World Applied Sciences Journal 32 (12): 2431-2435, 2014
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2014.32.12.1321

A Leader Selection Strategy for RFID Communication in the Internet of Things

J.P. Nivash, L.D. Dhinesh Babu, Ebin Deni Raj,
M. Nirmala and J. Sharon Moses

School of Information Technology and Engineering, VIT University Vellore, India

Abstract: Internet of things is about connecting the various embedded devices through internet connection beyond machine-to-machine communications. The inter connection of embedded devices are used widely in various applications in the daily life. All objects including people and animals were involved in this paradigm. The objective of this paradigm is gathering the data without the intervention of human. Objects communicate with each other with the help of wireless technologies.

Key words: RFID · Leader selection · Internet of things · Unique identification number

INTRODUCTION

The main aspect of this paper is the consolidation of communication solutions and several technologies. The term Internet of things (IOT) has been started using in various conferences, telecommunication scenarios, future wireless sensor paradigm and so on. The overall conception of IOT is about dealing with data sharing and information with each other [1]. The goal intended to be attained by IOT was to organize uniquely identifiable devices within the internet infrastructure. IOT is waiting to connect embedded devices beyond the machine-to-machine communication with various protocols and domains. Unprecedented numbers of connected devices are expected to connect in future due to its nature of ubiquity.

The world is connected, when all the physical products start to interact with each other. The machines will communicate with each other without the intervention of the human. Some of the commonly used gadgets to gather the information are smart TVs, webcams, thermostats and so on. There are many devices around us already interacting with each other. Some of them are Radio-frequency identification (RFID) tags, sensors, mobile phones etc. using unique addressing schemes interact with each other. In a recent survey it is said that, about seventy percent of IOT devices are hack able. Future predictions say that everything in next twenty years would be connected by IOT.

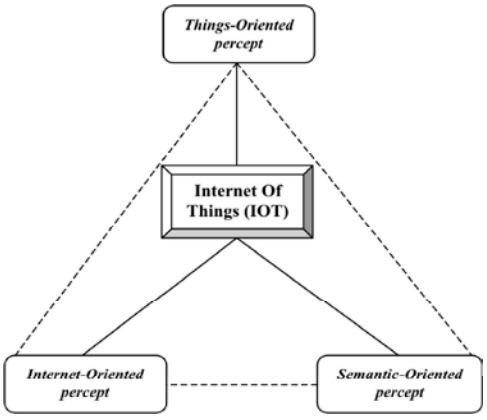

Fig. 1: Internet of things paradigm

Hence as the number of IOT devices increases, the security concern would also gets multiplied. Researcher state that, security issues in IOT has to be noted with attention and much research intervention is needed in this field.

Object Perspective of Iot: To improve the visibility of objects in the network Electronic product code (EPC) was designed. It is considered to be the key component of IOT. It supports to spread RFID in worldwide modern trading networks.

The distinct feature of RFID technology is item traceability and addressability [2]. IOT can be categorized with the combination of things, internet and semantic as described in Fig. 1.

Corresponding Author: J.P. Nivash, School of Information Technology, VIT University.

The considered things and vision of Things oriented percept are RFID tags, UID, Spime, NFC, WISP, Wireless sensor actuators, everyday objects, smart items and many.

RFID: Radio-frequency identification (RFID) tags are used for transferring data using electromagnetic fields [3]. Automatic identification and tracking the tags attached to the objects are the main purpose of these tags. The information in this tags are stored electronically. Using magnetic fields, some tags get power and read at small area. There are some RFID tags which gets power through battery, some collect energy through electromagnetic field interrogation. The tags which collect energy through EM field acts as a passive electrical device to emit micro waves. For distance like 100 meters of operation, battery powered RFID tags are used. RFID comes under Automatic Identification and Data Capture technology [4]. The usages of RFID tags are wide in industries.

UID refers to Unique Identification Number. It's a unique number for object identification. Spime is the term used in IOT which has all essential information of any particular object stored in cloud. It means any object can be tracked through space and time. Near Field Communication (NFC) is used in smart phones and similar devices to start a new radio communication by touching them or bringing the objects to some closeness. It is restricted to few centimeters. Wireless Internet Service Provider (WISP) is a wireless networking paradigm. CASAGRAS is a consortium in IOT proposed for RFID centric approach. Without the intervention of human, here things can communicate with each other automatically. It connects both virtual and physical generic objects. Hence IOT is considered as the high degree data capture, event transfer and network connectivity.

Internet Protocol for Smart Objects (IPSO) is a network topology for connecting smart objects around the world [5]. It is a light protocol that connects huge communicating devices and runs on embedded devices operated by small battery. To make IOT a reality, the IP has all qualities with it. By IPSO, the Internet Protocol address can be simplified further for object addressable and adapt any object. The main advantage is it can be reachable from any location.

Semantic-Oriented Percept: Semantic plays an important role in future internet. The major issues in this perception are interconnection, how to store, search and organize information generated by IOT. It will become challenging for IOT. This is the key role of semantic technologies.

IOT Technologies: With the integration of various enabling technologies, the real world concept is possible in IOT. Communication technology, Identification and Sensing is the context of IOT. To make the data available "Anytime, Anywhere, Any media", the wireless technologies have played the key role. These technologies made the ratio between human and radios usage approaching to 1:1. IOT steps into new era with the reduction in size, weight, consuming energy and cost of radio. The integration of these aspects makes radios in all objects. RFID systems are considered as the key component of IOT. It is the composition of several RFID tags and one or more readers. Tags can be identified as unique identifier. The readers generate an appropriate signal to spark the tags around certain area.

In general RFID is passive. They basically do not have power on board. It needs greater signal from the reader to harvest the power required for transmitting.

In Active RFID, it has internal source for power. It has a battery within it for transmission of RF (Radio frequency). Since it has power, it allows very low signals. Both active and passive RFID uses radio frequency energy for tags and reader communication. In case of semi-passive RFID, it has a battery within it. These batteries power the microchip while receiving the signal from the reader. These tags observe the input out of sensors even it is not in the range of RF field. Table 1 represents the all the three tags in brief.

The role of sensor networks in IOT is crucial. They have a strong co-operation with the RFID tracking the status of things i.e. their movements, location, temperature etc. between the physical and digital world sensor networks acts as a bridge. The wide usages of sensor networks in various applications are industrial plant monitoring, Environmental monitoring, military, intelligent transportation systems and e-health.

The objectives of sensor networks are robustness, energy efficiency, reliability and scalability. The considered problem in sensor networks is scarcity of IP address since the network consists of very large number of nodes. To save energy, a sensor network spends most of its time in sleep mode. During these periods communication cannot be done. By integrating other sensing technologies with RFID tags would enable a new

Table 1: Comparison of RFID Technologies

	ActiveRFID	PassiveRFID	Semi-passiveRFID
Power	Battery	No internalPower	Very small battery
Signal strength	Low	High	High
Communication range	Long(100 m)	Short(3m)	Long(100m)
Data storage	Large read/write (128 kb)	Smallread/write(128kb)	Large
Tag cost	High($15-$100)	Low($0.15-$5.00)	Low
Applications	Laboratories, Construction, Remote Monitoring	Libraries, Passport etc.,	Temperature, Pressure, Tamper Detectors.

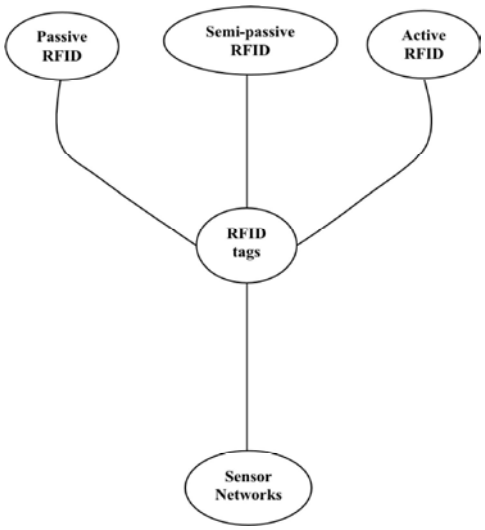

Fig. 2: RFID system

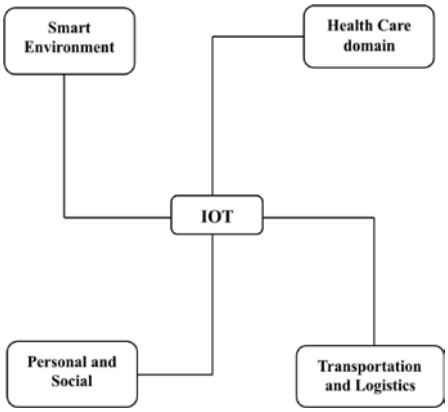

Fig. 3: Applications of IOT

context in IOT. For Internet Protocol networks, it is anomalous. The RFID tags can be linked on to cloud and can be used in the data collection of big data processing.

Applications of IOT: The inherent capacity of Internet of things to the society has reached its extent. But the in case of availability to the society, it is on board. The new applications in the various environments are at the pace of improving our lives. These applications can be broadly grouped into following categories.

Smart Environment: The smart environment domain focuses on comfortable homes & offices. It means the living space is activated with possible sensors for better living. Domestic distinct events can be prevented from happening with the suitable alarm monitoring system. The act of using the electricity can be made less automatically when it is not necessary. The efficiency of production part in industrial area can be achieved through automation. It is deployed by massive RFID tags.

Health Care Domain: The RFID usage in health care domain is at the pace. It applied in tracking the objects in motion. Both real-time tracking and tracking through choke points are used to examine the various necessities. Next is identification and authentication. It is used for patient identification especially for infants. Finally by making the automated data collection, the processing time can be reduced largely.

Personal and Social Domain: Automatic updates of social activities of a user, updating the places in real-time and many things helps the user social networking forum. The user's appointments, meetings, business discussion can be maintained automatically in a forum. So, it will help in historical queries. The lost and theft objects can be identified with the RFID signal. If the particular object gets out of the range without a proper authentication, it can be indicated by SMS.

Transportation and Logistics: The roads and vehicles are becoming equipped with RFID tags which transfer constant information about the traffic status, location, climatic condition and various other aspects. Monitoring the logistics in real time helps us to the stage of the product. The perishable goods can be tracked along the way using RFID tags. Likewise monitoring environmental parameters can be done to its extent.

Components of IOT: There are three major components which have to be considered while reading the performance of RFID tags in a restricted environment as shown in Fig. 4. They are technological, physical and

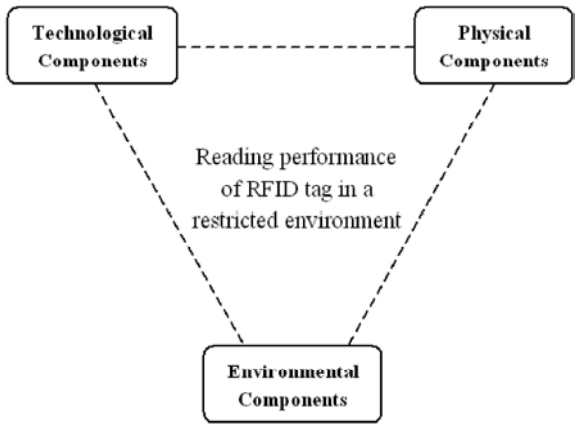

Fig. 4: Components of IOT

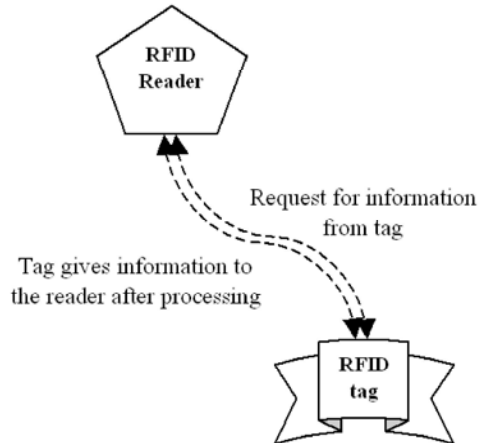

Fig. 5: RFID power scheme

environmental components [6]. The technological components are the RFID type, tag size, tag placement, tag angle, orientation, height, range, reader placement, reader antenna angle, power level, tag reader distance level and interference.

The physical components are area size, aisles number, number of racks, types of racks, forklift speed, conveyor speed, pallet patterns, types of material of material handling equipment, product package type, product types(liquid, metal). Finally the environmental factors are temperature, humidity, noise, dust & dirt, E-plane (electric field), H-plane (Magnetic field). The above represented are the factors which may affect in reading the performance of RFID tags in a restricted environment. In common the reader starts the communication by sending the signal to the tags as shown in Fig. 5. The tags in turn process the signal and acknowledges. It is same case for active RFID, passive RFID and semi-passive RFID [7]. In Figure 4, the communication between the reader and the tag is deployed. It depends upon the tag type for the distance range. Here each leader node will gather the information of the other nodes in the network [8].

This information will be handed over to the reader or the central server. Initially the leader node will send hello message to all the other nodes in the network as like other communication protocols. The other nodes will respond with the acknowledgement. The leader node will organize the group of active nodes in the network.

This paper analyzes the performance of RFID tag in a particular environment. It might be any restricted environment which is subjected to monitoring. The information of each and every move of the particular environment is gathered automatically. This paper concentrates on the gathering of information. There are various factors in mounting the performance of RFID tags.

Among the list of RFID nodes, the reader should able to select a leader node. To perform the various tasks, the leader node has to be selected.

Proposed Algorithm Towards Selecting the Leader Node: The leader selection among the group of nodes is done by the following RFID leader selection algorithm. Initially the active RFID nodes in the environment are noted. The reader authenticates the eligible RFID nodes in the network. Among the number of nodes in the network, the nodes within the range alone were taken into consideration. The number of nodes under a leader is based on the tasks and can be implemented in future. The nodes within the network range are considered as the eligible nodes. Here in RFIDLS algorithm, step by step representations were shown. The group of nodes can be formed according to the tasks. Once a task is selected, it is given to the appropriate leader node and its group. The number of leader nodes can be obtained with respect to the tasks. The number of leader nodes must be less than the number of active RFID nodes count. These are calculated according to the tasks given to the nodes.

RFIDLS Algorithm: for Selecting the Leader Node
BEGIN:

$\Delta \leftarrow [000 \ldots 0]^*$
$\nabla \leftarrow \infty$
for $\alpha = 1$ to β do
for $\rho \epsilon$
φ - {nodes already selected as leaders} do

$\delta \leftarrow \Delta$

Table 2: Description of variables used in algorithm

Variable name	Explanation
Δ	Active RFID nodes
∇	RFID nodes within the range
$\propto$	Number of tasks
φ	Number of leader nodes
ρ	Selected leader nodes
δ	Group of tasks
δ_γ	Task name
N	Matrix of tasks
Δ_{min}	Less than two RFID nodes

$\delta \leftarrow \Delta$

$\varphi \leftarrow \frac{1}{2}\ (N\ [\delta]^{-1})$

if $\varphi \leq \nabla$ *then*

$\nabla \leftarrow \varphi$

$\min \leftarrow\ \rho$

end if

end for

$\Delta_{min} \leftarrow 1$

end for

END.

CONCLUSION

In this paper a survey of Internet of things and their parameters were discussed. Various RFID devices were compared and their usages in various applications were discussed with examples. Various components determining the reading performance of the RFID tag were considered. Here RFIDLS algorithm was proposed to select the leader node among the group of RFID nodes in the restricted environment. The proposed algorithm can be implemented in the future project.

REFERENCES

1. Atzori, Luigi, Antonio Iera and Giacomo Morabito. 2010. "The internet of things: A survey." Computer Networks 54(15): 2787-2805.
2. Barchetti, Ugo, Alberto Bucciero, Mario De Blasi, Luca Mainetti and Luigi Patrono, 2010. "RFID, EPC and B2B convergence towards an item-level traceability in the pharmaceutical supply chain." In RFID-Technology and Applications (RFID-TA), 2010 IEEE International Conference on, pp: 194-199. IEEE,
3. Want, Roy, 2006. "An introduction to RFID technology." Pervasive Computing, IEEE, 5(1): 25-33.
4. Weinstein, Ron, 2005. "RFID: a technical overview and its application to the enterprise." IT Professional, 7(3): 27-33.
5. Vasseur, Jean-Philippe and Adam Dunkels, 2010. Interconnecting smart objects with ip: The next internet. Morgan Kaufmann.
6. Sarma, Sanjay E. Stephen A. Weis and Daniel W. Engels, 2003. "RFID systems and security and privacy implications." In *Cryptographic Hardware and Embedded Systems-CHES 2002*, pp. 454-469. Springer Berlin Heidelberg.
7. Juels, Ari and Ravikanth Pappu, 2003. "Squealing Euros: Privacy protection in RFID-enabled banknotes." In *Financial cryptography*, pp: 103-121. Springer Berlin Heidelberg.
8. Ganeriwal, Saurabh, Ram Kumar and Mani B. Srivastava, 2008. "Timing-sync protocol for sensor networks." In *Proceedings of the 1st international conference on Embedded networked sensor systems*, pp: 138-149. ACM.
9. Babu, L.D. and P. Venkata Krishna, 2013. "Honey bee behavior inspired load balancing of tasks in cloud computing environments." Applied Soft Computing.
10. Babu, L.D. Dhinesh, *et al*., 2011. "An analysis of security related issues in cloud computing." Contemporary Computing. Springer Berlin Heidelberg, pp: 180-190.
11. Ebin Deni Raj, L.D. Dhinesh Babu, Ezendu. Ariwa, M. Nirmala and P.V. Krishna. 2014. "Forecasting the Trends in Cloud Computing and its Impact on Future IT Business". IGI Global Publishers, 2014 In Green Technology Applications for Enterprise and Academic Innovation on. pp: 14-32.