Bluetooth

Sikkerhed and 5.1 forbedringer

Generelt

Bluetooth opererer på 2.4GHz ISM båndet, med to modulation modes. Det ene mode er et obligatorisk FM mode, kaldet "Basic Rate". Det andet mode er et valgfrit PSK mode, kaldet "Enchanced Rate". Basic Rate har en data rate på 1 Mb/s, mens Enhanced rate har to varianter, "π/4-DQPSK" og "8DPSK", som har 2 Mb/s og 3 Mb/s henholdsvist.
Bluetooth blev i 2005 standardiseret af IEEE under 802.15.1, men den standard er ikke blevet opretholdt siden.

Forbindelse

En bluetooth forbindelse er en ad hoc forbindelse med en master/slave struktur. Et bluetooth netværk med en master der har flere slaves kaldes en piconet. Det device som initierer forbindelsen er som standard master og det modtagende device er slave, men disse roller kan skifte efter forbindelsen er oprettet. Et rolleskift sker hvis det modtagende device allerede er master for en piconet og det initierende device skal modtage den samme info som resten af piconetten, fx Du forbinder dig med din smartphone til en vejrstation, der sender info til en piconet andre smartphones. Under forbindelses processen er din smartphone masteren, men efter forbindelsen er etableret vil vejrstationen initiere et rolleskift, for at få forbindelsen til at køre på sin egen clock-frekvens, så piconetten ikke skal vente på din smartphone før de kan få informationen.

Etablering af forbindelse

<u>Inquiry:</u> et device broadcaster en inquiry request og alle devices der lytter efter en sådan request svarer med deres unikke BD-ADDR (MAC-adresse lignende) og evt deres navn + yderligere info.
<u>Paging:</u> Når et device vælger et andet device at forbinde til starter paging sekvensen, som følger:

1. **Det initierende device(herefter master) sender en ID pakke til til det modtagende device (herefter slave).**
2. **Slaven svarer med en ID pakke.**
3. **Masteren sender en FHS pakke(Frequency Hopping Sequence). Denne pakke indeholder masterens adresse, clock-frekvens, den hop-sekvens masteren vil følge.**
4. **Slaven svarer med en ID pakke.**
5. **Masteren går i gang med hop-sekvensen fra FHS pakken. Forbindelsen er nu etableret.**

<u>Connection:</u>
Når forbindelsen er etableret, går de forbundene devices i connection state. i connection state er der 4 modes et device kan være i:

1. **Active mode - Devicet sender eller modtager aktivt data.**
2. **Sniff mode - Dette er et strømbesparende mode, hvor devicet kun lytter efter transmissioner ved bestemte intervaller, fx hver 100ms.**
3. **Hold mode - Devicet sleeper i et bestemt interval. Masteren kan tvinge en slave i hold mode.**
4. **Park mode - Masteren sætter slaven til sleep indtil masteren vækker slaven igen. dette mode er blevet udfaset med Bluetooth 5.**

Sikkerhed

Security Architecture

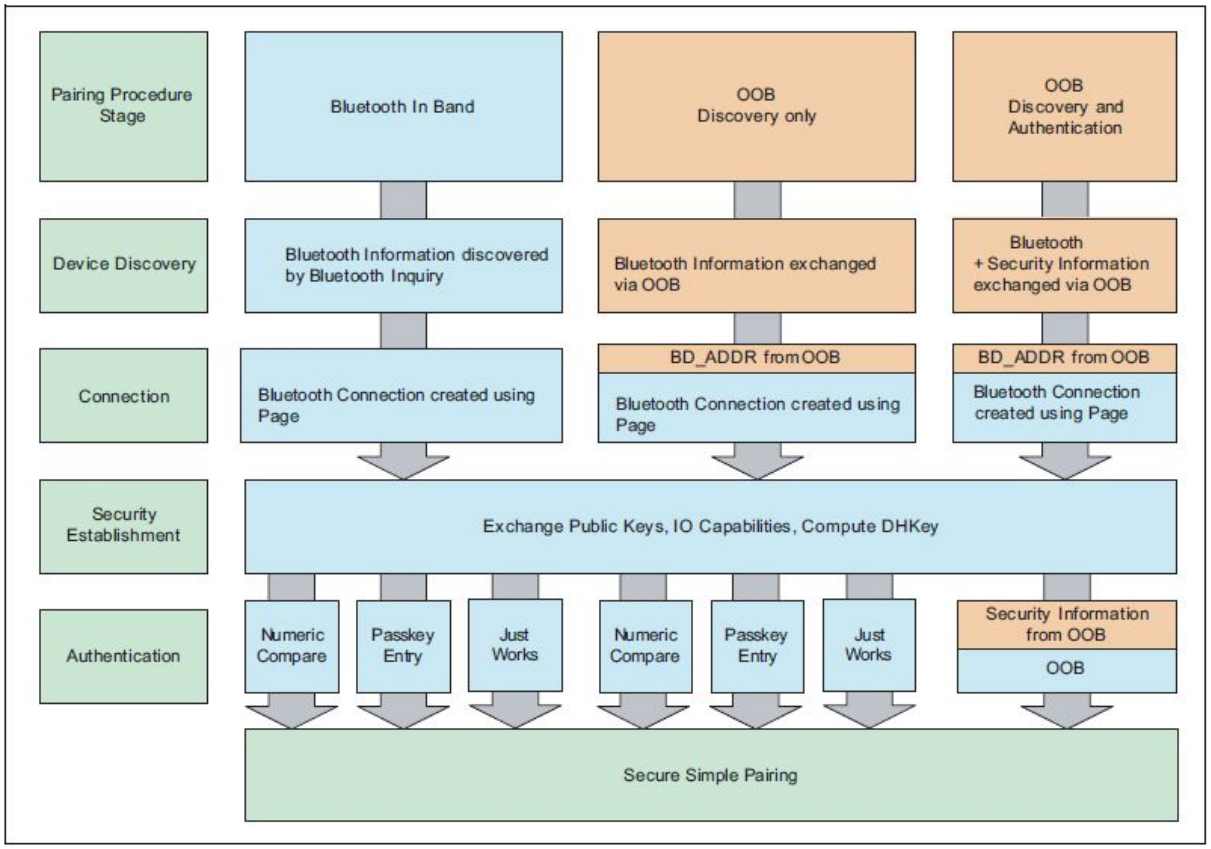
Pairing:
Generering af en til flere nøgler på devices for at parre dem sammen

Bonding:
Gemmer skabte nøgler for at have hurtigere adgang ved at lave "trusted Pairs"

Device Authentication:
Verificerer at enhederne har de samme nøgler

Encryption:
Ensuring Confidentiality by using ECDH:
ECDH(Ellipic Curve Diffie-Hellman) er en anonym nøgle godkendelsesprotokol som der tillader to enheder at dele en Secret over et usikkert netværk. Det er simpelt beskrevet en generering af to nøgler (En Public og en Private) på hver enhed som der beskytter dataen og trafikken mellem disse enheder. Den Public key er brugt til at finde og identificerer den anden enhed og den private key er brugt til at kryptere og dekryptere dataen.

Message Integrity:
Beskyttelse mod forfalskning af beskeder.



Protection Features

<u>Passive Eavesdrop Protection:</u>
Passive eavesdropping er når et device ikke kan interagere med nogle af enhederne i en forbindelse mellem to enheder, men eavesdropperen vil hente data fra begge enheder som den har forbindelse med. Fordi at attackeren ikke vil ændre i data er den meget svær at opsnappe. Ved at bruge ECDH så er forbindelserne sikret og dataen er krypteret, så det forhindrer en attacker i at kunne læse informationerne overhovedet.
Dette bliver også kaldet Secure Simple Pairing.
Når man bruger en LE version af Bluetooth har man ikke Secure Simple Pairing så man er nødt til at bruge en PIN.

<u>Man in the middle protection:</u>
MITM angreb er når to bruger opretter forbindelse til hinanden, men i stedet for at forbinde direkte med hinanden forbinder de til hinanden igennem et tredje device.
Det Tredje device opfører sig som en gateway mellem de to andre devices og vil opsnappe alt data der bliver sendt mellem de to enheder.
Det angribende device er også i stand til at modificere informationer eller data eller indsætte kommandoer der kan gøre skade på begge enheder.
Til at bekæmpe dette bruger Simple Secure Pairing to metoder. Numeric Comparison eller Pass Entry.

<u>Numeric comparison:</u>
Numeric Comparison er designet til at når de to devices der vil forbinde til hinanden opretter forbindelsen, et 6 cifret tal vil dukke op på skærmene og vil spørge om tallene er det samme på begge enheder. Man kan så trykke eller skrive "yes" for at fuldføre oprettelsen af forbindelsen.

<u>Passkey entry:</u>
Næsten ligesom numeric comparison, passkey entry genererer en nøgle på 6 cifre som der skal skrives ind på den anden enhed som man vil oprette forbindelse til.

<u>Just Works:</u>
Just Works er brugt i et tilfælde hvor en enhed man vil forbinde til ikke kan vise 6 cifre som i Numeric Comparison, og brugeren bliver bare spurgt om man vil oprette forbindelse. Den har stadig den numeric Comparison som beskytter den mod passive eavesdropping men ikke imod Man In The Middle Angreb.

<u>Out of Band:</u>
Out of Band er primært designet til tilfælde hvor en Out of Band mekanisme er brugt til at discover begge enheder som man vil forbindes med. Den overfører så kryptografiske numre mellem enhederne som en authentication. Den har en anden sikkerhedstype når man opretter en Out of Band kanal så den burde være beskyttet Imod MITM angreb, men hvis der opstår sådan et angreb er det i Authentication fasen.

Sikkerhed LE (Low Energy)

Just Works og passkey entry beskytter ikke imod passive eavesdropping, fordi Secure Simple Pairing bruger ECDH og LE bruger ikke Secure simple Pairing.

Bluetooth 5.1

Bluetooth 5 er dobbelt så hurtig, den har en overførselshastighed på 2 Mbps, men den sigter stadig efter at kunne opretholde en forbindelse over længere afstand, men med lavere bit hastighed.
I Bluetooth 4.* kunne man sende en pakke af 251 bytes data, som var sendt over en tidsramme af 2120 mikrosekunder, men med Bluetooth 5, så bliver det sendt over en tidsramme af 1060 mikrosekunder. Data hastigheden forbliver det samme, som den er i Bluetooth 4. dvs. at det tidsinterval mellem to fortløbende pakker ikke bliver hurtigere, det betyder, at data'en bliver sendt hurtigere, men det hul der er mellem pakkerne er stadig længere.

	Speed	Distance	Released Date	Bands	Backward Compatibility	New Hardware Requirement
Version 4.1	24MBs	100 m or 300 feet	4/12/2013	2.4 to 2.485 GHz	Yes	No
Version 4.2	24MBs	100 m or 300 feet	2/12/2014	2.4 to 2.485 GHz	Yes	For some feature
Version 5	48MBs	300 m or 985 feet	16/06/2016	2.4 to 2.485 GHz	No	Yes

Den nye Bluetooth version har også arbejde på en bedre form kommunikation, men ikke til de højttalere og smartwatch etc. Men en ny måde at kunne forbinde sig til "Internet of Things" over længere afstand. Med denne nye teknologi vil man kunne placere moduler i åbne områder, som kan hente temperatur, fugtighed, bevægelse eller trafikdata osv. Normalt vil problemet i dette tilfælde være, at disse moduler skal have strøm. Hvis det hele skulle kører over Wifi, men med Bluetooth 5 nye "Long Range", så behøver de moduler, som bruger bluetooth, ikke nødvendigvis at skulle have strøm fra en stikkontakt. Med Bluetooth "Long Range", så behøver de kun et batteri, for at kunne anvende sensorer. Men det er så her et nyt problem opstår. Hvis skal sende større pakker af data hurtig over en længere distance, så kommer modulet til at bruge mere strøm. Det problem løser Bluetooth ved at sænke hastighed på forbindelsen.

FEC

For at sikre at forbindelsen er pålidelig, så bruger Bluetooth en fejl korrektionsmetode kaldet FEC (Forward Error Correction), den bliver anvendt således, at et enkelt tal som "1" bliver multipliceret af det samme tal, så det danner et ord. Det er med til at sikre, at den data der bliver sendt ikke bliver korrupt, når afstanden er længere.
For eksempel hvis noget korrupt data bliver sendt med "0001" , så kan vi med sikkerhed forvente, at den oprindelig data er "0000" og omvendt hvis den er "1110", så ved vi at den oprindeligt er "1111". Men det eneste problem med denne metode er, hvis noget korrupt

data gå fra “0000” til “1010”, er der indtil videre ikke være nogen måde at vide hvad dataen var, før den blev korrupt.
Med Bluetooth 5 vil vi være i stand til at modtage data over 100 meter væk, og med FEC kan vi med større sandsynlighed sikre, at den data sendte ikke bliver korrupt.