DESIGN AND CONSTRUCTION OF MANUALLY OPERATED BEARING EXTRACTOR, A CATALYST IN NIGERIA MANUFACTURING SECTORS

Muriana, R. A.
Mechanical Engineering Department,
Federal University of Technology, Minna, Nigeria
E-mail: mraremu@yahoo.com

Abstract
Coupled bearings get stiffened and stuck to the harboring shaft as a result of some irregularities in the assembly. A bearing extractor of 600N working load was therefore designed and constructed to safely separate the components at will without damage. The results of the design calculations were utilized at the construction stage, as a factor safety of 1.5 was adopted. The calculated efficiency of the machine was 44 % - a good value for a machine of that kind. (Hall, 1982). The breakthrough achieved in designing and construction of the bearing extractor is therefore a pointer to the inherent latent potentials in the citizens of the federation to achieve her developmental vision in technology through the popular local content initiative.

Keywords: *Homogeneous, isotropic, lead angle, working stress and effective force.*

Introduction

The developmental aspiration of Nigeria's economy largely depends on drastic improvement in the nation's manufacturing sector. Most workshop tools including bearing extractors used in Nigeria are imported in large quantity from other nations. This work represents an effort to gradually rid off the consuming attribute of the nation and replace it with producing attribute as far as manufacturing is concerned. Bearings and other circular components harbored round solid or hollow shafts could be gradually extracted (pulled out) using the constructed machine without causing damage to both the bearing and the shaft, contrary to the crude method of using hammer to forcefully drive out bearings. The puller's components include a power screw, a frame with nut, two arms (claws) and fasteners.

Stiffness between two components:

Interface stiffness between two components can occur as a result of

1. Poor lubrication or inappropriate lubricants,
2. Irregular lubrication
3. Corrosion and
4. Expansion.

These irregularities can be prevented by ensuring direct opposite of each of them.

Design Analysis

Euler's equation: Columns are conveniently designed for using Euler's equation.

Assumptions:

1. The shaft used is of uniform cross-section
2. The shaft material is homogeneous and isotropic.

The working stress σ_w is given as

$$\sigma_w = C^1\pi^2 E / (L/K)^2 \quad \ldots\ldots 1$$

Where C^1 is determined using end condition.

L= length of shaft

K= least radius of gyration

E= modulus of elasticity.(Hall, 1982)

The working stress $\sigma_w = U.T.S./F.S$ 2

Equating '1' and '2'

$$C^1\pi^2 E / (L/K)^2 = U.T.S./F.S$$

Where U.T.S is Ultimate Tensile Strength and F.S is factor of safety. (Jones, 1989)

Power screw

Screw thread is one of the basic and efficient ways of mechanically transmitting power. It also changes the rotary force to translational force. The diameter of a screw is taken as 'D' such that:

D=2r ('r' is radius)

For a thread of single start and continuous ridge, the tangent of the lead angle 'λ' is:

Tan λ =lead of thread/ circumference of the minor diameter.

(Minor diameter is the pitch diameter)

Figure 1 shows the power screw.

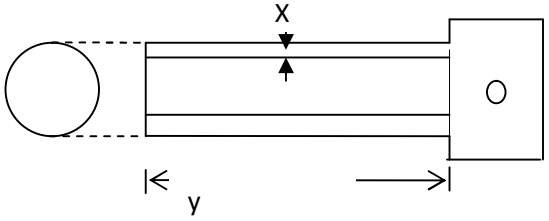


Figure 1:The power screw 2X (in mm) pitch and 'y' length of travel.

Square thread

Square thread is most suitable for its strength.

Figure 2 shows the lead and lead angle relationship for square thread.

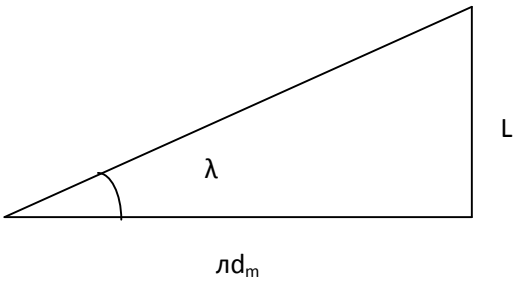


Figure 2: Square thread lead and lead angle. Hall (1982) and Shigley et al (2006)

where λ=lead angle in degree, L=lead of the thread and d_m= mean thread diameter

From figure 2,

$$\text{Tan } \lambda = \frac{lead}{2\pi r_m} \quad \text{..... 3}$$

Where r_m is mean thread radius.

The force diagram of a square thread in engagement is as shown in figure 3.

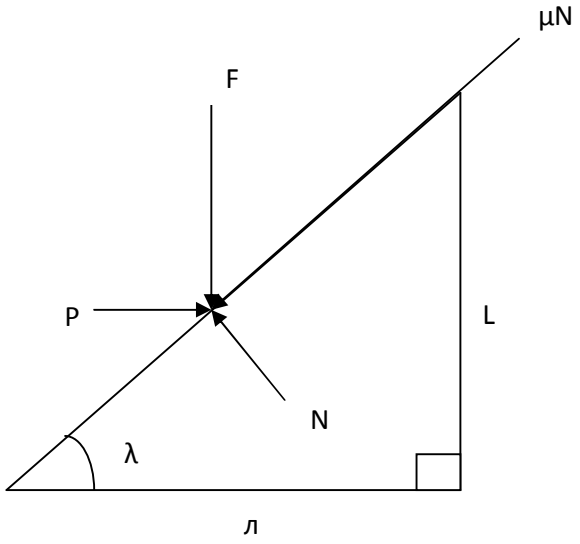


Figure 3: Force diagram of square thread in engagement. (Hall H.,1982) and Shigley et al (2006)

F = summation of all the unit axial forces acting upon the normal thread area

P = force acting to the right (to extract)

μN = the frictional force

N = normal force (reaction)

Лd$_m$ = circumference of the thread

Λ = lead angle in degree.

For successful extraction, the whole system should be in equilibrium under the action of the above forces.

Therefore, let $\sum F_h$ be summation of horizontal forces and $\sum F_v$ be summation of vertical forces.

$\sum F_h = 0$ and $\sum F_v = 0$

so,

$P - N\sin\lambda - \mu N\cos\lambda = 0$ along the horizontal direction 5

$N\cos\lambda - F - \mu N\sin\lambda = 0$

$F + \mu N\sin\lambda - N\cos\lambda = 0$ along the vertical direction 6

From equation 5,

$P = N\sin\lambda + \mu N\cos\lambda$

$P = N(\sin\lambda - \mu\cos\lambda)$

$N = \frac{P}{\mu\cos\lambda + \sin\lambda}$ 7

Putting 7 into 6,

$$F + \frac{\mu P\sin\lambda}{\mu\cos\lambda + \sin\lambda} - \frac{P\cos\lambda}{\mu\cos\lambda + \sin\lambda} = 0$$

$$F - P\left(\frac{\cos\lambda}{\mu\cos\lambda + \sin\lambda} - \frac{\mu\sin\lambda}{\mu\cos\lambda + \sin\lambda}\right) = 0$$

$$F - p\left(\frac{\cos\lambda - \mu\sin\lambda}{\mu\cos\lambda + \sin\lambda}\right) = 0$$

$$F = P\left(\frac{\cos\lambda - \mu\sin\lambda}{\mu\cos\lambda + \sin\lambda}\right)$$

and

$$P = F\left(\frac{\sin\lambda - \mu\cos\lambda}{\cos\lambda - \mu\sin\lambda}\right)$$

Dividing through by cosλ,

$$P = F\left(\left[\frac{\sin\lambda}{\cos\lambda} + \frac{\mu\cos\lambda}{\cos\lambda}\right] \Big/ \left[\frac{\cos\lambda}{\cos\lambda} - \frac{\mu\sin\lambda}{\cos\lambda}\right]\right)$$

But L / лd$_m$ = tanλ

Therefore

$$P = F\left[\frac{\left(\frac{L}{\pi d_m} + \mu\right)}{\left(1 - \left(\frac{\mu L}{\pi d_m}\right)\right)} \right] \quad \text{.......... } 8$$

'P' is the effective force to effect the extraction.

Bending stress, shearing stress and bearing pressure

The three stresses are calculated, so that the highest among them is designed for, to avoid the possible danger of failure due to its effect.

Bending stress:

The working bending stress is $\sigma_w = Mc/I$ 9

Ferdinand and Russell (1992)

so, $$Mc/I = \frac{\left(\frac{FL}{8}\right)\left(\frac{d}{2}\right)}{\frac{\pi d^4}{64}} \quad \text{.......... } 10$$

M=FL/8

C=d/2

And I=лd⁴/64

Where 'M' = bending moment in Nm

'C' = maximum distance from the neutral axis and

'I' = moment of inertial in m^4

Shearing stress:

The shearing stress is

$$\sigma_s = F/A$$

Jones (1989)

where 'A' is $2(\pi d^2/4)$

'F' is shearing force.

Bearing pressure:

The bearing pressure is

$\sigma_b = F/Ld$ 12

where F = bearing force

L =length of bearing and

d = diameter of bearing

Material selection

The selected material was mild steel with the following properties:

E=200 x 10^9 N/m^2

U.T.S = 517 x 10^6 N/m^2

DESIGN CALCULATIONS

Power screw rod

The maximum force expected to be applied to the extractor is 600N, owing to the fact that an average man's instant applied force is 580N and Factor of safety of 1.

At the cutting speed of 60rev/minute, square thread of 6mm pitch was cut on the rod with 279mm length of travel. The rod is desired to cover a maximum length of travel of the thread (28cm). so L= 30cm with 2cm clearance

End condition c^1 =0.25 (Fixed-free ends). (Hall, 1982)

The working stress

$\sigma_w = C^1\pi^2 E/(L/K)^2$

$\sigma_w = \frac{1}{4}(\pi^2)200x10^9 \Big/ (\frac{0.3}{k})^2$

also

σ_w= UTS/ factor of safety 13

$= 517x10^9/1.5$

= 342.6667x10^6 N/m^2

Therefore $342.6667 \times 10^6 = \dfrac{\frac{1}{4}(\pi^2)200x10^9}{(\frac{0.3}{k})^2}$

K = 7.9mm

Where k is radius of gyration.

But $k=\left(I/A\right)^{\frac{1}{2}}$ 14

(Ferdinand and Russell ,1992)

$I=Ak^2$

$I= \pi d^4/64$

$A= \pi d^2/4$

Hence

$k=((\pi d^4/64)/(\pi d^2/4))^{0.5}$

$k^2=d^2/16$

$d^2=998.56$

$d=\sqrt{998.56}$

= 31.6mm ≈30mm.

Thread design

Table 1 gives the basic dimensions for square thread.

Table 1: Basic dimensions for square thread

Normal series	Major Dia. Bolt	Nut	Pitch	H_2	h_1
24	24	24.5	5.0	2.0	2.5
30	30	30.5	7.0	2.5	3.0
40	40	40.5	6.0	3.0	3.5

P=pitch, a=clearance, h_1=thread depth, b=0.5 ,h_2=0.5p-b(all dimensions in mm)

h_1=thread depth. The lead angle is taken as 3.5^o. (Lingaiah and Narayana ,1985)

From figure 1, Tan λ = $lead/2\pi r_m$

r_m = 15mm

tan3.5=lead/2лr_m

lead = tan 3.5 x 2лr_m

=0.06116 x 2 x 3.1416 x 15

=5.76

≈6mm

Therefore picth=6mm

h=0.5(picth)+ clearance(table 3.1)

h=(0.5 x 6) + 0.25

= 3.25mm

h≈3.3mm

major diameter $d_o = 2r_m + 0.5$(pitch)

= 30 + 0.5 x 6

= 30 + 3

=33mm

minor diameter $d_i = 2r_m - 0.5$ (picth)

=30 – 0.5 x 6

= 30-3

=27mm

Effective force P from equation 8.

$$P = F\left[\frac{\left(\frac{L}{\pi d_m} + \mu\right)}{\left(1 - \left(\frac{\mu L}{\pi d_m}\right)\right)}\right]$$

F=600N , μ=0.08

$$P = 600\left[\frac{\left(\frac{6}{94.25} + 0.08\right)}{\left(1 - \left(\frac{0.08x6}{94.25}\right)\right)}\right]$$

=86.6N

Design of the frame

A rectangular cross-section rod was turned to get the frame. Internal rectangular thread was also cut to make the nut for the power screw, as shown in figure 4.

U.T.S = 517 x 10^6 N/m^2

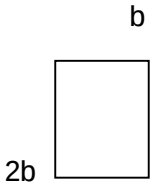
So, $U.T.S/1.5 = C^1\pi^2 E/(L/K)^2$

517 x 10^6/1.5 = $0.25\pi^2 200x10^9/(0.35/K)^2$

k=9.223m

from k= $\left(I/A\right)^{\frac{1}{2}}$,

I= $bh^3/12$ (for rectangular cross-section in 'b' units)



h=2b

k= $\sqrt{b(2b)^3}\Big/\frac{12}{2b^2}$

b=32mm

Figure 4 shows the frame.

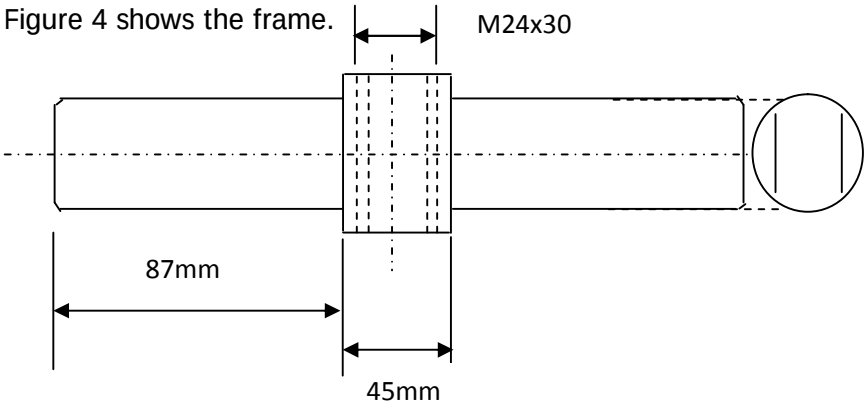


Figure 4: The extractor's frame and nut

Design of the arms (claws): 'L' is the desired arm's length.

L=0.2m. σ_w=3.446 x 10^8

$$\sigma_w = \frac{\frac{1}{4}\pi^2 x 200 x 10^9}{(\frac{0.2}{k})^2}$$

k=5.28mm

$k=\left(I/A\right)^{\frac{1}{2}}$,

$k= (\pi d^4/64)^{0.5} / (\pi d^2/4)^{0.5}$

$d^2 = k^2 \times 16$

d=21mm

A steel rod of 25mm diameter was turned to 21mm and 200mm length (Figure 5).

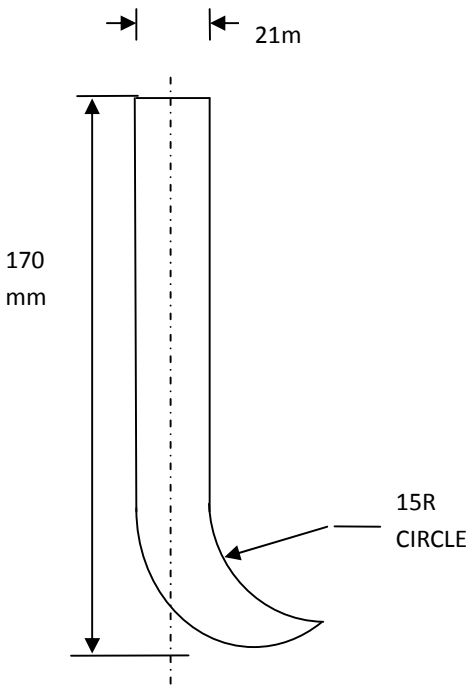


Figure 5: The extractor's arm [x2]

Design of the fasteners (bolt and nut)

The failures of the fasteners could be due to bending, shearing of bearing pressure Failure due to bending gave the maximum diameter of bolt as:

$$\sigma_{wbolt} = \frac{(\frac{FL}{8})(\frac{d}{2})}{\frac{\pi d^4}{64}}$$

σ_{wbolt} = 171.3335 x 10^6 (3.446 x 10^8 / 2)

L=32mm (power screw diameter is 30mm) F=600N.

d=6.6mm

Device Operation

The two arms (claws) of the device grasp the raceway edge of the outer ring of the bearing to be extracted, while the tip of the power screw rest firmly on solid base of the harbor. Upon manually loading, the applied torque is transformed to an axial extraction force to pull out the bearing while the screw runs through the internal thread of the nut.

The photograph of the coupled constructed device is shown in plate 1.

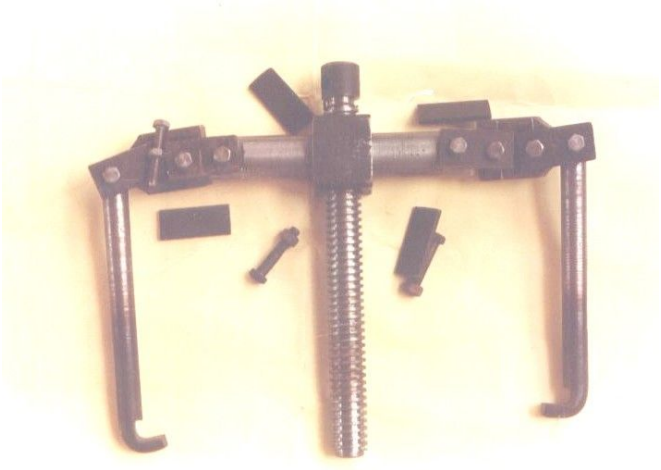


Plate 1: Photograph of the constructed bearing extractor

Efficiency of the machine:

The efficiency is calculated as $\rho = \frac{work\ output}{work\ input}$ x 100

$$= \frac{FL}{2\pi T}$$

$$= \frac{600 \times 0.06}{2\pi \times 12.99}$$

= 44%

Conclusion

The design and construction of the bearing extractor has been achieved. This potential can be tapped to further strengthen the nation's drive to achieving the vision 2020 aspiration. The machine can further be modified to operate electrically and number of claws increased for further improvement.

References

Ferdinand, P. B. & Russell, E. J, Jr. (1992). *Mechanics of materials.* Pp191, 632 - 636

Hall, A. S., Holowenko, A. R. & Laughlin, H. G. (1982). *Schaum's outline series, theory and problems of machine design (1st Ed).* New Delhi: Gram Hill Book Company.

Steve, F. (1981). *Machine tool operation*. Pp117 – 118.

Lingaiah, K. & Narayana, B. R. (1985). *Machine design data handbook (Metric Unit).* Pp XVIII,256,261 - 265.

Adeoye, O. J. (1998). *Design and construction of a simple hydraulic press.*

Jones, G. D. (1989). *Mechanical engineering science.* NY: EL-BS Longman. Pp 28, 88 - 100.

Shigley, J. E. & Mischke, C. R. (2006).*Mechanical engineering design (6th ed).* New Delhi, India: McGraw Hill, Pp447-454.

Rattan, S. S. (2006). *Theory of machines (2nd ed).* New Delhi, India: McGraw Hill, Pp 283-287.

SECURITY APPLICATION IN BLUETOOTH TECHNOLOGY

Ismaila, I. & Morufu, O.
Department of Cyber Security Science
Federal University of Technology, Minna, Niger State. Nigeria
E-mail: Ismi_idris@yahoo.co.uk[1] & lerejide@gmail.com[2]

Abstract

Before implementing some new technologies, a simulation program is usually designed to first demonstrate how the technology works. If it works perfectly, then the real implementation takes place, but if it fails, correction is made before the implementation. In this paper, we shall examine a program that demonstrates security application in Bluetooth technology. We shall also discuss how Bluetooth technology provides security measures at both the application layer and the data link layer. Finally we look at the two kinds of inherent features that make attacks more difficult.

Keyword: Bluetooth, Security, Network, Protocol, Application

Introduction

Over the years wireless technology has been promising a world without wires but look around, you will see lots of interconnecting wires. Look at your good old PC isn't it cluttered with wires? Wires connecting your PC to the printer, scanner, mouse, keyboard etc. It is a total mess. Some initial solutions using short range wireless connectivity with frequencies in the scientific, industrial and medical bands have resulted in some success in reducing this mess but there was very little scope for interoperability between devices due to their proprietary standards. A printer and a laptop could only be interconnected if they are bought from the same manufacturer. These and a host of other problems made these initiatives less feasible. But this is going to change for better. Bluetooth technology, originally developed by Ericsson but now controlled by the Bluetooth SIG (Special Interest Group), a consortium of 1000+ companies, offers the promise of a global standard for short-range wireless communication between an ever-increasing variety of devices and peripherals.

The fancy name for this short-range wireless connectivity protocol comes from the 10th century Viking king, Harald Bluetooth, who united Scandinavia after years of fighting and destructive competition. Today Bluetooth is following the same symbolic path to establish a common platform for communicating between disparate types of computing devices. Beyond the colorful origin of its name, Bluetooth is a compelling new radio technology that opens up a new world of opportunity for uniting and empowering mobile device users.

Bluetooth Specification in Brief

- Maximum data rate 750 kbps
- Master-Slave communication model.
- Operating Frequency is globally available 2.4-2.5 GHz free ISM band with spread spectrum technology
- Frequency hopping, full duplex signal at 1600 hops/sec.
- 79 frequencies with 1 MHz interval to provide noise immunity
- A device can be master of 7 slaves forming a network called piconet. Several piconets can interconnect to form a large network called scatternet.
- Royalty free standard

Bluetooth Protocol Overview

The Bluetooth protocol stack, can be divided into four layers according to their purpose, in the following ways:

1. Bluetooth Core Protocols, including Baseband, LMP, L2CAP, and SDP, comprise exclusively Bluetooth-specific protocols developed by the Bluetooth SIG that are required by most of the Bluetooth devices.
2. Cable Replacement Protocol, i.e. RFCOMM protocol, is based on the ETSI TS 07.10 that emulates serial line control and data signals over Bluetooth Baseband to provide transport capabilities for upper level services.
3. Telephony Control Protocols, including TCS Binary and AT-commands, are used to define the call control signaling, mobility management procedures, and multiple usage models for the Bluetooth devices to establish the speech and data calls and provide FAX and modem services.
4. Adopted Protocols, including PPP, UDP/TCP/IP, WAP, WAE, etc. Due to the open nature of the Bluetooth specification, additional protocols (e.g., HTTP, FTP, etc.) can be accommodated in an interoperable fashion.
5. Host Controller Interface (HCI), i.e. the boundary between hardware and software, provides a uniform command interface to access capabilities of hardware, e.g. Baseband controller, link manager, control and event registers.

Bluetooth Protocol Stack

The layers of Cable Replacement, Telephony Control, and Adopted Protocols form the application-oriented protocols that enable applications to run over the Bluetooth core protocols. Not all applications make use of all the protocols, applications run over one or more vertical slices of this protocol stack. In other words, applications may run over different protocol stacks (Bluetooth SIG, 2002). Nevertheless, each one of these different protocol stacks uses a common Bluetooth data link and physical layer, i.e. Bluetooth core protocols, including:

(i) Baseband. Based on the physical radio link, the Baseband can form the piconet between Bluetooth units and decide the roles of master and slave in the piconet. The Baseband provides physical links of both Synchronous Connection-Oriented (SCO) and Asynchronous Connectionless (ACL) to support the transmission of data and/or audio with corresponding packets (Java Community Process, 2001). Other functions include error correction, link management and control, audio transmission, etc.

(ii) Link Manager Protocol (LMP). The Bluetooth protocol LMP is responsible for link set-up between Bluetooth devices. This includes security aspects and the control and negotiation of Baseband packet sizes. Furthermore, it controls the power modes and duty cycles of the Bluetooth radio device, and the connection states of a Bluetooth unit in a piconet.

(iii) Logical Link Control and Adaptation Protocol (L2CAP). The protocol of L2CAP provides connection-oriented and connectionless data services to the upper layer protocols over the Baseband, with protocol multiplexing capability, segmentation and reassembly operation, and group abstractions, which permits higher level protocols and applications to transmit and receive L2CAP data packets. L2CAP is defined only for ACL links (Java Community Process, 2001).

(iv) Service Discovery Protocol (SDP). Using SDP to discover services is a crucial part of the Bluetooth framework and provides the basis for all the usage models. SDP query device information, services information, and the characteristics of the services, according to which a suitable connection between two or more Bluetooth devices can be established.

Security Framework

The Bluetooth technology provides security measures at both the application layer and the link layer. Besides there are two kinds of inherent features that make attacks more difficult.

A hop selection mechanism of up to 1600 hops/sec is employed to avoid the interference from external or other piconets. An automatic output power adaptation scheme is also included in the standard for the low power consumption of light-weight mobile devices, which can reduce the radio spread range for data transmission exactly according to requirements based on the detected intensity. A total of three different information security objectives are to be reached one or all. Confidentiality means that the data can only be used by authorized users and/or parties. Integrity means that the data cannot be modified during transfer and stored by adversaries. Availability means that the data is always available for authorized use (The Open Group, 1997). Typical attacks to a wireless network include DoS (Denial-of-Service), man-in the middle, spoofing, impersonating, session hijacking, eavesdropping, etc. Bluetooth launches three main techniques to achieve security features, including:

(i) Encryption: The process of transforming data into a form that it cannot be understood without a key. Both data and control information can be encrypted.

(ii) Authentication: The process of verifying 'who' is at the other end of the link. Authentication is performed for both devices and users.

(iii) Authorization: The process of deciding if a device is allowed to have access to a service. Authorization always includes authentication.

Security Modes

Each Bluetooth device can operate on one of the 3 security modes. First mode is a non secure mode in which a Bluetooth device shall never initiate any security procedure. Second mode is service-level enforced security where a device does not initiate security procedures before channel establishment at L2CAP level, and whether to initiate or not depends on the security requirements of the requested channel or service (Bluetooth SIG, 2003). Third mode is a link-level enforced security in which a Bluetooth device shall initiate security procedures before the link set-up at the LMP level is completed. Accordingly, two levels of Bluetooth security scheme can be identified as follows:

Link-level security corresponds to third mode. The Bluetooth device Initiates security procedure before the channel is established. This is the built-in security mechanism and it is not aware of service/application layer security. Second mode corresponds to service-level security. The Bluetooth device initiates security procedures after the channel is established, i.e. at the higher layers. This is a kind of add-in mechanism and is regarded as a practical issue.

Security Levels

Bluetooth allows different security levels to be defined for devices and services. Two security levels can be defined for a device. A trusted device has unrestricted access to all or some specific services. Basically this means that the device has been previously authenticated and marked as “trusted”. An untrusted device has restricted access to services. Usually the device has been previously authenticated but has not been marked as “trusted”. An unknown device is also an untrusted device. Three levels of service security are allowed to be defined so that the requirements for authorization, authentication, and encryption can be set independently, including services that require authorization and authentication, services that require authentication only, and services open to all devices. These three security levels can be described by using the following three attributes:

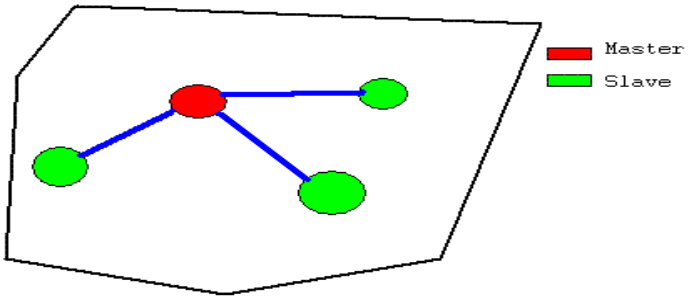
Authorization Required: Access is only granted after an authorization procedure. Only trusted devices would get automatic access.

Authentication Required: The remote device must be authenticated before being able to connect to the application.

Encryption Required: The link between the two devices must be encrypted before the application can be accessed.

How Bluetooth Works

Now a Bluetooth network actually consists of small subnets or piconets. A piconet consists of two or more connected nodes sharing the same channel. Every piconet have one master and up to 7 slaves. There is never a direct transmission between slaves. Rather all communications go through the master.



A Piconet

Two or more connected piconets form a scatternet. To connect piconets simply let them have a node in common. A node may be a slave in one piconet and a master in another. This is the basis for forming ad-hoc networks in Bluetooth.

The core Bluetooth protocol stack contains 5 layers. The radio and baseband layers describe the physical implementation of Bluetooth. It operates on the 2.4GHz frequency. There are 79 1MHz channels and upper and lower guard bands. The technology uses frequency hopping spread spectrum for information transmission with 1600 hops per second. Each channel is occupied for 0.625ms, called a slot and the slots are number sequentially. The master in the piconet determines the frequency hopping sequence and it is a function of the master's address

Conclusion

Conclusively, this paper explores security in Bluetooth technology and also layers in security implementation using Bluetooth technology. Security modes and also security level in Bluetooth technology is also examine.

Further research that will be recommended here is to design a complete simulation that can take care of all the security issues in a mobile ad hoc network including both misused and anomaly detection of intrusions. A real or physical implementation of the simulation on any JAVA enabled mobile phone is also recommended to see in real life how the security features will work physically.

Further research work can also be done to increase the radius covered by Bluetooth to discover devices and transfer data.

References

Bluetooth SIG, (2003). *Bluetooth Network Encapsulation Protocol (BNEP) Specification*, Revision 1.0.

Bluetooth SIG, (2002). *Hardcopy Cable Replacement Profile Interoperability Specification,* Revision 1.0a.

Java Community Process, (2001). J2ME Foundation Profile (JSR-46). Retrieved from http://www.jcp.org/en/jsr/detail?id=46.

The Open group, (1997). DCE 1.1: *Remote Procedure Call,* Appendix A. Document Number C706. Retrieved from http://www.opengroup.org/dce/info/faq-mauney.html