



Bluetooth 5 and Docker Container: Together We Can Move a Step Forward Towards IOT

Mohammad Equebal Hussain¹(✉) and Rashid Hussain²

¹ Computer Science and Engineering, Suresh Gyan Vihar University, Mahal, Jagatpura, Jaipur 302025, Rajasthan, India

mdequebal.60508@mygyanvihar.com

² Department of Computer Science and Engineering, Suresh Gyan Vihar University, Mahal, Jagatpura, Jaipur 302025, Rajasthan, India

rashid.hussain@mygyanvihar.com

Abstract. Virtual wireless sensor network (WSN) is an approach towards automated monitoring system with minimum cost and maximum throughput. vWSN is an approach to convert physical WSN [1] into virtual device using VM and docker container combined with Bluetooth 5, this designed can be further transformed into on demand IOT device that is efficient, secure and real time device used for monitoring system. In this manuscript we will propose the end to end design to achieve the desired result having lot of advantages. This model can be deployed on the cloud. We will also discuss the security aspect of vWSN.

Keywords: Internet of Things (IoT) · Bluetooth 5 · Docker container · Security · Virtual wireless sensor network (vWSN) · Virtual machine (VM)

1 Introduction

Recent transformation from physical server to virtual machine to docker container. The former has many advantages over its predecessor. Standalone server was expensive, running at low potentials therefore wastage of resource, Later the virtual machine (VM) came into picture which allows multiple applications to run concurrently on single server. Going forward VM's are also not perfect because every VM requires dedicated OS. Every OS consumes memory, storage, CPU as well as license, continuous upgrade and monitoring. This model has other challenges like slow boot, portability to cloud etc. Docker container share single OS therefore it is fast, portable, elastic and cost effective. Docker enables separating application from infrastructure which helps shipping, testing and deploying much quicker and faster. Bluetooth 5 with docker can be used to design an efficient, portable, low power consumable device called virtual WSN.

2 Background

Docker container is not a replacement of VM but analogous to it. VM and container are not mutually exclusive. Both can exist together. The major difference is that container

doesn't need full OS. Containers are based on linux kernel namespace, control groups (cgroup) and Docker. Major components of docker are server (daemon), REST API and CLI (client). Docker registry is used to store docker images. Running instance of docker image is called container.

Bluetooth is a technology for short distance wireless communication. It doesn't depend on IP or internet. Data exchange is done instantly between any Bluetooth enable devices [2] over a short distance ranging from 10 to 100 m. Bluetooth 5 is latest version released in 2016 after V4.x, V5.0 has many improvements like performance and functionality, privacy and security, less power consumption (BLE – Bluetooth Low Energy), double speed (48 Mbit/s) and 4 times distance range (300 m) as well as support for IoT.

IoT (Internet of Things) refers to scenario [8] where connectivity and computing extends to sensors and other items normally not considered as computer, allowing generating, exchange and consuming data with minimal or no human intervention. Each object is provided a unique id (UID), IP address in order to transfer data over internet. IoT devices share collected data to an IoT gateway in order to send it to cloud or local server for further processing. Addressing new and unique security challenge [15] is also a priority.

3 Related Work

Many research works has been proposed in the area of WSN but few of them discuss about end to end design using virtual WSN. Sensor nodes collect data and transfer it to other node using internet or mobile network. The critical aspect is the network lifetime due to power consumption either by battery or any other source [5]. In this paper we propose an efficient method by separating control plane and data plane using virtual device. Theoretical analysis is presented in this approach. The authors in [6] proposed wireless sensor network coverage problem. Authors in [7] proposed energy efficient data routing communication protocol to maximize the energy and lifetime of sensor nodes.

4 Problem Formulation

Virtual wireless sensor network (vWSN) is fairly new concept taking the advantage of Bluetooth and dockernization to propose an IoT device. The design proposed in this manuscript is not just specific to any single application but equally applicable for monitoring and recording physical conditions of environment, weather, temperature, sound, pollutions, insects monitoring [3, 18], health monitoring [4], cyber security etc.

In this paper we propose a method for virtual WSN based on Bluetooth for communication, docker container for data processing using Internet of Things (IoT) technique [14].

We will also discuss about Bluetooth-5, major protocol change from its predecessor version 4.x and its advantages, about IoT and Docker container.

4.1 About Bluetooth 5

Bluetooth 5 is a short-range wireless communication technology for data transmission up to 2 Mbps using radio waves between two or more devices. It is developed specially to support IoT use case scenario [9]. Any file type such as photo, videos, documents, music or real time data can be transmitted over a short distance ranging from 10 to 100 m. Bluetooth technology is expanding to support IoT and machine to machine (M2M) communication [10] using Bluetooth Low Energy (BLE) which consumes less power [8]. This technology is used in many IoT applications like smart home automation and a traffic monitoring system.

Any Bluetooth device consist either an inbuilt adaptor or external card connected to device. Communications between devices are done using pre-defined embedded instructions. When devices come in each other's radio range, the Link Management Protocol (LMP) performs link setup, negotiation of packet size, segmentation and reassembling. The Service Delivery Protocol (SDP) enables devices to join network. Each device has a unique global ID which is exchanged between the devices to setup the connection. Bluetooth 5 uses mesh topology to communicate between devices within the network (Fig. 1).

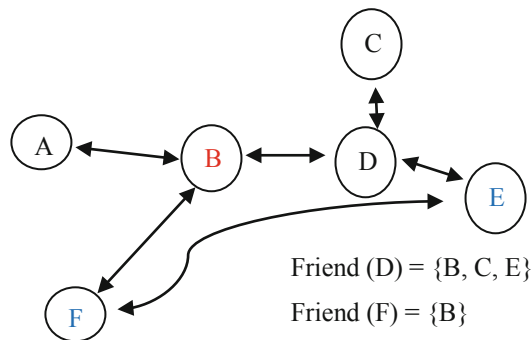


Fig. 1. Mesh network [11]

Suppose Node-F intend to send message to E, then F will send message (destination: E) to its entire neighbor i.e. node-B. Since B is not the destination hence it will re-broadcast the message to its entire neighboring i.e. node-A and node-D. A will discard the message, but node-D will forward the message to Node-E because D is a friend node of E.

4.2 Application of Bluetooth 5

Following are the major application of Bluetooth technology.

- a. peripheral devices keyboard, mouse, printer
- b. Healthcare and medical, motion detection
- c. Internet of Things (IoT) wireless sensors etc.

Advantages:

- a. Multiple devices can communicate to each other.
- b. Location based service
- c. More data transfer in short duration due to high speed
- d. Bluetooth 5 uses FEC (Forward Error Correction) technique to recover the data by receiver in case an error occurs during transmission [12].

5 Proposed System Architecture and Design

Major components:

- (i) Docker Engine – it consists of pre-configured pool of agents. Each agent represents one IoT device. It handles connection of device with agent. Agent talks to device collect data and pass it to other component for further processing [13].
- (ii) Record Parser -This is required to parse various fields of records generated by the device in order to store in database.
- (iii) In memory database. Redis will be used.
- (iv) HDFS uploader - its role is to upload parsed file to HDFS database.
- (v) Socket connection – TCP//IP wherever required.

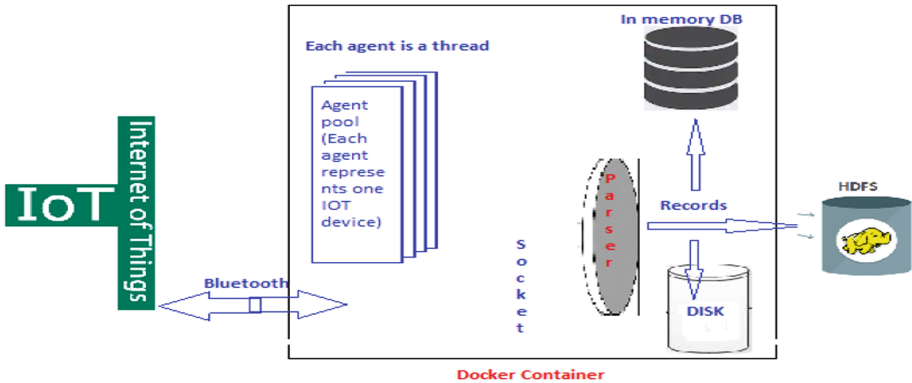


Fig. 2. Different components of proposed design

Docker container is the core backend component which collects data from IoT devices. It handles.

- Registration and De-registration.
- Filtering and distribution of work for parsing.
- Store records into in memory database.
- Define thread (Management thread, worker thread, Filter thread)

- Use RADIUS for authorization and authentication purpose wherever needed in order to assure security. RADIUS server is usually run as daemon process and communicates over UDP protocol.
- RADIUS server supports a variety of methods to authenticate a user.
- Response from server is Accept, Reject or Challenge.

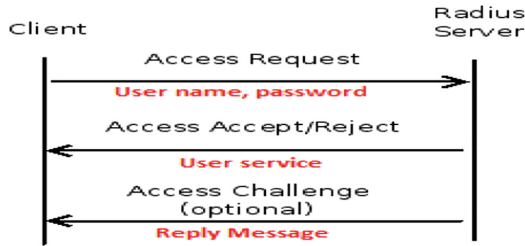


Fig. 3. Basic Authentication mechanism using RADIUS protocol.

5.1 vWSN as Virtual Machine vs. VWSN as Docker Container

Each VM has its own operating system whereas docker container focuses on deployment of application inside container, which can be packed and run as a single service. Single docker layer is shared among all containers within the same host. Authors in [16] proposed security implementation for this model (Fig. 4).

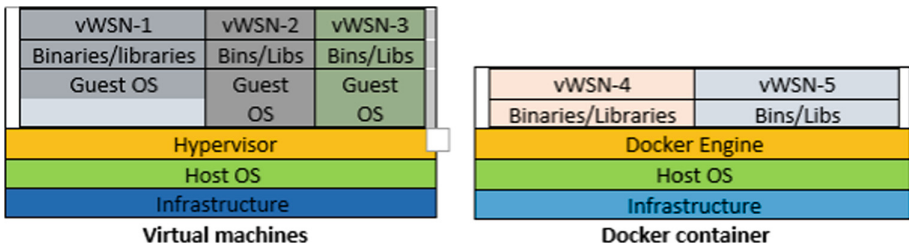


Fig. 4. VM vs. Docker container. <https://www.taksatech.com/containers-vs-vm/>

5.2 Docker Software Architecture

Docker underlying technology use Linux kernel to deliver its functionality Docker is based on namespace to provide isolation layers among container running in same host. Docker engine also relies on cgroups. This helps allocate resource like memory, CPU to a specific container (Fig. 5).

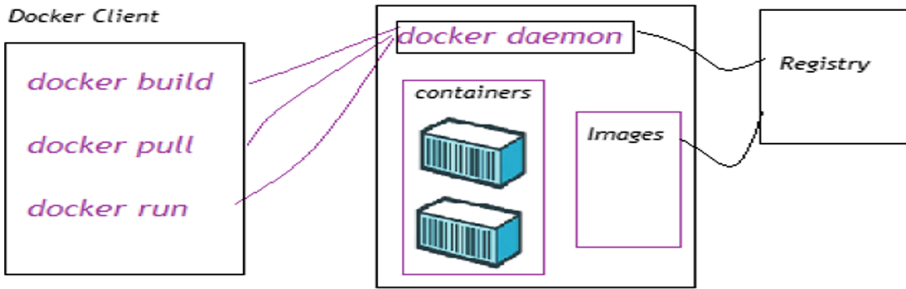


Fig. 5. Docker architecture. <https://www.taksatech.com/containers-vs-vms/>

Docker client is used to interact with docker daemon using various commands like docker build, docker run etc.

Docker daemon manages docker objects like containers, images, network and storage. It also listens to client request as shown in the above diagram.

Docker registry stores images. Docker pull, docker run and docker push commands are used to pull and push the images from docker hub registry.

Docker image is read only file consists of set of instructions to create a container. Dockerfile is used to create own docker image. Each instruction in Dockerfile creates a layer in image.

Docker is developed on the concept of namespace. Resources are visible only to those processes which run on the same namespace. Process running in one namespace can't see process running on another namespace. This provides a kind of virtualization and isolation of resource. Each container runs in its own namespace. This support is provided by the kernel which knows about the namespace and during API call; kernel makes sure that process can only access resource of its own namespace [13].

Docker hub is on the cloud registry service used to host various docker images built by other communities. We can also upload our own docker built images to docker hub.

Docker compose is used to define application using multiple container. Docker engine is used for building docker images.

Download and run docker image using below command.

```
$> docker run -it <image> /bin/bash
```

Displaying docker images.

```
$> docker images
```

```
REPOSITORY TAG IMAGE ID CREATED SIZE
virtual-wsn mhussain-1.0 b85ae2d81253 2 s 40 MB
```

To remove docker image.

```
$> docker rmi < image ID>
```

5.3 Building vWSN Image from Dockerfile

Dockerfile is a text file having series of instruction to build image. Some of the important commands are FROM, RUN, COPY, ADD, CMD, ENTRYPOINT, WORKDIR, USER, VOLUME etc. Start/stop/create/delete/move is some of the CLI command.

Dockerfile

```
FROM ubuntu: 1.0.18b1
MAINTAINER Mohammad Equebal Hussain
RUN apt-get update \
    && apt-get install -y vwsn \
    && apt-get clean \
    && rm -rf /var/lib/apt/lists/* /tmp/* /var/tmp/* \
    && echo "daemon off;" >> /etc/vwsn/wsn.conf
ADD default /etc/vwsn/sites-available/default EXPOSE 8080
CMD ["vwsn"]
```

Docker Build

```
docker build -t appliance/vwsn:1.0 -t appliance/vwsn: latest
```

Docker Push

```
Docker push appliance/vwsn: latest.
```

6 vWSN as Internet of Things (IOT)

IoT platform [17] helps to connect hardware, handle different communication protocols, Collect, visualize, and analyze data, provide security and authentication for users and devices as well as Integrate with other web services. IoT is a broad field and includes variety of applications. Many sensors/devices will collect data, Bluetooth as a connectivity technology that enables those sensors and devices to pass data to the backend (either docker application running locally or on the cloud). Activities like storage and data processing take place separately rather than on device, because large amount of computational power is extremely expensive and energy intensive therefore data from all the sensors and devices can be passed to the backend docker application running on the cloud is important for aggregating, processing and make intelligent decision. This gives high scalability. One of the biggest advantages of IoT platform is time to market.

One of the crucial parts is overall user experience which could be achieved using alerts and notification. When user get alert, how to get alert and what happens if alert is received but user doesn't react within the time frame.

There are some concerns need to be addressed while using cloud service. For example, Data ownership (actual owner vs. cloud provider), Latency (in IoT application, time is critical for taking decision) and potential crash (if connection broken then IoT application won't work).

6.1 IOT Elements

IOT provides many facilities and benefits to the user. In order to deliver functionality of IOT following elements are required [9].

Identify \Rightarrow Sense \Rightarrow Communication \Rightarrow Compute Services \Rightarrow Semantics

Identification refers to name and unique address (Ipv6).

Sensing refers to collecting information using sensing device such as RFID, smart sensor, actuators, wearable devices etc.

Communication refers to send and receive messages, files and other information using Bluetooth [10], Wi-Fi [8] and Long-Term Evolution (LTE) [11].

Computation refers to removing unnecessary information and keep useful information for further processing.

Services refers to making appropriate decision from collected and processed information on time every time.

Semantics is one of the most important elements of IoT which refers to getting all information and making appropriate decision to send response back to the device.

IOT is a 3-layer architecture consisting of perception or sensor layer (Lowest), Network or transmission Layer (Middle) and Application layer (Top).

6.2 Security Issue in Decernized IoT Solution

RFID: Radio Frequency Identification has three parts. Tags, reader and database. Encrypted information is transmitted between devices either using Data encryption (DES -symmetric key, 56 bit) or Advance encryption (AES-128 bit).

Reading information from tags is not secure because it gives information without authenticating the readers.

vWSN: Wireless Sensor Network consists sensors, microcontrollers and virtual memory. vWSN architecture consists physical layer, link, network, transport and application layer. Most common attacks on WSN is Denial of Service (DOS), man in the middle and DDOS attack [12].

Without proper security mechanism, IoT application is not useful. Existing securities are hash based encryption, Identity management framework, Intrusion detection system, Access control mechanism (ACL). Each device in IoT network need unique ID in order to communicate to each other. Therefore, support of such large number of devices is a big challenge. Other challenge is the huge data getting generated by these IoT devices over a period. In order to communicate and connect, dependency of device on other IoT device is also a challenge. There are many reasons to cause securities issues.

To overcome security issues, authentication (To verify user's identity using credentials) and ACL are used.

7 Conclusion

Internet of Things (IoT) is an emerging idea to quickly find the path to enhance the quality of modern life by connecting various smart devices. IoT allows to automate everything around us to make life easier, better and secure. This paper presents proposed design of vWSN as an IoT device using Bluetooth connectivity, Docker containers, possible security threat and their solution along with, their feature and limitations. This work can be further extended to propose secure docker containers to solve major security issues like malicious images in docker registry hub, denial of service attacks using access control list (ACL) and data loss prevention (DLP) solution.

Acknowledgements. I would like to thank Dr. Rashid Hussain for his encouragement and support during the research.

References

1. Venkatasubramanian, K., Deng, G., Mukherjee, T.: Ayushman: a wireless sensor network based health monitoring infrastructure and testbed distributed computing in sensor systems. In: Prasanna, V.K., Iyengar, S.S., Spirakis, P.G., Welsh, M. (eds.) DCSS 2005. Lecture Notes in Computer Science, vol. 3560, pp. 406–407. Springer, Heidelberg (2005). https://doi.org/10.1007/11502593_39
2. Ng, H.S., Sim, M.L., Tan, C.M., Wong, C.C.: Wireless technologies for telemedicine. *BT Technol. J.* **24**(2), 130–137 (2006)
3. Soni, K., Hussain, R.: WSN based insect monitoring: pest detection through MATLAB-artificial neural network, vol. 5, no. 1. ISSN 2278-1315
4. Yuce, M.R., Ng, P.C., Khan, J.Y.: Monitoring of physiological parameters from multiple patients using wireless sensor network. *J. Med. Syst.* **32**, 433–441 (2008). <https://doi.org/10.1007/s10916-008-9149-5>
5. Cardei, M., Du, D.: Improving wireless sensor network lifetime through power aware organization. *Wirel. Netw.* **11**, 333–340 (2005). <https://doi.org/10.1007/s11276-005-6615-6>
6. Huang, C., Tseng, Y.: The coverage problem in a wireless sensor network. *Mob. Netw. Appl.* **10**, 519–528 (2005). <https://doi.org/10.1007/s11036-005-1564-y>
7. Kumar, R., Kumar, D.: Multi-objective fractional artificial bee colony algorithm to energy aware routing protocol in wireless sensor network. *Wirel. Netw.* **22**, 1461–1474 (2016). <https://doi.org/10.1007/s11276-015-1039-4>
8. Abbas, Z., Yoon, W.: A survey on energy conserving mechanisms for the internet of things: wireless networking aspects. *Sensors* **15**(10), 24818 (2015)
9. Chang, K.H.: Bluetooth: a viable solution for iot? [industry perspectives]. *IEEE Wirel. Commun.* **21**(6), 6–7 (2014)
10. Gazis, V.: A survey of standards for machine to machine (m2m) and the internet of things (IoT). *IEEE Commun. Surv. Tutor.* **PP**(99), 1 (2016)
11. <https://electricalfundablog.com/wp-content/uploads/2019/01/Bluetooth-topology.png>
12. Nafaa, A., Taleb, T., Murphy, L.: Forward error correction strategies for media streaming over wireless networks. *IEEE Commun. Mag.* **46**(1), 72–79 (2008)
13. Martin, J.P., Kandasamy, A., Chandrasekaran, K.: Exploring the support for high performance applications in the container runtime environment. *Hum.-Cent. Comput. Inf. Sci.* **8**, Article number: 1 (2018)

14. Ruchika, V.: Evaluation of Docker for IoT application. *Int. J. Recent Innov. Trends Comput. Commun.* **4**(6) 624–628 (2016)
15. Singh, V., Pandey, S.K.: Cloud computing: vulnerability and threat indications. In: Pant, M., Sharma, T.K., Basterrech, S., Banerjee, C. (eds.) *Performance Management of Integrated Systems and its Applications in Software Engineering*. AA, pp. 11–20. Springer, Singapore (2020). https://doi.org/10.1007/978-981-13-8253-6_2
16. Mukherjee, T., Sahana, S., Sarddar, D.: A noble approach toward security implementation in cloud virtualization framework. In: Kundu, S., Acharya, U.S., De, C.K., Mukherjee, S. (eds.) *Proceedings of the 2nd International Conference on Communication, Devices and Computing*. LNEE, vol. 602, pp. 541–552. Springer, Singapore (2020). https://doi.org/10.1007/978-981-15-0829-5_52
17. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of Things (IoT): a vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* (2013). <https://doi.org/10.1016/j.future.2013.01.010>
18. Jha, T., Hussain, R.: WSN controlled insects monitoring: identification of onion thrips. *IJCAR* **6**, 5257–5260 (2014)