International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-10 Issue-5, June 2021

Evaluation of High Speed Communication Interfaces for Next Generation Secure Element

Gurunath Reddy, Sharvani G.S.

Abstract*: Secure element is a microprocessor chip that provides a secure environment to store the data, execute the applications and communicate the data to external entities securely. As secure element provides a promising security feature, it is used in various domains like IOT, automobile and mobile phones. Nowadays, the size of the security key and size of the data to be processed are increasing whereas the processing time of the secure element is expected to reduce. As the data size increases, the time to communicate the data between secure element and host increases. Host and secure element are connected via SPI over ISO IEC 7816-4 (T1) communication interface. In this paper, we evaluate the throughput of SPI over ISO IEC 7816-4 (T1) interface which is widely used in smart card domains. Throughput of the interface is evaluated by examining the time spent at communication interface for varying data size. We focus on understanding the parameters that affect the throughput of the SPI over T1 interface.

Keywords: ISO-IEC 7816-4 (T1), SPI, Throughput, Evaluation,

I. INTRODUCTION

A Secure Element is a tamper-resistant microprocessor chip capable of securely hosting applications and their confidential and cryptographic data in accordance with the rules and security requirements set by trusted authorities [1]. In present era, size of the cryptographic key is increasing and complexities of cryptographic algorithms are increasing, which increases time at communication interfaces and processing time of the Secure Element. But, the users expect the processing time of the data to be reduced. Secure element is used along with general purpose MCU in an embedded system to handle all the security related functions and data. Secure element is connected to general purpose MCU via SPI over T1 communication interface. In this paper, we evaluate the throughput of this communication interface and understand the parameters affecting the throughput.

II. SPI OVER T1 INTERFACE

Host and Secure element communicate via SPI over T1 interface. The physical layer protocol used for the communication is Serial Peripheral Interface (SPI) and the data link layer protocol is ISO-IEC 7816-4 standard T1 protocol. Application layer at host and Secure Element communicate via APDUs (Application Protocol Data Units). Host sends the Command APDUs (C-APDU) to Secure Element. SE processes the command and sends the Response APDU (R-APDU).

The SPI bus system is a synchronous serial peripheral interface that allows the MCU and various peripherals to communicate and exchange data in a serial manner [2]. SPI bus usually consists of four lines, which are serial clock line (SCLK), master device data input line (MISO), master device data output line (MOSI) and slave chip selection line (CS). The specific functions are as follows.

MISO – Master Input Slave Output: Data input from the Master Device and output from the Slave Device.

MOSI – Master Output Slave Input: Data output from Master Device and input from Slave Device.

SCLK – Serial Clock: Clock signal generated by the Master Device.

CS – Chip Select: Slave Device enable signal and controlled by the Master Device.

ISO/IEC 7816-4 standard T1 protocol is block oriented protocol, which means that one block is the smallest data unit that can be transmitted between the smart card and the interfacing device [3]. Data from application layer is transmitted in blocks. The size of the block is variable and is fixed during Answer to Reset (ATR) bytes exchange. T1 block structure consists of 3 fields Prologue field, information field and epilogue field as shown in fig 1.

Prologue field is of 3 bytes. It consists of NAD (Node Address) field, Protocol Control Byte (PCB) field and Length field.

Node address (NAD) is used to identify the source and destination nodes. It specifies the source and destination nodes for the frame being exchanged. Every node is addressed using 3 bits.

Protocol Control Byte (PCB) is mainly used for transmission of protocol control information [4]. It does not hold any application data. It indicates the type of the block. Bit configuration is different for I Blk, R Blk and S Blk.

For I Blk, it holds the sequence number of the block and more data information bit. For R Blk, it holds the sequence number of next I block and the error information. For S Blk, it holds the protocol control information like waiting time extension, change in information field size etc.

Information Field holds the actual data from application layer. It is present in I Blk always. It is optional in S Blk and R Blk.

Manuscript received on May 31, 2021.
Revised Manuscript received on June 08, 2021.
Manuscript published on June 30, 2021.

* Correspondence Author

Gurunath Reddy*, Student, Department of Computer Science and Engineering, Rashtreeya Vidyalaya college of Engineering, Bengaluru, Karnataka, India. Email: gurunathreddym.scn19@rvce.edu.in

Dr. Sharvani G. S., Associate Professor, Department of Computer Science and Engineering, Rashtreeya Vidyalaya College of Engineering Bengaluru, Karnataka, India. Email: sharvanigs@rvce.edu.in

Epilogue Field is of 1 byte of 2 byte. The size of the epilogue field is communicated during the ATR bytes exchange. It is checksum of all the bytes from prologue field and information field.

It is used for error detection. Checksum algorithm used is either CRC (Cyclic Redundancy Check) or LRC (Longitudinal Redundancy Check). The type of the algorithm used is communicated using ATR bytes.

prologue field			information field	epilogue field
node address NAD	protocol control byte PCB	length LEN	APDU	EDC
1 byte	1 byte	1 byte	0 ... 254 bytes	1 ... 2 bytes

Fig1: T1 protocol block structure [4]

T1 protocol supports 3 types of blocks. I Blk, R Blk and S Blk.

I blk (Information block) is used to send the application data.

R Blk (Response block) is used to acknowledge the reception of I Blk. R blk has 2 bits allocated to indicate the erroneous status of the received I blk. It is used to inform the sender that previous I blk is received without error, so that sender can send the next I blk or send the same I Blk in case of erroneous frame.

S Blk (System Block) is used to transmit control data of the protocol. It does not send any data from application layer.

III. EVALUATION

System set up for evaluation consists of Secure Element, card reader, card reader console application and a debugger as shown in fig 2. Card reader and the console application are used to exchange commands and responses with SE. Debugger is used for building and debugging the evaluation code.

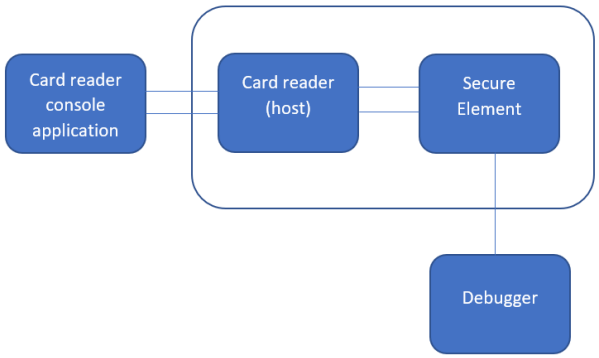

Fig2: Test set up for evaluation of the interface

SPI over T1 interface is evaluated using timers. Timer is started when the frame sent by the host arrives at the SPI device drivers. Timer keeps running during the frame processing at SPI Device Driver layer and frame processing at T1 layer. Timer is stopped when the frame is completely processed and C-APDU is forwarded to application layer as shown in fig 3. In this way, the time consumed for processing the frame is captured and hence the receive path is completely evaluated. Application layer processes the C-APDU and sends the R-APDU back to communication interface (T1 over SPI interface). T1 layer adds prologue field and epilogue field to R-APDU and forwards this frame to device driver layer. SPI DD layer adds the corresponding fields and sends out the data. Timer is started when the R- APDU is sent to T1 layer. Timer keeps running when the processing is done at T1 layer and SPI DD layer. Timer is stopped when the SPI DD sends out the data to host. In this way transmit path is evaluated completely.

Evaluation of communication interfaces is different for short data transfer and large data transfer. Short data transfer refers to the data where the application data is smaller than the block size of T1 frame. In case of short data, the application data can be sent from one device to another device in a single I block. Large data refers to the data where the application data is larger than the T1 frame block size. In case of large data scenario, the application data is sent via multiple I blocks.

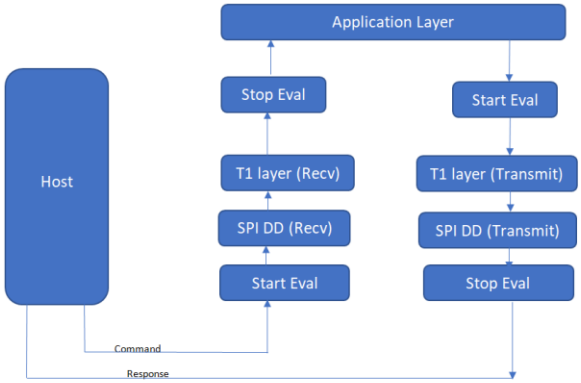

Fig 3: SPI over T1 Interface

A. Smaller Data Evaluation

The short C-APDU is transferred from host to SE in single I Blk frame. SE processes the C-APDU and sends R-APDU back to communication interface. Shorter R-APDU is transferred from SE to host in single I Blk frame. In this scenario, total two I Blk frames are exchanged.

The first I Blk frame containing the C-APDU is evaluated by starting the timer when the frame arrives at SPI DD.

Timer will be running when the data flows through SPI DD and T1 layer. Timer is stopped when the C-APDU is forwarded to application layer. The elapsed timer value gives the total time spent by the frame at communication interface. This evaluation is part of receive path.

The second I Blk frame containing the R-APDU is evaluated by starting the timer when the R-APDU is sent from application layer to T1 layer. The timer will be running during T1 layer and SPI DD processing. The timer is stopped when the SPI DD sends out the data to host. The elapsed timer value gives the total time spent by the frame at communication interface. This evaluation is part of transmit path.

B. Larger Data Evaluation

A memory buffer is allocated at T1 layer to store the contents of received frames. T1 layer copies the contents of the received I Blk frame to buffer allocated to it until the buffer is full. When the buffer is full, the C- APDU is forwarded to application layer.

Retrieval Number: 100.1/ijeat.E27370610521
DOI:10.35940/ijeat.E2737.0610521
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication

After copying the frame, T1 layer acknowledges the reception of the frame by sending the R Blk frame. In this case, two frames are exchanged, i.e. an I Blk and an R Blk. I Blk is evaluated by starting the timer when the data appears at SPI DD and stopping the timer when the frame is copied to buffer. R Blk is evaluated by starting the timer when the T1 layer generates the R Blk and timer is stopped when the SPI DD sends out the R Blk. Similarly, multiple I Blk and R Blk frames are exchanged until the entire C- APDU is transferred from host to SE. First I Blk frame and intermediate I blocks frames have more bit field as 1 in PCB byte. Last I block frame have the more bit field as 0 in PCB byte. When the last I block is received, T1 layers forwards the C- APDU to application layer and acknowledges by sending an R Blk. The sum of elapsed timer value for all the I Blk and R Blk frames gives the processing time at communication interface. This is part of **Receive path**.

Application layer processes the C-APDU and sends the R-APDU back to communication interface. Larger R-APDU is sent from SE to host in multiple I block frames. For every, I block frame host acknowledges by sending an R block frame. These frames are evaluated as described above. The elapsed timer value gives the time consumed at communication interfaces. This evaluation is part of **transmit path**.

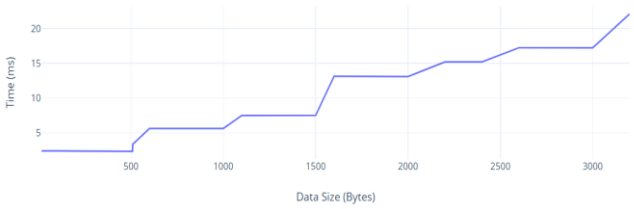

Fig 4: Graph plot - time consumed v/s data size

IV. THROUGHPUT

Total time consumed at communication interface is sum of time consumed at reception path and at transmit path.

$$\text{Throughput} = \frac{\text{Size of data transferred}}{\textit{Time taken to transfer the data}}$$

Fig 5: Graph plot - throughput v/s data size

V. ANALYSIS

In the graph as shown in fig 5, we see that throughput varies linearly as the data increases. Throughput is inversely proportional to time consumed at communication interface. For a given data size, throughput increases as the time consumed at communication interface decreases. Time consumed at communication interface is directly proportional to number of frames exchanged. Higher the number of frames exchanged for a given data, higher is the processing time at communication stack layer, hence throughput decreases.

If the T1 block size is 254 bytes, then a single I Blk frame can transmit data of size ranging from 1 byte to 254 bytes. Data of size 250 bytes can be transferred in single I Blk frame or multiple I Blk frames. When data is transferred using single I Blk frame, throughput is higher. If multiple I Blk frames are used, time at communication interfaces increases and hence throughput decreases.

Let data to be transmitted be x bytes

Let size of a T1 block be y bytes.

x >> y

$n = \frac{x}{y}$ if x mod y = 0

$n = \frac{x}{y} + 1$ if x mod y!=0

Optimal number of frames that should be used for transmission of the data to get higher throughput = (2* n) -1

VI. CONCLUSION

We have evaluated the throughput of SPI over T1 communication interface. We have also identified and analyzed the parameters that affect the throughput. Parameters that affect the throughput of SPI over T1 communication interface are buffer size at T1 layer, number of frames exchanged between the two devices and size of T1 block. Buffer size at T1 layer must be multiple of T1 block size to get better throughput. Data must be exchanged between host and SE with minimum number of frames to get higher throughput.

REFERENCES

1. YongSung Jeon, Yousung Kang, “Implementation of a LoRaWAN protocol processing module on an embedded device using Secure Element”, 2019 34th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC), JeJu, South Korea, 2019.
2. Marian Cingel, Marek Novak, Tomas Fryza, ”Characteristics of SPI Drivers in RTOS Environment”, 2017 27th International Conference Radioelektronika, Brno, Czech Republic, 2017
3. Abhay, Ganesh Krishna and Channabasappa Baligar, “Smart Card Reader Meeting ISO 7816-3 and EMV Level 1 Specifications using PIC24F Microcontroller”, International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-3 Issue-1, June 2013, pp. 70-73
4. ISO-IEC standard specification for T1 protocol: https://www.iso.org/obp/ui

AUTHORS PROFILE

Gurunath Reddy, is a M.Tech student at Department of Computer Science and Engineering, Rashtreeya Vidyalaya college of Engineering, Bengaluru, Karnataka. gurunathreddym.scn19@rvce.edu.in

Dr. Sharvani G. S., is working as Associate Professor at department of Computer Science and Engineering, Rashtreeya Vidyalaya College of Engineering Bengaluru, Karnataka India. sharvanigs@rvce.edu.in