

# False Clouds for Internet of Things and Methods of Protection

Ruslan Kirichek\*, Vyacheslav Kulik\*, Andrey Koucheryavy\*

\*Department of Telecommunication Networks and Data Transmission, St.Petersburg State University of Telecommunication, Russia

[kirichek@sut.ru](mailto:kirichek@sut.ru), [vaklicr@gmail.com](mailto:vaklicr@gmail.com), [akouch@mail.ru](mailto:akouch@mail.ru)

**Abstract**— This paper describes the results of a full-scale experiment, in which the data from a Thing of Internet is redirected to a false cloud. This paper also suggests methods of protection which can prevent this type of an attack and secure the connection between a Thing of Internet and Public communication network - Cloud service.

**Keywords**— Cloud, Internet of Things, Thing of Internet, protection, traffic

## I. INTRODUCTION

Internet of Things is a key trend in telecommunications, the discussion of which has recently been paid attention to. Thereby, there are new threats to the network security of the Internet of Things, such as attacks on the power systems, replications of the network nodes, interceptions of the data from an Internet device, substitutions of the device and cracking services which process and store data [2-5]. Classical approaches of identifying these problems are not always suitable due to the fact that the Internet of things uses a vast amount of 25 proprietary protocols.

The concept of the Internet of Things involves the use of cloud services for storing and processing data [7,8]. Meanwhile, the cloud service can be either the link between an Internet device and a person or the final element in the collection of the data from sensors [10]. Distortion, destruction or blockage of the transmitted information can occur in case of external interference of the third parties during any step of a data transfer. This type of attack is called a "man in the middle." However, the simplest type of an attack, which can be implemented at the access level, is sending an alternative cloud service, which is named False Cloud in the paper, the data from a Thing of Internet.

## II. REDIRECTING DATA FROM THE THING OF INTERNET TO FALSE CLOUD

To gain access to the confidential data coming from the typical Thing of Internet to a remote cloud services, it is possible to use a method of cloning a package containing the confidential information, and sending it to the duplicating cloud service (false clouds). The cloud service in this paper refers to a set of software and hardware (servers) which are connected to the Internet and carry out the data processing and the storage. In its simplified version, the cloud service can be

represented by the Web and Data Base-server, which is one of the key components of the model network of the Internet of Things.

We conducted a full-scale experiment on a model network of the Internet of Things Laboratory SPbSUT to test the feasibility of this attack and to develop methods of protecting [1].

The necessary access to the communication channel or the equipment at the access level, which is responsible for transporting the data from the Thing of Internet to the cloud server, was conducted to implement interception and sending confidential data to a false server.

Currently, WiFi technology is the most popular one among the wireless networks and is used to connect the Thing of Internet to such applications as "smart home", "smart city", "smart chair" etc. [9]. Sending data to a cloud service requires a Thing of Internet to have a connection to an access point which has connected with a public communication network [6]. Intercepting and forwarding data can be implemented in close proximity to the communication channel "Thing of Internet - access point." During the full-scale experiment, a single-board computer (Intel Edison), which had a software allowing to capture network traffic being transferred to a legal cloud service, has been configured to perform the scenario. Filtering data packets was performed by IP-address and the Port of destination. Packets, which had the address of the legal cloud service as their IP-address, were duplicated and forwarded to an alternative (false) cloud server, deployed in the Laboratory of the Internet of Things, by substituting the IP-address in a duplicate "on the fly".

## III. ARCHITECTURE TEST BENCH ON THE BASIS OF THE MOBILE NETWORK FOR IOT

The following configuration of the test bench had been developed for the realization of the duplicating hardware part of the data system (Figure 1):

- the typical Thing of Internet has been developed on the basis of the popular radio module ESP8266 with a microcontroller, a temperature sensor DS1620 and two batteries AA (Figure 2). This module has been configured to transmit the parameters of air temperature to the cloud service through the public communication network;

- as the access point was used WiFi-router Zyxel Keenetic 4G;
- as a cloud service for the Internet of Things was used the service Go + University Solution [11];
- as a device of interception (sniffing) of traffic, cloning and redirection of network traffic was used the single-board computer Intel Edison connected LTE-modem ZTE MF831, which could transmit data to the public communication network;
- on the false cloud server was running tcpdump utility to capture traffic coming to a dedicated port 10001 (for applications sniffing).

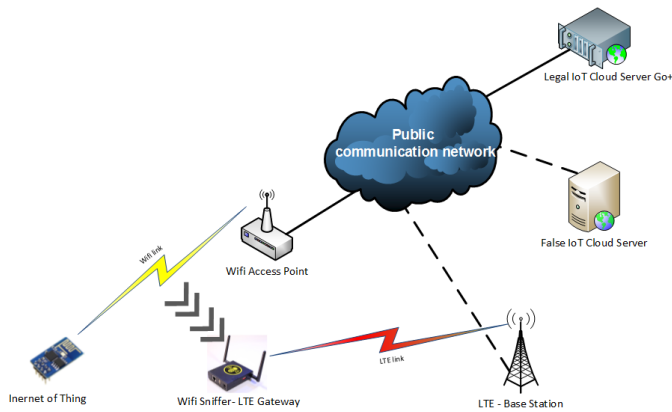


Figure 1. Structure of the test bench

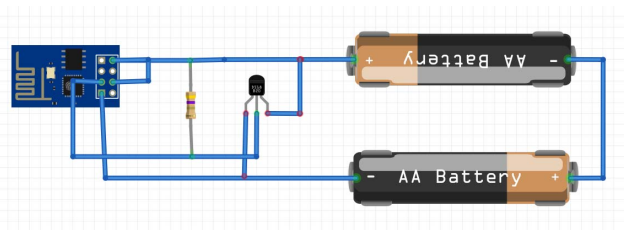


Figure 2. Circuit schematic of a typical Thing of Internet

To implement the program part of the duplication process of the data the software was developed that runs on a virtual machine Java - «openjdk7» with the support of programming language «Java», library analysis and traffic generation «JnetPcap». The software was run on the single-board computer Intel Edison, which is powered by a 12V battery.

#### IV. THE WORKING ALGORITHM OF TESTING BENCH

The operation algorithm of testing bench for the duplication of the data of the Things of Internet consists of a sequence of steps below:

Step 1. On the device WiFi sniffer - LTE gateway is running the script, with the aim to obtain an access to a WiFi router. An access control is obtaining through data-packet interception of wireless link "Thing of Internet - Access point" and receiving the key WPA2 at WiFi network by a brute-force attack based on distributed computing;

Step 2. An application, that has functions of capturing, analyzing, filtering and duplication of the traffic coming from

the Thing of Internet and further redirection of the data to the public communication network on a false cloud server via LTE-modem was run on the device WiFi sniffer-LTE gateway:

- the application gained access to the communication channel (the key WPA2), to intercept traffic from the Thing of Internet and to perform further analysis of packages for their belonging to the compound;
- after determining the format of data-packets coming from the Thing of Internet, the application complied with the temporary buffer array of captured packets in memory to speed up the substitution values of IP-address and Port of destination of the legal cloud service on the IP-address of the false cloud server and port 10001;
- further on, the application send duplicated the data-packets to public communication network for false cloud server via LTE-modem.

The process of capturing the data-packets and its substitution was carried out with a delay related to the computing capacity of the processor and RAM single-board computer.

Step 3. After the data-packets were received to a port 10001 of false cloud server, the packets have been captured and recorded on the ROM for the further analysis and visualization.

#### V. THE DESCRIPTION OF THE APPLICATION RUNNING PROCESS ON THE DEVICE WIFI SNIFFER - LTE GATEWAY

The software part, launched on the device, fulfilled the analysis of the header of each captured data-packet. After detection in the Destination address field (network layer) and Destination port field (transport layer) of the corresponding address and port of the legal cloud service or IP-address of the Thing of Internet in the Source address field, the program copied the contents of the data-packet in memory and started the subsequent replacement of the fields Address and Destination port on the IP-address and port of the false cloud server. Further on, the application accomplished sending of the data- package to the public communication network.

If the IP-address of the legal cloud server was unknown, it analyzes the structure of the traffic on the Thing of Internet. The Thing of Internet traffic key characteristics can significantly vary, depending on the type of device (sensor, actuator, combined device, etc.) or their purpose.

In the experiment, we used the Things of Internet type of sensor node, that sends the temperature data each 30 seconds, using the application layer protocol - MQTT without any encryption algorithms. At the network layer was used the IPv4 protocol. TCP was used protocol as the transport layer (for MQTT). It was assumed, that the IP-address of the legal cloud server is unknown.

To detect the data from the Thing of Internet and send them to a false cloud server, first of all, the IP-address of the legal cloud service should be determined. For this purpose it is necessary to analyse the behavior of traffic from the Thing of Internet and to get parameters of the main characteristics. MQTT protocol has a standardized format for the message exchange between the Thing of Internet and MQTT-broker

(Figure 3). The first criterion for filtration of the network traffic MQTT protocol is happened to be a detection of 4 outgoing the data-packets series from the Thing of Internet, namely:

- the data-packet that signals the start of transmission the data (transport protocol TCP);
- the data-packet with data from the Thing of Internet (transport protocol TCP. Application layer protocol MQTT);
- the data-packet that signals the end of the data transmission (transport protocol TCP);
- the data-packet that confirms the receipt of data MQTT-broker (transport protocol TCP. Protocol application layer MQTT).

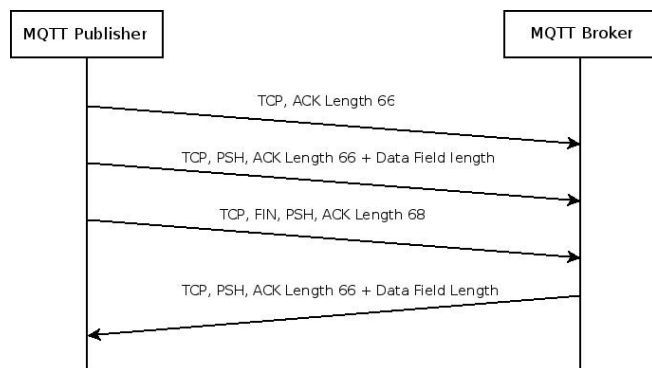


**Figure 3.** The exchange of messages between Thing of Internet and broker MQTT

To filter packets on this criterion was carried out the comparison of the Source address field in the packet coming from the Thing of Internet and Destination address field in the packets sent from the server.

This criterion is acceptable, on condition that the package is received from the server not further than through 7 packages after a package from the Things of Internet and at their coincidence comparison of the data fields was carried out. If the data fields were identical, the counter which at achievement of a certain value wrote down the IP address of the recipient server, the IP address of the Internet of a thing and port of the recipient in the RAM for the further use at duplication of the packages switched on. This criterion for the traffic analysis is acceptable under condition of using network layer protocols IPv4, IPv6, transport layer protocols UDP, TCP and application layer protocol MQTT.

Also, as a criterion for filtering, the Things of Internet traffic carried out the analysis of all the captured data-packets in terms of their similarity on the basis of the indirect characteristics. For this purpose an array of structures was used containing the Source IP-address, source port, Destination IP-address, the expected data type (symbols or number), the size of the data field of the package (with a small probability of deviation, depending on the type of the intercepted data), an array of 3 or more numbers, storing the time of arrival of last 3 or more packages of this type and count the number of captured packets. Such structure describes the number of the received data-packets that are

similar to each other. In case, if more than 3 data-packets had similar destination addresses and ports, data type, size of data fields and the time difference between two consecutive packets would be approximately equal to the difference of the other two consecutive packets in RAM the value of Destination address, Source address and Destination port for further use at duplication of packages registered. This criterion is expedient to use for the analysis of a traffic the Things of Internet on condition of use items subject to network layer protocols IPv4, IPv6, and transport layer protocols UDP, TCP, but the study of the structure of information exchange can take considerable time.

After determining the IP-address of the destination server (legal cloud service), IP-address of Thing of Internet and Destination port, each packet which is suitable for these criteria, is duplicated and stored in the RAM. Then there is a replacement of server IP-address and destination port in the server address duplication and port 10001.

## VI. TRAFFIC PROTECTING METHODS FOR THING OF INTERNET

Two methods of data protection are proposed to protect the data that is sent from the Things of Internet to a public communication network and for a duplication to a false cloud server.

### 1) The protection method based on the use of hybrid encryption algorithms:

These algorithms (e.g., RSA-512 and AES-128) require a relatively large computational capabilities from the Thing of Internet and are not suitable for low-power device, carried out on a microcontrollers, with 8 or 16-bit CPU (e.g., AVR or ARM), as well as devices with a small memory capacity. An example of such algorithm (Figure 4) consists of the following sequence of steps:

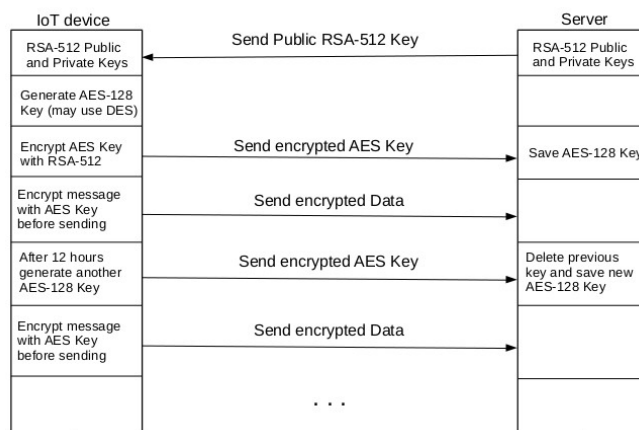


**Figure 4.** Hybrid encryption algorithm for Thing of Internet

Step 1. Generating a public and a private keys on a server for the organization of an asymmetric encryption (e.g., RSA-512);

Step 2. Generating a public and a private keys for the microcontroller and recording it to a Thing of Internet memory;

Step 3. The public keys are exchanged between the server and the Thing of Internet;

Step 4. Thing of Internet with a set of random characters generates a key for symmetric encryption (e.g., DES);

Step 5. The generated symmetric encryption key is encrypted with the public key and is sent to the server;

Step 6. Decoding its run on the server and a symmetric key is recorded to the ROM by using the private key;

Step 7. All subsequent data, which is sent from Thing of Internet, is encrypted using the symmetric key available on the Thing of Internet and on the server;

Step 8. Steps 4-7 must be repeated over a preset time depending on the complexity of deciphering the symmetric key brute force (bruteforce).

## 2) Protection method based on the unique patterns creation for the Thing of Internet network traffic:

The method involves making random changes in the structure of the information exchange between the Thing of Internet and the cloud server, as well as the use of multiple ports on the server to create an atypical traffic for the Thing of Internet.

This method is suitable for the majority of Things of Internet, including the low-power 8-bit microcontrollers. This method involves the following steps:

Step 1. Hashing all data stored in the data field of all the packets sent to the Thing of Internet (e.g., using the algorithm MD5);

Step 2. Adding random delay before the next data sending cycle (time differentiability) from the Thing of Internet;

Step 3: Use server-side multiple IP-addresses to receive data, which will enable Thing of Internet randomly record different values in the destination address;

Step 4. Using “port knocking” method before each data transmission. Portknocking method is accessing the certain ports to unlock the port access on which, eventually, data is transferred (Figure 5). In this case, it is proposed before each data transfer (or a certain period of time) to change data ports using this method. For this purpose the Thing of Internet pre-sends a request for a data transfer. The server sends back a list of hashed ports for transmission, and then the unit makes alternating requests to each port and sends data on a selected port;

Step 5. Creating a false data stream.

The proposed method can significantly increase the complexity for the interception from Thing of Internet traffic, which keeps confidential information.

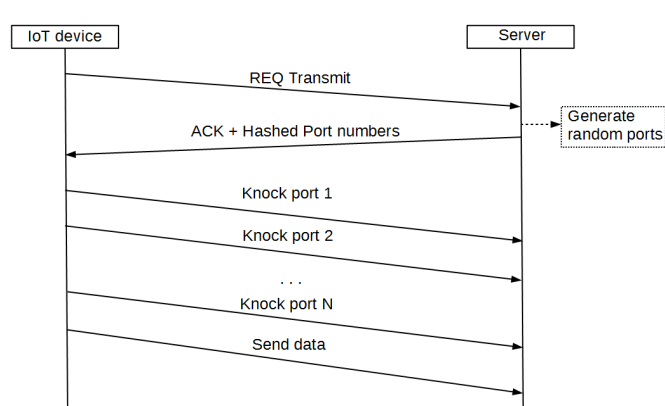


Figure 5. The structure of the information exchange for port knocking method

## VII. CONCLUSIONS

The paper describes a new type of vulnerability of the Things of Internet - interception and sending the data to a false cloud. Protective actions are proposed. The most effective one is the method of creating the unique patterns for Thing of Internet network traffic, suitable for microcontroller based on low-power Things of Internet, and for more powerful Things of Internet based on microprocessors.

## REFERENCES

- [1] Kirichek R., Koucheryavy A. Internet of Things Laboratory Test Bed // International Conference on Wireless Communication, Networking and Application. WCNA 2014. — LNEE – Vol. 348. — Heidelberg: Springer, 2016.
- [2] A.Koucheryavy. State of Art and Research Challenges for USN Traffic Flow Models. ICACT'2014, Proceedings, 16-19 February, Phoenix Park, Korea
- [3] A.Koucheryavy, I.Bogdanov, A.Paramonov. The mobile Sensor Network Life-Time under Different Spurious Flows Intrusion. LNCS, Springer. 13 th NEW2AN, LNCS 8121, 28-30, August, 2013.
- [4] T.Bhattasali, R.Chaki. A Survey of Recent Intrusion Detection Systems in Wireless Sensor Networks. Advanced in Network Security and Applications. Conference Proceedings of Fourth International Conference on Network security and Applications (CNSA 2011), Chennai, India, July 15-17, 2011.
- [5] T.Bhattasali, R.Chaki, S.Sanyal. Sleep Deprivation Attack Detection in Wireless Sensor Networks. International Journal of Computer Applications, v.40, №15, February 2012.
- [6] A.Koucheryavy, Yim Chu-Hwan, L.Gilchenok., S.Moiseev. Overlay IPOP-network for Russia PSTN. The 2nd International Conference on Advanced Communication Technology. ICACT-2000. Proceedings, Muju Resort, Korea. February 16-18, 2000.
- [7] A.Iera, C.Floerkemeier, J.Mitsugi, G.Morabito. The Internet of Things. IEEE Wireless Communications. December 2010, v.17, №6
- [8] J.Gubbi, R.Buyya, S.Marusic, M. Palaniswami. Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. Elsevier, Future Generation Computer Systems, 29, 2013.
- [9] J.Stankovich. A Vision of a Smart City in the Future. Smart Cities, v.1, issue 10, October, 2013.
- [10] A.Botta, W.de Donato, V.Persico, A.Pescape. On the Integration of Cloud Computing and Internet of Things. International conference on Future Internet of Things and Cloud. Proceedings, 27-29 August 2014, Barcelona, Spain.
- [11] Go+ Cloud Based IoT Platform//United University Solution: [www.goplusplatform.com](http://www.goplusplatform.com).



**Dr. Ruslan Kirichek** working in St.Petersburg University of Telecommunication as Associate Professor Department of Communications Networks. He was born in 1982 in Tartu (Estonia). He graduated Military-Space Academy A.F. Mozhaiskogo and St.Petersburg University of Telecommunication in 2004 and 2007 respectively. R.Kirichek received Ph.D from St.Petersburg University of Telecommunication in 2012. Since 2004 he worked at IT-department of the Air Force as a senior engineer. Since 2008 worked as a senior researcher at the Federal State Unitary Enterprise "Center-Inform". Supervised research testing communication networks in terms of destructive influences. Since 2012 worked as the Head of the Internet of Things Laboratory at St.Petersburg University of Telecommunication.



Viacheslav Kulik working in St.Petersburg University of Telecommunication as Engineer of Department of Communications Networks. He was born in 1994 in Stavropol (Russia). He graduated St.Petersburg University of Telecommunication in 2015 as bachelor of Software Engineering. Now he studying in St.Petersburg University of Telecommunication as master student. Since 2015 he worked as a engineer of the Internet of Things Laboratory.



Dr. Sc. Andrey Koucheryavy was born in Leningrad 02.02.1952. After graduated from Leningrad University of Telecommunication in 1974 he going to Telecommunication Research Institute named LONIIS, where A.Koucheryavy working up to October 2003 (from 1986 up to 2003 as the First Deputy Director). He became the Ph.D. and Dr.Sc. in 1982 and 1994 respectively. A.Koucheryavy is the St. Petersburg State University of Telecommunication (SUT) professor from 1998. He is Chaired professor of the department "Telecommunication Networks and Data Transmission" from 2011. He is honorary member of A.S.Popov's society. Prof. A.Koucheryavy was the vice-chairman Study Group 11 ITU-T (Study periods 2005-2008, 2009-2012). His scientific areas of interest are the network planning, teletraffic theory, IoT and its enablers.