



ISSN: 2278 – 0211 (Online)

## Wi-Bot In Defence Using Ad-Hoc Communication Networks

**P. Ram Prashanth**

Department of ECE, Panimalar Institute of Technology, Chennai, India

**S. George Britto**

Department of ECE, Panimalar Institute of Technology, Chennai, India

**M. U. Majeesh**

Department of ECE, Panimalar Institute of Technology, Chennai, India

### **Abstract:**

*This paper presents the design of an automated security system in defence using a wireless controlled robot (WI-BOT) continuously monitoring the surroundings. A wireless camera has been installed on it, so that it can monitor enemy remotely when required. It can silently enter into enemy areas and send us all the information required through its tiny Camera eyes. Communications and Communication protocols play a major role in wireless controlled robot system, which inturn makes them suitable to address many real world applications. The peculiar characteristic of this WI-BOT is that it can also monitor the soldier's health using RF Module. Thus our paper focuses on advanced security and control of wireless robot by presenting the background of RFID, ad-hoc network and RF Module.*

**Key words:** Wireless robot; RFID; RF module; ad-hoc network

### **1.Introduction**

India is developing in many fields especially in nuclear research. Thus there is a chance of attack from other nations and terrorists, in many areas like Parliament, Marketplaces, Railway stations and country borders. Thus it is indeed the work of engineers to develop a strong automated technology in the field of defence against such evils. Today Robots have traditionally been put to use in environments that are too hazardous for man. Robots also work under precarious conditions, for search and rescue after disaster survivors. Similarly, robots are also put to work in underground mines. The faithful robots do not hesitate to tread even the dreaded terrain of battlefields. These robots were controlled by humans. We aim to develop a model which will be efficiently used to minimize terrorist causality. Being able to achieve reliable long distance communication is an important open area of research in robotics as well as other technology areas. As interest in robotics continues to grow, robots are increasingly being integrated into everyday life. The results of this integration are end-users possessing less and less technical knowledge of the technologies. Currently, the primary mode of robot communication uses RF. RF is an obvious choice for communication since it allows more information to be transferred at high speed and over long distance. The advent of high performance wireless local area network (WLAN) and ad hoc networking technology at relatively low cost, their use for wireless communications among mobile robots has become a practical proposition. However, in a large system with many mobile robots, it becomes difficult for all robots exchange information at a time because of their limited communication capacities. In this case, an ad-hoc robot networking scheme is more promising. This eliminates the need of a new infrastructure and detailed technical research. Thus we propose a model of wireless robot which uses an ad - hoc network to monitor those areas and to provide security.

### **2.Proposed Model**

Our proposed model has the following description,

#### *2.1.Hardware Description*

### 2.1.1.Robot

The Robot uses ad-hoc wireless technology having mainly two phase of defending operation. The Robot keeps on monitoring in two modes

- Intelligent mode( i-mode )
- Manual mode( M-mode )

In i-mode WI-BOT starts moving over surface and takes action according to the scenario. Thus by doing so it can reduce the human burden of controlling the bot. In certain critical situations it can be brought under users control using Manual mode command. In this mode an external stimulus is sent from Control centre to WI-BOT using ad-hoc network.

In first phase of defence, it is provided with two cameras which can perform the monitoring functions. In second phase, the robot consists of a RF receiver which receives the signals from the Soldier's body to monitor his health.

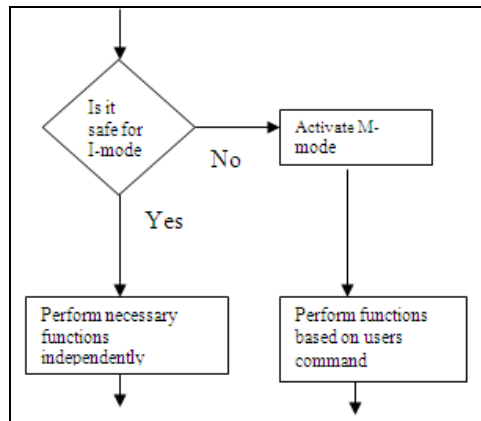


Figure 1: Flowchart For Robotic Control

#### 2.1.1.1.Cameras

The Robot is provided with two cameras to monitor both in day mode and night mode. In case of day mode, it is provided with a 360° IP camera which can rotate in all directions and entirely monitor the surrounding environment.



Figure 2: 360° IP Camera

In case of night mode, the thermal IR cameras present in the robot can perform the same functions. The automatic switching from one camera to other is being provided by means of LDR sensors. Thus by doing so it keeps track of the surrounding both in day and night mode and reports the control centre.

If the weather is cloudy the WI-BOT considers this as a critical situation and switches to manual mode.



Figure 3: Ir Camera

An Internet protocol camera, or IP camera, is a type of digital video camera commonly employed for surveillance, and which unlike analog closed circuit television (CCTV) cameras can send and receive data via a computer network and the Internet. Although most cameras that do this are webcams, the term "IP camera" or "net cam" is usually applied only to those used for surveillance. There are two kinds of IP cameras:

- Centralized IP cameras, which require a central Network Video Recorder (NVR) to handle the recording, video and alarm management.
- Decentralized IP cameras, which do not require a central Network Video Recorder (NVR), as the cameras have recording functionality built-in and can thus record directly to digital storage media, such as flash drives, hard disk drives or network attached storage.

A thermographic camera or infrared camera is a device that forms an image using infrared radiation, similar to a common camera that forms an image using visible light. Instead of the 450–750 nanometre range of the visible light camera, infrared cameras operate in wavelengths as long as 14,000 nm (14  $\mu$ m).

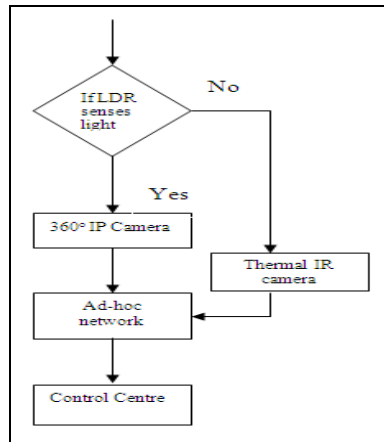


Figure 4: Flowchart For Camera Operation

#### 2.1.1.2. RF Module

The RF module operates at Radio Frequency. The corresponding frequency range varies between 30 KHz & 300 GHz. In this RF system, the digital data are represented as variations in the amplitude of carrier waves. This type of modulation is known as Amplitude Shift Keying (ASK).

Transmission through RF is better than IR because of many reasons. Firstly, signals through RF can travel through longer distances making it suitable for long range applications. RF signals can travel even when there is an obstruction between the transmitter & the receiver. RF transmission is stronger and reliable than IR transmission.

This RF module consists of an RF transmitter & RF receiver. The transmitter and receiver work at a frequency of 434 MHz. The transmission occurs at the rate of 1kbps-10kbps. The transmitted data are received by an RF receiver operating at the same frequency as that of the transmitter.

The soldiers are being provided with RF transmitter and sensors to measure the heart rate. The sensor output in the form of analog is converted in the form of digital form by means of an Analog to Digital Converter & provided to RF transmitter which is being received by the RF receiver by the Robot.

A regular update about soldier's health is provided to control office by the Robot. Thus by monitoring the heart beat rate any treat to soldiers by enemies can be identified by the WI-BOT and a rescue operation can be performed instantly without much damage to soldiers. The Reason behind the separate usage of RF Module is to reduce the work of controlling personnel in control room from frequent monitoring as this work is being done by WI-BOT itself.

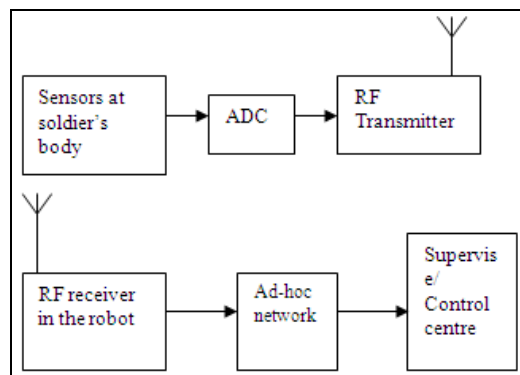


Figure 5: Block Diagram Of Soldiers Health Monitoring.

### 2.1.2. Supervise/Control Centre

The Control Centre is the place where all the nodes (Wi-Bots) are connected using Adhoc network. In supervisory state it monitors the image frames/videos taken from wireless cameras mounted in the Robot. The link is set by means of commercial WIFI boards, an access point placed on the Robot and another PCI board inserted on the desktop computer. In manual mode it produces signal accordingly.

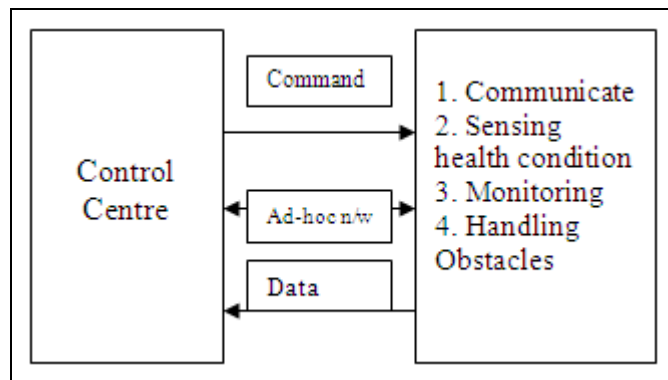


Figure 6: Operation Of Control Room

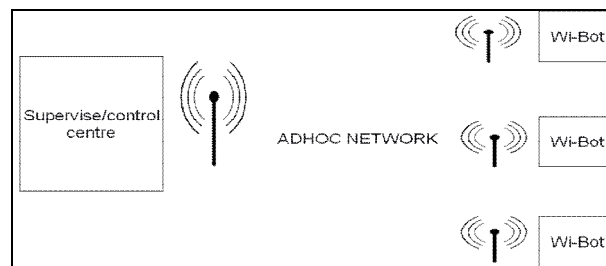


Figure 7: Layout Of Our Proposed System

### 2.1.2.1. RFID

Radio-frequency identification (RFID) uses a wireless non-contact system that uses radio-frequency electromagnetic fields to transfer data from a tag attached to an object, for the purposes of automatic identification and tracking.

In our proposed system, this provides the first line of defence against the spy attack from other nations or enemies. The authorized person is provided with RFID tag which is injected into his body (can also be put on his hand operated by his Fingerprint pattern) and RFID reader is placed at the entrance of the control room. Once the authorized person with RF tag enters within the range then automatically the door gets open. Thus it avoids the control of Robot manually by unauthorized persons (spy).

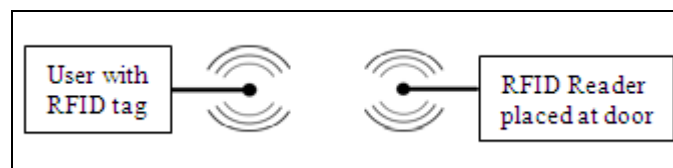


Figure 8

## 2.2. Ad-Hoc Robot Wireless Communication Network

### 2.2.1. Why Ad-Hoc Networking?

Consider a group of mobile robots that are required to autonomously disperse throughout a region, perform distributed sensing, monitoring or surveillance, and pass the sensed data to a single collection point. The robots are most likely equipped with only low power wireless transceivers whose range is too short to allow direct communication with the data collection point, but sufficient to allow robots to communicate with close neighbors. These circumstances qualify an ad hoc wireless networking scheme as a unique choice. The disadvantages of centralized control for robot teams are the robots had a single centralized point of failure. A whole team of robot will be rendered useless when their controlling computer was destroyed. This example clearly suggests that centralized control and communication could more easily lead to a fatal system breakdown. In other words, robustness may be low. Secondly, designers may not prefer a centralized system due to the design and cost consideration. To guarantee a certain level of QoS, expensive

base stations are required to cover the service area. Therefore, complex system management obviously increases the total cost of a system. On the other hand, decentralized and distributed systems based on local interactions among autonomous nodes support ad-hoc changes in population, connectivity and local constraints. They show robustness to local failures and scale very well and are sufficient for most applications. In unpredictable or unplanned environments mobile robots need to create a wireless network to cooperate and schedule tasks. Multi hop ad hoc networks capable of self creation and self- organization become a natural choice used to meet such needs.

	<b>IEEE 802.11b</b>
RF band (GHz)	2.4/5
Modulation	DSSS
Data rate(MBPS)	11(Shared)
Range(m)	30-1000
Network structure	ad-hoc
Power	$\leq 1\text{w}$

Table 1: Technical Specification Of WLAN

### 2.2.2.Mobile Robot Networking Layered Model

Mobile robot wireless networks provide the networking infrastructure to support the quality of service (QoS) needs (bandwidth, latency and reliability) of robot communications. They must support: quick reconfiguration (802.11, token ring, mobility management (mobile IP, AODV), service level agreement (SLA) management, and QoS (mobile Internet Protocol). The figure gives a layered model of mobile robot networking. It has transport, network, data link, and physical layers.

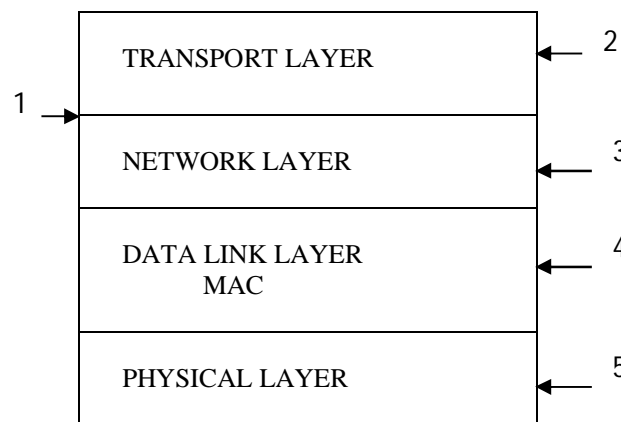


Table 2

1. Mobility Management
2. TCP/UDP
3. IP, Geographic Routing, Qos,
4. Token Ring, 802.11
5. Capacity

In the system of cooperative multiple mobile robots, communications among them are critically important. Each robot should exchange the information collected through its sensors and negotiate its task scheduling with other robots. These robotic communications are executed through the random access telecommunication among mobile robots. Experiments of robotic communication between several robots are reported using wireless LAN or infrared sensory systems. Wireless LAN devices that make use of spread-spectrum modulation and a UHF carrier (typically 2.4 GHz) offer the potential for high message data rates over a reliable physical layer implementation.

### 2.2.3.Robot Control And Communication Strategies:

Successful control and coordination of a group of wireless-networked robots relies on effective inter-robot communication. Robot controllers should be robust with respect to unpredictable and highly dynamic environment; due to the naturally hostile characteristic, controllers must also contend with imperfect wireless communication. Apparently the network is also part of the robot's environment and can contribute to the system's success or failure. At the simplest level, communication may succeed or fail between two nodes.

The robots typically operate under strict real time constraints; fast navigation and dynamic environments require that control inputs are acquired in a timely manner. Heavy load on a wireless network increases the average data transmission time, and reduces the frequency response of the controllers. Thus it may reduce the capability of the controller. Reducing load by more efficient communication can decrease latency and allow robots to be more responsive to dynamic environments.

Bandwidth is a precious resource if a robot's task involves transmitting huge data to a user (e.g. live video). Controller data is unwelcome overhead on the shared communications channel. Efficiency becomes increasingly important when scaling to a large numbers of nodes. Efficient communications are essential to save power and reduce latencies. It can be achieved by considering the interaction between controller and communication channel; controllers should be designed to take into account protocol characteristics and propagation conditions, and specialized protocols can be designed for mobile robot applications.

#### 2.2.4.Reason For Choosing Ad-Hoc Network

In an Ad - hoc network the network is formed dynamically through the cooperation of a set of independent nodes, without relying on preexisting infrastructure (routers or access points). Also each node participates in routing by forwarding data (made dynamically). This network is also mainly provided with Classic routing and flooding protocols. It also has other protocols like

Table driven routing protocol: This protocol mainly sends periodic updates of the routers.

On demand routing: This is one of the peculiar protocol which routes only when required to route data packets. But the cons in this is the longest transmission delay. Hence we have not provided much importance to this protocol as minimum delay is the major criteria in defence.

Hybrid routing protocol: Our proposed system uses a hybrid protocol which is the combination of two or more protocols.

#### 2.2.5.Benefits Of Ad-Hoc

- No expensive infrastructure
- Usage of unlicensed frequency spectrum
- Increased mobility and feasibility
- Reduced power consumption
- Communication beyond Line of site is possible by multihop Adhoc network.

#### 2.2.6.Cons Found And Its Remedy In Ad-Hoc Network

The problem that's been analysed by us is that as nodes compete for access to share in wireless medium, it results in a collision. This can be rectified using cooperative wireless communication which improves immunity to collision or CSMA/CA technique can be used.

Security is the main concern in wireless technologies,thus in order to enhance security 802.1x authentication is used,which uses an authentication server to validate users and provide network access on wireless network,802.1x can work with wired equivalent privacy(WEP OR WPA) keys.This type of authentication is typically used while communicating with work places only.Thus an alternate ,Wireless Protected Access(WPA) which encrypts data first and also checks for whether the network security key has been modified.

### **3.Application**

Robot communication applications choose ad-hoc networks when central bases are not available and/or a strong need arises to avoid the vulnerability of centralized infrastructure. In the following applications, they can be used to improve the robustness, scalability, and performance of a multi-robot system.

- Can be adequately implemented in national defence through military-industrial partnership.
- Can be vastly applied in Resorts, borders of noted buildings.
- Installation of these robots in the stadiums, sacred places, government and non government organizations assures top security.
- By means of ad hoc networks, robots can coordinate their activities with reliable communication regardless the conditions of all fixed infrastructures. This area becomes more and more important.
- Provides a secured control centre when compared to the most recent available security.

### **4.Conclusion**

As we all know, these days India is sick off massive terror attacks, bomb explosions at plush resorts. To avoid such disasters technological power must exceed human power.

Thus it's our onus to take an initiative to design a model of an apt robot that meets combatant needs. So to avoid terror attacks, to ensure more security at the border and high density areas it's wise to maintain a world class military technology in accordance with combatant needs.

Even every nation needs its own defence system for their integrity and security. In such a way construction of our proposed robots will carry the nation's name, fame globally. Thus by futurly enhancing these robots in all fame areas no threat from other countries can approach developing India.

**5. References**

- 1) zhigang wang, lichuan liu and mengchu zhou “ protocols and applications of ad-hoc robotwireless communication networks: an overview” international journal of intelligent control and systems vol. 10, no. 4, december 2005, 296-303
- 2) Dr.s.bhargavi , s.manjunath “design of an intelligent combat robot for war fields “ (ijacsa) international journal of advanced computer science and applications, vol. 2, no. 8, 2011
- 3) lemuel uitzil, michel garcía, cinhtia gonzález, sergio gonzález” wireless security system implemented in a mobile robot” ijcsi international journal of computer science issues, vol. 9, issue 4, no 3, july 2012
- 4) feng, borenstein, wehe ”a completely wireless development system for mobile robots” proceedings of the isram conference, montpellier, france, may 27-30, 1996, pp. 571-576
- 5) saliyah kahar1, riza sulaiman1,anton satria prabuwono1, nahdatul akma ahmad, and mohammad ashri abu hassan“a review of wireless technology usage for mobile robot controller” 2012 international conference on system engineering and modeling (icsem 2012) ipcst vol. 34 (2012) © (2012) iacsit press, singapore
- 6) christian hernández, raciel poot, lizzie narváez, erika llanes and victor chi “design and implementation of a system for wireless control of a robot” ijcsi international journal of computer science issues, vol. 7, issue 5, september 2010
- 7) mansouri hajar, medromi hicham, and sayouti adi “a gsm based remote wireless automatic monitoring of mobile robot “international journal of research and reviews in computer science (ijrrcs) vol. 3, no. 3, june 2012, issn: 2079-2557 © science academy publisher, united kingdom