comparado ao LTE e WiFi, em relação ao custo, complexidade e cobertura é uma melhoria.

Neste projeto vamos utilizar uma Criptografia de Curvas Elípticas em um ambiente com LoRaWAN e MQTT e fazer uma criptografia de ponta a ponta buscando ampliar a segurança em ambientes que integram as duas tecnologias.

5. Objetivos

O objetivo geral deste projeto de Iniciação Científica é investigar a segurança em arquiteturas IoT, baseadas em LoRaWAN e MQTT.

O objetivo específico deste trabalho é implantar um aplicativo IoT em um servidor com a plataforma InterSCity. Esse aplicativo se comunicará com o servidor localizado na Universidade de São Paulo por meio do protocolo MQTT e ele se conectará com os sensores por meio de uma rede LoRaWAN. Será responsabilidade deste bolsista de Iniciação Científica manter a aplicação e a plataforma operacional, assim como investigar fragilidades de segurança e as respectivas correções.

Para atingir os objetivos acima, as seguintes metas foram planejadas:

- **Servidor**
  - Instalar um servidor Linux com a plataforma InterSCity;
- **Aplicativo**
  - Desenvolver protótipo de um aplicativo de IoT;
  - Integrar o aplicativo com o servidor InterSCity;
- **Segurança**
  Uma vez instalado o ambiente de testes:
  - Executar experimentos de infiltração e de segurança do protocolo MQTT sobre LoRaWAN [6];

– Colaborar com a integração e avaliação de mecanismos criptográficos baseados em Curvas Elípticas [9].

O principal desafio a ser enfrentado será testar a segurança de IoT, usando MQTT sobre LoRaWAN. Pretende-se propor soluções para os problemas identificados.

6. Plano de Trabalho e Cronograma de Execução

A pesquisa e o desenvolvimento seguirão o cronograma apresentado na Tabela 2.

Tabela 2. Cronograma

Atividade	T3/20	T4/20	T1/21	T2/21
Levantamento bibliográfico	X			
Revisão sistemática da literatura sobre vulnerabilidades de cibersegurança de MQTT	X	X		
Instalação da plataforma InterSCity	X			
Manutenção do ambiente de testes baseado na plataforma InterSCity		X	X	X
Desenvolvimento de mecanismos de alarme para monitoração da plataforma		X		
Reprodução de ataques		X	X	
Correção de vulnerabilidades		X	X	X
Preparação de artigo para SBRC		X		
Preparação de artigo em inglês para revista			X	X
Preparação de relatório parcial para a Fapesp		X		
Preparação de relatório final para a Fapesp				X

7. Material e Métodos

O projeto está inserido no contexto do projeto temático FAPESP sobre Internet do Futuro (processos 14/50937-1 e 15/24485-9). Os equipamentos LoRaWAN para montagem do ambiente de testes estão em fase de aquisição. Outros requisitos para a execução do projeto estão disponíveis, tais como, livros, computadores com acesso à Internet, componentes de IoT e acesso ao portal CAPES de periódicos.

O mapeamento inicial das fragilidades e vulnerabilidades de ambientes LoRaWAN foi realizado e será utilizado para nortear o desenvolvimento deste projeto [11]. O estudo será complementado por meio de um estudo sistemático dos ataques mais comuns à aplicações MQTT [3].

As atividades de desenvolvimento serão conduzidas em um laboratório de informática, localizado no campus São José dos Campos da UNIFESP, reservado especificamente para projetos de pesquisa e atividades de iniciação científica.

Portanto, todos os recursos materiais necessários para a execução do projeto encontram-se assegurados.

8. Forma de análise dos resultados

O projeto irá analisar a resiliência do ambiente de testes aos ataques mais comuns [11]. Para isso, serão realizadas simulações de testes de penetração e de DOS [3], entre outros. Após os testes, será preparado um artigo científico publicando os resultados dos testes. O relatório de testes é um dos resultados da pesquisa.

Outro resultado esperado é a integração de novos serviços, com suporte à segurança, na Plataforma InterSCity.

9. Comitê de Ética

O projeto foi aprovado pelo Comitê. O CEP do projeto é 4756030520.

10. Considerações finais

Este projeto visa contribuir para o desenvolvimento do projeto InterSCity por meio da análise de fragilidades e de melhorias de segurança para ambientes de IoT. Os principais resultados deste estudo devem ser:

- Domínio da plataforma InterSCity;
- Criação de um aplicativo para cidade inteligente, avaliação da segurança do aplicativo em cenários IoT que utilizam o InterSCity, redes LoRaWAN e o protocolo MQTT;
- Experimentos para avaliação de técnicas de penetração no cenário experimental (InterSCity, LoRaWAN e MQTT);
- Apoiar a integração de novos algoritmos e de melhores práticas de segurança no ambiente InterSCity;
- Formação de recursos humanos na área de Segurança da Informação.

11. Observação do orientador

Bruno Maciel Rotondaro demonstra bom desempenho acadêmico e participa voluntariamente – com bom desempenho – do projeto de pesquisa InterSCity desde março de 2020, dedicando cerca de 10 horas semanais ao trabalho.

Referências

[1] A. V. T. Bardram, M. Delbo Larsen, K. M. Malarski, M. N. Petersen, and S. Ruepp. Lorawan capacity simulation and field test in a harbour environment. In *2018 Third International Conference on Fog and Mobile Edge Computing (FMEC)*, pages 193–198, 2018.

[2] INCT. Interscity. `https://interscity.org/software/interscity-platform/`. Acessado: 25 de março de 2020.

[3] Joseph Migga Kizza. *Guide to computer network security*. Springer, 4th edition, 2017.

[4] LoRa Alliance. Página inicial Lora Alliance. `https://lora-alliance.org/`. Acessado: 25 de março de 2020.

[5] Abdessamad Mektoubi, Hicham Lalaoui Hassani, Hicham Belhadaoui, Mounir Rifi, and Abdelouahed Zakari. New approach for securing communication over MQTT protocol A comparaison between RSA and Elliptic Curve. *Proceedings - 2016 3rd International Conference on Systems of Collaboration, SysCo 2016*, 0:1–6, 2017.

[6] Poliana De Moraes. FEDERAL UNIVERSITY OF S AO Institute of Science and Technology Master of Professional Studies in Technological Innovation CYBERSECURITY FOR IOT APPLICATIONS BASED ON. 2019.

[7] MQTT. Página inicial MQTT. `http://mqtt.org/`. Acessado: 25 de março de 2020.

[8] Swapnil Naik and Vikas Maral. Cyber security - IoT. *RTEICT 2017 - 2nd IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, Proceedings*, 2018-Janua:764–767, 2017.

[9] Christof Paar and Jan Pelzl. *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media, 2009.

[10] Keyur K Patel, Sunil M Patel, and P G Scholar. Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. *International Journal of Engineering Science and Computing*, 6(5):1–10, 2016.

[11] Arlindo F. da Conceição Poliana Moraes. A systematic review of security in the lorawan network protocol. Submitted to JNCA. Acessado: 12 de abril de 2020.

[12] Nibras Raad, Taha Hasan, Ahmed Chalak, and Jumana Waleed. Secure Data in LoRaWAN Network by Adaptive Method of Elliptic-curve Cryptography. *ICCISTA 2019 - IEEE International Conference on Computing and Information Science and Technology and their Applications 2019*, pages 1–6, 2019.

[13] Nibras Raad, Taha Mohammed Hasan, and Ahmed Chalak Shakir. ECC Based Data Retrieval Using LoRaWAN Technology. *International Journal of Engineering & Technology*, 7(4):4918, 2018.

[14] Bruno P Santos, Lucas A M Silva, Clayson S F S Celes, João B Borges Neto, Bruna S Peres, Marcos Augusto, M Vieira, Filipe M Vieira, Olga N Goussevskaia, and An-

tonio A F Loureiro. Internet das Coisas: da Teoria à Prática. *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos.*, page 50, 2016.

[15] R. B. Sinha, Hemant Kumar Srivastava, and Sumita Gupta. Performance based comparison study of rsa and elliptic curve cryptography. 2013.

[16] Routo Terada. Protocolos Seguros para Pairing e Acordo de Chaves Autenticadas.