Biometric Security

[Authentication of Bluetooth Using "Biometrics"]

Sany Jones R
IV-Year CSE
CSI College of Engineering
Ketti-643215

***Abstract*: Bluetooth is a short -range wireless technology that enables Connection less communication between devices. Bluetooth Technology redefines the very way we experienceConnectivity . The connectivity between the Bluetooth – enabled a device is based on device authentication . The connectivity Does not take into account the authentication of the user . The lack of any means of user authentication coupled with the reliance on device authentication leaves Bluetooth particularly vulnerable to spoofing attacks and the misuse of authenticated devices giving the unauthorized users access of the network using the Bluetooth - enabled device . We propose here a solution to the above problem . The solution uses biometric traits of a user for giving access to the ad hoc network of the Bluetooth - enabled devices . The paper discusses the framework for user authentication using the biometric technology , when a Bluetooth – enabled device is trying to get connected to a Bluetooth - enabled network.**

INTRODUCTION

Bluetooth is a wireless radio specification designed to transfer data and voice signals among the electronic devices in a close proximity without use of cables. The Bluetooth specification simplifies communication between electronic devices such as laptop computers , cellular phones , PDA's , digital cameras and other consumer electronic devices by automating the connection process.

Frequency range

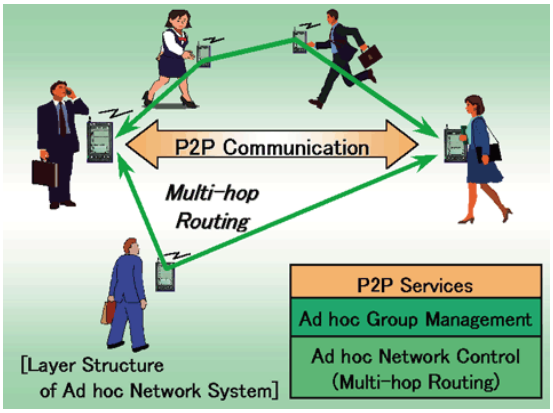
- Bluetooth operate in 2.4 GHz Industrial, Scientific, and Medical application (ISM) frequency range.
- Bluetooth uses a technology called "spread spectrum frequency "

Ad-hoc network

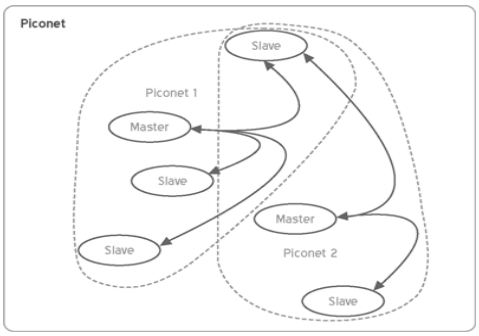
Bluetooth devices automatically attempt to communicate whenever one device comes with in close proximity of another device.

- Bluetooth devices form an Ad-hoc network that has a temporary and random topology. An Ad-hoc network of two or more Bluetooth devices is called a "piconet".

Adhoc network



Orientation of piconet

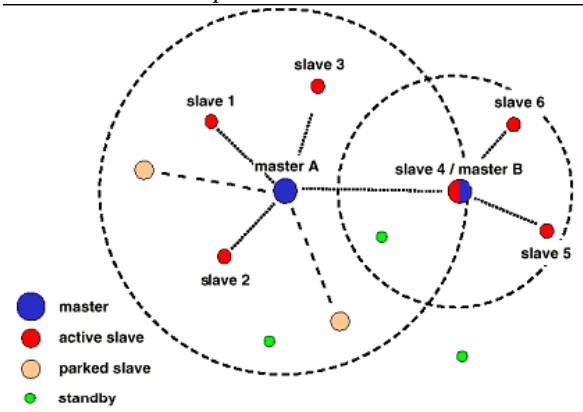


ESTABLISHING CONNECTION

When two Bluetooth devices initiate a connection, the device that initiates the communication takes the role of master and the other devices of the piconet becomes slaves. A master device can have up to seven slaves. A slave in one piconet can also be the master in another , thus allowing piconets to overlap and interact. During the connection establishment the master continuously broadcast 16 identical page messages across the Bluetooth frequency range, which the other devices listen in standby mode. The necessary condition for establishment of connection is that the master must know the slave devices Bluetooth address and

system clock settings. The slave will respond by synchronizing its frequency hoping sequence and system clock with the master and also sending the correct information about itself.

Master-slave description



EXISTING SECURITY FRAMEWORK IN BLUETOOTH

The current security framework of Bluetooth consist of three main security services namely

- Authentication.
- Confidentiality.
- Authorization.

Authentication involves verifying the user with whom the connection is to be established. The authentication process
involves two devices, one that want to establish the connection and the other with whom the connection is to be
established. The existing authentication process is as follows:

1 .Users enters an identical PIN to both devices.

2. An algorithm is then used to create a 128-bit Link Key. This link key is same for both devices. This link key after creation is kept secret.

3. The device that wants to establish connection sends its unique 48-bit address to the master device that decides if the connection is authenticated.

4. The master sends a 128-bit random number to the device for ensuring
further level of security.

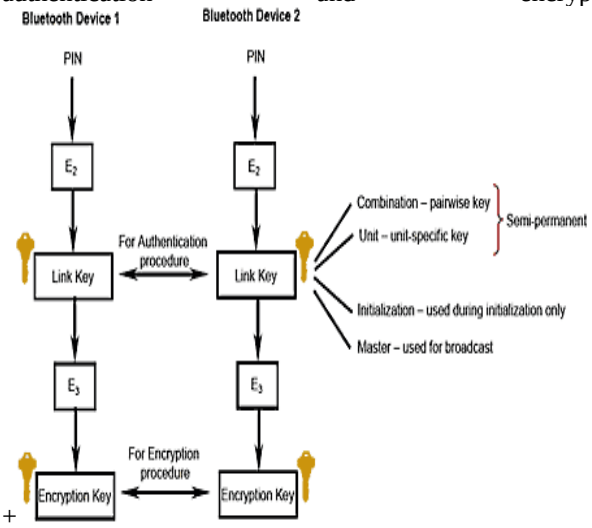
5. Both devices perform an algorithm taking 3 inputs link key, device address of the device who want to connect and the random number to generate a 32-bit Response.

6. The device that wants to connect sends its response to the master to
compare with the master's response.

7. If the two responses are identical, the connection is successfully authenticated

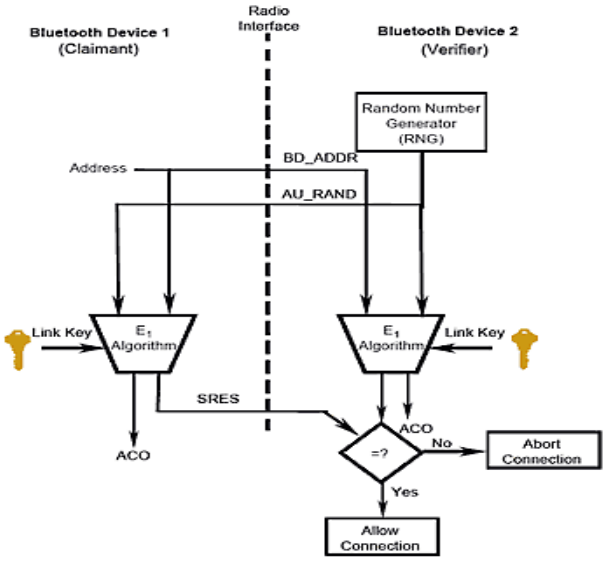
ENCRYPTION PROCEDURE

The International Standards Organization (ISO) has been defined by as "ensuring that information is accessible only to
those authorized to have access". Here the goal is to hide sensitive information transmitted over wireless link. Encrypting the data using key streams generated by some cryptographic technique ensures the confidentiality of the information that is passed during the connection establishment. The key stream is generated by taking inputs of master identity i.e. its unique address, a random number generated by master, the current slot number of the packet, the response generated during authentication phase and the link key**.** Authorization is to specify control of resources and access to services. Bluetooth categorizes the devices as trusted devices that get full access to all resources, and un trusted devices that get access to only a restricted set of services. Devices get authorized to be trusted only when it has been first authenticated. Bluetooth does not provide end-to-end security but only link authentication and encryption.



Authentication procedure:
Bluetooth operates in 3 different security modes namely

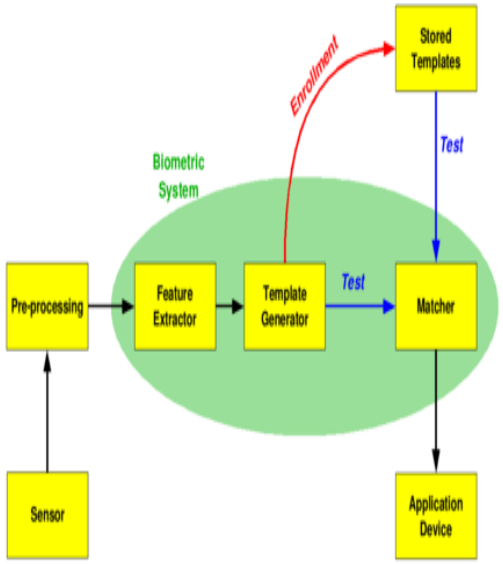
- Non-secure.
- Service-level enforced security.
- Link-level enforced security mode.



In non-secure mode it is believed that applications do not require any security
services and hence there is no security measures taken. Service-level enforced security mode initiates the security services after the connection is established and the master will control access to services and resources. This security mode provides all the three security services. The link-level enforced security mode initiates the security services before the connection is established. Only Authentication and Confidentiality services are provided in this mode.

PROPOSED FRAMEWORK FOR USING BIOMETRIC FORAUTHENTICATION AND AUTHORIZATION

The existing system that is using the pin numbers to be entered has its own limitation. The pin numbers are used to generate the link keys. The problems like forgetting a complex pin, stealing or changing of pin, breaking of pin by others leave the pin method insecure. The alternative to the pin number approach is the Biometric technology that uses the biological traits or behavioral characteristics to identify an individual. The traits or characteristics may be any biological character like retina, fingerprints, hand, face, voice etc. The Biological characteristics provide a better and reliable way of securing the systems. These characteristics are free of the threats like stealing, forgetting, change etc. The figure shows a Bluetooth system using the biometric template of a user for authentication during connection establishment
Figure shows, there are two devices one is the master device.



BIOMETRIC SYSTEM:

1.(M) that is going to authenticate and authorize the connection and a device A that want to get connected.

2. The user of both the devices enters their required biometric feature in the
device. The device here must have the facility to acquire the biometric traits.

3. The acquired biometric trait is then
processed through extraction feature part that exacts the essential features of the template.

4. These features are represented in terms of numbers and are used to generate the
required link keys.

5. The master continuously broadcast identical page messages across the Bluetooth frequency range, which the device A listens and respond.

6. The device A sends a request for connection that can be accepted or rejected at the initial level.

7. In case the master wants to accept and further ensure the validity of the device A, the master ask for its link key. This link key is searched across the database that contains an identification number of the device A and the corresponding link key.

8. If the link key is not found in the
Database then the master device ask the user whether to store the link key or not. The link key is stored for future reference
after getting the response from the user of the master device.

9. For future connection between the master and the device A the above steps can be saved. The master device can store
approximately 256 identification numbers along with the corresponding link key in 34KB memory.

10. The identification number is obtained from the database is sent to the device A. The device A responds by sending back
its 48 bits Bluetooth address. The master device now issues a 128 bit random number-based challenge to device A. Both
devices will compute an authentication response through an algorithm that is based on device A's Bluetooth address, the random number challenge issued by the master B, and the previously calculated identification key.

11. Device A will then transmit its authentication response and master device will compare it to its own calculations.

12. If the two agree, then the
device is authenticated. If the authentication responses do not
match, then the connection is refused.

13. Authorization is dependent on authentication as the authentication process establishes the device identity that is Used to determine access.

14. The first time when the device A
requested for the connection and the master device accepted, the device A is at the untrusted level i.e. its quickly to improve their understanding of Bluetooth so they can make informed decisions regarding how they will use Bluetooth and how to use it securely."

Biometric technology is considered more secure than the traditional pin number security. Biometrics is now an appropriate option, because the technology is reliable and cost effective. This paper tries to present a new framework for using Biometric to further enhance security measures for authentication at the time of device connections in Bluetooth.

Further refinements of the method proposed are been carried out. With further advances in the security threat these types of solutions are becoming more and more relevant.

access to services on master device is restricted by service security levels.

15. After the complete verification i.e. matching the response of M andA, a trust relationship is established between the two, which in other words means device A is allowed unrestricted access to the master device M.

16, The proposed framework maintains confidentiality by using a 128 bits encryption service that ensures that only a recipient with the proper decryption key can view the data.

A device's encryption key is based on its identification number. This simplifies the key generation process as both the sender and receiver have shared secret information upon which to key
their encryption.

FUTURE ENHANCEMENTS

This framework can be extended to computer network security and avoid cyber crimes. This can be also used to avoid non-ethical and illegal hacking.

CONCLUSION

Bluetooth technology tries to provide automatic connections between electronic devices, but this convenience comes with some compromise in security. Overtime the vulnerabilities in the Bluetooth specifications will be discovered and the efforts for improving the security levels also will go on increasing. Mitigating the security risks is of prime concern. Bruce Potter, a security expert with the Shmoo Group, predicts "Bluetooth security will become a real issue in the coming years. IT security professionals need to work

REFERENCES

[1] "Bluetooth Technology Overview". Version 1.0. 4 April 2003.
[2] http://ncsp.forum.nokia.com/downloads/nokia/documents/ Bluetooth_Technology_Overview_v1_0.pdf?ref=wdn (19 August 2003).
[3] "Bluetooth Hacking Tool Released". Bluetoothnews.com. 24 June 2003.
[4] Cox, John. "Study: Bluetooth Security Should Raise Red Flags". Network World Fusion. 9 September 2002.
[5] www.bluetooth.com/upload/24Security_Paper.PDF (14 August 2003).
[6] Bio API Consortium: http://www.bioapi.org, Bio API Consortium BIOAPI Specification, Version 1.1 March 16, 2001.