The International Conference on Research Perspectives : IoT in Hybrid Grid Integrated Renewable Energy Sources
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)

IoT Data Link Layer Communication Protocols Frame Format in Controller Area Networks

Dr. Sreekanth R
Department of MCA, New Horizon College of Engineering, Bengaluru, Karnataka, India

ABSTRACT

The crucial part of in Internet of Things (IoT) is its protocols. Protocols specify the communication for each layer of the network where the data is exchanged as per the specified frame formats. The Open System Interconnection model has specified and well-defined frame format of data link layer on how the data bits are taken from physical layer and formed as frames. This frame has a header field, payload field and trailer fields. Data link layer (DLL) provides an error free data to the above layer i.e Network layer. Data link protocols provide framing, error detection, correction and flow control. IoT has various standards mentioned for data link protocol. These standards for protocols are provided by few international organizations which are known as Internet Engineering Task Force (IETF), Institute of Electrical and Electronics Engineers (IEEE) and International Telecommunication Union (ITU). In this paper we first study about the DLL protocols, frame format and then propose an additional payload field required for extended protocols frame format in controller area networks (CAN).

Keywords - Error detection, Error Control, Flow control, Framing, Protocols.

I. INTRODUCTION

Data Link Layer provides services to network layer by utilizing various communication protocols that are used in IoT. Smart devices which are connected to the network the data communication happens with the assistance of protocols. There are several standard protocols provided by the telecommunication organizations. Bluetooth is a short-range wireless communication which is present in most of smart devices.

Data transfer rate for Bluetooth provides 3 Mbps for a short range of meters. Zigbee is similar to Bluetooth technology and supports Mesh topology. In this technology the physical layer link with data link layer protocol standards are provided by IEEE 802.15.4.

Blue Tooth Low Energy (BLE) is used in Personal Area Networks. Z-wave provides wireless communication for longer range IoT. Similarly, many other protocols like Sigfox, RFID also can be used in many smart devices for IoT. CAN is a bus standard which is designed so that the devices and microcontrollers communicate with each other with host computer.

II. CAN DATA LINK LAYER

The data link layer protocols for controller area networks have certain unique features. Bit errors are quite common in the communication. All Single bit errors are detected in this layer. There is high probability that multi but errors are also detected. The data frame for the CAN is shown in the fig1.

SOF	**Arbitration field**	Control Field	Data Field	CRC field	ACK field	EOF	MF
Arbitration Phase		Data Phase			Arbitration Phase		

Fig 1: A CAN Data Frame

The transmission speed limit for CAN usually for short networks is in the range of 1 Mbps. Payload field in this frame is 8 bytes. CAN with Flexible Data Rate, CAN FD can have a payload filed till 64 bytes. The standardized frame format of CAN link layer is mentioned in ISO 11898. The implementation services of this layer is mentioned in Logical Link Control and Medium Access Control layers of CAN. Fig 2 shows the Data Link layer services.

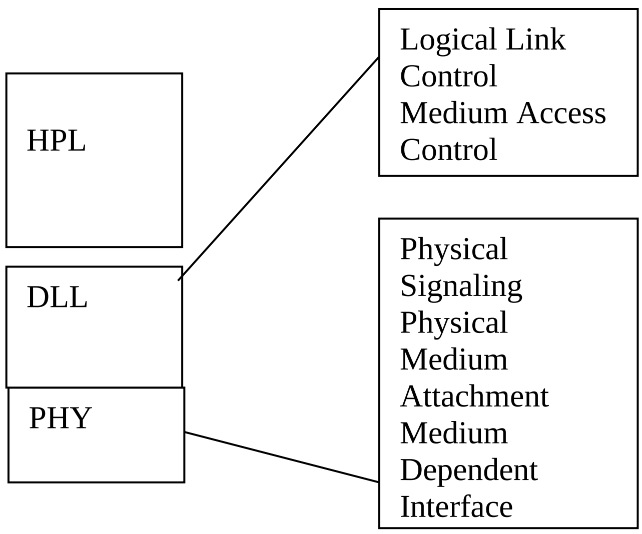

Fig 2. Data Link Layer Services

Some of the services like acceptance filtering, overload notification and recovery management are provided by the logical link control layer(LLC). Bit timing and Data Encapsulation is provided by medium access control layer .

MAC also responsible for the error detection, error signaling and acknowledgement. The data link layer should provide better communication services in order to provide an error free data to Network layer. there are two such services here in this layer. Write object service and Read Object service.

III. LITERATURE REVIEW

In [1] the authors proposed a common layered model which are used in standard models like OSI [2]. The model is also compared with the Transmission Control and Internet Protocol (TCP/IP) model [3]. The OSI model has seven layers while TCP/IP model has four layers. The authors proposed a protocol stack which require five layers for the IoT stack. In this layer the physical and data link layer provides the Radio Frequency capabilities.

In [4] Routing, security of data is provided by the Network layer in the IoT stack. Transport and application layers provide commands for the protocol. It was proposed to use few protocols like Open Stack for IoT, Blue Tooth Low Energy, Zigbee, Z-wave and Sigfox.

Each protocol mentioned has range, interoperability, security practices and topology type. In [5] the definition of Physical layer and data link layer are provided. In order to provide interoperability with non-IoT networks which are using IPV6, a layer called 6LoWPAN is introduced between data link layer and network layer. this layer ensures to provide interoperability in Non-IoT devices which will use the IPV6 address.

The Medium Access Layer is defined for two nodes which provides Reduce Function and Full Function device. The major challenge here for IoT is to transpose the IP network to networks which are using Low power wireless personal Networks.

In order to achieve this in [6] Internet Engineering Task Force provide a protocol named 6LoWPAN. Transport layer in IoT also relies on the basic protocols. Two such protocols are Transmission control protocol and User Datagram protocol. In [7] the authors provided control area networks communication services as write and read object service. Write object service will usually transmit the data frames in a way like producer to consumer.

IoT can be viewed as an integration of various networks which include wired networks, wireless networks, mobile networks, adhoc networks, and mobile ad-hoc networks[8]. The protocols used in IoT communication layer can be known from the below fig3.

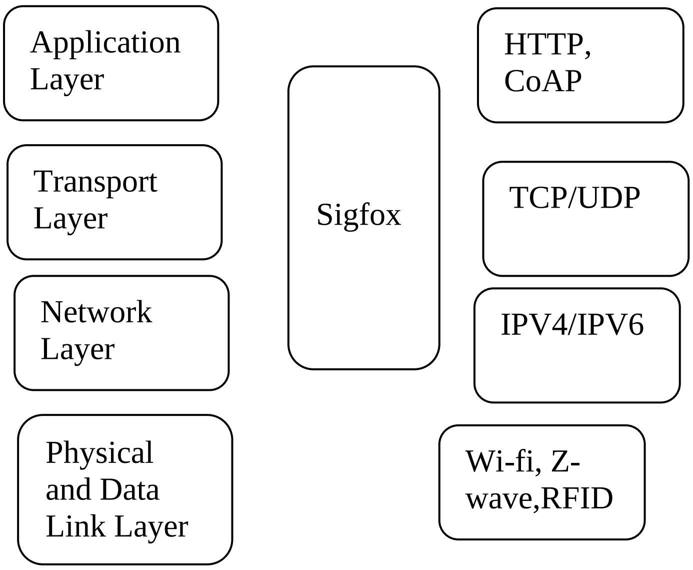

Fig 3. Protocols in IOT Communication

IV. IOT DATA LINK LAYER

MAC Layer is the sub layer of the Data link layer. IEEE 802.15.4 is the standard defined for MAC layer [9]. This standard defines the frame format which includes the header, trailer and payload fields. Node communication is also mentioned in this layer [10]. These formats can be used for traditional networks but when we use the low power communication protocols in IoT, these formats are not suitable due to their overhead. A new defined protocol is needed for low power communication protocols. These are defined in IEEE 802.15.4e[11] which supports low power in IoT devices and meet low-cost communication for IoT. The features that defined the standard for the frame format as shown in Table 1.

Feature	Description
Slot frame Structure	Scheduler for each node
Scheduling	Handles Mobility Scenarios
Synchronization	30 second Prespecified intervals
Channel Hopping	Changing Frequency channel
Network formation	Joining components

Table 1 Features for frame format

IEEE 802.11ah is another low power wireless standard access medium [12]. The features of this standard are given in below Table 2.

Feature	Description
Synchronization Frame	Probe delay can be configured
Efficient Bi directional packet exchange	Power saver for uplink and downlink
Short MAC Frame	Provides short MAC frame for 12 bytes
Null Data packet	Have ACK frames
Increase Sleep Time	Exchanging data

Table 2 Feature of 802.11 ah Frame format

V. EXISTING FRAME FORMAT OF DATA LINK LAYER OF CAN

Data exchange in any serial communication system usually will be in the form of frames. CAN networks has two basic formats [13]. One is the standard base format which supports bits for identifier, whereas extended frame format supports 29 bits for the identifier. In an extended frame format bit are assigned to the base frame and remaining 18 bits are assigned to extension which can be termed as identifier extension[14]. The frame format for standard base frame is shown in fig 4.

SOF	11bit	RT	Control	Data

Fig4. Standard base format

CAN controllers which support the extended base format can also able to send and receive the messages through standard base format [16] the extended base format for CAN is shown in Fig 5.

SOF	11bit	SRR	IDE	18 bit	RTR

Fig 5. Extended frame format

The control field in the extended format contains r1,r0 and DLC fields [17]. The bit filed of the standard and extended CAN can be summarized as follows in table 3

Field	Description
SOF (1 Bit)	Start of Frame – synchronize the nodes
Identifier (11 bit)	Indicates priority
Remote Transmission Request (1 bit)	Dominant in data frames
Reserver (2 bits)	Dominant
Data length code (4 bits)	Number of data bytes
Data field (0-8 bytes)	Determined by DLC
CRC (15 bits)	Cyclic Redundancy check
CRC delimiter (1 bit)	Recessive
ACK (1 bit)	Acknowledgement field
ACK delimiter (1 bit)	ACK delimiter field
EOF(7 bit)	End of Frame

Table 3. Bit field of Standard and Extended CAN

In the CAN data frame, a 15-bit Cyclic Redundancy Check Sequence need to be derived for the frames being transmitted [18]. This process is done by calculating the CRC from starting of the frame till the data field is encountered.

VI. CRC GENERATION FOR DATA FRAME

The CRC can be generated by using a generator polynomial. In this paper we use the LFS (Linear Feedback Shift) to generate the CRC code and implement it. A polynomial is generated and can be used here. This generator polynomial is shown as follows.

$$X^{15}+X^{14}+X^{10}+X^{8}+X^{7}+X^{4}+X^{3}+1$$

The transmitter of the frame is treated as polynomial and it will be divided by the polynomial generator. Modulo 2 division is performed on the sequence and then this is transmitted along with the message.

The receiver will also perform the same check as done by the transmitter. If the result found is not as same as the bits send by receiver the frames are discarded. It then transmits an error frame and then request the sender to retransmit the frame.

CAN sends the message from source to destination. Usually, CAN bus has four different frame types. Data frame is used to transmit the data over the network. Remote frame is used to request the data in an network from another node. Error frame is used to get the message again in case of error found.

VII. PROPOSED ADDITIONAL PAYLOAD FOR AN EXTENDED FRAME FORMAT

In this section an extended frame format with additional data field bits is proposed in order to accommodate more data. An error free frames can be sent in short time if the data in the payload field can be accommodated more than the currently available frame formats. Low power for IoT is taken care to accommodate more data with other fields designed to accommodate less bits. This will decrease the power consumption for low cost IoT devices.

The proposed frame format is shown in the following figure.

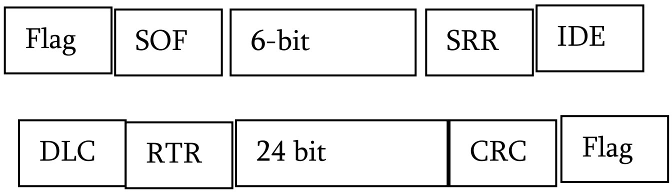

Fig 6. 24 bit payload proposed frame format

In the above fig we propose the frame format for IoT data link layer for 24 bit payload field. The other fields remain same as the previous format. We also propose a Flag field for beginning and ending of the frame format. This frame format better fits for current IoT devices which also require low power. The cost involved for these frame formats are also minimized.

VIII. RESULTS

From the above study and CRC generation for a data frame it can be observed that CAN has two standard formats one is base identifier and other is extended frame format for data link layer in IoT devices. But these frame formats also have some limitations for the communication and data transfer. This frame formats have the starting and ending of the frame which has 1-bit SOF and 7-bit EOF. In the proposed frame format, we can have a 1 bit Flag both at beginning and end which can reduce the bit size. As IoT devices require less power and minimize the cost design this proposed frame format may control the overhead.

IX. ACKNOWLEDGMENT

I thank New Horizon College of Engineering for providing me opportunity to write this paper. Further I thank my Department Head, Master of Computer Applications and all Colleagues for their continued support in completing this paper on time.

X. REFERENCES

[1]. H. Li, Z. Weishi, and Z. Weifu, "A Novel Vulnerability Detection Method for ZigBee MAC Layer," in IEEE 12th International Conference on Dependable, Autonomic and Secure Computing, 2014.

[2]. Shyan, S. Y. Wei, and S. C. Chou, "A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi," in The 33rd Annual Conference of the IEEE Industrial Electronics Society(IECON),2013pp5-8.

[3]. Z. Zhou, Kista, W. Zhiqang, W. Fan, and W. Yuexin, "A middleware of Internet of Things (IoT) based on Zigbee and RFID," in IET International Conference on Communication Technology and Application(ICCTA),2011,pp.34-41.

[4]. Y. Xiolin, J. Zhiqang, Z. Wenjun, and W. Zhingning, "The Research and Implementation of ZigBee Protocol-Based Internet of Things Embedded System," in International Symposium on Information Engineering and Electronic Commerce (IEEC), 2010, pp. 7-10.

[5]. C. H. Kuor, "Bluetooth : A Viable Solution for IoT?," in IEEE Wireless Communications, vol. 21, no. 6, 2011, pp. 6-7.

[6]. J. H. Christophher, "Internetworking with Bluetooth Low Energy," in Mobile Computing and Communications," 2015 pp 34-38.

[7]. Niemen, C. Gomez, M. Isomaki, and T. Savolainen, "Networking Solutions for Connecting Bluetooth Low Energy Enabled Machines to the Internet of Things," in IEEE Network, vol. 5, no. 4, 2014 pp. 83-90.

[8]. C. J. Hansen, "Internetworking with Bluetooth Low Energy," in Mobile Computing and

Communications, vol. 19, no. 2, 2015, pp. 34-38.

[9]. Z-Wave "Understanding Z-Wave Networks, Nodes & Devices"

[10]. P. Amaro, R. Corteso, R. Landeck, and J. Santos, "Implementing an Advanced Meter Reading infrastructure using a Z-Wave Compliant Wireless Sensor Network," in Proceedings of the 3rd International YouthConferenceonEnergetics,2011.

[11]. C. S. Zhengguo, Z. Chunseng, and C. M. Victor "Surfing the Internet-of-Things: Lightweight Access and Control of Wireless Sensor Networks Using Industrial Low Power Protocols," in EAI Endorsed Transactions on Industrial Networks and Intelligent Systems,vol.1,no.1,2014.

[12]. D. Baldo, G. Beneelli, and A. Pozzebon, "The Siesta Project : Near Field Communication," in Proceedings of 7th International Symposium on Communication Systems Networks and Digital Signal Processing, 2010, pp. 721-725.

[13]. V. Coskun, K. Ozdinici, Near Field Communicatioin (NFC), Wiley, 2012.

[14]. P. Urien, "LLCPS: A new security framework based on TLS for NFC P2P applications in the Internet of Things," in IEEE Consumer Communications and Networking Conference (CCNC), 2013, pp. 845-854.

[15]. C. Vedat, O. Busra, and K. Karim, A Survey on Near Field Communication (NFC) Technology. Springler, 2013.

[16]. HomePlug Powerline Alliance, HomePlug Green PHY 1.1, the standard for in-house smart grid powerline communications: an application and technology overview White paper, October 2012, 17p.

[17]. H. Jun, Qingdao, M. Zheng, S. Chungseng, "Energy-efficient MAC Protocol Designed for Wireless Sensor Network for IoT," in Seventh International Conference on Computational Intelligence and Security (CIS), 2011.

[18]. S. Eckehard, K. Matthias, A.N. Anas, D. Stefan, A. Moller, R. Luis, S. Florian, "Advances in Media Technology Internet of Things," technical report, Technische Universitat Munchen Institute for Media Technology, 2013. IoT "New Weightless 2-Way Communication IoT Standard launches"

[19]. A. Sikora and V. F. Groza, "Coexistance of IEEE 802.15.4 with other systems in the 2.4 Ghz-ISM-Band,' in Proc. IEEE Instrumentation & Measurement Technology Conference, May 2005,

[20]. K. Shuaib, M. Boulmalf, F. Sallabi, and A. Lakas, "Coexistance of ZigBee and WLAN: A performance study," in Proc. IEEE Int. Conf. Wireless & Optical Communication Network, April 2006.

[21]. P. S. Neelakanta and H. Dighe, "Robust Factory Wireless Communication: A performance appraisal of the Bluetooth and the ZigBee collocated on an industrial floor," in Proc. IEEE Int. Conf. ind. Electron. (IECON'03), November 2003, pp. 2831-2386.