Journal of information and communication convergence engineering
http://jicce.org

J. Inf. Commun. Converg. Eng. 16(2): 93-98, Jun. 2018 Regular paper

DoS Attack Control Design of IoT System for 5G Era

Kwangcheol Rim[1] and Dongho Lim[2*], *Member*, *KIICE*

[1]Department of Mathematics, Chosun University, Gwangju 61452, Korea
[2]Department of Mathematics Education, Sehan University, Chonnam 58447, Korea

Abstract

The Internet of Things (IoT) is a form of the emerging 4th industry in the 5G era. IoT is expected to develop naturally in our daily life in the 5G era in which high-speed communication will be completed. Along with the rise of IoT, concerns about security and malicious attacks are also increasing. This paper examines DoS attacks, which are one of the representative security threats of IoT and proposes a local detection and blocking system that are suitable for response to such attacks. First, systems of the LoRaWAN type, which are most actively researched in the IoT system field and DoS attacks that can occur in such systems were examined. Then, the inverse order tree algorithm using regional characteristics was designed as a cluster analysis form. Finally, a system capable of defending denial-of-service attacks in the 5G IoT system using local detection and blocking with the Euclidean distance was designed.

Index Terms: IoT system, Long range wide area network, 5G DoS, 5G IoT

I. INTRODUCTION

Recently, the Internet of Things (IoT) is expected to play critical roles in the construction of an ecosystem for the next-generation mobile communication services. Furthermore, mobile communication service experts and related companies are regarding the IoT as a core engine for the continued growth of the mobile communication industry. The number of IoT devices until 2025 is expected to increase to approximately 30 billion units. Among them, the number of devices accessing the low-power wide-area (LPWA) is expected to reach approximately 7 billion units by 2025.

LPWA requires low power consumption design, the supply of low-priced terminals, low development cost, and the provision of stable coverage. The existing transmission standards such as ZigBee, Wi-Fi, and Bluetooth failed to satisfy such requirements. Hence, new transmission standards have been proposed. The representative standards are SigFox from SIGFOX, and long range wide area network (LoRaWAN) supplied free of charge by LoRa Alliance, a non-profit organization. The LoRaWAN is pursuing free open policy and is expected to be the most advanced and activated transmission standard in the 5G era. The SMATRER, which is an ongoing study item that defines the requirements of the 5G system, has presented a requirement that the 5G mobile communication system must be defined in an efficient structure in support of the IoT. NestGen, which is a study item related to the 5G system architecture, is carrying out various tasks to efficiently define services on IoT terminals based on such requirements [1].

The IoT requires the same security in the general Internet environment because the same security conditions are applied when things are connected to the Internet. Such adverse effects of the Internet as hacking, viruses, and denial-of-service (DoS) attacks can occur, as well as cyber terrorism such

Received 02 April 2018, **Revised** 18 June 2018, **Accepted** 18 June 2018
***Corresponding Author** Dongho Lim (E-mail: dhlim@sehan.ac.kr, Tel: +82-61-469-1283)
Department of Mathematics Education, Sehan University, 1113, Noksaek-ro, Samho-eup, Yeongam-gun, Chonnam 58447, Korea.

Open Access https://doi.org/10.6109/jicce.2018.16.2.93 print ISSN: 2234-8255 online ISSN: 2234-8883

as defamation and privacy infringement. Among them, privacy infringement is a very important issue from the ethical, legal, social, and political point of view. The smooth operation of the IoT environment requires the inclusion of maintenance cost in the total cost in order to actively detect and remove security vulnerabilities in the software design phase. As a result of classifying and analyzing IoT-related studies, most studies were about proposed services, whereas few studies were about the platform and security, which play key roles in the value chain of the ecosystem [2-5].

It was found that around 70% of digital devices connectible to the IoT network sent collected information without encryption to the clouds or local networks, and around 60% of all IoT devices were using Web interfaces vulnerable to security. Furthermore, around 60% of users did not use encryption even when updating software, which shows very low awareness of security [2].

Consequently, this paper proposes an inverse order tree system that can examine and control DoS attacks, one of the most serious security concerns in IoT, which has become the most important subject in the 5G era. Section II describes the system architecture of the LoRaWAN type and examines plausible DoS attacks. Section III describes clusters applying the Euclidean distance, which is the basic framework of the proposed system. Furthermore, the inverse order tree is designed using the inverse data flow of the tree structure. Section IV defines clusters of end node and gateway using the Euclidean distance cluster and designs the terminal control DoS defense technique through them.

II. IOT SYSTEM IN THE 5G ERA

As shown in Fig. 1, end nodes send data via RF communication to all the surrounding gateways instead of one gateway. The surrounding gateways send the received data to the network server through a public network, 5G. The network server runs an application in line with the end node situation by sending it to each application server. In this process, the sections can be divided into communication between an end node and gateway, communication between a gateway and network server, and communication between a network server and application server. If the attackers regarded it as difficult to intrude in a communication section by 5G, they would plan an attack using RF communication. Such attacks will mainly consist of system intrusions or DoS attacks.

If a DoS attack is made on an end node side or a gateway side, the attacker can paralyze a network server or the desired application server through a network server. Every DoS attack is very difficult to prevent or detect in advance. It should be noted that it is difficult to prevent DoS attacks in the 5G era as well and the system should be designed to minimize damages.

The DoS attack in the IoT environment is carried out as follows. The attacker installs a malicious gateway outside the network and continuously collects join requests sent from terminals. Fig. 2 is show join request attack. The malicious gateway obtains AppEUI and DevEUI from the collected join request messages. The malicious gateway forwards fabricated join request messages to several normal gateways using the collected IDs. The normal gateways forward the fabricated join request messages to the network server, and the network server receives the join request message of the attacked node and sends a join accept message. Then, the malicious gateway does not set up the join procedure, but continuously sends the join request messages to cause overload in the network server with the effect of SYN flooding attack [6, 7].

III. CLUSTER ANALYSIS USING INVERSE ORDER TREE

Cluster analysis refers to the classification and analysis of the classification criteria of data, which express the characteristics of each object of observation, based on the similar-

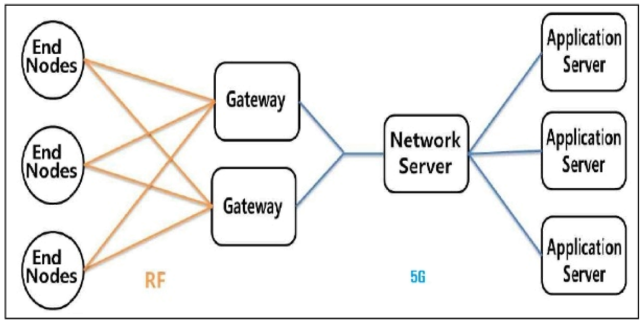

Fig. 1. Configuration of a LoRAWAN Network.

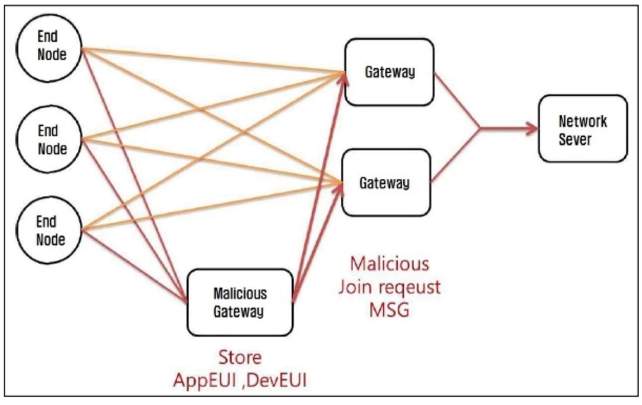

Fig. 2. Join request attack.

ity of the data. One of the cluster analysis methods by distance is to classify clusters using the Euclidean distance and include their weights [8].

To perform cluster analysis, if each object has a attributes, and there are b objects, a subjective measure can be given to each of the b objects, and a measurement for the data of which the observed value is changed for such a measure is determined. If two random objects among the b objects are x_u and x_v, they can be expressed as follows:

$$x_u = (x_{u1}, x_{u2}, x_{u3}, ..., x_{ua})$$
$$x_v = (x_{v1}, x_{v2}, x_{v3}, ..., x_{va})$$

These can be regarded as elements of a-dimensional vector space for a attributes. If the difference of variates corresponding to each object is small, it is used as a criterion for deciding similarity of two objects. Furthermore, the shape of the cluster can be expressed variably by giving weight to each variate.

The range of a cluster can be determined using the Euclidean distance concept.

The general Euclidean distance is as follows:

$$d_{uv} = \sum_{k=1}^{n}(x_{uk}-x_{vk})^2 \quad (1)$$

If weight w_k is given to each layer, the distance can be expressed as follows:

$$wd_{uv} = \sum_{k=1}^{n} w_k(x_{uk}-x_{vk})^2 \quad (2)$$

To determine the Pearson's product moment correlation coefficient using the scalar product of a vector:

$$x_u \cdot x_v = \sum_{k=1}^{n} \frac{(x_{uk}-\overline{x_u})}{\sqrt{\sum_{h=1}^{n}(x_{uh}-\overline{x_u})^2}\sqrt{\sum_{h=1}^{n}(x_{vh}-\overline{x_v})^2}}$$

$$\overline{x_u} = \frac{1}{2}\sum_{k=1}^{n} x_{uk} \quad (3)$$

If all the components of objects are binary data, the expressions of vector components of objects can be classified into the following four types:

$$\text{Number of } (1,1) = \sum_{k=1}^{n} x_{uk}x_{vk} \quad (4)$$

$$\text{Number of } (1,0) = \sum_{k=1}^{n} x_{uk}(1-x_{vk}) \quad (5)$$

$$\text{Number of } (0,1) = \sum_{k=1}^{n} (1-x_{uk})x_{vk} \quad (6)$$

$$\text{Number of } (0,0) = \sum_{k=1}^{n} (1-x_{uk})(1-x_{vk}) \quad (7)$$

The sum of these four numbers is total n.

A. Weighted Inverse N-Ary Tree

Weights can be applied depending on the importance among the bottom components or the components of a middle layer. The weight of such importance is defined by the user, and the determined weights are expanded by multiplication when they are moved to an upper layer.

As shown in Fig. 3, user-defined weight m_0 is given to each component of the last layer, and weight m_1 is given to the second layer. Each node component of the last layer is affected by weight and can be expressed as follows:

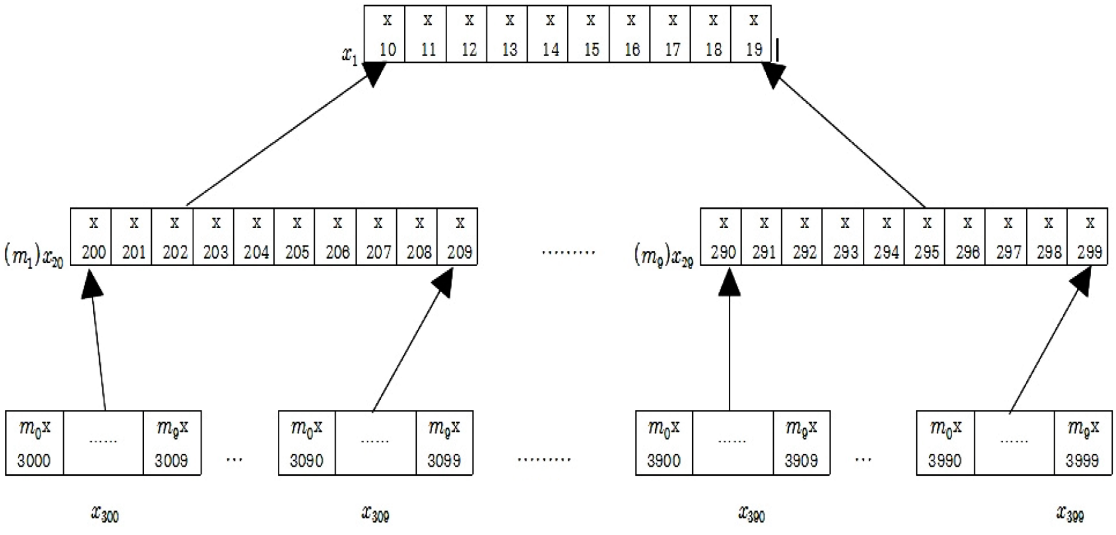

Fig. 3. Weighted tree with 3 layers and a weight of m.

$$x_{30} = (m_1x_{3000}, m_1x_{3001}, m_1x_{3002}, m_1x_{3003}, ..., m_1x_{3008}, m_1x_{3009}) \quad (8)$$

The sum of these components is transferred to a component of the one-step higher layer.

The movement of the components in Fig. 3 are as follows:

$$\begin{aligned} x_{10} &= \sum_{k=0}^{9} x_{20k} \\ &= x_{200} + x_{201} + \ldots + x_{208} + x_{209} \\ &= \sum_{j=0}^{9} m_j x_{300j} + \sum_{j=0}^{9} m_j x_{301j} + \cdots + \sum_{j=0}^{9} m_j x_{309j} \\ &= \sum_{k=0}^{9} \sum_{j=0}^{9} m_j x_{30kj} \\ &\vdots \\ x_{19} &= \sum_{k=0}^{9} x_{29k} \\ &= x_{290} + x_{291} + \ldots + x_{298} + x_{299} \\ &= \sum_{j=0}^{9} m_j x_{390j} + \sum_{j=0}^{9} m_j x_{391j} + \cdots + \sum_{j=0}^{9} m_j x_{399j} \\ &= \sum_{k=0}^{9} \sum_{j=0}^{9} m_j x_{39kj} \end{aligned} \quad (9)$$

IV. IOT SYSTEM USING INVERSE ORDER TREE

The IoT system design is dependent on the Euclidean distance. The network connection between things forms a network of adjacent things, and their traffic is gathered in a gateway within the Euclidean distance. Thus, in this study, the total network is configured by forming layers based on the Euclidean distance and expressing the components for the occurrence of specific data between layers.

The basic structure of the design is as follows:

1. Determine the gateway cluster by the end node cluster.
2. Determine the gateway cluster by the Euclidean distance.
3. Determine the logical network server layer by the Euclidean distance.
4. Determine the upper network server layer.
5. Configure the application service.

The end node, which is in charge of the lowest node, denotes the terminal point given to each thing. The end node sends traffic to the closest gateway, and the layer of the gateway is determined by such physical distance. Specific data that shows a sign of attack, etc. in clustered gateways is sent to the upper layer through the sum of the inverse tree components as described in Section III. A DoS attack can be blocked by local blocking after identifying the states of the clustered gateways in a local layer before the network server has an operation error owing to the accumulation of excessive traffic in the upper layer.

As shown in Fig. 4, the gateway groups are divided into A, B, C, and D depending on the region of the end nodes. The groups need not necessarily have the same number of gateways. If an attacker creates a malicious gateway in group D and generates specific traffic between an end node and gateway, the component of NS2, which is the upper layer of the D layer, is derived by an excessive sum of abnormal signs. The administrator should proactively block the network of NS2 or lower and treat the malicious gateway. For the overall system, only NS2 and lower nodes malfunction, and the network and application services of the remaining A and B groups will operate normally.

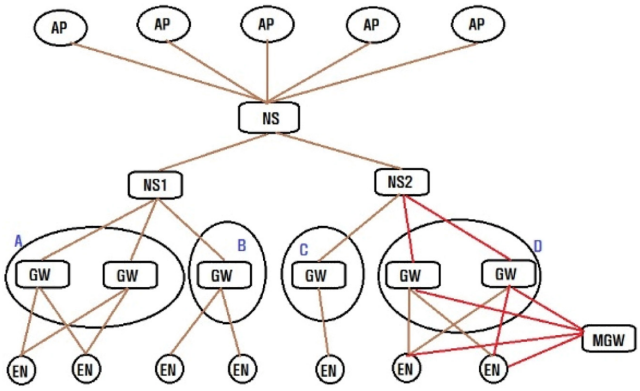

Fig. 4. DoS defense using inverse order tree.

For example, if end nodes that belong to D group at ordinary times generate t sequence and u sequence, a sequence that is different from the sequent that is generated at ordinary times is generated by MGW. This different sequence in turn affects the gateway component sequence in the D group. Then, the component sequences in the D group are added and stored in the component sequences of the NS2 layer. In this process, the administrator does not need to examine the entire system, but only the NS2 and lower network, which shows the sum of a specific component sequence. If there is a sign of attack, the NS2 and lower network is controlled, and the gateway of the lower group is reset to block MGW.

Let count of event group D

t = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0),
u = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0),
first gateway = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0),
second gateway = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0),

then occurrence of attack event at t and first gateway, second gateway

t = (0, 0, 0, 0, 0, 0, 0, 0, 1, 1),
u = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0),
first gateway = (1, 0, 0, 0, 0, 0, 0, 0, 1, 1),
second gateway = (1, 0, 0, 0, 0, 0, 0, 0, 1, 1).

By MGW the first element of the first gateway and second

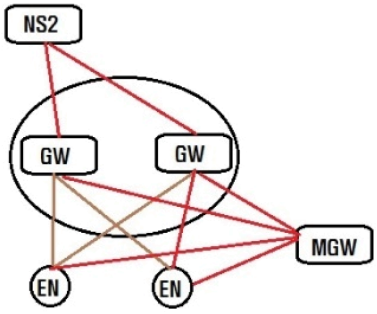

Fig. 5. DoS attack part.

gateway sequence has been changed to 1.

Because counter of NS2 sequences is

NS2 = (2, 0, 0, 0, 0, 0, 0, 0, 2, 2).

Fig. 5 shows the flow of data when the DoS attack proceeds.

The operation design of the defense system is as follows:

1. Data is generated at the end node.
2. Data and layer value are sent to the gateway determined by the Euclidean distance.
3. Send the layer value of each gateway to the upper layer.
4. If the cumulative sum of the layer values is determined as a singularity, the lower network is blocked.
5. Restore after identifying the physical location.

As described above, the proposed system does not build a defense system simply for traffic congestion. The currently distributed denial-of-service (DDoS) response systems show response performance above a certain level for simple attacks and traffic congestion attacks that only use the characteristics of network packets, but they still do not show satisfactory performance for DoS attacks for the application layer. This is because they just apply the past method of detecting traffic explosion attacks to the DoS attacks of the application layer. The DoS attacks of the traffic explosion detect the change in traffic amount in various ways and determine attack based on the detection result because the amount of attack traffic increases sharply compared to the network traffic in a normal situation. However, the application layer DoS attacks can attack even without increasing the amount of attack traffic compared to the normal situation. Thus, the method of judging attack using only the amount of attack traffic is inefficient for the detection of DoS attack of the application layer.

Therefore, about the DoS attack for the application layer, it must be possible to analyze the typical traffic characteristics of the application program and determine how the traffic is different from the analysis result, rather than detecting the amount of attack traffic.

The method proposed in this system, the normal state of the traffic generated at the end node is continuously sent to the upper layer. When an appropriate time passes after system installation, information about the normal situation sent from each end node is accumulated. When an attack is made, the traffic movement will be different from the normal situation, and because of the nature of IoT devices, the propagation to a malicious gateway that is far beyond the physical distance will be difficult. The gateways based on the Euclidean distance generated from the end nodes of IoT terminals will have a particular traffic pattern, and DoS attacks generated by the creation of a malicious gateway can be controlled by regional blocking.

The advantages and disadvantages of the proposed system are as follows:

1. The system has no problem because it requires a small amount of additional traffic.
2. It is easy to analyze in the 5G IoT system of the upstream transmission mode.
3. It is easy to respond to unknown attacks owing to the steady accumulation of specific data.
4. It is cheaper because only logical modifications are made to the existing method.
5. A small loss of power and traffic is generated even if it is small because the transmission of specific data is required inevitably.

IV. CONCLUSION

The 5G IoT is emerging as the core of the fourth industry. However, the security of IoT is not becoming an important topic for discussion among both users and administrators. In the 5G era, the basic operation method of the IoT is expected to be based on bottom-up information delivery. In the bottom-up information delivery method, the attackers will focus on DoS attacks to cause network paralysis. Owing to the nature of IoT, the network will be installed even in deep places of living. As a result, it will become impossible to live outside the IoT from daily life, to health, diseases, and industries. In this respect, DoS attacks using IoT will undoubtedly occur.

To cope with this, this study examined an open system of the LoRaWAN type that is widely known and designed a reverse tree structure using the Euclidean distance as a way to control attacks to this system. The inverse tree structure was applied to the LoRaWAN system to set up regional groups of the traffic generated at the lowest node to accumulate the number of specific data generation in the upper layer to promote the security of the entire system through local control. If multilateral studies on the singularities during DoS attacks and the signs of excessive traffic are conducted concurrently, we could expect safe operation of 5G IoT at low cost.

REFERENCES

[1] D. Y. Kim, J. S. Park, Y. H. Choi, and Y. C. Choi, "Device state and packet transmission control scheme of 5G networks for supporting uplink-oriented IoT services," in *Proceedings of the 2016 Institute of Electronics and Information Engineers Fall Conference*, Daegu, Korea, pp. 335-337, 2016.

[2] J. H. Lee, "A literature review on security for Internet of Things in Korea based on IoT S-P-N-D-Se ecosystem model," *Journal of Security Engineering*, vol. 12, no. 4, pp. 397-414, 2015. DOI: 10.14257/jse.2015.08.05.

[3] Y. A. Hur and K. H. Lee, "A study on countermeasures of convergence for big data and security threats to attack DRDoS in u-healthcare device," *Journal of the Korea Convergence Society*, vol. 6, no. 4, pp. 243-248, 2015. DOI: 10.15207/JKCS.6.4.243.

[4] S. H. Park and J. K. Park, "Security technology trend of IoTs," in *Proceedings of the Korea Institute of Information & Telecommunication Facilities Engineering Summer Conference*, pp. 169-171, 2016.

[5] H. S. Chang, H. J. Kim, and T. Shon, "Study of cyber security issues in industrial IoT," *KIISE Review*, vol. 25, no. 5, pp. 12-17, 2015.

[6] S. J. Na, J. W. Lee, and K. H. Kim, "A study of DoS attack scenario in LoRaWAN," in *Proceedings of the Korea Institute of Information & Telecommunication Facilities Engineering Summer Conference*, pp. 53-55, 2016.

[7] LoRa Alliance, "LoRaWAN Specification v1.0," 2015 [Internet], Available: https://lora-alliance.org/resource-hub/lorawantm-specification-v10.

[8] K. C. Rim and K. B. Lee, "An analysis of voter behavior in campaign scenes utilizing an inverse-order tree and a smartphone application," *International Journal of Applied Engineering Research*, vol. 11, no. 2, pp. 815-819, 2016.

Kwangcheol Rim

received the Ph.D. degrees in mathematics from Chosun University in 2006. He is currently a researcher in education and information security. His current research interests are applied education, endpoint security and big data.

Dongho Lim

received the Ph.D. degrees in mathematics from Hankuk University of Foreign Studies in 2013. He is currently a researcher in education and geometry. His current research interests are applied education, endpoint security and Manifold theory.