УДК 004.42

Ł. Filipek, student (Lublin Catholic University, Poland),
P. P. Urbanovich, prof. (BSTU, Minsk, Belarus)

INTERNET OF THINGS: CONCEPTS, RISKS, SECURITY

Internet of Things (IoT) is a concept of a connected network of things or objects. In the context of the IoT, the thing is the object of the physical world (physical thing) or the world of information (virtual thing), which can be identified and integrated in communication networks. This integration is implemented by means of communication devices. The integration of the thing and the communication device defines IoT [1].

The main goal of IoT is to create an intelligent environment by using a set of intelligent devices. They are supported not only by sensors or electronic identifiers enabling monitoring and ongoing assessment of the state of the environment, but they can also be based on a number of other information such as the location of the given object, weather forecast, information on the current traffic volume or any social or private business information. Thanks to this, the IoT creates the possibility of partial integration between the physical world and the computer system, offering an increase in the level of performance, security and comfort. Thanks to this, the IoT creates the possibility of partial integration between the physical world and the computer system, offering an increase in the level of performance, security and comfort. The amount of data provided by IoT devices as well as their scope and specification can be any depending on the requirements.

A characteristic feature of IoT are resource constraints. They mainly result from the fact that security functions such as cryptographic mechanisms cannot use too much computing resources of the device, its memory and, as a consequence, energy. Most of IoT devices are built-in and small devices. They have various resource limits - they don't have long battery backup; they don't have a lot of memory and they don't have a lot of computing power. Therefore, in addition to conventional cryptography in IoT, there is a need to use light cryptography. There are many ways to thwart cryptography if security features are not properly implemented. Access control systems in IoT must be able to dynamically revoke credentials and cross-verify with neighboring nodes [2, 3].

The challenge for IoT technology is to ensure an appropriate level of security. According to a Cisco report, the number of devices connected to the Internet will increase to 28.5 billion in 2022, compared with 18 billion in 2017. IoT devices are to contribute to such a large increase in the number of devices connected to the Internet. According to research conducted

by Hewlett-Packard on the commercialization of the Internet of Things, 80% of tested devices violate the privacy of personal data such as name, surname, home address or credit card credentials. 80% of them did not require passwords of adequate complexity or length. In addition, 70% of devices did not encrypt communications and 60% of them had user interface vulnerabilities. That is why IoT devices often become the first line of attack. Due to numerous vulnerabilities, they become the weakest point of the network. In turn, the security of the entire network is equal to the security level of its weakest element [4].

Due to the listed some conceptual features of the IoT, this environment is the object of not only well-known and other types of attacks. Here it is impossible not to take into account the law aspects of the problem [5].

A *botnet* is a collection of computers or any IoT devices controlled by malware. Network devices are infected by malicious software that is spread via computer networks. After infecting machines, they can be controlled remotely without the knowledge of their owners and can be used to attack any target. Any unsecured device with Internet access can be used by an intruder to create a botnet. Due to the increasing commercialization of the IoT, it is becoming the main target of cybercriminals. According to a Nokia report in 2018, 78% of infections in telecommunications networks are associated with IoT botnets, and IoT bots account for 16% of devices [6].

One of the most powerful identified IoT botnet is Mirai Botnet. It could perform *DDoS* attacks with a strength of 1.2 Tb / s using hundreds of thousands of end devices such as IP cameras, home routers, DVR players. The malware was infected after logging in to devices using a default or popular set of usernames and passwords. These attacks in October 2016 resulted in unavailability of websites such as GitHub, Twitter, Reddit, Netflix, Airbnb and many others. The Mirai Botnet code has been published so that more Mirai modifications such as IZ1H9, Ex0, Ares, LZRD and Miori are still appearing, which take into account newly created vulnerabilities.

In case of the IoT the communication between devices is held mainly with wireless media. Attacks based on a routing disorder allow eavesdropping on transmissions, modifying information, destroying messages, and strengthening DDoS attacks.

Wormhole is a specialized *Man-in-the-Middle attack* in which the attacker connects two remote regions of the network with a private low-latency link.

IoT connects stationary objects and those that often change their surroundings. The connection itself is also heterogeneous - it can be wired or wireless, depending on the geographical location. One or more malicious

nodes may be used in this attack. Malicious nodes have the task of creating the tunnel between sender and recipient with fewer hops than a regular route. The attacker node intercepts packets from one point and then tunnels to the next, which further distributes them. This type of attack combined with other attacks can become a serious security breach. This tunnel is also difficult to detect, especially when it is systematically turned on and off.

This attack is very popular on Ad-Hoc networks. With many network routing protocols in Ad-Hoc networks, the wormhole would prevent the algorithms from finding routes longer than one or two hops. A wormhole attack also effectively disrupts location-based wireless systems (see fig. 1).

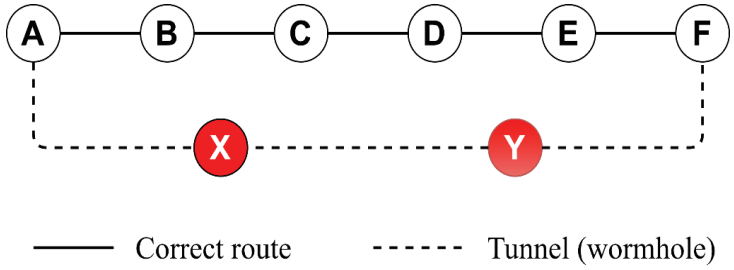

Fig. 1 – Wormhole attack on the example of communication of source node *A* with destination node *F*

In a S*elective-Forwarding Attack*, an infected node can freely filter messages by selectively forwarding or destroying them. A selective forwarding attack can also be used to perform DoS attacks by selectively forwarding packets to the victim node. One of the solutions to protect against this type of attacks is to create separate paths between the source and destination nodes.

Sinkhole attack. Sensors left unattended in the network for a long time are particularly vulnerable to sinkhole attacks. An infected node receives network traffic from all surrounding nodes by announcing erroneous routing information. The received data is modified or more often, mainly not transferred. The task of the infected node is to participate in as many routes as possible. So, unlike a blackhole attack, the node does not wait for communication intermediation in accordance with current routing tables, but wants to force communication with the largest number of neighboring nodes. Atak ten jest wykorzystywany w sieciach Ad-hoc opartych na protokołach AODV (Ad hoc On-Demand Distance Vector Routing), DSR (Dynamic Source Routing).

Initially, the attacking node observes the source node sequence number. It then maximizes the sequence number and creates the requested RREQ (Request Route) broadcast and adds a fake entry to its cache that says the source node is in the next hop from itself. The routing request is

emitted to subsequent nodes, which add successive hops to the table until they reach their destination. Figure 2 for the readability of the record does not take into account the broadcast nature of the RREQ package.

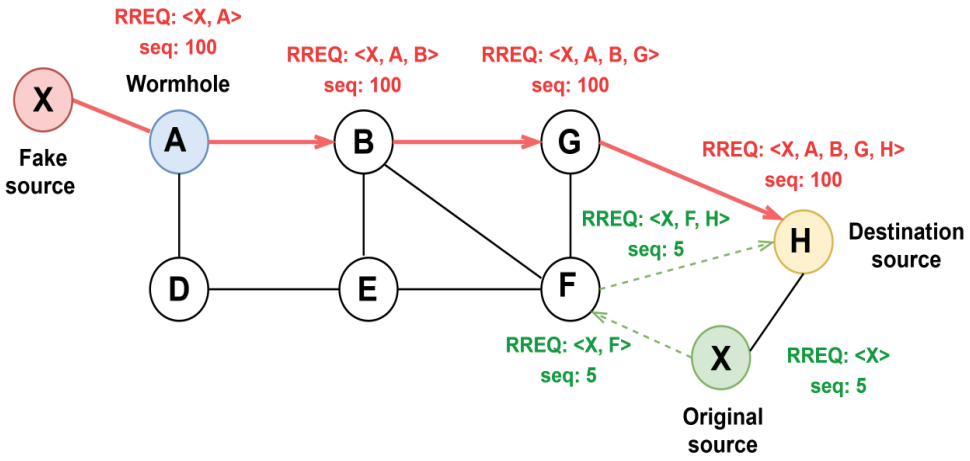

Fig. 2 – Creating and emission of a fake RREQ

Then unicast RREP (Route Reply) packets are sent back to the destination node with the least hop counts. A request with a higher sequence number than the previous route means that the neighboring nodes treat the given new route as the most recent one and add it to their route tables.

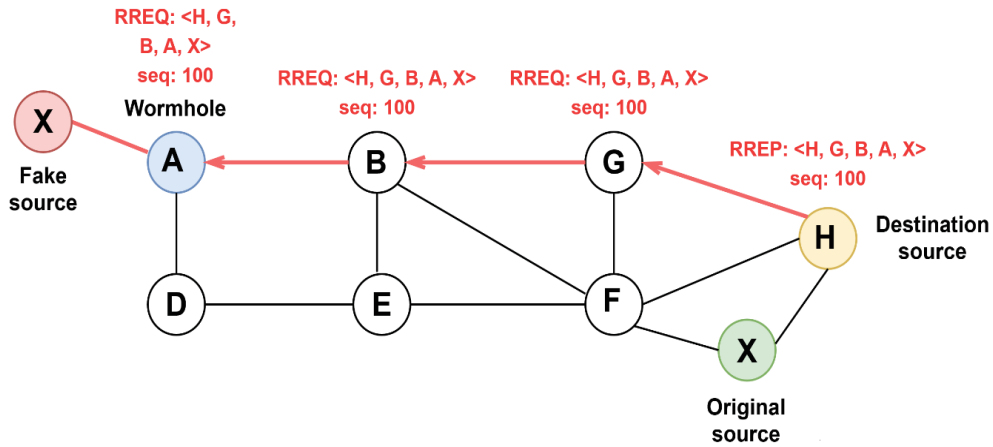

Fig. 3 – Emission of false RREP

It is clear that the types of attacks that we briefly analyzed in the Internet of things environment do not exhaust the full list. There are other security risks to the systems considered [7, 8].

The IoT environment requires secure communication with and between billions of devices. Without ensuring an adequate level of security, the IoT instead of a network of interconnected devices can become a network of interconnected threats. By using a significant scale of these devices in network traffic, their increasing role in communication and an upward trend in the market, these devices without providing an adequate level of

protection will become the first line of attacks in the space of computer networks. Due to limited devices resources, the correct integration of all security functions is extremely important in the context of the IoT security.

REFERENCIES

1. Overview of the Internet of things. International Telecommunication Union. – [Electronic resource]: https://www.itu.int/rec/T-REC-Y.2060-201206-I.

2. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации : учеб.-метод. пособие для студ. – Минск: БГТУ, 2016. – 220 с.

3. Ochrona informacji w sieciach komputerowych / pod red. prof. P. Urbanowicza. – Lublin: KUL, 2004. – 150 s.

4. Cisco Visual Networking Index: Forecast and Trends, 2017–2022, Cisco. – [Electronic resource]: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html.

5. Paweł Urbanowicz, Marek Smarzewski. Bezpieczeństwo w cyberprzestrzeni a prawo karne/ Księga pomiątkowa ku czci Księdza Profesora Andrzeja Szostka MIC. – Lublin: Wydawnictwo KUL, 2016. – S. 489-496.

6. Nokia Threat Intelligence Report 2019, Nokia. – [Electronic resource]: https://pages.nokia.com/T003B6-Threat-Intelligence-Report-2019.html.

7. O. El Mouaatamid, M. Lahmer, M. Belkasmi. Internet of Things Security: Layered classification of attacks and possible Countermeasures/ Electronic Journal of Information Technology, 2016, no. 9.

8. Урбанович, П. П. Защита информации: конспект-лекция, ч.1 = Information Protection, Part 1: INTRODUCTION TO THE SUBJECT AREA / П. П. Урбанович. – Минск: БГТУ, 2019. – 52 с. – [Electronic resource]: https://elib.belstu.by/handle/123456789/29335.

УДК 003.26+004.57

К.А. Ахраменок, маг.;
Н.А. Жиляк, доц., канд. техн. наук
(БГТУ, г. Минск)

ПОСТРОЕНИЕ СКОРИНГОВОЙ МОДЕЛИ С ИСПОЛЬЗОВАНИЕМ ЛОГИСТИЧЕСКОЙ РЕГРЕССИИ

Скоринг (от англ. Scoring — подсчет очков в игре) — это модель классификации клиентской базы на различные группы, если неизвестна характеристика, которая разделяет эти группы, но известны другие факторы, связанные с интересующей нас характеристикой [1].

Логистическая регрессия — статистическая модель для по-