DEVELOPMENT OF ANTI-THEFT SYSTEM FOR WIRELESS SENSOR NETWORKS IN CLOUD ENVIRONMENT

K.Kiran Kumar, K.V.S Krishna, S. Srilakshmi

Department of Electronics and Communication Engineering, MRITS,HYDERABAD, AP, INDIA. Department of Electronics and Communication Engineering, MRITS,HYDERABAD, AP, INDIA.
Email id: kumar.kakkireni@gmail.com

ABSTRACT: A new anti-theft system is designed using WSN in cloud environment, where broad ranges of vital applications that acquire and process information from the corporeal world are in the extensive need of Wireless sensor networks. However, the limited resources of a sensor, especially limited battery life, limited bandwidth and limited processing power, are the main challenges for deploying and operating WSNs. This paper proposes an architecture based on cloud computing for wireless sensor network in anti-theft system, where we can easily get know of the devices or the things that are missing in the prescribed region or place or in a company. These data if combined with various web-based virtual communities can prove to be beneficial in several significant areas like healthcare, military and data monitoring and analyzing, etc.
Keywords: WSN, Cloud Environment

1 INTRODUCTION

Wireless sensor network (WSN) is a self-organizing Network consisting of a lot of sensor devices that connect toothers through wireless communication channel in multi-hopmanner. Sensors collect environment parameters andtransmit sensing data back to a central management node(i.e., a sink node) for further processing. Nowadays, WSNhas been applied in many fields, such as environmentmonitoring, military, surveillance, disaster rescue andhealthcare etc., and it is more widely used in the Internet of things (IoT) era.

The communication among sensor nodes using Internet is often a challenging issue. At the same time the data of sensor network should be available at any time, at any place. It is possibly a difficult issue to assign address to the sensor nodes of large numbers; so sensor node may not establish connection with internet exclusively.

However, sensors are usually low cost devices equippedwith limited resources, e.g., processing power, memory,wireless bandwidth, and battery. The design of WSN musttake care of these constrains, especially the battery limitationthat determines the lifetime of a sensor and a sensor network.All layer protocols used in WSN areoptimized to reduce energy consumption, including MAClayer, network layer (routing protocols), transport layer, and cross-layer approaches.Since transmittingoperation consumes more energy comparing against sensingand processing operations, some other technologies havebeen proposed to save energye.g., in-network data processing, mobile sink for data collection, andtopology reorganization.

Cloud environment is considered as a cost efficient way of IT resource provision manner. It offers a number ofadvantages such as scalability, agility and economyefficiency, in comparison of traditional IT infrastructure. Thecloud computing technology invented by Google is suitablefor big data storage and processing.

Each sensor node is programmed with the required application. Sensor node also consists of operating system components and network management components. On each sensor node, application program senses the application and sends back to gateway in the cloud directly through base station or in multi-hop through other nodes.

In this paper, we propose a architecture based on cloud environment for wireless sensor network for anti-theft system. In thisarchitecture, a cloud acts as a virtual sink and collectssensing data in multiple points. Therefore, the WSN isnaturally divided into units which we refer as “zones”. Eachnode in the cloud is responsible for data collection of sensorsin a zone. The sensors in a zone are organized as a localWSN in flat or hierarchy topology, and these local networksare integrated together by the cloud. As a result, the averageend-to-end path length of packet transmission could beshortened, and the energy consumption would be reduced. Moreover, data in cloud are stored and processed indistributed manner, thus complicated tasks could becompleted timely, which would be preferred for largevolume data process.

The rest of the paper is organized as follows. In Section 2& Section 3 we have presented an overview of Clouds and Sensor Network. In section 4 we have discussed various application scenarios of Sensor Network in Cloud environment. Lastly, Section V concludes our work.

2 CLOUD: OVERVIEW

An all-cloud environment describes a company, organization or individual that uses a Web-based application for every task rather than installing software or storing data on a computer. All-cloud environments are not common, but a move toward this is a long-term goal for cloud computing enthusiasts and cloud capitalists.Servers in the cloud can be physical machines or virtual machines. It is an alternative to having local servers handle applications.

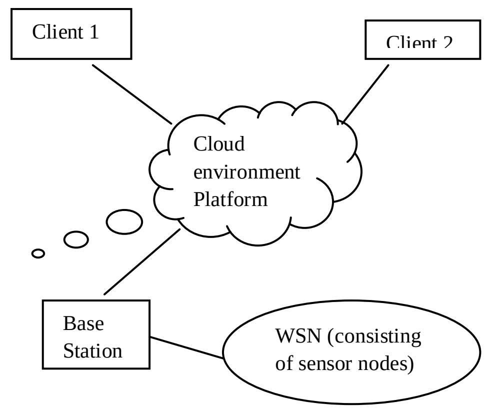

Fig 1: Block diagram of WSN in cloud environment

The end users of a cloud computing network usually have no idea where the servers are physically located they just spin up their application and start working. Advanced clouds typically include other computing resources such as storage area networks (SANs), network equipment, firewall and other security devices. Cloud computing also describes applications that are extended to be accessible through the Internet. These cloud applications use large data centers and powerful servers that host Web applications and Web services. Anyone with a suitable Internet connection and a standard browser can access a cloud application.

Many formal definitions have been proposed in both academia and industry, the one provided by U.S. NIST (National Institute of Standards and Technology) appears to include key common elements widely used in the Cloud Computing community:

Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

3 ARCHITECTURE:

The architecture is shown in Fig 1. A number of special nodes (sink points) distributed across the WSN area constitute a cloud. We refer this type node as "cloud node", which is equipped with more resources. Furthermore, a cloud node acts as a sink for sensors nearby.

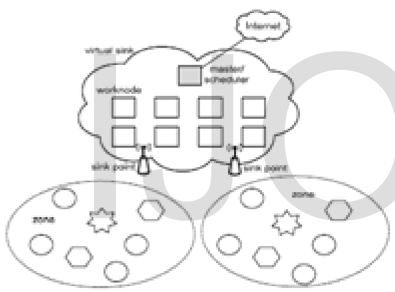

Fig 2: Cloud computing based WSN architecture

Therefore, the architecture is naturally cluster based. In order to differentiate from the term "cluster" in traditional WSN, we refer a cluster as a "zone" in this thesis. These sensors in a zone are organized as independent local WSNs (LWSN), and all LWSN are integrated together by the cloud. The cloud can be viewed as a "virtual sink" for the whole sensor network.

3.1 Organizing Sensors in a Zone:

We present a different way of heterogeneous sensors organization, as shown in Fig 2. The homogeneous sensors form a WSN (a different type sensor could be used as a gateway) and send their data to the sink. Each type sensors form a logical independent (and physical overlapped) WSN and these WSNs access the same sink. Data processing software is deployed in the cloud. After processing data from all sensors, the cloud can designate sensors to perform properly through the accessed sink point. If the size of a zone is reasonable, the scheduling commands from the sink point could reach the destination sensor timely. This way of organization is different from the single-tier clustered architecture of WMSN. First, the independent WSN is built in a zone of which the size is smaller, instead of the whole sensor network. Second, the cloud can control activities of a sensor timely based on data collected from the whole WSN.

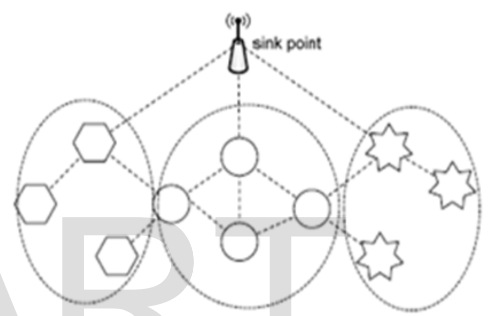

Fig 3: Organizing sensors in a zone

3.2 Features of Cloud:

The following are the essential features of cloud computing:

1) **Service on demand**: The request of the clients to avail resources can be fulfilled automatically without human interaction.

2) **Elasticity of demand**: There is no formal agreement or contract on the time period for using the resources. Clients can use the resources whenever they want and can release when they finish.

3) **Abstraction**: Resources are hidden to clients. Clients can only use the resources without having knowledge regarding location of the resource from where data will be retrieved and where data will be stored.

4) **Network access**: The client application can perform in various platform with the help of mobile phone, laptop and PDA using a secure internet connection.

5) **Service measurement**: Although computing resources are pooled and shared by multiple clients (i.e. multi-tenancy), the Cloud infrastructure can measure the usage of resources for each individual consumer through its metering capabilities.

6) **Resource pooling**: The resources are dynamically assigned as per clients' demand from a pool of resources.

3.3 Services of Cloud:

The cloud provides following three services:

1) SaaS(Software as a Service): This model provides services to clients on demand basis. A single instance of the service runs on the cloud can serve multiple end user.. Google is one of the service providers of SaaS.

2) PaaS(Platform as a Service): This model provides software or development environment, which is encapsulated & offered as a service and other higher level applications can work upon it.

3) IaaS(Infrastructure as a Service): This model provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data center space etc.

3.4 Cloud Computing Models:

The following models are presented by considering the deployment scenario:

1) Private Cloud: This cloud infrastructure is operated within a single organization, and managed by the organization or a third party irrespective of its location.

2) Public Cloud: Public clouds are owned and operated by third parties. All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. These are managed and supported by the cloud provider.

3) Community Cloud: This cloud infrastructure is constructed by number of organization jointly by making a common policy for sharing resources. The cloud infrastructure can be hosted by a third-party vendor or within one of the organizations in the community.

4) Hybrid Cloud: The combination of public and private cloud is known as hybrid cloud. In this model, service providers can utilize 3rd party Cloud Providers in a full or partial manner so that the flexibility for using the resources is increased.

4 ROUTING PROTOCOLS IN WSNS:

Routing protocols in WSNs are broadly divided into two categories: Network Structure based and Protocol Operation based. Network Structure based routing protocols are again divided into flat-based routing, hierarchical-based routing, and location-based routing. Protocol Operation based are again divided into Multipath based, Query based, QoS based, Coherent based and Negotiation based.

4.1 The Tcp/Ip Protocol:

The Transmission Control Protocol/Internet Protocol (TCP/IP) suite has become the industry-standard method of interconnecting hosts, networks, and the Internet. As such, it is seen as the engine behind the Internet and networks worldwide.

Although TCP/IP supports a host of applications, both standard and nonstandard, these applications could not exist without the foundation of a set of core protocols. Additionally, in order to understand the capability of TCP/IP applications, an

ISSN 2278-7763

understanding of these core protocols must be realized.

The TCP/IP stack is comprised of modules. Each module provides a specific function, but the modules are fairly independent. The TCP/IP layers contain relatively independent protocols that can be used depending on the needs of the system to provide whatever function is desired. In TCP/IP, each higher layer protocol is supported by lower layer protocols. The whole collection of protocols forms a type of hourglass shape, with IP in the middle, and more and more protocols up or down from there.

5 IMPLEMENTATION

In this project the anti-theft system using WSN in cloud environment is implemented with necessary modules present in it, such as microcontroller, RF sensor, WSN in cloud environment.

The LPC1769 is an ARM Cortex-M3 based microcontroller for embedded applications requiring a high level of integration and low power dissipation. The ARM Cortex-M3 is a next generation core that offers system enhancements such as modernized debug features and a higher level of support block integration.

Fig 4: ARM 3Cortex snap shot

6 RESULT

The results of Anti-theft system using WSN in cloud environment are shown below.

In this thesis a web page is created is created using the TCP/IP protocol as mentioned in IV chapter where it uses transfer the data using the layers and protocols mentioned in the layers. Where IP is the default address that can be used in TCP to transfer the data using the address.

Fig 5: Snapshot when interrupt occurred.

Whenever an interrupt comes in between the sensor nodes there occurs an intrusion as the data could not be transmitted from one end to the other as a result we can see that an intrusion is occurred (shown in Fig: 5).

When there is no interruption between sensor nodes the data is transmitted from one end to other as the data is transmitted between nodes there does not occur any intruder between the nodes (shown in Fig: 6).

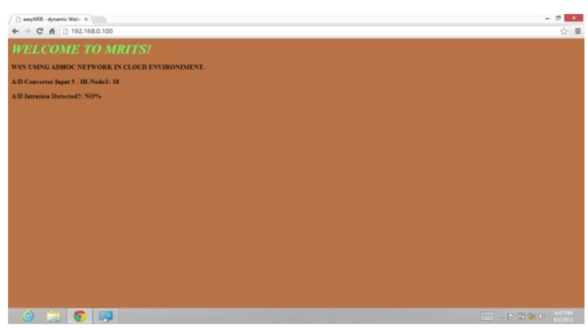

Fig 6: Snapshot when interrupt not occurred.

7 CONCLUSION

A novel architecture for wireless sensor network based on the cloud computing platform. The cloud acts as a virtual sink and has multiple sink points which could collect sensing data from WSN. Therefore, the WSN is naturally divided into a number of zones. The sensors in a zone could be organized in flat or hierarchy way as in traditional WSN. We also propose a new way of sensor organization in a zone: the homogeneous sensors form a WSN, while heterogeneous sensors form logical independent but physically overlapped WSNs. Sensors could be managed by the cloud through sink point accessed. All WSNs in zones are integrated together by the cloud. Sensing data in cloud are stored and processed in distributed manner.

8 FUTURE SCOPE:

Later this could be implemented using Wireless Sensor Networks in Hadoop, where the storage of the data is becoming a problem so that it can be done by using the sensors using the Hadoop.

REFERENCES

[1] S. Das, C. Perkins and E. Royer, "*Ad Hoc On Demand Distance Vector (AODV) Routing*", IETF RFC3561, July 2003.

[2] D. Johnson, "*The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR*)", IETF Internet Draft, draft-ietf-manet-dsr-09.txt, April 2003.

[3] P. Jacquet and T. Clausen, "*Optimized Link State Routing Protocol*", IETF Internet Draft, draft-ietf-manet-olsr-11.txt, July 2003.

[4] M. Lewis, F. Templin and R. Ogier, "*Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)*", IETF Internet Draft, draft-ietf-manet-tbrpf-09.txt, June 2003.

[5] M. Marina and S. Das, "*On-demand Multipath Distance Vector Routing in Ad Hoc Networks*", in Proceedings of the International Conference for Network Procotols (ICNP), Riverside, Nov. 2001.

[6] V. Park and M. Corson, "*A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks*", Proceedings of IEEE INFOCOM '97, April 1997.