Paper Review 1

CS 457: Wireless Security

By: Colin Quinn

Article Title: *A survey on IoT architectures, protocols, security and smart city based applications*

Source: <https://ieeexplore.ieee.org/abstract/document/8203943>

1. The world of Internet of Things (IoT) is definitely the way that the market is headed. It is through the use of technologies such as Bluetooth, ZigBee and RFID that any sense of security is available as these IoT devices take hold in every day life. Ideally the paper would have included specific numbers on how many IoT devices use each type of security service and what the success rates are. Using numbers like this allows for more interpretation rather than giving an overview of each type of technology.

Many IoT devices use different sorts of technologies to perform their specific purposes, and as a result leaves an open field for any bad actors as well as any security developers. The authors propose that a mixture of the available technologies will produce the most secure outcomes, however that does not take into account the user experience. These are often implemented in the 4 layers of IoT, IEEE defining the physical and MAC layers while Zigbee defines the Network and Security layer and the application layer.

2. The conclusion of the paper is rather broad and just restates the previously stated information without connecting any topics together. A better solution for this design would be to offer up some best practices when implementing any IoT related security measures. Another weakness of the paper is that it does not really aim to solve a problem. It simply offers up information on IoT security and leaves the reader up to make any extended analysis at all.

Where this paper accels is in its use cases and architectures with a focus on security. High level definitions of technologies like Zigbee in use on Bluetooth, RFID, and WiFi are accurate while still being general enough to be useful in many applications. These applications are then expanded upon to give use cases for any IoT device category such as home offices, identification, and social networking.

3. A main point of improvement is in the details. Providing more detail about how each technology works would give the reader a better understanding of the possible implementations. I would like to give perhaps a specific use case and how that would be implemented with best practices.

Another point of improvement is the comparisons between technologies. The table is incredibly barebones only showing the number of security modes and giving only a couple examples of potential threats.

A good point to rework is to give success related data, or even provide industry wide implementation percents. Some technologies are better than others and providing the adoption numbers of each would give more context to which options provide better results.

4. ZigBee uses 128-bit AES as its standard encryption algorithm with 3 keys, the network key, link key, and master key. Are there any competitors to ZigBee and how do they differ?

There are a few competitors to ZigBee, such as Thread, Z-Wave, and Bluetooth Low Energy (BLE). Some devices such as Google’s Nest device use a combination of these technologies. The Nest uses the Thread protocol in conjunction with BLE and Z-Wave for example. Using more than one of these technologies allows for overlapping security points. Spots where one may falter such as BLE not supporting mesh networks are made possible by others like Z-Wave being entirely mesh network based.