6lo Technology for Smart Cities Development:Security Case Study

Anass Rghioui
LIST Laboratory
FST Of Tangier
UAE University

Anass Khannous
LIST Laboratory
FST Of Tangier
UAE University

Said Bouchkaren
Labtic Laboratory
ENSA Of Tangier
UAE University

Mohammed Bouhorma
Pr. Research Director
LIST Laboratory
FST Of Tangier
UAE University

ABSTRACT

Excessive demand and the urgent need for the development of smart cities, evoke the need to provide the capacity for more low-resource devices to communicate and collaborate at a distance, in order to make the concept of the internet more real and practical.

For this, IETF "IPv6 over Networks of Resource-constrained Nodes" (6lo) workgroup works on equipment of all resource constrained devices by IPv6 protocol to integrate the internet.

From the security point of view, this integration is not without risks, the Internet carries many dangers and current security mechanisms are very greedy for such devices.

This paper analyses potential security threats in 6lo as a particular case of mobile ad hoc networks, and provides some countermeasures ideas, in particular, the two principal security defense lines: the cryptography as a first line and the intrusion detection system as the second line.

General Terms

Internet, IPv6, Cryptography, IDS, Security.

Keywords

Smart cities, 6lo, 6LoWPAN, Internet of Things, Network Security.

1. INTRODUCTION

With the immense and rapid development of the Internet of Things (IoT), integrating different devices to the internet becomes an indispensable need. Communication interaction are transformed from human-to-machine to machine-to-machine (M2M), and more specifically things-to-things.

In the practical field, this technology progress facilitates the leading of smart cities [1], where different cohabited object can communicate and interact to decide instead of human, or to help managers to make more effective decisions. It supports the improvement on many life applications like logistic, healthcare, industry ... etc. Mainly for monitoring requirement where we must use sensors devices to capture data in physical or environmental conditions.

Enabling resource-constrained devices to connect to the internet by implementing them by IPv6 protocol, gives the possibility to transfer data through the network to any location in the entire world. An IETF 6lo WG (IPv6 over Networks of Resource-constrained Nodes Work Group) was created as a successor to 6LoWPAN WG (IPv6 over Low power Personal Ad hoc Networks) who succeed to integrate IEEE 802.15.4-besed devices by IPv6 [2], [3] . 6lo WG was created as a normal evolution to find a solution for all devices with limited resources to connect to the internet.

The choice of the IP technology has many benefits, this solution allows the use of existing network infrastructure, also, 6lo devices can be connected easily to other IP networks without the need for translation gateways or proxies.

IPv6 is strategic choice too, it provides the addressing of a huge number of devices since an IPv6 address is 128 bits long, this provides 3.4 x 10^{38} addresses, more than 667 million billion addresses per square millimeter of land surface.

Inasmuch as the Internet of Things is based on an open architecture [4], and the weaker characteristics of resource-constrained devices, security issues becomes more sensitive. Another issue that can be added are security management in the case of implementing different devices from different origins in the same environment. In the IoT context, for giving the opportunity for intervention from different experts and encourage concurrence, devices from different origins must be cohabited in the same place.

This paper analyzes the security challenges in 6lo networks, it studied the various countermeasures to address these needs, their advantages and disadvantages, and it offers some recommendations to achieve a reliable security for a powerful 6lo network.

The structure of the paper is as follows: Section 2 gives a brief overview of Smart cities, IoT, 6lo and their main applications, Section 3 reviews the assumption and discusses the issues of 6lo security, Section 4 presents the requirements of the security application. Section 5 and 6 discusses some solutions for securing the network with the focus on the cryptography and the intrusion detection systems (IDS). Finally, Section 7 concludes the paper.

2. OVERVIEW

2.1 Smart cities

Smart cities is a set of interconnected systems collaborating together and using technology tools in order to offer a better city management system. Used tools are a whole of small connected devices accessed from a distance. Interaction between them facilitate communications and offer better coordination. They form a working group with huge possibilities in monitoring, surveillance, and management giving real time data to managers and citizens to anticipate problems and have sufficient information for better decisions.

Most of actors involved in such projects are industrial sectors of energy, water, transport, telecom network and infrastructure companies, builders working on the hardware equipment of smart cities, integrators and services companies.

2.2 Internet of Things

Internet of Things is a concept that aims to extend the internet to the real world by associating labels bearing codes, RFID tags or URLs to objects or places, making them available and accessible from anywhere and anytime.

For that, many technologies must be used and integrated to achieve this goal. Devices are different, and some of them, like Wireless Sensor Network (WSN) [5] are resource-constrained, they are not compatible with existing protocols for internet communication. These protocol must be adapted or new ones must be developed.

Fields of applications include: waste management, urban planning, environmental sensing, social interaction gadgets, sustainable urban environment, continuous care, emergency response, intelligent shopping, smart product management, smart meters, home automation and smart events [6].

through fragmentation and assemblies to be supported by the IEEE 802.15.4 link layer.

6LoWPAN network consists of one or more stub networks connected to the internet through the Edge Router. This latter, called also Border Router, routes traffic in and out of the LoWPAN, which is the collection of 6LoWPAN nodes sharing the same address prefix IPv6, ie the first 64 bits, it is used with IID (Interface Identifier) to form the IP address. This address is formed using the SSA (Stateless Address Autoconfiguration) [8] in the starting phase of the network construction: the bootstrapping. This phase is managed by the data link layer which allows the establishment of first communications between nodes to configure channel, security keys and addressing.

After the bootstrapping phase, and once the data link layer is functional, 6LoWPAN Neighbor Discovery protocol [9] - that was chosen instead of the Neighbor Discovery protocol [10] because of its incompatibility with the low-power wireless networks - is used to start the construction of the entire network through some messages exchanged between nodes that allow hosts, routers and Edge Router autoconfiguration.

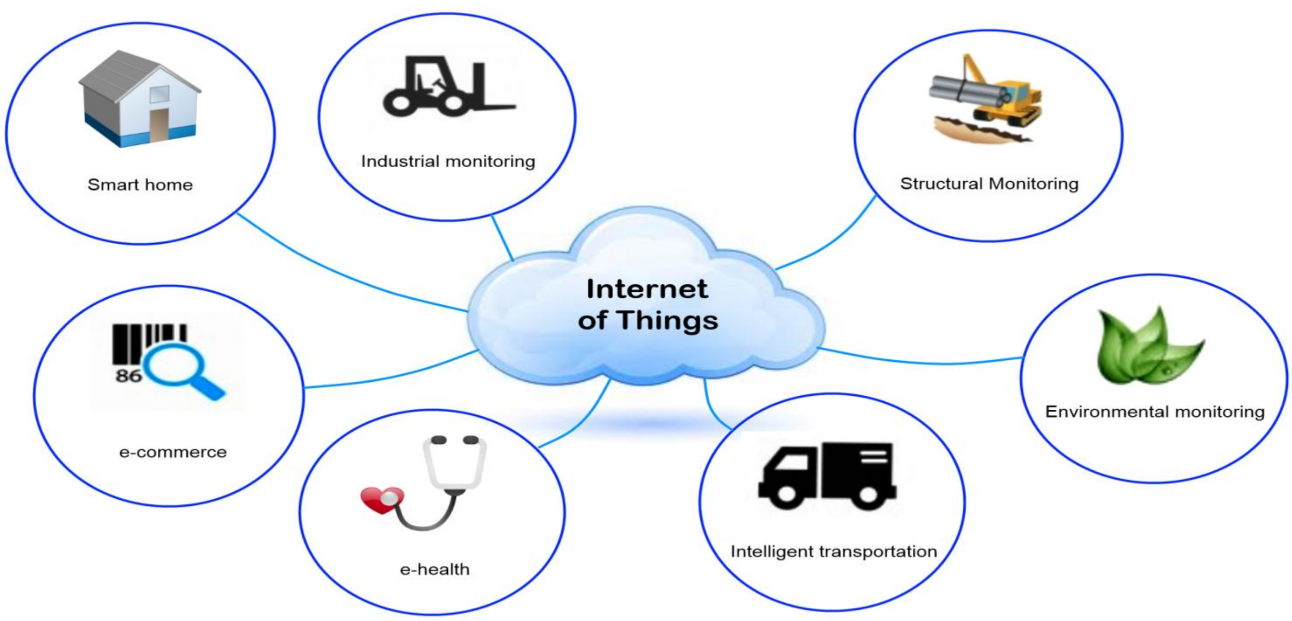

Fig 1: Smart city applications

2.3 6lo: IPv6 over Networks of Resource-constrained Nodes

As 6lo is successor of 6LoWPAN, it will follow the same structure and the same mechanism, with improvements.

6LoWPAN is a combination between the IPv6 and IEEE 802.15.4 [7], two totally different networks. The most important difference is the size of the IPv6 packet measuring 1280 bytes, but the 802.15.4 supports only 127 octets packets, where the solution proposed by the IETF 6LoWPAN working group to add an adaptation layer that optimizes IPv6 packets

3. 6lo SECURITY MENACES

This section analyzes the different possible attacks from the internal and external sides that target all layers of the 6lo devices.

These attacks can be classified into two types, internal attacks by malicious nodes or external attacks by unauthorized devices.

And they are classified into two categories, passive attacks where the attacker has as main purpose to spy the network and catch secret information, this kind of attack is difficult to detect because it takes no damage on the equipment, and active attacks that interfere directly on the network performance and can cause its malfunction as Denial of Service attacks.

Threats are several, and each layer in the 6lo devices stack can undergo specific attacks:

1) Physical layer: In the physical layer, the attacker can disrupt communications by Jamming attack targeting frequency used by nodes to communicate. In Tampering attack, the attacker captures and exploits the node to retrieve information such as secret keys of security and / or modify its information to control the node or just to spy it.

2) Link layer: The link layer undergoes several attacks, there are some attacks that drain the node battery as Exhaustion attack where the attacker sends a continuous and repetitive unnecessary packets to trigger the processes in the node to make it indispensable, or as Interrogation attack where the attacker sends RTS messages repetitively to make the receiver responds with a CTS messages continuously to cause its energy depletion. Other attacks targeting the same layer are Collisions attack, where the attacker sends packets with the same frequency to cause the packets collision and therefore the loss of information communicated between nodes, and Sybil attack where malicious node acts as a normal node to change the information exchanged in the network and causes its malfunction.

3) Network layer: The network layer is the layer that undergoes the majority of attacks such as Sinkhole attack where malicious node's goal is to divert all messages communicated to other nodes. The Hello flood attack occurs by sending excessive Hello messages to a node to make it sends answers too, to consume more energy. In Blackhole attack, compromised nodes throw received messages to cause routing problems. The Sybil attack happens at this level as follows: malicious nodes create false routes to divert the messages circulating through the network. In Wormhole attack, the malicious node creates a false road to destabilize the routing within the network. The Spoofing attack goal is falsifying routing information. In Internet Smurf attack, the attacker imitates the victim node address and sends echo messages to other nodes, to flood the victim by their answers. Other dangerous attacks are the attacks on the IPv6 neighbor discovery protocol that is crucial in establishing the network and the communication between nodes, there is a secure version of this protocol but it is not compatible with this kind of networks.

5) Transport layer: There are not a lot of attacks targeting the transport layer, the attacker tries to exhaust the energy of the victim node via multiple connection requests by Flooding attack, or force him to react with synchronization messages imitating error messages by the De-synchronization attack.

6) Application layer: Two dangerous attacks can target the network through the application layer, the Overwhelm attack aimed destroying the routing by generating huge traffic to the Edge Router, and Path-based Dos attack aimed depleting resources by injection of false messages.

4. 6lo SECURITY REQUIEREMENTS

In the smart city context, many domains can benefit from 6lo advantages, especially domains that require monitoring, where security is a necessary thing to protect the collected information and prohibit control by non-identified entities.

1) Industrial monitoring: Applications based on the 6lo network can be very beneficial for industrial operations such as machines remote monitoring, especially energy efficiency side, the production quality, and the production machine supervision. The current monitoring methods are expensive and difficult to implement, unlike 6lo devices that are easy to implement, inexpensive and they can be manipulated remotely via the internet. Thus, 6lo applications in this area may be beneficial for stock and storage operations monitoring to provide instantaneous data to make quick decisions.

The main security requirements in this area are insurance of 6lo devices operation and the reliability of collected information by the monitoring devices. Also, the access should be allowed only to authorized persons.

2) Structural Monitoring: In large construction projects, important and critical structures, such as bridges, the monitoring is essential, for intervening in emergency cases or even eliminate them before they occur, also for monitoring the process and the work progress.

In this case, the reliability of the information and authentication of senders and those who have access to this information are the most important security elements to be predicted.

3) Environmental monitoring: Monitoring of specific environmental places is one of the most difficult tasks to do in place because of the access difficulties.

Using 6lo devices, information gathering will be a possible mission. In this case, monitoring can help prevent natural disasters that can cause a lot of damages.

The reliability of information is important, and if there is the possibility of control, authentication must be considered.

4) Vehicle telematics: Integration of 6lo in intelligent transportation is an important thing. The implementation of 6lo devices in roads, vehicles and the traffic signals will make accessibility and monitoring data transport easy and possible at any time, and it will help to manage transport traffic.

In this case, the security elements that must be taken are the assurance of the information availability and provide devices physical security.

5) Smart homes: Smart homes are those containing manipulable and programmable objects to facilitate chores and make them more convenient.

6lo technology will surely help this kind of houses to promote and will offer intelligent tools manipulated through the internet to monitor the house security, and have the ability to control it in distance.

For security, the parameters needed to prevent depend on the application, if it is to control dangerous devices, controller authentication is essential. If there is secrets information to communicate, confidentiality in this case is important and mandatory.

6) Healthcare: In the medical field and patient monitoring, 6lo devices can save lives by monitoring the state of a patient remotely to check his health, and react with alarms that can trigger the medical devices.

This field can have multiple applications that vary according to the patient needs, or any person with difficulties that needs to be monitored, to let the others react at the crucial moment.

The privacy and security of data is mandatory in this case, also the authentication of persons who can control these devices.

7) Commercial: 6lo can be beneficial also in commercial or entertainment applications, where users can have 6lo devices embedded in everyday objects or for entertainment purposes. And through these objects, companies will have the opportunity to contact their customers directly.

This application must absolutely ensure the confidentiality of communications and data exchanged, and the authentication of each user.

5. SECURITY GOALS

To be publicly accepted, 6lo needs to have a strong security defense system. However, existing security protocols cannot be applied directly in this devices because of their constraints resources. An important thing that must be applied it's the security of end-to-end communications to provide a secure way to 6lo devices to communicate with other IP hosts via the internet.

6lo will not be very different from other MANETs, especially 6LoWPAN as it represents its successor, for that, 6lo security goals will be approximately the same as it mainly aim to protect communication between the end users. The most important requirements are:

1) Confidentiality: to ensure the confidentiality, limit network access and data to authorized users.

2) Authentication: the reliability of the data transmitter

3) Integrity: the data must not be changed during transmission between the transmitter and the receiver.

4) Freshness: consider for both data and key to ensure no replayed of old messages

5) Availability: the availability of data in case of need

6) Resiliency: provide an acceptable level of security even in the case some nodes are compromised

7) Energy efficiency: reduce the control overhead to maximize network lifetime

Aside basic security requirements shared between all this kind of ressource-contrained networks, 6lo has its additional specifies as it is an IP-based network:

9) End-to-end security**:** The IP address provides the end-to-end communication between any two nodes in a network, for this we need an end-to-end security mechanism that will guarantee reliability of exchanged data through the whole network. Normally, end-to-end security is provided by encryption, but face constraints arise in this solution due to low resource devices. For this, we must consider many parameters to establish a right specific cipher suite since existing solutions are not compatible with 6lo. Many other questions must be asked like what will the possible situations in which end-to end security will be inevitable? How to handle security vs. packet size tradeoff? And how to split work between low capability end nodes and border proxy devices? What key management solutions to be used?

10) Malicious node detection mechanism: A device in a network is a node among others, it operates either alone or with a group of nodes as in the case of wireless sensor networks, the presence of a malicious node can jeopardize the integrity of the whole network. The device itself can behave in an incorrect manner due to a malfunction on its software level or in its hardware level.

In case of a large network consisting only of resource-constrained devices, the intrusion of a malicious node or compromising a healthy node will be an easier scenario for the attacker. To avoid this scenario, obtaining a system, which detects these node and protects the network from a failure, will be crucial.

6. SECURITY SOLUTION

6.1 Cryptography

6.1.1 Analysis of existing solution

Cryptography is the basic and the most used solution in any security system, since it guarantees authentication, confidentiality and integrity, only the nodes that have the correct key can read, decrypt and verify the integrity of exchanged messages.

Cryptography will also ensure the end-to-end security, for that, IPsec already exists to secure the network layer that works with IP, IPsec based asymmetric cryptography, claiming to be heavy for a network of devices limited resources. There has lightweight release to adapt this protocol to such networks testing to be compatible with devices with limited resources.

Normally, most of recommendations suggest the use of symmetric key cryptography for these networks, for it did not need a lot of computation and therefore it preserves energy. However, recent research developments showed ways to combine RSA (Rivest - Shamir - Adelman asymmetric encryption) and ECC (Elliptic Curve Cryptography) technical with several modes to adjust to resource-constrained network scenarios.

A major problem in cryptography is key management, especially in the case of 6lo networks where there is not a well-known established infrastructure that can be used as a basis for keys sharing. IPsec uses the Internet Key Exchange (IKE) solution, but is not considered as a feasible solution because of its heavy signaling messages, which is unsuitable for the small packet size and nature of the energy efficiency requirement.

Many solutions have been proposed to solve the problem of key management in low resources and constrained networks like WSN and RFID, but they operate at the level of local networks and does not guarantee an exchange between two nodes separated by long distances and communicating through the internet.

6.1.2 Proposed solution measures

In the case of smart cities, a lot of information will be shared and exchanged between several nodes of various origins cohabited in the same place. A Remote Server located somewhere in the internet that will manage the authentication nodes and key exchange between them will be a good solution.

Any node unless those defined in the Remote server has permission to join the network, or has the possibility of establishing a security key. Also, no IP host can communicate with a 6lo node directly, it must pass by the Remote server and only authorized ones can communicate with network nodes.

In smart city context, most of nodes will be placed in distributed topologies, for that, two elements are important to take into consideration, flexibility and scalability, we must deal with this two concepts by modeling a schema that tolerates changes in topology and do not depend in a specific infrastructure.

Any key management solution must be evaluated relative to three criteria: energy efficiency, an essential element for resource-constrained networks, scalability of the model in a dynamic network like distributed networks, and security the main objective of cryptography.

The key management system must be flexible towards changes in: topology, nodes positions, and network density, in any position, both can establish a secure communication using their shared key. A device should easily change a router by another, for route optimization, due to a malfunction of a node, a change of position, or for another reason.

We must avoid any sharing of information that may present a risk to the network, if it is possible, the key generation should be done in the node itself. And all communications and data exchanged in the network must be encrypted.

From energy point of view, which is a critical criterion of choice to adopt or not a solution, the solution must not require a lot of calculation or exchange between devices to establish security keys. For that, is better to use a symmetric cryptography which is recommended by experts in the field.

6.2 Intrusion Detection System

6.2.1 Analysis of existing systems

IDS ensure network security by providing a mechanism for detecting and revoking malicious nodes. In its operation, it is based on several approaches that differ according to the environment in which it is deployed.

In the case of 6lo networks, there may be two types of IDS, as the operation of the device that is equipped with this technology, the NIDS (Network Intrusion Detection System Based), they provide security at the network level, and HIDS (Host Based Intrusion Detection System), they provide security at host.

In general, the operation of the IDS is based on the collection and analysis of node or network data, it needs a lot of computation and a huge storage space for these data, and which will be performed by the collaboration of multiple nodes between them, the thing that consumes a lot of energy.

Having a hybrid IDS that combines between NIDS and HIDS functionalities, that does not consume a lot of energy, and has a high rate of intrusion detection is a very important solution for 6lo but also a huge challenge for researchers.

6.2.2 Suggested solution: AIS-based IDS

The Human Immune System (HIS) has long been a source of inspiration in several areas including the computer networks security as the main scope of application. Researchers have taken advantage from the benefits of HIS to be the best system that protects human body against invasive pathogenic intrusions in order to propose several artificial immune algorithms that are all part of what we call Artificial Immune Systems (AIS). However, it is not only interesting to draw inspiration from HIS while producing AIS based algorithms as much as it is interesting to propose an algorithm with high performance. We claim here that 6lo networks is a perfect application area since there is lot of similarities between the operation mechanism of such networks and the HIS mechanism. Also, 6lo could be seen as a collection of mobile, decentralized, self-organizing and self-adaptive network nodes, thing which adds more challenge to the security of this kind of environment.

The role of HIS is to protect the human body against invading pathogens and to detect danger coming from outside as well as from inside. It consists of immune cells moving inside the body tissues and communicating with each other while forming all together a dynamic and self-organized network. All these characteristics lead us to think of taking inspiration from HIS to enhance 6lo IDS since there is a strong analogy between 6lo environment’s own characteristics and the abstraction of HIS properties.

They can be resumed in the following characteristics:

1) Distribution: Both of them form a parallel, distributed and adaptive system.

2) Collaboration: Nodes in 6lo networks complete specific tasks collaboratively. Similarly, various immune cells cooperate with each other.

3) Dynamism: Dynamic topology means that new nodes join the network while expired ones leave it. Similarly, new immune cells born on one side and other existing die. The organizational structure is dynamically adjusted.

4) Exclusion: 6lo network should be able to identify and resist against enemy nodes attacks. Similarly, HIS can also identify the antigen and exclude it efficiently.

HIS is an ideal protection of the human body which dates from millions of years. Modern medical research has disclosed HIS principles. We took inspiration from common features mentioned above to demonstrate that HIS mechanism can be introduced in 6lo IDS. This is in order to build an immunization model and solve 6lo IDS security problems.

7. CONCLUSION

This paper tried to study the impact of the proposed 6lo in the development of smart cities, in the context of the Internet of Things. It focused on the pillar of security, it had presented the problems and needs of security according to different applications used in smart cities projects. It analyzed two important lines of defense that must be used to secure 6lo networks, it discussed the incompatibility of existing solutions and it proposed some measures and some guidelines for good security protocols compatible with networks 6lo.

We hope that our research results have a positive impact on future standards of 6lo networks.

8. REFERENCES

[1] K. Su, J. Li, and H. Fu, “Smart city and the applications,” in *2011 International Conference on Electronics, Communications and Control (ICECC)*, 2011, pp. 1028–1031.

[2] N. Kushalnagar, G. Montenegro, D. E. Culler, and J. W. Hui, “Transmission of IPv6 Packets over IEEE 802.15.4 Networks.” [Online]. Available: http://tools.ietf.org/html/rfc4944.

[3] C. P. P. Schumacher, N. Kushalnagar, and G. Montenegro, “IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals.” [Online]. Available: https://tools.ietf.org/html/rfc4919.

[4] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[5] G. J. Pottie, “Wireless sensor networks,” in *Information Theory Workshop, 1998*, 1998, pp. 139–140.

[6] D. Kyriazis, T. Varvarigou, A. Rossi, D. White, and J. Cooper, “Sustainable smart city IoT applications: Heat and electricity management amp; Eco-conscious cruise control for public transportation,” in *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013 IEEE 14th International Symposium and Workshops on a*, 2013, pp. 1–5.

[7] J. A. Gutierrez, M. Naeve, E. Callaway, M. Bourgeois, V. Mitter, and B. Heile, “IEEE 802.15.4: a developing standard for low-power low-cost wireless personal area networks,” *IEEE Netw.*, vol. 15, no. 5, pp. 12–19, Sep. 2001.

[8] T. Narten, S. Thomson, and T. Jinmei, “IPv6 Stateless Address Autoconfiguration.” [Online]. Available: http://tools.ietf.org/html/rfc4862.

[9] T. Narten, W. A. Simpson, E. Nordmark, and H. Soliman, “Neighbor Discovery for IP version 6 (IPv6).” [Online]. Available: https://tools.ietf.org/html/rfc4861.

[10] S. Chakrabarti, Z. Shelby, and E. Nordmark, “Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs).” [Online]. Available: http://tools.ietf.org/html/rfc6775.