Internet of Things – An Inconspicuous Naked Giant

Yingzhou Yu

Yingzhou.Yu@tufts.edu

Mentor: Ming Chow

Abstract

The connection of physical things to the Internet makes it possible to access remote sensor data and to control the physical world from a distance. [1] The term Internet of Things (IoT) has recently become popular to emphasize the vision of a global infrastructure of networked physical objects. [2] 6LoWPAN(IPv6 over Low power Wireless Personal Area Networks) is a new type of wireless network, usually used on low-power resource-limited devices or sensors. It is probably going to be used on scientific data collection, industry monitoring and detection, etc.; hence preventing 6LoWPAN from attacks will be an important issue. Various attacks on typical 6LoWPAN, including rank attack, local repair attack and resource depleting attack, may destroy the whole network. This paper will briefly introduce Internet of Things, 6LoWPAN and RPL routing protocol, then show some techniques of attacking 6LoWPAN, a demonstration of attack, and discuss possible schemes to defend them at the end.

To the Community

Few revolutionary technologies have created new value pools, displaced incumbents, changed lives, liquefied industries, and made a trillion dollar economic impact. That is, until the Internet of Things (IoT) sprang to life. Today, the next big thing is embedding sensors, actuators, and traditional low-power systems on chips (SoCs) into physical objects to link them to the digital world. However, security issues are easily ignored by the mass. In a report by HP this year, it is mentioned that among all consumers of those IoT devices, 80 percent failed to require passwords of sufficient complexity and length, 70 percent did not encrypt communications to the Internet and local network, 60 percent raised security concerns with their user interfaces, and 60 percent did not use encryption when downloading software updates. [3] All those personal sensitive data could be gathered by means of different IoT attacks.

1. Introduction

1.1 Internet of Things

The Internet of Things (IoT) is the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure. Generally IoT uses small wireless devices to build a network that organizes itself and sends all useful information to a data center (personal computer, server, cloud, etc.).

IoT devices are poised to become more pervasive in our lives than mobile phones and will have access to the most sensitive personal data such as social security numbers and banking information. As the number of connected IoT devices constantly increases, security concerns are also exponentially multiplied. A couple of security concerns on a single device such as a mobile phone can quickly turn to 50 or 60 concerns when considering multiple IoT devices in an interconnected home or business. [3] Thus the security of IoT is becoming more and more important.

1.2 6LowPAN

6LoWPAN is a protocol definition to enable IPv6 packets to be carried on top of low power wireless networks, specifically IEEE 802.15.4. 6LoWPAN is a developing standard from the Internet Engineering Task

Force (IETF) 6LoWPAN Working Group and it was designed from the start to be used in small / pico sensor networks. It is not the case that IP is too "expensive" to use; expensive, in this case, being a measure of code size, protocol complexity, required configuration infrastructure or header / protocol overhead. Implementations of 6LoWPAN easily fit into 32K flash memory parts (typically smaller than Zigbee or other protocols). [4]

1.3 RPL

6LowPAN uses IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) as its routing protocol. Low-power and Lossy Networks (LLNs) consist largely of constrained nodes (with limited processing power, memory, and sometimes energy when they are battery operated or energy scavenging). These routers are interconnected by lossy links, typically supporting only low data rates that are usually unstable with relatively low packet delivery rates. Another characteristic of such networks is that the traffic patterns are not simply point-to-point, but in many cases point-to-multipoint or multipoint-to-point. Furthermore, such networks may potentially comprise up to thousands of nodes. These characteristics offer unique challenges to a routing solution: the IETF ROLL working group has defined application-specific routing requirements for a Low-power and Lossy Network (LLN) routing protocol. [5]

1.4 Contiki and Cooja

Wireless sensor networks are composed of large numbers of tiny-networked devices that communicate untethered. For large-scale networks it is important to be able to dynamically download code into the network. In this paper we did simulation in Contiki, a lightweight operating system with support for dynamic loading and replacement of individual programs and services. Contiki is built around an event-driven kernel but provides optional preemptive multi- threading that can be applied to individual processes. [6]

Cooja is the Contiki network simulator. Cooja allows large and small networks of Contiki motes to be simulated. Motes can be emulated at the hardware level, which is slower but allows precise inspection of the system behavior, or at a less detailed level, which is faster and allows simulation of larger networks.

2. IoT attacks

2.1 Rank (Sinkhole) attacks

In sinkhole attacks a malicious node advertises an artificial beneficial routing path and attracts many nearby nodes to route traffic through it [6] by changing its rank. The RPL routing rule states that ‘rank strictly

increases in the downstream direction and strictly decreases in the upstream direction'. This rule is created to prevent the nodes from creating unoptimized path or loop path. The RPL creates node rank as its unique parameter for easily choosing and maintaining the optimized path. The RPL requires all the nodes to check and follow this rule; however, its mechanism cannot protect against attacks from cooperated malicious node behaviors.[7] The rank attack is easy to be implemented but difficult to be revealed because it does not need to spoof anything and most of the behaviors of the compromised nodes look like normal from their neighbors' point of view. This attack in itself does not necessarily disrupt the network operation; however when coupled with another attacks, it can become very powerful. What's more, if the transmit power of malicious node can be tuned to maximum, the effect range would be even wider and thus the attack would be more powerful.

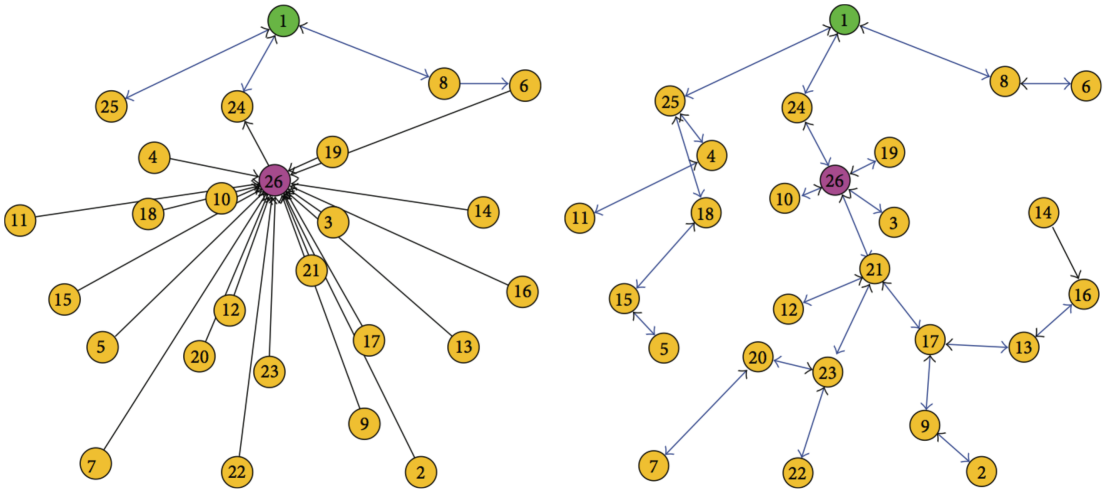

Fig 2.1 Left shows an attacked network while right is not attacked (sketch)

2.2 Selective-Forwarding attacks

With selective-forwarding attacks it is possible to launch DoS attacks where malicious nodes selectively forward packets. This attack is primarily targeted to disrupt routing paths; however, it can be use to filter any protocol. For example, an attacker could forward all RPL control messages and drop the rest of the traffic. This attack has severer consequences when coupled with other attacks, for example, sinkhole attacks.

2.3 Resource depleting attack

Nodes in RPL are resource constrained so if they have to do too many missions, they will become exhausted. However, there is no mechanism in RPL to limit the actions that a node should do. The adversary, therefore, can reprogram a node so that it starts resource costing activities such as broadcasting, sending control messages much more than needed. This behavior can also affect the operations of other neighbors. Once the activities are large enough, the node becomes exhausted and network operations will be downgraded. [7]

2.4 More attacks

There are other typical attacks like local repair attack, wormhole attack, clone ID / Sybil attack, etc., but we will not discuss further here.

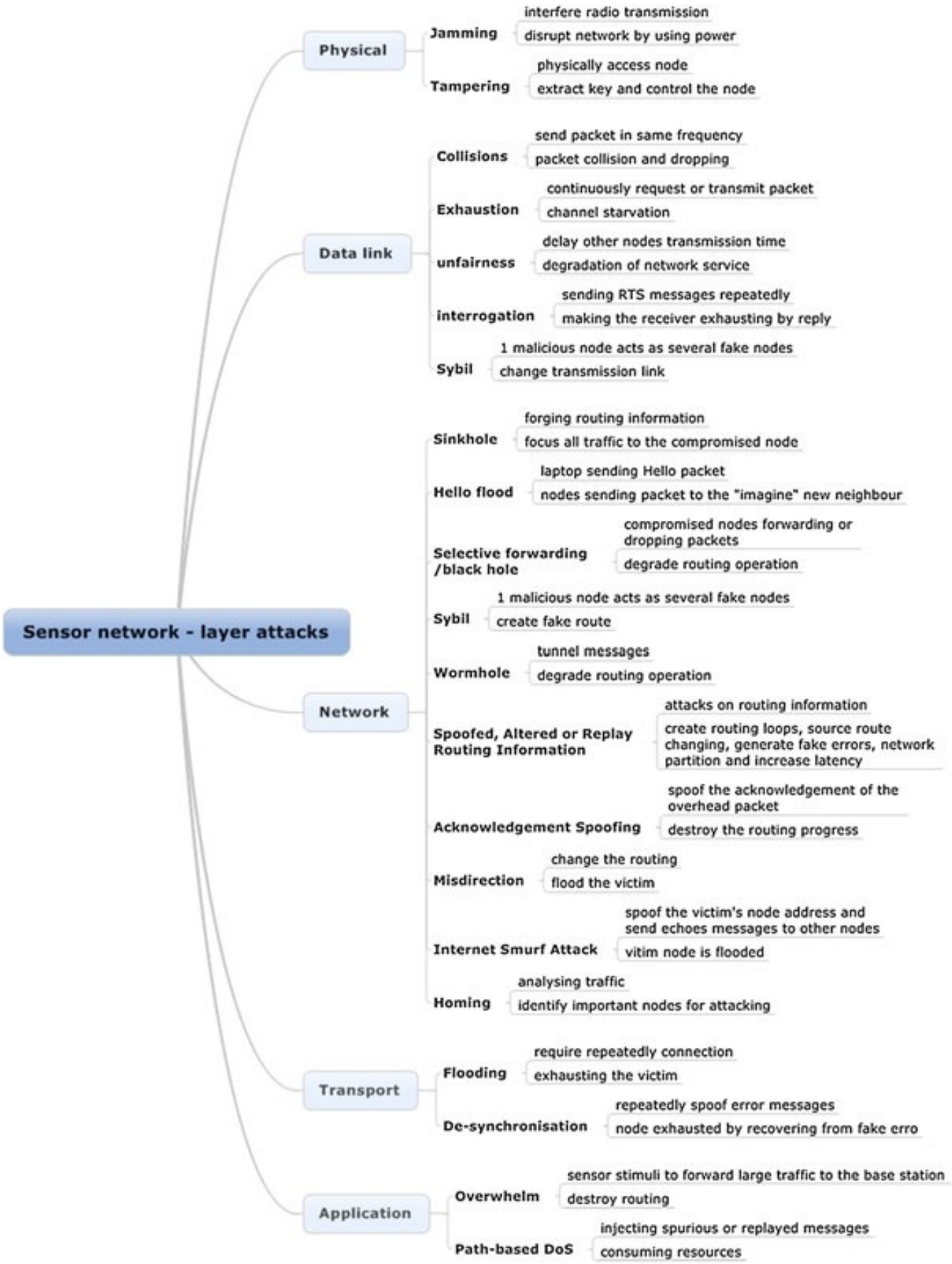

Figure 2.2: Various attacking methods of wireless sensor networks [7]

3. Action Items

3.1 Preparations

I installed and configured Contiki, following the tutorial. Then I learnt how to modify Contiki source codes. I also studied how 6LowPAN and RPL works. Finally the Cooja simulator works properly and with enough output information, as is shown below:

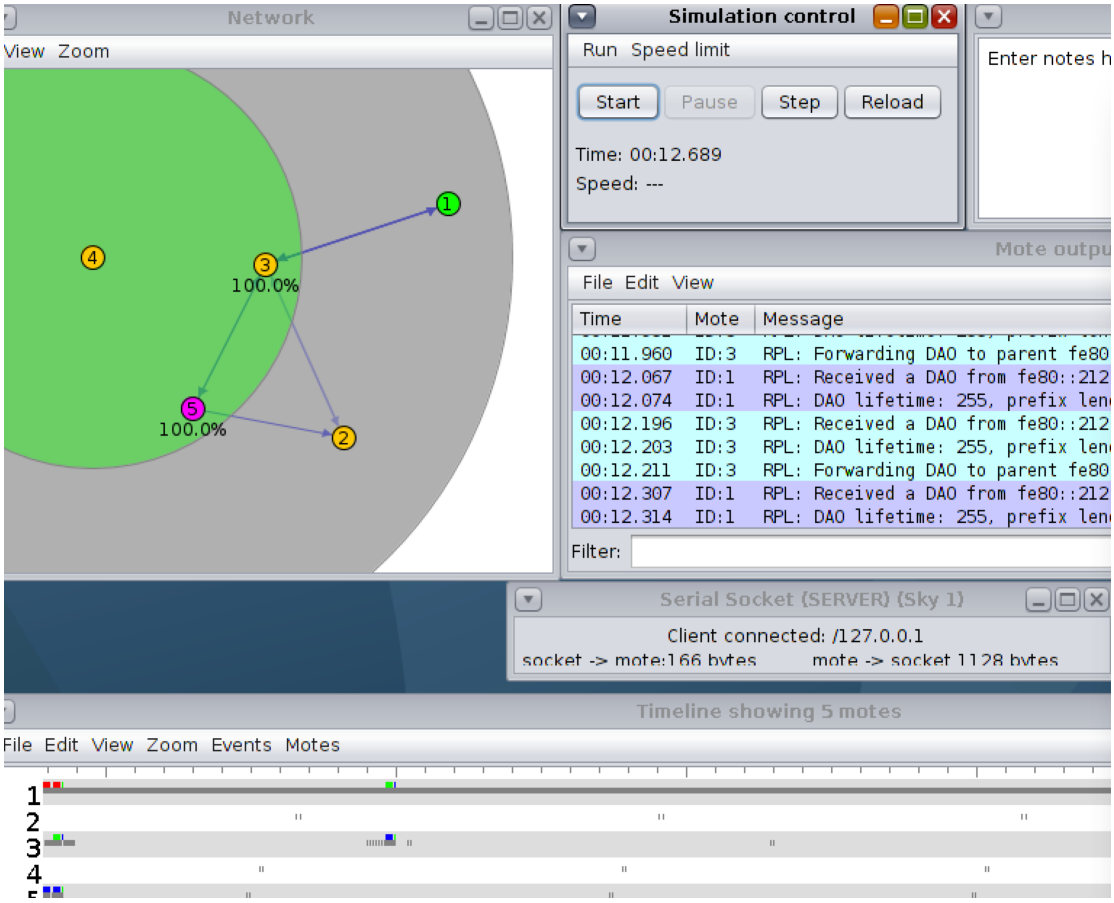

Figure 3.1: A handy simulator with proper debug information

3.2 Code modification

Contiki OS is based on Ubuntu, but it has its own layer of code compiling. Mote's code is written by C, but with many limits because Cooja uses

MSP430-GCC instead of general gcc. The size of code is also limited because of mote's ROM/RAM size. I spent several weeks modifying example code and finally implemented Sinkhole attack and Selective-Forwarding attack. For selective-forwarding attack, I blocked all packages other than ICMP packages, and dropped them.

Key files are included:

contiki/core/net/rpl/rpl-icmp6.c (for sinkhole attack)

contiki/core/net/uip6.c (for selective-forwarding attack)

Replacing corresponding file makes mote's code malicious.

The example codes I use to simulate are:

contiki/examples/ipv6/rpl-boarder-router/boarder-router.c

contiki/examples/ipv6/sky-websense/sky-websense.c

3.3 Attack results

First, I tried sinkhole attack:

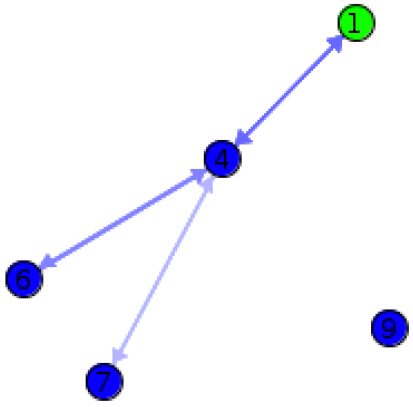

Figure 3.1(a): Left - before attack

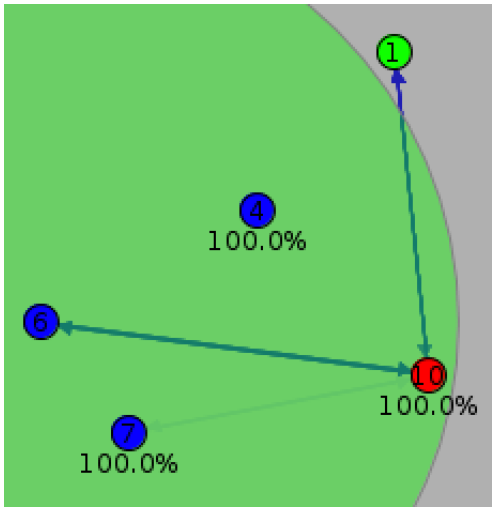

Figure 3.1(b) Right - after attack

As is shown, generally nodes can figure out their shortest/best path to router, in the snapshot node #4 is the next hop of node #6 and #7. After I replaced the normal node #9 to a malicious node #10 and several minutes later (so that the routing table of node #6 and #7 will refresh), node #10 took over the job of #4, which any applications running above it wouldn't even notice (actually I kept pinging node #6 and #7 and found nothing abnormal from the terminal, and small servers running on them were working properly).

Then I tried selective-forward attack:

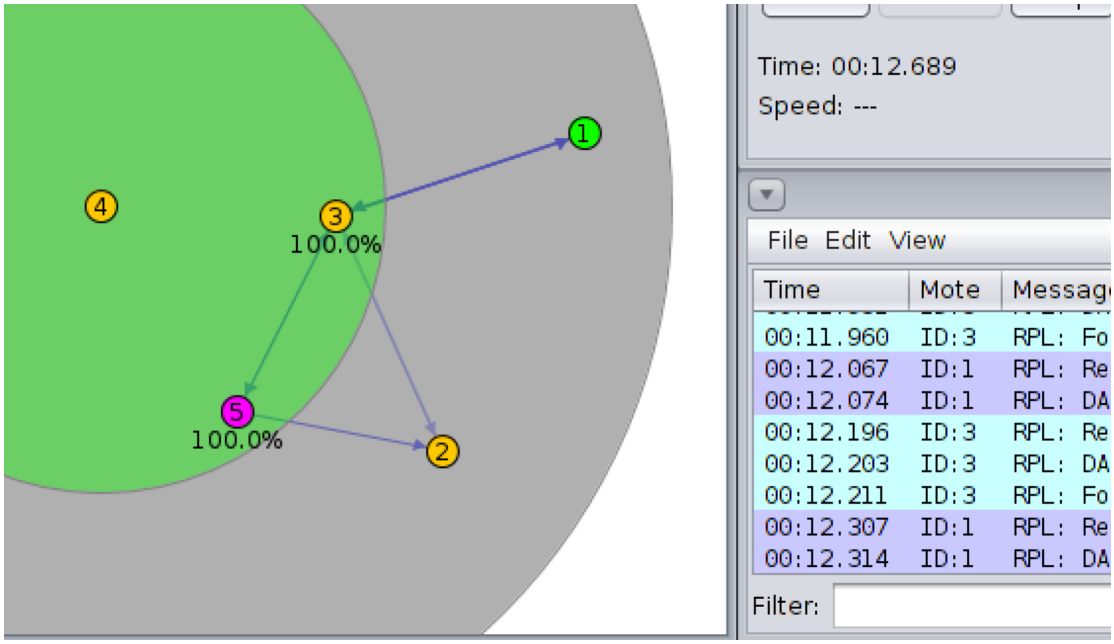

Figure 3.2: selective-attack result

The snapshot seems normal after I replace node #3 with malicious code, as node #3 is transmitting data with server node #5 and router node #1. The only difference is I cannot reach node #5 after attack starts. The blue arrows on the snapshot indicate that ICMP messages are sent properly.

This selective-attack node transmits ICMP messages as usual, but drops all other data, for example, HTTP request.

Finally I tried to combine the two attacks together and succeeded, just by replacing both files to malicious ones. No change can be seen from Cooja; those nodes' servers simply went down.

4. Defenses - Intrusion Detection Systems

To counter attacks in a network, Intrusion Detection Systems (IDSs) are used. An Intrusion Detection System analyzes activities or processes in a network or in a device and detects attacks, reports them, and/or mitigates the harmful effect of the detected attacks. Due to the diversity of attacks and the unpredictable behavior of novel attacks, IDSs are subjected to false positives (to raise an alarm when there is no attack) and false negatives (not raising an alarm when there is an attack). Generally, there are two categories of IDSs: **signature based** and **anomaly based**. Signature based detections compare the current activities in a network or in a device against predefined and stored attack patterns called signatures. This approach cannot detect new attacks, needs specific knowledge of each attack, has a significant storage cost that grows with the number of attacks, and has a high false negative but low false positive rate. Anomaly based detections determine the ordinary behavior of a network or a device,

use it as a baseline, and detect anomalies when there are deviations from the baseline. This approach can detect new attacks but has comparatively high false positive and false negative rates because it may raise false alarms and/or cannot detect attack when attacks only show small deviations from the baseline. [6] The current trend in IDS research is to combine these methods for having more accuracy and more functions.

6LoWPAN is still a new and on-going research area. At this time, there are only a few security solutions proposed for the standard. Cryptography solutions focus on choosing a fast, lightweight and secured encryption, and an effective key management method. Even when 6LoWPAN has an ideal cryptography line defense, there is still a need for implementing an IDS for dealing with network performance threats such as DoS and other resource attacks. The IDS will discover and stop most of the attacks that break cryptography protection to make changes on the network operation. However, no IDS solution has been proposed for 6LoWPAN security. This part takes the natural characteristics of 6LoWPAN to analyze the difference to other networks to clarify a 6LoWPAN IDS.
6LoWPAN combines 802.15.4 and IPv6 so its IDS needs to monitor traffic arriving from both sides. The traffic patterns between the two networks are different, so no single traditional solution from IPv6 or WSN can be applied straight away. The IDS solution should have two

modules, one to keep track of the sensor network and the other to check the traffic patterns from the IP network. These two units should cooperate for better performance and resource saving. [7]

5. Conclusions

Internet of Things is a fresh but important area in terms of security, and people are more likely to ignore it. When security comes to resource constraint wireless networks, e.g. 6LowPAN, it is more likely a tradeoff between security and low-cost/easy-implementable. I’m working on another project that also use Contiki and Cooja, and when I was coding those motes, I can hardly burn my code into motes because of limited ROM and RAM. The real problem is that there seems to be no place for simpler security codes, not to mention those professional IDSs. Also, the CPU and power usage for IDSs could be even larger than motes themselves. I don't think this is good for IoT, however, the only solution now I can come up with is to expand resource limits of motes. Maybe we should start further discussion about standards of 6LowPAN and add frequency hopping/encryption choices.

References:

1. Kopetz, Hermann. "Internet of things." *Real-Time Systems*. Springer US, 2011. 307-323.

2. Zhang, Qi, and Dewei Peng. "Intelligent Decision-Making Service Framework Based on QoS Model in the Internet of Things." *Distributed Computing and Applications to Business, Engineering & Science (DCABES), 2012 11th International Symposium on*. IEEE, 2012.

3. Hewlett Packard (HP Inc.) “Internet of Things Research Study” report, 2014.

4. Mulligan, Geoff. "The 6LoWPAN architecture." *Proceedings of the 4th workshop on Embedded networked sensors*. ACM, 2007.

5. Winter, Tim. "RPL: IPv6 routing protocol for low-power and lossy networks." (2012).

6. Wallgren, Linus, Shahid Raza, and Thiemo Voigt. "Routing Attacks and Countermeasures in the RPL-based Internet of Things." *International Journal of Distributed Sensor Networks* 2013 (2013).

7. Le, Anhtuan, et al. "6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach." *International Journal of Communication Systems* 25.9 (2012): 1189-1212.

8. Hummen, René, et al. "6LoWPAN fragmentation attacks and mitigation mechanisms." *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*. ACM, 2013.

9. Chugh, Karishma, Aboubaker Lasebae, and Jonathan Loo. "Case Study of a Black Hole Attack on 6LoWPAN-RPL." *SECURWARE 2012, The Sixth International Conference on Emerging Security Information, Systems and Technologies*. 2012.