Available online at www.elixirpublishers.com (Elixir International Journal)

Adoc Network

Elixir Adoc Network 58A (2013) 15060-15063

ISSN: 2229-712X

Ad-hoc network and microcontroller remote for early warning system in forest fire control

S.Philomina, T.V.U.Kiran Kumar and S.Beulah Hemalatha
Department of ECE, Bharath University, Chennai.

ARTICLE INFO

Article history:
Received: 23 November 2012;
Received in revised form:
15 May 2013;
Accepted: 21 May 2013;

Keywords
Remote,
Fire,
Microcontroller.

ABSTRACT

Using ad-hoc network a reliable technological condition has been provided for automatic Real-time monitoring and control of forest fires. This paper presents a new type of early warning systems which use a wireless sensor network to collect the information of forest fire, wireless sensor motes constitute microcontroller and zigbee protocol for smart monitoring and control the network through the self-organization of route.

Introduction

Traditionally, fire prediction can only analyzed and calculated the predicted weather conditions to get a rough and rigid fire index value. What's more, it used the traditional manual inspection methods which can't realize on-site and real-time monitoring and control. In recent years, because of the rapid development of sensors, microprocessors, and network technology, a reliable technological condition has been provided for our automatic real-time monitoring of forest fires control. This paper presents a new type of early warning systems which use a wireless sensor network to collect the information of forest fire-prone sections for forest fire, wireless sensor nodes constitute a smart monitoring and control network through the self-organization and transmits the messages to the control centre through the network, thus we can achieve the remote control of the forest fire.

During summer, when there is no rain for months, the forests become littered with dry senescent leaves and twigs, which would burst into flames ignited by the slightest spark. Forest fires can be either natural or controlled and caused by heat generated in the litter and other biomes in summer through carelessness of people (human neglect). Sometimes, forest fires purposely caused by local inhabitants.

Types Of Forest Fire

Forest fires differ depending upon its nature, size, spreading speed, behaviour etc. Basically this can be sub grouped into four types depending upon their nature and size as follows

1. Underground Fire (muck fire): Fire of low intensity consuming the organic matter beneath and the surface litter of forest floor are sub-grouped as underground fire. This fire spreads very slowly and may continue to burn for months and destroy vegetative cover of the soil and difficult to detect.
2. Surface Fires: Burning of undergrowth & dead material along the floor of the forest. In general it is very useful for the forest growth and regeneration. It may be a very hot, fast moving fire.
3. Ground Fires: Ground fires burn underneath the surface by smouldering combustion & are most often ignited by surface fires. A true ground fire spreads by a slowly smouldering edge with no flame and little smoke and hard to detect.
4. Crown Fires: Most unpredictable fire, which burns the top of trees or shrubs & spread rapidly by wind.

In India the Central Government and each State and Union Territory has its own separate forest department. The Ministry is implementing a plan scheme "Modern Forest Fire Control Methods". Major areas affected by the forest fire are eastern and western Himalayan regions and in the western gauds. Of the total inventoried forest area of the country, on an average 8.92% is affected by frequent fire and 44.25% by occasional fire. Burning of forests leads to global warming, pollution, depletion of ozone layer, soil erosion and landslide. In India there is as yet no proper action plan to control forest fires.

Wireless sensor networks have a wide application prospect and great value in the military, agriculture, environmental monitoring, medical and health, intelligent transport, building monitoring, industrial production control, as well as commercial and other fields.

This project is about forest fire prevention by giving information about fire sensed using sensors and transmitted through ad-hoc network. This method prevents forest fire and maintains our countries natural wealth. It achieves shortest path communication using Mesh topology and distance vector routing algorithm. It reduce size, improve precision, increase life cycle and to save energy. In this work sensors, microcontrollers and network technology has been used for automatic real time monitoring of forest fires control. Today, the application of ad-hoc network getting familiar because it doesn't require any access point and utilizes the shortest path algorithm.

Wireless Sensor Networks

Features of wireless sensor networks are Interoperability and Interference, Real time data acquisition and processing, Reliability and Robustness, Energy conservation, Data Management, Data privacy and Security and Comfort and Unobtrusive operation

Tele:
E-mail addresses: philomina.november83@gmail.com

Design space for wireless sensor networks are Deployment of sensor nodes, Mobility, Cost and Size of the Wireless node, Infrastructure of the Network, Network Coverage, Network Size, Power Management, Life time of the Sensor networks and Quality of service requirements in the network

Scope Of Ad-Hoc Routing In Communication

A reliable technological condition has been provided for our automatic Real-time monitoring of forest fires control. This project presents a new type of early warning systems which use a wireless sensor network to collect the information of forest Fire-prone sections for forest fire, wireless sensor nodes constitute a "smart" monitoring and control network through the self-organization and transmits the messages to the control centres through the network, thus we can achieve the remote control of the forest fire

Ad-hoc networks

An ad-hoc network is a local area network (LAN) that is built spontaneously as devices connect. Instead of relying on a base station to coordinate the flow of messages to each node in the network, the individual network nodes forward packets to and from each other. In the Windows operating system, ad-hoc is a communication mode (setting) that allows computers to directly communicate with each other without a router.

Peer-to-peer communication

Ad-hoc routing uses peer-to-peer communication, Peer-to-peer is a communications model in which each party has the same capabilities and either party can initiate a communication session. Other models with which it might be contrasted include the client/server model and the master/slave model. In some cases, peer-to-peer communications is implemented by giving each communication node both server and client capabilities. In recent usage, peer-to-peer has come to describe applications in which users can use the Internet to exchange files with each other directly or through a mediating server. IBM's Advanced Peer-to-Peer Networking (APPN) is an example of a product that supports the peer-to-peer communication model.

Distance vector routing

In computer communication theory relating to packet-switched networks, a distance-vector routing protocol is one of the two major classes of routing protocols, the other major class being the link-state protocol. A distance-vector routing protocol uses the Bellman-Ford algorithm to calculate paths. A distance-vector routing protocol requires that a router informs its neighbours of topology changes periodically and, in some cases, when a change is detected in the topology of a network. Compared to link-state protocols, which require a router to inform all the nodes in a network of topology changes, distance-vector routing protocols have less computational complexity and message overhead.

Distance Vector means that Routers are advertised as vector of distance and direction. 'Direction' is represented by next hop address and exit interface, whereas 'Distance' uses metrics such as hop count. Routers using distance vector protocol do not have knowledge of the entire path to a destination. Instead DV uses two methods:

1. Direction in which or interface to which a packet should be forwarded.
2. Distance from its destination.

The methods used to calculate the best path for a network are different between different routing protocols but the fundamental features of distance-vector algorithms are the same across all DV based protocols.

Common Ad-Hoc Routing Protocols

This section briefly summarizes four popular ad-hoc routing protocols AODV, DSR, OLSR, and BATMAN. For all of these protocols, implementations for real world use are existing as a stable running version.

A. Ad-hoc On-demand Distance Vector (AODV)

The AODV routing protocol is a reactive routing protocol and searches for a route on-demand. In case a certain node is part of an active route, Hello messages are used to obtain the route status. These Hello messages are broadcasted periodically to all neighbours. If a neighbour does not send a Hello message within a specified time a link loss is detected and the node is deleted from the routing table. In addition, a Route Error message (RRER) is generated. To discover a route to an unknown destination, a Route Request (RREQ) message is broadcasted. Each intermediate node which is not the destination and without a route to the destination receiving and broadcasts RREQ. In case the RREQ is received more than once, only the first reception will result in a broadcast. To avoid uncontrolled dissemination of RREQ messages, each RREQ has a certain time to live (TTL) after which it is discarded. When the destination receives a RREQ message, a Route Reply (RREP) message is generated a sent back to the source in unicast hop by hop fashion along the route which was determined by the RREQ message. After generating a RREP message, the RREQ message is discarded at this node. As the RREP propagates, each intermediate node creates a route to the destination. After the source receives the RREP, it records the route to the destination and begins sending data. In case the source receives multiple RREPs, the route with the shortest hop count is chosen. The status of each route is maintained in the local routing table and timers are used to determine link failures which will result in the creation of Route Error messages (RERR).

B. Dynamic Source Routing (DSR)

DSR is also a reactive ad-hoc routing protocol which works similar to AODV without using Hello messages for route maintenance. However, it uses source routing. DSR allows the network to be completely self-organizing and self-configuring, without the need of any existing network infrastructure or administration. DSR does not use any periodic routing advertisement, link status sensing, or neighbour detection packets, and does not rely on these functions from any underlying protocols in the network. DSR is composed of two main mechanisms that work together to allow the discovery and maintenance of source routes in the ad-hoc network. In case source node (S) wants to send data to an unknown destination host (D), S initiates the Route Discovery mechanism. S broadcasts a Route Request message which identifies the source and destination of the Route Discovery to all neighbours. A Route Request also contains a record listing the address of each intermediate node which was forwarding this particular copy of the Route Request. A node which receives this Route Request without being the destination looks up for a source route to the requested destination in its route cache. Without any source route present in its own route cache, the node appends its own address to the route record and broadcasts the Route Request message. In case this request message was received more than once, it is simply discarded. As soon as the Route Request message arrives at the desired destination D, a Route Reply message to S is created which contains an accumulated route record of the Route Request. After S receives this Route Reply, it caches the corresponding route in its route cache and S is ready to transmit data. Of course, there exist mechanisms to omit flooding of the network with Route Requests. A hop limit was introduced and every time a Route Request is forwarded, the hop limit is decremented by one. As soon as it reaches zero, the request is discarded. Also mechanisms for avoiding infinite recursion of Route Discoveries are implemented.

C. Optimized Link State routing (OLSR)

OLSR is a table-driven, pro-active routing protocol for mobile ad-hoc networks. It uses hop-by-hop routing – each node uses its local information to route packets. OLSR minimizes the overhead from flooding of control traffic by using only selected nodes – called Multipoint Relays (MPR) – to retransmit control messages. Each node in the network selects a set of nodes in its neighbourhood, which may retransmit its messages. This set of selected neighbour nodes is called the MPR set of that node. The neighbours of node N which are not in its MPR set receive and process broadcast messages but will not retransmit broadcast messages received from node N. The MPR set is selected such that it covers all 2-hop nodes. That means every node in the 2-hop neighbourhood of N must have a link to the MPRs of N. OLSR continuously maintains routes to all destinations in the network. Therefore, it is suitable for a large set of nodes communicating with each other. To distribute link and neighbourhood information, Hello messages are exchanged periodically. These messages are also used for link sensing and for checking the connectivity. Thus, the network topology is discovered and disseminated through the network, which allows the route calculation.

D. BATMAN

BATMAN (Better approach to mobile ad-hoc networking) is a new approach to ad-hoc routing. Unlike other algorithms that exist right now, BATMAN does not calculate routes. It continuously detects and maintains the routes by receiving and broadcasting packets from other nodes. Instead of discovering the complete route to a destination node, BATMAN only identifies the best single-hop neighbour and sends a message to this neighbour. These messages contain the source address, a sequence number, and a time-to-live (TTL) value that is decremented by 1 every time before the packet is broadcasted. A message with a TTL value of zero is dropped. The sequence number of these messages is of particular importance for the BATMAN algorithm. As a source numbers its messages, each node knows whether a message is received the first time or repeatedly.

Existing System

In the existing system Individual node requires access point to gate way in ordinary wired networks, more expensive, more power consumes in conventional wireless sensor networks, and difficult to replace and recharge battery in each nodes and Sensor networks are data centric, so addressed to every node to satisfy some conditions to initiate communication.

Proposed System

In the proposed system Ad-hoc network introduced instead of conventional wireless sensor networks and wired networks, Number of nodes and remote transmitting station reduce, Real time automation provided with RTOS, To prevent forest fire and maintain our countries natural wealth, To achieve shortest path communication using Mesh topology and shortest path routing algorithm, To reduce size, improve precision, increase life cycle and to save energy.

Proposed system involves following hardware components, PIC16F877A, XBee, MAX232, pc, sensors LM35, LDR, crystal oscillator, 5v supply unit, resistors, capacitors, diodes and a led indicator. And the following software components ccs compiler, proteus simulator, turbo c.

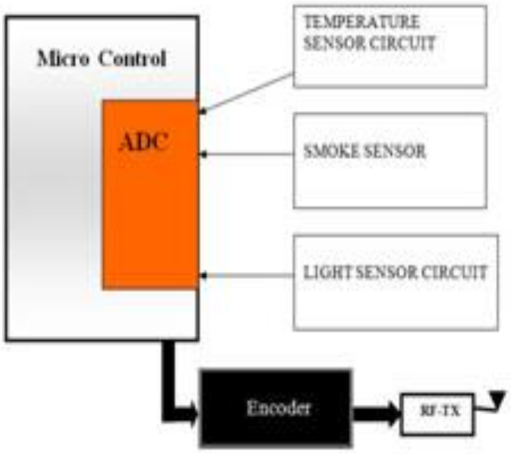

Figure 1: Slave 1

For the each slave there will be a micro controller unit, XBee unit, sensor unit, ADC convertor, microcontroller programmed with ccs compiler and tested using proteus simulator, distance vector routing is programmed in the microcontroller.

Initially each slave unit sends information to the neighbor nodes and waits for the acknowledgement. Each slave nodes identifies the nearest node to it and if any insertion of deletion of nodes also identified using this Distance vector routing method.

There after the data send to the nearest node and that node is forwarded it to the master unit by searching for the shortest path, because the shortest path the power consumption using this method can be reduced drastically.

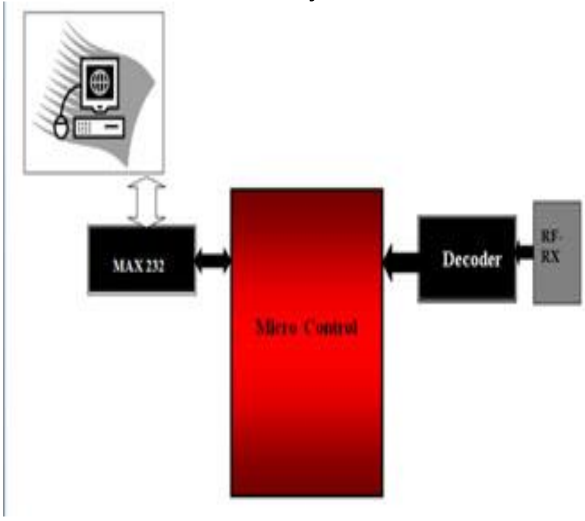

Figure 2: Master unit

Master unit consist of micro controller serial communication protocol RS232, XBee for transmission and reception, pc with turbo c to display the output. Microcontroller used here is PIC16F877A which is flash micro controller with inbuilt timer, i/o ports, ram and rom units. MAX232 used for the serial communication. Microcontroller is programmed using the simulator ccs compiler, and it is tested with proteus simulator.

Data received at the XBee unit is processed using microcontroller and send to the pc using serial communication. Pc shows the output whether fire happening or not, what is the temperature at the node, with the sending nodes identity.

Advantages:

* Use of ad-hoc networks could increase mobility and flexibility, as ad-hoc networks can be brought up and down in very short time.

* They could be more economical in some cases as they eliminate fixed infrastructure costs and reduce power consumption at mobile nodes.

* They are more robust than conventional wireless networks because of their non-hierarchical distributed control and management mechanisms.

* Because of short communication links (node-to-node instead of node to a central base station), radio emission levels could be kept at low level. This increases spectrum reuse possibility or possibility of using unlicensed bands.

* Because of multi-hop support in ad-hoc networks, communication beyond Line Of Sight (LOS) is possible at high frequencies.

Conclusion

Wireless sensor network technology is considered one of the important technologies which affect the lives of mankind in the future, and is being more and more concerned by technicians and scientists, the forest fire prevention is just one example of its applications, this technology can also be used in such as intelligent transportation, environmental detection, alarm floods, monitoring animal habitat, monitoring health status of bridges, monitoring the security situation under hole. Its development and application will give a profound impact to various fields of living and produced.

A pervasive application for fire fighting and over a ad-hoc network is presented and evaluated. Nodes of the application are: 1 aircraft, 9 tethered balloons, 1 control station and around 50 personal devices communicating, all with zigbee equipment. The aircraft, a sensor, flies in a survey over the burned area, capturing temperatures and images, and subsequently downloading the captured information to the ground devices. The only function of the tethered balloons is to improve the ad-hoc communications. The analysis of the connectivity graphs showed that the equipment on the tethered balloons should have at least a 4Km range to be useful in connecting fire fighter crews on a medium to large wild fire. Moreover, if the range rise up to 8Km, then multi-hop routing could be almost eliminated.

Adding the sensor as a new network node of the ad-hoc is shown to be very useful in this 4Km scenario. The sensor was already equipped with zigbee equipment because it was needed for downloading data to the ground control station. Thus the only modification needed is a costless introduction of the ad-hoc protocol. Great benefits are given for the fire fighters, who can obtain directly information’s taken from the sensors and commands from a direct connection with their manager.