Fuzzy-Based Protocol for Secure Remote Diagnosis of IoT Devices in 5G Networks

Vishal Sharma[1], Jiyoon Kim[1], Soonhyun Kwon[1], Ilsun You[1(✉)], and Hsing-Chung Chen[2]

[1] Department of Information Security Engineering, Soonchunhyang University,
Asan-si 31538, Republic of Korea
vishal_sharma2012@hotmail.com, 74jykim@gmail.com,tnsgus08@gmail.com,
ilsunu@gmail.com

[2] Asia University, Taichung, Taiwan
cdma2000@asia.edu.tw

Abstract. Internet of things (IoT) aims at connecting a large number of devices for supporting "Connectivity to All" in the 5G networks. With connections between the majority of computing devices, capturing a single entity can expose the perimeter of the entire network. Remote diagnosis of the IoT devices can help in identification of such loopholes. However, if an intruder is already present in the network, it can falsify the diagnostic procedures and can cause serious threats to the network. Thus, an efficient strategy is required which can provide remote diagnosis along with the secure validation of IoT devices. In this paper, fuzzy logic is used to resolve the safety decisions and remote diagnosis of IoT devices in 5G networks. The proposed solution uses a two-pass methodology to generate inference rules at the central as well as the local inference engine. The proposed approach evaluates the network in two phases. The first phase emphasizes on the remote diagnosis and the second phase emphasizes on the remote validation. On the basis of these phases, a remote assessment protocol is also proposed which helps in remote validations with lower overheads and ease of deployment.

Keywords: IoT · Fuzzy · Security · Remote-diagnosis · 5G

1 Introduction

The modern era has changed every entity into a computing object making a way for connecting a billion of devices as predicted for 2020 [1,2]. With the aim of "Connectivity to All", Internet of Things (IoT) has emerged victorious in defining new rules and standards for the exchange of services between the network entities. IoT is seen as a next big market for computing as it provides control over every day's activity [3,4]. IoT supports connectivity of our daily usage objects and entities via a common network. This allows easy access to information as well as control over the connected devices. The management of

Y.-B. Lin et al. (Eds.): IoTaaS 2017, LNICST 246, pp. 54–63, 2018.
https://doi.org/10.1007/978-3-030-00410-1_8

network has been facilitated by IoT. IoT has enabled to access data without any excessive burden on a single computing entity. It also reduces the time and cost involved in the evaluation of acquired data. Supply chain maintenance, information gathering, remote monitoring are some of the key advantages of IoT networks [5–7].

Despite a large number of advantages of IoT networks, there are certain challenges and issues associated with their actual operations and deployments. The middleware which connects different IoT devices needs to be compatible with every entity in the network. A non-compatible middleware may cause replanning of the entire network. Further, the incompatible units in IoT directly influence the cost of operation as well as the deployment complexities. Another major issue is the mode of communication and standards to be used for all the types of information flows. The standard may vary, but the underlying hardware should be operable without any change in the type of media and information. Privacy of data and security are the other requirements of services over IoT networks. Overcoming these issues allows the development of a highly robust, fault-tolerant and stable network without much complexity as well as cost [8,9].

IoT devices are used to make different applications and information seeking solutions. However, one crucial issue which is generally not considered is the evaluation of the IoT devices. Every IoT device in a network requires periodic updates in operations and firmware [10]. The introduction of the new security measures is often required in these types of network. All these procedures are subject to the level of information about the IoT device. The information regarding the functionalities of every device can be obtained using remote diagnosis. Remote evaluation of IoT nodes helps in identification of the state of operations as well as the working conditions. However, remote diagnosis procedures are always under the threat of attackers as a control over a single IoT device may open the perimeter of the entire network. Misleading information regarding the state of IoT device makes the network vulnerable to various types of attack. Thus, remote diagnosis needs to be secure and validated to protect the network from any attacker.

Remote diagnosis can be secured by using the security protocols for IoT devices. Some of the key security solutions which can be extended for securing the remote diagnosis of IoT networks include lightweight security protocols by Lee et al. [11] and Raza et al. [12], two-way authentication by Kothmayr et al. [13]. Remote monitoring solutions which are usually used for medical purposes can be altered to check the functionality of IoT devices [14]. Deployment of various intrusion detection systems can also be considered for securing the remote diagnosis of IoT devices. Although all such solutions can be efficient, these will surely increase the overheads because of excessive computational burden.

Modern day IoT devices are small and have limited resources; also these are operated over the same channel which is used for other communication activities. Thus, the solution for remote diagnosis needs to adopt the similar policies and should not cause excessive overheads while analyzing the IoT devices. Thus, aiming at such requirement, a fuzzy-based secure assessment protocol is proposed in this paper. The proposed protocol utilizes the two-pass aspect-oriented fuzzy inference system, one for the remote diagnosis and the other for remote validation. The success of the proposed approach lies in its low-complex and less overhead solution for analyzing any IoT devices considering its properties irrespective of the type of connectivity between them.

2 Problem Definition

Connections between large numbers of computing devices are highly sensitive, time bound and vulnerable to various types of threats. To make the network function all the time without fail, it is necessary to diagnose its devices for any threat and fault. However, the identification procedures and diagnosis strategies need to be secure to prevent any intruder from falsifying the exact state of IoT devices. Wrong information about the devices may cause the analyzing node to see a correct network even in the presence of a faults or threats. This problem can be worst in the presence of a large number of devices as it becomes extensively slower to identify every potential threat on the IoT device. There is a requirement of efficient solutions which are low-complex and can be used to securely diagnose every device in the network without fail as well as with lower computational overheads.

3 Network Model

The proposed approach utilizes the core components of the standard 5G network which comprises a core node, controlling switches, multiple hubs, terminals, and Access Points (APs). The standard 5G-IoT network emphasizes on providing services to IoT devices either by a direct connection between the near APs or via a Home Gateway (HGW). The network further comprises Mobile Nodes (MNs) that opt for diagnosing the particular IoT device remotely. The proposed approach does not alter the actual architecture of the 5G networks, rather it uses a fuzzy support system on all the crucial nodes as shown in Fig. 1. The fuzzy inference engines are deployed on all the hubs that conduct fuzzy-based layoffs with both the MN and the IoT devices via APs or HGW. A local fuzzy inference engine can also be deployed on the HGW. However, this is an optional validation procedure which may enhance the security but may also cause much latency. A heavy functionality-based fuzzy inference evaluator is also deployed on the core node of the 5G network. This is also termed as the validation server. This server comes in operation only when the validation of the fuzzy rules is to be conducted for any MN or the IoT device.

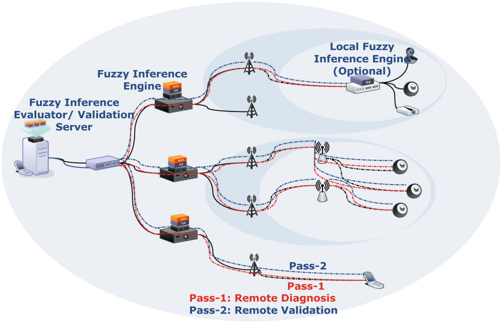

Fig. 1. An illustration of the fuzzy-based 5G architecture considered in the proposed solution.

4 Proposed Approach

The proposed approach uses two-pass fuzzy inference system as shown in the network model. The proposed approach relies on the decision taken by the fuzzy inference engine operable at each hub and validates the decisions periodically by using the IoT-context over the validation server. The fuzzy inference system over each hub operates over three main parameters, namely, trust score, content pattern, and connection strength. All these parameters are calculated for every instance of an IoT device and the output from the fuzzy inference system helps in confirming the safety level of an IoT device. The details of these parameters are as follows:

- Trust Score: It is calculated as the ratio of the total connections made by an IoT device to a legitimate entity in the network to the total legitimate connections available in the network. This parameter helps in identification of the current role and relation of each IoT device with every connectable entity in the network. A higher value means a node is known to multiple legitimate entities and is safe to operate.
- Content Pattern: It is calculated as the ratio of the total incoming requests from an IoT device to the permissible incoming requests. This helps to check if the device is falsifying the traffic or not. A lower value refers to the safe state and a higher value means a possible threat.
- Connection Strength: It is evaluated in the context of the reliability of an IoT device and is defined as the ratio of the total responses made by an IoT device in lieu of the total requests made by the server. A higher value refers to safe operations and a lower value identifies a potential threat.

The fuzzy inference rules operable at each hub for every IoT device are shown in Fig. 2. The figure shows a threat state with a safety value extremely lower at 0.2 for a higher content pattern value and lower trust score and connection strength. The output (Safety) is defined for threat, vulnerability, possible threat, borderline, and safe states. Each of these outputs is set on low, medium and high ranging between 0 and 1 with a gap of 0.2. Any property generating output above 0.6 is treated as safe for the IoT device. Trust score, content pattern and connection strength are defined considering medium at 0.5, 0.5 and 0.6, respectively.

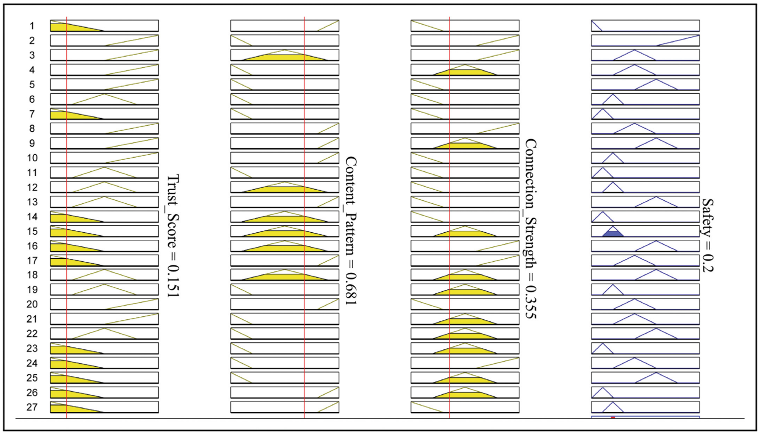

Fig. 2. An illustration of the fuzzy rules for threat decision.

4.1 Remote Diagnosis and Validation

In the proposed solution, the intermediate hub equipped with fuzzy inference servers allows checking the safety level of each device. This helps MN to believe in the report sent by an IoT device or not. The remote diagnosis process operates in parallel operation. The first operation is when an MN demands the information from a device about its working status. The second operation is when the hub identifies the IoT device from where the information is sought and computes its safety level. Once acquired, the hub shares the information with the MN to conclude the diagnosis operations. Also, the hub sends the information directly to the core server in the case of extremely low safety level for an IoT device. This initiates the remote validation procedures in the entire network. The evaluator is invoked when a hub encounters any IoT device with extremely low safety level as per the initial evaluations of the fuzzy system. The invoked evaluator determines the level of threat and alerts the corresponding entities about the status of harmful IoT device. The validation procedure is accompanied by the diagnosis steps, and thus, uses a separate pass for evaluation. The steps for remote validation after diagnosis are:

- The proposed approach uses a content to content matching procedure to identify potential threats. The key parameters used by the validation procedure include device-ID, type of device, energy consumption, usage, connections

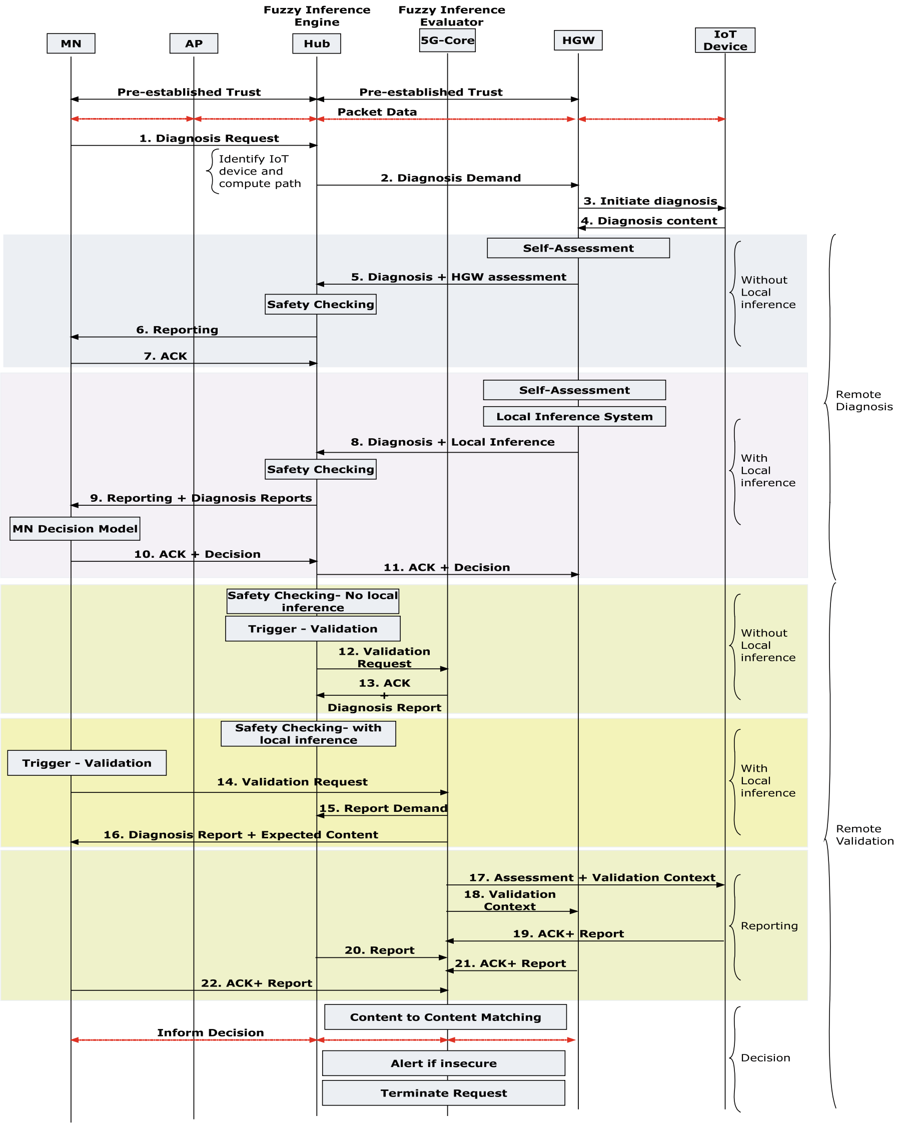

Fig. 3. Two-pass assessment protocol for remote diagnosis and validation.

supported, data rate, firmware, and registration number. Considering these parameters, the core of network maintains a corpus of this information which contains the details of every legal entity and updates it in coordination with the hub. The hub sends the periodic updates to the core for the details of IoT devices. Also, once an IoT validation request is received by the validation server, it also fetches the similar contents to verify its correctness.

- The validation server takes into account the information from both the MN as well as the IoT devices. The validation server analyzes the frequency of variations in the content and checks for threat level to other devices. Once the content matching is performed, the validation server generates alert messages to every hub which informs the corresponding MN. This helps MN in taking a decision for on-site evaluations. For further confirmations, a local inference engine can be used on the gateways as shown in Fig. 2. The local inference engine allows direct decisions without much latency. However, in such cases, trust needs to be established with the gateways. Also, it is to be noticed that the trust and control over MN are not considered in this article and will be a subject of evaluation in our future reports.

4.2 Two-Pass Assessment Protocol for Remote Diagnosis and Validation

The procedures for remote diagnosis and validation are performed as a security routine presented in Fig. 3. The protocol clearly distinguishes the validation phase from the diagnosis procedures. The detailed working of the protocol is explained below:

- The proposed protocol assumes a pre-established trust between the MN and the HGW. This trust can be secured once the entity gets activated in the network.
- Steps 1–4 deals with the diagnosis demands and is independent of the diagnosis and validation phase. These steps are used to obtain the required information from a requested IoT device.
- Steps 5–11 are the part of remote diagnosis procedures. The steps 5–7 are used in the absence of local inference system whereas the steps 8–11 are used when a local governing entity is deployed as an inference engine. These steps are the remote diagnosis pass of the proposed approach and do not uses the core as prescribed in the network model. The reports are generated on-demand irrespective of the validation.
- Next, the protocol operates for its second pass which is termed as the remote validation. Steps 12–16 are the governing rules for validation procedures and steps 17–22 are used to obtain the necessary validation context and diagnosis reports for taking final decisions.

5 Performance Case Study

In order to understand the operational activities of the proposed approach, a performance case study is conducted to analyze its operations in terms of the deployment and overheads. The details of the performance case study are presented below:

- **Deployment:** The proposed approach can be deployed as a stand-alone solution as well as a server-inhabitant solution along with the other facilities of the network such as route selection, load balancing, resource allocation, etc. The proposed approach depends on the installation of fuzzy inference systems on the key entities of the network. This installation is software assisted and algorithmic thus requires normal computational resources and no excessive network nodes. In a network, where cost and latency are not an issue, and security is a primary aspect, separate servers can be used to deploy the inference systems. However, such deployment provides deep security but at the cost of excessive computations.

- **Overheads:** The success of any approach depends on the overheads caused by it during the regular network operations. The proposed approach with its two pass facility is capable of managing the IoT networks efficiently without leveraging excess computational burden on its entities. The overheads of the proposed approach are evaluated in terms of cost of operations and response time.
  - **Cost of operations:** It identifies the run-time complexities and the number of computations required by both the diagnoses and the validation passes. The complexity of the fuzzy inference system for the remote diagnosis depends on the number of combination and the number of inputs considered for generating the safety outputs. The proposed approach utilizes three variables as an input each with three possible states, thus, the fuzzy part of the proposed approach is operable in constant time, which does not yield much complexity. The number of times an entity requests the reports from the other entities depends on the timestamp and the intermediate nodes for both diagnosis and validation procedures. Thus, the run-time complexities are the function of the number of hops and the timestamp. Small periodic updates will increase the cost of operation as well as the number of computations associated with each pass. Since the proposed approach utilizes only single-pass validation, the cost of operation is extremely low and depends only on the number of entities involved in operations.
  - **Response time:** It is the time taken by the proposed approach for deciding the safety of a particular IoT device. Without the involvement of core, the response time will depend on the time consumed in generating the fuzzy rules, inference decision, and the message exchanges. Since the fuzzy rules are defined during the initial setup of the network, the overall response time for diagnosis depends only on the inference decision and the message exchange time. However, the diagnosis time is much affected if the approach accounts for local validation along with the central validation in its second phase. In the case of local validation, the response time increases with a scale of the number of such units installed in the network. In general operations, the proposed approach is highly suitable for scenarios with pre-registered context with the core server that maintains the device-corpus for validation.

6 Conclusion

In this paper, a scenario of remote diagnosis of IoT devices along with its validation in 5G networks was considered. The proposed approach allowed identification of the safety levels of any IoT device as per the requirement of a mobile node. The proposed solution used two-pass aspect-oriented fuzzy logic to generate inference rules at the central as well as a local inference engine. These fuzzy rules helped in identification of the safety levels of an IoT device. The proposed approach evaluated the network in two phases. The first phase emphasized on the remote diagnosis and the second phase emphasized on the remote validation. On the basis of these phases, a remote assessment protocol was also proposed which helped in remote diagnosis and validation with lower overheads and ease deployment. The details of actual implementation and evaluations in the real-time with variant attacker environments will be presented in the future reports.

References

1. MacGillivray, C., Turner, V.: Worldwide internet of things forecast, 2015–2020, May 2015. http://www.idc.com/getdoc.jsp
2. Sharma, V., You, I., Kumar, R.: ISMA: intelligent sensing model for anomalies detection in cross platform osns with a case study on IOT. IEEE Access **5**, 3284–3301 (2017)
3. Sharma, V., Lim, J.D., Kim, J.N., You, I.: SACA: self-aware communication architecture for IOT using mobile fog servers. Mob. Inf. Syst. **2017**, 1–17 (2017)
4. Kumar, R., Sharma, V., Kaur, R.: UAVs assisted content-based sensor search in the Internet of Things. Electron. Lett. (2017). https://doi.org/10.1049/el.2016.3487
5. Skarlat, O., Schulte, S., Borkowski, M., Leitner, P.: Resource provisioning for IOT services in the Fog. In: 2016 IEEE 9th International Conference on Service-Oriented Computing and Applications (SOCA), pp. 32–39. IEEE (2016)
6. Aram, S., Shirvani, R.A., Pasero, E.G., Chouikha, M.F.: Implantable medical devices; networking security survey. J. Internet Serv. Inf. Secur. (JISIS) **6**, 40–60 (2016)
7. Jiang, X., Ge, X., Yu, J., Kong, F., Cheng, X., Hao, R.: An efficient symmetric searchable encryption scheme for cloud storage. J. Internet Serv. Inf. Secur. (JISIS) **7**, 1–18 (2017)
8. Sbeyti, H., Malli, M., Al-Tahat, K., Fadlallah, A., Youssef, M.: Scalable extensible middleware framework for context-aware mobile applications (SCAMMP). J. Wirel. Mob. Netw. Ubiquitous Comput. Depend. Appl. (JoWUA) **7**, 77–98 (2016)
9. Baiardi, F., Tonelli, F., Isoni, L.: Application vulnerabilities in risk assessment and management. J. Wirel. Mob. Netw. Ubiquitous Comput. Depend. Appl. (JoWUA) **7**, 41–59 (2016)
10. Hernández-Ramos, J.L., Jara, A.J., Marin, L., Skarmeta, A.F.: Distributed capability-based access control for the Internet of Things. J. Internet Serv. Inf. Secur. (JISIS) **3**(3/4), 1–16 (2013)
11. Lee, J.-Y., Lin, W.-C., Huang, Y.-H.: A lightweight authentication protocol for internet of things. In: 2014 International Symposium on Next-Generation Electronics (ISNE), pp. 1–2. IEEE (2014)

12. Raza, S., Shafagh, H., Hewage, K., Hummen, R., Voigt, T.: Lithe: lightweight secure coap for the Internet of Things. IEEE Sens. J. **13**(10), 3711–3720 (2013)
13. Kothmayr, T., Schmitt, C., Hu, W., Brünig, M., Carle, G.: DTLS based security and two-way authentication for the Internet of Things. Ad Hoc Netw. **11**(8), 2710–2723 (2013)
14. Jara, A.J., Zamora-Izquierdo, M.A., Skarmeta, A.F.: Interconnection framework for mhealth and remote monitoring based on the Internet of Things. IEEE J. Sel. Areas Commun. **31**(9), 47–65 (2013)