The deployment of an IoT zero configuration network using mDNS and DNS-SD

E Ali[1], A Diaa[1] and H Dahshan[1]

[1]Communication Department, Electrical Engineering, Military Technical College, Cairo, Egypt

E-mail: eslamsnono45@gmail.com

Abstract.

Growth of IoT networks is exponentially increasing. IoT is evolving as an integral part in both of our daily lives and the industry. IoT is highly pervasive in many applications today. Smart grids, smart retail, smart transportation, smart agriculture, and home automation are all examples of IoT applications. IoT devices are linked together to fulfil variuos needs for a user in an application.

IoT systems are multi-layered networks with layers for perception, network, data processing and application. The perception layer can interact with physical objects and entities in IoT network through nodes. Adding new nodes to the network should be easy for the user. In most of IoT systems, adding new nodes requires that user should conifgure both the node and the netwrok.

This paper proposes the architecture and methodology of an IoT network with zero configuration. Additional nodes merely need to be turned on in the IoT zero configuration netwrok; no configuration is needed to add new nodes. By using a node along with a WiFi transceiver, such a system can be made available as a service. The WiFi transceiver will benefit from mDNS and DNS-SD protocols to build IoT system with zero configuration network.

1. Introduction

The Internet of Things (IoT) is a technology that connects objects and things so that they can communicate with each other and provide an improved services to users while also making users' lives easier. Objects and things may consist of sensors, actuators, smartphones, and other devices.

IoT's rapid expansion generated other problems and difficulties that must be considered when creating an IoT applications. Since the Internet of Things (IoT) can connect any physical object, integration of the devices enter the scene of IoT. In order to integrate IoT, a unified architecture or middleware is required. Many models were proposed [1] for creating IoT architecture and many middleware were proposed [3, 4, 5] for implementing IoT on current Internet architecture.

The great connectivity that IoT can provide and the data flow from a group of sensors that can be processed then based on the data processing actions can be taken lead to raise the value of IoT. The IoT value was really seen in the pandemic of COVID. The market of IoT has been changed and exponentially increased breaking all the expectations. The Gartner report said that the connected devices in 2022 [6] was expected to be 20.4 billion connected devices.

The huge number of IoT devices made alot of researchers to design, build and troubleshoot the IoT networks to allow data flow, minimize latency, add nodes, revoke nodes and manage

IoT netwroks. The IoT network architecture compose of layers [7]. The basic three model is three layer [8, 9, 10] that consist of perception, network and application layers. Other models added more layers to be four or five layers. Figure 1 shows The three and five layers models.

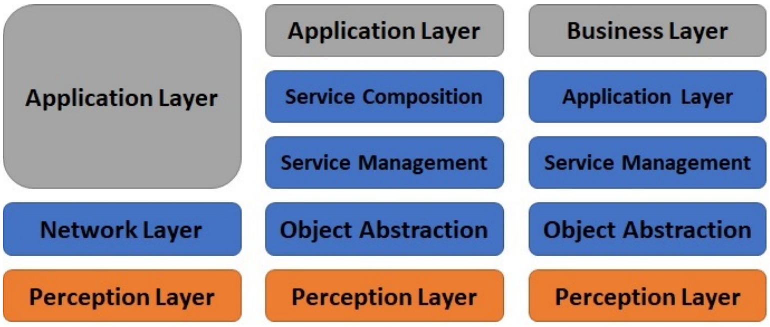

Figure 1.
IoT three and five layers models

In new IoT approaches, the IoT architecture is defined in tiers. The IoT is composed of three tiers (IoT devices - Fog and Edge computation - Cloud computation) [11, 12, 13]. Figure 2 shows the architecture of IoT netwrok corresponding to the three tiers. All models tries to handle the flow of the data from the IoT devices considering that the number of the devices is really large and increasing exponentially. In past IoT architecture, the devices send data to cloud [14].

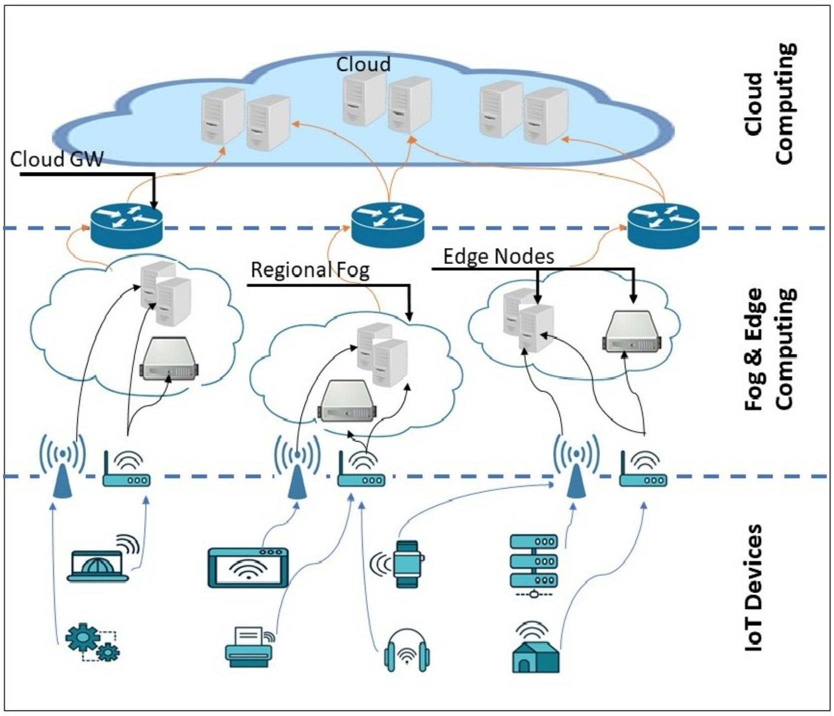

Figure 2.
IoT Tiers (Devices - Fog - Cloud)

The generated data exceeds 1 zettabyte in 2010 [16] and 2.5 exabytes of new data is generated each day since 2012 [17]. The IoT devices generate a massive amount of data. The networks architectures can't manage This massive data amount. This lead to the current model of edge then fog computing [18, 19]. In which, the data can be processed before uploading to cloud. In Fog computing all data is processed [15], then the reuired logs are sent to cloud. This allow the data to flow easily and decrease the problems to the network.

Fog nodes are located close to IoT devices [15]. The main benefit from being close to IoT devices is minimizing latency. Allowing, latency-sensitive applications to operate seamless.

The IoT devices provide many applications and services [6], Figure 3 shows the different fields of IoT applications.

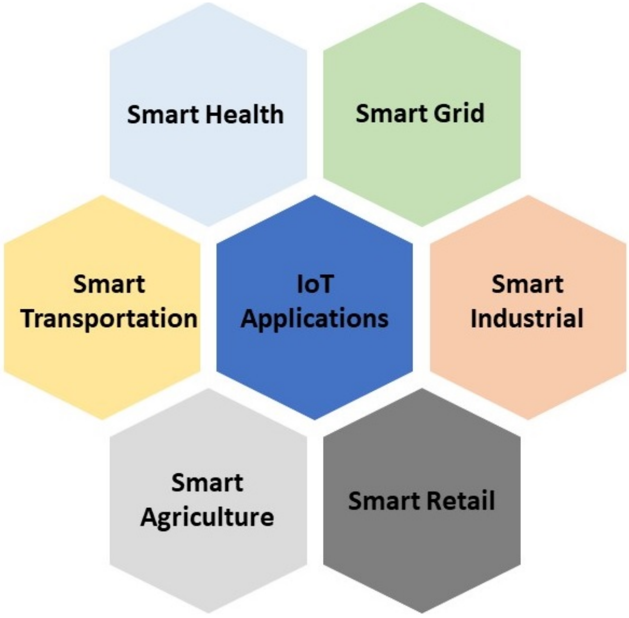

Figure 3.
IoT Applications

The diversity of IoT applications add more complexity to the networks, the edge and fog computing tries to simplify the operation of IoT devices (nodes) to communicate with the cloud and in turn provide the users with the required data. The edge and fog computing gateways need to identify the nodes function. IoT has different elements to compose IoT as in figure 4 [7]. The identification is the first element in IoT elements, adding a new node to an IoT network needs identifcation of the node service.

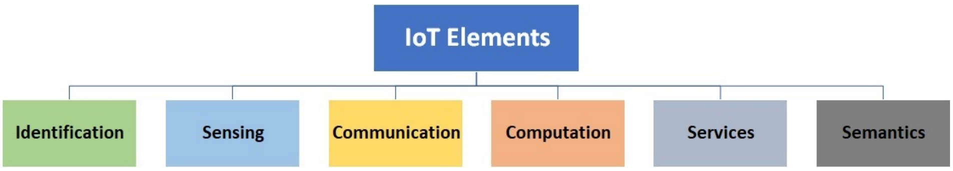

Figure 4.
IoT Elements

Identification is vital for adding new nodes to map the node's name and function to the correct provided service. Many identification models were proposed such as electronic product codes (EPC) and ubiquitous codes (uCode) [20]. In this paper, a new identification model is proposed using the known mDNS and DNS-SD protocols.

The DNS (unicast) is the phonebook of the internet that can map the domain names to ip address, and the mDNS also map the names to ip but locally inside LAN. The mDNS (multicast) is using a query-response mechanism. In IoT, When IoT device needs to connect to a gateway, it sends multicast query to all devices in the netwrok to get the hostname related IP. The targeted hostname response with its IP address and then all devices update their DNS cache with the IP of that hostname. The DNS-SD, it is a service discovery protocol that usuallu used in conjunction with mDNS. The DNS-SD is really suitable for IoT networks for different parameters the large number of IoT clients, non homogenous IoT devices and IoT devices are spread.

Identification process is the extraction of the node ID -The node ID may be something like ”H1” that means a humidity sensor- and address inside the communication netwrok. The proposed model tries to use the discovery protocols to force node identify itself to the gateway and by then it's the gateway role to add this node's ID and address and extract the data from it on demand. The discovery prtotocols process [23] allow the service clients -the gateways in the proposed model- to discover available provided services -the IoT devices in the proposed model- with the knowledge of the existance of any service is zero for the service client (Figure 5).

The proposed model eleminiate any user interaction for configuring and adding the new nodes and make adding new nodes to the network easier and safer.

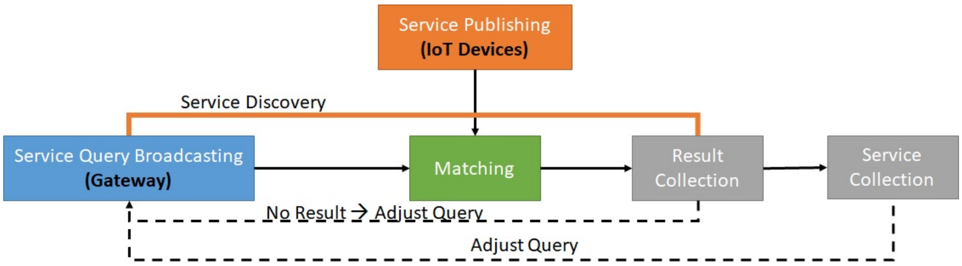

Figure 5. Service Discovery

The paper is organized as follows, section 2 describes the previous related work about adding new nodes in IoT network. Section 3 describes the proposed model and the usage of mDNS and DNS-SD protocols. Section 5 describes the conclusion of the proposed model and the advantages of it compared to the previous related models.

2. Realted Work

Identification isn't a new element or standard. Passing through all the IoT development, there was always a question about how to identify the nodes. In 2003, there was a successful attempt and as a result a nonprofit open forum called the Ubiquitous ID (uID) Center was built. Many companies and organizations particapted in it and publish uID standards [20]. uID architecture [20] consists of RFID tags, bar codes and IR beacons and there was also resolution servers that was assigning the uID to a service or application. Identification of ID comes from the tag and the service or application related to ID comes from the network. These standards is concerning about adding nodes to the network and mapping their ID to a service and fitting the past IoT networks architecture [14] where IoT devices were connected to cloud and computation was done in cloud.

The Present IoT networks architecture [14] have added edge and fog computing to the network. Most of the exisitng models for dynamic allocation of nodes is concerning with fog nodes and the fog resources [21]. Scaling the fog nodes was discussed to state the number of fog nodes related to the IoT workload [14]. Other models were concerning with how the IoT devices will query the fog nodes [21]. There were another model [23], in which, it offers a context based model using mDNS and DNS-SD to identify IoT devices for the client. The IoT device was acting as a client and server to fit this model. The model described in [24] has omitted the gateways and perform the case study for IoT devices identification to users through TCP/IP links.

The real examples of IoT systems also keeps the same conceptual of adding IoT devices, The administrator or the owner of the device has to configure the devices and define them to the network using diverse means liek QR codes, web pages and mobile applications [22].

The proposed scheme is concerning with identifying new IoT devices to the fog/edge nodes and identification means the type, service and the address of the device. The proposed scheme is using the same concept of zero configuration network where the protcols mDNS and DNS-SD are used.

3. Proposed Model

In this proposed model for identification of IoT devices, The mDNS and DNS-SD are used to ease the process of node identification. The proposed model considers the present IoT network (tiers) and the user can be connected to the IoT devices remotely or locally. So, the user can launch a request to read data from a sensor or to drive an actuator through cloud that passes the request to fog node (gateway) then finally to the targeted IoT device. The opposite is also possible, the gateway can get a consistent reading from added IoT devices and process the data, the critical data can be sent through cloud to the IoT users.

mDNS makes the IoT device act as a client and the gateway to act as a server. The IoT device try to query the the gateway with the top level domain (TLD). This query is a multicast which will allow all the devices to update their DNS cache about the new device and the gateway. The multicast wuery can be very useful for the future IoT where all the IoT devices and gateways will be connected [14].

The DNS-SD with mDNS makes the IoT device acts as a server and the gateway acts as a client. The gateway (client) query the service provider (IoT device) for the provided service. This is a text based where more data can be added as location and value of the data.

The proposed model consists of two phases:

- The first phase happens when the IoT device is turned on or rebooted. The IoT device send query to find the gateway that it will be associated to. It query for TLD ”GW.local”. This TLD shoukld be commisioned at phases before user-hand. The gateway should response to the query and the IoT device and all settled IoT devices update their DNS cache.
- The second phase happens when new IoT device is identified. The gateway get all the data from the IoT device like hostname, IP, service type, location. All these data can be sent as the DNS-SD is text based.

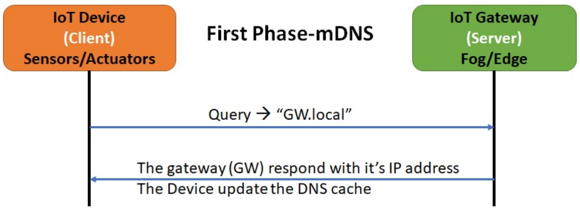

Figure 6. First phase: IoT device identify the gateway using mDNS.

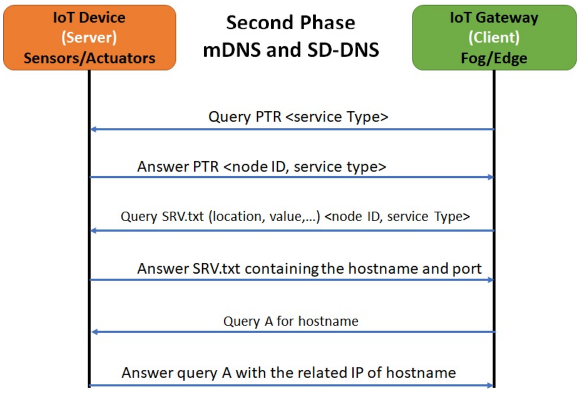
IoT Device
(Server)
Sensors/Actuators
Second Phase
mDNS and SD-DNS
IoT Gateway
(Client)
Fog/Edge
Query PTR <service Type>
Answer PTR <node ID, service type>
Query SRV.txt (location, value,...) <node ID, service Type>
Answer SRV.txt containing the hostname and port
Query A for hostname
Answer query A with the related IP of hostname

Figure 7. Second phase: Gateway discover services using DNS-SD with mDNS.

The IoT user can now dump or drive data from or to the IoT devices. This can be done as all the computation is done through the gateway and now the gateway has all the information about the associated IoT devices (ID - location - service type - ....).

4. Evaluation

The proposed model tries to figure out all drawbacks of previous mDNS and DNS-SD based IoT schemes. Stolikj Milosh, et al [24] had used also mDNS and DNS-SD to simplify the IoT netwrok procees when adding new devies, but they use a one way traffic approach. The approach optimization was putting the IoT device in a passive mode and it publishes its service periodically. In the proposed scheme, we figured that out. When ever a new IoT device tries to login and register to the network, then it acts as a client and query the gateway (acts as a server) and identify the gateway with its services. When ever the gateway needs to get or set any data from/to the IoT device, then it acts as a client and query the IoT device (acts as a server). The proposed scheme is two way traffic but not periodically, it is only when registering IoT device or get/set data from/to IoT device.

Stolikj Milosh, et al [23] scheme use the mDNS and DNS-SD to allow clients to discover the services based on location and sub-protocols. The scheme allow the clients to identify and locate the IoT devices and the services. This sure is done in local networks (LAN), the mDNS and DNS-SD is used and works in LAN only. The proposed scheme considers that the client may be remotely and need to use the IoT device, The client can communicate to the gateway through cloud and use the IoT devices. The gateway has all the information of IoT devices and know the provided services and even in our scheme, the location can be added to the context easily.

Koshizuka, et al [20] scheme depends on uID and use that uID to contact other resilution server or information servers to know the service and all the information. In the proposed scheme, no need to contact a resolution server or even no need to send the data of IoT device to information servers, the IoT device can publish its identity and services when ever it is turned on.

The mDNS and DNS-SD is considered a great protocls that can ease the process of IoT network. The paper also proposed the scheme trying to enhance the existing schemes of these protocols in IoT.

5. Conclusion

The proposed model has offered some advantages over the other models. The mDNS used in [23] was only allowing client to identify the existing IoT devices. That approach isn't considering that client may need to use the IoT network remotely. Other models were concerning with the fog nodes and how to alocate their resources and how to expand and they abandon the IoT devices management althoug, the IoT devices are really large number and they are constarined devices, that need more care to save the limited resources.

In the proposed model, The IoT present architecture is taken into consideration allowing the client to use the IoT devices from any location. Also, the first step in the model that identify the IoT device to the gateway, unintenionally update all the IoT devices DNS cache whcih can be very useful to the future IoT where all IoT devices are connected. The second phase is providing a service discovery text based in which the values can be returned when the device is queried and in turn the communication cost is minimized as there will no be more packets to get the value and in turn it will be less power consumption. The proposed model was designed to consider the present and future architecture of IoT and the fact that these IoT devices are constrained and have limit resources.

The paper proposed model that fit the first element in IoT which is identification. The used protocls doesn't offer any authentication or integrity. The next steps are adding authentication and integrity to the IoT devices when added to IoT network -considering that these devices are limited resources in processing, storage and power- and evaluating the performance of the network. The light weight cryptography will be one of the solution to overcome the limited resources of the IoT devices.

References

[1] Zhu Q, Wang R, Chen Q, Liu Y, Qin W 2010 Iot gateway: Bridgingwireless sensor networks into internet of things. *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing* pp 347–352.

[2] Fan C, Wen Z, Wang F, and Wu Y 2011 A Middleware of Internet of things based on Zigbee and RFID. *In IET international conference on Communication Technology and Application* (ICCTA) pp 732–736.

[3] Castellani A, Loreto S, Bui N and Zorzi M 2011 Quickly interoperable Internet of Things using simple transparent gateways *In Position paper in interconnecting smart objects with the internet workshop* pp 1–2.

[4] Chi Q, Yan H, Zhang C, Pang Z and Xu L 2014 A reconfigurable smart sensor interface for industrial WSN in IoT environment. *IEEE Transactions on Industrial Informatics* pp 1417–1425.

[5] Valdivieso A, Peral A, Barona L and Garcia Villalba 2014 SDN—Evolution and opportunities in development of IoT application. *International Journal of Distributed Sensor Networks*

[6] Sobin CC 2020 A survey on architecture, protocols and challenges in IoT. *Wireless Personal Communications* v.112(3) pp 1383–429.

[7] AlFuqaha A, Guizani M, Mohammadi M, Aledhari M and Ayyash M 2015 Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys and tutorials* pp 2347–2376.

[8] Khan R, Khan SU, Zaheer R, Khan S 2012 Future internet: the internet of things architecture, possible applications and key challenges. *In2012 10th international conference on frontiers of information technology* pp 257–260.

[9] Yang Z, Yue Y, Yang Y, Peng Y, Wang X, Liu W. Study and application on the architecture and key technologies for IOT. *In2011 International Conference on Multimedia Technology* pp 747–751).

[10] Wu M, Lu TJ, Ling FY, Sun J, Du HY 2010 Research on the architecture of Internet of Things. *In2010 3rd international conference on advanced computer theory and engineering* (ICACTE) pp V5-484.

[11] Yuriyama M, Kushida T 2010 Sensor-cloud infrastructure-physical sensor management with virtualized sensors on cloud computing. *Proceedings of the 13th International Conference on Network-Based Information Systems* (NBiS) pp 1–8

[12] Li W, Santos I, Delicato FC, Pires PF, Pirmez L, Wei W, Song H, Zomaya A, Khan S 2017 System modelling and performance evaluation of a three-tier cloud of things. *Future Gen Comput Syst* pp 104–125

[13] El Kafhali S, Salah K 2017 Efficient and dynamic scaling of fog nodes for IoT devices. *The Journal of Supercomputing* 2017 pp 5261–5284.

[14] Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B. 2019 A survey on IoT security: application areas, security threats, and solution architectures. *IEEE Access* pp 82721–82743.

[15] Yousefpour A, Fung C, Nguyen T, Kadiyala K, Jalali F, Niakanlahiji A, Kong J, Jue JP 2019 All one needs to know about fog computing and related edge computing paradigms: A complete survey. *Journal of Systems Architecture.* pp 289–330.

[16] Gantz J, Reinsel D.2011 Extracting value from chaos. *IDC iview.* pp 1–12.

[17] McAfee A, Brynjolfsson E, Davenport TH, Patil DJ, Barton D. 2012 Big data: the management revolution. *Harvard business review.* pp 60–68.

[18] Bonomi F, Milito R, Zhu J, Addepalli S. 2012 Fog computing and its role in the internet of things. *The first edition of the MCC workshop on Mobile cloud computing* pp 13–16.

[19] Garcia Lopez P, Montresor A, Epema D, Datta A, Higashino T, Iamnitchi A, Barcellos M, Felber P, Riviere E. 2015 Edge-centric computing: Vision and challenges. *ACM SIGCOMM Computer Communication Review.* pp 37–42.

[20] Koshizuka N, Sakamura K. 2010 Ubiquitous ID: standards for ubiquitous computing and the internet of things. *IEEE Pervasive Computing.* pp 98–101.

[21] Pinto D, Dias JP, Ferreira HS. 2018 Dynamic allocation of serverless functions in IoT environments. *IEEE 16th international conference on embedded and ubiquitous computing* pp 1–8).

[22] Gill SS, Garraghan P, Buyya R.2019 ROUTER: Fog enabled cloud based intelligent resource management approach for smart home IoT devices. *Journal of Systems and Software.* pp 125–138.

[23] Stolikj M, Cuijpers PJ, Lukkien JJ, Buchina N. 2016 Context based service discovery in unmanaged networks using mDNS/DNS-SD. *IEEE international conference on consumer electronics* pp 163–165.

[24] Klauck R, Kirsche M. 2012 Bonjour contiki: A case study of a DNS-based discovery service for the internet of things. *Ad-hoc, Mobile, and Wireless Networks: 11th International Conference, ADHOC-NOW 2012* pp 316–329.