We are living in a place surrounded by a lot of information generated by sensors and appliances that we are dealing with in every day and the Internet of things (IoT) is meant to be connect those devices to each other for several benefits. So, they can be readily accessed from the local network or managed through the Internet. These devices can also communicate to each other (and of course to a hub, as a base station,) to build the entire home network. One of the most popular protocol specialized for using in the constrained nodes and networks (which are usually low-power, low-resource with high-potential to packet loss) is the Constrained Application Protocol (CoAP). Basically, we have identified that there could be three potential source of threads to the network from the communication perspective. **1) An unauthorized access from the Internet** This is stem from the fact that these are limited resources devices and implementing full–fledged authentication system may not be feasible. Hence, the gateway should employ some technique to recognize an unauthorized access and then filter out from the network. **2) Bootstrapping** For the first time setup the nodes in the network, they should be able to agree on some configuration that they want to use for the further communications, like sharing the common key for encrypting their connection. But with respect to the fact the nodes are resource-constrained, they usually can not efficiently perform the task and thus try to use some simple approaches like hard-coding the key and possibly share it in plain text for the initialization purpose. **3) Indoor communication** There could be some security issues to the communication between the nodes in the network because they usually use some open-source implementations of CoAP or other CoAP-based protocol that may not conform the protocol specifications. The indoor communications are also very important because they can be still threated by nearby attacker to for example breach the smart lock and trespass to a house.

In the research, we would like to focus on addressing these threats by using two approaches. Chiefly, we are interested in formally verifying some open-source implementations of CoAP to make sure they conform all the requirements in the protocol specification. Moreover, we are going to design a filtering approach that employs a finger-printing technique to identify an unauthorized access.