IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

Integration between WSN (Wireless Sensor Networks) and IoT (Internet of Things)

Rashmi Raj[1], Amitesh Kumar[2]

Computer Science Department, Poornima Group of Institutions Jaipur, Rajasthan, India[1,2]

Abstract: Wireless sensor networks (WSNs) are increasingly leasing in impact in our day to day lives. They are experiencing a wide range of applications in various fields, including health maintenance, served and enhanced-living scenarios, industrial and production monitoring, control networks, and many other topics. In future, WSNs are expected to be incorporated into the "Internet of Things", Where sensor nodes join the Internet dynamically, and use it to catch together and take out their tasks. However, when WSNs Suit a part of the Internet, we must carefully investigate and analyze the security of involved with this integration. In this paper, we evaluate different approaches to incorporate WSNs into the Internet and outline a set of challenges.

Keywords: Web; Internet of Things; Net; Security.

I. INTRODUCTION

Wireless sensor nets, it's misguided thinking into this mess attention worldwide WSN these instructions are relevant to an intellectual follow the key enablers for the "internet (I trust) where WSNs will play an important role in future "cyberspace" by collecting surrounding context and environment information the innovation of integration of WSNs into things over "the promotion of new technology sciences" for scientific communities. The research observes about into WSNs for IOT is needed in everyday lives. The future Internet, designed as an "Internet of Things" is expected to be "a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols" [1].

Plucked out by a unique address, any objective, including computers, sensors, RFID tags or mobile telephones will be able to dynamically join the network, collaborate and cooperate efficiently to carry out different tasks. Including WSNs in such a scenario will open new offices. Encompassing a wide application field, WSNs can play an important part by collecting surrounding context and environment data. Even then, deploying WSNs configured to access the Internet raises novel challenges, which need to be tackled before taking advantage of the many benefits of such integration. The primary contributions of this report can be summarized follows: We look at WSNs and the Internet holistically, in Line with the vision where WSNs will be a component of an Internet Of Things. Thereby, we identify a representative diligence scenario for WSNs (see Section II) from the multidimensional WSN design space [2], in lodge to obtain insights into the issues Involved with the integration. These example applications Scenarios, open up different schemes for integrating the WSNs Into the Internet, which we confront and compare in Section III. A closer investigation of the integration possibilities, and then helps identify critical challenge, which need to Be addressed if the full potential of the integration of WSNs And the Internet has to be solved. Lastly, in We summarize our discussion, giving pointers for potential resolutions to address the identified challenges while regarding The resource limitations present in common WSN nodes. We also discussed about the what is solution and application of this challenges, security through the gateway in this topic.

II. PICKED OUT WSN APPLICATION

The wireless sensor network field can be split into three main classes agreeing to [3] Supervising objects, supervising space and supervising interactions between objects and space[9]. The propose categorization can be extended by an additional category monitoring human beings. One object lesson of the first category is environmental monitoring. WSNs are deployed in particular environments, including glaciers [4], forests [3], and mountains [2] in order to gather environmental parameters during long stops. Temperature ,moisture or light sensor readings allow analyzing environmental Phenomena, such as the influence of climate change on the rock fall in permafrost areas [2]. The second category centers on observing particular object structure, supervising is one of the possible instances of this category. By sensing modes of vibration, acoustic emissions and responses to mechanize modifications of bridges [6] or buildings [5] indicating potential breakages of the expression may be discovered. Supervising interaction between objects and space is the combination of both previous categories and includes monitoring environmental threats like floods [8] and volcanic activities [10]. Presenting an extension to the presented classification, the last category focuses

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

on supervising human beings. Worn close to the torso, the deployed sensors can gather acceleration information and physiological parameters like heartbeat rate. Especially in applications in the medical arena, such deployments may help diagnose bipolar patients and supervising elderly people in a home care scenario . The suggested classification, and particularly the selected deployments, illustrate the high diversity of WSN applications in term of supervising events and environments. Good for the Internet of Things, this significant scenario variety must however be learned into account by considering suitable approaches for the WSN integration into the Internet.

III. COSOLIDATION APPROACHES

Connecting WSNs to the Internet is possible in the three main approaches mentioned by [12], differing from this integration degree into the Internet structure. Currently adopted by most of the WSNs accessing the Internet, and presenting the highest generalization between networks.

A. Independent Networks

First proposed approach (Fig. 1) Consists of connecting both independents and the Internet through a single gateway:

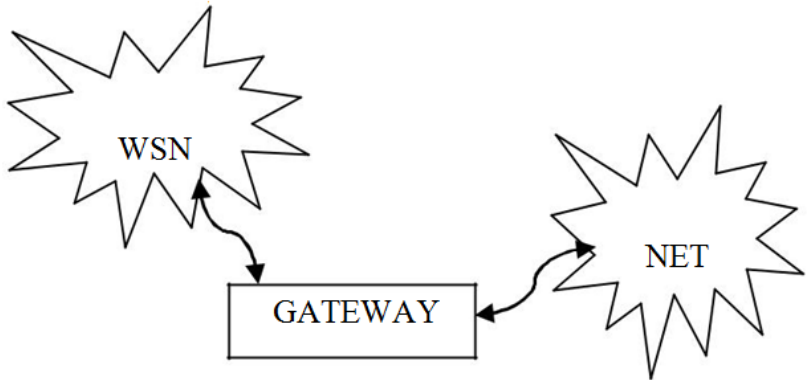

Fig. 1. Independent network

B. Hybrid Network

Approach (Fig.2) forms a hybrid network composed of both considered network structures remain independent, but few dual sensor nodes can access the internet.

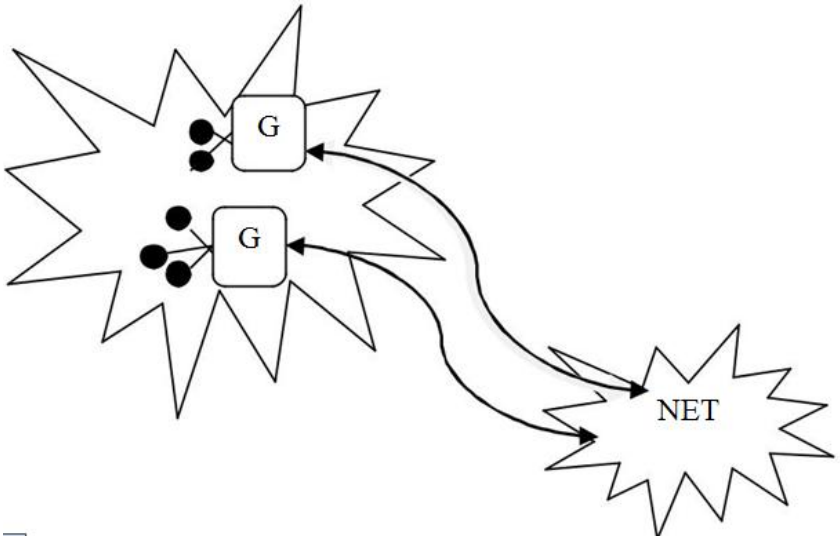

Figure 2: Hybrid network

C. Access Point.

Illustrated by Fig. 3, the last approach is inspired from current WLAN structure and forms a dense 802.15.4 access point network, where multiple sensor nodes can join the Internet in one hop.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

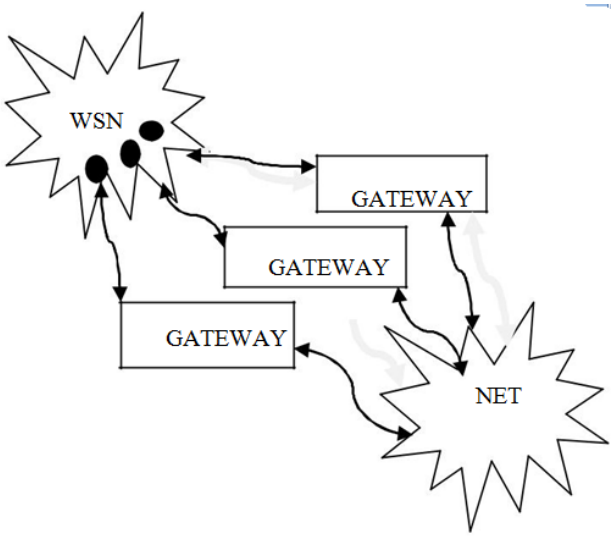

Fig. 3. Access Point Networks

It is obvious that the first approach gives a single period of failure due to the gateway uniqueness. Gateway dysfunction breaks down the connection between both WSN and the Internet networks. With several gateways and access points, the second and third scenario doesn't present such weakness. Ensuring network robustness, they may therefore be preferred. The choice between both remaining integrating approaches is influenced by the WSN application scenario. Allowing covering important distances, the second approach can been is aged for WSNs organized in a network topology. Consequently, this attack would be especially adapted to deployments belonging to the first "monitoring space" and the second "monitoring interactions between objects and space" categories previously introduced in the proposed application classification. By providing Internet access in one-hop, the third and last approach can be adopted by WSN applications requiring low latency and therefore direct connections. Presenting mainly star topology, the concerned WSNs can conserve such organization by accepting a central gateway instead of a common base station without Internet access. By studying the previous WSN application classification, this third approach can be suited for objects and human beings monitoring and may be employed in the [3], [5], [6], deployments for example. Nonetheless, both second and third integration approaches support only static network configuration. Indeed, each new device wanting to connect the Internet needs a time-consuming gateway reprogramming. Thus, the flexibility wanted by the future Internet of the Tings cannot be accomplished by both approaches in their current configuration. To satisfy the flexibility expectation, taking the "IP to the Field" paradigm [2] may be appropriate. In the considered paradigm, sensor nodes are expected to be intelligent network components, which will no more be limited to sensing tasks .By changing the intelligence to the sensor nodes, the gateway functionalities would be restricted to repetition and protocol translation. Consequently, gateway reprogramming operations would no more be required and dynamic network

IV. CHALLENGES FO WSN AND IN AN IOT

The formally introduce in "IP address to the field" involves assigning additional responsibilities to sensor nodes in addition to their usual sensing functionality. To highlight and talk about the challenges emerging from such novel responsibility assignment, we Choose three potential projects that the sensor nodes would have to accomplish: Security and quality of service (QoS) management, and network configuration.

A. Security

In common WSNs without Internet access, the sensor nodes may already act as an important role to ensure data confidentiality, integrity, availability and authentication depending on the application sensitivity.[7]Nevertheless, the current identified attack scenarios require a physical presence near the targeted WSN in order to jam, capture or introduce malicious nodes

B. Quality of Service

With gateways, acting only as repeater and protocol translators, sensor nodes are likewise required to contribute to quality service management by optimizing the resource usage of all heterogeneous devices that are part of the future Internet of Things. Not seen as a weakness, the device heterogeneity opens new views in terms of workload distribution. In fact, resource difference may be to share the current workload between nodes available resources.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

Improving the QoS, such collaborative work is consequently promising for mechanisms requiring high amount of resources like security mechanisms.

C. Configuration

In addition to security and QoS management, sensor nodes can also be needed to control the WSN configuration, which includes cutting through different tasks, such as address administration to ensure scalable network constructions and ensuring self-healing capabilities of detecting and eliminating faulty nodes or managing their own shape. Nevertheless, self configuration of participating nodes is not a common feature in the Internet. Rather, the user is expected to install applications and recover the system from crashes. In contrast, the unattended operation of autonomous sensor nodes requires novel means of network configuration and management.

V. CONSOLIDATION SOLUTION AND APPLICATION

We suggested in the previous section that a pure TCP/IP integration solution has certain limitations, mainly in terms of security, that must be taken into account. Nevertheless, the demands of the applications will finally decide what type of integration solution is more desirable. To assess this assertion, we will analyze two sensor network applications: WSN-enabled SCADA systems and First Responder systems. A SCADA (Supervisory Control and Data Acquisition) system utilizes novel technologies to monitor in real-time many of the critical infrastructures deployed in our club, such as energy systems, transport systems or oil/water distribution schemes The primary components of a SCADA system are the central control systems, where human operators remotely monitor the different components of the critical infrastructure, and the remote substations, which are settled within the critical infrastructures themselves and offer the data streams generated by elements of such bases. In other words, remote substations are primainly based on Remote Terminal Units which receive physical data (e.g. Pressure or voltage, temperature readings) from infrastructures, and transmits the. Equally for the sensing elements of the remote substation, WSN are being more and more covered by industrial companies and marketers. These sensor nodes are smart and autonomous devices capable of treating any information gained from their sensors and sending it to a central organization with considerable hardware and software resources, such as an RTU working as a data accumulation device. In summation, they can offer auto-configuration, self-monitoring and self-healing capabilities, as well as detection/tracking of anomalous situations, alarm generation and reporting of any dangerous situation [7]. These features have involved that WSNs are nowadays taken a key technology for the protection of many of our infrastructures and a suitable alternative of or SCADA systems, the real benefits of employing a pure TCP/IP solution for remote substations are not plenty to justify a full integration between WSN and the Internet. These sing elements of remote substations may not need to cognize about the existence of the Internet and other substations, since they only gather data and carry out orders from the cardinal organization. In conditions of protection, it is necessary to protect the WSN from any kind of trespass, as yet an increment in the network traffic can become problematic for the sensor nodes due to their special capabilities. Besides these security topics, there are other aspects in the TCP/IP solution that need to be taken. In particular, a TCP/IP-based WSN will not profit from the specific optimizations of native WSN protocols likeISA100.11a. Moreover, the capabilities of the sensor nodes may not be adequate to go through all the security protocols that can be applied during the lifetime of the web (e.g. Both such as store and forward (wait until the device is backwards and functioning) and redundancy (access another device that is supervising the same region). Short letter, however, that the existence of a central entry point gets to this solution vulnerable against availability attacks. This can be resolved by using the Hybrid and Access Point solutions (i.e. Increase the number of access points to the network), although these solutions deliver their own specific problems (primarily due to the replication of resources) The Front-End solution and the Gateway solution can still be applied, but the benefits linked with these solutions are not so important in these emergency scenarios. For instance, most of the nodes have a unique role, such as covering the location of aK9. As a consequence, the only advance that can be applied if a node is not available is stored a forward. In summation, there are some details that must be carefully weighed. As the nodes cannot access the Internet instantly, they depend on the existence of the gateway. Referable to the active nature of the application, it might not be possible to have multiple gateways in order to improve the redundancy of the web.

TABLE I DIFFERENT SECURITY CHALLENGES BETWEEN WSN AND IOT

SECURITY TYPE	RESULT	TCP LAYER
1. Trust, security and privacy	• The technology of TSP WSNs consists of message authentication, encryption, access control, individuality authentication,	Application Layer
2. Crypto algorithms	• Their wireless sensor devices have supported those libraries basically.	Data Link, Network Layer,

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

	• Libraries are designed for different encryption mechanism and consultation mechanisms at the data.	Application Layer
3. Secure routing of WSNs	• Typical methods of secure routing protocols include methodology based on feedback information, location information.	MAC Layer
4. Assure data assembling of WSNs	• The higher assembling nodes judge the credibility of data and do assemble calculation based on redundancy.	Network Layer
5. Key management of WSNs	• Key management adds key generation, distribution, affirm, update, storage, backup, valid and destroy..	Physical Layer

VI. CONCLUSION

In this first analysis step to integrate WSNs into the Internet of Things, we have considered many application scenarios representing a high diversity in conditions of monitoring issues and environments. By bringing into account their main features, we have analyzed three integration approaches and showed that they were inappropriate in their current state . They allow sensor nodes joining dynamically the Internet of We consider applying the IP to the Field paradigm, which implies assigning additional responsibilities to the sensor nodes as an equal resolution to integrate WSNs with the Internet. We have taken three important task assignments in order to spotlight the challenges coming forth from the paradigm adoption: Security, QoS, and configuration management. We conclude that some applications should not plug in their guests directly to the Internet (e.g. SCADA systems), but other applications can benefit from using TCP/IP directly (e.g. First responder systems). Short letter, however, that there is more security type using with multiple OSI model given different result that must be taken data privacy. More or less of these issues have been partially surveyed in this report.

REFERENCES

[1] I. Talzi, A. Hasler, S. Gruber, and C. Tschudin, "PermaSense: investigating permafrost with a WSN in the Swiss Alps," in Proceedings of the workshop on Embedded networked sensors (EmNets), 2007.K.
[2] "Internet of Things in 2020: Roadmap for the Future," 2008.
[3] JHA, M. K. And SHARMA, T. P. Secure data aggregation in wireless sensor network: a survey. International Journal of Engineering Science and Technology (IJEST), Vol. 5, No. 3, 2011
[4] .P. Katsikogiannis, E. Zervas, and G. Kaltsas, "A Wireless Sensor Network for Building Structural Health Monitoring and Seismic Detection,"Physica status solidi (c), vol. 5, 2008.
[5] M. H. Teicher, "Actigraphy and Motion Analysis:New Tools for Psychiatry," Harvard Review of Psychiatry, vol. 3, 1995
[6] C.P. Mayer. Security and Privacy Challenges in the Internet of Things.Ki VS Workshop on Global Sensor Network, 2009.
[7] J. Lopez, R. Roman and C. Alcaraz , Analysis of Security Requirements, Technologies and Standards in Wireless Sensor network ,Foundations of Security Analysis and Design V , LNCS 5705,289–338, Springer, 2009.
[8] Modbus -IDA, The Architecture forAutomation, http://www.modbus.org/,accessed on October 2010.
[9] Challenges in integrating Wireless Sensor Networks into The Internet**Kour Tejasvit** Chandigarh Group of Colleges,Chandigrah, India.
[10] W. Werner-Allen, K. Lorincz, M. Ruiz, O. Marcillo, J Johnson, J. Lies, and M. Welsh, "Deploying a Wireless Sensor Network on an Active Volcano," IEEE Internet Computing, vol. 10, no. 2, 2006.