Turkish Journal of Computer and Mathematics Education
DOI: https://doi.org/10.17762/turcomat.v9i3.13906 *Vol.09 No.03 (2018), 1155-1162*

Research Article

Effective Methods for MAC Protocol Routeing in Cyber-Physical-System-Enabled Networks

Rahul Chauhan

Asst. Professor, Department of CSE (Computer sc)

GEHU-Dehradun Campus

Abstract: A Cyber Physical System (CPS) is a networking environment that uses wireless communication to keep tabs on the flow of physical events and take corrective measures as needed to keep the entire thing running smoothly. Cyber-physical systems, or CP-systems, are often referred to as "smart systems" because of the value they provide by providing intelligent services during emergency circumstances. Since Medium Access Control (MAC) plays a significant role in CPS applications, any modifications to MAC will have an effect on CPS performance. This thesis proposes a number of strategies for improving MAC in order to boost wireless network performance. Despite the fact that CPS is a hybrid network, efforts have been made to include some wiggle room into the more conventional "back off" process. Energy Hashed Virtual Back off Algorithm (EHVBA) is used, which is a back off approach that conserves power. This algorithm incorporates energy as a new method parameter to boost CPS performance. However, because MAC is crucial in CPS networks, the standard back off procedure needs some flexibility. To prevent interference in the unspotted mode of the 802.15.4 protocol, we give each device a priority and counter. Even though IEEE 802.15.4 may be breached by competing wireless technologies, problems only arise after a certain phase of medium access has been resolved.

Keywords: IEEE 802.15.4, Energy Hashed Virtual Backoff Algorithm (EHVBA), Medium Access Control (MAC), Cyber Physical System (CPS).

Introduction

Systems that are utilised to carry out certain tasks are referred to as "cyber," while the devices that carry out those tasks are referred to as "physical" in the context of Cyber Physical Systems. CPS denotes the consolidation of these two characteristics under a single authority. In practise, CPS functions as a command and control hub for distributed computing resources, issuing orders to connected computers to carry out a wide range of tasks. As a result, CPS hears back from people about these incidents. Using the Internet, CPSs may communicate with many systems and get insight into the goings-on in the real world. In addition, it can adapt to changing conditions in its environment when many network components are used in a CPS application. Accessing any channel also increases the likelihood of encountering complexity.

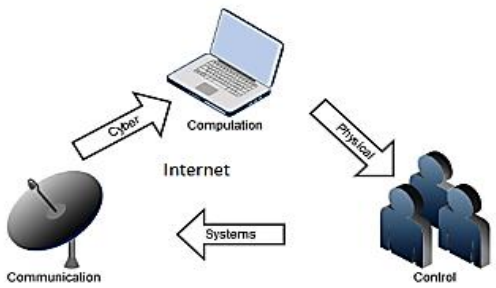

Figure 1. CPS Communication Scenario

Figure 1 depicts cyber as the process of calculating instructions and physical as the implementation of those instructions. For the system to work, the replies must be sent to the server. To demonstrate how the whole planet is linked to the Internet, the aforementioned procedure is carried out in a closed wireless loop. Cyber-Physical Systems (CPS) are often referred to as "smart" systems. The components of a cyber-physical system are the sensors and the actuators. That is to say, it is equipped with sensors and actuators for timely analysis and response. Collectively, these heterogeneous wireless networks make up what is known as a CPS.

Features of CPS

In 2006, the National Science Foundation (NSF) made the research of cyber physical systems a top priority. This NSF panel recognised CPS in 2007 as a cutting-edge area of embedded research for scientists looking to solve challenges using both software and hardware components. Wireless sensors and actuators in a CPS exchange data with one another and other devices through the web. Information is gathered by sensors or sensor cum actuators, which then pass on the information to the proper hardware to do the required actions.

As shown in Figure 2, the controller uses a wireless network to exchange data with the sensors and sensor cum actuator devices. Cyber physical systems are distinguished by features that are not shared by traditional computer networks. That's why we can't just call it a software or hardware system. CPS provides a mechanism to improve emerging technology. These goals are met by CPS's unique combination of characteristics, which set it different from both traditional wireless networks and cutting-edge sensor-based networks. In CPS, real-world objects are inextricably linked to the specific computational procedures needed to complete a job.

Cyber interference with a low-resource physical entity:

Integrated thoroughly: CPS relies heavily on close coupling between the physical world and computer processes for the execution of certain tasks.
Second, as CPS is a hybrid solution, it makes less use of resources like system bandwidth and operational capabilities than purely software-based solutions.
Third, CPS combines several networks into one: it is a wireless heterogeneous network with many channels of communication.
Time-based measurements vary in complexity, but CPS systems may be relied upon to regulate events that must take place at certain times or in specific orders.
Self-organization via dynamic system construction: CPS, being a complex computational system, may arrange its components in whichever way it sees fit.
a closed-loop framework in which the digital devices are always receiving feedback from the physical ones.
CPS is a reliable and secure system since it ensures the continuity and security of higher-level operations.
Merging of digital and physical processes: CPSs are designed to carry out automated processes in accordance with the instructions supplied to them.

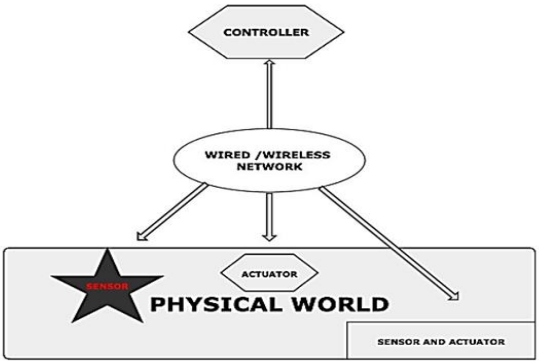

Figure 2 CPS Overview

Functionality of CPS

CPS plays a significant role in emergency management but is not typically regarded a study field. Sensors, input, computation, and action are all capabilities of CPS. CPSs, with the support of other distributed systems, should be efficient and well-designed so that the procedures may be carried out at a certain time or in an inaccessible area. These decentralised networks are made up of pre-configured hardware and software modules. Thanks to the cyber physical system, the digital age now has a face. Digital communication has evolved into a sophisticated means of communication in the modern world. Smart gadgets' ability to connect with one another has greatly improved the quality of human existence. This is because CPSs have many moving parts, some of which are time-based characteristics of hardware. Also, CPSs have efficient transmission in a wireless network since they mix different actions of physical entities with the computational operations. Figure 3 demonstrates how CPS carries out any given operation in response to orders received from the network's physical devices. Figure 3 from (Wang et al., 2010) explains the four phases that make up the functioning of CPS (Baheti and Gill, 2011). These steps include monitoring, communicating, computing, and acting. a) Monitor: This first phase allows the system to track any modifications made to the CPS (Lee, 2007) software. In addition to ensuring that the whole system operates well, it provides feedback based on what has already taken place. DC refers to the transmission of the gathered sensor data for use in communication. In step b) "communicate," information is gathered from the sensor devices and distributed to the different nodes in the CPS (Lee, 2007) based wireless network. Different procedures are used to dispatch the physically ready data to the next stage of processing. DA refers to the process of acquiring data from a wireless network for the purpose of calculation.

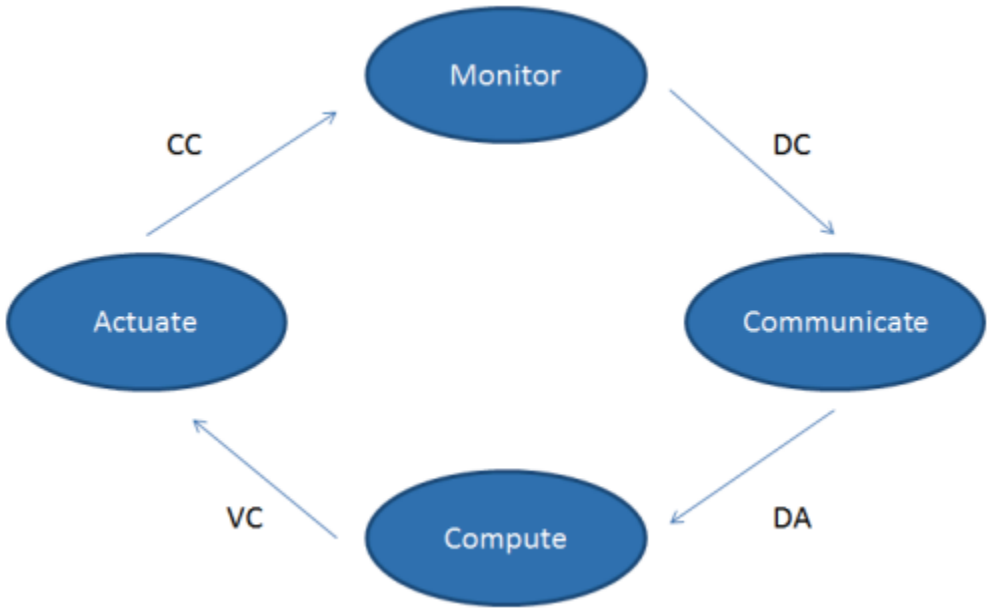

Figure 3 Functionality of CPS

Literature Review

By using a learning automata model, the authors of (Misra et al., 2013) alter the way we think about applications that combine Visual Basic and Computer Science. Since it is well-known that the characteristics of each wireless network vary in a CPS context, the number of channel access trials is tailored to the specifics of the network in question. As measured by average latency and amount of loss % during packet transmission, the approach had produced enhanced outcomes. The bandwidth range of a node is disregarded in this technique on

the assumption that this results in reduced energy consumption by the nodes. In the case of a wireless sensor network node requiring access to a medium, this is the norm.

Semi-Distributed Backoff (SDB) (Misra and Khatua, 2014) shows that consecutive collisions in an IEEE 802.11 protocol based wireless network may be avoided. There are two modes used in this process: sender mode (S-mode) and receiver mode (R-mode) (Misra and Khatua, 2014). At the outset, a counter value between zero and the total number of transmitting nodes is given to each node.

Lee (2006), Shi et al. (2011), and Wu et al. (2011) all describe emerging research into systems that combine the "real" and "virtual" worlds of computing. The many uses and effective results of CPSs are explored.

Guaranteed Time Slots (GTSs) are the foundation of the two-tiered collision avoidance system presented in (Huang et al., 2008). All devices are given priority at the root level, determined by the GTS request from the device. Priority is given to devices that need more GTSs. The coordinator sends out packets from nodes in accordance with the adaptive GTS mechanism known as Adaptive GTS Allocation (AGA). The beacon functionality of the IEEE 802.15.4 MAC protocol is used by this AGA technique. If the server is not actively processing requests, lower priority nodes will be examined. Node hunger was addressed by prioritising the highest-priority devices.

Two-level Medium Access Control in Cyber Physical System based Smart Wireless Networks

Using intelligent sensor nodes, a CPS-based Smart Wireless Network (CPS_SWN) is built for usage in high-tech buildings including smart homes and smart workplaces. This CPS_SWN operates in an IEEE 802.15.4 mode that does not make use of beacons (Xia et al., 2013; Sayuti et al., 2014). This wireless network employs smart sensor nodes that are all RFDs (Xia et al., 2013). These nodes are very well linked to the sink node, which is known as the Centre Coordinator (CC). The coordinator at the network's epicentre is seen as an FFD in WSANs (Xia et al., 2013), meaning it may talk to any and all RFDs that are connected to it. This CPS_SWN connects to the smart nodes using a star architecture. Take for granted that this network's smart nodes are immutable, and that their relative importance—and any associated countervalues—are determined only by their operational behaviour.

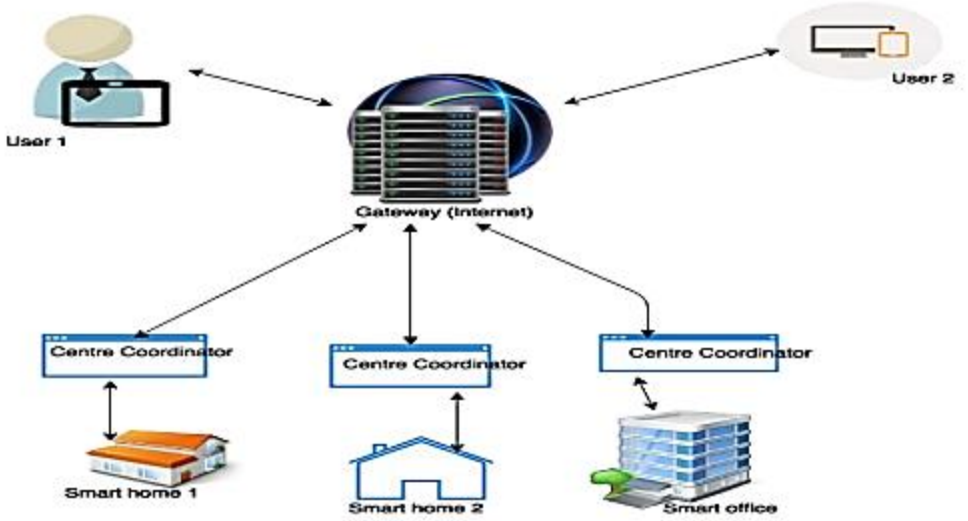

Figure 4. CPS based Smart Wireless Network

Figure 4 shows that the gateway node is linked online with the smart office and two smart residences. Gateway nodes operate as command centres, relaying information to the managed devices they are connected to. When

data is ready, it is sent to the Centre Coordinator (CC) from the smart houses. CC will send the information to the gateway node if it is not being used. The information is stored in the CC buffer in case Centre Coordinator is occupied. As CC idles, it will send the most crucial information to the gateway node as quickly as possible. If the gateway node discovers that the requested resource is available, it will proceed with the data transmission. The data is saved with a counter in a two-level buffer if the counter is not zero. High priority packets from nodes are stored in buffer1, while lower priority packets are held in buffer2. The data packet is discarded from the buffer1 and a negative acknowledgement is delivered to the associated CC when the counter value of the node's data reaches 4. As a result, PCMB employs the following approach in an effort to put into practise the aforementioned technique and prevent further crashes.

Experimental Observation

In this CPS-based smart wireless network, two smart houses are studied. Each of the 10 smart nodes in these smart houses has been given a priority cum critical value based on the tasks it performs. The door locks and fire alarm nodes that store life-saving information are prioritised. These nodes are permanently situated in a certain network. Each of these nodes acts as a relay for data (RFD) to the central controller, and they all use a star topology. Only other RFDs on the same network may be communicated with via CC. CPS_SWN's network performance is evaluated using NS2. Both the IEEE 802.11b protocol standard for gateway connections and the IEEE 802.15.4 protocol standard are utilised in a smart home. CPS_SWN is measured on a scale that takes into account packet throughput, collision ratio, packet delay, and packet loss rates. The simulation parameters and their values are shown in Table 1

Parameters	**Value**
Network Type	802.15.4 - PAN 802.11b - LAN
Traffic Type	CBR
Frequency Bandwidth	2.4GHz
Data Rate	802.15.4 - 250kbps 802.11b - 11Mbps
Simulation time	350s – 500s
Transmitter Power	802.15.4 - 1mW 802.11b - 1000mW
Transmission range	802.15.4 - 75m 802.11b - 140m
Carrier Sense Sensitivity	-85dBm for 802.15.4
Synchronization Mode	802.15.4 -Non-beacon 802.11b - Infrastructure

.

Table 1. PCMB Simulation Parameters

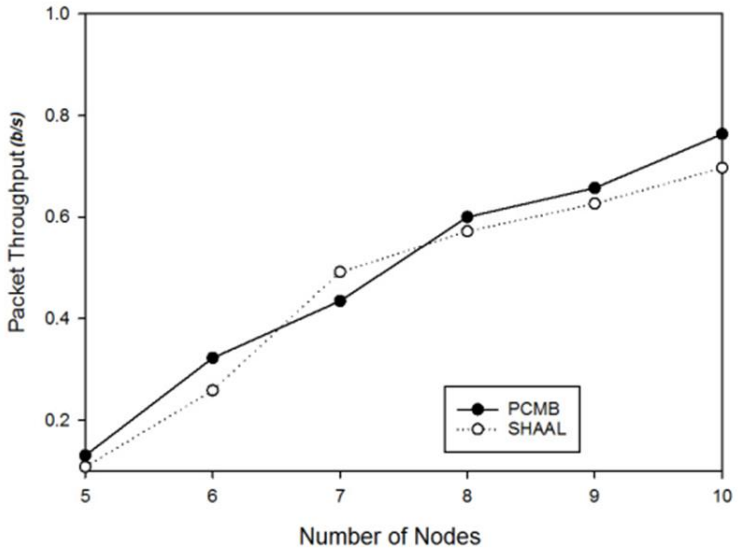

Figure 5.Packets throughput between PCMB and SHAAL

Figure 5 shows a head-to-head contrast between the PCMB gateway and the SHAAL system in terms of the percentage of packets that were successfully sent. From the graph, it is clear that the packet transmission throughput reaches about 80% as the number of nodes grows, but in the SHAAL technique, it reaches just 65%.

The collision ratio between the PCMB and SHAAL methods is shown in Figure 6. The estimated collision ratio is between 12 and 23 percent in both methods. However, with the PCMB technique, the collision ratio at the gateway is not more than 20%, which is a huge step forward over the SHAAL approach. While the SHAAL system places more emphasis on Ambient Assisted Learning, it cannot compete with PCMB on a large enough scale.

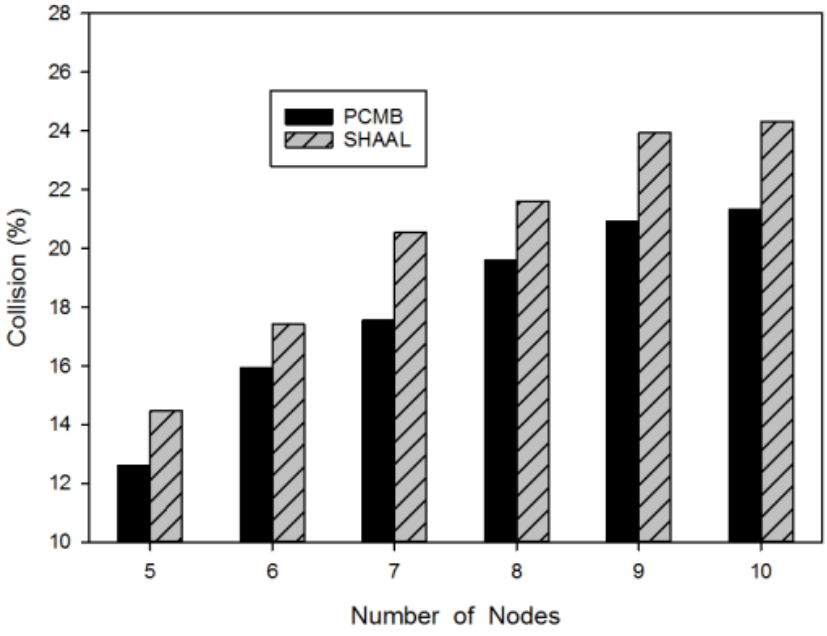

Figure 6 Comparison of PCMB and SHAAL Collision ratio

Any system suffers a performance hit due to packet latency. However, in priority-based systems, more delay actually speeds up the delivery of packets. Channel use in the PCMB and AAL (Sayuti et al., 2014) of the SHAAL system is shown in figure 6. Delay increases in PCMB approach when more data packets are scheduled at the gateway. This is done to guarantee the quickest possible transmission of mission-critical information. Figure 6 shows that the maximum delay ranges from 25ms in the SHAAL approach to 30ms in the PCMB method.

Conclusion

Most collision avoidance methods in the literature are time slotted modes of wireless sensor and actuator networks. The unslotted mode of sensor based MAC protocol was only utilised by a handful of methods. Multiple investigations concluded that collision avoidance is performed mostly at the stage level rather than at subsequent stages. The suggested solutions start with wireless networks that are mobile and progress to a MAC protocol based on a cyber physical system to prevent collisions, taking into account the aforementioned difficulties. And in order to avoid channel access collisions in sensor-based wireless networks.

References

1. Antonescu, B. and S. Basagni, S. (2013). Wireless body area networks: challenges, trends and emerging technologies. Proceedings of the 8th International Conference on Body Area Networks, Brussels, Belgium, pp. 1-7.
2. Atzori, L. , A. Iera and G. Morabito (2010). The Internet of things: A survey. Computer networks, Vol. 54, No. 15, pp. 2787-2805. Baheti, R. and H. Gill (2011). Cyber-Physical Systems. The Impact of Control Technology, IEEE Computer Society, Vol. 12, pp. 161-166.
3. Banerjee, A. , S.K. Gupta, G. Fainekos and G. Varsamopoulos (2011).Towards Modeling and Analysis of Cyber-Physical Medical Systems. In Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies, ACM, New York, USA, pp. 154-158.
4. Bao, L. , S. Liao and B. Liu (2009). Scheduling Heterogeneous Wireless Systems for Efficient Spectrum Access. EURASIP Journal on Wireless Communications and Networking, Vol. 2010, No. 45, PP. 1-14.
5. Broy, M. (2013). Challenges in Modeling Cyber-Physical Systems. Proceedings of the 12th International Conference on Information Processing in Sensor Networks, ACM, New York, USA, pp. 5-6.
6. Cardenas, A.A. , S. Amin and S. Sastry (2008). Secure Control: Towards Survivable Cyber-Physical Systems. The 28th International Conference on Distributed Computing Systems Workshops, IEEE, Beijing, pp. 495-500
7. Chen, A. W. (2010). Enhanced MAC Channel Selection to Improve Performance of IEEE 802.15.4. International Journal of Innovative Computing, Information and Control, Vol. 6, No. 12, pp. 5511-5526
8. Conti, M., S.K. Das, C. Bisdikian, M. Kumar, L.M. Ni, A. Passarella, A., George Roussos, G. Tröster, G. Tsudik, and F. Zambonelli (2012). Looking Ahead in Pervasive Computing : Challenges and Opportunities in the era of Cyber–Physical Convergence. Pervasive and Mobile Computing, Vol.8, No.1, pp.2-21
9. Gao, R., F. Xia, L. Wang, T. Qiu, and A. Vinel (2011). Performance Analysis of nonBeaconed IEEE 802.15.4 for High-Confidence Wireless Communications. In Proceedings of the Baltic Congress on Future Internet Communications, Riga, Lativa, pp.83–89
10. Gubbi, J. , R. Buyya, S. Marusic and M. Palaniswami (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, Vol. 29, No. 7, pp. 1645-1660.
11. Gunes, V. , S. Peter, T. Givargis and F. Vahid (2014). A Survey on Concepts, Applications and Challenges in Cyber-Physical Systems. KSII Transactions on Internet and Information Systems, Vol. 8, No. 12, pp. 4242-4268

12. Hatcliff, J., A. King, I. Lee, A. Macdonald, A. Fernando, M. Robkin, E. Vasserman, S. Weininger and J. M. Goldman (2012). Rationale and Architecture Principles for Medical Application Platforms. In IEEE/ACM Third International Conference on Cyber-Physical Systems, Beijing, pp. 3-12
13. Haque, S. A. , S.M. Aziz and M. Rahman (2014). Review of Cyber-Physical System in Healthcare. International Journal of Distributed Sensor Networks, Vol. 2014, Article ID. 217415.
14. Kaur, G. , K. Malik and K. Ahuja (2013). Impact on power consumption of zigbee based home automation network using various traffic. International Journal of Future Generation Communication and Networking, Vol. 6, No. 6, pp. 17-24
15. Krishna, P. V. , S. Misra, V. Saritha, H. Agarwal and N. Chilamkurti (2013). Learning Automata-based Virtual Backoff Algorithm for Efficient Medium Access in Vehicular Ad Hoc Networks. Journal of Systems Architecture, Vol. 59, No. 10, pp. 968-975.
16. Lee, I. , O. Sokolsky, S. Chen, J. Hatcliff, E. Jee, B. Kim, A. King and K.K. Venkatasubramanian (2012). Challenges and Research Directions in Medical Cyber– Physical Systems. Proceedings of the IEEE, Vol. 100, No. 1, pp. 75-90.
17. Macana, C. A. , N. Quijano and E. Mojica-Nava (2011). A Survey on Cyber Physical Energy Systems and their Applications on Smart Grids. IEEE PES Conference on Innovative Smart Grid Technologies, Medellin, pp. 1-7
18. Misra, S. , P. V. Krishna, V. Saritha, H. Agarwal, L. Shu and M. S. Obaidat (2013). Efficient Medium Access Control for Cyber-Physical Systems with Heterogeneous Networks. Systems Journal, IEEE, Vol. 9, No. 1, pp. 22-30
19. Mounib, K. , G. Mouhcine and T. M. Hussein (2012). Priority-Based CCA Periods for Efficient and Reliable Communications in Wireless Sensor Networks. Wireless Sensor Network, Vol. 4, No. 2, pp. 45-51.
20. Pereira, V. , J. S. Silva, J. Granjal, R. Silva, E. Monteiro and Q. Pan (2011). A taxonomy of wireless sensor networks with QoS. In Proceedings of the 4th IFIP International Conference on New Technologies, Mobility and Security, Paris, France, pp.1–4
21. Sampigethaya, K. , and R. Poovendran, R. (2013). Aviation cyber–physical systems: foundations for future aircraft and air transport. Proceedings of the IEEE, Vol. 101, No. 8, pp. 1834-1855.
22. Sayuti, H., R. A. Rashid, A. L. Mu'azzah, A. H. F. A. Hamid, N. Fisal, M. A. Sarijari, A. Mohd, K.M. Yusof and R.A. Rahim (2014). Lightweight Priority Scheduling Scheme for Smart Home and Ambient Assisted Living System. International Journal of Digital Information and Wireless Communications, Vol. 4, No. 1, pp. 114-123.
23. Shafi, Q. (2012). Cyber Physical Systems Security: A brief Survey. 12th International Conference on Computational Science and its Applications, IEEE, Salvador, Bahia, Brazil, pp. 146-150.