Issues and Challenges in the Integration of Wireless Sensor Network and IOT

Mamatha T.
Asst. Professor
RVCE, Bangalore

Smriti Srivastava
Asst. Professor
RVCE, Bangalore

Aishwarya, PhD
Professor & HOD
Atria Institute of Technology

ABSTRACT
Living in smart world where every entity is connected requires collaboration of different research communities. The interaction among these communities like IOT, PC, MC, WSN and CPS will speed the progress towards building a smart world which includes smart cities, smart cars and smart homes.

Building a smart world requires solution towards this collaboration, like communication among heterogeneous entities which pose challenges like architecture, data fusion, security and identifying useful information. Research in this area is open with endless issues in hand. Generalization of the common data format is required. In this paper challenges and issues of integration of WSN and IOT would be addressed with Fault tolerant approach proposed.

General Terms
Emerging Technology.

Keywords
IOT, WSN, Issues, Challenges.

1. INTRODUCTION
In the near future human being will be living in an environment where every entity surrounding will have intelligence built in them. And will have capability to exchange information with us. Whether be it a garment or shoes or plantation or wood surrounding us. This interaction between living and non living entity is possible by embedding computational capabilities in these entities. Building a smart world like smart car, smart homes to smart bracelet requires integration of different research communities like IOT, MC, PC and WSN.In fact one of the most important element of IOT paradigm is WSN [1].The fundamental pillars towards building a smarter world are sensors.IOT and WSN would impact positively the qualitative living in the world with safe transportation, monitoring energy consumption of smart building and checking on delays in transportation. In general a smart world would contribute in large towards reducing global warming. Systems will synergistically interact with each other to build holistic, new, common and unpredictable services. Integration of two research communities, WSN and IOT must be carefully investigated since sensor node joins the Internet dynamically. There is lot of issues involved with this integration. This paper presents different approaches of integration of WSNs and Internet, issues and challenges.

2. LITERATURE REVIEW
Tables 1 list the different integration approaches and their challenges.

Table 1. Review of Different Integration approaches and Challenges

Title of the paper	Literature Review
1. Wireless Sensor Networks and the Internet of Things: Selected Challenges[1]	• WSN is integrating into IOT, during this process issues and challenges involved in the integration, is addressed. • The paper discusses about different integration approaches like using a single gateway between independent WSN and internet. Second is Hybrid approach uses more than one gateway. Last approach is Access point where the distant between the sensor and internet is one hop. • The drawback of these approaches dynamically nodes cannot be added to network. • Challenges of sensor nodes are discussed where node is give additional responsibility like Security, QOS and network configuration. • This approach seems impractical since nodes are resource constraint.
2. Wireless Sensor Networks and the Internet of Things: Do We needs a Complete Integration?[2]	• This paper highlights on security challenges that arises in integrating WSN with IOT. • Different integration approach is discussed to connect both the infrastructure, WSN and IOT at the network level. Stack based, Topology Based • The factors determine the integration approach is Resilience, user authentication and

	authorization , Accountability ,Functionality ,network redundancy and protocol optimisation discussed
3. Integration of Smart Sensor Networks into Internet of Things: Challenges and Applications[8]	• With advancement in MEMS technology and increased computational power of processor WSN can be applied to large number of areas like health, military application, environment monitoring. • This paper discuss about different hardware and software security challenges in collaborating WSN and IOT will be
4. Fault Tolerance in Wireless Sensor Networks[6]	• The paper discuss about fault detection and recovery mechanism in WSN. • Different types of fault is discussed and classified. • Different sources of fault in WSN application are node faults which could be malfunctioning of hardware or software component. • Another type of fault is network fault which may be due to link failure or software bug in routing layer. • The third type of fault is sink fault, a sink is node that collects and processes data from the entire network and sends it to backend system, and this can be subjected to bugs which can lead to loss of data. • Fault leads to failures. The different failures in WSN are classified as Crash, timing ,value and arbitrary • The different fault detection techniques discussed here are self diagnosis, group detection and hierarchical detection. • The different fault recovery techniques are Active replication in WSN and Passive replication in WSN.
5. WSN Gateways Fault Tolerance for Surveillance Transmission in Smart Grid Communication[7]	• This paper discusses about fault tolerance of gateway in smart grid communication. • Three types of faults: single, multiple and area fault have been discussed. • Proposes a network model with backup node attached to the transmission line for fault tolerance. The backup node is placed next to gateway node in the direction of relay. The topology considered here is linear topology, in case of failure of gateway node the redundant data in backup node is relayed hop by hop fashion. • Simulation result shows that network model is suitable for fault tolerant in wireless sensor network for distributed power transmission in smart grid.

3. ISSUES

- One of the issues is deciding on ownership of the data collected.
- Another issue is giving control to the machine for making decision which may result in unpredictable affects on the society and the environment. For

example: a refrigerator requesting replenishment for milk and butter at the local store for its owner, or as complex as a robot that has been programmed to survive in a harsh environment that originally did not foresee human interaction [5].

4. INTEGRATION

To leverage the benefits of IOT and WSN, it is necessary to know different types of integration approaches that can be used to connect both infrastructures. Approaches can be further classified into two categories: Stack Based and topology based.

In **Stack based** Approach the integration between WSN and IOT requires similar type of network stack or a compatible network layer protocol to enable them to exchange information. The interaction between the external internet host and the sensor nodes happens via a centralized device such as base station. The base station routes all data stream and queries between WSN and external entities via web service interfaces. This approach is categorized as Front-End Solution**.**

In second approach of Stack based classification that is **Gateway Solution**, the base station will acts like an application layer gateway. The difference between these two approaches lies in the fact that sensor node provide web service interfaces to external entities without altering their lower layer protocol.

In the third approach, **TCP/IP Solution**, sensor nodes are considered to be full fledged elements of internet .This approach[1] uses compatible set of protocol such as 6LOWPAN in 802.15 .4 networks that enables low power devices to participate actively in IOT.

In Topology based classification the actual location of the node that provides access to internet is considered for integration. This can be further classified into three categories: Independent network, hybrid network and access network.

Nodes, gateways and software form the main component of WSN.The gateway acts like a network coordinator, collects measured data and bridges to the network for further processing.

The above three approaches of topology based are basically classified on number of gateways used and how they connect WSN and Internet.

Independent Network consists of single gateway connecting WSN and internet. This approach is prone to network failure due to single gateway.

This can be overcome by using several gateway and access point ensuring network robustness. Hybrid based is a fault tolerant approach where there are several gateways with direct access to internet. Redundancy of gateway is tolerable as compared to network failure with single gateway. The access based approach is a tree based which enables direct access to internet via single hop.

5. PROPOSED MODEL

In a regular system where there is no fault tolerance of the gateway, dysfunctioning of the gateway will bring down the entire network.

It becomes impossible to route the data sensed by WSN to forward it to the internet without gateway. Especially in critical application which works on hard real time data such as health monitoring. Hence there is a need for fault tolerance in gateway.

Fault tolerance of gateway will enable a network to continue to operate properly in the event of the failure of gateway. Tolerance to gateway failure is important to the robustness of integration of IOT and WSN.

Placing too many Gateways will, on one side improve the throughput and reduces congestion but on the other side increase interference and cost [4].

In Hybrid approach where several gateways are placed for fault tolerance can lead to problems like increase in cost, inference and simultaneous usage of all the gateways may not add to the benefit of fault tolerance. Hence in this approach a technique is proposed where the secondary gateway which is the backup gateway is activated only in the event of failure of main gateway or primary gateway.

In the proposed model works as follows

Hardware failure of the gateway is considered in this proposed model.

1. IOT element which wants to query the WSN network or vice versa should establish connection to Primary gateway by sending connection requests message to gateway.
2. Once the connection is established between IOT element and WSN through primary gateway, messages are routed through and fro.
3. To ensure the reliability of communication between IOT and WSN, the backup gateway receives periodic active message from primary gateway.
4. In this course if primary gateway is establishing connection with any device, then the communication details will also be sent to the backup gateway.
5. If in a defined amount of time acknowledge is not received by the backup gateway, we consider the primary gateway has failed. The backup gateway takes over the role of primary gateway.

5.1 Iot Gateways

A device is needed to connect the IOT elements to internet, which should be capable of handling different data formats and parse them. It should also be able to handle different communication protocols. This bridging device is the IOT Gateway.

Identifying when there is a possibility of gateway failure.

This approach can be beneficial in the following ways.

1. Reduction in the cost of maintaining all the gateways at the same time.
2. Reduction in inference.
3. Reduction in the usage of the bandwidth

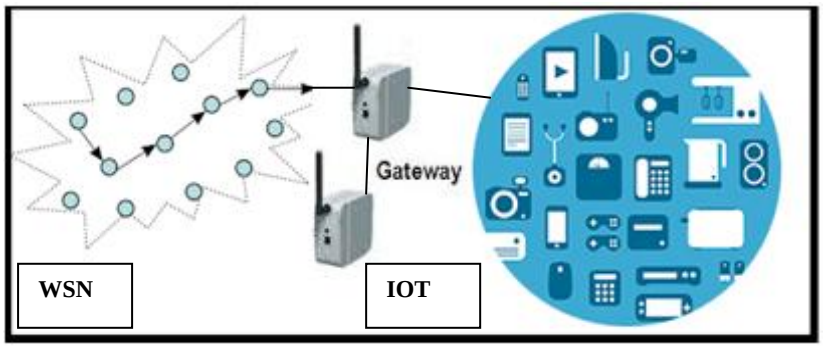

Fig 1: Integration of IOT and WSN

6. CONCLUSION

In this paper various issues and challenges in the integration of IOT with WSN has been discussed. Gateway plays an important role in the integration of IOT and WSN. Failure of the gateway can bring down the entire network to stand still. In order to increase the reliability of the Network there is need for a fault tolerate gateway. Proposed approach considers hardware failure of gateway with secondary gateway taking over the role of primary gateway in case of failure.

Implementation and link failure must be considered in the future for reliable integration of WSN and IOT.s

7. REFERENCES

[1] Delphine Christin, Andreas Reinhardt, Parag S. Mogre, Ralf Steinmetz," Wireless Sensor Networks and the Internet of Things: Selected Challenges", Multimedia Communications Lab, Technische Universit¨at Darmstadt Merckstr. 25, 64283 Darmstadt, Germany.

[2] C. Alcaraz, P. Najera, J. Lopez, and R. Roman, \Wireless Sensor Networks and the Internet of Things: Do We Need a Complete Integration?" 1stInternational Workshop on the Security of the Internet of Things (SecIoT10), pp. xxxx, 2010.

[3] "Internet of Things in 2020: Roadmap for the Future," 2008,online,http://www.smartsystemsintegration.org/public/internet-of-things.

[4] Smriti Srivastava, Anant Kumar Jaiswal," Clustering based Load Balanced Gateway Placement Approach", International Journal of Computer Applications (0975 – 8887) Volume 63– No.5, February 2013.

[5] *http://www.iec.ch/whitepaper/pdf/iecWP-internetofthings-LR-en.pdf.*

[6] Sushruta Mishra , Lambodar Jena ,Aarti Pradhan ," Fault Tolerance in Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, October 2012, Volume 2, Issue 10, October 2012, ISSN: 2277 128X.

[7] Kaixuan Wang1, 2, Xuesong Qiu1, Ning Fu3, and Haijian Yang3," WSN Gateways Fault Tolerance for Surveillance Transmission in Smart Grid Communication", Journal of Sannella, M. J. 1994 Constraint Satisfaction and Debugging for Interactive User Interfaces. Doctoral Thesis. UMI Order Number: UMI Order No. GAX95-09398., University of Washington.

[8] Dan Partynski ; Dept. of Math. & Comput. Sci., Univ. of San Diego, San Diego, CA, USA ; Simon G. M. Koo," Integration of Smart Sensor Networks into Internet of Things: Challenges and Applications", Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing

[9] C.P. Mayer. Security and Privacy Challenges in the Internet of Things.KiVS Workshop on Global Sensor Network, 2009.

[10] J. Claessens. Trust, Security, Privacy, and Identity perspective. Panel on Future Internet Service Offer, 2008.

[11] R. Roman, J. Lopez. Integrating Wireless Sensor Networks and theInternet: a Security Analysis. Internet Research, Vol. 19, no. 2, pp. 246-259, 2009.

[12] D. Christin, A. Reinhardt, P.S. Mogre, R. Steinmetz. Wireless SensorNetworks and the Internet of Things: Selected Challenges. 8th GI/ITG KuVS Fachgesprch "Drahtlose Sensornetze",2009.

[13] "Internet of Things in 2020: Roadmap for the Future," 2008,online,http://www.smartsystemsintegration.org/public/internet-of-things.

[14] Smart Energy Alliance, online, http://www.smart-energyalliance.com/solutions/ip-to-the-field/.

[15] Crossbow Technology, online, http://www.xbow.com.