Düzce University Journal of Science & Technology

Research Article

Network Forensics of RPL-Based Attacks

Gökçe KARACAYILMAZ [a], Serkan GÖNEN [b], Harun ARTUNER [a], Ercan Nurcan YILMAZ [c,*], Hasan Hüseyin SAYAN [c], Erhan SİNDİREN [c]

[a] *Forensic Sciences, Hacettepe University, Ankara, TURKEY*
[b] *Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul, TURKEY*
[c] *Institute of Natural and Applied Sciences, Gazi University, Ankara, TURKEY*
* *Corresponding author's e-mail address: enyilmaz@gazi.edu.tr*
DOI : 10.29130/dubited.788006

ABSTRACT

IoT devices, which are increasing in highly manner day by day, are now in everywhere in our life. WSNs are used together with IoT devices to monitor real environments. In this study, attacks against WSNs were carried out. The attack chosen for this study is a flood attack. In addition, solution suggestions for this attack are presented. In this context, firstly reference and attack packages have been collected, and then the collected packages have been compared with the reference packages and forensic investigations have been carried out. The result of the evaluation has shown the importance continuous monitoring on 24/7 basis and detecting abnormal behaviors in IoT traffic with forensics analysis for preventing attacks.

Keywords: *Wireless Sensor Networks, Flood Attack, Network Forensics, Continuous Monitoring*

RPL Tabanlı Atakların Ağ Adli Bilişimi

ÖZET

Her geçen gün hızla artan IoT cihazları artık hayatımızın her yerindedir. WSN'ler (Kablosuz sensor ağları), gerçek ortamları izlemek için IoT cihazlarıyla birlikte kullanılır. Bu çalışmada WSN'lere yönelik saldırılar gerçekleştirilmiştir. Bu çalışma için seçilen saldırı sel saldırısıdır. Ayrıca sonuçta bu saldırıya yönelik çözüm önerileri sunulmuştur. Bu kapsamda önce referans ve saldırı paketleri toplanmış, ardından toplanan paketler referans paketlerle karşılaştırılarak adli incelemeler yapılmıştır. Değerlendirme sonucu, saldırıları önlemek için 7/24 bazında sürekli izleme ve ağ adli bilişim analizi ile IoT trafiğindeki anormal davranışları tespit etmenin önemini göstermiştir.

Anahtar Kelimeler: *Kablosuz Algılayıcı Ağlar, Sel Saldırısı, Ağ Adli Bilişimi, Sürekli İzleme*

Received: 30/08/2020, Revised: 21/10/2020, Accepted: 21/10/2020

I. INTRODUCTION

Smart environments are increasingly used in buildings, military, health, ecological, industrial and transportation applications. These environments are based on smart devices that receive data from the real world, subsequently process and transmit this data to information processing centers, produce some knowledge-based services, and sometimes produce some action in the environment. The information used by smart environments is provided by Wireless Sensor Networks (WSNs), which are responsible for monitoring and recording physical or environmental conditions and transmitting the collected data to a central location via IoT devices [1].

According to a study by Cisco[2], the number of devices to be connected to the Internet under the Internet of Things is estimated to reach 50 billion in 2020. This new concept, which will connect billions of devices over the Internet, is called the Internet of Things (IoT). With the inclusion of devices on the Internet of Things networks, these devices will have to deal with security issues that the Internet is exposed to [3]. RPL is an IPv6 based routing protocol developed for Low Power and Lossy Networks (LLNs). In LLNs, features such as processing power, memory and energy consumption are restricted in both routers and interconnects. RPL routing protocol operates according to the Destination Oriented Acyclic Graphs or DODAGs principle. Difficulties arise in ensuring security due to the limited resources used in devices used in IoT networks and the mostly wireless communication. RPL protocol is a commonly used protocol in IoT devices [4, 5], so vulnerabilities of this protocol are one of the most devastating attack vectors of attackers.

In this study, IoT attacks has been carried out by exploiting the vulnerabilities of IoT devices. Subsequently, the network forensic packages of Flood Attack, which is one of the most important one on RPL-based attacks [6, 7, 8], has been analyzed by examining the effects of attacks on the system.
WSNs have emerged as an important application of the paradigm of Ad-Hoc Networks such as physical environment monitoring. These sensor networks have limitations in system resources such as battery power, communication range, and processing capacity. Low processing power and wireless connectivity make these networks vulnerable to various network attacks [9]. One of the best known attack is the hello flood attack [10]. In this attack an attacker fills the network traffic with hello requests and disrupt the WSN (wireless sensor network) security. Normally, flood is used to spread code updates and parameter changes in the network. It affects the operation of all nodes deployed in WSN. When flood occurs, each node typically publishes the flood packets once. However, flood costs can be significant because a node is required to transmit several unicast transmissions, rather than a single broadcast. Naive support for streaming via multiple unicast transmissions for flood code updates (a common process in WSN because they are not physically accessible) can be very costly [11]. Link-level DoS attacks can have a negative impact on the performance of the IoT network. Types of DoS attacks include packet flooding and scrambling, whose purpose is to disrupt the device's communication signal. This can greatly affect critical network parameters such as control pack overhead, power consumption, latency, and reliability [12]. In addition, IoT devices can be abused and turned into bots to carry out DoS attacks against selected targets. Chalubo and Mirai botnets are the latest examples of this type [13, 14].

The aim of the project is to implement network forensics, examine performance of the in depth under flood attack of WSN on various network parameters and find the possible security threats and countermeasures for this attack.

II. NETWORK FORENSICS FOR IOT TECHNOLOGIES

In this study, after carrying out cyber attacks on IoT technologies, forensic network analysis has been performed by examining the changes on the network continuously. Attacks and analysis have been carried out on the Cooja Simulator in Contiki Operating System.

A. CONTIKI OS

Contiki is an open source, which is Linux-based, operating system developed by Adam Dunkels in 2002 with the C programming language. Developed for internet of things (IoT) devices and wireless sensor networks (WSN) nodes with limited memory and low power [15].
Contiki makes it possible to develop applications that operate on low power microcontrollers and provide standardized wireless communication for various hardware platforms, while ensuring efficient use of the hardware. Contiki is used in many systems such as smart cities, smart electricity meters, industrial monitoring, site monitoring, alarm systems, smart home monitoring.

B. COOJA SIMULATOR

The Cooja simulator runs on the Contiki operating system. A wireless sensor network simulated using Cooja is shown in Figure-1. Developers can improve their own simulations using Cooja Simulator [16].

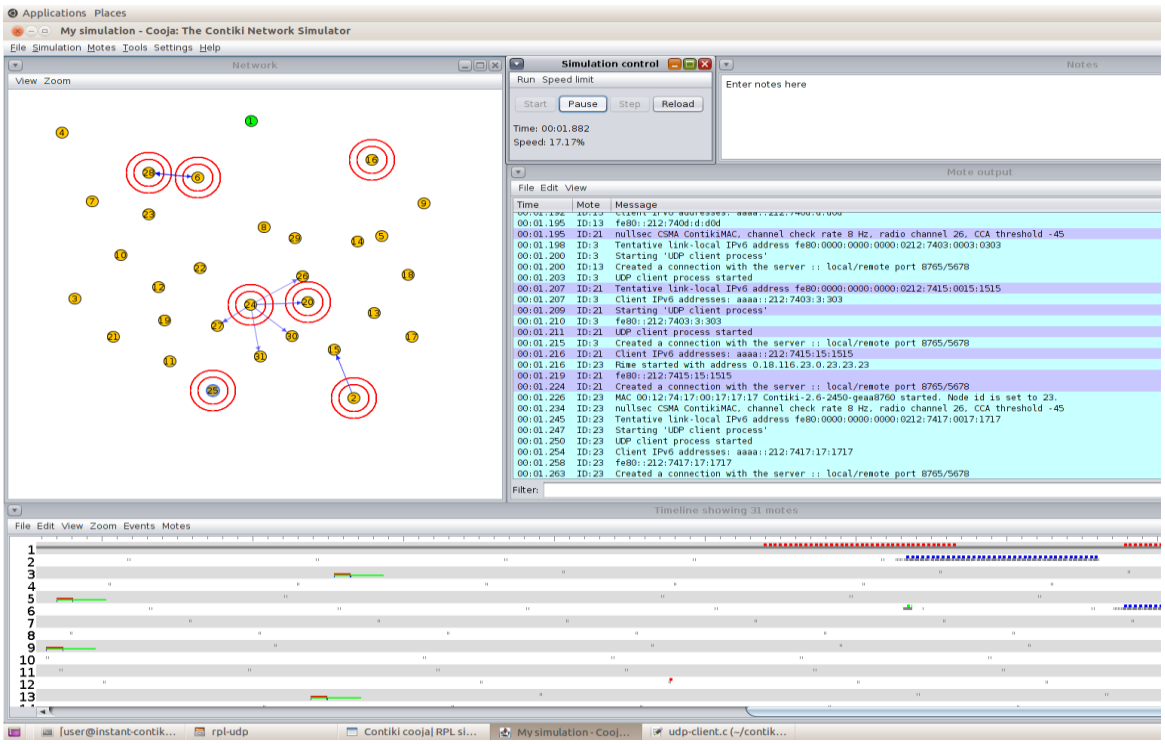


Figure 1. *Wireless Sensor Network*

Packet information and the node topology is depicted in the left window of Figure-1. Efforts are underway to connect small and large physical objects to the Internet using IPv6 protocols to create the Internet of Things (IoT). Routing Protocol (RPL) [17] for Low Power and Lossy Networks has recently been standardized as a routing protocol for IoT.

IoTs have many application areas including environmental monitoring, home automation and home security management, industrial automation, smart energy monitoring and management, item and shipping monitoring, surveillance and military, smart cities and health monitoring [18].

III. IOT ATTACK FRAMEWORK

In this section, Flood Attack, which is one of the important attacks on IoTs, has been carried out and its effect on the system has been discussed with forensic analysis. In section 4, the solutions to be taken has been indicated.

A. IOT ATTACK STEPS

The IoT Attack Framework has been carried out in the following stages. This framework is specially designed to network forensic analysis of RPL-based attacks.

- Simulating an Internet of Things (IoT) devices network traffic using Contiki OS,
- For simulating an IoT devices 25 motes have been used in the topology. (1) is a sink mote, (1) is an attacker mote and the other (23) is designed as standard mote.
- Carrying out RPL-based attacks on IoT devices,
- In this phase, RPL-based attacks including Flood Attack, DODAG Version Attack, Blackhole Attack and Rank Attack have been carried out on simulated IoT devices.
- Capturing network traffic using Test Anything Protocol (TAP) techniques,
- Network traffic of IoT attacks have been captured for further forensics analysis.
- Analyzing the network packets via Wireshark for gathering suspicious ones,
- In this study, captured packets of Flood Attack have been analyzed. However, captured packets of other IoT attacks (DODAG Version, Blackhole and Rank Attacks) will be handle in the further studies.
- Countermeasures to prevent these attacks,

Attack on IoT nodes, as seen in Figure 2 flow diagram, consists of information gathering, attack observation and attack detection phases. During the information gathering phase, it is aimed to identify the nodes on the network. At this stage, important information (brand, model, etc.) of the detected nodes has been determined and the protocol and communication times used by the nodes have been monitored. In the attack observation phase, a flood attack has been organized on target nodes based on the information obtained from the nodes and it has been observed whether the communication times of the nodes increased. In the attack detection phase, communication intervals, packet transmission and reception times, and changes in battery level have been detected by continuously monitoring the captured communication packets of the target nodes. At the end of these stages, a pattern related to the attack has created and it is aimed to detect as soon as possible in the case of a similar attack and to prevent and / or minimize the damage to critical systems.

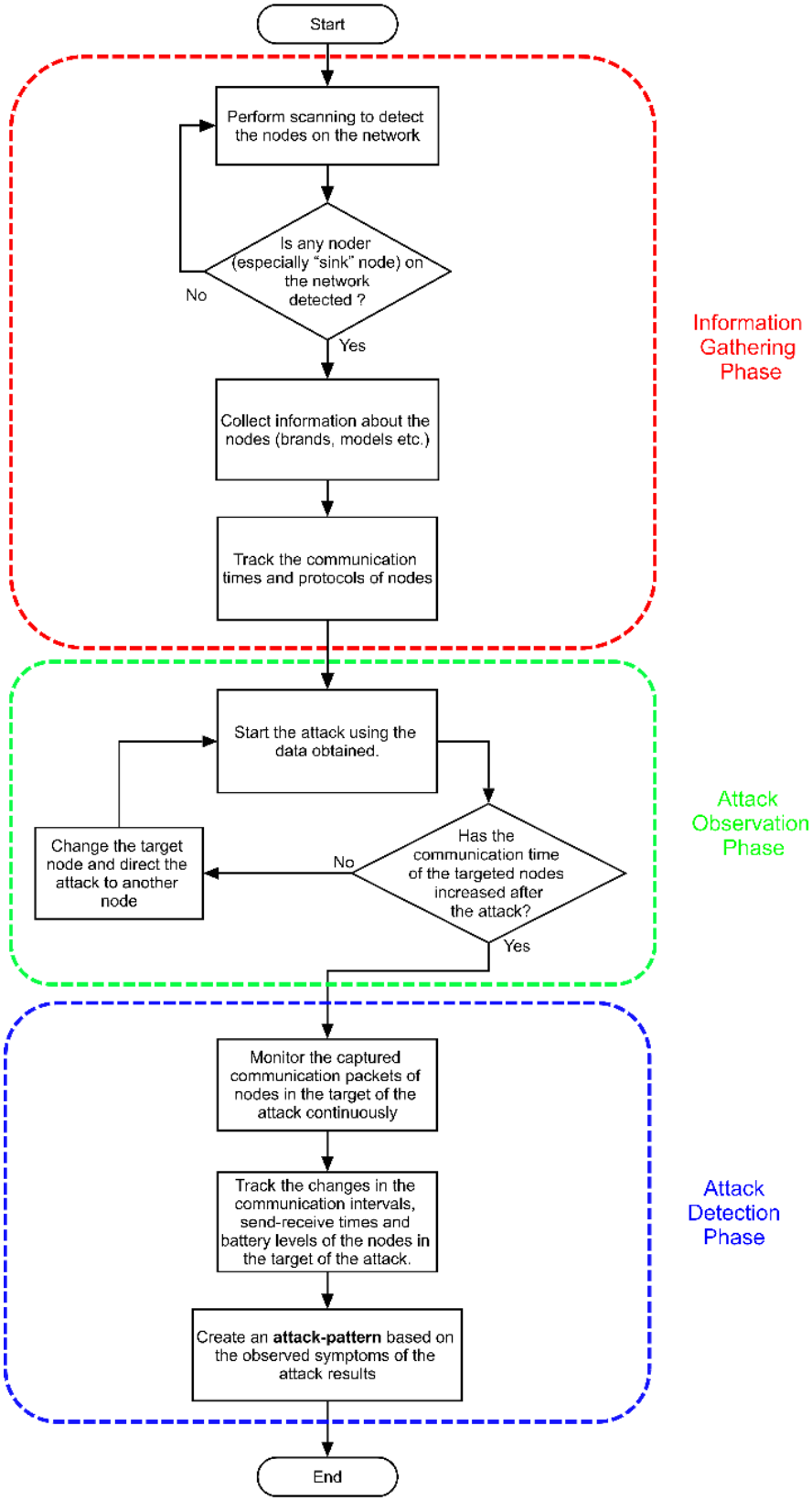


***Figure 2**. Steps of IOT flood attack*

This framework is specially designed to network forensic analysis of RPL-based attacks. This phase is explained in section 4 in details.

B. IOT ATTACK ANALYSIS

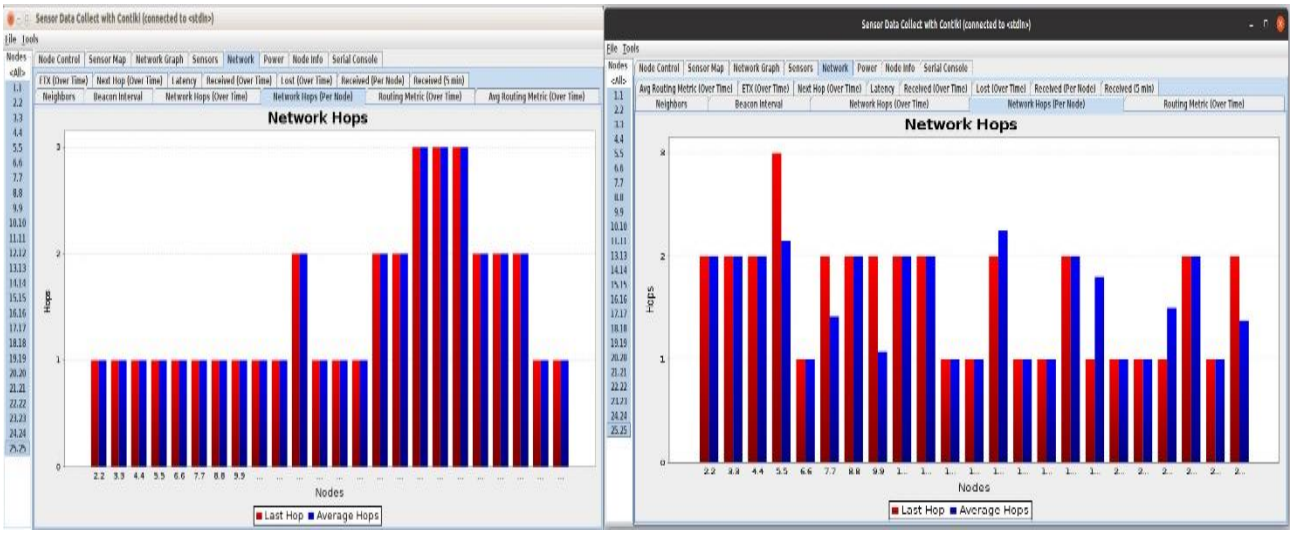
In this section, the effects of the attack on IoT devices are examined by comparing the reference values and the flood attack values as depicted in Figure 3.

***(a)** Reference Model* ***(b)** After Flood Attack*

***Figure 3.** Average Power Consumption Graph*

The sensor networks are completely dependent on battery power, so the main purpose of maximizing the life of the network is to conserve battery power or energy with some safety considerations. As can be seen in Figure 3, while the average energy consumption values required by the IoT sensor is 1.5mW before the attack, these values are increased up to 62mW during the Flood attack. In addition, before the attack, each device was listening (green area) and sending (yellow area) packets, but it stuck in the listening mode and could not send any packets during the attack. When working principles and requirements of IoT are evaluated, the importance of energy consumption for WSN can be understood. WSNs are a group of spatial distributed-self-operating detection devices (nodes). Sometimes nodes also integrate with actuators and / or displays that provide actions / information to the environment. In general, such networks consist of low-cost, low-power, resource-constrained multifunctional sensor nodes, often with limited computing and detection capabilities in an unattended hostile environment. For this reason, IoT devices (sensors) can be completely disabled with Flood Attack and could not send the sensor values they should transmit. For example, if the environmental values (temperature and humidity) of the data center cannot be transmitted under flood attack, so large disasters can occur and counter-measures cannot be taken in a timely manner due to an incorrect monitoring system.

In order to analyze the effect of Flood attack on WSN, the pre-attack references and the values during the attack were compared for the Hop Counts required for each mote to access the sink mode. The graphical representation of the packages captured related to these values can be seen in Figure 4. When Figure 4 is examined, it is seen that the hop counts before the attack increased remarkably during the attack. During the Flood attack, the motes could not broadcast location information in the topology to the other motes. In this case, each mote has to perform an excessive hop count to access the sink mote, which leads to unnecessary energy consumption. As a result, the motes cannot perform their functions in time and the sensor values cannot be transmitted to the units needed.



(a) *Reference Model* ***(b)*** *After Flood Attack*

Figure 4. *Hop Count Graph*

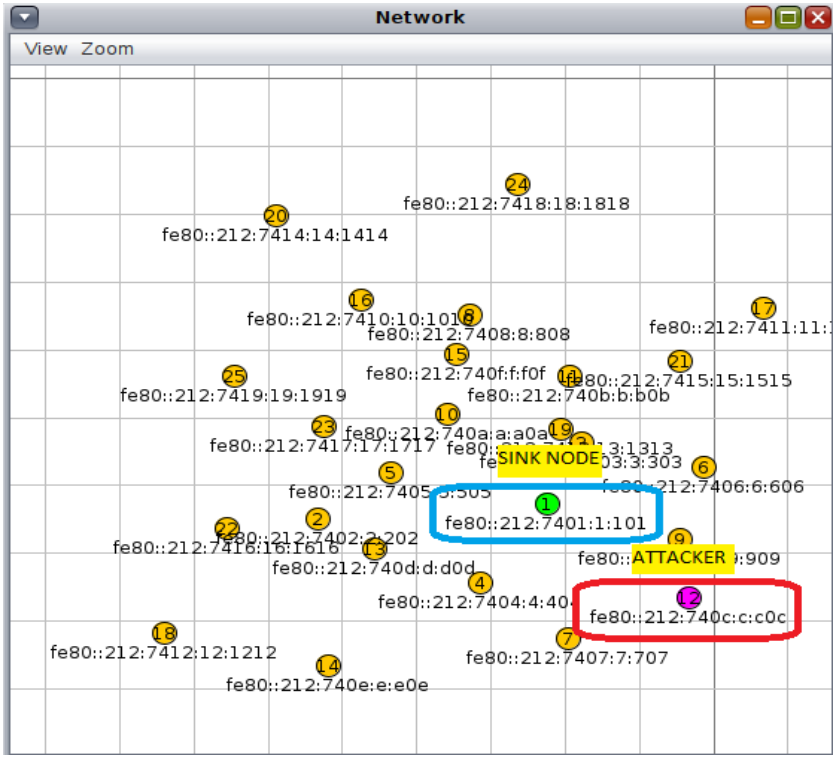


Figure 5. *Network Topology*

As seen in Figure 5, the mote with fe80 :: 212: 7401: 1: 1: 101 IPV6 address is sink mote, while the mote with fe80 :: 212: 740c: c: c0c IPV6 address is attacker mote. The analysis of the Wireshark Pcap file in Figure 6, most of the packets (86%) are Flood attack packets produced by the attacker. Only 14% packages were sent by other motes. For example, 668. package is the package transmitted by sink mote, it is also seen that other motes cannot respond to this package due to Flood attack.

Furthermore, as seen in the Figure 6, during the Flood attack analysis, the Cooja Simulator was halted with an out of memory error as a result of the attack test performed.

Analysis of the packages in Figure 3 - Figure 7 above shows the importance of preventing attacks with continuous monitoring on 24/7 basis and detecting abnormal behaviors in IoT traffic with forensics analysis.

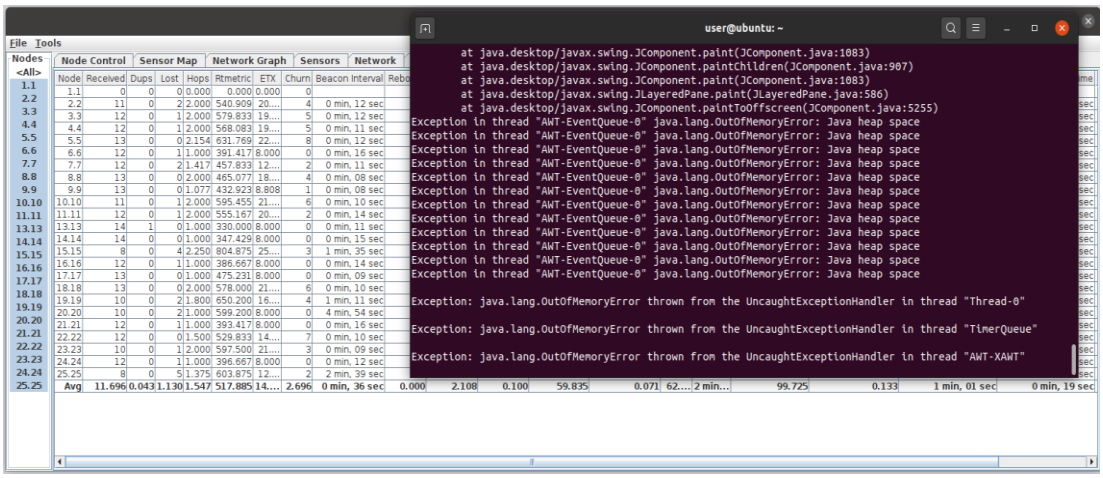


Figure 6. *System Out of Memory Error Due to Flood Attack*

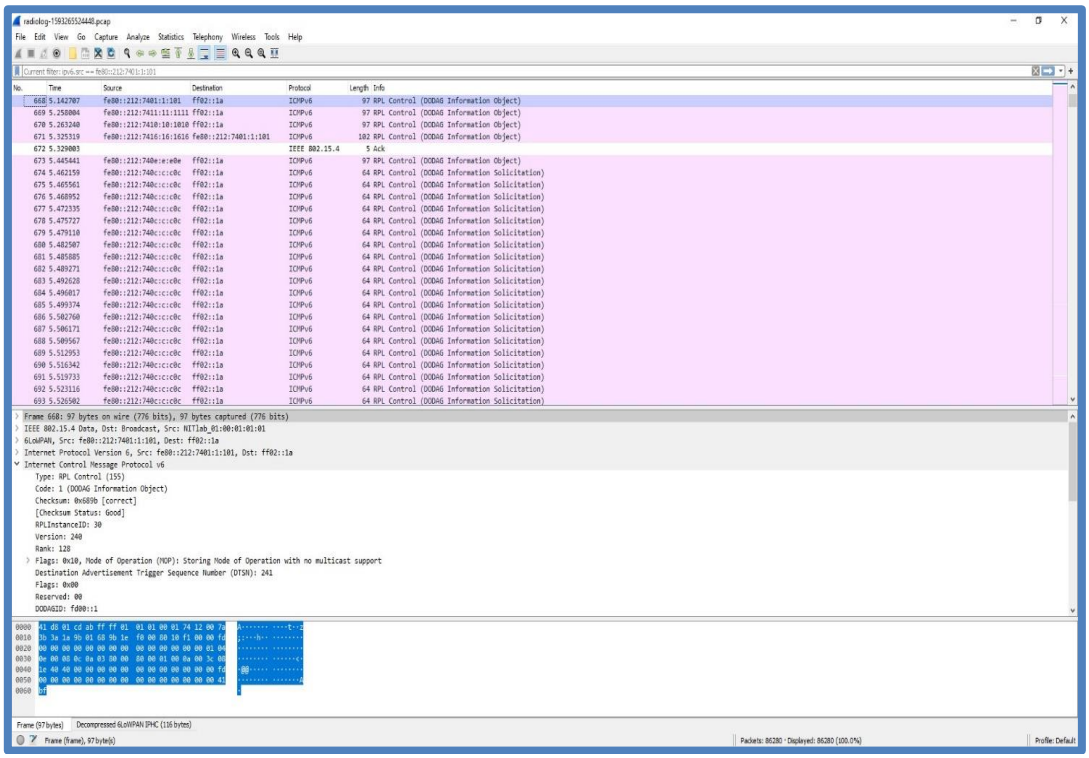


Figure 7. *Network Packet Inspection*

IV. SOLUTIONS PROPOSALS FOR IOT COMMUNICATION SECURITY

It is important that end-to-end (E2E) protection of communication between IoT devices, in other words, the confidentiality and integrity of messages should be implemented between the source and target devices. We can use IP security (IPsec) or Datagram TLS (DTLS) to force E2E message security in IoT using standard protocols. Research is ongoing to securely connect restricted nodes in the 6LoWPAN

network to the Internet using lightly compressed IPsec, light DTLS [19] and IEEE 802.15.4 link layer security [20].

When the literature on cyber security of IoT devices is examined, there are lots of works on IDS systems to ensure cyber security of them. We can divide these IDS systems into 2 types: signature-based and behavior-based. When these systems are evaluated, the signature database is very important in signature-based structures, and it is seen that harmful codes that are not found in the database can easily overcome these systems. On the other hand, in behavior-based systems that can make intuitive detection against this problem, the detection success increases but the probability of false positive also increases with the success of the system. Therefore, the need for error correction of the heuristic systems will appear as an additional cost.

Due to the diversity of attacks and the unpredictable behavior of new attacks, behavioral IDSs are exposed to false positives (to alarm when there is no attack) and false negatives (not to alarm when attack). Therefore, the vulnerabilities of IDS systems can be eliminated by 24/7 continuous monitoring and the opportunity to conduct a forensic analysis emerges after an incident by recording the network traffic.

V. CONCLUSION

In this study, the aim clearly stated at the beginning of the paper has been achieved. Forensics analysis of average power consumption, hop count and captured packets have been implemented. The simulation results which clearly demonstrated that the flood attack reduced the performance of the wireless sensor network. The attack analysis has showed that the Flood attack rendered IoT devices dysfunctional, caused excessive power consumption, so sensor data couldn't be transferred. For these reasons, continuous monitoring and packet analysis become vital in scenarios where changes in sensor values and / or sensor values are not transmitted as a result of attacks on IoTs. Only in this way, the system can be recovered as soon as possible, the system can be recovered with the least damage and can be activated again as soon as possible. In addition, by means of the forensics analysis, necessary measures can be taken to avoid similar disaster scenarios.

VI. FUTURE WORKS

This study focuses on the flood attack. In the following study, the results of DODAG Version, Blackhole and Rank Attacks will be emphasized, the effects of these attacks on the WSN network and the precautions to be taken will be examined with forensics analysis to be performed on the packets captured during the attack.

VII. REFERENCES

[1] Z. Sun, M. Wei, Z. Zhang, G. Qu, "Secure Routing Protocol Based on Multi-Objective Ant-Colony-Optimization for Wireless Sensor Networks," *Applied Soft Computing*, vol. 77, pp. 366-375, 2019.

[2] D. Evans, "How the Next Evolution of the Internet Is Changing Everything," 2011. [Online]. Available: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. Accessed: 17.09.2020.

[3] S. Görmüş, H. Aydın, G. Ulutaş, "Security for the Internet of Things: A Survey of Existing Mechanisms, Protocols and Open Research Issues," *Journal of the Faculty of Engineering and Architecture of Gazi University*, vol. 33, no. 4, pp. 1247-1272, 2018.

[4] H. Lamaazi, N. Benamar and A. J. Jara, "RPL-Based Networks in Static and Mobile Environment: A Performance Assessment Analysis," *Journal of King Saud University-Computer and Information Sciences*, vol. 30, no. 3, pp. 320-333, 2018.

[5] H. Lamaazi, N. Benamar, "A Comprehensive Survey on Enhancements and Limitations of the RPL Protocol: A Focus on the Objective Function," *Ad Hoc Networks*, vol. 96, 2020.

[6] I. Butun, P. Österberg and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 616-644, 2020.

[7] I. Wadhaj, B. Ghaleb, C. Thomson, A. Al-Dubai and W. J. Buchanan, "Mitigation Mechanisms Against the DAO Attack on the Routing Protocol for Low Power and Lossy Networks (RPL)," *IEEE Access*, vol. 8, pp. 43665-43675, 2020.

[8] C. Pu, "Sybil Attack in RPL-Based Internet of Things: Analysis and Defenses," *IEEE Internet of Things Journal*, 2020.

[9] A. L. Imoize, T.R. Oyedare, C. G. Ezekafor, & S. Shetty, "Deployment of An Energy Efficient Routing Protocol for Wireless Sensor Networks Operating in A Resource Constrained Environment," *Transactions on Networks and Communications*, vol. 7, no. 1, pp. 41-41, 2019.

[10] K. N. Qureshi, S. S. Rana, A. Ahmed, & G. Jeon, "A Novel and Secure Attacks Detection Framework for Smart Cities Industrial Internet of Things," *Sustainable Cities and Society*, vol. 61, 2020.

[11] X. Sun, W. Liu, T. Wang, Q. Deng, A. Liu, N. N. Xiong, & S. Zhang, "Two-Hop Neighborhood Information Joint Double Broadcast Radius for Effective Code Dissemination in WSNs," *IEEE Access*, vol. 7, pp. 88547-88569, 2019.

[12] A. Verma & V. Ranga, "Addressing Flooding Attacks in IPv6-Based Low Power and Lossy Networks," *TENCON 2019-2019 IEEE Region 10 Conference (TENCON)*, pp. 552-557, 2019.

[13] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, & Y. Elovici, "N-Baiot—Network-Based Detection of Iot Botnet Attacks Using Deep Autoencoders," *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 12-22, 2018.

[14] X. Zhang, O. Upton, N. L. Beebe & K. K. R. Choo, "IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers," *Forensic Science International: Digital Investigation*, vol. 32, 2020.

[15] A. Dunkels, B. Gronvall, & T. Voigt, "Contiki-A Lightweight and Flexible Operating System for Tiny Networked Sensors," *IEEE International Conference on Local Computer Networks*, pp. 455-462, 2004.

[16] E. Sesli & G. Hacıoğlu, "Contiki OS Usage in Wireless Sensor Networks (WSNs)," *Turk J Electrom Energy*, vol. 2, no. 2, pp. 1-6, 2017.

[17] L. Wallgren, S. Raza & T. Voigt, "Routing Attacks and Countermeasures in the RPL-Based Internet of Things," *International Journal of Distributed Sensor Networks*, vol. 9, no. 8, pp. 794326, 2013.

[18] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal & B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*, vol. 7, pp. 82721-82743, 2019.

[19] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig & G. Carle, "DTLS Based Security and Two-Way Authentication for the Internet of Things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2710-2723, 2013.

[20] S. Raza, S. Duquennoy, J. Höglund, U. Roedig & T. Voigt, "Secure Communication for the Internet of Things—A Comparison of Link-Layer Security and IPsec for 6LoWPAN," *Security and Communication Networks*, vol. 7, no. 12, pp. 2654-2668, 2014.