Demo Abstract: Home Jamming

James Brown, Ibrahim Ethem Bagci, Alex King and Utz Roedig

School of Computing and Communications, Lancaster University
Lancaster, UK

Abstract. Wireless sensors and actuators are increasingly used to automate residential properties. Such home automation (HA) systems are generally built around simple devices and network protocols in order to keep system complexity and prices low. Nearly all used protocols do not provide any security mechanisms and it is possible to inject messages accidentally or on purpose. As it is not feasible to upgrade already deployed devices or to simply re-design the used protocols it is desirable to find a protection mechanism that can be used to augment existing systems. We propose to use jamming in order to prevent unsolicited messages from reaching devices in home automation systems. We demonstrate a jamming device that can be used to augment HA systems to add an additional layer of protection. The device can be integrated into existing home automation systems.

1 Introduction

Sensors and actuators are increasingly used to automate residential properties. Wireless devices are generally used as existing homes have to be retrofitted and rewiring should be avoided. The resulting home automation (HA) system may be used to improve the energy efficiency of the heating system, monitor electrical appliances or control lighting within the property.

A vast number of HA devices are available on the market, using a variety of communication protocols with no particular standard being widely adopted. To reduce cost and system complexity, vendors typically use proprietary protocols, designed with simplicity in mind. A common Modulation scheme used amongst such cheap devices is On-Off-Keying (OOK), combined with a medium access control (MAC) layer designed only to support single hop networks with a limited address range.

Lack of any implemented security mechanisms is a commonality amongst these protocols; confidential data is openly transmitted, and more importantly, message authentication is unsupported. Messages can be injected into a network (accidentally or intentionally), which may then be inadvertently processed by actuator nodes. In many cases this may just be an inconvenience, the heating may turn on when not needed, for example. Other times this may lead to serious situations, such as lights being switched off when walking down steep stairs, or the front door unlocking during the night.

Existing HA systems could be improved by using devices which implement proper security mechanisms. However, given the vast number of protocol specifications, the number of stakeholders involved and the number of already deployed devices, it can be assumed that HA systems will continue to make use of insecure devices and protocols for the foreseeable future.

To add security to existing HA systems we propose the use of jamming. It has been shown that protection against message injection into a wireless network can be provided by jamming [1]. The communication medium is monitored and if an unsolicited message is detected, an interference signal is generated to prevent the target device from processing this message. Obviously such jamming must be executed carefully, only messages targeted to particular nodes should experience interference; other communication, for example in neighbouring properties, should not be affected.

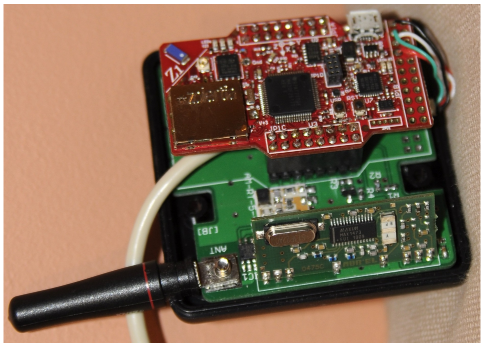

Fig. 1. Jamming device consisting of a Zolteria Z1 node running Contiki with attached daughterboard featuring a $433MHz$ AUREAL RX4MM5 receiver and RF-Solutions AM-RT5-433 transmitter used for directed jamming.

We have constructed a jamming device (see Figure 1) capable of blocking transmissions using a variety of popular home automation protocols in the $433MHz$ band. The device consists of a Zolteria Z1 [**?**] node running Contiki with an attached daughterboard featuring a $433MHz$ AUREL RX-4MM5 receiver and RF-Solutions AM-RT5-433 transmitter. The device can be attached to a HA controller which uses it to improve system security while retaining existing protocols and devices. Our demonstration shows this device in action.

2 HA Protocols

Most HA devices use simple On-Off-Keying (OOK) where a carrier wave (typically $433MHz$, although other frequencies are used as well) is alternately switched on and off. The various implementations of this modulation scheme vary in the timing and semantics of this on-off transition, used to represent data bits. To reduce cost, devices typically only provide receive or transmit capability but not both, thus in the absense of any feedback or acknowledgement channel, the sender will normally transmit each packet a number of times to ensure reception. Error detection codes, such as CRC, are

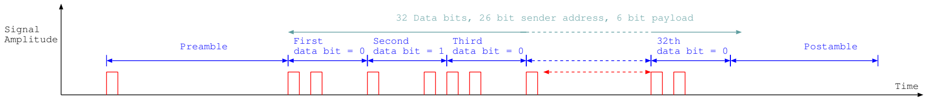

Fig. 2. Unmodulated signal of a packet transmission using the HomeEasy protocol. Each data bit is represented by 2 pulses with specific timing constraints. The described unmodulated signal is multiplied with a carrier signal of $433MHz$ for transmission.

not implemented, and instead a receiver will only process a message if a number of consecutive, identical messages are received. Receivers are paired with specific transmitters, and react upon receiving a message containing a matching transmitter address (included in every message). Multi-hop communication is not used as the transmission range of $433MHz$ signals is sufficient to cover average sized properties.

Figure 2 shows the popular HomeEasy protocol as example. Transmissions begin with a preamble consisting of a $275\mu s$ carrier wave transmission (on) followed by a $2675\mu s$ silent period (off). A transmission ends with an off period of $10ms$ (postamble). A 0 is encoded as a $275\mu s$ on period followed by a $275\mu s$ off period followed by a $275\mu s$ on period and $1225\mu s$ off period. A 1 is encoded as sequence $275\mu s$ on, $1225\mu s$ off, $275\mu s$ on and $275\mu s$ off. A data packet is 32 bits long and contains a 26 bit source address and 6 bit payload (e.g. on or off for switches).

3 Jamming Strategy and Jamming Device

At the centre of a typical HA system lies the controller, which may be equipped with a number of wireless transceivers to communicate directly with devices. All communication runs through the central controller entity. Thus, the controller is aware of all activity in the system; it knows when genuine messages have to be transmitted to actuator devices. Hence, we use the controller to configure and control jamming devices, a number of which may be placed about the property to provide good coverage.

The simplest form of a working jammer would be a device which continuously transmits a high power carrier wave signal, which the controller may interrupt to transit one of its own messages. Unfortunately, it is not advisable to operate such a jammer as it is illegal in most countries to block a frequency range in such a way, and it would also prevent operation of any HA system in neighbouring properties.

Our jamming device is capable of understanding the protocol semantics of a number of HA protocols, such as the HomeEasy Protocol shown in Figure 2. The device scans the observed frequency band continuously until the transmission signature of specified HA protocols is detected; for the HomeEasy protocol the transceiver searches for the preamble sequence. When an ongoing transmission is detected the transmitted address is monitored. The device may only scan the start of the address transmission (address range) to determine if jamming is required. Scanning for address ranges rather than a complete address has the advantage that more time remains to apply the interference signal, which in our current implementation is a continuous carrier wave, applied for the remaining duration of packet transmission after address detection.

Our prototype device is based on a Zolteria Z1 [**?**] which contains a MSP430 processor and a 802.15.4. wireless transceiver. The on chip AES encryption can be used to communicate securely between a home automation controller and a number of deployed jamming devices in a property. A daughter board utilising a $433MHz$ AUREL RX-4MM5 receiver and RF-Solutions AM-RT5-433 transmitter is connected to a single shared antenna via an analogue switch.

4 Demonstrator

The demonstration consists of a HA controller and a number of devices, such as wirelessly controlled socket plugs. The setup operates in the $433Mhz$ band. Our jamming device is attached to the home automation controller and monitors the address range of the devices used. A wireless remote control is provided to represent a potential attacker (using an address of the devices in the setup). Jamming can be activated/deactivated and the system can be tested to see if messages are successfully intercepted.

5 Summary

The prototype device is able to prevent processing of unsolicited messages at actuators within HA networks. However, this protection is not 100% effective. There is a small probability that jamming may not be successful. The jamming device may fail to detect an incoming message or the applied jamming signal may fail to prevent reception of the message at the target device. Jamming failure rates are low (around 0.5% using Home-Easy in usual setting) but our future work aims on lowering failure rates to increase protection.

The demonstrated system does not address all security issues present in HA systems. For example, spoofing of messages originating from sensors or message confidentiality in general are not addressed. However, the device may represent a valuable security building block for future work.

References

1. I. Martinovic, P. Pichota, and J. B. Schmitt, “Jamming for good: a fresh approach to authentic communication in wsns,” in *Proceedings of the second ACM conference on Wireless network security*, ser. WiSec ’09. New York, NY, USA: ACM, 2009, pp. 161–168. [Online]. Available: http://doi.acm.org/10.1145/1514274.1514298