Design of SMART (Secure, Multichannel, Adaptive, Real Time, Tiny) Gateway for Cyber Physical System

Mr. SUNIL TAMHANKAR
Department of Electronics Engineering
Walchand College of Engineering, Sangli. (MS),
INDIA
sunil.tamhankar@walchandsangli.ac.in

Dr. FARUK KAZI
Department of Electrical Engineering
V. J. T. I. Matunga, Mumbai(MS)
INDIA
fskazi@vjti.org.in

Mr. SACHIN PATIL
Department of Computer Science and Engineering
Rajarambapu Institute of Technology, Sakahrale (MS),
INDIA
sachin.patil@ritindia.edu

***Abstract*—** Cyber Physical systems (CPSs) are being increasingly deployed for complete or partial automation, in manufacturing and process industries, electric utilities, transportation systems and many other plants. Due to legacy physical infrastructure of such systems; interoperability and seam-less data transfer between devices operating on various protocol is a critical issue.

A gateway is a network node that connects two networks using different protocols on either side. Today in Cyber Physical System era gateway plays an important role in a communication system. The concept of SMART gateway is proposed which can able to provide **S**ecurity feature by introducing node ID and route filtering, **M**ultichannel functionality to transfer data in the desired form as streaming, polling, and live**, A**daptive in nature as per system requirements, **R**eal-time capability for live monitoring and control with **T**iny in nature in Size and OS. This SMART gateway will serve the desired requirements of Cyber Physical System and enhances the performance.

Keywords—CPS Cyber Physical System, BLE Blue Tooth Low Energy

1. Introduction

Cyber Physical Systems (CPSs) are electronic control systems that control physical devices like motors, pumps, and valves in the plant. In a networked environment, the security of the physical machines depends on the security of the electronic control systems, but cybersecurity is not typically considered.

CPSs integrate computational resources, communication capabilities, sensing, and actuation in an effort to monitor and control physical processes. CPSs are found in critical infrastructures such as nuclear power generation, electric power distribution networks, water and gas distribution networks, transportation networks, Unmanned Aerial Vehicles (UAVs), and advanced communication systems.

The main concern for CPSs is the availability of the physical devices. In the CPS due to insecure Internet-of-Things (IoT) devices in their industrial processes, the underlying security of their operations becomes increasingly vulnerable. Secure CPSs are necessary for keeping critical infrastructure safe.

A key difference between CPSs and traditional Information Technology (IT) systems is that CPSs interact strongly with the physical environment,

and the availability of the physical devices is the most important security aspect. However, CPSs are also cyber systems and are therefore vulnerable to cyber-attacks. In this, the communication with physical devices is an important challenge for designing system with security features.

The gateway communicates with sensor side node with short distance communication protocols which is a non-IP method, and with other devices server side or accessing nodes using IP on the other side. Here gateways work at the application layer and it needs to strip down the data coming in from the local or sensor network and structure it with a TCP/IP stack to enable communication with the server or other stations with an Internet service.

One of the disadvantages of the TCP/IP stack is that it is bulky and complex, and therefore requires a good amount of processing power and memory, that leads to more development time and usage of expensive devices. The complexity of the protocol results in sizable data packets, hence required power is more to send and receive. This embedded devices may not cater the need. As gateway plays an important role in the remote control and monitoring system. It is envisaged that wireless is an ideal solution for distributed sensors because it enables the easy mobility of sensors.

A. Gateway Limitations

Many gateways have finite local storage capacity with Limited processing power and RAM with these expandability becomes very complex.

The gateway must be evaluated in the context of its requirements, which has a limited ability to translate dissimilar concepts with the capability of protocol conversion, from short distance wired or wireless protocols to standard TCP/IP packets.

For the device configuration from a remote location, it is difficult to pass the messages through the gateway so bypassing the gateway is only alternative solution. So specifications of the gateway must clearly state that what information must be available through the gateway. As most of the gateways are application specific only, information access is limited through the gateway and that lead to difficulty in troubleshooting and for integrated applications prioritizing and other facility implementation is very complex.

Because of transmission speed difference and overhead of processing and translation time gets introduced there may be irregular delay at the gateway which is not suitable for certain applications.

2. SMART Gateway

The SMART gateway can mitigate the limitations of current gateway solutions and with additional functionality try to give a better solution.

Secure:

Device ID with Route/ Path filtering technique can be implemented so data coming from only authorized sensor is confirmed
For physical security, plant images can be captured and sent to the gateway over regular interval so the other side can get the information regarding plant status.
For server-side connection and network security, IPSec / VPN gateway can be implemented so that data can be travel securely over the internet.

Multichannel:

The gateway can capable to transfer data as per application requirement like polling, streaming data triggered or data delivery with regular or desired interval. This will help on the server side for data management and control.

Adaptive

Based on Type of data and priority the queue implementation with priority and queue management with traffic can be implemented,
From the data point of view from which device data is collected/ received the gateway will act depending on the criticality.

If at all due to many features overhead on Gateway performance controlled by buffer management and avoid data loss.

Real Time:

In the CPS it is very important to get the information regarding the time of event occurrence. So time stamp is important and using RTC is connected to sensor node this information is captured.

Only lower 5 digits of time stamp are sent with the data to decrease the payload.
Delay calculations are carried out and attempt is made to minimize the delay by implementing optimized algorithms.

Tiny in nature

As everything is built on an embedded platform with tiny OS with required functionalities in the gateway in an optimized way and mainly the power consumption problem gets solved which is otherwise tedious in a remote location.

3. Gateway design

Gateway design built on 32-bit MCU with Linux based OS ported on it. The process scheduling is done by Linux kernel. Mainly three processes as BLE data transfer, ZigBee polling data transfer and ZigBee data streaming transfer handled by the gateway. Each process has multiple threads running. One BLE radio module and two ZigBee radio modules are embedded on the gateway with their respective interfaces (UART or I2C) for connectivity[1].

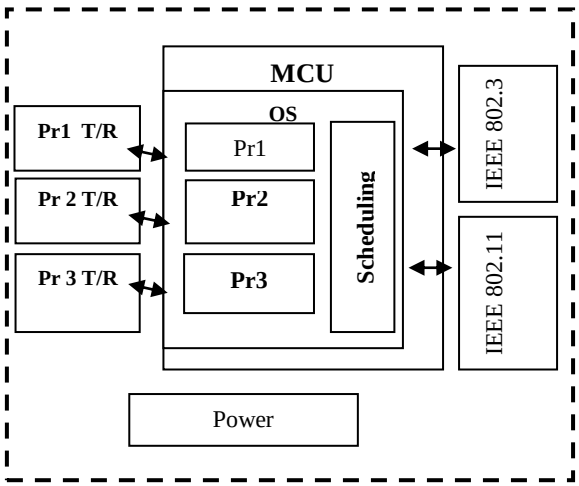

Fig.1. Block diagram of Gateway

For IP connectivity on the other side of the gateway, Ethernet, as well as Wi-Fi interface, is provided. SSL enabled TCP socket connection is created for polling data transfer over the internet using Open SSL[6]. For secure streaming data transfer, DTLS connection is used [8].

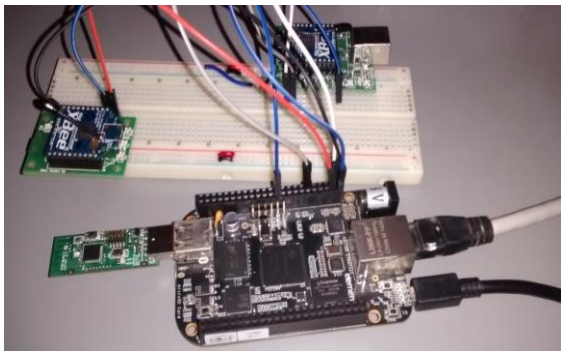

Fig. 2: Experimental setup

3.1 security

Using Device ID

At the time of sensor or device deployment in the system, we will provide unique ID to them and same can be used at the time of communication and gateway will identify the only authorized devices and it will not allow any other device communication.

Route Filter

A standard RSA algorithm for security is tried because of its complexity and communication overheads implementation on the embedded platform has many drawbacks like delay and more power requirement degrade the system performance, which is not suitable for the real-time environment.

Another option of Route filtering in this route through authenticated nodes which are deployed by the system administrator is only allowed path if packet travelled through any unknown node or unauthorized node is detected and gateway level and decision is made whether to keep the packet or drop the packet these scenarios are tested at the simulation level and verified that packet travel takes place with the authenticated route only and other packets get dropped this will help in detecting unauthorized node as well as intrusion detection up to certain level.

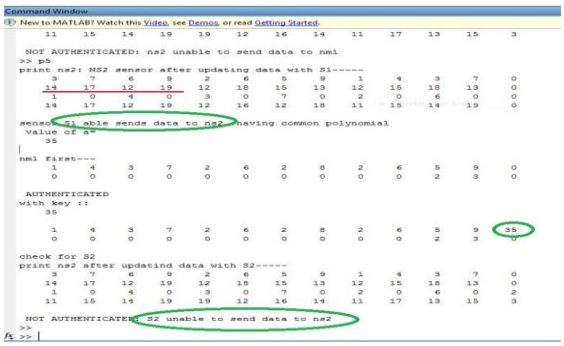

Fig.3: Route Filtering

On the IP side IPSec and SSL use for communication for secure data transfer over the channel. Experimentation is carried out with VPN connection and packets are captured in Wireshark for checking and testing. VPN is a better solution but in the case of a firewall, we required permission to transfer or access the data.

Physical security of plant

A camera is set to capture images of a critical section of the physical plant and captured need to be sent over the network in the regular interval of time so that physical state can be monitored for corrective measures.
Here sending images on the network consume higher bandwidth and that may hamper the other traffic so optimum time is decided such that it will pass the vital information without hampering the network traffic. This is tested with the interface of a web camera and the images transferred to the server with a delay of 180 ms.

3.2 Multichannel Capability

For the experimental results, we have selected wireless protocols BLE, Bluetooth, Zigbee same can be extended to any industry standard protocol.

Polling data transfer

To configure the sensor node for sending periodic data, the user needs to create appropriate profile according to a sensor attached to the node. The profile has values of interval duration, for data collection and sensor connection configuration.

Steps for polling data transfer

S1: The coordinator sends the user selected profile to the sensor node.
S2: According to the profile, ZigBee end device starts sending sensed data at specified intervals.
Coordinator collects the data and checks whether the data is the inappropriate format.
S3: If not, data gets rejected. If the data is authenticated then an acknowledgment is sent back to the sensor node.
At the gateway, the data is collected in a buffer. Collected data is sent to monitoring server using SSL enabled TCP socket where it gets stored in the database [7].
S4: Monitoring server sends back the acknowledgment response to the gateway. An authenticated user can monitor the data by logging in to the monitor using Web Browser.

Streaming data

Steps for data streaming transmission are as follows:

S1: Initialize the hardware serial with baud rate of 38400
S2: Store the sampled data in an array every 2 ms.
S3: After 32 samples make payload of the array for the packet with required destination address and checksum.
S4: Transmit the packet.
S5: For successful delivery of packet 32 ms. (approx.) time is required. Meanwhile, at the same time next packet will be ready for the following step back to the S1:

BLE data transfer sequence

Following are steps illustrates the network initialization and data transfer sequence for Bluetooth Low Energy (BLE)
BLE sensor node acts as peripheral and broadcasts advertisement on Advertisement channel for connection, and gateway BLE radio acts as central node and recognizes the peripheral after scanning. The user needs to accept the pairing with peripheral.

S1: The gateway sends service discovery request to the peripheral for available services in

GATT profile. To which peripheral provides a response with available services on sensor node device.

S2: From which central chooses the required service and requests the peripheral for reference to enable characterization of the service, for those characteristics the peripheral responses with the coefficients.

S3: Central writes the values to that characteristic to enable that sensor. Now sensor on the node becomes enabled.

S4: To read the sensor value, central obtains a reference to read characteristics. Value of those characteristics provides the sensor reading.

S5: Notify value request for the corresponding characteristic will provide sensor reading value when the parameter changes. Similarly, data streaming can also be done on BLE.

Collected data is transferred to monitoring server using SSL enabled socket. And the user can monitor the data by logging in to the server using a web browser.

Some results are carried out for polling, streaming and live data

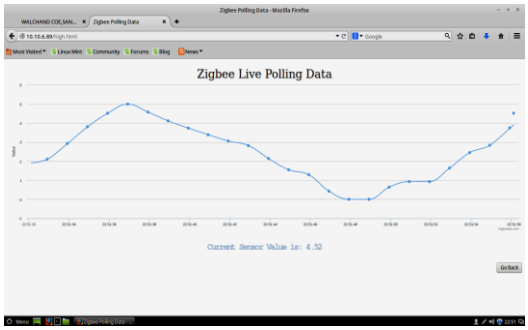

Fig. 4: ZigBee Polling Data

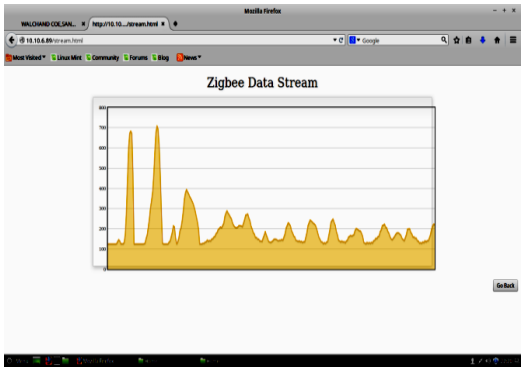

Fig. 5: ZigBee Streaming Data

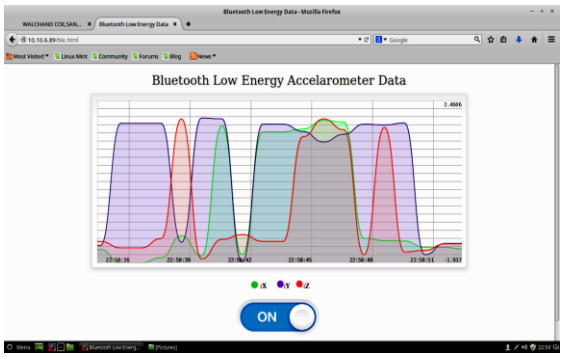

Fig. 6: BLE Live Data

3.3 Adaptive

When connected networks work at different speeds and combined together for moving data, the flow of packets from the faster network must be maintained in order to avoid a long queue, otherwise, it will affect as buffer bloat. Buffer bloat will exits when the higher speed network continues to send data packets at a rate more than the capacity of the other network and it leads to packet queue at the gateway level.

An unmanaged gateway causes the buffer full or overflow. This overflow causes packet drop and or increase in packet queue and creates a bottleneck that impedes the transfer of data to the slower connection. This also negatively impacts the timely prioritization of packets.

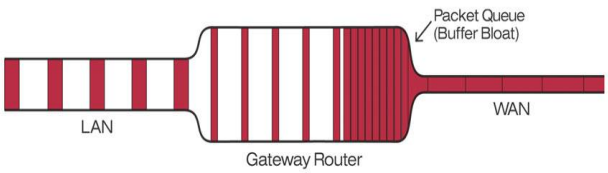

Fig. 7: Buffer Boat

A suggested buffer implementation scheme will adaptively balance gain between congestion situation and optimized as per to cache congestion. For minimum congestion scheme will tend to drop packets fairly in order to ensure access. For moderate congestion, with dropping packet reduces sending rate using scheduling algorithm that avoids the congestion. In congestion situation, the algorithm will tend to fairly drop packets, and with the flow control mechanism it will try meet the QoS requirements and reduces sending a flow

of packets in order to speed up the process of congestion release.
Buffer management or packet scheduling algorithms improves the performance of the system to have flow control with better conditions for transmission. This will make optimization in bandwidth and buffer management
A standard Random Early Detection (RED) algorithm implemented with Average queue size calculation and compare with maximum and minimum with average and decision is made to drop and introduce probability and en-queue packets

Calculation of average queue size is calculated based on old average and time when the queue is not empty.
The Adaptive RED algorithm implemented with target limit and average and process is repeated

3.4 Real Time

Data transfer from the sensor node to monitoring server is calculated for 100 samples. Delay for polling sensor is plotted and illustrated in fig. : 8.

Here data collected from sensor node which is immediately connected to the gateway. As the number of levels increases, the delay also increases. Here the number of hops is limited to two as we increase the number of hops for sensor node to gateway connectivity there is an increase in delay.
The calculated average delay is 63 ms. which is within the range of soft real-time system

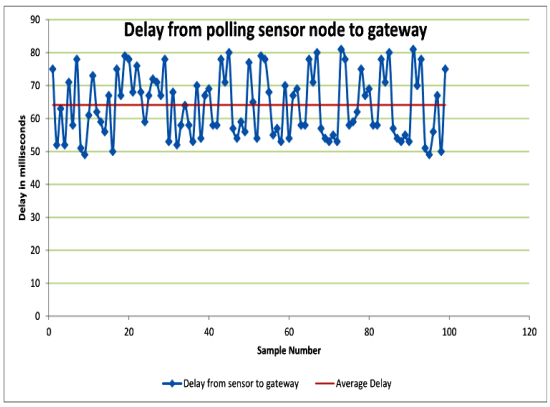

Fig. 8: Delay form polling sensor node

Delay for streaming ZigBee sensor is plotted in fig. : 9. It is difficult to calculate the delay in Bluetooth Low Energy. But from the reference[12] maximum delay for sensed data to reach the master is around 100 milliseconds.
The calculated delay for ZigBee is compared with the similar gateway [2] found to be less. The difference is mainly due to the more powerful controller and higher priority to the streaming process in the Linux scheduling.

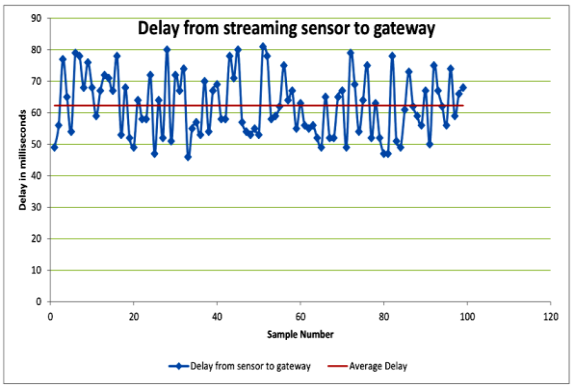

Figure 9: Delay form streaming sensor node

Time Stamping at sensor node:

A DS1307 RTC is connected to ZigBee polling sensor node. DS1307 time and calendar are converted to Unix timestamp. Only lower 5 digits of the time stamp are sent with data to decrease the payload.

Unix Time Stamp:

Unix Timestamp is a system for describing instants in time, defined as the number of seconds that have elapsed since 00:00:00 Coordinated Universal Time (UTC), Thursday, 1 January 1970, not counting leap seconds. It is used widely in Unix-like and many other operating systems and file formats. Because it does not handle leap seconds, it is neither a linear representation of time nor a true representation of UTC.

3.5 Tiny in nature

As entire Gateway is designed using embedded platform the size of entire product is tiny and also running on battery so biggest advantage is we can use this at remote location where power is the main problem but at the same time disadvantage of processing power and memory is there to overcome

these drawbacks we have to write very optimized algorithms so that it will not get overburdened and I running state at any point in time.

4. Conclusion

Proposed embedded gateway is tiny in nature and in terms of power consumption it achives 50% saving in power and runs on battery. An additional feature of security will have 29% overheads and that enables the packet filter and gateway level security. The multichannel capability will enable a single solution for multiple protocols as well as data delivery mechanism saves the cost for multiple device requirements. Buffer management avoids the bottleneck allow the traffic to its optimum capacity. RTC is giving the time information of occurrence of an event which is missing in other systems. As everything is built on an embedded platform its inherent limitations of computing power and memory capacity are there, hence this can be integrated with medium system applications.

References

[1] Mayur Hawelikar, Sunil Tamhankar "A Multi-Channel Embedded Gateway for Cyber Physical System with Security Feature" International Conference on Advancements in Automation, Robotics, and Sensing (ICAARS 2016) 2016.

[2] Nieminen, J., Gomez, C., Isomaki, M., Savolainen, T., Patil, B., Shelby, Z., Xi, M., and Oller, J. "Networking solutions for connecting Bluetooth low energy-enabled machines to the internet of things." Network, IEEE 28, 6 (Nov 2014), 83-90

[3] H. Y. Tung, K. F. Tsang, H. C. Tung, K. T. Chui, and H. R. Chi,"The design of dual radio ZigBee homecare gateway for remote patient monitoring," Consumer Electronics, IEEE Transactions on, vol. 59, no. 4, pp. 756–764, 2013

[4] Linlin, Z., Weimin, L., Wei, Z., and Shaowei, L. "The implementation of a secure RTP transmission method based on dtls." In Instrumentation, Measurement, Computer, Communication and Control (IMCCC), 2013 Third International Conference on (Sept 2013), pp. 379-383.

[5] Nanda, K., Nayak, K., Chippalkatti, S., Rao, R., Selvakumar, D., and Pasupuleti, H. "Web-based monitoring, and control of WSN using wingz (wireless IP network gateway for ZigBee)." In Sensing Technology (ICST), 2012 Sixth International Conference on (Dec 2012), pp. 666 - 671.

[6] Wei, X., Jian-fu, L., and Guo-dong, Z. "Applications of web technology in a wireless sensor network." In Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on (July 2010), vol. 5, pp. 227-230.

[7] Benocci, M., Farella, E., Benini, L., and Vanzago, L. "Optimizing ZigBee for data streaming in body-area bio-feedback applications." In Advances in sensors and Interfaces, 2009. IWASI 2009. 3rd International Workshop on (June 2009), pp. 150 -155.

[8] Brunelli, D., and Teodorani, L. "Improving audio streaming over multi-hop ZigBee networks." In Computers and Communications, 2008. ISCC 2008. IEEE Symposium on (July 2008), pp. 31-36.

[9] Chee Wooi Ten, Govindarasu Manimaram, Chen Ching Liu "Cybersecurity for Critical Infrastructures: Attack and Defense Modeling" IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans 40.4 (2010) 858-865.

[10] Xinyu Yang, Jie Lin, Wei Yu, Paul-Marie Moulema, Xinwen Fu, and Wei Zhao "A Novel En-Route Filtering Scheme Against False Data Injection Attacks in Cyber-Physical Networked Systems" IEEE TRANSACTIONS ON COMPUTERS, VOL. 64, NO. 1, JANUARY 2015

[11] C. Gomez, J. Oller, and J. Paradells, "Overview and evaluation of Bluetooth low energy: An emerging low-power wireless technology," Sensors, vol. 12, no. 9, pp. 11 734–11 753, 2012.

[12] V. Pimentel and B. Nickerson, "Communicating and displaying real-time data with WebSocket," Internet Computing, IEEE, vol. 16, no. 4, pp. 45–53, July 2012.

[13] G. Song, Y. Zhou, W. Zhang, and A. Song, "A multi-interface gateway architecture for home automation networks," Consumer Electronics, IEEE Transactions on, vol. 54, no. 3, pp. 1110–1113, August 2008.

[14] W. Chou, "Inside SSL: the secure sockets layer protocol," IT Professional, vol. 4, no. 4, pp. 47–52, Jul 2002.

[15] Eric Ke Wang, S. M. Yiu " Security Issues and Challenges for Cyber Physical System" IEEE/ACM International Conference on Green Computing and Communication 2010.

[16] Guangyu WU, JianSUN, Jie CHEN "A Survey on the security of Cyber Physical Systems" Springer Control Theory Tech, Vol. 14, No 1, pp 2-10, February 2016.

[17] Benazir Fateh, Govindarasu "Joint scheduling and Message for Energy Minimization in Interference-Aware Real-Time Sensor Networks" IEEE Transactions on Mobile Computing, vol. 14, no. 1, January 2015.