Materials Today: Proceedings xxx (xxxx) xxx

Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

Designing of internet of things for real time system

Majd S. Ahmed

Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, Iraq

ARTICLE INFO

Article history:
Received 9 March 2021
Accepted 18 March 2021
Available online xxxx

Keywords:
Internet of things
IOT
Real-time systems
Recent time Internet of things
Attacks and threats
Platform
Nodes

ABSTRACT

The internet of things is the key for converting any system to be intelligent. Recent operating systems are used to meet the requirements of the modern systems. There are a lot of platforms for Internet of things which have been developed. However, most of them are made for certain implementations and don't manage the current limitations of the recent systems.

In our research, we will discuss a general overview of Internet of things, the mechanism of operation, the limitation of resources, properties of Internet of things nodes and mixed traffic communications. Also, we will discuss recent technologies which use a platform for Internet of things used in many applications.

Current advances demand recent time devices to be linked with the internet, which develops the recent time Internet of things, and which creates better experience of users through strong connection and effective usage of the devices of the upcoming generation. But, recent time Internet of things became aim for the attacks, that is worsened by that enhanced connectivity. We will discuss the common attacks and threats to security of Recent time Internet of things and approaches for protection from these attacks.

I suggested implementing a platform of Internet of things including the nodes, server, protocol of communications. Also, I did an experiment and drew conclusions and recommendations from the results.

Selection and peer-review under responsibility of the scientific committee of the Emerging Trends in Materials Science, Technology and Engineering.

1. Introduction

Internet of things is growing rapidly and significantly sharing in improving the life quality. Huge modern inventions and development is the key agent in advancements of Internet of things. The easily available hardware of low costs is mandatory for unceasing adaptation of that system. Developing the operating systems of Internet of things for supporting those recently developed hardware in parallel with the current techniques and standards for all layers of communication are the path ahead [1].

The availability of various operating systems of Internet of things requires supporting inter-operability which needs following certain rules for advancement and functional capacities for supporting heterogeneous scenarios of deployment. Internet of things demands being smart to adapt itself in accordance to the conditions of network. In that research, we will present an overview of various operating systems of Internet of things, enhanced hardware, and future directions for research. Through which we will discuss the validated papers on our issue about management of operating systems of Internet of things: the chances, obstacles, and the possible solutions. Eventually, we will review our conclusions and recommendations.

Internet of things is the key driving factor behind transforming all technology aspects. The unified technologies integration is the challenge. Current developments in the 'Millimeter wave', modern cellular networks, 5th generation spectrum of the smart Internet of things, existence of wireless systems, communicating device to device, resources of Internet of things, and its operating systems, etc. Research smooths the way for developing the upcoming generation of Internet of things. The advancing in technologies of Internet of things and their availability by low costs flourish the distance accessibility and connectivity of devices [1].

Therefore, following the standards is crucial for allowing the communication between those various networks in Internet of things. Connection of industrial components by using distributed or central manners for increasing the efficiency and productivity is essential for manufacturing Internet of things. The 4th revolution of industry is still developing. It creates large challenges for autonomous and intelligent system which produces enormous amounts of information to be handled and so requires to be smart by accepting machine algorithms for learning.

E-mail address: majdsami@uomustansiriyah.edu.iq

https://doi.org/10.1016/j.matpr.2021.03.527
2214-7853/
Selection and peer-review under responsibility of the scientific committee of the Emerging Trends in Materials Science, Technology and Engineering.

1.1. Mechanism of operation and characteristics

The device of Internet of things aims to connect to other devices for exchange of information. The platforms of Internet of things connect the sensors to the networks, and it makes the developers capable of making and deploying Internet of things. Various research types were done for serving the applications of Internet of things taking into consideration the platforms and the publications concerned on the comparison between the various protocols of communication of Internet of things as 'Message Queue Telemetry Transport' and the other many protocols [2], 49.

There was a comparison which was made between 4 protocols by using some files from readings of the sensors without the platforms of Internet of things, they investigated for the amount and the parameters delayed.

A lot of these platforms were applied by the researchers for certain implementations, and they utilized the made protocol of 'Message Queue Telemetry Transport' and the embedded ready-made kits of hardware. For instance, the researchers did the medical and healthcare implementations, they didn't utilize an operating systems of Internet of things in their platforms which were previously made. A general platform is given by using portable processors and a non-recent operating system [2], 53.

Internet of things of recent time intersects largely with the recent cyber and physical systems. Recent systems of Internet of things could be recognized as a widely innterconnected network, where the nodes could be remotely controlled and connected. We aim to focus on the elements of recent time Internet of things and the topic of issues of security.

Allowing security in recent time Internet of things is usually harder than general systems of Internet of things because of the additional current limitations. Our concern is to present the properties, limitations and threats to security for recent time Internet of things, summarize solutions for security especially designated for these critical issues of safety. There are some surveys made on issues of privacy and protection in general systems of Internet of things, there is no comprehensive discussion made about security recent time Internet of things [3], 131.

The Fig. 1 shows an overview of daily recent time Internet of things. The blue lines refer to the wireless connection made by those devices. Each device of Internet of things implement periodic certain tasks needed for the secured operation of the system.

1.2. Requirements of safety and limitation of resources

Many devices of recent time Internet of things, as for example: sensors, controllers, autonomic vehicles, automatic flying vehicles, etc. have very limited resources as the processors, memory, batteries, etc. and usually need power tasks for completing in multiple milliseconds. Recent time Internet of things nodes, need that time-based properties to be fulfilled too. Those properties are usually represented in terms of deadlines [5], 71.

The valuableness of the results which are generated by the drops in the system on missing of a certain deadline. If the valuableness sharply drops, then we consider the system as a firm recent system as nuclear power factories, systems of the 'antilock braking' in vehicles, etc. and, if the valuableness drops in a slow manner, then they are considered as soft recent systems as the streaming of multimedia, automatic glass wipers, etc.

1.3. Properties of most of the recent time Internet of things nodes

Applied as system of periodic tasks, Strict requirements of time and deadlines, The worst limits and cases are known well, No dynamically self-adjusted or loaded codes, Recursion isn't even used or is very statically restricted, Power of processing and memory is usually constrained [6].

1.4. Mixed traffic of communication

Many traditional recent time systems consist of various nodes operating independently with no communications or limited abilities. But, with the development of Recent time Internet of things, cyber and physical nodes communicate through industrial networks of communication and usually connected through the Internet.

As most of the recent applications require triggering events depending on certain information conditions, a recent time channel for communication with certain service quality as amounts and requirements for processing of data, etc. are essential for supporting these applications [7], 50.

Also, Recent time Internet of things has the property of usually including flows of traffic with mixed significances, for example, those traffics with variable degrees of requirements of timing, availability and bandwidth.

The high priority traffic, which is crucial for the secured and correct system operation, for example, the sensors for control of closed circuit and real commands of control in the avionics, automotive systems, and systems for security in home.

The medium priority traffic, which is crucial for the correct system operation, but with some delays tolerances, drops, etc.; for example, the systems of navigation in aircraft, monitoring the system in power sub-stations, messages of communication which are sent between the electric vehicles and the charging stations, heating, water sprayers in stations, air conditioning, devices used for lighting, food cooking machines, etc [8].

The lowest priority traffic, which is mainly all the other traffic in the system which doesn't require guarantees on bandwidth or delays as the traffic of engineering in power sub-stations, flows of multimedia in aircraft, messages of notifications from home smart machines, etc.

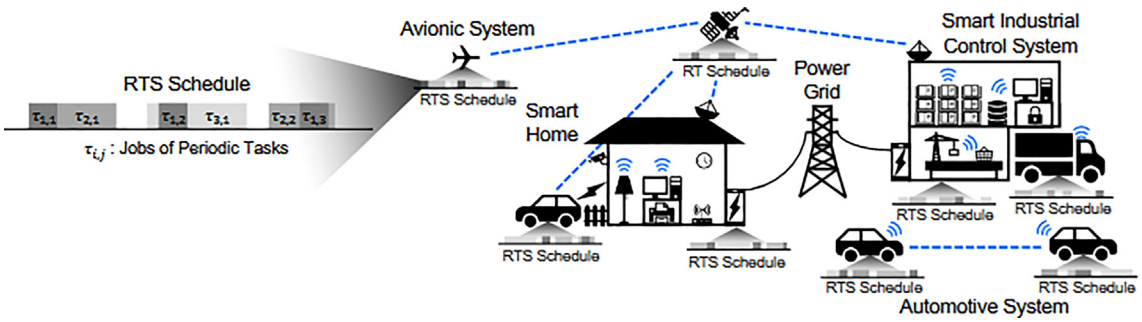

Fig. 1. Overview of daily recent time Internet of things.

Usually, in many critical Recent time Internet of things of safety, the properties of all the high criticality flows are known well, while the properties and number of the other flows are dynamic [10], 33.

1.5. Recent technology

The idea of having modern resources near the known data resources might seem not a new thing. The term 'edge computing' first developed in 2004 to show a system which allow distributing program approaches and the corresponding information to the edge of network towards increasing the efficiency and performance. Also, the idea of having technology of virtualization based on resources for computing in the Wi-Fi subsystem has been developed in 2009. But, the real interest in expanding resources for computing to the edge of network started only after introducing of 'fog computing' for Internet of things.

In the last years, researchers have been utilizing various terms to show the same styles with 'fog computing'. For instance, the author of cloudlet based on virtual machines used the 'edge computing' for describing the idea of cloud at the network-edge. In addition to, the last work of the author showed that fog is a portion of the 'edge computing' [11].

Clearly, the first cloudlet objective was providing a substitution for the mobile applications from the remote cloud, where the applications could distribute the intensive computing tasks to the nearer cloudlet virtual machines placed in the similar Wi-Fi subsystem. While, the first presentation of 'fog computing' purpose was completing the cloud by expanding the cloud to the gateways of network themselves. In concern, cloudlet could be considered as one of the applicable methods for 'fog computing' when the near server devices are present.

There are many other works which describe 'Edge Computing of multiple accesses' as another term for 'fog computing'. Basically, The European institute of standards of telecommunications introduced 'Edge Computing of multiple accesses' as a specific standard from the telecommunication perspective, in which The European institute of standards of telecommunications specified the standards of Interface of Programming applications about how companies of telecommunication are capable of providing computing service based on virtualization to their clients depending on expanding the available infrastructure utilized in virtualization of network functions, 'Edge and Fog Computing' and Internet of things, that has been implemented already in the available equipment [11].

In spite that, it's not correct to describe 'Edge Computing of multiple accesses' as another term for 'fog', in accordance to the current cooperation between The European institute of standards of telecommunications and 'Open fog'. the 'Edge Computing of multiple accesses' will become an applicable method for hastening the 'fog computing' realization.

Also, 'Mist computing' was another term for 'fog' in the old stages. But, current works had referred to mist as a subsection of 'fog'. As a result, mist focused on the requirement to distribute mechanism of computing to the Internet of things extreme edge, in which the devices of Internet of things are placed, to decrease the latency of communication between devices of Internet of things to milliseconds [12], 105.

Basically, the incentive of 'mist computing' is granting the devices of Internet of things with the ability of self-recognition in terms of self-organization, self-management and various self-methods. So, the devices of Internet of things will be capable to operate continuously even when the connection of internet is unstable.

Generally, 'mist' devices might sound the same as the fixed services or services of mobile web, where the services of applications are introduced in various devices which are constrained in resources as actuators, mobile phones and sensors.

But, 'mist' concerns on the ability of self- recognition and awareness of situations, where it allows remote deploying dynamic software code to the different devices depending on the condition and the surrounding changes. Exactly as 'fog' in supplying a platform which allows flexible reconfigurations and deployment of software [12], 109.

So knowing that, the 'fog' needs support of all the connected technologies of ' edge computing'., which means that no one is capable of deploying and managing 'fog' without integrating the technologies of 'edge computing'.

1.6. The attacks and threats of security for Recent-time Internet of thing

Recent systems for Internet of things are faced by many threats in different ways based on the goals and the system of an opponent. In a system made by utilizing a model based on vendors, one of the contributing vendors could maliciously act. That potentially untrusted vendor can embed do various hateful functions in the tasks of the system.

Also, bad practices of coding could cause weaknesses even if the contributing vendors aren't hateful. In a system which has network connection, the opponent might target the interfaces of communication. Because of lacking the authentication in most of those systems, the channels of communication could be forged and intercepted easily.

The methodologies of attacks on Recent time strategy are classified depending on the control over the processes of computing and the functional aim of attacking. Only one way for acquiring control over a target system could be the introduction of malicious virus or code or by utilizing legal code for hateful aims. In addition to, since nodes of Recent time Internet of things are capable of communicating over untrusted channels as the internet, the system is susceptible to network attacks too [14], 98.

Also, other than the continuous trials for crashing the system aggressively. The opponent might attach itself silently to the system and obtain sensitive data as the attacks on the subset channels. The attacks on the subset channels depend on detecting the properties of the system as patterns of using memory, scheduling tasks, consumption of power, etc. That data might be used later by the attackers for launching more attacks.

1.7. Attacks on recent systems for Internet of things

- Violation of integrity with introduction of malicious codes: A smart opponent is capable of getting a position in the system.

For instance, an opponent might introduce a hateful task which respects the system recent guarantees to evade rapid detection and damage 1 or more present recent tasks. The attacker might utilize that task for manipulating sensors and modifying behavior of system in unwanted manners [14], 101.

Violation of integrity by attacks of injection of codes consists of 2 steps. Firstly, the opponent sends snippets of instruction to the device which is stored then anywhere in the memory by the software which receives it. These snippets of instruction are known as 'gadgets'. Secondly, the attacker induces a susceptibility in the software, for example: the recent operating system or the codes used for diverting the flow of control.

- An attack of subset channel manipulates channels which are unknown previously for acquiring valuable data from the victim. Access to memory, traces of consumption of power, scheduling preemptions and temperature, etc. are examples of some subset channels which are used by the attackers. Those

attacks are applicable particularly to attacking nodes of Recent time Internet of things which implement recent time tasks because of the deterministic actions in these systems [14], 104.

- Attacks on channels of communication: Recent time Internet of things elevates the internet as the key medium of communication between the entities. But, the internet, as an unsafe medium of communication, presents various susceptibilities which might put the privacy and security of Recent systems of Internet of things under risk.
- Threats to the communication involves interception or spying, falsifying, interfering of control and messages of information. From the viewpoint of Recent time Internet of things, protecting from threats of communication isn't easy. That's because it's a challenging thing to differentiate rogue communication traffic from the legal communication traffic, particularly for the communication traffic of high priority, without damaging the service quality [15].
- Threats to the communication are often handled by integrating mechanisms of 'cryptographic' protection. But that increases the engineering technology of wireless communication of the recent tasks and might need adjustement of present schedulers. Many operations of cryptography are so expensive too for executing on limited resources especially which are present in fixed devices of Recent time Internet of things.

So, present approaches of cryptography might not be a preferred option for many Recent systems of Internet of things. There's a solution for integrating mechanism of security which can be utilized to deal with threats to the communication but doesn't need modification of present recent tasks [15].

- Attacks of service denial: Because of resource limitations as low capabilities of memory, limited resources for computing, etc. and strict requirements of time, Nodes of Recent time Internet of things are susceptible to attacks of service denial.

The attacker might control the recent tasks and exhaust system resources as disk, central processing unit, memory, etc. A more dangerous type of the attacks of service denial is the attack of distributed services denial, in which large numbers of malicious nodes attack the devices simultaneously. Particularly, when significant tasks are scheduled to start, the attacker might capture ports of network and attack the network to interfere with the system integrity and privacy [16].

The mechanisms made for defensing general information technology or fixed systems don't take into consideration the timing, limitation of resources and safety of Recent time Internet of things and aren't adaptable easily without critical modifications.

Our current recent work might be unitized for protecting from attacks of service denial. But firstly, for these attacks to success, Investigation and preparation of attacks are the initial steps which the attacker require doing. We will discuss that in the following:

2. Approaches for protection from attacks on recent time Internet of things

Those approaches could be classified to 2 main classes:

1- Solutions which need certain hardware support for providing security.
2- Solutions at the level of software which don't need any adjustements.

Firstly, Protection with hardware support:

The main idea of offering protection without weakening the system safety depends on the 'Simplex' structure. 'Simplex' is a recent time structure, which is well known, that uses a small controller of safety as a substitute when the complicated controller with high performance isn't present or isn't working well [16].

The 'Simplex' method goal is guaranteeing that even if a system is regulated by a complicated controller, the system would still be safe.

The main idea of using 'Simplex' structure for protection is to utilize a little simplified system for monitoring the properties as the behavior of time, access to memory, traces of system calls, anomalies of behavior, etc. of an untrustworthy entity which is designated for more complicated tasks and susceptible to less protected media as network, output and input channels, internet, etc.

Secondly, Protection without any adjustments:

In spite the fact that, the architectural adjustments are capable of improving the protection posture of nodes of Recent time Internet of things, these approaches need a general redesigning and might not be proper for the developed systems utilizing components of service of connection-oriented transport [16].

2.1. We will overview some approaches which had been proposed recently for enhancing protection in recent time Internet of things without hardware support

Dealing with attacks on subset channels: It has been demonstrated that the attacker is capable of carrying out a timed attack to estimate behavior of usage of memory indirectly. It is because of the absence of isolation for the distributed resources among various tasks in majority of Recent systems of Internet of things based on service of connection-oriented transport. Overlapping between the tasks occurs when the system changes between various tasks. So, capturing the limitations of protection between the tasks becomes significant for avoiding attacks on subset channels.

Integrating protection in Recent time Internet of things has been proposed by introduction of techniques for adding limitations to the tasks which are scheduled with high priority recent schedulers. Depending on defined levels of protection for every task, the scheduler clears the distributed cache when the system changes from a task of high protection as a task which demands more privacy to a task of low protection as an unprotected task which is mostly damaged [18], 7.

3. Implementation of platform of Internet of things

We built some applications by using the platform of Internet of things which have the key services of recent operating systems, the hardware stratus relates to sensors, modules of communication and the actuators. For building the system of Internet of things, it must have the upcoming sub-systems:

- The prototyping platform of nodes of Internet of things that allows the development of Internet of things, the server of Internet of things that allows communication between the nodes, the structure that explains how the exchanging of data occurs, and the protocol of communication that controls the transfer of messages between the recent time server and nodes of Internet of things.

A large range of smart applications of Internet of things is capable of using the suggested system efficiently, it offers reliability and connectivity to Internet of things. The suggested platform of Internet of things is implemented by using the 'ARM 'Cortex-M4', as it's suitable and robust consumption of power, the suggested node of Internet of things can be a smart mobile phone. The

Internet of things key server and nodes are the main constituents of the suggested system. The key server is in charge of the communication between the nodes of the system by using the internet as the solid backbone Fig. 2 [18], 18.

3.1. The suggested nodes of the system are categorized into major 4 types:

- 'Sensor' nodes that sense the surroundings.
- 'Actuator' nodes that impact the surroundings.
- 'Hybrid' nodes that sense and impact the surroundings.

3.2. The system well be discussed in detail in the following

Nodes of Internet of things

The suggested platform is a fixed system that could be designated for any controller types that meet the requirements of the system, it was developed, implemented and successfully operated in the experiments, the suggested model is implemented by using 'Nucleo Board' that utilizes the processor of 'ARM Cortex-M4′, this processor is especially developed for great performance, low consumption of power and low prices of devices, so it's proper for the nodes of Internet of things.

Every node merely consists of various units as a controller that is required for managing the tasks of node, WI-FI hardware that is utilized for connecting to the network wirelessly for access of internet, sensors for sensing the surroundings and actuators for impacting the surroundings [19], 58.

All nodes of the system are connected to the key server for doing certain tasks so that they are classified into 4 major types: the 'Sensor' nodes, the 'Actuator' nodes, the 'Hybrid' nodes and the 'Monitoring' nodes.

The 'Sensor' nodes used to sense the surroundings and periodically transfer the sensed information to the server within a certain configuration time, they are nodes that contain one sensor or more and don't contain any of the actuators.

The 'Actuator' nodes impact the surroundings depending on an order from the monitoring nodes, they are nodes that include one actuator or more and don't contain any of the sensors [19], 61.

The 'Hybrid' nodes have the functions of the actuator and the sensor nodes. They are nodes that contain both actuators and sensors, the behavior of the node is firstly communicating with the server of Internet of things and then transmits its data of sensor to the Internet of things server and obtains and performs the orders from the monitoring nodes across the server.

The monitor nodes, could be smartphones which control and monitor the system nodes. They are the nodes which don't include sensors and actuators, but they control the actuators and monitor the sensors readings by sending commands, and receiving and processing the sensor data.

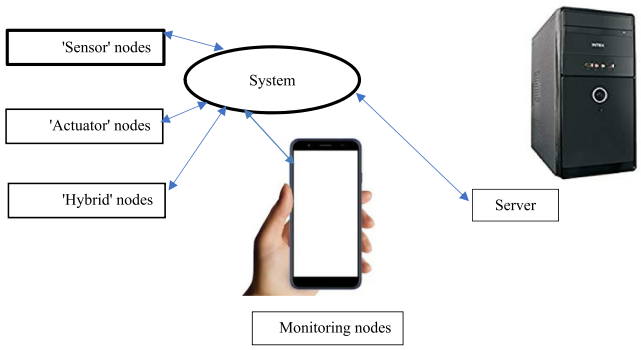

Fig. 2. The suggested structure of system of Internet of things.

3.3. Server of Internet of things

The Server of Internet of things is the key system block that allows communicating all the nodes of Internet of things together in the system, the server is capable of communicating with all nodes types and allows the monitoring nodes visualizing data of sensor [19], 62.

If the connected node is a 'Sensor' node, the server will transmit its data to the monitors which are registered. Also, if the node is an 'Actuator' node, the server will transfer the orders of monitoring nodes to it.

Also, if the node is a 'Hybrid' node, the server will do the tasks for the actuator nodes and the sensor nodes together, and if the node is a 'Monitoring' node, the server obtains the orders and transmits them to the 'Actuator' nodes, and transmits the data of sensor to this 'Monitoring' node [21], 134 Fig. 3.

3.4. Suggested protocol of communication

The key server is in charge of communicating between the nodes of the system for doing the tasks, all the nodes open the connection of protocol of control of transmission with the key server and identifies itself to the system by transmitting its number of identification to the key server waiting for the acknowledgement of the server.

The 'Sensor' node identifies itself, then it's ready for sending the periodic information that it possesses, the 'Actuator' node, after the process of identification, receives orders sent by the 'Monitoring' nodes across the key server, the 'Hybrid' Node does the functions of both the actuator and the sensor nodes. The 'Monitoring' node, after the process of identification, it registers to receive data from certain sensor nodes and transmits its orders to specific actuator nodes [21], 13.

The communication between nodes is done across the server, every node tries identifying itself and connecting with the server, after gaining the acknowledgement of the server, they are capable of communicating successfully with each other.

3.5. Setup of the experiment

Experiments are carried out for studying the performance of the suggested protocol of communication and the performance of protocol of 'Message Queuing Telemetry Transport' by setting various parameters of network that impact the protocol performance [22], 86.

The assessed metrics of performance are the time of delay and the overall sent bytes per each message transmitted successfully, the time of delay is the interval between the message publishing and the received acknowledgement from the server.

The setup has 3 machines used, a laptop that performs the software of emulator of wide-area network to impact the network for implementing losses of channel and delays in communication, a personal computer which is considered as the server for allowing the platforms to communicate with each other, and another personal computer which is considered as a node for message publishing and waiting for its acknowledgment.

The 2 protocols run on the server, the node publishes every message then it goes to the server across the machine of emulator of wide-area network, and the acknowledgement of the server is sent to the node across the machine of emulator of wide-area network too.

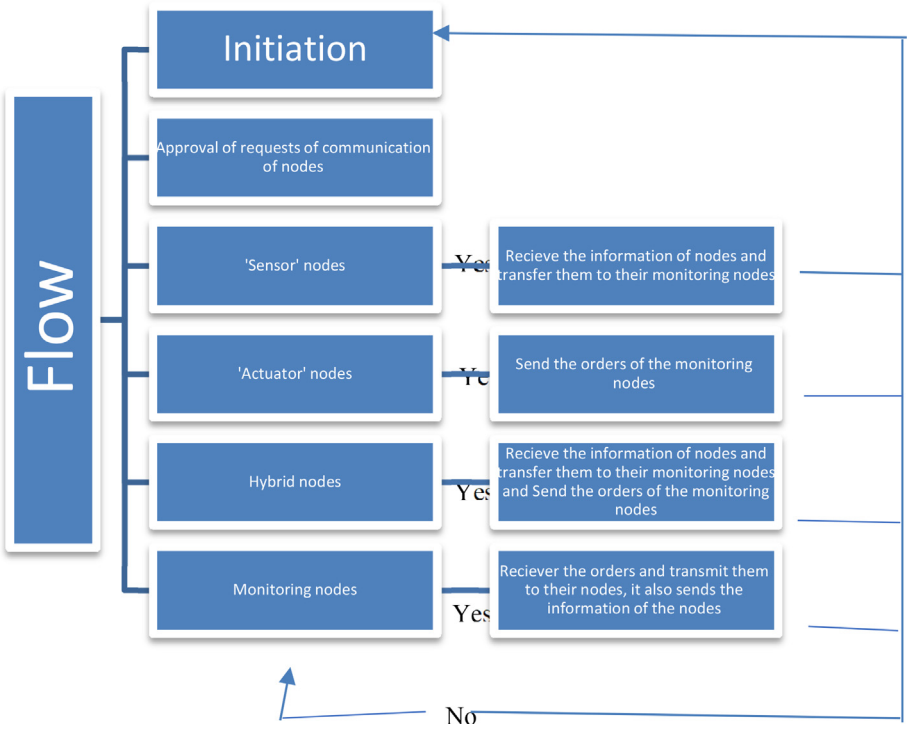

Fig. 3. The flow of data across the server of Internet of things.

4. Results of the experiment

For the experiment setup that is 1 node and 1 server, the two protocols achieved delivering their messages without concerning on the % of loss applied, which means that the two protocols have a good technique for delivery of messages for working with the various rates of losses, so the assessments of performance are studied for the delay of message and the overall amount of the transmitted data for each message transmitted successfully.

The delay of messages is a significant metric, especially for the Recent systems, in which the time is much more significant, the applied rates of losses have an impact on the delay of messages because of the retransmission of messages to deliver the message successfully, the protocol of 'Message Queuing Telemetry Transport' 'MQTT' with certain service quality is compared with the suggested protocol of communication with certain state of acknowledgment for similar messages [22], 87.

'Message Queuing Telemetry Transport' has lower size of packet than the suggested protocol, so its delay of messages is less than that of the suggested protocol. As shown in the following Fig. 4.

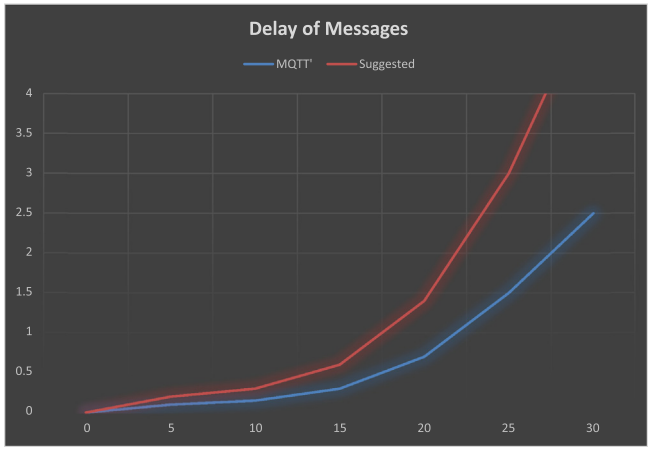

Fig. 4. Delay of messages is less than that of the suggested protocol.

5. Conclusion

Recently, smart devices as cameras, home automatic systems, smart televisions, etc. are internet connected, which rises the term of 'Internet of things', which connects devices and applications together which were isolated before.

The complexity of current attacks on Recent time Internet of things demands rethinking of solutions for protection of these systems. This paper aims at raising the awareness of recent time protection and bridging the gaps in the current protection of the systems of Internet of things with the recent limitations.

The technique suggested here differ from various viewpoints, from protection assisted by hardware to protection without any adjustments. The research developed suggested system for Internet of things. We believed that the worlds of Recent time and Internet of things are connected closely and will be inseparable in the future.

Recommendations

I recommend using systems of Internet of things in more technologies and expanding their usage as they facilitate transmission of data between devices wirelessly.

Also, I recommend developing more techniques for ensuring the safety and confidentiality of data of Internet of things and secure the data from being hacked or attacked, extending the resources of safety is significantly required too.

I recommend giving some attention to my suggested model as I think it can be used for further research and discussion, Internet of things is a very wide topic that one never get enough of.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The authors would like to be a gratitude for Al-Mustansiriyah University Baghdad-Iraq (www. uomustansiriyah.edu.iq) for its appreciated support in this work.

References

[1] F. Al Turjman, Artificial Intelligence in IoT, Springer Science & Business Media, Berlin, Germany, 2019, pp. 93–105.
[2] Cassimally, H. & McEwen, A., Designing the Internet of Things, John Wiley & Sons, United States, 47-54.
[3] Brooks, T., (2017), Cyber-Assurance for the Internet of Things, John Wiley & Sons, United States, 129-132. (2013).
[5] L. Zhang, D. Georgakopoulos, Internet of Things – ICIOT 2018, Springer Science & Business Media, Berlin, Germany, 2018, pp. 70–74.
[6] P. Waher, Mastering Internet of Things, Packt Publishing, United States, 2018, pp. 308–314.
[7] P. Friess, O. Vermesan, Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, River Publishers, Netherlands, 2013, pp. 48–51.
[8] M. Qiu, Smart Computing and Communication, Springer Science & Business Media, Berlin, Germany, 2018, pp. 103–108.
[10] M. Agueh, R. Zitouni, Emerging Technologies for Developing Countries, Springer Science & Business Media, Berlin, Germany, 2018, pp. 32–40.
[11] Hassan, Q., Internet of Things A to Z: Technologies and Applications, John Wiley & Sons, United States, 113-124. (2018).
[12] Buyya, R. & Srirama, S., Fog and Edge Computing: Principles and Paradigms, John Wiley & Sons, United States, 103-112. (2019).
[14] Li, S. & Xu, L., Securing the Internet of Things, Syngress, United States, 97-108. (2017).
[15] Hu, F, Security and Privacy in Internet of Things (IoTs), CRC Press, United States, 355-368. (2016).
[16] Gilchrist, A., IoT Security Issues, Walter de Gruyter, Berlin, Germany, 130-142. (2017).
[18] Cheruvu, S. & Kumar, A. & Smith, N. & Wheeler, D., Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment, Apress, United States, 5-40. (2019).
[19] Kantarci, B. & Oktug, S., Wireless Sensor and Actuator Networks for Smart Cities, MDPI, Switzerland, 56-74. (2019).
[21] J. Park, H. Shen, Y. Sung, H. Tian, Parallel and Distributed Computing, Applications and Technologies, Springer Science & Business Media, Berlin Germany, 2019, pp. 130–142.
[22] Cristian, G. & García-Díaz, V. & García-Bustelo, B. & Lovelle, J., Protocols and Applications for the Industrial Internet of Things, IGI Global, United States, 85-93. (2018).

Further reading

[4] B. Alhayani, H. Ilhan, Efficient cooperative imge transmission in one-way multhop sensor network, Int. J. Electr. Eng. Educ. 57 (2) (2020) 321–339.
[9] BSA. Al Hayani, H. Ilhan,"Visual Sensor Intelligent Module Based Image Transmission in Industrial Manufacturing for Monitoring and Manipulation problems," Journal of Intelligent Manufacturing, Volume 32, Issue 2 (2021), P. 597. 2020.
[13] B. Alhayani, A.A. Abdallah, Manufacturing intelligent Corvus corone module for a secured two way image transmission under WSN, Eng. Comput. 37 (9) (2020) 1–17.
[17] B. Alhayani and Milind Rane,"face recognition system by image processing" International journal of electronics and communication engineering & technology (IJCIET),vol.5, no.5, pp. 80–90. 2014.
[20] Bilal Al Hayani, Haci Ilhan, Image transmission over decode and forward based cooperative wireless multimedia sensor networks for Rayleigh fading channels in medical internet of things (MIoT) for remote health-care and health communication monitoring, J. Med. Imag. Health Inform. 10 (1) (2020) 160–168.