# Analyzing the Costs of Security on Low Power IoT Devices

Sean Caster, Vincenzo Piscitello, Adam Barton, Ryan Howerton, and Terri Hewitt

Senior Design

Fall 2018

**Abstract**

The goal of this project will be to implement a secured, decentralized meshnet with low minimum resource requirements to enable the connection of a wide variety of low-end devices which lack a general purpose operating system. Our objective will be to investigate the amount of security offered and resources required by various cryptosystems in order to provide organizations interested in securing their low-end device networks with a quantified estimate of the costs and benefits. In addition, we hope to accomplish graceful degradation on our network, meaning that the elimination or temporary unavailability of a given node will have minimal negative impact on the inter-connectivity of other nodes. This will encourage the securing of many resource limited devices which play a critical role in meeting a wide variety of human needs.

October 19, 2018

# 1 Problem Definition

As it stands, a wide variety of mission critical tasks for many utility grids (water, power, etc.) are accomplished by low-end (cheap) devices. The sheer quantity of these devices required to fulfill human needs has lead to a systemic problem wherein increasing their average specifications to facilitate hardened encryption and authentication techniques has been forgone due to the proportionally large amount of resources their implementations would require. In other words, when a device requires few resources to perform its normal workload, dedicating adequate resources for security on that device will require a large percentage of its *overall* resources. What this has meant for many organizations responsible for ensuring the delivery of things, such as water and heat for shelter, is a cost-benefit analysis of high risk, high-avoid-cost. However, this approach is unsustainable as we've already seen in Ukraine and elsewhere where denial of civilization's most fundamental services has already been accomplished through relatively easily recreatable [1]exploits on utility grids.

# 2 (Our Contribution to) The Solution

## 2.1 Setting up our network

To begin, we will need to implement a pseudo-mesh network which will be used as the platform for our research on the financial and computational costs of securing a node. The implementation of our base network will be composed of a central routing authority and low power nodes. The central routing authority will operate on a remote server which will perform verification and authorization of the network nodes. The mode of authentication will use an aggregate or sequential encryption puzzle to verify the potential network node while also providing some level of DDOS protection. The central server interface will request the nodes UUID as input and listen for the individual node to make contact. Upon first contact to node will compute a encryption puzzle based on their production key provided from installation.

After a node has successfully solved the check it will be provided routing information to a coordinator node for its specific communication technology. If the network has separate clusters and the user has requested to join a specific group, that information will be provided to the new node for routing. Given that the node network will be developed based on a multihop mesh network, the new node will perform a series of acknowledgements to be configured into the topology. During this configuration process the node will generate a transmission "line" table to be able to communicate with as many peers it has access too. Utilizing the information of it's cluster the node will be able to perform it's base operation and listen for failed peers. If a peer has failed it's security check, as it has been compromised or has gone offline, the coordinator will be notified and the network will reconfigure.

## 2.2 Using our network for research

Though it's true the security of infrastructure supporting humankind's most basic needs will not come cheap, we believe that a combination of quantification of the costs associated with it and implementation of creative cost reduction techniques for low-end network cryptosystems will demonstrate to many organizations the feasibility of securing their IoT devices that are currently un(der)secured in favor of cutting corners. Our group will set out to quantitatively weigh the costs of electricity and computational power posed by different cryptosystems against the benefits of different levels of security. It's our hope, in doing this, that we will be able to offer insight into the security available to many different users of IoT devices that will have very different budgets, with an eye toward inclusivity for organizations that may only have the budget for less than stalwart security, but an interest in improving all the same.

A key part of our research, then, will revolve around trying out different cryptosystems on many devices utilizing various networking protocols and physical channels (4G LTE, wi-fi, etc.). In addition to testing cryptosystems intended for different resource *distributions*, we'll also look to test systems intended for different resource *quantities*; this will provide data not only for securing highly asymmetric networks, but also more highly resource-limited ones in general. Though the quantification of costs should prove very straightforward (we'll simply measure the battery costs and CPU time required for cryptographic functions), the quantification of security provided will likely be a more involved task. We plan to address this through offering insight into the theoretical "bit-security" of different cryptosystems (i.e. how many bits it takes to express the number of tries a computer will have to make to lie about who it is, read protected information, learn about secret keys, etc.) as well as more holistic analysis in the form of executing attacks on our own network to determine the ease of exploits such as person-in-the-middle and Denial of Service attacks. Though we're certain to find costs for such things that prove prohibitive to some

more risk-oriented organizations, we hope to offer some degree of disambiguation of costs to organizations that are currently on the fence about upgrading security on their low-end devices (or, for those already equipped with adequate resources, implementing effective cryptosystems).

It should be noted that we believe utilization of a recently published authentication system called Fast Authentication with Aggregate Signatures (FAAS) [2] (which allows for a high level of signing efficiency for communications, at the cost of more involved verification) as well as similar resource asymmetric cryptosystems will drastically improve the efficiency of our network. It's clear to us that a big part of making IoT security affordable in the future will come down to distributing costs to those computers best equipped to handle them, by developing systems with strong consideration for the context in which they'll be operating. For example, it may make the difference in a power company's cost-benefit analysis of authentication implementation if resource limited meters could start signing their packets more efficiently while deferring an increased cost of verification to already over-equipped central servers. By consciously distributing the transmission and computational costs of security to hardware, we can make authentication and privacy affordable in many situations where it would've otherwise required costly hardware upgrades.

### 2.3 Deliverables

Given the inquiry-based nature of our project, the final physical implementation of our network will likely be less notable than the findings we accrue along the way. For this reason, in addition to producing an interconnected network of IoT devices running whichever cryptosystem we feel is the best we've come across, our group will provide the following:

- Table enumerating the power and computational cost of authentication with different cryptosystems (as well as number of leakless signatures accomplished under the same key)
- Table enumerating the power and computation cost of encryption with different cryptosystems (as well as a bit-security estimation of the encryption in use for different key sizes)
- Table enumerating the cost of different key exchange protocols, with an eye toward minimizing transmission required of low-end 4G LTE devices
- Reports on success of periodic attacks upon the cryptosystems investigated (responsiveness of network to partial DoS, time taken to detect network irregularity, etc.)
- A list or flow chart of suggested cryptosystems for different resource distributions (e.g. one authentication scheme recommended for resource limited signers, and another for resource limited verifiers)

## References


[1] Q. Z. Y. W. J. L. Ping Yi, Ting Zhu, "A denial of service attack in advanced metering infrastructure network." https://ieeexplore.ieee.org/document/6883456, 2014.

[2] M. O. Ozmen, "Efficient public key cryptography frameworks for emerging iot applications." https://ir.library.oregonstate.edu/concern/graduate_thesis_or_dissertations/9306t4280, 2018.