Chapter 3 Specification and Design

3.1 Overview

In this section I will be looking at the specification for the message types I will be supporting and my design approach to the problem.

3.1.1 Specification per Message Type

When looking at the message types being used, GOOSE, SMV and MMS its it important to separate them on the different design criteria and topologies. Which means one design approach may not cover all the criteria of all message types in all scenarios.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Message Type | Requirement Name | Criteria | Comment |
| R1 | GOOSE, SMV | Time Constraint | The total time from Publisher Encryption to the message being decrypted by the subscriber should take no longer than 3ms | This is the defining requirement for the algorithm as the time complexity will dictate what solutions should discussed |
| R2 | GOOSE, SMV | Model | The system should support multicast communication for Publisher-Subscriber model | This is to emulate the real-world communication the Smart Grids use to communicate |
| R3 | MMS | Time Constraint | Time is less critical with total time ranging from 100-500 depending if tis a low/medium or command message | These are not very quick time conditions so a wide range of algorithms should be applicable |
| R3 | MMS | Model | Follows a client-server model | This is a more standard model to implement |

3.1.2 Prototype and Algorithm specifications

The messages take part on Intelligent electronic devices (IEDs) and such to make the model practical other design considerations should be used when looking at the system for any Encryption algorithm introduced. The Non-Functional requirements for the prototype and Algorithm follow.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Requirement Name | Priority | Criteria | Comment |
| NF1 | The algorithms must be light weight | High | In order to be deployed to IEDs the algorithms must be able to run in a limited environment | This directly ties into how quickly the algorithm runs with most fast encryption’s methods based around lightweight methods |
| NF2 | Time constraints | High | The specification for message types must be met | The constraints for each message type as mentioned previously must be met by any implementation |
| NF3 | Message Integrity | High | The message sent on any model must be able to be decoded and read by the recipient | All encryption must be able to be decrypted by the intended recipient |
| NF4 | Attack prevention | High | All encryption algorithms used must not be susceptible to any known attack | The implementation must be cryptographically secure from known attacks such as Man-in-the-middle or replay attacks |
| F1 | User Comparison | High | It should be easy for the user to compare different algorithms with different message types. | Using the tool, it should be easy to look at results of |