TSEA56 - Kandidatprojekt i elektronik

Säkerhet i kommunikationen

Förstudie, uppgift 2

Version 1.1

Fridborn, Fredrik, `frefr166`
Skytt, Måns, `mansk700`

Birgitte Saxtrup, TEMA-handledare
Jan-Åke Larsson, ISY-Handledare
Kent Palmkvist, Beställare

2015-04-28

Status

Granskad	AB	2015-04-28
Godkänd		

PROJEKTIDENTITET

2015/VT, Undsättningsrobot Gr. 2
Tekniska högskolan vid Linköpings universitet, ISY

Namn	Ansvar	Telefon	E-post
Nikolaj Agafonov	Dokumentansvarig (DA)	072-276 99 46	nikag669@student.liu.se
Adnan Berberovic	Projektledare (PL)	070-491 96 07	adnbe196@student.liu.se
Andreas Brorsson	Testansvarig (TA)	073-524 44 60	andbr981@student.liu.se
Fredrik Fridborn	Designansvarig Sensormodul (DSE)	073-585 52 01	frefr166@student.liu.se
Robert Oprea	Designansvarig Styrmodul (DST)	070-022 10 18	robop806@student.liu.se
Måns Skytt	Designansvarig Kommunikationsmodul (DK)	070-354 28 84	mansk700@student.liu.se

E-postlista för hela gruppen: adnbe196@student.liu.se

Kund: Kent Palmkvist, 581 83 Linköping, Kundtelefon: 013-28 13 47, kentp@isy.liu.se

Kursansvarig: Tomas Svensson, 013-28 13 68, tomass@isy.liu.se
Handledare: Olov Andersson, 013-28 26 58, Olov.Andersson@liu.se

Dokumenthistorik

Version	Datum	Utförda förändringar	Utförda av	Granskad
0.1	2015-03-05	Första utkastet	FF & MS	A. Brorsson
1.0	2015-04-01	Slutlig version	FF & MS	A. Brorsson
1.1	2015-04-28	Reviderad version	FF & MS	A. Brorsson

Innehåll

1 Inledning

För att skicka information finns många olika metoder och standarder som lämpar sig olika bra för olika tillämpningar. Denna rapport behandlar ett antal av de vanligaste trådlösa seriella kommunikationsprotokollen - främst de som överensstämmer med Institute of Electrical and Electronics Engineers (IEEE) 802.15 standarder (standard för Wireless Personal Area Network - WPAN). En jämförelse mellan dessa görs ur ett perspektiv där information ska skickas mellan en autonomt styrd robot och en dator. Aspekter som tas in i jämförelsen är bland annat *säkerhet*, *kostnad* och *lämplighet*.

I avsnitt 3 ges först en kort introduktion till begreppet *radiokommunikation*. Därefter förgrenas teorin i avsnitt som behandlar de olika kommunikationsprotokollen. I dessa avsnitt behandlas teknikerna bakom de olika kommunikationsprotokollen samt uttryck som förekommer frekvent reds ut för att ge en bra kunskapsbas att stå på inför jämförelsen i avsnitt 4.

När teorin bakom de olika protokollen avhandlats jämförs de olika protokollen (avsnitt 4). Teoriavsnittet är upplagt så att fördelar och nackdelar för behandlade metoder identifieras individuellt för att sedan jämföras mot varandra i en avslutande sammanfattning. För att besvara frågeställningar och redovisa uppnådda mål analyseras slutligen vilken kommunikationsstandard som bäst tillämpas i fallet med en autonomstyrd undsättningsrobot.

1.1 Syfte och Mål

Syftet med denna förstudie är att ge en bred kunskapsbas inom trådlös kommunikation och en spetskompetens inom vissa typer av trådlösa tekniker för dataöverföring. Detta för att kunna göra en jämförelse mellan de olika överföringsstandarderna och utvärdera vilken standard som passar bäst för vilken tillämpning. I just detta fall för en undsättningsrobot i projektkursen TSEA56 (Kandidatprojekt i elektronik). Detta innebär informationsutbyte mellan dator och kommunikationsenhet på roboten. [1]

Målen med denna förstudie kan konkretiseras i de punkter som följer nedan:

- *Att beskriva och utvärdera berörda kommunikationstekniker*
- *Att jämföra berörda kommunikationstekniker och deras fördelar samt nackdelar*
- *Att utifrån jämförelsen välja den bäst lämpade metoden i en specifik situation*
- *Att ta ställning till kända samt möjliga säkerhetsbrister*
- *Att komma fram till den bästa kommunikationsstandarden att tillämpa vid kommunikation mellan PC och en prototyp på undsättningsrobot*

1.2 Definitioner

- IEEE - Institute of Electrical and Electronics Engineers

- WPAN - Wireless Personal Area Network
- WLAN - Wireless local area network
- UWB - Ultra-wideband
- UHF - Ultra high frequency (0.3-3 GHz)
- SHF - Super high frequency (3-30 GHz)
- MAC - Media Adress Control
- OSI - Open Systems Interconnection
- SPD - Service Discovery Protocol
- GAP - Generic Acess Profile
- ACO - Autentiseringskrypteringsoffset

1.3 Kommunikation

I denna förstudie behandlas trådlösa seriella kommunikationslösningar för att komma fram till den bästa kommunikationslösningen för en autonomt styrd robot. Kommunikationen behöver därför vara trådlös för att inte dess funktionalitet skall hämmas för mycket även om en trådad kommunikation mest troligt skulle öka överföringens säkerhet och stabilitet.

1.4 Säkerhet

En viktig aspekt när det kommer till trådlös kommunikation är säkerhet. I och med att kommunikationen sker trådlöst så måste man ha insikt i hur man skyddar kommunikationen från störningar. Det kan röra sig om störningar från annan strålning eller rent fysiska hinder som en vägg, men även om störning från angripare som vill störa telekommunikationen eller rentutav avlyssna den och skicka iväg egna meddelanden.

1.5 Parter

Utöver projektgruppen på sida i är följande personer involverade i förstudien:

- Birgitte Saxtrup - TEMA-handledare. *Svarar för språkgranskning av förstudien.*
- Jan-Åke Larsson - ISY-handledare. *Svarar för teorigranskning av förstudien.*
- Kent Palmkvist - beställare. *Svarar för slutgiltigt godkännande av förstudien.*

1.6 IEEE standarder

De i studien behandlade kommunikationsprotokollen är alla i enlighet med IEEE:s standarder för dessa, se Tabell 1

Tabell 1: *Behandlade kommunikationsprotokoll samt korresponderande IEEE-standarder* [2]

Bluetooth	-	IEEE 802.15.1
ZigBee	-	IEEE 802.15.4
Wi-Fi	-	IEEE 802.11

1.7 Avgränsning

För att förstudien inte ska ta för många timmar i anspråk har den avgränsats till att bara undersöka tre stycken olika kommunikationsmetoder - Bluetooth, Wi-Fi och ZigBee. De kommer att analyseras och jämföras med avseende på deras säkerhet, kryptering, komplexitet, kostnad och lämplighet för projektet.

2 Problemformulering

Förstudien ska beskriva tre olika kommunikationsmetoder - Bluetooth, Wi-Fi och ZigBee. Detta för att kunna besvara frågan

Vilken av beskrivna kommunikationsmetoder är lämpligast för projektet?

2.1 Metod

För att besvara problemformuleringen kommer akademisk forskning bedrivas genom litteraturgranskning. Först hittas relevanta artiklar, därefter sammanställs informationen och materialet analyseras.

3 Teori

Detta avsnitt syftar till att sammanställa nödvändig bakgrundskunskap så att de olika kommunikationsmetoderna kan analyseras. Inledningsvis beskrivs radiokommunikation generellt och därefter introduceras några grundbegrepp inom IT-säkerhet och kryptering.

3.1 Radiokommunikation

Radiokommunikation är ett sätt att trådlöst överföra information som till exempel ljud, bild eller data. Man kan förmedla information i elektromagnetiska vågor (radiovågor) genom att simulera binära meddelanden via modulering av vågen på olika sätt, exempelvis att ändra amplitud, frekvens eller att fasförskjuta signalen. Frekvensen för vågorna varierar beroende på ändamål men kan vara allt från 10^0 [3] - 10^{12} [4] Hz. Signalerna skickas från och tas emot av en antenn. Våglängden som antennen ska ta emot påverkar hur stor antennen ska vara. Vanligtvis brukar antennen göras till en hel, halv eller fjärdedels våglängd. Om sändning sker kring 500-1500 kHz blir våglängden hundratals meter lång [5].

3.2 Trådlös IT-Säkerhet

När datorer gick från att vara ihopkopplade via nätverkskablar till att få trådlös uppkoppling ökade användarens frihet markant - man tvingades inte längre sitta vid ett nätverksuttag för

att kunna kommunicera med andra datorer. Att förflytta kommunikationen från sladdar till radiovågor gav däremot upphov till att kommunikationen mellan enheterna hamnar ute i etern. Det kan i sin tur leda till störningar från angripare som antingen bara vill störa telekommunikationen eller rentutav avlyssna den och skicka iväg egna meddelanden på samma kommunikationskanal.

3.2.1 Störningar

När informationen som ska skickas och tas emot ligger i etern är det mycket enkelt för angripare att påverka hur signalen uppfattas. Det är ofta ganska enkelt för angripare att förhindra signalen från att komma fram på rätt sätt till rätt person. Det kan handla om något så enkelt som att kontinuerligt försöka få åtkomst till en tjänst med många olika enheter för att ta på så sätt förhindra andra enheters åtkomst.

En av de mest vanliga störningarna av en angripare är en Denial-of-Service-attack (DoS-attack). DoS är ett medvetet försök att förhindra legitim användning av en tjänst. En Distributed-DoS-attack är en DoS-attack som utförs av flera olika enheter och den blir således mer potent. En angripare kan med DoS-attacker utsätta offret för stora datamängder illasinnad trafik som kan åstadkomma skada. Detta kan till exempel ske genom att delvis eller helt störa ut de tänkta användarna från att använda en tjänst eller att förhindra dem att kommunicera med varandra.

DoS-attacker kan genomföras på många olika sätt. Ett av de vanligaste sätten är att skicka en stor mängd datapaket. Paketen tar upp stora resurser hos mottagaren och förhindrar därmed åtkomst för de tänkta användarna. En annan vanlig metod är att angriparen skickar felaktiga datapaket som skapar förvirring hos mottagaren. För att åtgärda detta kan man antingen agera preventativt eller reaktivt. Preventativa åtgärder kan vara att eliminera chanserna för DDoS-attacker genom att till exempel förbättra protokolldesignen. Exempelvis innehåller många protokoll operationer som användaren genomför snabbt men som är mer resurskrävande för servern. Detta gör den känsligare för DDoS-attacker. Reaktiva åtgärder kan vara att detektera attacker i ett tidigt skede och motattackera. Detektionen kan vara att undersöka inkommande trafik och se om man ser kända attackmönster eller ovanligheter. För att sedan motattackera kan man exempelvis begränsa bandbredden som går till de paket som detekterats för att således minimera hotet [6].

3.3 Trådlös kryptering

För att lyckas skapa säkra kommunikationskanaler har det genom historien varit vanligt att kryptera information, vanligtvis till pseudo-slumpmässiga tecken. Efter att ett meddelande krypterats måste det dekrypteras med hjälp av en nyckel. Det är möjligt för en angripare att avkoda meddelandet utan denna nyckel men det kräver kraftfulla datorer och färdigheter i kodbrytning. Om en krypteringsnyckel väljs så att den innehåller 10 slumpmässiga ASCII-tecken tar det en angripare 4 miljarder år att dekryptera, om angriparen försöker med 10000 krypteringsnycklar i sekunden [7]. Att angriparen testar ett stort antal nycklar tills dess att rätt nyckel hittas kallas brute-force-attack.

Data Encryption Standard (DES) lanserades 1977 och var en av de första krypteringsstandarderna. Den var kraftfull men baserades på hårdvara vilket gjorde den

känslig när mjukvaran blev mer och mer kraftfull. Därmed ställdes det krav på att en ny, mer avancerad, standard skulle utvecklas. Denna är mer känd som Advanced Encryption Standard (AES) och den fasade ut DES under början av 2000-talet. Eftersom AES baserades på både hård- och mjukvara har den visat sig vara mycket motståndskraftig och väl lämpad för de säkerhetskrav som finns på dagens ökade behov av internethandel och transaktioner över internet [8], [9].

3.4 Kostnad

För att kunna undersöka den ekonomiska aspekten kommer kommunikationsmetoderna analyseras med avseende på effektivitet och hårdvara. Effektivitetsanalysen kommer avgöra om man uppnår god effekt med rimlig kostnad.

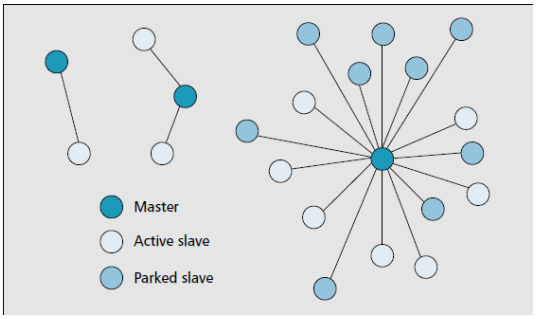
3.5 Bluetooth

Bluetooth (eller Blåtand) är en trådlös kommunikationsstandard som utvecklades under sent 90-tal och produkter med Bluetooth togs i bruk runt millenieskiftet. Det har blivit en vida använd standard och används främst vid kortare dataöverföring mellan exempelvis datorer, skrivare, mobiltelefoner och andra enheter som tidigare kopplades samman via kabel. Numera är Bluetooth en av de dominerande standarderna för trådlös dataöverföring över kortare avstånd [10], [11].

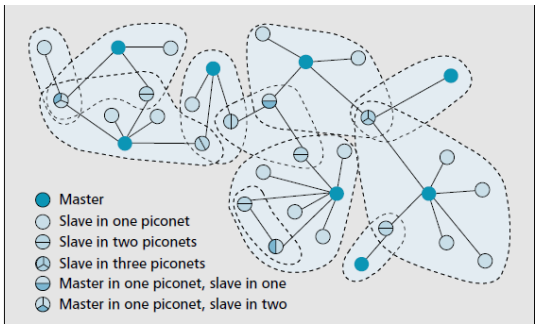
Det frekvensband som Bluetooth använder är ISM-bandet (2.45 GHz). Här i europa samt USA sträcker bandet sig från 2 400 till 2 483.5 Mhz men i övriga världen varierar detta intervall något [1][12].

3.5.1 Scatternet/Piconet

När Bluetoothenheter upprättar kontakt med varandra görs detta med en typ av anslutningstopologi som kallas *Scatternet* som är en utvidgning av anslutningstopologin *Piconet*. Scatternet består av flera Piconet [2].



Figur 1: *Olika varianter av Piconet illustreras*



Figur 2: *Ett mer komplext Scatternet*

Ett Piconet består av en enhet som är *master* (d.v.s. enheten i kontroll) samt minst en enhet som tjänar som *slav* under masterenheten. Alla slavar som är anslutna till en master är

[1]Spanien och Frankrike har endast delar av detta band tillgängligt. Japan: 2 471 till 2 497 MHz

synkade efter dess klocka och slavarna kan bara kommunicera med sin master. Antalet enheter i ett piconet är begränsat till 8 av dess 3-bitars adressrymd ($2^3 = 8$). Slavar kan även vara i ett stand-by-läge, *parkerade*, då de inte är aktiva och har en kraftigt reducerad strömförbrukning. I Figur 1 visualiseras olika Piconet-topologier med både aktiva och parkerade slavar.

Scatternet är en stor mängd ihopkopplade Piconet. Detta möjliggörs genom att en enhet kan angera som master- och slavenhet, dock inte inom samma Piconet. En enheten kan delta i upp till tre piconet men endast vara master i ett av dessa. I Figur 2 kan ett mer komplext Scatternet ses. Varje ljusare område med streckad gräns motsvarar ett Piconet.

3.5.2 Kanaldefinition

När enheter utbyter information via Bluetooth vill man undvika störningar från omgivningen. Bluetooth utnyttjar som tidigare nämnt ISM-bandet som är öppet för alla. Denna öppenhet medför att störningar förekommer frekvent. För att lösa störningsproblemet (en av flera anledningar) använder man en teknik som innebär att man hoppar mellan frekvenser, en metod som kallas *Frequency-hopping spread spectrum (FHSS)*. Detta görs via ett pseudo-slumpmässigt mönster som genereras från masterenhetens klocka och dess 48-bitar långa adress. Hoppen görs över 79 kanaler à 1 MHz med en frekvens av 1 600 hopp per sekund [13].

3.5.3 Upprättande av kontakt

För att upprätta kontakt mellan två enheter via bluetooth måste ett antal steg genomföras för att informationsutbyte ska påbörjas. Dessa steg är som följer:

- **Steg 1** - En enhet, E1, påbörjar en så kallad förfråganssökning (inquiry scan) då den söker efter enheter inom räckhåll.
- **Steg 2** - En annan enhet, E2, gör en förfrågan (inquiry) vilket gör att E1 upptäcker E2.
- **Steg 2b** - För extra säkerhet kan pairing utföras här
- **Steg 3** - E1 svarar på förfrågan med sin adress.
- **Steg 4** - E1 och E2 synkroniserar sedan frekvens och adress (för frekvenshoppning) med en teknik som kallas ”paging”.
- **Steg 5** - En basbandsanslutning har nu upprättats mellan de båda enheterna.
- **Steg 6** - Nu startas en SPD (Service Discovery Protocol) sökning, vanligtvis från E1 men kan även ske från E2. SPD är ett protokoll som gör att enheterna utbyter information om deras vilka ”tjänster” de har och identifierar deras karaktäristik.

3.5.4 Säkerhet

När man talar om datasystem är det vanligt att dela in säkerhetshot i kategorier. Det finns tre distinkta typer som säkerhetshot vid användning av Bluetooth kan delas in i. Dessa tre typer är integritetshot (innefattar icke-auktoriserade ändringar på information), informationsläckor (innefattar läckage av information till främmande parter som inte bör ha tillgång till) och till sist överbelastningshot (innefattar blockage av tjänster) [13].

Bluetoothapplikationer kategoriseras och beskrivs av så kallade *profiler*. Det finns både mer generella, övergripande profiler som utnyttjas av många andra profiler som har en specifik tillämpning. En sådan profil är *The Generic Acecss Profile* (GAP) som bland annat beskriver proceduren vid upprättande av en anslutning mellan två enheter. Denna profil definerar även de olika fundamentala säkerhetsprocedurerna som en Bluetoothenhet har.

Det finns tre stycken säkerhetslägen som en Bluetoothenhet kan befinna sig i och dessa innebär olika säkerhetsprocedurer [14].

- **Säkerhetsläge 1** - Detta är den lägsta säkerhetsnivån som en Bluetoothenhet kan befinna sig i och det innebär att enheten inte kräver något autentisering eller kryptering av Bluetoothlänken.
- **Säkerhetsläge 2** - Detta säkerhetsläge kräver inte heller någon kryptering eller autentisering vid upprättandet av basbandsanslutning utan säkerhet krävs vid upprättandet av kanal.
- **Säkerhetsläge 3** - Det läge med högst säkerhetsnivån av de tre. Vid detta säkerhetsläge krävs det att säkerhetsprocedurer påbörjas innan basbandsanslutningen är avslutad. Detta kan göras i två varianter:
  - **Säkerhetsläge 3a** - Autentisering begärs alltid
  - **Säkerhetsläge 3b** - Autentisering och kryptering begärs alltid

Genom *pairingproceduren* upprättas ett förtroende mellan enheter. Pairing har som syfte att skapa en gemensam, *delad hemlighet* som kallas *länknyckel*. En delad hemlighet är, inom kryptografi, en bit data som endast är känd för de inblandade parterna; I detta fall är denna delade hemlighet en nyckel som är unik för varje anslutning. En länknyckel associeras med en enhetsadress (unik för varje enhet).

Förutom länknyckeln finns fyra ytterligare nycklar varav en av dessa är den PIN (Personal Identification Number) som är vanlig att man som användare får ange manuellt. Dessa nycklar genereras ur varandra och ur enhetens unika adress.

Förutom pairingproceduren används också en autentiserings- och krypteringsprocess. Detta görs genom att en av enheterna skickar en slumpad siffra till den andra enheten som tillsammans med länknyckeln tar fram ett ”korrekt” värde. Detta är dock endast en envägsautentisering och för att båda enheterna ska få likvärdigt förtroende för varandra måste detta göras från båda enheterna. Under denna autentisering genereras en såkallad *Autentiseringskrypteringsoffset* (ACO). Denna ACO används sedan, tillsammans med en bit av länknyckeln och ett slumpat värde, för att generera en chiffreringsnyckel [15].

3.6 ZigBee

ZigBee är en kommunikationsstandard som är oerhört energisnål men den klarar inte så höga datahastigheter. Detta gör att ZigBee är en populär kommunikationsstandard vid sensorövervakning och dylikt. Tack vare dess låga strömkonsumtion kan enheter som använder sig av ZigBee klara sig mycket länge på en begränsad mängd ström vilket (tillsammans med fler faktorer) möjliggör stora antal enheter med en totalt, förhållandevis, låg strömkonsumtion [16].

En speciell kategori av WPAN defineras av IEEE 802.15.4, nämligen: LR-WPAN (Low-Rate Wireless Personal Area Network). Fördelen LR-WPAN är att det är en mycket stabil överföring, kostar lite och är enkel att implementera. ZigBee använder sig av tre stycken frekvensband:

- 2.4 GHz-bandet - 16 kanaler
- 915 MHz-bandet - 10 kanaler
- 868 MHz-bandet - 1 kanal

ZigBee har en räckvidd på 10-100 m beroende på miljöfaktorer och hur mycket ström som appliceras. Flera ZigBee-enheter bildar ett meshnätverk vilket erbjuder möjligheten att transportera data via närliggande enheter för att nå mer avlägsna enheter.

3.6.1 Kanaldefinition och överföring

Vid överförning via ZigBee används en metod som kallas Direct Sequence Spread Spectrum (DSSS). DSSS används för att undvika störningar och liknande. Det som sker när DSSS används är att signalen som ska skickas multipliceras med en ”brussignal” som har mycket högre frekvens än originalsignalen. Brussignalen är en pseudoslumpad sekvens av +-1. Mottagaren behöver då endast använda samma sekvens av +-1 för att få tillbaka ursprungssignalen [17].

Det är mycket tack vare DSSS som ZigBee blir en såpass stabil signal eftersom anslutningen är stabilare mot blockage, kan dela kanal och minskar bakrundsbrus.

Kommunikation på de olika banden moduleras dock på olika sätt. 2.4GHz-bandet moduleras med Offset Quatrature Phase Shift Keying (O-QPSK) medan de andra två banden, 915 och 868 MHz, moduleras med Binary Phase Shift Keying (BPSK) [17]. Båda dessa moduleringar använder sig av fasskiftning, vilket man kan förstå från namnet. BPSK använder sig endast av två faser som är separerade med 180° och är den enklaste av de två moduleringsmetoderna. Detta gör BPSK till en långsammare överföring men mycket tåligare mot brus eftersom den endast kan modulera 1 bit/symbol (p.g.a. moduleringen med 180° separerade faser). En symbol är den information som varje fas ”bär” på och symbolen avkodas till ett visst antal bitar.

O-QPSK är, i likhet med BPSK, fasskiftning. I fallet med O-QPSK används dock fyra faser och därmed kan 2 bit/symbol moduleras. Skillnaden mellan O-QPSK och QPSK är hur mycket fasen är skiftad vid en viss tidpunkt - QPSK (utan offset) är skiftad 90° och

O-QPSK är skiftad 180°. Demodulerare och modulerare för att realisera O-QPSK är dock mer komplexa men O-QPSK/QPSK är ändå den vanligaste och tillämpas i större utsträckning än BPSK.

3.6.2 Säkerhet

ZigBee använder sig av krypteringsnycklar som är 128-bitar långa och den krypteringsstandarden som tillämpas är AES (Advanced Encryption Standard). Data kan skyddas av kryptering både inom nätverket (en gemensam nätverksnyckel) och för kommunikation mellan par av enheter (en länknyckel som skyddar den interna kommunikationen i nätverket).

Det är med dessa nycklar som enheter autentiserar varandra och detta minskar risken för lyckade attacker inifrån nätverket och utifrån. Detta gör kommunikationen säker i sig så länge som nycklarna genererats på ett säkert sätt.

En masternyckel används för att generera länknyckeln. Denna masternyckel kan komma till på ett flertal sätt. Antingen genom fabriksinställning av masternyckeln eller genom att den skickas utanför bandet eller från ett så kallat trust center (TC). Detta TC är en enhet som alla andra enheter i nätverket litar på. Man kan genom detta TC ändra länk- och nätverksnycklar. TC har två olika säkerhetslägen beroende på nätverkets tillämpning.

- **Kommersiellt läge** - Alla enhetsnycklar, masternycklar och nätverksnycklar underhålls av TC vilket möjliggör uppdateringar av nycklar och en centraliserad kontroll av nätverket.
- **Förtroende läge** - Endast alla masternycklar och nätverksnycklar underhålls av TC vilket ställer mindre krav på TC.

3.7 Wi-Fi

Wi-Fi är en WLAN-teknologi som baseras på radiosignaler nätverkande med hjälp av radioband på UHF (2.4 GHz) och SHF (5 GHz). Tekniken har sina rötter i sent 80-tal men IEEE-standarden (IEEE 802.11) togs fram först 1997 och namnet uppkom först 1999. IEEE-standarden har tilldelat Wi-Fi flera frekvensband och Wi-Fi-tekniken bygger på att dela upp informationen i bitar och dela upp dem på olika frekvenser. På detta sätt blir överföringen inte lika krävande och flera enheter kan använda samma Wi-Fi-sändare. Detta innebär även ekonomiska fördelar - att ha en unik sändare och mottagare för varje enhet hade blivit dyrare. Man måste däremot investera i en basstation [18].

Eftersom att signalen kan färdas genom väggar och att flera användare kan använda samma Wi-Fi-sändare är det populärt att använda Wi-Fi som WLAN i hemmamiljöer för att koppla ihop diverse enheter - mobiltelefoner, tablets, laptops och PC utan sladdar. Wi-Fi-sändaren kallas router och är det centrala i Wi-Fi. Om man kopplar ihop denna basstation med internet kommer även alla användare ut på internet. Det är numera vanligt att det finns så kallade hot spots på allmäna platser - områden där Wi-Fi-enheter kan koppla upp mot internet, ofta kostnadsfritt [18]. Det bör tilläggas att Wi-Fi är ökänt för sin

energiförbrukning. Om man jämför med Bluetooth använder Wi-Fi 80 mW för att skicka 75 bytes/sekund och Bluetooth använder 2 mW för samma överföring, cirka 3 % av den totala förbrukningen för Wi-Fi [19].

3.7.1 Säkerhet och kryptering

Sedan Wi-Fi lanserades har många krypteringssätt lanserats och knäckts.

Wired equivalent privacy (WEP) var det första krypteringsprotokollet som lanserades under Wi-Fi standarden 802.11. Som namnet antyder skulle det kryptera trafiken så användaren blev lika säker som via trådad uppkoppling. Tekniken visade sig snabbt innehålla stora säkerhetsbrister. Om en angripare avlyssnar paket kan man dekryptera nyckeln inom loppet av timmar [20] men rekorden ligger i minutklassen [21].

För att ersätta WEP utvecklades Wi-Fi Protected Access (WPA). Den hade en mer sofistikerad kryptering men tvingade inte användarna att byta hårdvara. Lösningen var dock inte långvarig - det konstaterades att man kunde avlyssna trafiken och hitta krypteringsnyckeln med hjälp av en dictionary-attack, där man testar ett stort antal ord från exempelvis en ordbok. För att möta framtida säkerhetshot lanserades år 2000 WPA2 och idag anses standarden fortfarande vara väldigt kraftig, mycket tack vare den kraftiga krypteringsmetoden AES. Det är en väldigt väldokumenterad och vältestad kryptering som används internationellt [22].

Wi-Fi Protected Setup (WPS) lanserades 2007 [23] av Wi-Fi Alliance som ett frivilligt certifieringsprogram. Det var tänkt att underlätta konfigurationen av säkerheten för Wi-Fi-nätverk i hemmiljö. WPS användes och var obligatoriskt hos nästan samtliga routertillverkare[23]. För att göra det enkelt för ovana användare använde WPS enkla metoder som att fylla i en PIN-kod [24]. Det var just PIN-koden som visade sig vara problematisk för säkerheten i systemet, vilket uppmärksammades i december 2011 av Stefan Viehböck[25]. Ett av autentiseringsstegen krävde ingen form av autentisering vilket gjorde den känslig för brute-force-attacker. Vidare var svaret från servern uppdelat - vilket gjorde att angriparen kunde se vilken del av PIN-koden som var korrekt. Detta reducerade antalet försök som behövdes innan koden knäcktes från 10^8 försök till $20 \cdot 10^3$. Vidare var den sista biten i PIN-koden en kontrollbit vilket minskade antalet försök som krävdes till $11 \cdot 10^3$. [23] I brist av en lösning på problemet uppmanades kort därefter allmänheten att stänga av WPS-funktionen på sina routrar, om den möjligheten fanns. [25]

4 Jämförelser

I detta avsnitt analyseras först kommunikationsmetoderna individuellt. Därefter jämförs de med avseende på säkerhet, kostnad och lämplighet för projektet.

4.1 Analys av Bluetooth

Införandet av Bluetooth syftade till att eliminera behovet av kablar och sladdar vid kommunikation över kortare avstånd. Detta syfte uppfylls mycket tack vare det faktum att

Bluetooth är ett mycket energieffektivt och relativt stabilt trådlöst kommunikationsprotokoll. Säkerhetsnivån för enheter som använder Bluetooth för att kommunicera med omvärlden är dock relativt låg.

PIN-koden är den enda säkerhetskoden som inte överförs trådlöst och denna kod är ofta runt 4 siffror lång vilket gör den relativt lätt att ta sig förbi. När man sedan tagit sig förbi den är det möjligt att söka sig till en härledning av säkerhetsnycklarna. Den kryptering (E0) som Bluetooth använder sig av för att skydda informationen anses inte heller vara speciellt stark. Bluetooth SIG (Special Interest Group) har fått kritik för att den standardiserade säkerheten är låg och att det ofta inte finns stöd för högre nivåer av säkerhet.

Det faktum att två enheter som anslutits en gång använder samma länknyckel vid fortsatt kommunikation gör att om denna nyckel har blivit känd för en främmande enhet kan denna avlyssna framtida kommunikation utan några svårigheter alls.

En ytterligare fördel med Bluetoothenheter är dess obundenhet. Inget krav på yttre nät eller dylikt finns tack vare Piconett/Scatternet-topologin.

Sammanfattningsvis så erbjuder Bluetooth dock relativt hög säkerhet för praktiskt taget ingen ansträngning. Dessutom är signalen ganska störningssäker tack vare dess frekvenshoppning och kräver lite hårdvara (ingen basstation eller dylikt behövs). Detta gör Bluetooth perfekt för mindre trådlösa enheter som mobilitet är en viktig faktor för. Den låga energiförbrukningen gör det till ett än mer tacksamt kommunikationsprotokoll för små, batteridrivna enheter och enheter som kommunicerar i en kontrollerad miljö och inte över jättestora avstånd.

4.2 Analys av ZigBee

ZigBee är en kommunikationsstandard som lämpar sig väl för överföringar av mindre mängder data under lång tid över stora nätverk. Detta på grund av dess väldigt låga energiförbrukning, dess låga dataöverföringskapacitet samt att ett nät av ZigBee-enheter kan vara upp till 65 000 enheter stort.

Fördelarna med ZigBee märks främst vid användning av mycket stora nätverk av enheter som kräver en mindre mängd dataöverföring. Detta för att överföringen då är mycket stabil, relativt säker och strömsnål. Det faktum att all säkerhet kan kontrolleras från ett trust center gör att byte av säkerhetsnycklar kan göras beroende på hur känslig man anser informationen vara.

En nackdel, förutom låg dataöverföringskapacitet, är att det krävs tre typer av enheter i ett ZigBee-nätverk: Koordinator, Router och slutpunkt. Detta gör att större krav ställs på omgivande faktorer och peer-to-peer-överföring mellan endast två enheter kräver extra hårdvara utöver de två.

4.3 Analys av Wi-Fi

Mycket av den trådlösa kommunikationen i hemmet kan tillskrivas WLAN och Wi-Fi. Att många olika enheter kan använda samma router har gjort WLAN enkelt och billigt för

hushållet. Det har även kopplat upp alla enheter till internet och har därigenom bidragit kraftigt till internetrevolutionen.

Säkerheten hos Wi-Fi är väldigt beroende på vilken standard som används i enheterna. Om man använder en gammal standard som WEP kan man inte garantera säkerheten men om man använder en mer sofistikerad standard som WPA eller ännu hellre WPA2 är det säkrare. Man får däremot se till att WPS inte är påslagen. Det är även viktigt att använda ett kraftfullt lösenord som inte är känsligt för vare sig DoS-, DDoS- eller dictionary-attacker.

För att använda Wi-Fi måste man använda en router som basstation vilket kan vara problematiskt om man bara vill skicka information mellan två enheter. Det gör däremot att räckvidden hos Wi-Fi är ganska lång och ofta täcker in hela hushållet.

Sammanfattningsvis är Wi-Fi en välanvänd, säker metod med god räckvidd. Det kräver dock konfiguration och ett bra lösenord för att få god säkerhet. Vidare kräver Wi-Fi en basstation och är förödande för strömförbrukningen.

5 Sammanfattning

I denna studie har tre vanliga kommunikationsstandarder utvärderats och analyserats och man kan konstatera att lämpligheten för standarderna är olika. För- och nackdelarna för de olika kommunikationsmetoderna visualiseras i figur 3.

	Bluetooth	Wi-Fi	Zigbee
Säkerhet	Medel	Hög	Medel
Kostnad	Låg	Medel	Medel
Lämplighet	Hög	Låg	Låg

Figur 3: *Jämförelse av kommunikationsmetoder*

Wi-Fi är en mycket kraftfull kommunikationsmetod. Säkerheten och räckvidden är högre än hos Bluetooth, men kravet av basstation och den höga energiförbrukningen gör den ointressant för ändamålet.

ZigBee har en låg energikonsumtion, precis som BlueTooth, men kräver tyvärr en basstation.

Bluetooth förefaller mest lämplig för ändamålet. Den låga energikonsumtionen är viktig för roboten, som har begränsad batterikapacitet och batteri laddningen tar lång tid. Den enkla konfigurationen är bekväm för användaren och säkerheten är inte den viktigaste prioriteten.

Bluetooth är den mest lämpliga kommunikationsmetoden för projektet.

Referenser

[1] ISY. (Hämtad 2015-04-27). Tsea56, URL: http://www.isy.liu.se/edu/kurs/TSEA56/.

[2] J.-S. Lee, Y.-W. Su och C.-C. Shen, "A comparative study of wireless protocols: Bluetooth, uwb, zigbee, and wi-fi", i *Industrial Electronics Society, 2007. IECON 2007. 33rd Annual Conference of the IEEE*, nov. 2007, s. 46–51. DOI: 10.1109/IECON.2007.4460126.

[3] E. B. editors. (Hämtad 2015-03-04). Encyclopædia britannica modulering, URL: http://global.britannica.com/EBchecked/topic/387402/modulation.

[4] ——, (Hämtad 2015-03-04). Encyclopædia britannica mikrovågor, URL: http://global.britannica.com/EBchecked/topic/380750/microwave.

[5] ——, (Hämtad 2015-03-05). Encyclopedia britannica antenn, URL: http://global.britannica.com/EBchecked/topic/27190/antenna.

[6] J. Mirkovic och P. Reiher, "A taxonomy of ddos attack and ddos defense mechanisms", *ACM SIGCOMM Computer Communication Review*, vol. 34, nr 2, s. 39–53, 2004.

[7] E. B. editors. (Hämtad 2015-03-31). Data encryption, URL: http://global.britannica.com/EBchecked/topic/152175/data-encryption.

[8] ——, (Hämtad 2015-04-01). Des, URL: http://global.britannica.com/EBchecked/topic/152178/Data-Encryption-Standard-DES.

[9] ——, (Hämtad 2015-04-01). Aes, URL: http://global.britannica.com/EBchecked/topic/930236/AES.

[10] ——, (Hämtad 2015-03-04). Encyclopædia britannica bluetooth, URL: www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/bluetooth.

[11] K. Grahm. (Hämtad 2015-03-04). Nationalencyklopedin bluetooth, URL: www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/bluetooth.

[12] J. Haartsen, "Bluetooth-the universal radio interface for ad hoc, wireless connectivity", *Ericsson review*, vol. 3, nr 1, s. 110–117, 1998.

[13] C. Gehrmann, J. Persson och B. Smeets, *Bluetooth security*. Artech house, 2004.

[14] I. Bluetooth SIG. (Hämtad 2015-03-25). Baseband architecture, URL: https://developer.bluetooth.org/TechnologyOverview/Pages/Baseband.aspx.

[15] C. Gehrmann och K. Nyberg, "Enhancements to bluetooth baseband security", i *Proceedings of Nordsec*, vol. 2001, 2001, s. 191–230.

[16] P. Kinney m. fl., "Zigbee technology: Wireless control that simply works", i *Communications design conference*, vol. 2, 2003, s. 1–7.

[17] P. Baronti, P. Pillai, V. W. Chook, S. Chessa, A. Gotta och Y. F. Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and zigbee standards", *Computer communications*, vol. 30, nr 7, s. 1655–1695, 2007.

[18] E. B. editors. (Hämtad 2015-03-04). Encyclopedia britannica wi-fi, URL: http://global.britannica.com/EBchecked/topic/1473553/Wi-Fi.

[19] E. Vogler. (Hämtad 2015-04-01). Bluetooth vs. wi-fi power consumption, URL: http://science.opposingviews.com/bluetooth-vs-wifi-power-consumption-17630.html.

[20] H. Luo. (Hämtad 2015-04-01). Wep, URL: http://www.accessscience.com.e.bibl.liu.se/content/wireless-fidelity-wi-fi/802040.

[21] P. Sayer. (Hämtad 2015-04-01). Crack wep, URL: http://www.techworld.com/news/security/researchers-crack-wep-wifi-security-in-record-time-8456/.

[22] M. M. S. D. Arash Habibi Lashkari, "A survey on wireless security protocols (wep, wpa and wpa2/802.11i)", i *Computer Science and Information Technology, 2009. ICCSIT 2009.*, aug. 2009, s. 48–52. DOI: 10.1109/ICCSIT.2009.5234856.

[23] S. Viehböck. (Hämtad 2015-03-31). Wps hacking, URL: https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf.

[24] W.-F. Alliance. (Hämtad 2015-03-31). Wps, URL: http://www.wi-fi.org/discover-wi-fi/wi-fi-protected-setup.

[25] J. Allar. (Hämtad 2015-03-31). Disable wps, URL: http://www.kb.cert.org/vuls/id/723755.