Master Thesis Proposal

Smart Home Intrusion Detection Using Network Intrusion Detection Techniques

Student name: Manuel Munoz

Introduction

Recent years have seen the increase of interest in smart homes[1]. The number of products geared towards smart homes has also increased, as is it can be seen at trade shows like CES[2]. Big manufacturers of consumer electronics have reacted to this trend, and have launched product lines aimed towards that market segment. These products take advantage of wireless communication technologies to control and monitor the environment they are in. Wireless communication technology enables seamless integration of these products into everyday life, enabling more ways of interacting with the environments, making them more comfortable, or even more secure.

Problem

According to the statistics gathered by the German police, 2014 saw the highest number of break-ins in 16 years. In comparison with the previous year, there was a 2% increase of break-in cases[3]. These increasing numbers make the people feel less safe in their own homes.

The best known method to secure a household is to hire a security company to provide, install, and also monitor a security system. When a sensor of the security system is triggered, the security company is notified, and can alert both the authorities and the user.

This approach has some drawbacks. The installation of the system comes with a price, because it involves breaking the walls to hide cables and panels that are used to control the system. In order to monitor the household, the security company has access to the the security system, which may raise user's privacy concerns. When the system is triggered, the security company reacts by contacting local authorities or the user. Different events, such as pets being detected, can trigger the system resulting in waste of resources.

One way of tackling some of the existing drawbacks of current security systems, is to take advantage of the increasing ubiquity of smart sensors present in smart spaces. By collecting and analyzing data from smart sensors, it is possible to recognize the usual behavior of the inhabitants of the household [4]. Using the data from the same sources, unusual behavior of the inhabitants can be detected [5].

Proposed Solution

Unusual behavior of network users can be recognized using network intrusion detection systems. These systems analyse communication the temporal patterns of network traffic loads

and the content of the payload. The same type of information can be found in smart environments. In this thesis, we would like to explore the possibility of applying existing network intrusion detection techniques in smart home environment, with a goal of detecting unusual behavior of inhabitants. Special focus will be set on burglary detection scenarios.

As a part of this thesis, we foresee the development of a software infrastructure that will enable us to compare the performance of different algorithms used in network intrusion detection systems. The architecture of the software will have to enable simple ways of extending the software with new intrusion detection algorithms. Our software will have to support seamless integration with the existing OpenHab framework.

References

[1] Google trends. *Smart Home*, https://www.google.com/trends/explore#q=smart%20home (April 2015)

[2] CNET. *A washer in your washer and smart-home sprawl at CES 2015*, http://www.cnet.com/news/a-washer-in-your-washer-and-smart-home-sprawl-at-ces-2015/ (April 2015)

[3] Die Zeit. *Zahl der Wohnungseinbrche auf 16-Jahres-Hoch*, http://www.zeit.de/gesellschaft/zeitgeschehen/2015-04/kriminalitaet-wohnungseinbrueche-deutschland (April 2015)

[4] Chen, C.-W., Aztiria, A., and Aghajan, H.: *Learning human behaviour patterns in work environments.* Conference on Computer Vision and Pattern Recognition 2011 Workshops, 47–52. (2011)

[5] Cook, D. J., and Jakkula, V.: *Anomaly Detection Using Temporal Data Mining in a Smart Home Environment.* Methods of Information in Medicine. (2008)