ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 5, July 2012

A smart Home Security system based on ARM9

B. Srinivasa sarma, Dr. P. Sudhakar Reddy, IEEE member
Department of Electronics and communications engineering,
Sri Kalahastheeswara Institute of Technology, Andhra Pradesh-517640
srinivas_bondu@yahoo.com
psr_vlsi_dsp@rediffmail.com

***Abstract*:**

This paper A Smart Home Security System is based on ARM 9 and Ethernet technology. The total Smart Home Security System is build around the MINI 2440 board in which micro controller like S3C2440 is embedded.

The current paper Smart Home Security System discusses about how to acquire the data about the parameters (temperature, release of any poisonous gases and light intensity) present inside a house and how to send those parameters to the BOA server based on wireless technology like Zigbee and how a server can send the data to the remote client based on the technology like Ethernet when client makes a request to the BOA server. The server uses an USB type Web camera to capture the video images that are running currently in that house.

Keywords: Home security systems, ARM9, Ethernet, Embedded microcontroller, S3C2440

INTRODUCTION:

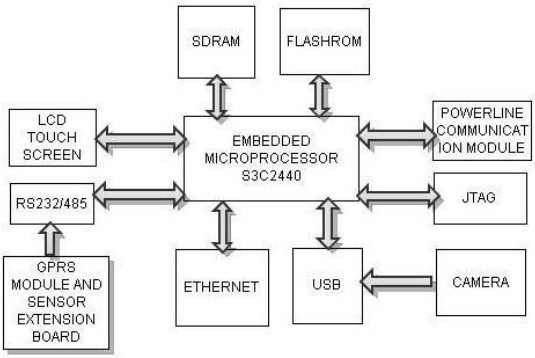
The S3C2440 chip is used as the core of these embedded systems which is associated with the technologies of fingerprint recognition and current high speed network communication. The primary functions are shown as follows:

I. Hardware Design:

The S3C2440 chip is used as the core of entire hardware. Furthermore, the modules of LCD, USB camera, RJ-45 cable, sensor expansion board are connected with the main chip (S3C2440).The SRAM and FLASH are also embedded in the system.

System Controller

The system uses 32-bit RISC processor Samsung S3C2440 with various features and peripherals. It's based on ARM 920T core and supports embedded Linux, WinCE, VxWorks and other embedded operating system. All the properties meet the requirements of the remote monitoring system. The System hardware architecture is shown in Figure.



System hardware architecture

The hardware of the system is mainly composed of the ARM9 processor based on S3C2440 and wireless transceiver transmission network based on CC2430.ARM data control unit hardware platform includes embedded CPU, Ethernet interface, serial communication port, Flash program controller, SRAM

static memory, debug ports, reset, power interfaces etc. The central processing uses 32-bit microprocessor of S3C2440, whose highest frequency is 533MHZ, and normal operating frequency is 400MHz. This system uses supervision to program the Linux system image. In this system, embedded Linux system image is as a gateway, use transplant BoA as system web server, and transplant SQLite database to storage the state of the detected environment and action information [2].

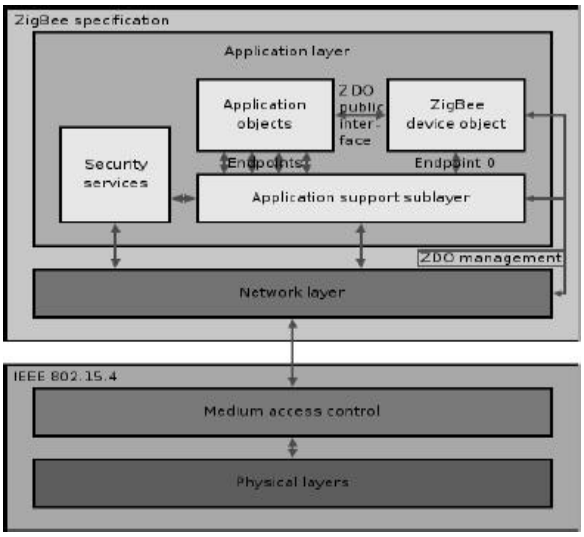
II. ZIGBEE:

ZigBee is the name of a specification for a suite of high level communication protocols which is simpler and cheaper than other networks replacing the string of wires present all over the place. The data rates of the Zigbee are above the levels of RS 232 and RS 485.Zigbee network modules employ different topologies depending on to the extent of the distance of communication [3].

(a) OVERVIEW:

ZigBee protocol is similar to that of OSI reference model which has the major advantage of upon the physical layer and medium access control defined in IEEE standard 802.15.4 (2003 version) for low-rate WPAN's.The different layers of the Zigbee which are dynamic in nature, which include: network layer, application layer, ZigBee device objects (ZDO's) and manufacturer-defined application objects which allow for customization and favor total integration.

Each layer easily can be modified with the changing time hence makes it easier to modify the particular layer without affecting the entire module. These are responsible for a number of tasks, which include keeping of device roles, management of requests to join a network, device discovery and security.



(Fig 1: zigbee specifications)

The various operating frequencies corresponding to the specification, particularly in the industrial, scientific and medical (ISM) radio bands; 868 MHz in Europe, 915 MHz in countries such as USA and Australia, and 2.4 GHz in most jurisdictions worldwide When compared with the Bluetooth and Wireless personal area network, Zigbee module reduces the complexity and cost of the overall network[3]. The most capable ZigBee node type is said to require only about 10% of the software of a typical Bluetooth or Wireless Internet node, while the simplest nodes are about 2% However, actual code sizes are much higher, closer to 50% of Bluetooth code size ZigBee chip vendors have announced 128-kilobyte devices.

The different layers that are present inside the zigbee communication are given below.

(b) NETWORK LAYER:

The network layer lays emphasis in determining how packets are routed from the source to destination. On the other hand, there is the layer control, which is used to handle configuration of new devices and establish new networks: it can determine whether a neighbouring device belongs to the network and discovers new neighbours and routers. The control can also detect the presence of a receiver, which allows direct communication and MAC synchronization.

(c) APPLICATION LAYER:

An application layer employs the protocols which vary with the common needs. It deals with the application objects which are defined by the manufacturer. The top most layer of the protocol is, the application layer which acts as an effective interface to its end users.

(i)Main Components:

ZDO, one of the main components of the application layer enables the description of the different devices with in the network such as Zigbee coordinator and the end device. It also ensures the secured relation by initiating the binding request between the devices.

The other, is the Application support sub layer (APS) which is main standard component of the layer, The APS, establishes the logical connection of devices based on their needs and services. It handles various addressing modes such as direct, indirect and broadcast. The direct addressing mode is adopted by specifying the destination Zigbee address (16 or 64 bit) and the APS destination end point, where as in the indirect addressing; we do not have to specify the destination of APS data unit. APS, which handles Zigbee coordinator, acts as the managing unit by extracting the required information from the binding table. As the union between both specified layers, it also routes messages across the layers of the protocol stack.

(d)SECURITY SERVICES:

The security services of Zigbee intend to promote three types of mechanisms, which are the important parts of Zigbee specification. They lay emphasize on the secured encryption of the data, distributed within all the devices. The usage of the services develops the protection of the frames, device management, key establishment and transportation of keys.

(i)Security architecture: Key architecture of the Zigbee security allows a set of 128 encryption keys which were commonly shared by Medium access layer, Network layer and application layer. All layers share the same set of keys by which the Network, Master and link keys were accessed by the Medium access sub layer. All stack layers use the Network key which is acquired by either pre installation or key transportation and the link keys, secured by the uni cast communications. Master keys used in the key establishment process enables the derivation of link keys.

(e)PROTOCOLS:

Zigbee provides three different types of protocols which allow the access of the network taking the concept, IEEE 802.15.4 of Full function device (FFD) and reduced function device (RFD).The formation of the Zigbee network, lies with the Zigbee coordinator, which is one of a kind FFD. The binding table entries are maintained by the Zigbee coordinator after establishing the Zigbee network and allocate the network addresses for those that are allowed to join the network. Zigbee networks support the beacon and non beacon enabled networks. An un slotted CSMA/CA channel access mechanism is used in the case of non-beacon-enabled networks (those whose beacon order is 15),The non beacon networks require more power supply, since the receivers remain continuously active. However, this allows for heterogeneous networks in which some devices receive continuously, while others only transmit when an external stimulus is detected. One of the examples of a heterogeneous network is a wireless light switch: where the Zigbee node, at the lamp may receive constantly, since it is connected to the mains supply, but when we consider a battery-powered light switch, which remains asleep until the switch is thrown. The switch then wakes up, sends a command to the lamp, receives an acknowledgment, and returns to sleep. In such a network the lamp node will be at least a ZigBee Router, if not the ZigBee Coordinator; the switch node is typically a ZigBee End Device.

In the case of beacon-enabled networks, the special network nodes called ZigBee Routers transmit

periodic beacons to confirm their presence to other network nodes. The synchronization of the devices lies with the Zigbee coordinator that has the option to transmit beacon signals. The Zigbee coordinator periodically generates the super frame which can also be called as beacon frame. Nodes may sleep between beacons, thus lowering their duty cycle and extending their battery life. Beacon intervals may range from 15.36 milliseconds to 15.36 ms * 214 = 251.65824 seconds at 250 kbit/s, from 24 milliseconds to 24 ms * 214 = 393.216 seconds at 40 kbit/s and from 48 milliseconds to 48 ms * 214 = 786.432 seconds at 20 kbit/s. However, low duty cycle operation with long beacon intervals requires precise timing which can conflict with the need for low product cost.

Zigbee devices are required to conform to the IEEE 802.15.4-2003 Low-Rate Wireless Personal Area Network (WPAN) standard. The standard specifies the lower protocol layers—the physical layer (PHY), and the medium access control (MAC) portion of the data link layer (DLL). This standard specifies operation in the unlicensed 2.4 GHz, 915 MHz and 868 MHz ISM bands. In the 2.4 GHz band there are 16 ZigBee channels, with each channel requiring 5 MHz of bandwidth. The center frequency for each channel can be calculated as, FC = (2405 + 5*(k-11)) MHz, where k = 11, 12, ..., 26.

The radios use direct-sequence spread spectrum coding, which is managed by the digital stream into the modulator. BPSK is used in the 868 and 915 MHz bands, and orthogonal QPSK that transmits two bits per symbol is used in the 2.4 GHz band.

The raw, over-the-air data rate is 250 kbit/s per channel in the 2.4 GHz band, 40 kbit/s per channel in the 915 MHz band, and 20 kbit/s in the 868 MHz band. Transmission range is between 10 and 75 meters (33 and 246 feet), although it is heavily dependent on the particular environment. The maximum output power of the radios is generally 0 dBm (1 mW).

The basic channel access mode specified by IEEE 802.15.4-2003 is "carrier sense, multiple access/collision avoidance" (CSMA/CA). There are three notable exceptions to the use of CSMA. Beacons are sent on a fixed timing schedule, and do not use CSMA. Message acknowledgements also do not use CSMA. Finally, devices in Beacon Oriented networks that have low latency real-time requirements may also use Guaranteed Time Slots (GTS) which by definition does not use CSMA.

LINUX SYSTEMS AND LINUX KERNEL DESCRIPTION

A complete system consists of five components: hardware, boot loader, kernel, operating system services and user applications, as shown in Figure.

User application refers to those word-processing program, internet applications, or other user-prepared in a variety of applications; Operating system services provided by the program is pointing to the user interface program such as system calls; Boot loader mainly take charge of completing the hardware detection and system boot. The operating system kernel is the main core of the operating system, which

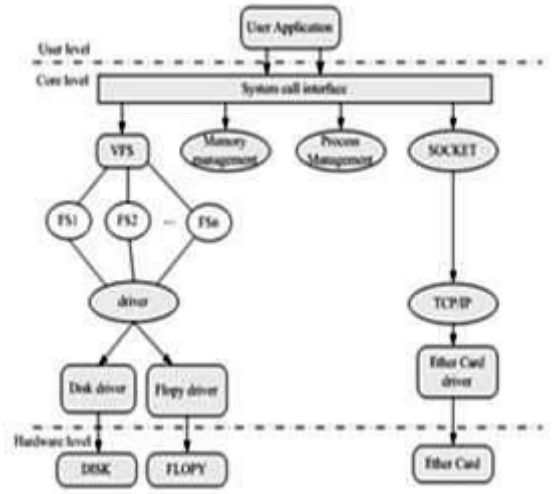


FIGURE 2. Linux Kernel Architecture

is the soul of the whole system. The operating system service program, the operating system kernel and Boot loader be seen as part of the operating system [4].

Linux kernel mainly constituted by the five modules, namely: the process of scheduling module, memory

management module, the virtual file system module, inter-process communication module and network interface modules. Figure 2 illustrates an important part of Linux kernel, as well as the relationships between them. Process scheduling module is responsible for controlling the process for the use of CPU resources, using a scheduling strategy to enable the process can be fair and reasonable access to the CPU, while ensuring the timely implementation of the core hardware operation; Memory management module is used to ensure the safety of all processes share the machine main memory area. It also supports virtual memory management, so that the process of Linux can use more memory than the actual memory capacity, and take use of the file system for temporary data in memory to exchange to an external storage device, when needed and then exchange back; The file system module used to support external drives and storage devices; Inter-process communication module used to support the multi-way exchange of information between processes; Network interface module provides access to a variety of network communication standards and support many network hardwares.

Linux is open source, and Linux operating system not only designed to have portability between different platforms, but also the required storage space is small. Linux kernel is the most bottoms and core part of the Linux and Linux operating system grows up based on Linux kernel, while the transplantation of Linux core is the most critical part for the development of any embedded Linux. All source code of kernel can be found in the /usr/src/Linux, and most application softwares are also designed to follow the GPL, while many of the Linux enthusiasts and the Linux developers around the world is a powerful technical support.

WEB SERVER

The system diagram of Embedded Web server

The system structure of embedded Web server is shown in Fig. 3. The entire system uses B/S mode. The client PC is connected to the Internet through a browser and then gets access to the embedded Web server. Through this way, remote login and operation are realized.

Compared with the traditional C/S mode, this mode is simple to use, convenient to maintain, and easy to extend.

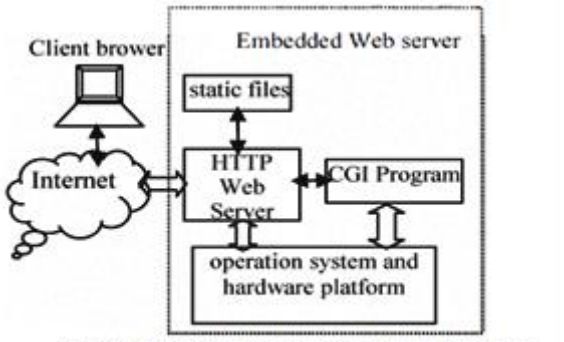


Figure 3. The system diagram of Embedded Web server

B. The choice of Embedded Web server

Generally speaking, the embedded devices have limited resources and don't need to handle the requests of many users simultaneously. Therefore they do not need to use the most commonly used Linux server Apache. Web server which is specifically designed for embedded devices are applied in such case. This kind of Web server requires relatively small storage space and less memory to run, which makes it quite suitable for embedded applications. If Web server only provides some static web pages such as simple online help and system introduction, then a static server can be adopted; if you need to improve system security or interact with users such as real-time status query and landing, then you have to use dynamic Web technologies.

Like a common Web server, an embedded web server can accomplish tasks such as receiving requests from the client, analysing requests, responding to those

requests, and finally returning results to the client. The following is its work process.

• Complete the initialization of the Web server, such as creating an environment variable, creating socket, binding a port, listening to a port, entering the loop, and waiting for connection requests form a client.

• When there is a connection request from a client, Web server is responsible for receiving the request and saving related information.

• After receiving the connection request, Boa analyses the request, calls analysis module, and Works out solutions, URL target, and information of the list. At the same time, it processes the request accordingly.

• After the corresponding treatment is finished, the Web server sends responses to the client browser and then closes the TCP connection with the client. For different request methods, the embedded Web server Boa makes different responses. If the request method is HEAD, the response header will be sent to the browser; If the request method is GET, in addition to sending the response header, it will also read out from the server the URL target file of the client request and send it to the client browser; If the request method is POST, the information of the list will be sent to corresponding CGI program, and then take the information as a CGI parameter to execute CGI program. Finally, the results will be sent to client browser [3].

WORKING PRINCIPLE:

The smart home security system is composed of sensor expansion board, video processing, and wired communication making use of Ethernet Protocol. The sensor expansion board consists of sensors like Temperature, Gas and LDR. The sensors data is digitized through parallel and 8-channel ADC like ADC0809 and given as an input to the processing device. This processing device makes use of UART technology to feed the sensor data to the Mini 2440 board (Friendly ARM) board. This Mini 2440 board consists of a micro controller like S3C2440.The video processing module like USB camera is interfaced to the Mini 2440 board. The USB camera is controlled manually to capture the continuous video images and these video images are saved to the buffer [1]. The application program transplanted into the ARM target board is used to display and processes the saved video images in the buffer. The current paper makes use of BOA server to handle the request from the clients so that clients can access the data related to the sensors and camera at the remote location.BOA server is a single tasking server. It means internally multiplexes all HTTP connections rather than forking of multiple copies for each connection. Client can access the data related to sensors and camera through B/S architecture at the remote location. The Ethernet technology on the server side helps to make the data global. The Ethernet technology on the server side helps to communicate with the clients for a speed of 100 Mbps (Mega Bits per Second).

CONCLUSTION:

ARM9 based embedded video processing technology provides the smart home security system, which has high reliability, cost effectiveness due to its recording parameters and remote monitoring features which can be easily upgraded and integrated with new functional modules to make an intelligent home security system.

REFERENCES

[1] A. Murat Tekalp, Digital video Processing, 1995.

[2] Andreas Krall, Softwares and compilers for embedded systems, 2003

[3] Robert Fauldi,Building Wireless Sensor Networks: With Zigbee, 2010

[4] Roderick Weskit Advanced Linux Networking, 2002.

[5] www.microcontroller.com