2016

ICMR LIBRARY BULLETIN

Volume- 13, Issue no-1 January - March

INDIAN COUNCIL OF MEDICAL RESEARCH
V Ramalingaswami Bhawan,
Ansari Nagar New Delhi-110029

CONTENTS

RFID

Radio Frequency Identification Device

(CHANDAN KUMAR)

SUMMARY

The deployment and use of Radio Frequency Identification (RFID) technology is growing rapidly across many different industries. Developers apply the technology not only in traditional applications such as asset or inventory tracking, but also in security services such as electronic passports and RFID-embedded credit cards. However, RFID technology also raises a number of concerns regarding privacy, security and law enforcement1. In this paper, the basic concepts behind RFID technology are introduced, and the associated security issues and threats in using RFID technology, along with possible measures on how to tackle them, are discussed. The objective is to deliver a greater understanding of the security related aspects of this technology.

INTRODUCTION

RFID stands for Radio-Frequency Identification. The acronym refers to small electronic devices that consist of a small chip and an antenna. The chip typically is capable of carrying 2,000 bytes of data or less Radio Frequency Identification (RFID) technology is a non-contact, automatic identification technology that uses radio signals to identify, track, sort and detect a variety of objects including people, vehicles, goods and assets without the need for direct contact (as found in magnetic stripe technology) or line of sight contact (as found in bar code technology). RFID technology can track the movements of objects through a network of radio-enabled scanning devices over a distance of several meters. A device called an RFID tag (or simply a tag) is a key component of the technology. An RFID tag usually has at least two components:-

1. An integrated circuit for modulating and demodulating radio signals and performing other functions;

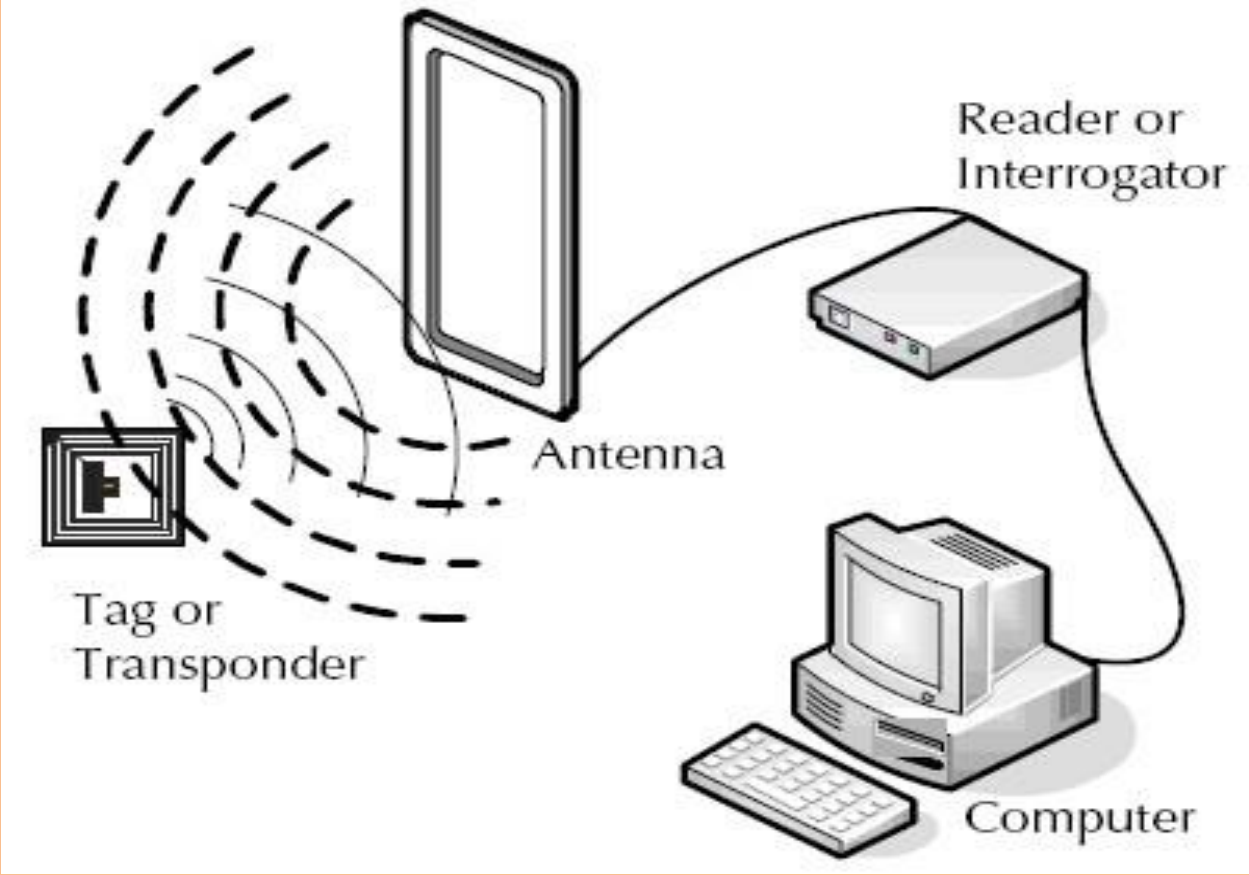
2. An antenna for receiving and transmitting the signal.

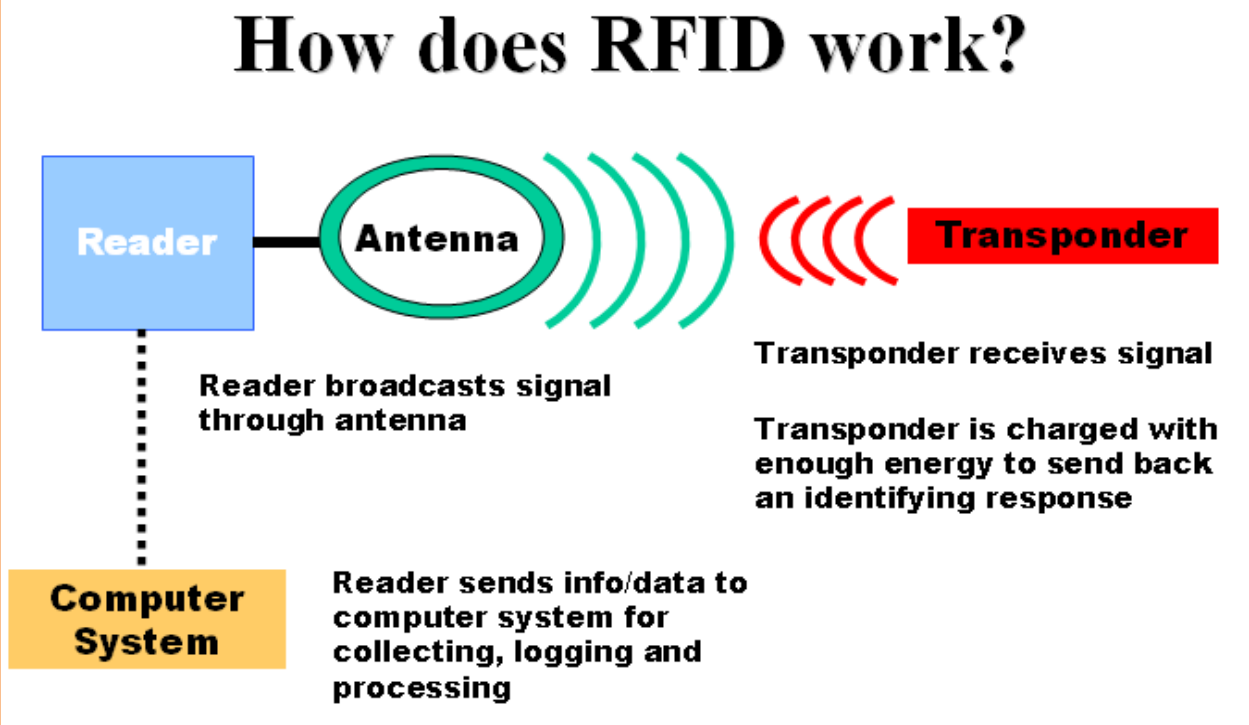
HOW DOES RFID WORK?

Systems that make use of RFID technology are typically composed of three key elements:-

1. An RFID tag, or transponder, that carries object-identifying data.
2. An RFID tag reader, or transceiver, that reads and writes tag data.
3. A back-end database, that stores records associated with tag contents.

Each tag contains a unique identity code. An RFID reader emits a low-level radio frequency magnetic field that energizes the tag. The tag responds to the reader's query and announces its presence via radio waves, transmitting its unique identification data. This data is decoded by the reader and passed to the local application system via middleware. The middleware acts as an interface between the reader and the RFID application system. The system will then search and match the identity code with the information stored in the host database or backend system. In this way, accessibility or authorization for further processing can be granted or refused, depending on results received by the reader and processed by the database.





RFID WORKS BETTER THAN BARCODES

A significant advantage of RFID devices over the others mentioned above is that the RFID device does not need to be positioned precisely relative to the scanner. We're all familiar with the difficulty that store checkout clerks sometimes have in making sure that a barcode can be read. And obviously, credit cards and ATM cards must be swiped through a special reader.

In contrast, RFID devices will work within a few feet (up to 20 feet for high-frequency devices) of the scanner. For example, you could just put all of your groceries or purchases in a bag, and set the bag on the scanner. It would be able to query all of the RFID devices and total your purchase immediately.

ADOPTION OF RFID

Commercial applications of RFID can be found today in supply chain management, automated payment systems, airline baggage management, and so on. According to RFIDupdate.com, one of the catalysts for the RFID industry has been mandates issued by Wal-Mart and the US Department of Defense (DOD) for their suppliers to adopt RFID technology. Although the market has not grown quickly or as large as originally expected, these two mandates continue to be important drivers in development of the industry.

SECURITY AND PRIVACY ISSUES

With the adoption of RFID technology, a variety of security and privacy risks need to be addressed by both organizations and individual.

TAG DATA

RFID tags are considered "dumb" devices, in that they can only listen and respond, no matter who sends the request signal. This brings up risks of unauthorized access and modification of tag data. In other words, unprotected tags may be vulnerable to eavesdropping, traffic analysis, spoofing or denial of service attacks. We will look at each of these in turn.

TRAFFIC ANALYSIS

Even if tag data is protected, it is possible to use traffic analysis tools to track predictable tag responses over time. Correlating and analyzing the data could build a picture of movement, social interactions and financial transactions. Abuse of the traffic analysis would have a direct impact on privacy.

SPOOFING

Based on the data collected from eavesdropping or traffic analysis, it is possible to perform tag spoofing. For instance, a software package known as "RF Dump", 11 that runs on a notebook computer or personal digital assistant, allows a user to perform reading or writing tasks on most standard smart tags if they are not properly protected. The software permits intruders to overwrite existing RFID tag data with spoof data. By spoofing valid tags, the intruder could fool an RFID system, and change the identity of tags to gain an unauthorized or undetected advantage. One example is trying to save money by buying expensive goods that have had their RFID price tags spoofed to display cheaper prices.

DENIAL OF SERVICE ATTACK

The problems surrounding security and trust are greatly increased when large volumes of internal RFID data are shared among business partners. A denial of service attack on RFID infrastructure could happen if a large batch of tags has been corrupted. For example, an attacker can use the "kill" command, implemented in RFID tags, to make the tags permanently inoperative if they gain password access to the tags. In addition, an attacker could use an illegal high power radio frequency (RF) transmitter in an attempt to jam frequencies used by the RFID system, bringing the whole system to a halt.

RFID READER INTEGRITY

In some cases, RFID readers are installed in locations without adequate physical protection. Unauthorized intruders may set up hidden readers of a similar nature nearby to gain access to the information being transmitted by the readers, or even compromise the readers themselves, thus affecting their integrity. Unauthorized readers may also compromise privacy by accessing tags without adequate access controls. As a result, information collected by readers and passed to the RFID application may have already been tampered with, changed or stolen by unauthorized persons. An RFID reader can also be a target for viruses. In 2006, researchers demonstrated that an RFID virus was possible. A proof-of-concept self-replicating RFID virus was written to demonstrate that a virus could use RFID tags to compromise backend RFID middleware systems via an SQL injection attack.

PERSONAL PRIVACY

As RFID is increasingly being used in the retailing and manufacturing sectors, the widespread item-level RFID tagging of products such as clothing and electronics raises public concerns regarding personal privacy. People are concerned about how their data is being used, whether they are subject to more direct marketing, or whether they can be physically tracked by RFID chips. If personal identities can be linked to a unique RFID tag, individuals could be profiled and tracked without their knowledge or consent. For instance, washing clothes tagged with RFID does not remove the chips, since they are specially designed to withstand years of wear and tear. It is possible that everything an individual buys and owns is identified, numbered and tracked, even when the individual leaves the store, as far as products are embedded with RFID tags. RFID readers can detect the presence of these RFID tags wherever they are close enough to receive a signal.

RFID SECURITY TRENDS

Since RFID remains an emerging technology, development of industry standards for protecting information stored on RFID chips is still being explored and strengthened. Research into the development and adaptation of efficient hardware for cryptographic functions, symmetric encryption, and message authentication codes and random number generators will improve RFID security. In addition, advances in RFID circuit design and manufacturing technology can also lower development costs releasing more resources in tags that can be used for other functions, such as allocating power consumption towards security features. Today, certain public key technologies are also being studied and in some cases deployed by RFID vendors. This helps improve confidentiality, user authentication and privacy of RFID tags and associated applications. RFID vendors are also conducting research into integrity and confidentiality issues around RFID reader infrastructure. Data can now be stored on a token using dynamic re-keying, where specific readers can rewrite a token's credentials/signature, and verify the token's identity. However, the cost and performance issues around using public key technologies in RFID applications have stalled its use for critical security applications.

APPROACHS FOR TACKLING SECURITY AND PRIVACY ISSUES

There are a variety of solutions for tackling the security and privacy issues surrounding RFID. They can be categorized into the following areas:-

1. Tag Data Protection
2. Reader Integrity
3. Personal Privacy

SOLUTIONS FOR TAG DATA PROTECTION

PASSWORD PROTECTION ON TAG MEMORY

Passwords can be used to protect tag data, preventing tags from being read without the original owner's permission. But if the passwords for all the tags are identical, then the data becomes virtually public. However, if each tag is going to have a different or unique password, there may be millions of passwords that need to be recorded, meaning the reader would have to access the database and perform a lot of comparisons for each reading attempt.

PHYSICAL LOCKING OF TAG MEMORY

The tag manufacturer locks information such as a unique identifier into tag before the tag is released into an open environment. In other words, the chip is read-only and is embedded with information during the manufacturing process. This provides proof of origin. The limitation of this method is that no rewriting of data can be done on the tag chip. Additional memory would be required for storing modifiable or extra information and an algorithm would be needed for finding the latest tag data. This would result in higher memory cost and a larger size memory.

AUTHENTICATION OF THE "AUTHOR" IN TAG MEMORY

The author or owner of the tag encrypts the tag data with his own private key (i.e. digitally signs the tag) and writes the encrypted data into tag memory along with the author's name, a reference to his public key and the algorithm used in non-encrypted form. When the reader wants to verify the authenticity of information, it retrieves the author's name and other non-encrypted information from the tag to verify that the data has been actually written by the original author as claimed. However, if the RFID reader needs to update the tag with new data, a key management system is required in order to manage the private key.

SOLUTIONS FOR RFID READER INTEGRITY

READER PROTECTION

Readers can reject tag replies with anomalies in response times or signal power levels which don't match the physical properties of tags. If passive tags are used, this can be a way to prevent spoofing attempts. Readers can also use random frequencies with tags designed to follow a frequency dictated by the reader. Readers can change frequencies randomly so that unauthorized users cannot easily detect and eavesdrop on traffic. On top of this, data transmitted between the reader and the RFID application server could require verification of the reader's identity. Authentication mechanisms can be implemented between the reader and the backend application to ensure that information is passed to the valid processor.

READ DETECTORS

RFID environments can be equipped with special devices to detect unauthorized read attempts or transmissions on tag frequencies. These read detectors may be used to detect unauthorized read/update attempts on tags, if they are used together with specially designed tags that can transmit signals over reserved frequencies, indicating any attempts to kill or modify tags.

SOLUTIONS FOR PERSONAL PRIVACY

KILL TAG

By executing a special "kill" command on a tagged product, the RFID tag will be "killed" and can never be re-activated. This "kill" command may disconnect the antenna or short-circuit a fuse. This ensures that the tag cannot be detected any further, and thus protects the privacy of the individual who possesses the product. However, there may be instances where tags should not be "killed". A store may wish for example to re-detect the tags on defective products returned by customers. Also, smart-cards embedded with RFID chips for access control will need to be activated continuously.

ACTIVE JAMMING

Active jamming of RF signals refers to the use of a device that actively broadcasts radio signals in order to disrupt the operation of any nearby RFID readers. This physical means of shielding may disrupt nearby RFID systems. However, the use of such a device may be illegal, depending on the broadcasting power of the device and government regulations in force. There is a risk of severe disruption to all nearby RFID systems if the jamming power is too strong.

"RSA" SELECTIVE BL OCKER TAG

A blocker tag is a passive RFID device that uses a sophisticated algorithm to simulate many ordinary RFID tags simultaneously. It provides an endless series of responses to RFID readers through the use of two antennas to reflect back two bits simultaneously, thereby preventing other tags from being read, performing a kind of passive jamming. However, this approach gives individuals a lot of control. In addition, a blocker tag may be used maliciously to circumvent RFID reader protocols by simulating multiple tag identifiers.

COMMON PROBLEMS WITH RFID

Some common problems with RFID are reader collision and tag collision. Reader collision occurs when the signals from two or more readers overlap. The tag is unable to respond to simultaneous queries. Systems must be carefully set up to avoid this problem. Tag collision occurs when many tags are present in a small area; but since the read time is very fast, it is easier for vendors to develop systems that ensure that tags respond one at a time. Some of these problems are:-

RFID READER COLLISION

Reader collision occurs in RFID systems when the coverage area of one RFID reader overlaps with that of another reader. This causes two different problems:-

SIGNAL INTERFERENCE

The RF fields of two or more readers may overlap and interfere. This can be solved by having the readers programmed to read at fractionally different times. This technique (called time division multiple access - TDMA) can still result in the same tag being read twice.

Multiple reads of the same tag

The problem here is that the same tag is read one time by each of the overlapping readers. The only solution is to program the RFID system to make sure that a given tag (with its unique ID number) is read only once in a session.

CONCLUSION

While the use of RFID technology is increasing across a range of different industries, the associated security and privacy issues need to be carefully addressed. Because RFID tags come in different flavors, there is no overall, generic RFID security solution. Some low-cost passive and basic tags cannot execute standard cryptographic operations like encryption, strong pseudorandom number generation, and hashing. Some tags cost more than basic RFID tags, and can perform symmetric-key cryptographic operations. Organizations wishing to use RFID technology need to therefore evaluate the cost and security implications as well as understand the limitations of different RFID technologies and solutions.

REFERENCES:-

1. HALL, J., BARBEAU, M., AND KRANAKIS, E. Radio frequency fingerprinting for intrusion detection in wireless networks. Submission to IEEE TDSC (Electronic Manuscript) (2005).

2. HALAMKA,J., JUELS, A., STUBBLEFIELD, A., AND WESTHUES,J. The security implications of VeriChiTMcloning. Manuscript in submission, 2006.

3. http://www.technovelgy.com/ct/technology-article.asp

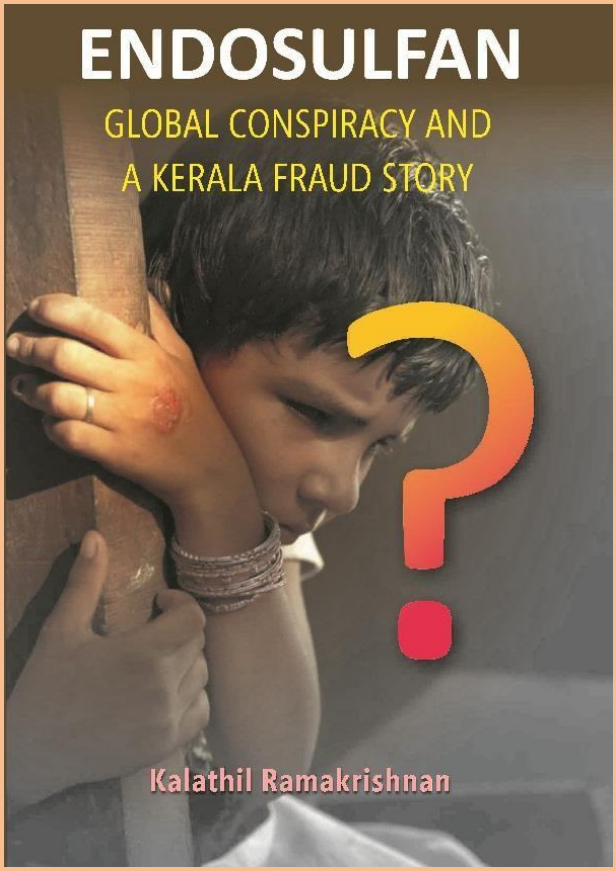
4. HALL, J., BARBEAU, M., AND KRANAKIS, E. Enhancing intrusion detection in wireless networks using radio frequency fingerprinting. In Proc. CIIT (2004).

5. HALL, J., BARBEAU, M., AND KRANAKIS, E. Detecting rogue devices in Bluetooth networks using radio frequency fingerprinting. In Proc. CCN (2006).

6. GRUNWALD, L. Cloning Passports without active authentication.In BlackHat (2006**).**

NEW ARRIVALS

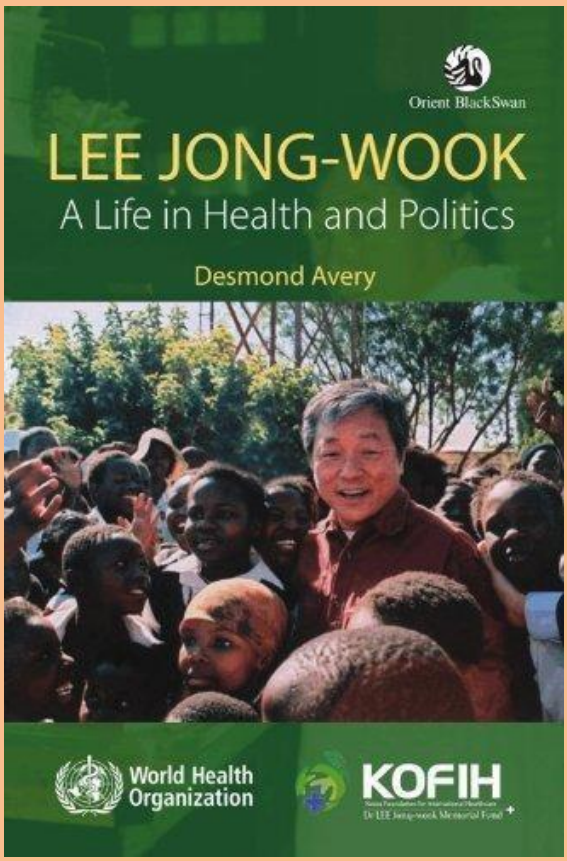
ENDOSULFAN: GLOBAL CONSPIRACY AND A KERALA FRAUD STORY



The book, a venture on investigative journalism, questions the version created by the media and the Environmental NGOs that the aerial spraying of endosulfan had caused widespread diseases and deaths in Kasargod in North Malabar. All the pre-existing diseases in the area were described as Endosulfan diseases by anti-pesticide activists. Though it was described as an event next only to the Bhopal gas tragedy, the controversy was the fallout of a global conspiracy hatched by the European Union to sell its patented pesticides. The whole episode boils down to competition among pesticide manufacturers of the EU to create its hegemony in the global market. The conferences on Multilateral Environmental Agreements were manipulated by the European Union. Endosulfan was phased out at the Conference of Parties at the Stockholm convention in 2011 by flouting the rules of the convention.

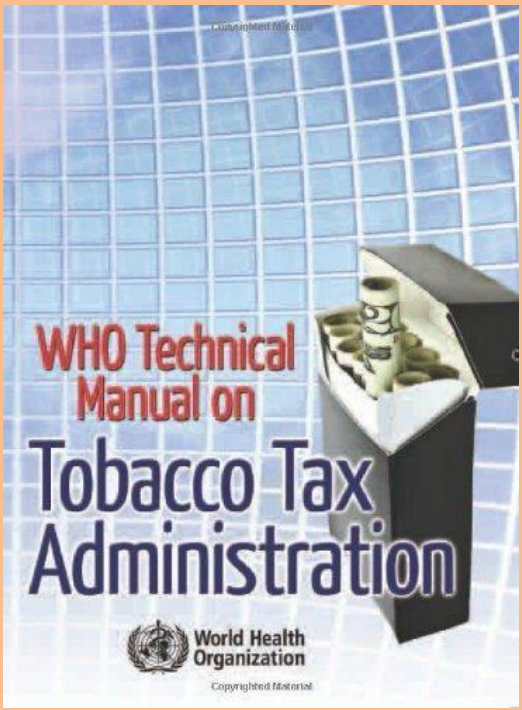
ABOUT THE AUTHOR:- Kalathil Ramakrishnan, a Kerala based independent journalist, joined the Indian Express as its staff correspondent at Kannur bureau in 1989 after resigning his job with a Government owned financial company. He had worked as the district correspondent and bureau chief of the New Indian Express in Kasargod district from 2001 to 2012. He covered the endosulfan controversy which was widely reported in the media in the country and abroad. Some of his reports had been adopted by prestigious media publications in the country. Many of his stories appeared in the Indian Express in all its editions across the country.

LEE JONG-WOOK: A LIFE IN HEALTH AND POLITICS



A newly qualified doctor, Lee Jong-wook, offers his services treating leprosy patients at St Lazarus Village outside his home town, Seoul. Here he finds both directions for his future work and his wife, like himself a volunteer. Desmond Avery describes Lee Jong-wook?s international adventures from Korea to Hawaii as a postdoctoral student, then to American Samoa as an emergency room clinician, and to Fiji as a World Health Organization medical officer for leprosy. As Lee? s WHO responsibilities expand to other areas, they take him to the Philippines, and then to Switzerland where, in 2003, he is elected Director-General of WHO, the first Korean to head an international organisation. Through this account of Lee Jong-wook?s career in health and politics, the author touches upon many important questions: Will there be a next global pandemic of deadly influenza? To what extent are AIDS, tuberculosis and malaria controllable? Who will foot the bill for polio eradication? The biography also yields important insights into international public health policy-making.

WHO TECHNICAL MANUAL ON TOBACCO TAX ADMINISTRATION

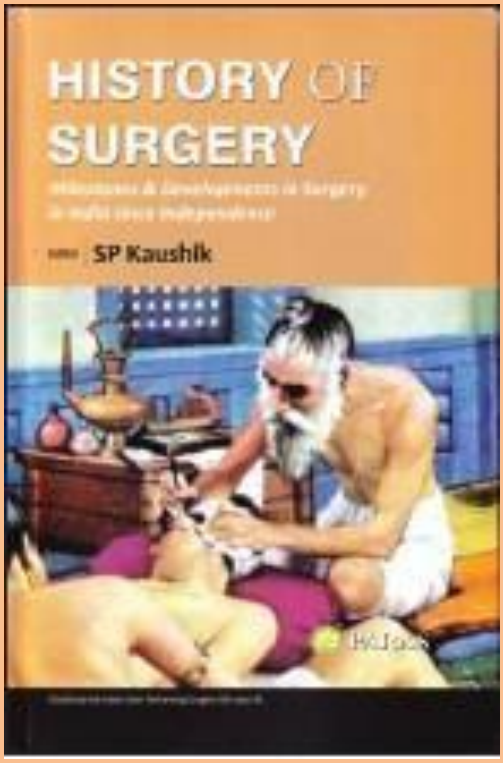


World Health Organization is a Specialized Agency of the United Nations, charged to act as the world's directing and coordinating authority on questions of human health. It is responsible for providing leadership on global health matters, shaping the health research agenda, setting norms and standards, articulating evidence-based policy options, providing technical support to countries and monitoring and assessing health trends.

Tobacco use is the single largest cause of preventable death globally, killing more than five million people each year. Tobacco use also creates considerable economic costs, from greater spending on health care to treat the diseases it brings on in users and those exposed to tobacco smoke to the lost productivity resulting from the premature deaths it causes.

Of all the many interventions for reducing tobacco use, a significant increase in tobacco product taxes and prices has been demonstrated to be the single most effective and cost-effective intervention, particularly among the poor and the young. At the same time, because of the inelasticity of demand for tobacco products in most countries and the low share of tax in price in many, significant increases in tobacco taxes generate significant increases in the revenues generated by these taxes.

HISTORY OF SURGERY-MILESTONES AND DEVELOPMENTS IN SURGERY IN INDIA SINCE INDEPENDENCE



The book has 19 chapters written by both Indian and foreign contributors. It enumerates the origin of various surgical societies as well as their controlling agencies such as Medical Council of India and the National Board of Examination. The role of missionary hospitals as well as the Royal Colleges of Surgeons, UK in training surgeons from India has been highlighted. The history of development of anesthesia as well as all the surgical specialties including transplantation and minimal access surgery is detailed. A single reviewer would not feel competent to comment on the development of all the surgical specialties and I would confine myself to the advancement in neurosurgery whose growth paralleled those of other super specialties in the country. Dr. Kak has summarized the development of neurosurgery since independence in the country but it would be rewarding to know about early pioneers in neurosurgery in our country.

The book is the product of research by scholars in each branch of surgery and is highly commendable and should be made available to every practicing surgeon and those who are planning a career in surgery. This would be a basic guide book for further study and each specialty can be expanded and improved upon. For a very great effort put out by individual contributors, absence of bibliography appears to be a lacuna, which could be corrected in future revisions of the book.

UPCOMING PROGRAMMES

SEMINARS/CONFERENCES/WORKSHOPS

- **UGC Sponsored National Seminar on "Exertion to Establish Knowledge Society: Responsibility of Academic Libraries"**

  - **Date: September 24, 2016 at 9:30am to September 25, 2016 at 5pm**
  - **Venue:- Shimurali, Nadia, West Bengal**

- **IT Application for Information Management in Health Science Libraries**

  - **Date: - September 26, 2016 at 9:30am to September 30, 2016 at 5:30pm**
  - **Venue:- National Institute of Health & Family Welfare (NIHFW), New Delhi**

- **One Day Workshop on "Future Libraries in 2020: Changes and Challenges"**

  - **Date: September 30, 2016**
  - **Venue:- Kamaraj Auditorium, Technology Tower, 7th Floor, VIT University, Vellore-632014,-Tamil Nadu.**

- **3 day National Workshop on "Management & Use of E-Resources".**
  - **Date: October 1, 2016 to October 3, 2016**
  - **Venue:-The Department of Library& Information Science, Dr.B.R.Ambedkar Open University- Hyderabad**

- **Multidisciplinary National Conference on Emerging Issues and Challenges in Higher Education**
  - **Date:-September 17, 2016 all day**
  - **Venue:- Khapar Dist. Nandurbar- Maharashtra**