TSEA56 KANDIDATPROJEKT

Förstudie kommunikation

Trådlös kommunikation

Version 1.1

Matilda Östlund Visén & Emma Söderström

2015-05-06

Sammanfattning av dokument

Denna rapport presenterar två kommunikationsstandarder, Bluetooth och ZigBee, för att sedan jämföra standardernas förmåga att skicka och ta emot information säkert och störningsfritt mellan en robot och PC. Både Bluetooth och ZigBee tillhör IEEE 802.15 standarden för trådlös kommunikation men har olika signalspridningsmodeller. Standarderna skiljer sig åt i flera aspekter, de skillnader som påverkar valet av standard är pålitlighet i Wi-Fi-täta områden, säkerhet och smidighet. Det visar sig att ZigBee påverkas mer av Wi-Fi-placering än Bluetooth och att Bluetooth förefaller smidigare i användarfallet. Däremot finns säkerhetsstandarder i båda fallen som ger hög säkerhet på informationsdelning samt skydd mot icke-auktoriserade användare. Sammantaget anses Bluetooth vara det bättre valet för användarsyftet.

Innehållsförteckning

1. Inledning

Dagens samhälle blir mer och mer trådlöst allteftersom tekniken går framåt. Kommunikation mellan enheter kan nu ske utan att fysiskt koppla ihop dem med kablar eller liknande. Den trådlösa kommunikationen förenklar många småsaker i vardagen och tillåter informationsdelning snabbt, smidigt och enkelt. Allt ifrån mobiltelefoner till vitvaror kan kommunicera trådlöst med varandra och exempelvis tillåta användaren att ändra inställningar på kylskåpet eller sätta på tvättmaskinen, utan att behöva befinna sig i samma rum. Metoden för att dela information mellan enheter varierar beroende på syftet med informationsdelningen. Vid långa avstånd med mycket hinder är vissa metoder mer effektiva medan andra är mer effektiva vid korta avstånd utan hinder. Även säkerhet och pålitlighet varierar mellan metoderna vilket innebär att vid val av metod måste flera variabler tas i beaktning för att syftet med enheten ska uppfyllas på bästa vis.

2. Mål och syfte

Det huvudsakliga syftet med denna skrivuppgift är att studenten individuellt ska få träna på tekniskdokumentation. Huvudfokus ligger på de vetenskapliga delarna samt det tekniska språket som används. Denna skrivuppgift kan också ses som en introduktion till ett framtida examensarbete.

Målet med denna förstudie är att beskriva och diskutera olika principer/metoder för trådlös styrning och övervakning av en robot för att sedan välja den mest fördelaktiga metoden för projektets robot. Olika kommunikationslösningar kommer att utvärderas utifrån olika funktionaliteter och frågeställningar. Målsättningen är även att besvara dessa frågeställningar i rapporten.

3. Problemformulering

För att kunna styra en robot via en dator, vilket efterfrågas i projektet, behövs någon form av trådlös uppkoppling. Styrkommandon, kartinformation, sensorvärden och liknande behöver skickas till och från roboten. Det eftersökta är en metod som fungerar bra på korta avstånd och som är pålitlig i normala rumsförhållanden med Wi-Fi-tillgång. Krav på informationsdelningen består bland annat i:

- Säkerhet: Kan någon avlyssna informationen eller skicka falska kommandon?
- Prestanda: Hur snabbt kan data skickas utan att datapaket försvinner? Kan andra enheter, så som Wi-Fi, påverka hastighet och pålitlighet? Hur bra presterar kommunikationsmetoden på korta respektive långa avstånd?

Det är även önskvärt med smidig uppkoppling och få komponenter. Även programvarutillgänglighet och användarvänlighet bör tas i beaktning vid valet av standard.

I rapporten kommer ovanstående krav jämföras mellan Bluetooth och ZigBee för att komma fram till vilken av de två metoderna som är mest fördelaktig för syftet att styra projektets robot.

4. Bakgrundsteori

Det som överlägset flest trådlösa tekniker använder sig av är radiovågor och IR [1], i vissa fall kan även elektromagnetiska vågor eller ljud användas. Det som skiljer de olika

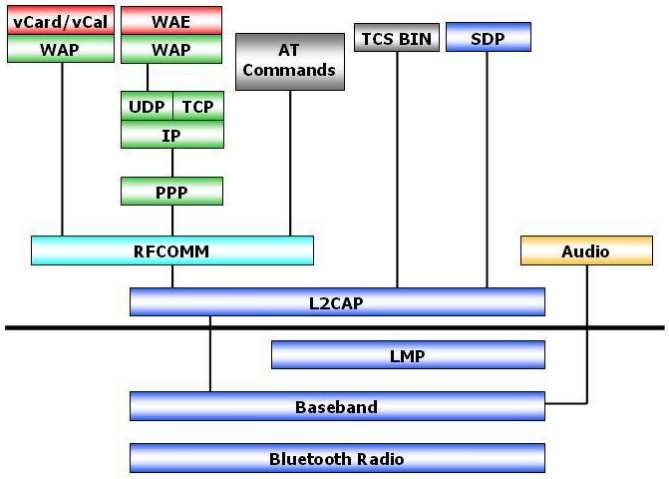
standarderna åt är hur mycket information som kan överföras på en viss tid, vilka frekvenser och spektrum som används samt hur säker och störningsfri transmissionen är. Det finns exempelvis standarder som Bluetooth, Bluetooth Low Energy, ZigBee, WLAN, WiMax och Wireless USB (UWB) som alla använder sig av olika frekvenser och spektrum vid transmission.

4.1. Bluetooth

Bluetooth är namnet på en standard (IEEE 802.15.1) utfärdad för trådlös kommunikation mellan enheter via radiovågor. Tekniken strävar efter att vara så ekonomi- och energisnål som möjligt samtidigt som den ska vara robust [2] . Standarden gör det möjligt att överföra information från en enhet till en annan utan att behöva kabel som ansluter dem. Kommunikation kan ske även om föremål befinner sig mellan enheterna förutsatt att de befinner sig tillräckligt nära varandra. Räckvidden för Bluetoothteknologin är minst 10m vid fri väg men är obegränsad uppåt, dock finns begränsningar beroende på enhetens uppgift, given effekt och tillverkarens önskemål.

4.1.1. Hårdvara

Bluetoothenhetens hårdvara (figur 1) består av en kombinerad radiosändare och mottagare för att kunna både skicka och ta emot information via radiovågor, ett "Baseband Protocol" (BBP) som matar radiosändaren med rätt data samt ett "Link Manager Protocol" (LMP) som ser till att BBP:n matar rätt information till radion och att informationen kommer till rätt ställe.



Figur 1 Protokollhierarki inom Bluetooth [i]

4.1.2. Radiokommunikation

Radiokommunikationen är verksam inom ISM-bandet som i dagens samhälle är rätt trångt, vilket kan leda till störningar i informationsdelningen [2]. För att undvika dessa störningar vid datatransmissionerna byter Bluetoothenheterna frekvensområde i bestämda mönster, även kallat FHSS (Frequency Hop Spread Spectrum). Genom att hoppa mellan de olika frekvenserna fås mindre störningskänslighet och säkerheten ökar i transmissionen. Standarden har 79 kanaler utspridda mellan 2.402 GHz och 2.48 GHz [3] där var och en av kanalerna har en bandbredd på 1MHz [2]. Dataöverföringshastigheten mellan Bluetoothenheter är maximalt 1Mbps, men om man tar hänsyn till länkar och dylikt fås en resulterande överföringshastighet på 723kbps.

4.1.3. Uppkoppling mellan enheter

Alla Bluetoothenheter har en helt unik 48 bitars adress som används för identifiering av enheten samt för att ge information om vilken hoppsekvens enheten använder sig av [4]. Varje Bluetoothenhet både skickar ut identifieringsmeddelanden, så kallade "beacons", och avsöker det direkta närområdet efter andra enheters beacons. När en annan enhets beacon upptäcks svarar enheten genom att skicka tillbaka en adress för möjlig uppkoppling mellan enheterna, så kallad parningsförfrågan. När parningsförfrågan besvarats kan en master-slav kommunikation upprättas mellan enheterna efter att användaren skrivit in en förutbestämd säkerhetskod i en av enheterna (ibland båda). En av enheterna får ansvaret som master medan den andra blir slav. Mastern har kontroll över hoppsekvenserna och slaven får rätta sig efter masterns hoppsekvens och klocksignal. Bluetoothenheterna sägs nu vara parade.

Det finns två typer av uppkoppling mellan enheter, Asynkron Anslutningslös (ACL) länk för dataöverföring med en överföringshastighet på maximalt 723.2 kB/s och Synkron Anslutningsorienterad (SCO) länk för ljudöverföring med en hastighet på maximalt 433.0kB/s [5]. Vid asynkron överföring tas ingen hänsyn till i vilken ordning bitarna kommer utan de sätts ihop i mottagaren medan vid synkron överföring skickas data i den ordning som de ska vara, exempelvis ljud bör vara synkront. Vid dataöverföring och styrning av en robot är ACL att föredra eftersom det har en högre överföringshastighet och ordningen på data inte spelar någon roll.

4.1.4. Informationsdelning

När två enheter är ihopkopplade kan informationsdelning genomföras. Data som ska skickas är ofta långa paket som inte kan skickas direkt via radiosändaren. Första uppdelningen sker i "Logical Link Control and Adaption Protocol" (L2CAP) där informationen delas upp i delar lagom stora för Baseband protokollet (BBP) att hantera. Väl i BBP:n delas datastycket ytterligare för att kunna skickas via radiosändaren till en annan enhet. När information tas emot går den återigen via BBP:n som sätter ihop datapaketen och skickar vidare till L2CAP för ytterligare sammansättning till ursprungsstorlek. Kommunikationen mellan enheterna upprättas via Link Manager Protokollet (LMP) som även hanterar FHSS och datastorleken till BBP.

4.1.5. Säkerhet

Det finns tre grundläggande säkerhetstjänster specificerade i Bluetoothstandarden [6]:

- Autentisering: Verifiering av de kommunicerande enheternas identiteter baserat på enhetsadresser.
- Konfidentialitet: Förhindrar informationskompromisser orsakade av avlyssning genom att säkerställa att enbart behöriga enheter har tillgång till skickad information.
- Auktorisation: Tillåter kontroll av resurser genom att säkerställa att enheten har rätt att använda en tjänst innan den får tillåtelse att göra det.

Bluetoothstandarden erbjuder fyra säkerhetslägen för enheterna [6] [7].

Säkerhetsläge 1 anses vara osäker. Inga säkerhetsfunktioner, så som autentisering eller kryptering, initialiseras. Följaktligen är enheten mottaglig för attacker. Läget tillåter att andra Bluetoothenheter att upprätta anslutning utan verifiering men om den andra enheten vill upprätta en säker anslutning, så som parning, autentisering eller kryptering, så stödjer säkerhetsläge 1 det. Alla versioner av Bluetooth stödjer detta läge men det är inte rekommenderat att använda.

Säkerhetsläge 2 är ett servicenivåförstärkt läge där säkerhetsprocedurerna initieras efter att länkning i LMP initieras men före upprättning av L2CAP-kanalen. En lokal säkerhetsansvarig ansvarar för policys kring tillgång till protokoll och gränssnitt mellan andra protokoll och enhetsanvändare. Det är möjligt för enheten att tillåta tillgång till vissa tjänster utan att ge tillträde till andra tillgängliga tjänster. I säkerhetsläge 2 introduceras även auktorisering, där enheten får avgöra om en specifik enhet ska få tillgång till en viss tjänst. Säkerhets nivå 2 är tillgänglig för alla Bluetoothmoduler.

Säkerhetsläge 3 är ett länknivåförstärkt läge där alla säkerhetsåtgärder initieras innan den fysiska länken är helt upprättad. Säkerhetsnivån kräver autentisering, kryptering och auktorisation innan andra enheter får upprätta förbindelse eller upptäcka eventuella tjänster. Alla senare versioner av Bluetooth stödjer säkerhetsnivå 3.

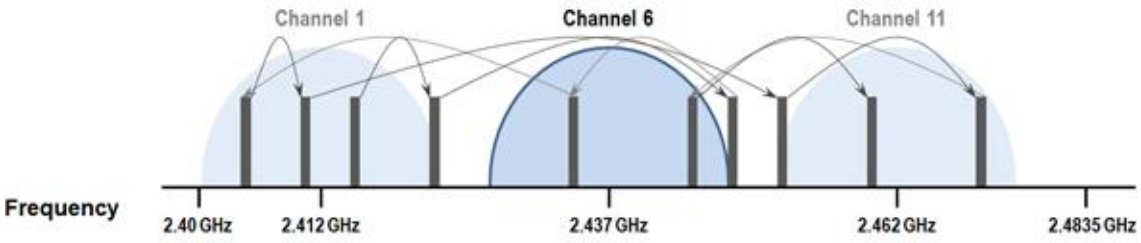
Precis som säkerhetsläge 2 är säkerhetsläge 4 ett servicenivåförstärkt säkerhetsläge där säkerhetsprocedurer initieras efter fysisk länkning men efter logisk länkning. Läget använder sig av "Secure Simple Pairing" (SPP) där en annan version av nyckel genereras. Säkerhetsläge 4 kräver att säkerhetskraven klassificeras som en av följande modeller:

- autentiserad länknyckel krävs
- Icke-autentiserad länknyckel krävs
- Ingen säkerhet krävs

SPP avgör vilken modell som ska användas.

4.1.6. Prestanda

Bluetoothstandarden strävar efter att vara så robust som möjligt. FHSS förhindrar i stor grad både avlyssning och störningar från andra enheter. Dock kan exempelvis mikrovågsugnar och IEEE 802.11 standarder med DSSS som spridningsmodell, vilket exempelvis Wi-Fi använder sig av, påverka prestandan om de verkar i samma frekvensområde [8] (se figur 2). Studier visar [9] [10] att för mindre datapaket (100kB) är störningen av Wi-Fi och överföringstid försumbar men vid delning av större datapaket minskar prestandan avsevärt. Syftet med robotens Bluetoothuppkoppling är dock inte att skicka datapaket som överskrider 100kB, prestandan borde därmed inte påverkas.



Figur 2 FHSS och DSSS i samma frekvensspektrum [ii]

4.1.7. Övrigt

En Bluetoothantenn är standardiserad till att ha en bandbredd på 100MHz och en effekt >50%. Effektförbrukningen är i jämförelse med exempelvis Wi-Fi låg, Bluetooth kräver ca

3% av den ström Wi-Fi behöver för att utföra samma uppgift [11]. Bluetoothmoduler drivs av batterier som är uppladdningsbara.

Priset på Bluetoothmoduler varierar mellan 300 och 800kr beroende på önskad hastighet, tillbehör etc.

4.2. ZigBee

ZigBee är huvudsakligen en standard för trådlös kommunikation. Den använder sig av digitala radiovågor för att styra och kommunicera med andra trådlösa enheter. Trådlös kommunikation via radiovågor innebär att föremålen ej behöver vara inom så kallade "*Line of sight",* vilket betyder inom synligt avstånd. Fjärrkontroller till exempelvis tv-aparater är sådana föremål som behöver vara inom synligt avstånd, då de enkelriktat kommunicerar med infrarött ljus. Detta är alltså inte fallet med ZigBee, som är en standard för dubbelriktad kommunikation där informationen skickas mellan olika trådlösa enheter i en nätverksstruktur. ZigBee standardens räckvidd är 30 meter inomhus och upp till 100 meter utomhus med "line of sight" [12].

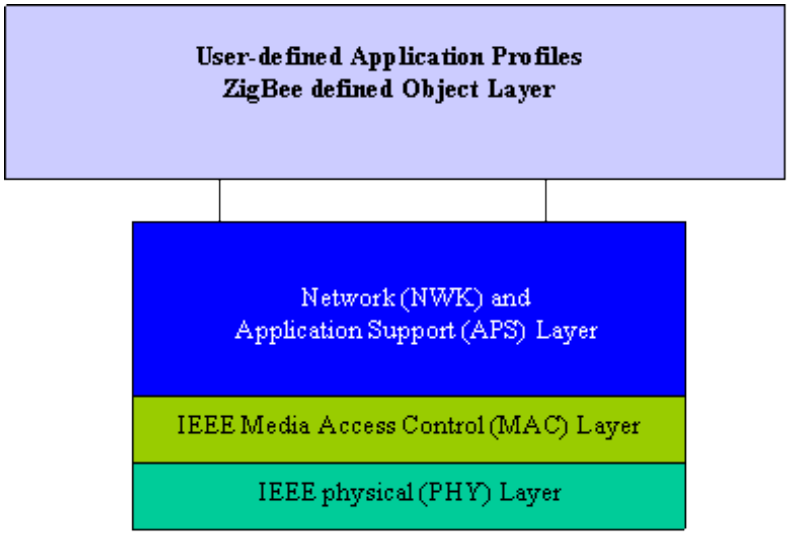
Det som kännetecknar ZigBee-standarden är att den är utformad för att ge en enkel användningsarkitektur för trådlösa nätverk med låg energiförbrukning. ZigBee används ofta för enheter som inte kräver en hög hastighet på dataöverföringen men kräver lång batteritid och ett säkert nätverk. Övervakning och styrning av olika applikationer är väsentliga användningsområden för denna standard. Inom industrin, där många olika delar ska kommunicera med varandra, kan tekniken utnyttjas av sensor-, övervaknings- och styrenheter. Patientövervakning inom hälsovården är ytterligare ett exempel på ZigBee-teknikens användningsområde. Men framförallt kan man också föreställa sig att ett ZigBee-nätverk är en mängd enheter i hushållet, så som trådlösa strömbrytare, högtalare, brandalarm och termostater, som kommunicerar med varandra [3].

4.2.1. Uppbyggnad

Arkitekturen av ZigBee-standarden, vilket är ett låg hastighets WPAN[1], är uppbyggd av ett antal block som kallas lager. Grunden för denna standard byggs upp av två lager från IEEE standaren 802.15.4 [2]för låghastighets WPANs, det så kallade fysiska lagret och "Media access control layer". Två nivåer uppåt återfinns Nätverks och Applikationslagret, vilket har designats av själva "ZigBee-Alliansen".

[1] WPAN - wireless personal area networks

[2] IEEE standaren 802.15.4 för mer information http://en.wikipedia.org/wiki/IEEE_802.15.4



Figur 3 IEEE 802.15.4 / ZigBee Stack Architecture [ZigBee: 'Wireless Control That Simply Works'] [iii]

Det så kallade fysiska lagret, vilket definierar de grundläggande elektriska egenskaperna för nätverket, är den lägsta nivån (skiktet) i hierarkin. Lagrets huvudsakliga uppgifter är överföring av data och mottagning, vilket innebär att ta emot och skicka information via radiovågor. På den tekniska och elektriska nivån innebär detta att lagret kartlägger samt bygger upp, beroende på mottagning eller sändning, de logiska bitarna så att informationen kan transformeras till en våg som går i luften (radiovåg).

Media access control lagret styr hur många radios som arbetar i samma område ska dela på dessa vågor som går i luften. Med detta menas att det tar hand om att styra sändarens och mottagarens, så kallade transceiverns, tillgång till den delade radiolänken samt kartläggning och dirigering av dataframes.

Nätverks-och applikationslagret tar hand om den information som fås från själva radioblocket, alltså det fysiska lagret och MAC-lagret. Huvuduppgiften för nätverkslagret är att säkerställa korrekt drift av det underliggande MAC-lagret samt tillhandahålla ett gränssnitt till applikationslagret. Det är även i nätverkslagret som själva nätverket byggs upp genom att tilldela nya enheter en adress. Mer information om nätverkslagrets funktioner tas upp i avsnitt uppkoppling/nätverksstruktur. Applikationslagret delas upp i flera dellager med lite olika uppgifter men sammanfattningsvis sköter den så kallade matchning mellan två enheter samt kommunikationen mellan dem. Det ansvarar alltså för att upptäcka andra enheter som arbetar inom samma operationsområde [12].

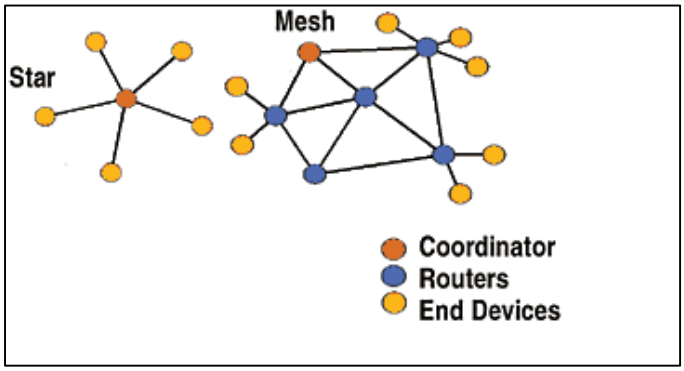
4.2.2. Radiokommunikation

ZigBees radioenheter är anpassade för att ha en låg kostnad i stor produktion samt har få analoga stadier och använder sig ofta av digitala kretsar. De har relativt snäva ramar för effekt och bandbredd. Radiokommunikationen sker inom ISM-bandet och kommunicerar huvudsakligen inom det globala 2.4 Ghz ISM-bandet men standarden kan även kommunicera inom 915Mhz(Amerika och Australien) samt 868MHz (Europa) ISM-banden [13]. I 2.4GHz bandet sker kommunikationen, för ZigBee-standarden, genom 16 olika kanaler som ligger utspridda mellan 2.405 till 2.480 GHz där varje kanal har en bandbredd på 2MHz och ligger med ett avstånd på 5Mhz mellan varandra. Radioenheterna använder sig av direct-sequence spred spectrum (DSSS) kodning vilket innebär att man sprider ut signalen

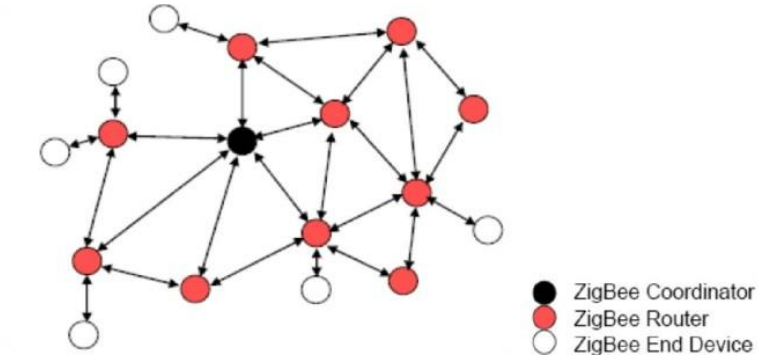
över ett stort frekvensband. Det minskar störningar i transmissioner men leder i sin tur till att säkerheten minskar eftersom ett fixt frekvensspektrum används [14] [12].

4.2.3. Uppkoppling mellan enheter

Det speciella kring ZigBee-standardens uppkoppling mellan enheterna är att den har stöd för en nätverksstruktur som kallas Mesh (se figur 4). Den möjliggör snabbare informations-delning och gör att informationen kan skickas nästintill oberoende av andra delar i systemet, vilket är en fördel om delar av nätverket är ur funktion. Det är det speciella master-slave-förhållandet med att det kan upprättas i olika kombinationer (att systemet inte har en fast master som styr allt) som bland annat gör att informationsdelningen kan ske snabbare. Standarden kan givetvis använda sig av så kallade Star-topologin med det vanliga master-slave-förhållandet, en master och flera slaves. Vilken nätverkstopologi som upprättas beror på vilka ZigBee-enheter som används. ZigBee-koordinatorn är exempelvis det som upprättar själva nätverket, vilket såklart är den viktigaste enheten. Därefter kan man även komplettera med en eller flera routrar som dirigerar datatrafiken vidare till så kallade slutenheter, vilka är kopplade till själva enheten man önskar att styra/övervaka, och då upprättas den så kallade mesh-strukturen.



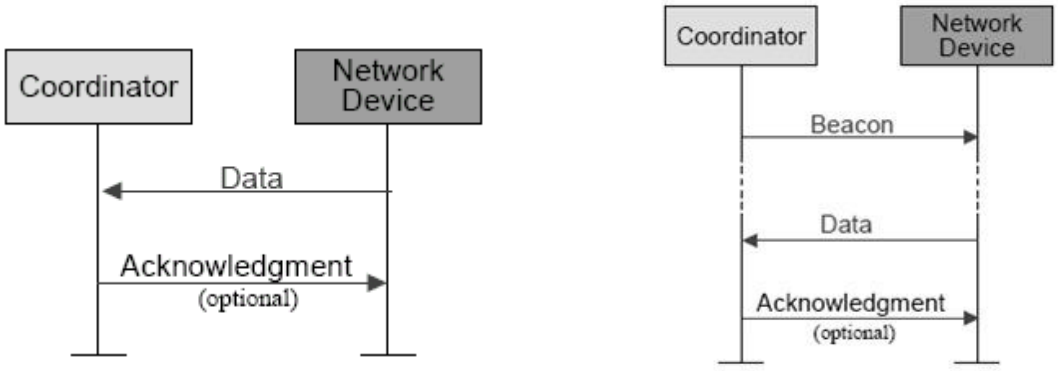
Figur 4 Mesh och star topologi struktur. [iv]



Figur 5 Mesh struktur med de olika ZigBee enheterna. [v]

4.2.4. Informationsdelning

Denna trådlösa nätverksstandard har stöd för både beacon och non-beacon aktiverade nätverk (se figur 5). Det betyder att den har stöd dels för nätverk som skickar ut identifieringsmeddelanden (beacons) för att känna av andra enheters identifieringssignaler samt nätverk som ej använder beacons. De så kallade non-beacon aktiverade nätverken har då vanligtvis sina ZigBee routrar kontinuerligt aktiva för att kunna ta emot information hela tiden alternativt för att endast sända då en extern signal upptäcks. Detta gör också att nätverket drar otrolig mängd energi så den behöver en robust energiförsörjare. Med beacons, identifierings meddelanden, kan man istället spara energi i nätverket. De skickar nämligen ut periodiska beacons, vilket gör att slav-enheterna kan ingå i någon form av standby-läge (sleep-mode) mellan intervallen och ”vaknar” endast för att bekräfta sin närvaro i nätverket.



Figur 6 ZigBee MAC Data Service Diagrams. [vi]

ZigBee-standarden använder sig av två olika metoder av adressering för dataöverförningen, 16-bitars NWK adress eller 64-bitars IEEE-adress. Innan en ZigBee-enhet (som har en IEEE 802.15-kompatibel radio) ansluts till ett nätverk, har den en global unik 64-bitars adress. Därefter tilldelas enheten ytterligare en 16-bitars NWK adress av nätverkslagret efter att enheten anslutits till nätverket [12]. Det är via en enkel ”lookup table” kartläggning av varje 64-bitars adress till en unik NWK adress sker som gör att båda adresserna kan användas för kommunikation. Denna 16-bitars adress kan då användas för kommunikation inom ett enklare nätverk, vilket gör att man sparar på adresseringsminnet genom att man har kortat ned meddelandet [15].

Tillgängligheten av 64-bitars adressering betyder att nätverket kan ha maximalt 2^64 enheter, vilket kan ses som att nätverket kan ha gränslöst många anslutna enheter. Ytterligare en utmärkande funktion för ZigBee-standarden är att den kan hantera över 65000 aktiva enheter i nätverket samtidigt utan att prestandan försämras [14].

4.2.5. Säkerhet

ZigBee-standarden använder sig huvudsakligen av nyckelbaserade krypteringssystem för att säkert kunna skicka och ta emot information. Datan krypteras innan den skickas iväg från källan och dekrypteras vid mottagaren genom ett 128-bitars krypteringssystem, vilket är baserat på AES (Advanced Encryption Standard) algoritmen [16]. Standardens säkerhetssystem bygger på tre olika nycklar Master, Link (länk) och Nätverksnycklar. Master nycklarna är förinstallerade i varje nod och dess funktion är att hemlighålla de konfidentiella länknycklarna mellan två noder då första nyckelutbytet sker. Länknycklarna är nämligen unika mellan varje nodpar och används för att kryptera all dataöverföring mellan två enheter. Nätverksnyckeln är en unik 128-bitars nyckel som delas mellan alla enheter i nätverket. Säkerhetsfunktionen med detta är att inga nya noder (enheter) ska kunna anslutas till nätverket utan en korrekt nätverksnyckel. Det är så kallade förtroendecentrat (Trust center) som generar denna och oftast är förtroende centrat koordinatorn i nätverket [17].

Den information som skickas mellan två enheter vill man ibland inte skicka igen, vilket betyder att man vill förhindra så kallade ”replay-attacker” på nätverket. Denna säkerhetsfunktion använder sig av en frame-räknare till meddelandet, varav dess värde jämförs med enhetens tidigare frame-räknarvärde, för att kunna avgöra hur gammalt ett mottaget meddelande är. Detta värde avgör i vilken ordning meddelandena skickats och kan då användas för att avvisa dessa meddelanden [16].

4.2.6. Prestanda

ZigBee-standarden anses vara en robust och säker standard men prestandan kan gå ned en aning i samverkan med andra nätverksstandarder. De nätverksstandarder som verkar inom samma frekvensband och arbetar nära varandra kan uppleva störningar och dataförluster. Tekniker som delar samma signalspektrum är bland annat Wi-Fi, Bluetooth och ZigBee. ZigBee-standarden har liten inverkan på Wi-Fi:s prestanda däremot kan Wi-Fi ha stor inverkan på ZigBees prestanda om tilldelningen av kanalerna inte noggrant beaktas. Detta är ett vanligt problem inom de tekniker som delar samma signalspektrum samt är tillräckligt nära varandra i avstånd [18]. Däremot förhindras avlyssning och störning ganska effektivt av krypteringssystemet i ZigBees säkerhetssystem.

5. Resultat

Både Bluetooth och ZigBee är verksamma i 2.4GHz frekvensbandet och tillhör samma WPAN (IEEE 802.15). Båda standarderna är energisnåla dock har Bluetoothbatteriet kortare livslängd än ZigBee-batteriet men är däremot uppladdningsbart.

Sammanfattningsvis ses följande skillnader mellan modulerna (B=Bluetooth, Z=ZigBee):

- Kommunikation och hastighet
  - B: Max 1Mb/s (asynkront) men realistiskt med protokoll blir hastigheten 723kbps
  - Z: Max 250kbps men realistiskt lägre än så.
- Uppkoppling och spridning
  - B: 48bitars adress, FHSS
  - Z: DSSS
- Informationsdelning:
  - B: 250kb protokoll stack
  - Z: 28kb protokoll stack
- Säkerhet:
  - B: 4 säkerhetslägen, krypterad nyckel
  - Z: nyckel
- Prestanda:
  - B: kan påverkas av Wi-Fi om de är verksamma i samma frekvensband
  - Z: stor påverkan var modulen befinner sig i förhållande till Wi-Fi sändare.

6. Diskussion

Syftet med kommunikationsenheten är främst att skicka sensor- och kartdata samt styrkommandon till och från roboten. Datapaketen är små och inte beroende av synkron dataöverföring, därför kommer inte maximala datahastigheten överskrida 250kbps.

Miljön där kommunikation med roboten kommer upprättas har Wi-Fi signaler i luften. Bluetooth använder sig av FHSS vilket, enligt studier, inte helt utesluter interferens med Wi-Fi signaler. ZigBee har också problem i Wi-Fi-täta miljöer då ZigBees spektrum till större del täcks av Wi-Fi-signalernas spektrum. Det visade sig i studierna att Bluetooth inte påverkas så mycket av Wi-Fi-modulens position utan har relativt konstant påverkan av Wi-Fi med varierat avstånd. ZigBee däremot påverkades mycket av positionen till Wi-Fi-sändaren, med ökat avstånd minskade påverkan markant. Miljön där roboten kommer kommunicera har

bestämda platser för Wi-Fi-sändarna, därför kan kommunikationspålitligheten visa sig olika beroende på var i miljön man befinner sig. Bluetooth är därför att föredra då pålitligheten inte förändras i förhållande till Wi-Fi-radioplacering.

Vid uppvisning av roboten kommer flera åskådare att infinna sig. Därmed är det viktigt att styrkommandon inte påverkas av andra Bluetoothenheter, då dessa finns lättillgängliga i dagens mobiltelefoner. ZigBee påverkas inte märkvärt av Bluetoothnärvaro likaså stör inte Bluetoothenheterna ut varandra.

Säkerheten på kanalen kommer också vara viktig i sammanhanget då roboten inte ska kunna styras av obehöriga. Bluetooth har flera möjliga säkerhetslägen där autentisering, konfidentialitet och auktorisering tas i beaktning, FHSS bidrar också till ökad säkerhet då endast de två kommunicerande enheterna vet hoppsekvensen via en delad nyckel. ZigBee använder sig av nyckelbaserade krypteringssystem för att säkert kunna skicka och ta emot information. Krypteringssystemet består av olika slags nycklar för olika säkerhetsfunktioner. För nätverksauktorisation krävs exempelvis tillgång till en 128-bitars nätverksnyckel medan en så kallade länknyckel används för att kryptera all dataöverföring mellan två enheter (noder) i nätverket.

Det finns många praktiska fördelar med Bluetooth gentemot ZigBee. Kommandon, datapaketen, kommer att skickas via en dator till roboten vilket gör att Bluetooth föredras, eftersom datorn har redan en förinstallerad Bluetoothenhet. Kommunikation via ZigBee kräver att gruppen måste ansluta ytterligare enheter till PC då PC:n inte har förinbyggda ZigBee-komponenter.

7. Slutsats

Slutsatsen är att Bluetoothstandarden är förhållandevis bättre för kommunikation mellan PC och robot än ZigBee-standarden i och med att dataförlusterna och störningarna är mindre vid användning av Bluetooth än ZigBee i Wi-Fi-förhållanden, vilket är en önskvärd egenskap för trådlös kommunikation. Tävlingen som roboten avser att delta i kommer även att ske i ett Wi-Fi-tätt område. Detta gör att roboten måste kunna kommunicera i ett extra störningskänsligt område oberoende av Wi-Fi-sändares placering. Ur den praktiska synpunkten föredras också Bluetooth eftersom både dess programvara och enhet är förinstallerad på PC:n. Ur säkerhetssynpunkt är däremot båda nätverksstandarderna relativt likvärdiga.

Utifrån prestanda och smidighet är Bluetooth den mest fördelaktiga metoden för styrningen av roboten.

Referenser

[1] Wikipedia, ”Wireless,” [Online]. Available: http://en.wikipedia.org/wiki/Wireless. [Använd 06 05 2015].

[2] K. Cho, W. Park, M. Hong, G. Park, W. Cho, J. Seo och K. Han, ”Analysis oc Latency Performance of Bluetooth Low Energy (BLE) Networks,” *Sensors,* nr 15, pp. 59-78, 2014.

[3] gc, ”tutorial-reports,” Tutorial-Reports, 18 02 2013. [Online]. Available: http://www.tutorial-reports.com/wireless/zigbee/zigbee-architecture.php. [Använd 03 03 2015].

[4] L. Harte, ”Bluetooth Basics,” i *Introduction to Bluetooth*, ALTHOS Publishing Inc., 2004.

[5] N. J. Muller, ”Basic Concepts,” i *Bluetooth Demystified*, New York, McGraw-Hill, 2000, p. 56.

[6] J. Padgette, K. Scarfone och L. Chen, ”Guide to Bluetooth Security,” National Institute of Standards and Technology, 2012.

[7] L. Chen, J. Ji och Z. Zhang, ”Security in Bluetooth Networks and Communications,” i *Wireless Network Security*, Beijing, Higher Education Press, 2013, pp. 82-83.

[8] S. Whilte, ”Wi-Fi and Bluetooth coexistance,” ESN, 2012.

[9] S. Pudaruth, H. K. Ramdolin och A. Bissoonee, ”An Assessment Of The Performance Of Bluetooth As Broadcasting Channel,” London, 2010.

[10] L. G. S. G. L. T. Rosario G. Garroppo, ”Experimental assessment of the coexistence of Wi-Fi, ZigBee, and Bluetooth devices,” Dept. of Information Engineering, University of Pisa, Italy, Pisa.

[11] E. Vogler, ”Bluetooth vs. Wi-Fi Power Consumption,” Demand Media.

[12] A. Tomar, ”element14,” 2011. [Online]. Available: https://www.element14.com/community/servlet/JiveServlet/previewBody/37177-102-1-219424/Introduction%20to%20Zigbee%20Technology.pdf. [Använd 03 03 2015].

[13] ”wikipedia,” 24 02 15. [Online]. Available: http://en.wikipedia.org/wiki/ISM_band. [Använd 04 03 15].

[14] ”wikipedia,” 14 02 15. [Online]. Available: http://en.wikipedia.org/wiki/ZigBee#Radio_hardware. [Använd 04 03 15].

[15] S. Farahani, ZigBee Wireless Networks and Transceivers, Newnes, 2011.

[16] Jennic, ”jennic,” 2007. [Online]. Available: http://www.jennic.com/elearning/zigbee/files/html/module5/module5-4.htm. [Använd 30 03 2015].

[17] D. Gascón, ”sensor-networks,” 05 02 2009. [Online]. Available: http://sensor-networks.org/index.php?page=0903503549. [Använd 30 03 2015].

[18] A. N. S. L. R. Challoo, ”An Overview and Assessment of Wireless Technologies and Co-existence of ZigBee, Bluetooth and Wi-Fi Devices,” Cihan H. Dagli, Washington D.C, 2012.

[19] G. Eriksson och P. Enmalm, ”Vetenskapsmetodik, CT3620”.

[20] D. P. F. Robert Lau, ”sensorsmag,” 01 06 2004. [Online]. Available: http://www.sensorsmag.com/networking-communications/wireless-sensor/the-realities-dealing-with-wireless-mesh-networks-774. [Använd 05 03 15].

[21] N. J. Muller, ”Bluetooth Security,” i *Bluetooth Demystified*, New York, McGraw-Hill, 2000, p. 290.

Bildreferenser

[i] Wikimedia, "Bluetooth protocolstack" [Bild]. http://upload.wikimedia.org/wikipedia/it/f/f2/BluetoothProtocolStack.JPG [Besökt 2015-04-01]

[ii] ECN, “FHSS ans DSSS transmissions and collisions” [Bild] http://upload.wikimedia.org/wikipedia/it/f/f2/BluetoothProtocolStack.JPG [Besökt 2015-04-01]

[iii] ZigBee Tutorial “Stack architecture of ZigBee” [Bild] http://www.tutorial-reports.com/sites/default/files/zigbee-architecture.gif [Besökt 2015-04-01]

[iv] SensorsOnline “Topology structure” [Bild] http://www.sensorsmag.com/files/sensor/nodes/2004/774/fig2.gif [Besökt 2015-04-01]

[v] Theater Controller “ZigBee mesh network” [Bild] http://www.csurambox.com/documents/report/images/report_img_5.jpg [Besökt 2015-04-01]

[vi] Element14 “ZigBee MAC Data Service Diagrams” [Bild] https://www.element14.com/community/servlet/JiveServlet/downloadBody/37177-102-1-219424/Introduction%20to%20Zigbee%20Technology.pdf (s.23) [Besökt 2015-04-01]