TDDC03 Projects, Spring 2004

Wardriving i Linköping

Christofer Wallén
Anders Haglund

Supervisor: David Byers

Wardriving i Linköping

Anders Haglund
Christofer Wallén
Linköpings Universitet
{andha859, chrwa535}@student.liu.se

Sammanfattning

Denna rapport är skriven för kursen TDDC03, informationssäkerhet, vid Linköpings Universitet. Rapporten behandlar trådlösa nätverk i Linköping och innefattar följande områden. Juridiska aspekter på wardriving, insamlandet av data, analys, presentation av data samt slutsatser och resultat.

1. Inledning

Att installera en ny trådlös anslutning är en enkel process, varvid allt fler använder trådlös kommunikation. Tyvärr innebär detta ökade säkerhetsrisker eftersom de flesta inte känner till de inställningar i anslutningen som behövs för att göra den säker, om det går att göra den tillräckligt säker? Säkerhetsexperternas uppfattning är att trådlösa nätverk ofta utgör ett stort hot mot den övriga datasäkerheten hos företag och privatpersoner. Den här rapporten försöker ta reda på i vilken utsträckning användare av trådlösa nätverk känner till de säkerhetshot som uppkommer med trådlös kommunikation.

2. Syfte och målgrupp

Syftet med denna rapport är att genomföra en kartläggning av 802.11b nätverk inom Linköpings Y-ring (och Mjärdevi) samt att undersöka vilken säkerhet de använder. Vidare kommer vi att beskriva den utrustning och arbetsmetodik vi använt oss av. Juridiska aspekter kommer tas upp från olika intressenters perspektiv, alltså vad de anser om Wardriving laglighet.

Målgruppen för rapporten är personer inom det datavetenskapliga området med inriktning mot säkerhet och trådlösa.

3. Problemformulering

Projektet omfattar en kartläggning av 802.11b nätverk inom Linköpings Y-ring (även Mjärdevi). Kartläggningen utfördes med hjälp av en bärbar dator med nätverkskort för 802.11b och en GPS-mottagare som kommunicerar med Kismet som i sin tur sparar den inhämtat information i en MySQL databas.

4. Frågeställning

Den rapporten utgår från flera frågeställningar och dessa är:

- I vilken utsträckning används WEP/WPA kryptering?
- I vilken utsträckning har standardkanaler ändrats?
- I vilken utsträckning används har standard SSID ändrats?
- Finns det signifikanta skillnader mellan olika områdens inställningar med avseende på säkerhet? (Jämför teknikområde med bostadsområde)
- Vilken är skillnaden mellan att använda en extern antenn eller ingen extern antenn i avseende på hur många nät som hittas och går det se någon signifikant skillnad av säkerhet och nätverk från tidigare år?
- Finns det skillnader i inställning till hur lagligt wardriving är mellan universitet, polis/åklagare och företag.

5. Utrustning

Följande utrustning användes:

- Dator: Dell Latitude CPi D266XT
- Nätverkskort:
- Extern antenn
- GPS-mottagre: GM48 RS 232/PS 2
- Mjukvara: Debian, Kismet, GPSDrive, GPSD

6. Arbetsmetodik

Vi genomförde körningarna under tre dagar då olika områden inom Linköpings Y-ring täcktes in. När körningarna var avklarade började vi med att analysera all inhämtad data och sortera informationen för att det skulle vara lätt att arbeta vidare med.

Informationen som sparades var adresser och informationen som accesspunkterna sänder ut för att kunna lokalisera dem, s.k. BEACON-paket. Ingen datatrafik har avlyssnats, sparats eller använts för denna rapport.

Parallellt med körningarna genomfördes intervjuer med berörda parter i avsikt att insamla kunskap om de juridiska aspekterna i rapporten.

7. Juridiska aspekter

De juridiska aspekterna var det första vi började utreda då inget fall av trådlös avlyssning än ägt rum i Sverige som lett till åtal. Nedan följer en redovisning av olika synvinklar på lagligheten i wardriving som är den tekniska termen för trådlös avlyssning medelst bil och bärbar dator.

7.1 Polisen synvinkel

Vi var i kontakt polisens IT-enhet och de menade att syftet med avlyssningen var det centrala. Om det finns uppsåt att använda informationen som inhämtas för att exempelvis göra intrång så är det olagligt men det är lagligt att lyssna på etern. Vidare får inte informationen föras vidare, och därmed hamnar täckningskartor och annan kartläggning i gränszonen för vad som är lagligt. Vid avlyssning på etern får den endast utföras i passivt läge, alltså är ändring av informationen olagligt.

Sammanfattningsvis är syftet det centrala. Syftet avgör om det är lagligt eller inte, men det kan vara svårt att bevisa att det inte finns ont uppsåt då samma utrustning som används för wardriving även kan användas för intrång.

7.2 Åklagares/domares synvinkel

Åklagare och domare hade ingen insikt i problematiken kring laglighet med wardriving och visste inget konkret fall då detta har prövats. De ansåg dock att detta är en situation som lagstiftaren inte har tänkt på vilket gör att det blir fråga om lagtolkning. Att lagen inte explicit anger trådlös avlyssning som förbjuden innebär dock inte att det är lagligt.

7.3 Skolans synvinkel

Om hänvisning till radiolagen görs menas att trådlösa nätverk är radiosändning rent tekniskt och då är avlyssning tillåten om inte spridning eller förändring av informationen sker, men det är inte etiskt riktigt.

(För skolans synvinkel har vi varit i kontakt med David Bayers och Viiveke Fåk)

7.4 Företags synvinkel

Företagen ser sina trådlösa nätverk som interna nät och ser därför avlyssning som intrång. Ur deras perspektiv är detta naturligt, men ytterst tveksamt eftersom de använder etern och radiosändning. Det företag vi har varit i kontakt med menade att varje uppmärksammat försök till avlyssning av deras nätverk skulle leda till en anmälan från deras sida.

8. Sammanställning av insamlad data

Kapitlet redovisar en sammanställning av det data som samlats in. För att underlätta beräkningar i kapitel 9 har informationen delats in i olika grupper.

De olika grupperna är:

- Gruppen Mjärdevi representerar de nätverk som geologiskt placerade sig inom teknikringen och i viss mån runt Linköpings Universitet. Den tekniska kompetensen hos populationen är hög.
- Gruppen Ryd representerar de nätverk som geologiskt placerade sig runt stadsdelen Ryd. Den tekniska kompetensen hos populationen är medel.
- Gruppen Centrum representerar de nätverk som geologiskt placerade sig i resten av Linköping. Den tekniska kompetensen hos populationen är låg.

Indelningen har gjorts av oss själva med hjälp av följande resonemang. Mjärdevigruppen innehåller teknikföretag som har anställda utbildade i säkerhetsfrågor och därför har en hög teknisk kompetens. Centrumgruppen innehåller en blandning mellan privatpersoner och företag utan särskild utbildning i säkerhetsfrågor varvid denna grupp har låg teknisk kompetens. Rydsgruppen innehåller uteslutande privatpersoner och studenter. Skillnaden mellan Ryd och Centrum är populationen av studenter som vi anser har högre teknisk kompetens än andra privatpersoner. Rydsgruppen ger vi därför

högre teknisk kompetens än Centrumgruppen men lägre än Mjärdevigruppen.

Typen av nätverk delas in i följande kategorier av Kismet: infrastructure (BSS), ad-hoc (IBSS), probe, unknown, och turbocell. I nätverk av typen infrastructure sker all kommunikation via en eller flera accesspunkter medan i nätverk av typen ad-hoc sker kommunikationen direkt mellan klienterna, alltså ”peer-to-peer”. I nätverk av typen probe så är det datorer som söker efter nätverk. Nätverk av typen turbocell är ett alternativt protokoll för trådlösa nätverk och skiljer sig från 802.11b standarden. Vad som skiljer ligger utanför denna rapports omfång men kortfattat använder sig inte turbocell av infrastructure och ad-hoc utan har två alternativa sätt och sägs vara mer säkert [2].

Nätverk av typen Unknown är de som Kismet inte kunde identifiera vilken typ de tillhörde och de sätts av Kismet automatiskt till kanal 0. [1]

Nedan har vi sammanställt en tabell över totalt antal funna nätverk, typ och om de använder WEP eller inte.

Totalt antal accesspunkter	WEP		Type				
	True	false	Infrastructure	Probe	Unknown	ad-hoc	Turbocell
826	311	515	660	130	19	14	3

Tabell 1: Sammanställning av totalt antal nätverk funna, antalet med WEP kryptering aktiverat eller inte samt vilken typ av nätverk.

8.2 Grafisk presentation av nätverk i Linköping

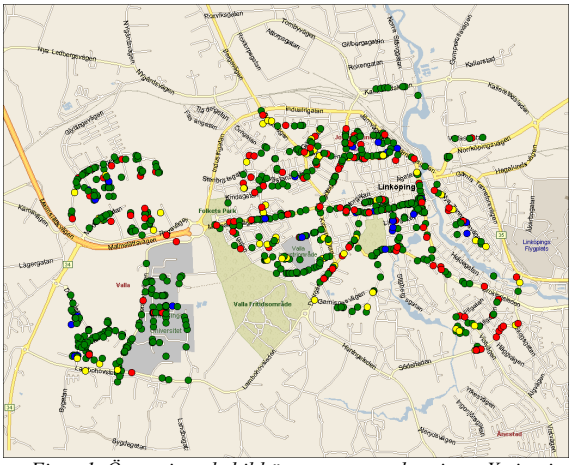
Nedan presenteras fyra kartor med tillhörande tre diagram vardera. Kartorna (figur 1, 5, 9 och 13) innehåller en övergripande karta över Linköping samt mer ingående kartor över Mjärdevi, Ryd och centrum. Varje cirkel på kartorna representerar en accesspunkt och de olika färgerna representerar olika typer av konfigurationer av varje accesspunkt.

- Grön innebär att standard SSID har ändrats.
- Gul innebär att standard SSID används men WEP-kryptering har aktiverats eller att standardkanalen är ändrad.
- Blå innebär att standard SSID använts och att WEP-kryptering inte aktiverats men att standardkanalen ändrats.
- Röd innebär att varken standard SSID ändrats, WEP-kryptering inte aktiverats och standardkanalen använts.

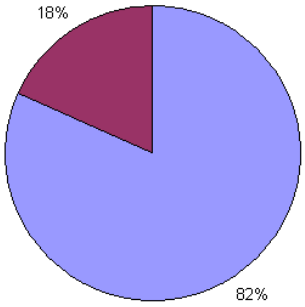
Gröna punkter är de säkraste accesspunkterna medan röda är de som inte ändrat något från grundinställningarna. För större versioner av kartorna se appendix A.

För varje karta finns diagram över typ av nätverk, SSID användning samt om WEP-kryptering används.

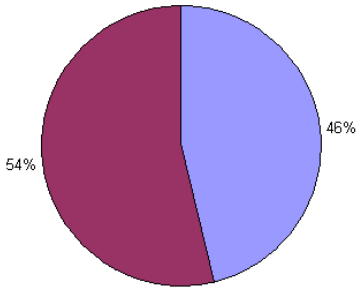
Typ av nätverk delas in i infrastructure/ad-hoc och övriga. I gruppen övriga ingår probe, unknown samt turbocell.



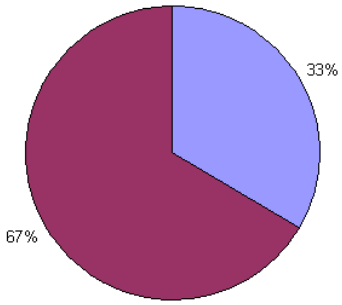
Figur 1. Övergripande bild över accesspunkter inom Y-ring i Linköping.



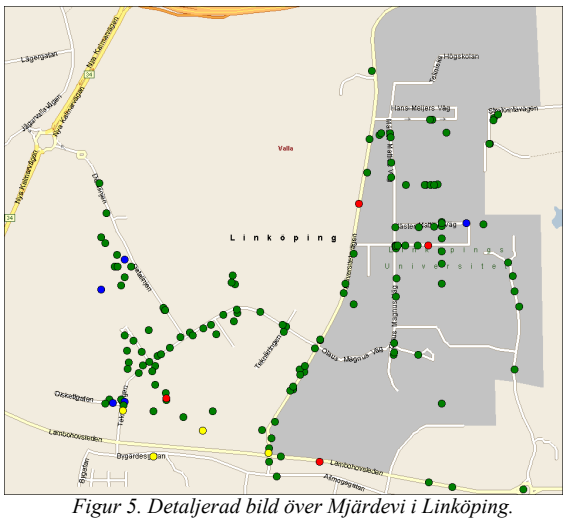
Figur 2. Fördelningen av nätverk av typen ad-hoc/infrastructure (blå) och övriga typer av nätverk (röd) inom Linköping.



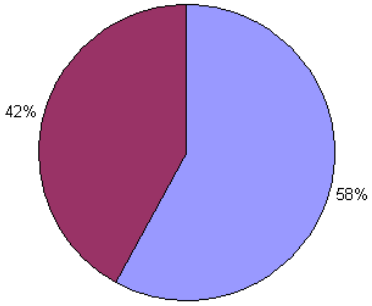
Figur 3. Fördelningen av hur många accesspunkter som har WEP på (blå) respektive av (röd) inom Linköping.



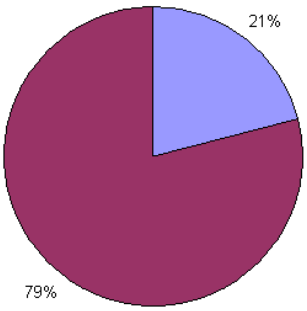
Figur 4. Fördelningen av hur många som har ändrat standard SSID (röd) respektive inte ändrat SSID (blå) inom Linköping.



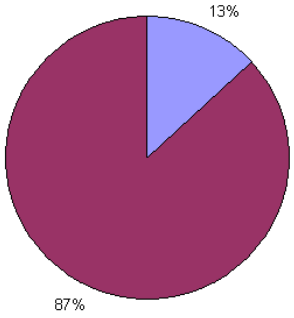
Figur 5. Detaljerad bild över Mjärdevi i Linköping.



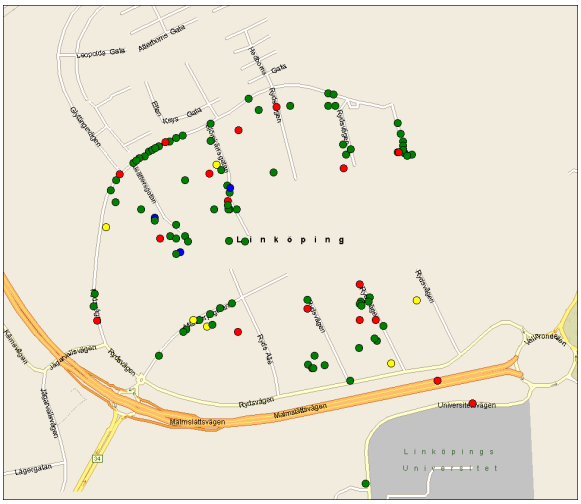
Figur 6. Fördelningen av nätverk av typen ad-hoc/infrastructure (blå) och övriga typer av nätverk (röd) inom Mjärdevi.



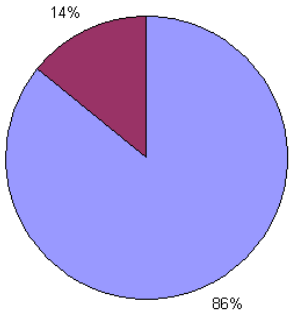
Figur 7. Fördelningen av hur många accesspunkter som har WEP på (blå) respektive av (röd) i Mjärdevi.



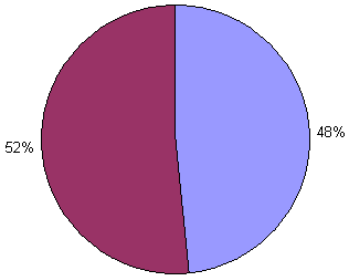
Figur 8. Fördelningen av hur många som har ändrat standard SSID (röd) respektive inte ändrat SSID (blå) i Mjärdevi.



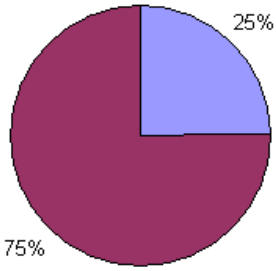
Figur 9. Detaljerad bild över Ryd i Linköping.



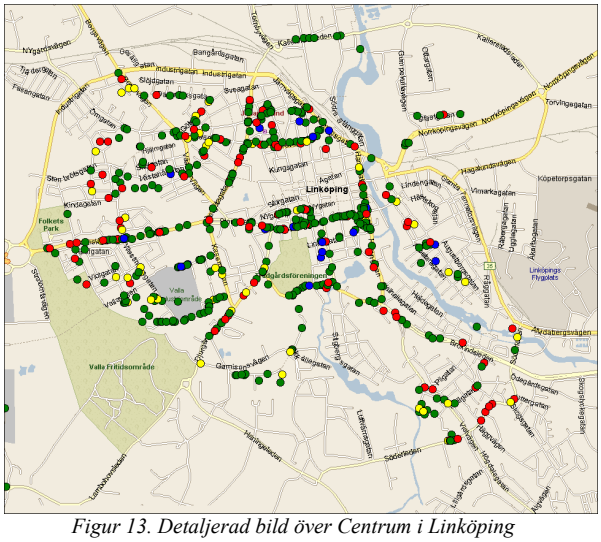
Figur 10. Fördelningen av nätverk av typen ad-hoc/infrastructure (blå) och övriga typer av nätverk (röd) inom Ryd.



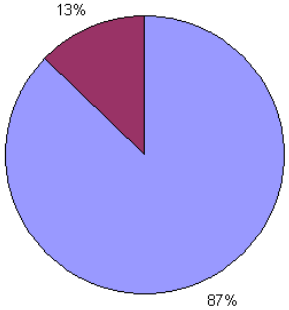
Figur 11. Fördelningen av hur många accesspunkter som har WEP på (blå) respektive av (röd) inom Ryd.



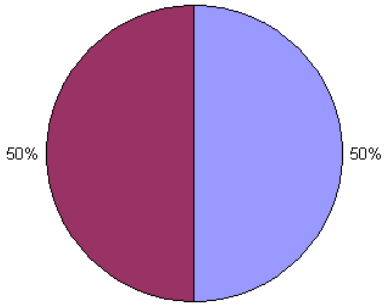
Figur 12. Fördelningen av hur många som har ändrat standard SSID (röd) respektive inte ändrat SSID (blå) i Ryd.



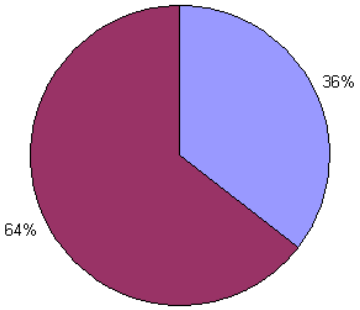
Figur 13. Detaljerad bild över Centrum i Linköping



Figur 14 Fördelningen av nätverk av typen ad-hoc/infrastructure (blå) och övriga typer av nätverk (röd) i Centrum.



Figur 15. Fördelningen av hur många accesspunkter som har WEP på (blå) respektive av (röd) inom Centrum.



Figur 16. Fördelningen av hur många som har ändrat standard SSID (röd) respektive inte ändrat SSID (blå) i Centrum.

Typen av nätverk skiljer sig mellan gruppen Mjärdevi och de två andra, se figur 6,10 och 14. I Mjärdevi fanns en betydligt större del av övriga nätverkstyper än i de båda andra grupperna. Anledningen till att det skiljer sig kan bero på att det är uteslutande företag i Mjärdevigruppen och dessa använder andra nätverkstyper medan vanliga privatpersoner använder infrastructure och ad-hoc. Värt att nämna är att ad-hoc endast utgör en liten del jämfört med infrastructure hos samtliga grupper.

Vad gäller WEP-kryptering så skiljer sig även här Mjärdevigruppen från de båda övriga då ~21 % använder WEP-kryptering jämfört med ~50 % hos de båda övriga grupperna, se figur 7, 11 och 15. Resultatet var inte förväntat då vi först trodde det skulle vara tvärtom, men det kan förklaras med att företagen använder andra säkerhetsmekanismer än WEP-kryptering. Dessa mekanismer kan vara mer avancerade och dyrare vilket resulterar i att privatpersoner inte använder dessa. Det vore konstigt om teknikföretagen skulle ha sämre säkerhet än vanliga hemnätverk, som är konfigurerade av personer med lägre grad av säkerhetstänkande och kompetens.

Det finns inga markanta skillnader mellan de olika grupperna i avseende på användning av standard SSID och det går därför inte att dra några direkta slutsatser, se figur 8, 12 och 16. De som ändrat SSID i störst utsträckning är Mjärdevigruppen vilket skulle

kunna tyda på att säkerhetstänkandet är bättre förankrat än hos de båda andra grupperna.

8.3 Kanalanvändning

802.11b delar upp frekvensspektrumet i 14 överlappande 22 MHz kanaler var. Olika kanaler är lagliga i olika länder och tre eller fyra kanaler kan användas samtidigt då flera accesspunkter används. I Europa finns 13 kanaler tillgängliga och tumregeln är att använda kanal 1,7 och 13 för upp till tre accesspunkter [3] [4]. Dessa har valts för att undvika så att inte intilliggande kanaler ska överlappa varandra [5].

För nätverk med bara en accesspunkt spelar det ingen större roll vilken kanal som väljs då ingen överlappning sker. En accesspunkt levereras från tillverkaren med en på förhand inställd kanal med rekommendationen att endast ändra kanalen om den kolliderar med ett närliggande nätverk. [7, 8, 9]

Tabell 2 nedan redovisar olika tillverkares standard SSID samt standard kanal som används.

Tillverkare	Standard SSID	Standardkanal
Intel, 3Com, Symbol	101	3
3Com	3Com	11
Apple	Airport Network	10
SMC, Dlink, Asus	Default	6
Linksys	Linksys	3, 6, 11
Netgear	NETGEAR	11
Linksys, Zyxel, Netgear	Wireless	1, 3, 6, 11
Dlink, Belkin, Canyon	WLAN	11

Tabell 2. Sammanställning av olika tillverkares standard SSID och standard kanal. [7, 8, 9, 10, 11]

I tabell 3 nedan finns en sammanställning över kanalanvändning för alla unika nätverk funna.

Kanal	Antal
0	168
1	88
2	18
3	30
4	9
5	6
6	244
7	30
8	10
9	12
10	26
11	170
12	3
13	12

Tabell 3. Sammanställning av alla unika nätverk med avseende på kanalanvändning.

Kanal 0, 1, 6 och 11 är de kanaler som används mest frekvent och detta beror på att tillverkarna levererar sina accesspunkter med förinställda standardkanaler. De kanaler som Kismet inte klarar identifiera sätts automatiskt till kanal 0. [11, 12]

8.4 Standard SSID

Tabell 4 nedan finns en sammanställning över användningen av standard SSID. Sammanlagt kunde vi identifiera 234 accesspunkter med standard SSID av totalt 826. Vi har i tabellen inte tagit hänsyn till typ av nätverk vilket resulterar i något fler antal accesspunkter med standard SSID än i tabell 5.

Standard SSID	Antal
101	11
3Com	30
Airport Network	1
Default	114
Homerun	7
Linksys	2
NETGEAR	27
Wireless	9
Wireless	26
WLAN	7

Tabell 4. Användning av standard SSID.

8.5 Hypotesprövning av signifikanta skillnader mellan områden i Linköping

En av rapportens huvudfrågeställningar var om det finns signifikanta skillnader mellan olika områdens inställning med avseende på säkerhet. Denna fråga kommer att besvaras av ett X^2-test på 99,95 % signifikansnivå. Samtliga formler är hämtade från ”Formelsamling i matematisk statistik”. [6]

I tabellerna som följer (tabell 5) visas utfallet av SSID, WEP och SSID broadcast från vår körning där datan består endast av unika nätverk av typen ad-hoc eller infrastructure.

Urvalsgrupp	Totalt antal	SSID	WEP	Broadcast
Mjärdevi	90	12	19	12
Ryd	97	24	47	9
Centrum	483	172	242	47

Tabell 5: Användning av SSID, WEP och SSID broadcast i de tre områdena

8.5.1 X^2-test av Mjärdevi, Ryd och Centrum

Hypotes:

H_0: De olika områdena har samma värden på de tre sannolikheterna.

H_1: H_0 är ej sann.

Om H_0 är sann så är sannolikheten:

P(SSID)	0,310448
P(WEP)	0,459701
P(Broadcast)	0,101493

Där sannolikheten för exempelvis SSID beräknas genom $\frac{\sum n_{SSID}}{\sum n_{totalt}}$ ur tabell 5 ovan.

De skattade förväntade frekvenserna blir då:

	SSID	WEP	Broadcast
Mjärdevi	27,9403	41,37313	9,134328
Ryd	30,11343	44,59104	9,844776
Centrum	149,9463	222,0358	49,0209

Där den skattade förväntade frekvensen beräknas genom $n_{totalt} p_i$.

Teststorheten $Q = \sum_i^k \frac{(N_i - n_{totalt} p_i)^2}{n_{totalt} p_i}$, där N_i är utfallet och $n_{totalt} p_i$ är de skattade förväntade frekvenserna.

Q 28,65751

Q är approximativt $X^2(5)$ om H_0 är sann d v s H_0 förkastas om Q>a. Tabell ger a=22.11 på nivån 99.95 % vilket ger att H_0 förkastas.

Det finns med mycket stor sannolikhet skillnader i säkerhetstänkande mellan olika områden i Linköping.

8.5.2 X^2-test av Mjärdevi och Ryd

Hypotes:

H_0: De olika områdena har samma värden på de tre sannolikheterna.

H_1: H_0 är ej sann.

Om H_0 är sann så är sannolikheten:

P(SSID)	0,192513
P(WEP)	0,352941
P(Broadcast)	0,112299

De skattade förväntade frekvenserna blir då:

	SSID	WEP	Broadcast
Mjärdevi	17,3262	31,76471	9,134328
Ryd	18,6738	34,23529	9,844776

Q 14.01687

Q är approximativt $X^2(2)$ om H_0 är sann d v s H_0 förkastas om Q>a. Tabell ger a=13,82 på nivån 99.90 % vilket ger att H_0 förkastas.

Det finns med mycket stor sannolikhet skillnader i säkerhetstänkande mellan Mjärdevi och Ryd.

8.5.3 X^2-test av Mjärdevi och Centrum

Hypotes:

H_0: De olika områdena har samma värden på de tre sannolikheterna.

H_1: H_0 är ej sann.

Om H_0 är sann så är sannolikheten:

P(SSID)	0,321117
P(WEP)	0,455497
P(Broadcast)	0,102967

De skattade förväntade frekvenserna blir då:

	SSID	WEP	Broadcast
Mjärdevi	28,90052	40,99476	9,267016
Centrum	155,0995	220,0052	49,73298

Q 26,68056

Q är approximativt $X^2(2)$ om H_0 är sann d v s H_0 förkastas om Q>a. Tabell ger a=15,20 på nivån 99.95 % vilket ger att H_0 förkastas.

Det finns med mycket stor sannolikhet skillnader i säkerhetstänkande mellan Mjärdevi och Centrum.

8.5.4 X^2-test av Ryd och Centrum

Hypotes:

H_0: De olika områdena har samma värden på de tre sannolikheterna.

H_1: H_0 är ej sann.

Om H_0 är sann så är sannolikheten:

P(SSID)	0,337931
P(WEP)	0,498276
P(Broadcast)	0,096552

De skattade förväntade frekvenserna blir då:

	SSID	WEP	Broadcast
Ryd	32,77931	48,33276	9,365517
Centrum	163,2207	240,6672	46,63448

Q 2,884853

Q är approximativt $X^2(2)$ om H_0 är sann d v s H_0 förkastas om Q<a. Tabell ger a=15,20 på nivån 99.95 % vilket ger att H_0 ej kan förkastas.

Det finns ingen anledning att tro att det finns skillnader i säkerhetstänkande mellan Ryd och Centrum.

9 Resultat

Kapitlet innehåller en sammanställning som svarar mot rapportens frågeställningar.

9.1 WEP/WPA-kryptering

För att analysera i hur stor utsträckning WPA-kryptering används skulle krävas att vi sparar undan data och analyserar ”headers” i datapaketen, eftersom inte Kismet känner av denna typ av information. Vi gjorde bedömningen att detta var tveksamt lagligt och genomförde aldrig denna typ av analys.

WEP-kryptering användes av ~46 % av accesspunkterna i Linköping (se avsnitt 8.2). Vi trodde från början att användningen av WEP-kryptering skulle vara låg. Vår teori var att de som hade låg grad av säkerhetstänkande inte skulle veta om att de behövde sätta på WEP-kryptering medan de med hög grad av säkerhetstänkande skulle använda sig av andra sorters mekanismer för säkerhet. Denna hypotes stämde till viss del överens med vårt resultat då endast ~21 % av Mjärdevigruppen använde WEP-kryptering men hela ~50 % av både Ryd- och Centrumgrupperna använde WEP-kryptering.

9.2 Standardkanaler

Ur avsnitt 8.3 framkommer att tillverkare av accesspunkter rekommenderar användning av förinställda kanaler. Rekommendationen från tillverkare är att endast ändra kanal om flera accesspunkter används och det sker kollision mellan deras kanalanvändande. Enligt tabell 2 används kanalerna 1, 3, 6, 10 och 11 som standard av tillverkare. Vi tycker att detta resultat stämmer bra överens med utfallet från vår körning där vi ur tabell 3 kan utläsa att ~80 % av accesspunkterna använder kanaler som används som standardkanaler av tillverkare. Det är dock svårt att avgöra om detta verkligen är standardkanaler eftersom vi inte kan identifiera tillverkare med hundraprocentig säkerhet.

9.3 Standard SSID

Ur avsnitt 8.4 framkommer att ~28 % använder standard SSID vilket är en ansenlig del särskilt då en av de första rekommendationerna är att ändra standard SSID. Om SSID ändras har vi sett att många ändrar till sitt namn eller företagsnamn vilket är tvärtemot tillverkarnas rekommendation.

9.4 Signifikanta skillnader mellan grupperna med avseende på säkerhet

Det går att påvisa signifikanta skillnader mellan de olika områdena Mjärdevi, Ryd och Centrum. Vidare går det att påvisa signifikanta skillnader mellan Mjärdevi och Ryd samt Mjärdevi och Centrum. Intressant att notera är att det inte går att påvisa signifikanta skillnader mellan Ryd och Centrum.

Slutsatsen blir alltså att Mjärdevi har en högre grad av säkerhetstänkande än Ryd och Centrum medan Ryd och Centrum har samma grad av säkerhetstänkande.

9.5 Skillnaden mellan att använda en extern antenn eller inte

Tanken var att vi skulle jämföra skillnaden i att genomföra en wardriving med en extern antenn och utan en extern antenn. Vi hann inte med att genomföra en körning utan extern antenn och utelämnar därför denna jämförelse. För den intresserade hänvisar vi till föregående års rapport, där endast körning utan antenn genomfördes. [12]

9.6 Skillnader i inställning till hur lagligt wardriving är mellan universitet, polis/åklagare/domare och företag

Utredningen av uppgiftens juridiska aspekter visade på att det råder förvirring i vilka regler som gäller för trådlösa nätverk. Det bästa svaret vi kunnat utröna är att detta faktiskt är ett fall där lagen inte hängt med i teknikutvecklingen men att det fortfarande är tillåtet att avlyssna trådlösa nätverk. Det är dock inte tillåtet att använda avlyssningen i syfte att göra intrång eller sprida information från avlyssningen vidare i syfte att underlätta intrång.

Vi poängterar att vår avlyssning endast skett i undervisningssyfte och att ingen information i den här rapporten ska kunna användas för att genomföra ett intrång. Därför kommer vi inte att publicera några koordinater eller namn på specifika nätverk eller liknande information.

10 Referenser

[1] http://www.kismetwireless.net, 2004-04-28

[2]http://www.karlnet.com/Documents/WhitePaper/TurboCellWhitePaper/TurboCell%20White%20Paper.htm, 2004-04-28

[3] http://en.wikipedia.org/wiki/IEEE_802.11, 2004-04-28

[4] http://www.uninett.no/wlan/ieee80211.html, 2004-04-28

[5] http://www.wi-fiplanet.com/tutorials/article.php/972261, 2004-04-28

[6] Formelsamling i matematisk statistik, Matematiska institutionen, LiTH, 2002

[7] http://www.netgear.com, 2004-04-28

[8] http://www.3com.com, 2004-04-28

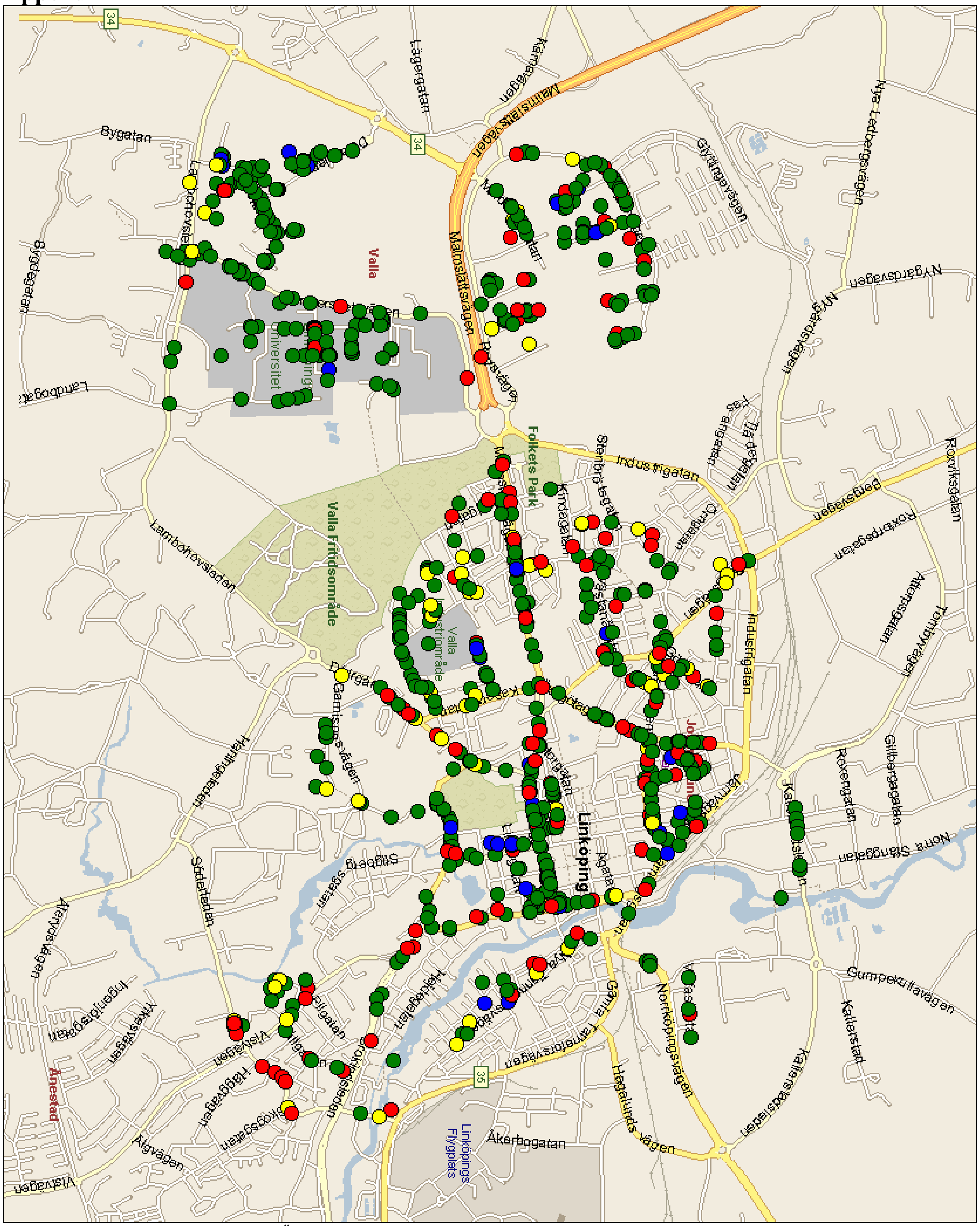
[9] http://www.apple.com, 2004-04-28

[10] http://mediawhore.wi2600.org, 2004-04-28

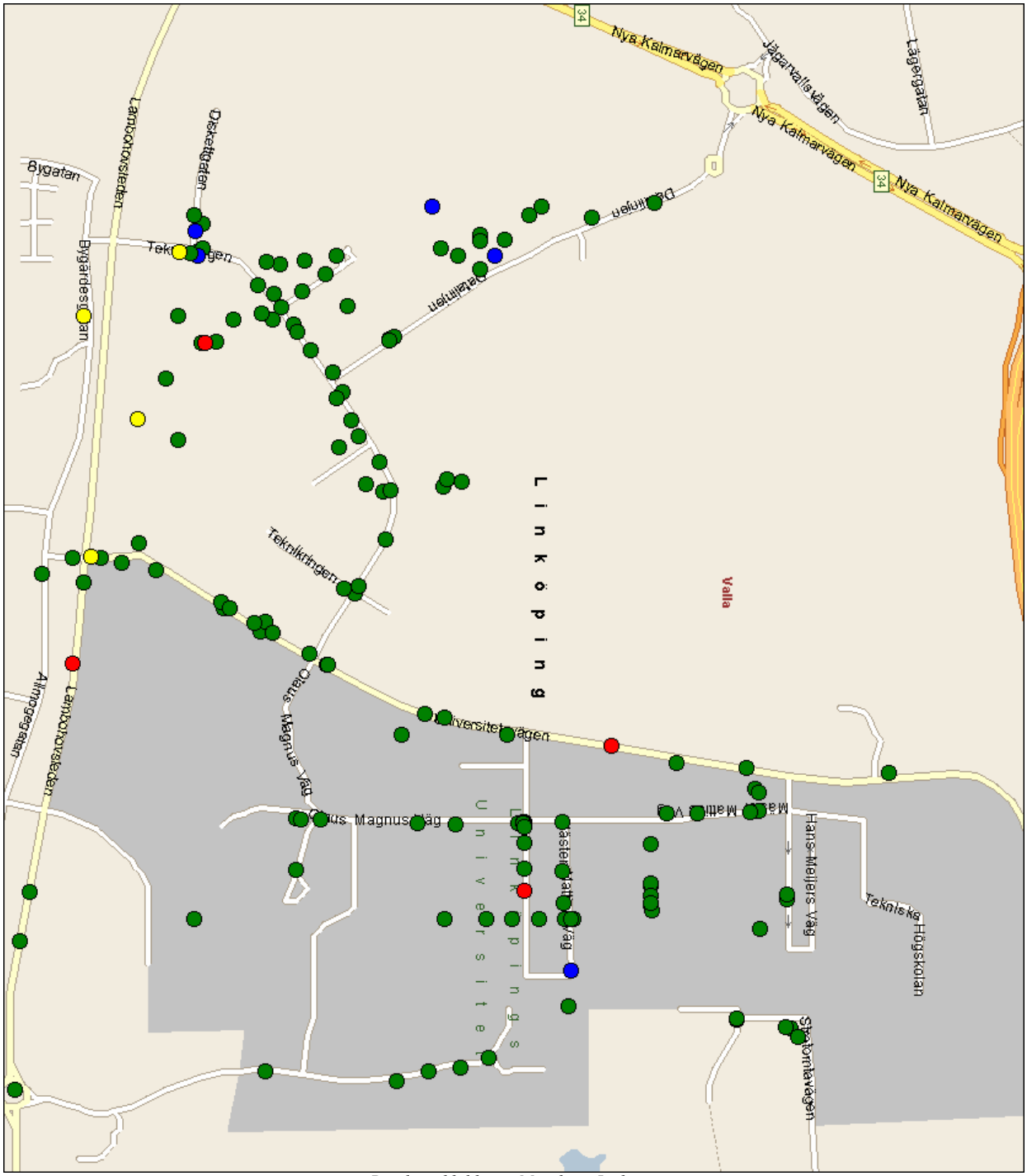
[11] http://server1.h07.org/~sneaker/output.php, 2004-04-28

[12] http://www.ida.liu.se/~TDDC03/old/projects/grp_3.pdf, 2004-04-28

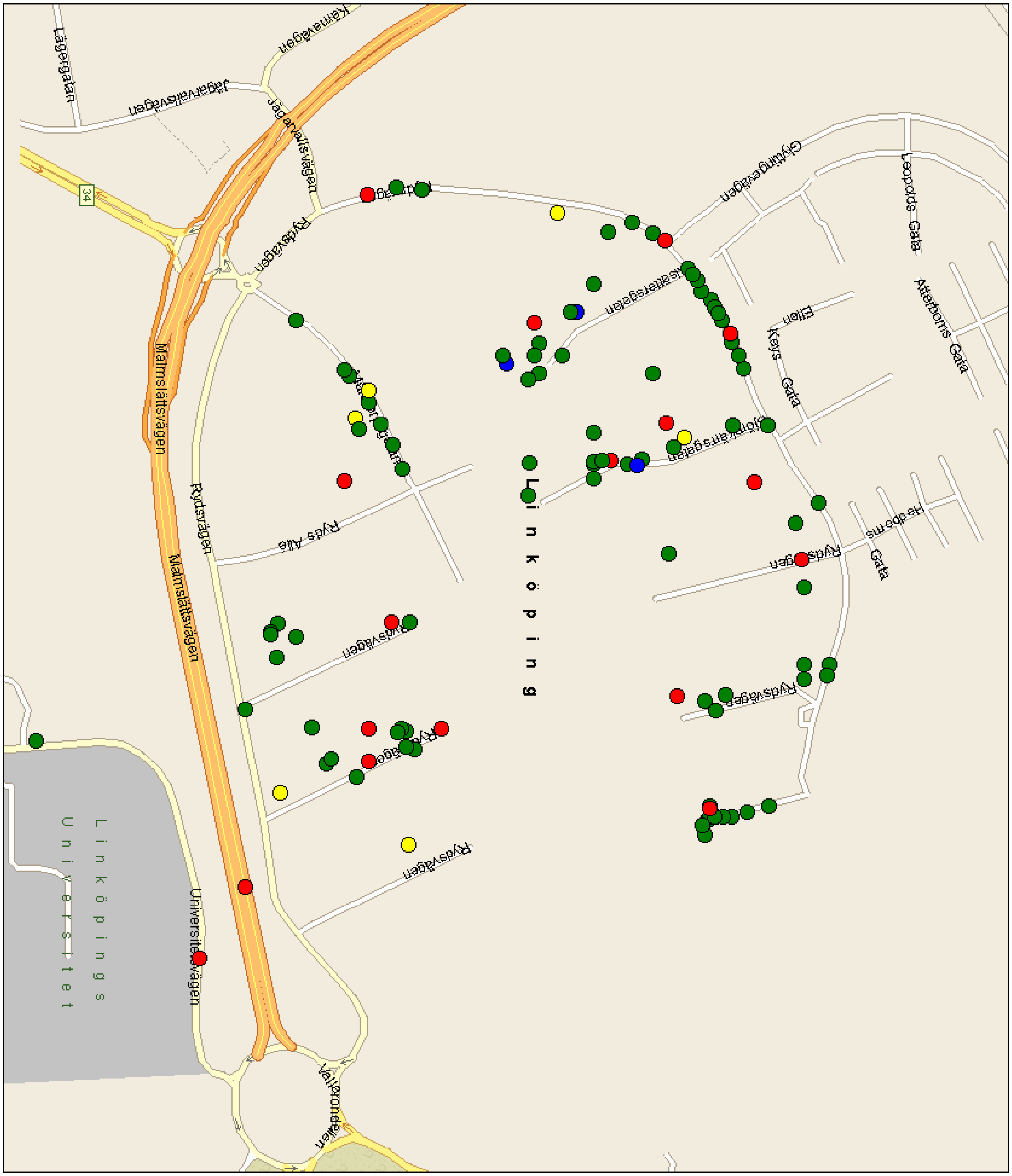
Appendix A



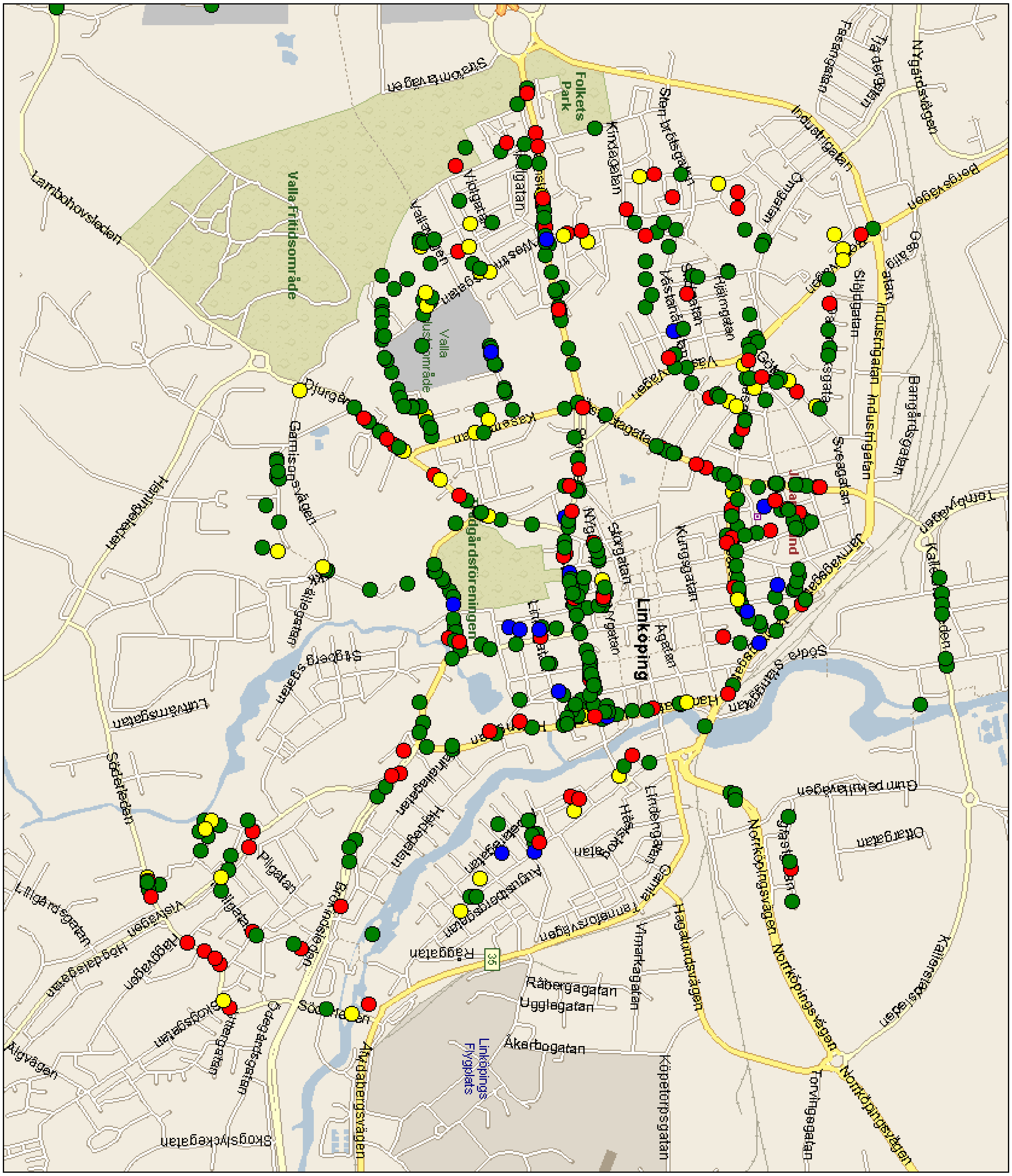
Övergripande bild över accesspunkter inom Y-ring i Linköping.



Detaljerad bild över Mjärdevi i Linköping.



Detaljerad bild över Ryd i Linköping.



Detaljerad bild över Centrum i Linköping.