Device Identification and Authentication for Internet of Things using predefined characteristics

T.Kirubadevi\textsuperscript{1}, Dr.S.Ramamoorthy\textsuperscript{2}, Dr.V.N.Rajavarman\textsuperscript{3}

\textsuperscript{1}Dept of CSE ,Dr.M.G.R Educational and Research Institute, Chennai,India
\textsuperscript{2}Prof and Dean Computer Applications, Dr.M.G.R Educational and Research Institute, Chennai,India
\textsuperscript{3}Dept of CSE, Dr.M.G.R Educational and Research Institute
Chennai,India
kirubadevi.t@drmgrdu.ac.in\textsuperscript{1},  srm24071959@yahoo.com\textsuperscript{2}   rajavarman.it@drmgrdu.ac.in\textsuperscript{3}

Abstract—The Internet of Things (IoT) has been growing rapidly in the past few years. IoT constitutes various components such as smart devices, users and internet services which interact with each other to share the resources. IoT has lot of security and authentication issues. The need for device identification is still being a big challenge. There is a demand to identify the device ID operated in heterogeneous environment. The devices with different properties and characteristics needed to be managed and identified. Then consistency in the state of devices is required to manage its identity. This paper involves an approach to find or identify a device by extracting its features and combining it to record as a pattern on time basis. Thereby device authentication also becomes feasible. The Result of the simulation justifies that the patterns that are used to identify a device becomes noteworthy.

Keywords— IoT, properties, characteristics, pattern, consistency, identification, authentication.

1. INTRODUCTION

Device identification is one of the foremost topics in Internet of Things (IoT). Beside identification of the things itself, many other entities have to be identified in IoT solutions. In this paper we discussed the device identification within a network. Furthermore we look at the approach of addressing a mobile device at various locations within the network and record the pattern of features in a database. To certain extent, we can use the pattern in the database to differentiate old devices to any new device. Also from security point of view, device authentication can be initiated from recognizing the device before and after the changes in the state of the devices.

The structure of the paper is as follows. Section 2 explores the related work. Section 3 introduces the proposed work - Process of the individual device identification. Section 4 exhibits the Results of Simulation and Section 5 summarizes the Conclusion and future work.

2. RELATED WORK

Identifiers identify a single entity or a class of entities uniquely. Any single entity is called as an instance identifier and type identifier is used to state the context in IoT Standards [12]. There is a technology to differentiate between inherent patterns and dedicated patterns. Inherent patterns are used for identification like fingerprints and face recognition whereas dedicated patterns used for Quick response codes, bar codes and electronic codes, etc [11].

Miettinen, Markus, et al. introduced a system to identify the types of devices in the IoT network automatically. The system also restricts the rules for communication of unwanted devices to decrease the amount of discrepancies. They claimed that their system is used to identify device type productively [5].
This paper has architecture with a secure API. This API is used to disconnect the various services, protocols and network elements. The portability between the systems also facilitated by the API. Hence it act as a strong interface between the backbone and to the networks with maximum relocation if required. The interoperability of the systems is based on the services for a better Quality of service QoS, naming, security required for utility provisioning. [1].

The system proposed by G.Chong provides a popular and adaptable smart home system. The analysis of pros and cons of a smart home is performed. They introduced a B/S(Browse/Server) module in the smart home system. The house hold devices can be controlled remotely and conveniently through publishing the house sensor data to a remote server web page. [2]

In IoT, to identify devices in multiple environments is unmanageable since different device ID systems is employed in different devices.[3]

There is also an IDM model to differentiate the smart devices connected in the network. This variation is due to number of different devices connected to multiple users in the network. The existing IDM model required to be upgraded. [4]

Noguchi, Hirofumi, et al came out with an idea for device identification in various environments like homes, industry, institutions, roads, etc. However, the consistencies of the devices need to be checked in order to interpret the behavior of the devices. [6]. This work played as a motivation of this paper.

The interoperability of the different devices is also considered to identify a device. Despite the research linking to heterogeneous IoT networks the devices also can be diverse in nature which has to be identified and managed. The focus on the interoperability of different devices including the detection of objects or to notice the places of observation and other places to be sensed.[8] [10]

Results from another paper have shown that fingerprints are mainly used for device identification. However the accuracy may lead to small imperfections in the scenario. This research on specific electronic device released fingerprints which is used to identification of components and of the device itself. [9]

There were some problems with managing IoT devices proposed by Baldini. OpenIoT [7] is used to effectively change the environment which is used to add or remove devices in the network. The changes in the network, software version and type of software are the few reasons for the change in the environment.

There is no prominent technique for device identification as mentioned above. Hence it is essential to identify devices, equipments and users in the IoT network and proves to be an essential topic of future research in the field of IoT.

3. PROPOSED WORK

This section explains the proposed device identification approach. To identify a device automatically within a network, we first estimate the device identity. This approach is on the characteristics extracted from the device based on the changing time stamp. These characteristics in pieces are combined together to form the pattern of the device addressing scheme. Thus the reliability of the data from a device can be ensured. The device patterns are maintained in the database for further process checking. The following diagram (Fig.1) depicts the device identification approach and the individual device identification process is narrated below.

A) Extraction of Features

The main step in the process of device identification is the extraction of characteristics
Fig. 1: Device Identification Architecture

from the device signal. The features such as communication delay, communication distance from the Access point and amount of data transferred are extracted for a particular period of time to calculate the behavioral pattern of the device. The pieces of information are combined together to form a pattern. Since the state of the device vary periodically due to software and operating system updates, the behavioral pattern of the device identification pattern tends to change. Therefore in this approach, pattern extraction process is carried with all the devices.

B) Pattern recording

Every individual device is extracted with its characteristics to generate a pattern. This pattern is collected in the database. Every device generates individual pattern from its device characteristics. The process of comparing the new pattern with the stored patterns in the database is used to identify the different devices. The new pattern and the device ID are recorded in the database. This change pattern is calculated by using a similarity checking or calculator with patterns stored already in the database.

C) Similarity Checking

When identifying a target device the similarity degree is calculated with the recorded patterns. The degree of similarity calculated using normal distribution equation 1:

\[ S = \bar{X} \pm \sigma \]  

The weight of the each characteristics feature amount is calculated. Whenever a new target device is extracted the similarity checking is done with the weight of the stored device. Using the normal distribution the weights are compared and calculate the pattern for the device. Similarity checker calculates the standard deviation of the similarity degree of all the old and new patterns. This approach uses the Equation 2 to calculate the weight.

\[ \sigma = \sqrt{\frac{\sum_{i=1}^{N} (x_i - \bar{x})^2}{N-1}} \]  

where \( \sigma \) is the weight of the feature amount, \( x_i \) is the amount of the each device, \( \sum \) is the summation of features of each device for time period and \( S \) is calculated as the similarity checking range. The deviation is used to find the pattern of each feature amounts where its min value and max value is identified. These values are employed to frame the pattern for each device. The same method is used to calculate the patterns of other feature amount also. The characteristics patterns are framed for individual devices.
D) Applying the results

The final step in the process is storing the identified pattern in the database. The target device (database) uses to record the patterns of various characteristics of the devices. This approach is used to store the state of the devices in the database. In addition, it is used to record the change pattern in the database. This architecture also updates the device pattern database.

**Device Identification algorithm**

The proposed Device Identification algorithm is given below.

**Algorithm**

1. Input: signal(s) from the mobile device
2. Extract the features of a signal(s)
   AP x1, dist x2, metric x3, delay x4, os x5.
3. Calculate the pattern:
   Perform Individual weight calculation for (x2, x3, x4) as \( \sigma_{x2}, \sigma_{x3}, \sigma_{x4} \) respectively,
   \[
   \sigma = \sqrt{\frac{\sum_{i=1}^{N} (x_i - \bar{x})^2}{N - 1}}.
   \]
4. Generated patterns are stored in the database.
5. In case of new input: Repeat steps 2 and 3.
   5a. Similarity degree (S) is calculated:
   \[ S = \bar{x} \pm \sigma \]
   5b. Similarity range for 3 characteristics (x2, x3, x4) is verified.
6. If the input range is satisfied for (x2 && x3 && x4) then
   The “Device is identified”
   else
   “Store as new record in database”
   (note: x1 & x5 are not used for this calculation.)

**4. SIMULATION RESULTS**

This proposed approach is evaluated using simulation. Cooja Contiki OS simulator is used. It is tried to simulate the characteristics of mobile devices to identify a device. The degree of similarity is calculated to find the pattern in the database. Simulation was carried out with 10 mobile devices of same or different models and all have 5 features such as access point, communication distance from the access point, delay is calculated from the access point, amount of data transferred between the nodes to the access point and operating system. The datasets for 10 devices were generated as per the features extracted. Sample data set is available in Table 1. Sample Processed Dataset. Assuming the movement of mobile devices from the access point, the mobility plug-in was activated for the nodes or motes in the simulator.

The processed dataset is derived from the basic dataset of the simulator is available in Table 2.

On the basis of change in frequency we extracted the pattern of the devices for 1sec duration. The fig.2b and fig.2c depicts the sample output of device Id-6 generated using the simulator. The fig.2a represents simulation configuration of overall output for the various characteristics. However,
summation of the samples is used to calculate the pattern of a device for individual characteristics and stored in the database.

For any new device the pattern is generated and similarity in the pattern is verified using the stored patterns. The degree of similarity is calculated to identify the device. If it does not match with the stored patterns, it is likely to be stored in the database as another record (i.e., new record).

Table 1: Sample Processed Dataset

| Device Id | Distance (hop count) | Data amount (Kbyte) | Delay (ms) |
|-----------|----------------------|---------------------|------------|
| D1        | 0.84 - 1.01          | .10 to 81.9         | 58.28 to 379.72 |

Table 2: Sample Basic Dataset from the simulator

| feature | Time | AP | dist hps | ant metric | delay | os |
|---------|------|----|----------|------------|-------|----|
|         | 12.21| 1  | 0.22     | 122        | 0     | 7  |
|         | 12.22| 1  | 0.12     | 123        | 0     | 7  |
|         | 12.23| 2  | 0.06     | 124        | 0     | 7  |
|         | 12.24| 2  | 0.01     | 125        | 0     | 7  |
|         | 12.25| 2  | 0.12     | 126        | 0     | 7  |
|         | 12.26| 3  | 0.02     | 127        | 0     | 7  |
|         | 12.27| 3  | 0.04     | 128        | 0     | 7  |
|         | 12.28| 4  | 0.056    | 129        | 0     | 7  |
|         | 12.29| 4  | 0.08     | 130        | 0     | 7  |
|         | 12.3  | 5  | 0.054    | 131        | 0     | 7  |
|         | 12.3  | 5  | 0.054    | 132        | 0     | 7  |

Fig. 2a: Simulation Configuration
Fig. 2b: Sample Distance Calculation of Device Id -6

Fig. 2c: Sample Routing Metric of Device Id -6

Fig. 2d: Node Information using cooja simulator

The tables, 3a, 3b and 3c exhibit the distance table, Routing metric table and delay table respectively. The sample database derived from the characteristics is also given in the table 4.
The similarity checking is done with the input device values and if the values of all 3 features falls within the range of database record pattern, then the device id can be matched and recognized otherwise included as a new record in the database. In fig 3. The given input is matching with the Device Id-4 and hence it is identified.

Table 3a: Distance table

| Time/Device | d1  | d2  | d3  | d4  | d5  | d6  | d7  | d8  | d9  | d10 | Avg |
|-------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| 12.21       | 0.32| 0.35| 0.1 | 0.1 | 0.03| 0.03| 0.06| 0.06| 0.12| 0.12| 0.12|
| 12.22       | 0.12| 0.12| 0.32| 0.06| 0.05| 0.05| 0.03| 0.03| 0.21| 0.12| 0.11|
| 12.13       | 0.06| 0.32| 0.1 | 0.25| 0.16| 0.16| 0.05| 0.05| 0.13| 0.61| 0.15|
| 12.24       | 0.1 | 0.12| 0.1 | 0.3 | 0.03| 0.12| 0.175| 0.1 | 0.1 | 0.113|
| 12.25       | 0.03| 0.13| 0.5 | 0.06| 0.175| 0.175| 0.03| 0.03| 0.16| 0.06| 0.13|
| 12.26       | 0.12| 0.48| 0.44| 0.32| 0.2 | 0.2 | 0.2 | 0.12| 0.12| 0.12| 0.12|
| 12.27       | 0.02| 0.04| 0.06| 0.09| 0.1 | 0.1 | 0.885| 0.885| 0.14| 0.881|
| 12.28       | 0.04| 0.12| 0.12| 0.06| 0.06| 0.06| 0.06| 0.08| 0.885| 0.1 | 0.063|
| 12.29       | 0.06| 0.05| 0.27| 0.018| 0.018| 0.018| 0.05| 0.05| 0.09| 0.017| 0.069|
| 12.3        | 0.08| 0.52| 0.13| 0.08| 0.125| 0.125| 0.04| 0.04| 0.07| 0.06| 0.177|

Table 3b: Routing amount table

| Time/Device | e1  | e2  | e3  | e4  | e5  | e6  | e7  | e8  | e9  | e10 | e11 |
|-------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| 12.21       | 0   | 0   | 250 | 142 | 16  | 142 | 142 | 0   | 142 | 500 |
| 12.22       | 0   | 0   | 250 | 142 | 16  | 142 | 142 | 0   | 142 | 500 |
| 12.23       | 0   | 0   | 250 | 142 | 16  | 142 | 142 | 0   | 142 | 500 |
| 12.24       | 0   | 0   | 250 | 142 | 16  | 142 | 142 | 0   | 142 | 500 |
| 12.25       | 0   | 0   | 250 | 142 | 16  | 142 | 142 | 0   | 142 | 500 |
| 12.26       | 0   | 0   | 250 | 142 | 16  | 142 | 142 | 0   | 142 | 500 |
| 12.27       | 0   | 0   | 250 | 142 | 16  | 142 | 142 | 0   | 142 | 500 |
| 12.28       | 0   | 0   | 250 | 142 | 16  | 142 | 142 | 0   | 142 | 500 |
| 12.29       | 0   | 0   | 250 | 142 | 16  | 142 | 142 | 0   | 142 | 500 |
| 12.3        | 0   | 0   | 250 | 142 | 16  | 142 | 142 | 0   | 142 | 500 |

Table 3c: Delay table

| Time/Device | f1  | f2  | f3  | f4  | f5  | f6  | f7  | f8  | f9  | f10 | f11 |
|-------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| 12.21       | 20  | 10  | 250 | 142 | 16  | 142 | 142 | 0   | 142 | 500 |
| 12.22       | 20  | 10  | 250 | 142 | 16  | 142 | 142 | 0   | 142 | 500 |
| 12.23       | 20  | 10  | 250 | 142 | 16  | 142 | 142 | 0   | 142 | 500 |
| 12.24       | 20  | 10  | 250 | 142 | 16  | 142 | 142 | 0   | 142 | 500 |
| 12.25       | 20  | 10  | 250 | 142 | 16  | 142 | 142 | 0   | 142 | 500 |
| 12.26       | 20  | 10  | 250 | 142 | 16  | 142 | 142 | 0   | 142 | 500 |
| 12.27       | 20  | 10  | 250 | 142 | 16  | 142 | 142 | 0   | 142 | 500 |
| 12.28       | 20  | 10  | 250 | 142 | 16  | 142 | 142 | 0   | 142 | 500 |
| 12.29       | 20  | 10  | 250 | 142 | 16  | 142 | 142 | 0   | 142 | 500 |
| 12.3        | 20  | 10  | 250 | 142 | 16  | 142 | 142 | 0   | 142 | 500 |

Table 4: Sample stored Database

| Device ID | Dist (hops) | Amount (Kbyte) | Delay (ms) |
|-----------|-------------|----------------|------------|
| D1        | 0.01        | 0.18           | 1.25       |
| D2        | 2.04        | 5.88           | 26.12      |
| D3        | 4.16        | 8.95           | 44.06      |
| D4        | 6.25        | 9.03           | 39.56      |

Stored Database

The similarity checking is done with the input device values and if the values of all 3 features falls within the range of database record pattern, then the device id can be matched and recognized otherwise included as a new record in the database. In fig 3. The given input is matching with the Device Id-4 and hence it is identified.
5. CONCLUSION AND FUTURE WORK

The state and characteristics of various devices are used to differentiate the devices used in the IoT Environments. It is necessary to identify the appropriate device in order to secure the network. In case of diversity of the devices it is not easy to identify a device as they do not have a common addressing scheme. Hence it is important to identify a device within the network using its properties and characteristics. However it is still little complex due to the inconsistency of the devices employed. We analyze the issue by combining the portion of information that can be obtained from the device with a time change pattern for the signal characteristics extracted from the device. The model results that generated the patterns from the signal is stored in the database and every time when a device is encountered the degree of similarity will be calculated and checked with the recorded patterns in the Database. This comparison ends up in determining the devices based on its properties and characteristics. This study of Identification will in turn be likely helpful in device authentication.

A ample variety of devices were used in the IoT environments. In future this study can be extended to different type of devices and verify the effectiveness by employing it in the real environment.

6. REFERENCES

[1] Grønbæk, Inge. "Architecture for the Internet of Things (IoT): API and interconnect." Sensor Technologies and Applications, 2008. SENSORCOMM'08. Second International Conference on. IEEE, 2008.

[2] Chong, Gao, Ling Zhihao, and Yuan Yifeng. "The research and implement of smart home system based on internet of things." Electronics, Communications and Control (ICECC), 2011 International Conference on. IEEE, 2011.

[3] Chen, Ju, Yi Liu, and Yueting Chai. "An Identity Management Framework for Internet of Things." e-Business Engineering (ICEBE), 2015 IEEE 12th International Conference on. IEEE, 2015.

[4] Koo, Jahoon, and Young-Gab Kim. "Interoperability of device identification in heterogeneous IoT platforms." 2017 13th International Computer Engineering Conference (ICENCO). IEEE, 2017.

[5] Miettinen, Markus, et al. "IoT Sentinel: Automated device-type identification for security enforcement in IoT." Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on. IEEE, 2017.

[6] Noguchi, Hirofumi, et al. "Autonomous device identification architecture for Internet of Things." Internet of Things (WF-IoT), 2018 IEEE 4th World Forum on. IEEE, 2018.

[7] Hyun-seong, Lee, et al. "Design of Automatic Identification Gateway System for Different IoT Devices and Services." 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). IEEE, 2018.
[8] Darwish, Dina. "Improved Layered Architecture for Internet of Things." *International Journal of Computing Academic Research (IJCAR)* 4.4 (2015): 214-223.

[9] Baldini, Gianmarco, and Gary Steri. "A survey of techniques for the identification of mobile phones using the physical fingerprints of the built-in components." *IEEE Communications Surveys & Tutorials* 19.3 (2017): 1761-1789.

[10] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." *Computer networks* 54.15 (2010): 2787-2805.

[11] Vermesan, Ovidiu, et al. "Internet of things strategic research roadmap." *Internet of Things-Global Technological and Societal Trends* 1.2011 (2011): 9-52.

[12] Identifiers in Internet of Things 1 (IoT) 2 3 Version 1.0, February 2018 4 AIOTI WG03 – IoT Standardisation.

[13] Pb Agus Ristono*, "Design Of Reliable And Efficient Manchester Carry Chain Adder Based 8-Bit Alu For High Speed Applications", *Journal Of VLSI Circuits And Systems*, 1 (01), 1-4, 2019

[14] Sulyukova, "Analysis of Low power and reliable XOR-XNOR circuit for high Speed Applications", *Journal of VLSI Circuits And Systems* 1 (01), 23-26, 2019.