International Journal of Engineering & Technology, 7 (3.34) (2018) 781-785

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Performance Analysis of IoT Adaption Layer Protocol

Nikshepa[1], Vasudeva Pai[2], Karthik Pai[3], Udaya Kumar K Shenoy[4]

[1234]Department of Information Science and Engineering
NMAM Institute of Technology, Nitte
**Corresponding Author Email : [1]nikshepa8594kumar@gmail.com , [2]paivasudeva@nitte.edu.in , [3]karthikpai@nitte.edu.in, [4]ukshenoy@gmail.com*

Abstract

The network communication in the real world has a significant consumption of energy and the processing power involved. The components used for the network communication like the protocol and the other mechanisms used consumes a large amount of energy. As a result the low power networks like WSN and the IoT motes face a lot of difficulties for the processing. As a solution to this IETF group called for a new protocol that utilized a low energy in Low power and a Lossy networks. IPv6 over Low Power Wireless Personal Area Networks abbreviated as 6LowPan protocol was designed for the working in the low power networks.In the paper, we have a detailed analysis carried out on the performance of the 6LowPan protocol with different number of nodes. The performance are evaluated for number of parameters like throughput, latency, power etc

Keywords: IoT, 6LowPan, RPL, DODAG, Cooja

1. Introduction

Internet of Things commonly called as IoT advent brought a tremendous impact among the technological domain. This made an evident advantage for the researchers to begin working with the automation phenomenon. As a result the world was introduced to large number invention that made the life of the people simple to big extent. Common examples include Smart Homes, Smart watches, Smart cars etc. According to the survey there are currently billions of the devices connected to the IoT environment. The IoT protocol stack supports the communication between the devices connected to the system.

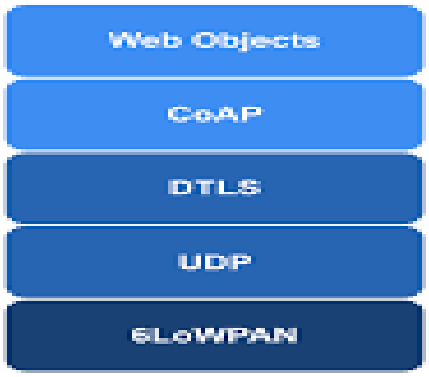
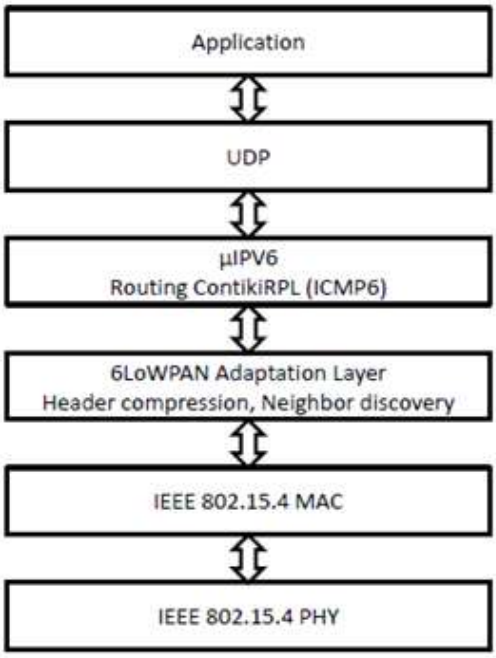


Fig. 1 IoT Protocol Stack

The IoT protocol stack looks similar to that of the IP protocol stack but the difference is the addition of adaption layer. The adaption layer has an intermediate function associated with it, which involves the functionalities of the layer above and below it i.e. the data link and the network layer. Excluding that the overall working is same as that of the Internet Protocol Stack. The overall functionality of the stack includes the similar mechanisms across all the stack layers like fragmentation-reassembly, error control, flow control, routing, multiplexing etc.

1.1 IPV6 over Low Power Wireless Personal Area Networks (6LowPan)

The 6LoWPAN works on a solution to empower remote IPv6 correspondence over the institutionalized IEEE 802.15.4 low-radio for gadgets with restricted space, energy and storage, for example, sensor devices[13][14].The major difference with the IoT protocol layer is the presence of a new adaption layer making its presence between the data link and the network layer.As a delineation, 1280 bytes of length was the value for the maximum transmission rate, and the payload of 127 Bytes. From the bottom to top perspective, the 6Lowpan possess the features of the two layers between them and is independent of the lower stack layers.the following figure has a depiction of the IoT 6LowPan Protocol stack similar to the IoT stack



a

Fig. 2 6LowPan Protocol Stack

1.2 Routing for Low Power and Lossy Networks (RPL)

The RPL is one of a foundation conventions, it is a separation vector and a source directing convention that is composed over a few network layer systems including the physical layer and the Mac layer belonging to the standard IEEE 802.15.4 standard. It targets accumulation systems (WSNs) which involve up to a great many switches (nodes), where the larger part such switches have extremely compelled and restricted assets. RPL has adopted three major modes of communication namely P2P, P2MP and MP2P. P2P is a one-to-one way of data transfer where only two devices are in the part of communication. Similarly as the name suggest P2MP is a point to multipoint mechanisms where the transmission is a multicast communication mechanism. The last mode MP2P is a reverse of the P2MP model. The RPL has a two to three components namely DODAG, RPL control messages and the Objective functions (OF).

1.3 Cooja Contiki Simulator

A recreated Contiki Mote in COOJA is a genuine gathered and executing Contiki framework. The framework is monitores and broke down by COOJA. This is implemented by sorting Contiki for the local stage as a common library, and stacking the library into Java utilizing Java Native Interfaces (JNI). A few distinctive Contiki libraries can be aggregated and stacked in the same COOJA reproduction, speaking to various types of sensor nodes (heterogeneous systems). COOJA controls and breaks down a Contiki framework by means of a couple of capacities. For example, the test system illuminates the Contiki framework to deal with an occasion, or gets the whole Contiki framework memory for examination. This approach gives the test system full control of reproduced frameworks. Sadly, utilizing JNI additionally makes them pester symptoms. The hugest is the reliance on outside apparatuses, for example, compilers and linkers and their run-time contentions. COOJA was initially created for Cygwin/Windows and Linux stage, however has later been ported to MacOS.

2. Literature Survey

The work carried out so far has a lots of contribution from the research papers surveyed during the period. A lot of research and experimentation has been carried out in the domain of IoT, their protocols and similar others stuffs. This chapter details about the references used inaccommodating significant amount of knowledge for the project in IoT protocols.

Dan Dragomir et. al [1] explained the various IoT communication protocols along with different security considerations for the different stack layers. It also stated the security mechanisms that can be implemented across different layers for better robustness and stability.

In a survey carried out by Dr. S. S. Sonavane in [2] the authors were keen into specifying the concerns related to IoT and the support provided by different IoT protocols for security requirements. They also went on to explain the security methods to be incorporated into layers.

Jorge Granjal et. al in [3] performed a survey on existing IoT protocols and also stated the different insecurities associated with the different protocols and also proposed the protection mechanism to be implemented across these protocols for their secure functionality.

The survey on RPL presented by Emran Aljarrah [4] has a detailed information on the working of the protocol. The paper describes the resource constraint in the IoT nodes and inclusion of DODAG models and Objective function for efficient routing of the data among nodes in a low power and Lossy networks.

Arvind Kamble et. al in [5] describes the different types of attacks across the RPL networks. The different types of attacks include the direct attacks, indirect attacks, Traffic attacks and Topological attack. It also details the counter measures for these attacks. They have described the DODAG formation in a RPL network and their maintenance.

Pavan Pongle et. al in [6] has explained the different types of attacks on the RPL and the 6LowPan topology. The major attacks on RPL networks Selective forwarding, Sybil attack, Sinkhole attack, Hello forwarding attacks, Wormhole attacks etc. The common attacks on 6LowPan networks are Fragmentation Attack, Authentication Attack, Confidentiality Attack and Security threats from internet side.

Yuang Chen et. al in [7] quantitatively compared the working of IoT protocols, namely MQTT (Message Queuing Telemetry Transport), CoAP (Constrained Application Protocol), DDS (Data Distribution Service) and a custom UDP-based protocol in a medical setting. The performance was analysed using a network emulator, which optimizes the lower bandwidth, higher latency systems and rate of higher packet loss wireless devices.

Shadi Al-Sarawi et. al analysed the different protocols in various types of IoT networks like Low Power Wide Area Network (LPWAN) and Short Range Network. Various new IoT protocols were introduced like Sigfox, BLE and Z-Wave etc. [8]

Gordana Gardasevic et. al in [9] experimented on the 6LowPan using the motes and analysed the different behaviour of the protocol in different scenarios. The report results in terms of average round-trip-time, packet loss rate and throughput for varying sizes of the payload and hop count for the traffics involving unicast and multicast.

Brendan Cody-Kenny et. al in [10] evaluated the performance of the 6LowPunicast and multicastan on different types of motes. The common parameters were evaluated and also specified the advantages of the 6LowPan.

3. Experiment Mechansims and Set

Destination Oriented Directed Acyclic Graph (DODAG)

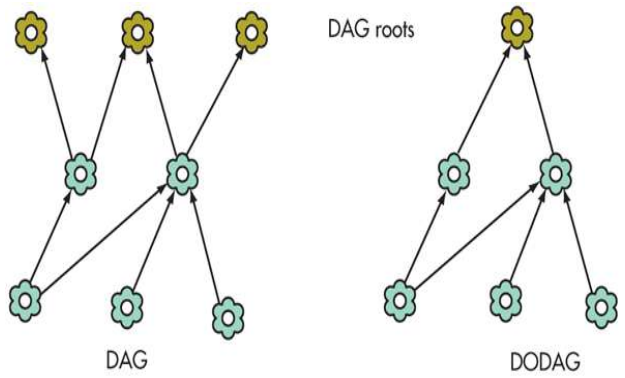


Fig. 3: DODAG Formation in a RPL network

RPL routing protocol generates a Destination Oriented Directed Acyclic Graph (DODAG).This graph is identified by the help of a ID called DODAGID which is assigned to the parent of the corresponding DODAG. Root/Parent devices are determined by considering the link costs, node attributes, note status information, and its associated objective function. The topology is formed in accordance on anattribute called rank metric. Rank Metric for every node of the network is determined by finding the distance from the node to the destination node.

The basic RPL network arrangement isformed by a single DODAG including a single node, complex network scenarios can also be constructed. It is also possible to compile many instances of the RPL parallel in the network, along with their standard optimized objectives.

The RPL includes its own arsenal of control messages, particularly DIO (DODAG Information Object), DIS (DODAG Information Solicitation), DAO (Destination Advertisement Object), DAO-ACK (DAO acknowledgment) and CC (Consistency Check) messages. Every node determines the rank information of other nodes by receiving a DIO from the node. These are required to determine the rank of the individual nodes as they have to join a DODAG and to choose an arrangement of guardians and the suitable ancestor in that DODAG among every conceivable neighbour.This message might be asked for by communicating something specific of sort DIS. The two control messages are utilized for the foundation of courses upward in the RPL directing tree, while descending ways are set up by having DAO messages to back-spread steering data from leaf hubs to the roots. This message is activated by the gathering of a DIO message, and its beneficiary sends a corresponding acknowledgement packet to the parent or to the root of the DODAG. The security from the replay attacks are guaranteed among the communicating nodes with the help of Consistency Check messageswhich also ensures the synchronized counter values. [3].

Simulation Setup

The simulation was performed to analyse the behaviour of the IoT Adaption layer protocol 6LowPan. During the simulation, different scenarios were built to perform the protocol evaluation. As a result, the scenarios involved the different number of nodes set for each simulation. The node numbers were varied as 5,10,25,50 etc. In order to bring up the uniformity, all nodes were arranged in the circular fashion with most of the source nodes connected to the sink. All the nodes were static and no mobility was implemented. The following section builds up the result and analysis performed from the simulation. The different parameters like RT Metric, ETX and power values are all analysed.

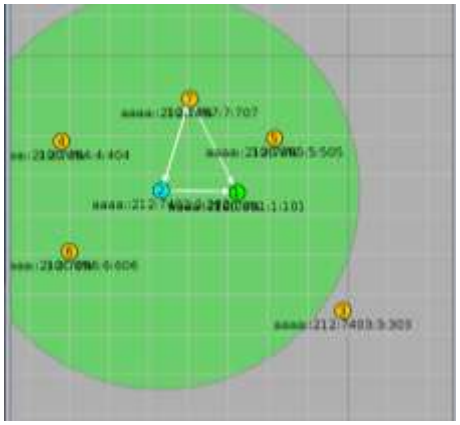


Fig. 4 6 Node Network Setup

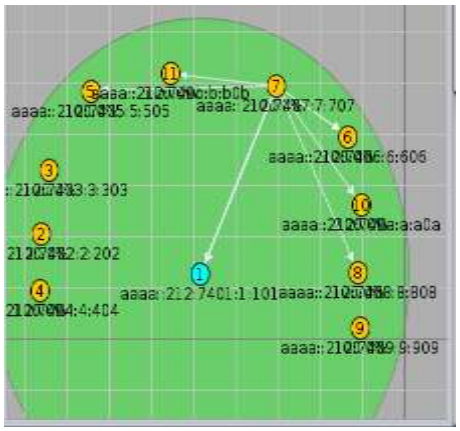


Fig. 5:10 Node network Setup

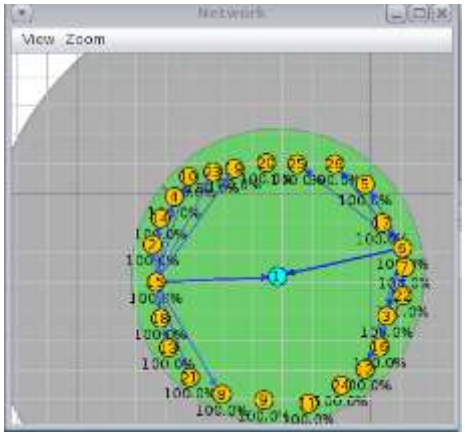


Fig. 6: 25 Node Network Setup

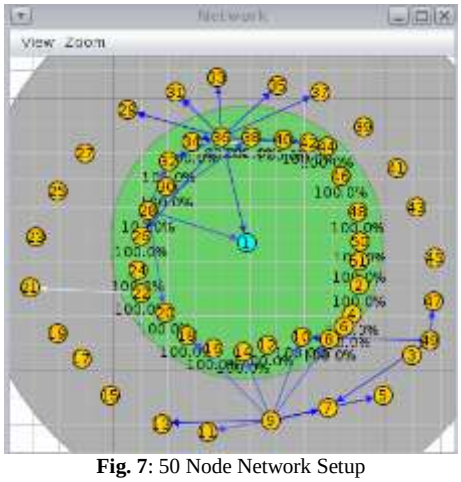


Fig. 7: 50 Node Network Setup

4. Result and Analysis

This section discus the simulation results of the 6LowPan protocol during different setup and the effects on the different metrics are learnt.

4.1 Metrics used for the Performance Analysis

The metrics used for the performance analysis of 6LowPan are Energy Consumption, Temperature along the nodes, packet related information and intervals.

4.2 Simulation Parameters

The table shows the network parameters used for the simulation.

Table 1 simulation parameters

Parameters	Value
Simulator	Cooja Contiki
Routing Protocol	6LowPan with RPL
Traffic Generated	UDP
Number of nodes	6,10,25,50
Number of Sinks	1
Simulation time	1-60 minutes

4.3 RT Metric Evaluation

This parameter usually defines the total packet received and transmitted ratio across the network. Depending on the total duration time the values will be higher or lower accordingly.

Table 2 rt metric comparison

Number of Nodes	Average RT Metric
6 Source	462.506
10 Source	410.660
25 Source	437.460
50 Source	821.528

We have a table of values showing a values for different networks. We can see the varying values associated with the networks with different nodes. Among them the 50 node network has the highest of the value which is evident with the large number of nodes present in their network. As many control packets are transmitted across the network the RT Metric results to be big.

4.4 Expected Transmission count (ETX)

The ETX Metric is a measure of the nature of a path between two nodes in the network. This basically depends on the medium and its capacity, packet behaviour. It also suggests the error probability along the transmission medium.

Table 3: etx count comparison

Number of Nodes	Average ETX
6 Source	16
10 Source	17
25 Source	17
50 Source	24

The ETX is supposed to be the same across all the links. The large number of nodes may bring an additional overhead associated with the error control phenomenon. As a result once again a higher node network results in the higher ETX count for the network.

4.5 Total Power Consumption

The total power consumption is the metric that evaluates the energy consumed by the entire network for its communication. This energy consists of the energy required by the nodes to listen to the radio signal, power to transmit power and the total CPU power consumed by the network

Table 4*: energy consumption values*

Number of Nodes	Total Power Consumption
6 Source	0.878mW
10 Source	0.868mW
25 Source	0.988mW
50 Source	1.310mW

The above results were straightforward where the total energy of the network is increased with the expansion of thenodes in the network. The reason is the large amount of processing associated with the nodes like sending the control messages across the neighbours, DODAG formation, actual data transfer etc. considering all this the higher node networks results in higher energy consumption.

Fig. 5: Energy Consumption chart for 10 node network

6. Conclusion

The proposed work involved the performance evaluation of the 6LowPan IoT adaption layer protocol. The protocol was tested for energy consumption and packet related information like RTMetric etc. Under many circumstances the energy consumption was observed with the deployment of the different number of nodes in the network. The latency related intervals was also increased with the increased number of the nodes. The multi sink phenomenon decreased the packet interval to some extent.

However in the future work the variation in the nodes behaviour on adding mobility should be evaluated. Also the phenomenon of dynamic node property changes can be introduced to determine the changes among the node/network performance.

References

[1] Dragmoir, D., Gheaorge, L., Costea, S. and Radovici, A. “A Survey on Secure Communication Protocols for IoT Systems”, International Workshop on Secure Internet of Things, 2016.

[2] Sonavane, S.S. and Deshmukh, S. “Security Protocols for Internet of Things: A Survey”, IEEE Conference, 2017.

[3] Granjal, J., Moteiro, E. and Silva, J.S., “Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues”, IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 17, NO. 3, 2015.

[4] Aljarrah, E., Yassein, M.B. and Aljawarneh, S., “Routing Protocol of Low-Power and Lossy Network:Survey and Open Issues”, IEEE onference, 2016.

[5] Kamble, A., Malemath, V.S. and Patil, D., “Security Attacks and Secure Routing Protocols in RPL-based Internet of Things:Survey”, International Conference on Emerging Trends & Innovation in ICT (ICEI), 2017.

[6] Pongle, P. and Chavan, G., "A Survey: Attacks on RPL and 6LoWPAN in IoT", International Conference on Pervasive Computing (ICPC), 2015.
[7] Chen, Y. and Kunz, T., "Performance Evaluation of IoT Protocols under a Constrained Wireless Access Network", 2016.
[8] Al-Sarawi,S., Anbar, M., Alieyan, K. and Alzubaidi, M., "Internet of Things (IoT) Communication Protocols : Review", 8th International Conference on Information Technology (ICIT)", 2017
[9] Gardasevic, G., Mijovic, S., Stakjic, A. and Buratti, C., "On the Performance of 6LoWPAN through Experimentation", IEEE Conference, 2015.
[10] Cody-Kenny, B., Guerin, D., Ennis, Desmond., Carbaj, R.S., Huggard, M. and Goldrick, C.M. "Performance Evaluation of the 6LoWPAN protocol on MICAz and TelosB motes", School of Computer Science and Statistics Trinity College Dublin Dublin 2, Ireland.
[11] Bhat, S., Pai, V. and Kallapur, P., V.,"Energy Efficient Clustering Routing Protocol based on LEACH for WSN", International Journal of Computer Applications, Vol. 120, No. 13, June 2015.
[12] Pavan, R., Pai, V. and Kallapur, P., V., "Energy Efficient Clustered Routing Protocols of LEACH", International Journal of Research in Applied Science & Engineering Technology, Vol. 3, Issue V, May 2015.