

Managing Enterprise Resource and Environment through Real-Time Tracking, Monitoring and Actuation of Enterprise Objects using Internet: a Conceptual Framework and Test-Bed Implementation

Anurag D¹, Siuli Roy¹, Somprakash Bandyopadhyay¹

¹Indian Institute of Management Calcutta, India

anurag@email.iimcal.ac.in, siuli@iimcal.ac.in, somprakash@iimcal.ac.in

Abstract. In this paper, we present a unified framework for both asset and environment visibility of an enterprise through real-time tracking and monitoring of enterprise objects using the Internet. The objects that are monitored can be personnel, equipment or an environmental condition. The architecture also enables the control of asset utilization by triggering actuators. Active RFID tags, combined with sensors and actuators, form a wireless mesh network based on IEEE 802.15.4. We develop a new routing algorithm oriented for these tracking applications where the network is sparse but comprises of extended legs. In such cases, the C_{skip} algorithm used in ZigBee fails to develop a tree based network structure. The new algorithm builds a hierarchical tree network to maintain routing at its efficient best. Lastly, we elaborate a test-bed implementation for tracking underground miners and equipment along with monitoring the underground environment for possible emission of toxic gases.

Keywords: Internet of Things, 802.15.4, Remote Tracking, Static Routing.

1. Introduction

The availability of consistent, accurate and timely information greatly improves the quality and speed of planning and decision making in any organization. Total Asset Visibility (TAV) [10] is a term, used in US Department of Defense's logistic practices, that implies knowing where assets are at all times. It also implies having a unique identity for each item and knowing what is happening to it, as it happens. TAV can usefully be applied to any organization for improving enterprise visibility. Timely and accurate information on the location, movement, status, and identity of units, personnel, equipment, material and supplies can improve the resource utilization by a great extent. It also improves the capability to act upon that information for better performance of the organization. The core of this kind of Asset Visibility System is the Automatic Object Identification technology, like RFID, integrated with wireless mesh networks to communicate this identification data to a remote station.

An Enterprise visibility system is not confined to asset visibility only. The same framework can be used to monitor the enterprise environment, to protect it against possible damage by terrorist attacks, fire or emission of toxic gases (in case of chemical industries). Wide variety of sensors connected together using wireless sensor networks forms the core of this **Environment Visibility System**.

Moving a step further towards a "better" visibility, all this information should be available in real-time from anywhere. This "anywhere" accessibility of information through the Internet, which in turn is linked with the core visibility system in an organization, enables a corporate manager to access relevant enterprise information in real time, as and when needed.

This paper presents a unified framework for both asset visibility and environment visibility of an enterprise through real-time tracking and monitoring of enterprise objects using the Internet. It also allows controlling the asset utilization and the environment by triggering actuators, which are also part of the enterprise objects. The core objective is to develop a system that helps not only to view but also to control enterprise objects through the Internet.

The paper is structured as follows. Section 2 develops a conceptual framework and section 3 explains the detailed system architecture and its three components: the wireless mesh network, central server and the Internet connectivity with the web end point. Section 4 proposes a new routing algorithm for wireless mesh network suited for tracking and monitoring application in real-time. The practical implementation of the system for tracking underground miners and mine equipments with real-time environment sensing to warn against emission of toxic gases is presented in Section 5. The related work, in the area of the "Internet of Things", is discussed in section 6. We provide the scope for further work and conclude in Section 7.

2. Conceptual Framework

Small, autonomic wireless devices, cheaply priced and capable of forming communications networks are expected to be the next technological innovation to bring about a mass cultural change. This new concept is due to the emergence of Personal Area Networks (PAN) where billions of devices are inter spread in the everyday activities of humans. The devices help organize, manage and control a host of equipment and services. The impact of this new paradigm is often compared to the digital revolution brought about by the Internet in the late nineties.

The Personal Area Networks comprise of, typically, sensors and actuators which are capable of forming wireless networks among themselves and are designed to run on batteries for prolonged periods of time. These devices and such networks need to support a low data rate and the computational capability is restricted. Low data rate protocols have been designed specifically for these needs lately, a significant

deviation from the trends of building high-bandwidth networks. The protocol ratified by IEEE is 802.15.4 in 2003 and updated in 2006 [6]. The 802.15.4 standard provides specifications for the Physical and Medium Access Layer. The upper layers (Network to Application) have been developed by a consortium of wireless device manufacturers and enthusiasts called ZigBee [15]. The aim of the ZigBee Alliance is to ensure interoperability among similar devices from the different manufacturers and provide a common platform for dissemination of research findings and solutions. A typical example envisioned is the automation of electronic devices in a home where a single controller (can be a mobile phone or a PDA) can control a television, music system, fans, lights, ovens, refrigerators and even personal computers.

The "Internet of Things" paradigm is to now to control such appliances from a remote location through the Internet. For example, you could turn on your oven, or check the quantity of food in the refrigerator from your office, located miles away. Further, the devices could be automated to talk to each other over the Internet. The Internet would thus act as the connecting medium for these numerous devices. The widespread adoption and the extensive reach of the communications network would provide connectivity at anytime, at anyplace and for anything. The ITU, in its report on the Internet of Things [7], has foreseen the emergence of a new ecosystem due to the Internet of Things. The key players of this ecosystem would be: the Government (and its regulations), the Social System (and the acceptance of ubiquitous technology by the users), the commercial players (the economic viability of the technology) and the R&D Organisations (the usability of the technology).

In this paper, we have developed an end to end architecture for such remote visibility of enterprise "objects" and remote actuation necessary for controlling these "objects". The architecture comprises of three basic components: (a) the wireless mesh network, consisting of RFID tags, sensors and/or actuators, (b) the gateway and the central server and (c) the Internet. The mesh networks house local information which is communicated through a gateway to the central server. The gateway handles the messages to and from the mesh network. The gateway is expected to be mains powered while the individual nodes (sensors/actuators) are battery driven. The information is then transported to a web end-point by the Central Server. The central server essentially does the job of protocol conversion from the Internet to the sensor network and vice-versa. The information is displayed in the requisite format and provides an interface for object management. The web end point application can be a simple hosted page viewed on a personal computer or a message transmitted to a mobile device. We could think of supporting both push based and pull based systems. A push based system updates the status of the devices automatically, either periodically or when a status changes. In a pull based system, the latest information is provided when the user asks for it. The conceptual framework is pictorially depicted below.

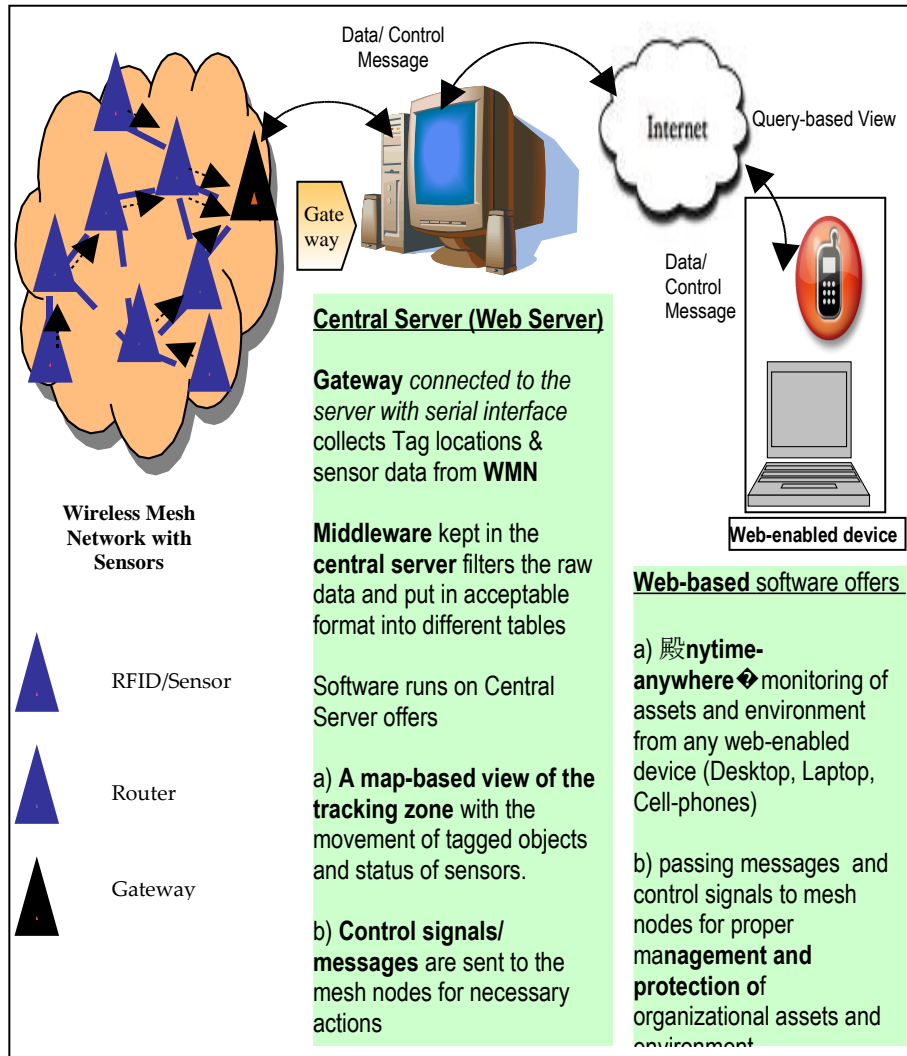


Fig. 1. A conceptual Framework for Tracking, Monitoring and Actuation of Enterprise "objects" through the Internet

3. Detailed System Architecture

As depicted in figure 1, the proposed architecture has three components: Wireless Mesh Network, Central Server or Control Station, any web-enabled device accessing the central server through the Internet.

3.1 Wireless Mesh Network

Wireless Mesh Network, as its name implies, is a type of network where each node in the network can communicate with multiple wireless nodes, thus enabling better overall connectivity. A wireless mesh network has two kinds of nodes: the mesh routers and the mesh clients [1]. The mesh clients can be made to communicate with multiple routers/other clients, or arranged in a hierarchical fashion where every client has a single router as its parent. A major advantage of this kind of networks, other than self-forming and self-healing capability, is multi-hop routing. This means that data from a wireless node can jump through multiple nodes before delivering its information to a remote host gateway or controller that collects the data from tags for further processing. Low power mesh networking, sensing and active RFID-based real-time location tracking is a combination that has enabled us to design systems for tracking, locating and monitoring people and things and environmental conditions.

Passive RFID tags (RFID without a battery) [13] is already driving shifts in supply chain and retail capabilities for automatic identification of objects. However, Active RFID has much broader potential in the enterprise. Firstly, active RFID can form a wireless mesh network, providing automatic, dynamic visibility into what is going on in and around the enterprise. Secondly, active RFID technology, if combined with sensors and actuators in a networked environment, enables a spectrum of applications that can exponentially increase visibility and monitoring. Offering much more information than passive RFID, sensors can monitor and record conditions like temperature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, chemical concentrations, pollutant levels and so on.

The mesh network proposed here has three components which are elaborated below.

3.1.1 Active RFID Tags with Sensor /Actuators

Designed for fixing on different types of objects/assets (wearable tags for humans), active RFID tag is versatile in its usage. It is possible to attach analog sensors, digital sensors and actuators using its ADC and digital Input/Output ports. So, the same device can be used as RFID tag for tracking objects, as a sensing device to read the environmental condition, as a messaging device to send pre-coded emergency messages to remote control stations or as an alarm device to receive the alert message sent from the remote station. These active RFID tags are battery-operated devices that are designed to communicate with a Gateway in its vicinity. In order to communicate with the gateway that is out of the communication range of a tag, sufficient number of routers may be introduced in between the tag and the gateway so that data can be propagated in multi-hops.

3.1.2 The Gateway

The Gateway is essentially the master controller that coordinates the formation of mesh network, collects the tag data and transfers it to the host computer. On one hand, it supports bi-directional communication with active RFID tags either directly or via intermediate routers. On the other hand, it has wired / wireless interfaces to the host computer so that the tag data received by the gateway can be sent to a host computer (Laptop, PDA, PC) for further processing.

3.1.3 The Routers

Routers can be used for range extension of the active RFID devices. In real-time location system (RTLS), routers are fixed at strategic locations within the tracking zones forming wireless mesh network with other routers, gateway and active tags in its vicinity. Location of a tag is determined in terms of the locations of these fixed routers.

3.2 The Central Server

The data obtained from the wireless mesh network is primarily stored in different staging tables in a server database and subsequently processed and analyzed by the software to get a real-time view and status of the tracking and monitoring zone. The data may be classified into three categories:

- Location data/Sensor data from tags/ sensors
- Periodic beacons from Routers indicating their presence and battery status
- Emergency messages from tags

The software system consists of the following modules:

- The Middleware:** It accepts the data through the serial port of the server and filters them for duplicates and is stored in an acceptable format in different tables depending on the type of data. It also accepts the control messages from the software system (central server or Internet), translates it into a proper format and is dispatched to the Gateway for actuating a particular tag in the mesh network.
- System Configurator:** It is used to map the mesh network components into the software system. The Mesh network is essentially a tracking zone with routers and actuators placed at different strategic locations. The system configurator, thus enables the user to:
 - *Configure the site* (Tracking zone): To get a real-time view of the tracking zone, a map of the tracking zone is to be loaded into the system.
 - *Configure the network devices:* A “*site configuration toolbar*” in the *system configurator* allows the user to drag and drop router icons on the

maps as per their actual placement in the tracking zone and allow the user to configure them as per their real configuration.

- iii) **Network Manager:** Allows the user to view the network topology and status of the devices in the network (alive, dead, battery status etc.).
- iv) **Tracker:** Allows the user to view the movement of tagged assets/ objects within the Tracking Zone in real-time.
- v) **Finder:** Allows the user to locate a particular or a group of tagged objects/ sensor nodes.
- vi) **Sensor Monitor:** Allows the user to monitor the status of different sensor nodes in the Tracking Zone.
- vii) **Response Handler:** It enables the user to send context-sensitive control message/commands to any device (actuators) in the network in response to some critical event simply by clicking the desired device (actuators) from the Map-based view provided by **Tracker** or **Sensor Monitor**. It can be used to generate an alert on a tagged object, to give some instruction to open some valves in a process control, or, to send some signal to open a sprinkler etc.
- viii) **Report generator:** Allows the user to generate customized reports based on the available location and sensor data in the system.
- ix) **Query Manager:** This is a query-driven interface that allows the user to send a query to the mesh network asking for some required information about the status of a tagged object/ group of objects or sensor node(s). For example, specify the locations where temperature is above 45 degree, etc.
- x) **Message Viewer:** Allows the user to receive messages from the devices in the network and display them on a message inbox with timestamp.

3.3 Accessing the Central Server through Web-Enabled Devices

Web-based Tracking and Monitoring system offers the flexibility to track and monitor the organizational resources and environment through internet providing “*anytime anywhere*” visibility of the enterprise. Remote users can track the organizational resources and monitor the environment based on the data accumulated in the server at the control station and based on that user may take some control decisions. Other features like, *Tracker, finder, Sensor monitor, Response handler, Report generator, Query Manager and Message viewer* are also available in the web-based version of the software.

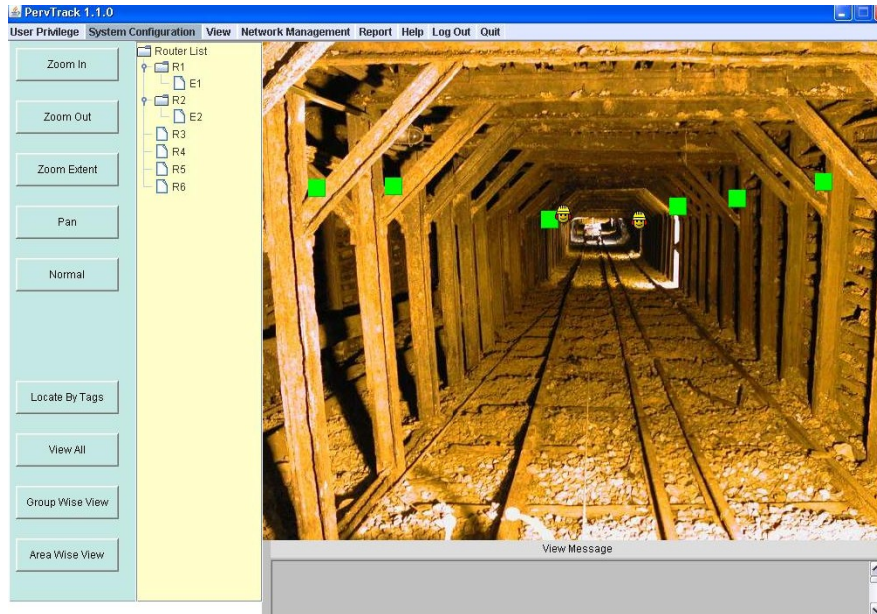


Fig. 2. Locating workers in a Mine Shaft

4. Data Acquisition and Data Delivery in Wireless Mesh Network

The natural choice for the mesh network would be the ZigBee standard; however, the C_{Skip} algorithm used in ZigBee was found lacking when a sparse, but large network is needed. In this section, we first develop the need for tree based network and highlight its properties. We then move on to elicit the deficiencies of the current addressing algorithm in ZigBee. We thus propose a static addressing scheme where the routing is still maintained at its efficient best. This algorithm has been tested by way of an implementation for practical use on TI based boards – CC2420 [3].

4.1 The C_{skip} Routing Algorithm

The ZigBee standard based on the IEEE 802.15.4 PHY and MAC Layers provides specifications for two kinds of network topologies- mesh and tree. Mesh networks utilize the slightly modified ad-hoc on-demand distance vector (AODV) [9]. However, we are interested and this paper delves on the hierarchical or the tree based routing scheme. As said above, the hierarchical scheme is preferred over a pure mesh networks in the realm of tracking applications. The characteristics of such applications are:

- A pre-determined area of deployment where the path to be tracked is known. Thus the routers (FFDs) are placed along this path.
- The data flow is always between the coordinator and an end device (RFD) and vice-versa. There is never a need for two end devices to talk to each other.
- Tracking applications are typified by a large area, but a well defined path. Further, the paths are bounded on either side (for example walls of a building). Therefore the network is sparse and the probability of forming a mesh is low.

The tree based routing has been shown to be the most efficient [12] among the different routing algorithms supported by ZigBee. However, this is conditional to the successful formation of the network topology in the form of a tree. ZigBee uses the C_{skip} algorithm for the address allocation and the buildup of the network topology. According to the C_{skip} algorithm, new devices which request association are given a short address. The address assigned follows rules set by the network parameters. These parameters are predetermined and are static. The Parameters are C_m , R_m and L_m ; where C_m = Maximum Number of children that a full functional device (FFD) can have; R_m = Maximum number or children (out of C_m) which are FFDs; and L_m = Maximum depth of the network. The values of these parameters are stored in the NIB (Network Information Base) in each device [5].

A device given to a requesting child is generated by the equation :

$$A_n = A_{\text{parent}} + C_{\text{skip}}(d) R_n + n \quad (0)$$

Where A_n is the address which the new device will take. A_{parent} is address of the parent of the device that will assign the address. $C_{\text{skip}}(d)$ is determined as follows:

$$C_{\text{skip}}(d) = (1 + C_m - R_m - C_m * R_m^{C_m - d - 1}) / (1 - R_m) \quad (0)$$

$C_{\text{skip}}(d)$ determines the block of address which the parent device must skip before assigning the next address. The algorithm assumes the worst case scenario and makes provision for accommodation for all devices in the pre determined network architecture. This assumption of a worst case scenario severely restricts the network depth. For example, values of $C_m = 6$, $R_m = 6$ makes $L_m=7$ for a 16 bit short address.

The addressing scheme based on C_{skip} develops a tree topology which makes possible the optimum routing. Routing in such networks is made by comparing the destination address with the c_{skip} allocation block. If the destination address is within the C_{skip} block of any of its children, then forward the packet to that child, else forward the packet to its parent. It has been shown that such tree based routing provides the minimum latency [12].

4.2 The Static Addressing Algorithm

The motivation for a new algorithm arises from the need to prevent the wastage of address space but at the same time maintain efficient routing through a tree based structure. A pictorial topology is first prepared with the Routers (FFDs) placed appropriate distances along the path. The maximum number of end devices each router would have to handle is estimated (En). The Address of each Router is then determined by the simple algorithm as shown below. The algorithm works on the depth first concept where the deepest router is assigned an address first and the algorithm works up the topology. The needs of tracking allow us to set the address in advance to preserve the tree structure.

```
Addressing Algorithm

function main ()
{
  assign PAN_Coordinator_address = 0;
  current_address = En + 1;
  assign_address ( PAN_Coordinator );
}

function assign_address ( node )
{
  for ( all children of node from left to right )
    assign_address ( child_node );

  node_address = current_address;
  for ( all children of node )
  {
    parent_address( child_node ) = current_address;
    append into address list, child_node address;
  }
  current_address += En + 1;
}
```

Fig. 3. The Node Addressing Algorithm

Every Router maintains an address list, which has the addresses of its child routers. The routing is done based on this. The address allocation is pictorially depicted below. Assume, a network topology as shown and $En = 6$.

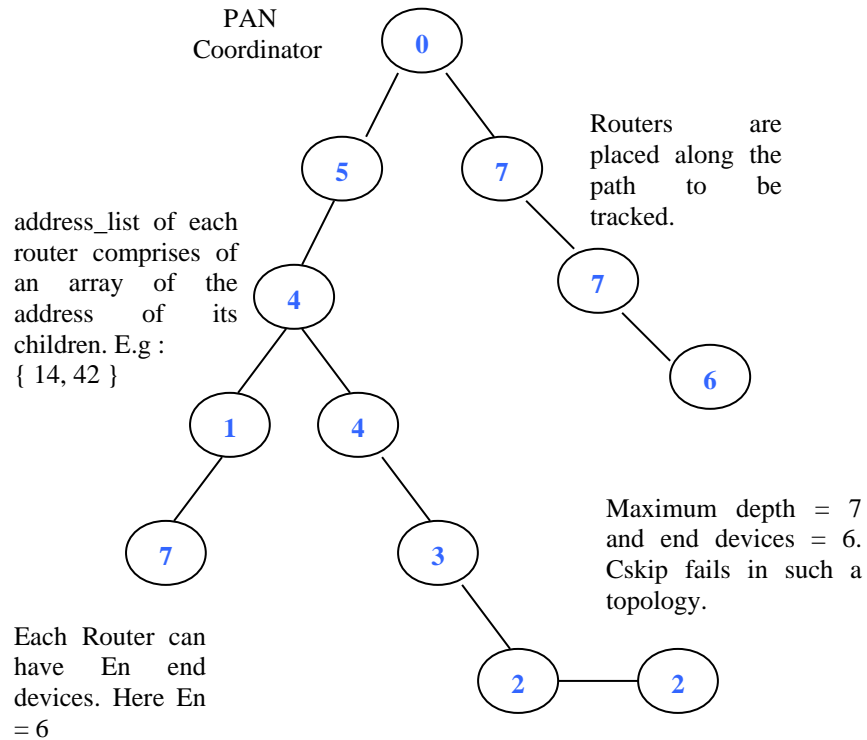


Fig. 4. A sample topology with max end devices per router = 6.

The addressing algorithm is akin to the Cskip in the sense of addressing in the depth first approach. However, Cskip assumes the worst case and would earmark addresses for non-existent nodes. This leads to a huge amount of address wastage and this precisely avoided in the static algorithm. The tracking applications have a well defined path and this is known in advance. Thus, the need to maintain addresses for future nodes does not arise. Further, the address allocation can be suitably tweaked to include an address provision for future nodes as the need may be. This can be achieved, by including a larger value for En.

The address of a node denotes the maximum address of all devices under it. A router assigns address to end devices as $\text{node_address} - n$. Where $1 \leq n \leq E_n$. At any given point, the property of the node addresses is maintained and thus routing is achieved. For example, consider an end device joins the network at node 35. It is assigned an address of 34. The routing decisions would be at each node and checks under which child, can the destination address exist and forward accordingly. The algorithm and the pictorial representation are shown below.

```

Routing Algorithm

address_list = { child router addresses};
if ( dest_address = child_end_device)
    next_hop = dest_address;
else
{
    next_hop = parent_address;
    for all address_list_entries
        if (dest_address of packet <= address_list_entry)
        {
            next_hop = address_list_entry;
            break;
        }
    loop
}
send_packet(next_hop);

```

Fig. 5. The Routing Algorithm

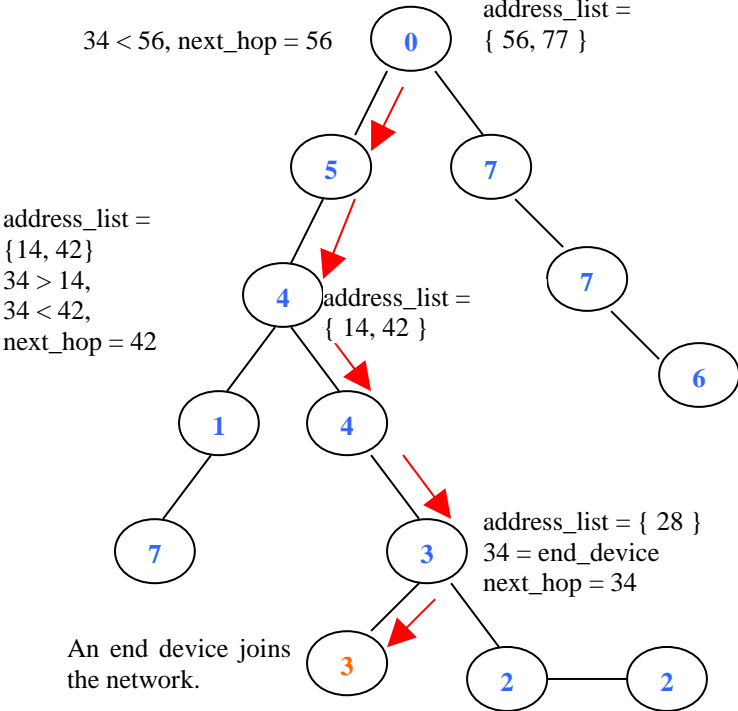


Fig. 6. A pictorial representation of the Routing Decisions for a packet destined to 34

The addressing and routing algorithms have been tested on CC-2420, TI (Texas Instruments) based board. The network layer was written over TIMAC (TI supplied PHY and MAC layers) [14].

5. A Test-bed Implementation for Underground Mines

Underground mines are disaster-prone where disasters occur due to inundation of mines with underground water, or, explosion due to excessive emission of poisonous gases, or, lack of adequate roof support. During disaster, the main problem is to identify the pits or tunnels where exactly the workers are trapped. The mine authorities can only count the cap lamps to conclude the total number of miners trapped inside but have no clue about their locations. Therefore, tracking and monitoring of miners is a basic need in hazardous environment of mines. Apart from miners, continuous tracking and monitoring of mining equipments is also necessary for better resource utilization and improve productivity. Moreover, an early warning system to detect the excessive emission of poisonous gas or a system to prevent the entry of miners in an unsafe zone inside mine is also necessary to ensure mine safety.

In our proposed system, cap lamp allotted to a miner has an additional attachment that is essentially an IEEE 802.15.4-enabled RF Active Tag. Each such tag carries a unique identification number and it sends beacon periodically to inform its presence. Similar devices are statically placed as routers at different strategic locations covering the entire underground mine to uniquely identify each area within the mine. During a shift, tagged miners work at different areas inside mine and a router in an area captures unique identification numbers periodically emitted by all the tags present in that area. So, the location of a tagged miner or equipment can be determined in terms of the location of its nearest router. These active tags and routers form a rapidly deployable wireless network on ad hoc basis inside the mine which serves as a network backbone to carry the tag ids and their location information in multi-hop from underground to the control station on the surface that in turn is connected to Internet. The miners could be now tracked from a central or sub-central control points as well as through Internet.

Tracking performance is evaluated in a real-life scenario where a network is configured replicating the floor plan of a mine. We have used 8 Routers 1 Coordinator and 1 to 10 tags to evaluate the system in a lab scale as per the configuration shown in fig 1. We have also configured the software system accordingly by loading the map of the site and placing the routers on the map as per their placement in the actual site so that the map with routers placed on it maps the actual tracking zone.

After successful establishment of our network, we observed the movement of multiple tags throughout the network. Here each router sends a periodic beacon to the coordinator to notify that it is alive in the network. The beacon contains router's name (R1, as given by the user during software configuration) and a software-Id

automatically allocated by coordinator during network configuration. Each end device also sends a periodic beacon to the coordinator, and the message contains its parent's Id (associated Router's Software Id) and a Unique Tag Name (like E1). After getting those beacons at coordinator's end, coordinator can easily map the association of a tag with its nearest router.

In order to evaluate the tracking performance of the system in the above topology, we evaluated the effect of beaconing rate of tags on tracking performance. We have repeated the test in the same scenario (8 Routers, 1 Coordinator) keeping the beaconing rate at 2 seconds and 5 seconds respectively. We have also repeated the experiment keeping beaconing rate at 2 second and increasing number of tags in the system gradually from 1 to 10. Similarly, keeping beaconing rate at 5 seconds we have also observed the effect of increasing number of devices in the network on tracking efficiency.

Probability of getting a beacon (η) is measured as per the following formula.

$\eta = \text{Actual number of beacons received by the coordinator} / \text{Total number of beacons sent by a tag}$

The probability of getting beacons in different scenarios is shown in figure 2. The graph shows that the probability of getting beacons decreases very slightly for high beaconing rate because increase in beaconing rate increases chance of beacon loss due to congestion caused by multiple beacons in the system. As we decrease the beaconing rate the probability of getting beacons increases. However, since movement of miners is slow compared to beaconing rate, tracking performance will not get affected by loss of a few beacons.

Tracking precision depends on the transmission range of routers. To get high precision, transmission range of routers may be reduced. But that in turn will require placement of more number of routers in order to form a connected mesh network.

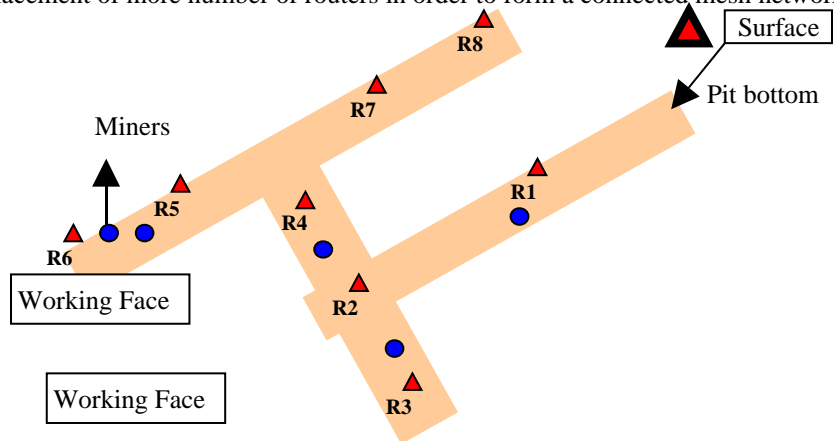


Fig. 7. The Test Bed Implementation in an underground mine

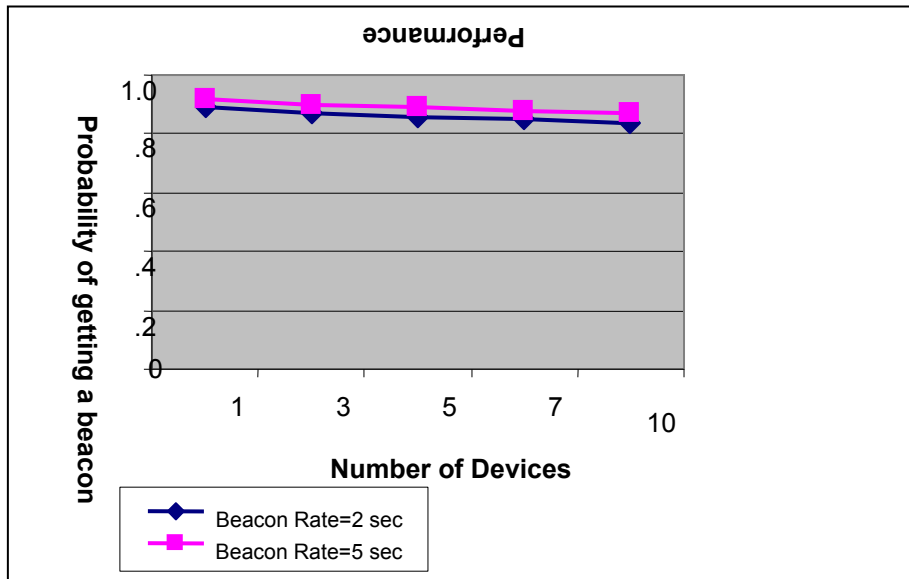


Fig. 8. Analysis of Tracking performance varying Beacon Rate & Number of tag

6. Related Work

The International Telecommunications Union (ITU), in its report on the future of the Internet, coined the term “Internet of Things” in November 2005. The report envisioned a case where we could see “remote controlled clothing, cars that alert their driver when they have developed a fault, managers who check on workers through the RFID devices embedded in their phones, and bags that remind their owners that they have forgotten something” [2]. It highlighted the situation where humans would be the minority in generating and using information over the internet. Devices and “things” would be smart enough to communicate with each other and establish a “thing to thing” network.

Research on establishing a practical “Internet of Things” has been sedate with little articulated work. [4] develops an architecture for a uniform protocol architecture between different things with the Internet forming a major chunk of the communication network. RFID tags are considered for the wireless mesh network.

The architecture proposes adapting the TCP/IP protocol structure for wireless needs termed STP/SP (Smart Transport Protocol/ Smart Protocol). Similar work has been done in [11] where the active RFID tags are built to run on the Host Identification Protocol (HIP). This makes it possible for the tags to talk to IP endpoints on the Internet.

The Internet of Things has also spawned interest in the middleware architecture which acts as the gateway between the sensor networks and the Internet. [8] looks to develop abstractions for the sensors in a network and thus support a flexible architecture and zero programming of the sensor devices.

The architectures developed so far explore a homogeneous protocol structure from an end to end perspective. However, the devices and the networks are diverse enough to predict the formation of a single standard that fits best in every circumstance. The research in each aspect of the “Internet of things” has been significant with the development of structures efficient for their respective needs. Our architecture thus uses the already well defined protocol structures in each domain and develops an abstraction to the underlying structure.

7. Conclusion

In this paper, we have developed a unified framework for asset visibility environment tacking through the Internet. The architecture comprises of the sensor network with active RFID devices on one end and the web enabled asset management interface on the other. The protocol conversion is made at the gateway which links the sensor network to the Internet. The tracking applications are typified by a well known path to be covered. Using this apriori information, we develop a modification of the C_{skip} algorithm for addressing of the sensor network nodes and the routing of packets. Through this, we avoid the address wastage of the C_{skip} algorithm and thus can realize an arbitrary topology. We provide a simple algorithm to realize the addressing and the routing. This new algorithm has been implemented for practical use on CC2420, a TI based board. The test bed implementation in an underground mine, we have implemented an “Internet of Things” has been elaborated.

There are a few aspects we would like to address in the future. The unified framework developed in this paper, gives the power of abstracting the underlying architecture at the gateway. For example, the sensor network can be an Ethernet based IP system or a host of WiFi Hotspots. The underlying structure and nature of the network does not affect the architecture of the “Internet of Things”. However, this abstraction requires a formalization of the services that must be offered at the sensor network and gateway interface. This set of services can only be determined when the entire end to end service requirements are ascertained. We, thus, would like to develop a structured approach and framework for identifying and designing the services at the interfaces.

References

- [1] Akyildiz, I.F., Xudong Wang: A Survey on Wireless Mesh Networks, IEEE Communications Magazine (September 2005)
- [2] BBC News: <http://news.bbc.co.uk/go/pr/fr/-/1/hi/technology/4440334.stm> (November 2005)
- [3] CC2420: <http://focus.ti.com/docs/prod/folders/print/cc2420.html>
- [4] Guy Pujolle, An Autonomic-oriented Architecture for the Internet of Things, IEEE JVA (2006)
- [5] Ho-In Jeon, Yeonsoo Kim: Efficient, Real-Time Short Address Allocations for USN Devices Using LAA (Last Address Assigned) Algorithm, 9th International Conference on Advanced Communication Theory (February 2007)
- [6] IEEE Std. 802.15.4-2003, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (2003)
- [7] ITU Report on Internet of Things – Executive Summary: www.itu.int/internetofthings/
- [8] Karl Aberer, Manfred Hauswirth, Ali Salehi, Middleware support for the “Internet of Things”, www.manfredhauswirth.org/research/papers/WSN2006.pdf (2006)
- [9] Kwang Koog Lee, Seong Hoon Kim, Yong Soon Choi, Hong Seong Park: A Mesh Routing Protocol using Cluster Label in the ZigBee Network, IEEE International Conference on Mobile Adhoc and Sensor Systems (October 2006)
- [10] Michael J. Hammons, Greg Chisholm: Enabling Total Asset Visibility, Defense Transportation Journal (August 2006)
- [11] Pascal Urien, et al, HIP-based RFID Networking Architecture (2007)
- [12] Ran Peng, Sun Mao-heng, Zou You-min, ZigBee Routing Selection Strategy Based on Data Services and Energy-balanced ZigBee Routing, IEEE Asia-Pacific conference on Services Computing (December 2006)
- [13] RFID Journal, www.rfidjournal.com
- [14] TIMAC : <http://focus.ti.com/analog/docs/gencontent.tsp?familyId=367&genContentId=31261> (2007)
- [15] ZigBee Alliance: www.zigbee.org