GOA COLLEGE OF ENGINEERING

"Bhausaheb Bandodkar Technical Education Complex"

Experiment No: 7

Case Study of Bluetooth

Bluetooth

Bluetooth technologies are local area networks with a very limited coverage and without the need for an infrastructure. This type of network is needed to connect different small devices in close proximity(about 10m) without expensive wiring or the need for a wireless infrastructure.

At the same time the Bluetooth development started, a study group within IEEE 802.11 discussed wireless personal area networks(WPAN) under the following 5 criteria:

1. Market Potential: How many application, devices, vendors, customers are available for a certain technology?
2. Compatibility: Compatibility with IEEE 802.
3. Distinct Identity: Originally the study group did not want to establish a second 802.11 standard. However, topics such as low cost, low power or small form factor are not addressed in the 802.11 standard.
4. Technical Feasibility: Prototypes are necessary for further discussion, so the study group would not rely on paper work.
5. Economic Feasibility: Everything developed within this group should be cheaper than other solutions and allow for high-volume productions

Bluetooth fulfills these criteria so the WPAN group cooperated with the Bluetooth consortium. IEEE founded its own group for WPANs, IEEE 802.15, in March 199. This group should develop standards for wireless communications within a personal operating space. A POS has been defined as a radius of 10m around a person which the person or devices of this person communicate with other devices.

States of Bluetooth Devices

To save battery power, a Bluetooth device can go into one of three low power states:

1. Sniff State: The sniff state has the highest power consumption of the low power states. Here the device listens to the Piconet at a reduced rate. The interval for listening into the medium can be programmed and is application dependent. The master designates a reduced number of slots for transmission to slaves in sniff state. However the device keeps its AMA.

2. Hold State: The device does not release its AMA but stops ACL transmission. A slave may still exchange SCO packets. If there is no activity in the piconet, the slave may either reduce power consumption or participate in another piconet.

3. Park State: In this state the device has the lowest duty cycle and the lowest power consumption. The device releases its AMA and receives a parked member address(PMA). The device is still a member of the

piconet, but gives room for another device to be- come active(AMA is only 3 bit, PMA is 8bit) Parked devices are still FH synchronised and wake up at a certain beacon intervals for re-synchronisation. All PDUs sent to parked slaves are broadcast.

Types of services

Connection of peripheral devices:

Today, most devices are connected to a desktop computer via wires. This type of connection has several disadvantages: each device has its own type of cable, different plugs are needed, wires block office space etc. In a wireless network no wires are needed for data transmission.

Support of ad-hoc networking:

Support of ad-hoc networking: Imagine several people coming together, discussing issues, exchanging data. For instance, students might join a lecture, with the teacher distributing data to their personal digital assistants(PDA's). Wireless networks can support this type of interaction; small devices might not have WLAN adapters following the IEEE 802.11 standard but cheaper Bluetooth chips built in.

Bridging of networks

Using wireless piconets, a mobile phone can be connected to a PDA or laptop in a simple way. Mobile phones will not have full WLAN adapters built in, but could have a Bluetooth chip. The mobile phone can then act as a bridge between the local piconet and, e.g., the global GSM network. For instance, on arrival at an airport, a person's mobile phone could receive e-mail via GSM and forward it to the laptop which is still in a suitcase.

Piconet

A piconet is a collection of Bluetooth devices which are synchronised to the same hopping sequence. One device in the piconet can act as a master(M), all other devices connected to the master must act as slaves(S). The master determines the hopping pattern in the piconet and the slaves have to synchronise to this pattern. Each piconet has a unique hopping pat- tern. If a device wants to participate it has to synchronise to this.

Each piconet has exactly one master and up to seven simultaneous slaves. More tha n200 devices can be parked. The reason for the upper limit of eight active devices is the 2-bit addresses used in Bluetooth. If a parked device wants to communicate and there are already seven active slaves, one slave has to switch to park mode to allow the parked device to switch to active mode.

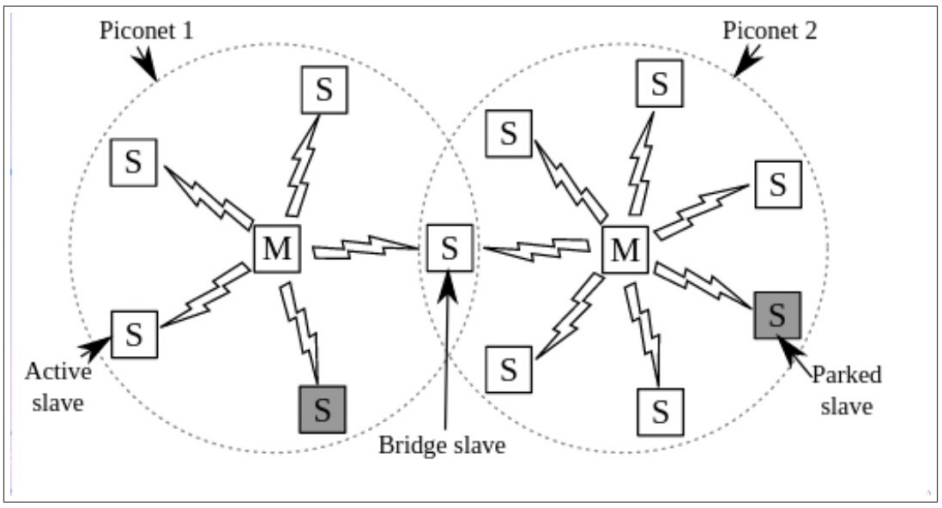

Figure 1

Scatternet

All users within one piconet have the same hopping sequence and share the same 1MHz channel. As more users join the piconet, the throughput per user drops quickly. This led to the idea of forming groups of piconets called scatternet. Only those units that really must exchange data hare the same piconet so that many piconets with overlapping coverage can exist simultaneously.

If a device wants to participate in more than one piconet, it has to synchronise to the hopping sequence of the piconet it wants to take part in. Before leaving one piconet, a slave informs the current master that it will be unavailable for a certain amount of time.

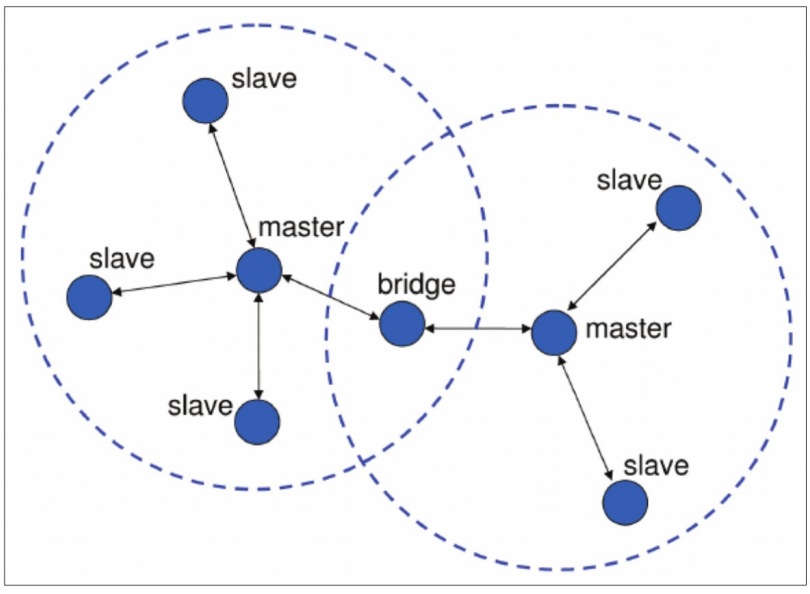

Figure 2

Security

The main security features offered by Bluetooth include a challenge response routine for authentication, a stream cipher for encryption, and a session key generation. Each connection may require a one-way, two-way, or no authentication using the challenge-response routine. All these schemes have to be implemented in silicon and higher layers should offer stronger encryption if needed. The security features included in Bluetooth only help to set up a local domain of trust between devices.

The security algorithms use the public identity of a device, a secret private user key, and an internally generated random key as input parameters. For each transaction, a new random number is generated on the Bluetooth chip. Key management is left to higher layer software

Conclusion: A case study of bluetooth was successfully conducted