Arbetsrubrik: ”Jämförelse mellan olika nätverkstopologier för trådlösa sensornätverk”

Referat (skriv till sist < 1 sida)

Innehållsförtecking WIP

1. Inledning (skriv till nästsist – 2-3 sidor)
	1. Led in läsaren på området som avhandlingen behandlar
	2. Problemformulering – varför har du skrivit avhandlingen
	3. Vad går avhandlingen ut på? Kontributioner
2. Bakgrund (skriv detta kapitel först – 3-4 sidor)
	1. Nätverk överlag – hur fungerar de i stora drag
	2. Trådlösa nätverk
	3. Sensorer
	4. Utvecklingen av dessa – vad har skett över åren
3. Trådlösa sensornätverk (3-4 sidor)
	1. Hur byggs de upp
	2. Nätverksstandarder
	3. Exempelanvändningsområden
4. Nätverkstopologier – en jämförelse (4-6 sidor)
	1. Olika strukturer – star network, mesh network, o.d.
	2. Prestanda
	3. Energiförbrukning
5. Sammanfattning (1-2 sidor)
6. Inledning
7. Bakgrund
	1. Nätverk överlag

Ett datornätverk består två eller flera apparater som är sammankopplade Dessa apparater kan till exempel vara datorer, modem eller sensorer och de brukar kallas för noder inom nätverket. Ett av de mest kända nätverken är internet.

Larry Peterson and Bruce Davie [1] visar olika sätt att få datorer kopplade med varandra utan att vara i direkt koppling med varandra. Ett sätt som kan användas är en så kallad switchnätverk (eng. switched network). Ett switchnätverk består av värd (eng. host) och switchar. Switcharna arbetar med att ta emot och föra paket vidare till den rätta mottagaren. Värden är oftast datorer eller servrar som fungerar som ändnoder i nätverken. Värdens uppgift är att använda nätverket, till exempel med att använda data de tagit emot inom ett program. Ett annat sätt är med att använda en router eller en gateway för att koppla ihop två eller flera nätverk med varandra i ett internätverk. Ett internätverk räknas också som ett typ av nätverk och kan då innehålla flera mindre internätverk inom sig. Det världsomfattande Internetet är också en väldigt stor internätverk med flera mindre nätverk inom sig.

Bara en koppling räcker inte till för att få kommunikation mellan noder att ske. Peterson och Davie [1] anger att noder behöver också en adress. Adressen används för att föra paket framåt. Oftast är värden de som är den ursprungliga avsändaren och slutliga mottagaren av datan och switcharnas och routernas uppgift är att avgöra rutten till mottagaren med hjälp av adressen och skicka paketet vidare. Peterson och Davie [1]definierar processen för att räkna ut rutten som dirigering (eng. routing).

Det finns två olika adresser som är viktiga för att kunna identifiera en nod. Dessa adresser är MAC (Media Access Control) och IP (Internet Protocol). MAC adressen är den fysiska adressen, medan IP adressen är den logiska adressen. Mac adressen är fast vid hårdvaran och är unikt. Den används för att identifiera noden inom ett lokalt nätverk. IP adressen används för att hitta noden inom internetet. IP adressen ges av en internetleverantör och är inte bunden till nodens hårdvara och kan därför ändras.



Figur 1: OSI-modellen

Peterson och Davie [1] hävdar hur viktigt det är att ett nätverk kan skötas av människor av olika nivåer av kunskap. Nätverk kan vara väldigt komplexa system och de flesta av dem förändras och uppdateras regelbundet. Därför har nätverksarkitektur utvecklats. Figur 1 visar en av de mest kända nätverksarkitekturen, OSI-modellen. Enligt Peterson och Davie [1] är moderna nätverk inte byggda med OSI-modellen, men modellen fungerar som en bra visualisering till hur ett nätverk är uppbyggd. Den första och lägsta lagret, det fysiska lagret, sköter överförandet av bitar genom någon form av kommunikativ länk, som till exempel en Ethernet tråd. I den andra lagret, datalänkslagret, tas bitarna emot och lagras in i ramar (eng. frames). På nätverkslagret sköts om dirigeringen mellan noderna och data handlas i paket i stället för ramar, även om de är ungefär samma sak enligt Peterson och Davie [1]. I transportlagret finns de funktioner som ser till att meddelanden (eng. message) kommer framtill den rätta mottagaren. Meddelanden är datamängden som används i transportlagret. Sessionslagret innehåller funktionerna som skapar och avslutar kommunikationskanaler, som kallas för sessioner, mellan noder. Där sammanställs också de olika transportströmmar som ett program kan innehålla. Presentationslagret handlar om formateringen av data och att mottagaren ser meddelandet i rätt form. Den översta lagret, applikationslagret, innehåller funktioner som sköter kommunikationen mellan program som till exempel HTTP (Hypertext Transfer Protocol), som är ett protokoll för att överföra webbsidor.

* 1. trådlösa nätverk

Trådlösa nätverk skiljer sig från trådbundet nätverk på flera olika sätt. Peterson och Davie [1] nämner att trådlösa nätverk har en större risk för bitfel (eng. bit error) på grund av brus (eng. noise) i miljön. Det är också svårt att reglera åtkomstkontroll (eng. access control) i trådlösa nätverk eftersom de är uppbyggda med multipelåtkomst (eng. multiaccess). Det betyder att det är svårt att skicka en signal till bara en mottagare. Andra apparater som kan också ta in samma signal.

Det finns olika teknologier att bygga trådlösa nätverk med. Vissa exempel på det är Wi-Fi, Bluetooth och 4G. Peterson och Davie [1] visar att de skiljer sig från varandra med till exempel deras räckvidd och datatakt (eng. data rate). De har också olika användningsområden. Till exempel Bluetooth används för att ansluta en kringutrustning till en dator.

* 1. Sensorer

Sensorer används för att mäta olika slags fenomen från den fysiska världen. Det finns olika slags sensorer som mäter olika saker. Det finns till exempel sensorer för att mäta temperatur, luftfuktighet eller mängden rök i luften. Robert Sheldons artikel [2] definierar två typer av sensorer, aktiva och passiva. Aktiva sensorer behöver en extern strömkälla för att kunna fungera. Passiva sensorer klarar av att producera den nödvändiga energin själva med hjälp av miljön. Sensorer kan också enligt artikeln [2] delas in i analoga eller digitala sensorer. Skillnaden mellan dessa har och göra med hurudana utsignaler de ger. En analog sensor ger ut en kontinuerlig analog signal, medan en digital sensor ger ut en diskret digital signal i binär form.

1. Trådlösa sensornätverk

Trådlösa sensornätverk (WSN) är ett av de mest populära områden inom nätverk. WSN blir mer och mer vanliga inom flera olika användningsområden. WSNs uppgift är att övervaka och mätta fysiska fenomen på distans.

* 1. Hur byggs de upp

En WSN innehåller en stor mängd av sensornoder för att mäta någon typ av fysiskt fenomen. Dessa sensorer både genererar data och fungerar som relä för ett nätverk. Enligt F. Akyildiz och Mehmet Can Vuran [3] är en sensornod byggd upp av trådlös moduler som också kallas för stoftkorn (eng. mote), ett sensorkort och en programmeringstavla (eng. programming board). Stoftkornet består oftast av ett mikrokontroller, sändtagare, en minnesenhet, en strömkälla och kan också innehålla ett par sensorer. Det är inom stoftkornet där nodens kommunikationsförmåga är byggt in. Stoftkornets minne är också programmeringsbart och det är där programkoden (application code) finns. Sensorkortet är ihopsatt med stoftkornet och är kopplad till flera olika sensorer. Programmeringstavlan innehåller flera olika portar för att kunna koppla noden med nödvändiga gränssnitt som till exempel Wi-Fi, USB. Portarna används till exempel för att programmera noden eller ta ut data från dem.

Enligt Akyildiz och Vuran [3] är en av de viktigaste utmaningarna inom ett WSN sensorernas energihantering. Sensornoderna brukar innehålla batterier med begränsad kapacitet. Sensornoderna reglerar deras energiförbrukning dynamiskt och kan till exempel sluta sända data till nätverket tillfälligt. Eftersom nätverket kan ändras dynamiskt är det svårt att hålla anslutning inom nätverket och samtidigt försöka minimera energiförbrukningen. En stor skillnad till traditionella nätverk är att WSN har som mål att optimera energihanteringen till skillnad från att förbättra throughput och minska på dröjningen (eng. delay).

Noderna i en WSN kan också utnyttja multihop kommunikation. Sensornoderna har oftast kort signalräckvidd och därför har ett sätt för sensornoderna att kommunicera med varandra utvecklats. Multihop möjliggör att en signal kan hoppa från nod till nod innan den når till exempel basstationen. Alla WSN använder dock inte multihop, utan de kan vara singlehop nätverk där sensornoderna inte kan kommunicera med varandra.

Sensornoderna inom ett WSN behöver inte ha förbestämda positioner. Akyildiz och Vuran [3]] hävdar att noderna kan placeras slumpmässigt inom området som behövs mätas. Det kräver dock att noderna har protokoll för att kunna organisera nätverket automatiskt. Det används till exempel när terrängen är svåråtkomlig eller vid katastrofhjälp.



Figur 2: Sensorfält (bildkälla: <https://www.researchgate.net/publication/4128327_Power_efficient_communication_protocols_for_data_gathering_on_mobile_sensor_networks>)

Området sensornoderna är placerade i kallas för ett sensorfält (eng. sensor field) som visas i Figur 2. Figur 2 visar hur en multihop WSN är byggd i stora drag. Noderna klarar av att kommunicera med varandra och med hjälp av det föra en signal fram till basstationen. Basstationen kommunicerar sedan med användaren via till exempel internet. Akyildiz och Vuran [3] påpekar att det kan finnas flera basstationer och användare i denna typ av WSN.



Figur 3: Sensornätverk protokollstack (bildkälla: <https://www.researchgate.net/figure/The-sensor-network-protocol-stack_fig2_309426019>)

Figur 3 visar hur ett sensornätverks protokollstack är uppbyggt. Den baserar sig på OSI modellen och innehåller fem av OSI-modellens lager. Protokollstacken har dock flera plan som är specifika för sensornätverk.

Enligt Akyildiz och Vuran [3] är det fysiska lagret som sköter allt som har med signalerna att göra. Där tas signaler emot och skickas framåt. I lagret sköts fekvensgenereringen, signaldetektering och krypteringen. OBS Måste skriva mera, hitta en till källa

Datalänkslagret, som också kan kallas för MAC-lagret, ansvarar för multiplexingen av dataström, detekteringen av dataramar (eng. data frame) och felkontroll. Multiplexing betyder kombinationen av flera signaler till ett signal för att signalerna ska bättre kunna gå igenom ett gemensamt medium. Till exempel flera telefonsamtal kan utföras samtidigt genom samma tråd med hjälp av multiplexing. Till datalänkslagret tillhör MAC-protokollen. Enligt Akyildiz och Vuran [3] används MAC-protokollet för att reglera när en sensornod avbryter dess kommunikationsförmåga för att spara på energi. Regleringen behövs för att noden kommer att använda mer energi om dess sändtagare ofta stängs av och startas upp än om den var på hela tiden. Akyildiz och Vuran [3] nämner också två viktiga uppgifter MAC-protokollet har inom en multihop självorganiserande WSN. Protokollet måste skapa själva infrastrukturen för nätverket så att noderna kan kommunicera med varandra och den ska dela resurser som tid, energi och frekvenser mellan sensornoderna rättvist och effektivt.

I nätverkslagret sköts dirigeringen (eng. routing) för hur data förs framåt inom nätverket. Akyildiz och Vuran [3] fokuserar på multihop WSN när de beskriver vad som görs inom nätverkslagret. De beskriver hur viktigt det är att ha en effektiv dirigering på grund av sensornodernas korta räckvidd och den potentiellt långa avståndet från basstationen. Enligt Akyildiz och Vuran [3] fungerar inte vanliga dirigeringstekniker från normala ad hoc nätverk för WSN. När man designar nätverkslagret inom ett WSN ska man ta hänsyn till energieffektivitet, hur ett sensornätverk är datacentrerad, en nod kan också aggregera data den fått från andra noder och att en nod kanske inte har en unik adress på grund av den stora mängden noder nätverket kan innehålla. Då kan noden identifieras med till exempel med hjälp av var den är placerad eller med hjälp av data den skickar. Denna identifiering är praktiskt på grund av att man oftast inte är intresserad vad bara en nod mäter. Akyildiz och Vuran [3] ger som exempel att man vill veta områden inom nätverket där noderna mäter en viss temperatur.

Transportlagret är väldigt viktigt då ett WSN behöver kontaktas med hjälp av ett externt nätverk som internet. Akyildiz och Vuran [3] nämner att andra nätverksprotokoll som till exempel TCP fungerar inte så bra för WSN på grund av de unika problemen som WSN har. Dessa problem är samma som man måste ta i beaktande när man designar nätverkslagret inom ett WSN. Om ett WSN behöver ha kontakt med ett externt nätverk kommer kommunikationen med det att ske via basstationerna. Sensornoderna har inte hårdvaran för att göra det på grund av alla andra kraven som de måste uppfylla. Akyildiz och Vuran [3] nämner också att transportlagret har viktiga uppgifter också med kommunikationen inom ett WSN. WSN klarar inte av att använda traditionella tillförlitlighetsmekanismer från sändare till mottagare och måste använda lokaliserade pålitlighets mekanismer. Ett WSN behöver också protokoll för att sköta överbelastning inom nätverket och det sköts inom trasportlagret.

Applikationslagret innehåller huvudprogrammet, flera hanteringsfunktionaliteter, frågebehandlingen samt koden för de olika programmen som ett WSN innehåller. Applikationslagret har olika plan för uppgifter som måste utföras. I Figur 3 kan man se de tre planen som hör till applikationslagret: topologihantering, synkronisering och lokalisering. Enligt Akyildiz och Vuran [3] sköts det som håller upp anslutningen inom ett WSN i topologiplanet. Sykroniseringsplanet sköter om att hålla tidsinformationen för den samlade data konsekvent. Akyildiz och Vuran [3] skriver om hur viktigt det är att tidssykroniseringen är konsekvent mellan data de olika sensorerna samlat för att få en korrekt helhetsbild av det man försöker mäta. Inom lokaliseringsplanet används information på placeringen och läget av sensornoderna. Enligt Akyildiz och Vuran [3] behövs nodernas läge för vissa typer av mätningar som till exempel spårning. Vissa kommuniktaionsprotokoll behöver också infromation av nodernas läge.

I Figur 3 finns tre hanteringsplan som inte hör till bara ett lager inom protokollstacket. Dessa plan är uppgiftshanteringsplanet, mobilitetshanteringsplanet/rörlighetshanteringsplanet och energihanteringsplanet. Enligt Akyildiz och Vuran [3] behövs planen för att få sensornoderna att samarbeta. Samarbetet mellan noderna ökar på livslängden av nätverket och gör den mer effektivt. Uppgiftshanteringsplanet sköter ordningen på när olika uppgifter sköts inom ett visst område i ett WSN. Till exempel alla noder inom området behöver inte göra samma sak på samma gång. Vissa noder kanske också behöver arbeta mindre på grund av deras energitillstånd. I mobilitetshanteringsplanet/rörlighetshanteringsplanet övervakas sensornodernas rörlighet och läge. Det behövs för att hela tiden upprätthålla kontakten till grannoderna och basstationen eller användaren. I energihanteringsplanet sköts energihanteringen av sensornoderna. När energinivån i en nod är låg kan den sluta ta emot signaler och måste då signalera grannoderna att den inte tar emot mera signaler.

* 1. Nätverkstandarder (zigbee + andra)

På grund av utvecklingen av flera olika sensorsystem kunde kommunikationsproblem inom nätverket uppstå. Det visade behovet för standardiseringen av kommunikationen inom WSN. Tre olika band för kommunikationsfrekvensen bestämdes enligt Akyildiz och Vuran [3]. Banden var den globala (2.4 GHz), den amerikanska (915 MHz) och den europeiska (868 MHz). Standardiseringsorganet IEEE 802.15.4 grundades också för att specificera trådlösa sändtagare med låg datatakt och liten energiförbrukning. Akyildiz och Vuran [3] nämner också andra standarder som utvecklats inom WSN. Standardiseringar som ZigBee och WirelessHART används för trådlös kontroll och övervakning av applikationer medan 6LoWPAN används för att möjliggöra kommunikationen mellan WSN och externa nätverk.

IEEE 802.15.4 är en standardisering som arbetar inom det fysiska lagret och MAC lagret. Det är IEEE 802.15.4 som standrdiserade bandfrekvenserna som skulle användas. Enligt Ketan Devadiga [11] är överföringshastigheten (eng. transmission rate) 20 kb/s för den europeiska, 40 kb/s för den amerikanska och 250 kb/s för den globala. Devadiga [11] definierar det fysiska lagrets uppgifter att vara sändandet och mottagande av data, LQI (link quality indication), CCA (clear channel assessmen) och energi detektering av den nuvarande kanalen. MAC lagret är ett del av datalänkslagret. MAC lagret i IEEE 802.15.4 har enligt Devadiga [11] som uppgift att sköta kanalernas åtkomstmekanismer, bekräftande av ramar kommit fram och valideringen av ramarna. Lagret sköter också hanteringen av fyrramar (eng. beacon frames)



Figur 4: Zigbee protokollstack (bildkälla: <https://www.researchgate.net/figure/IEEE-and-ZigBee-protocol-stack_fig1_283951808>)

ZigBee är en standard som är utvecklad för att ge en kostnadseffektiv standard för trådlösa nätverk med låg datatakt och energiförbruk samt öka nätverkets säkerhet enligt Akyildiz och Vuran [3]. ZigBee används ofta tillsammans med IEEE 802.15.4 standarden. Standarden används i olika delar av protokollstacken och kan därför används inom samma WSN, vilket Figur 4 visar. ZigBee definierar inom nätverks- och applikationslagret medan IEEE 802.15.4 definierar hur datalänks- och fysiska lagret ska vara byggt. Enligt G. Aju [5] sköter ZigBees nätverkslager initialiseringen av nätverket, adresseringen, dirigeringen, säkerhetesmetoderna för meddelanden och tilläggning och borttagning av noder. Enligt G. Aju [5] visar appikationslagret ett gränssnitt av ZigBee systemet till användaren. Figur 4 visar hur ZigBee delar upp applikationslagret till ZigBee Device Object (ZDO), Application Support Sublayer (APS) och applikations ramverket (eng. application framwork). Enligt G. Aju [5] är en av ZDOs uppgifter att ge funktioner till alla ZigBee apparater i nätverket. Det betyder att ZDOn är den som styr vilka uppgifter en nod skall utföra. ZDOn sköter också säkerhetsrelaterade uppgifter som till exempel krypteringen. APS har som uppgift att möjliggöra ZDOs och ZigBee slutenheternas, det vill säga sensornoderna inom WSN, kommunikation med nätverkslagret. Applikationsramverket används enligt G. Aju [5] för att se till att ZigBee apparater från olika tillverkare kan fungera i samma nätverk.

ZigBee används för att definiera hur ett WSN:s datatrafik ska organiseras. Akyildiz och Vuran [3] definierar tre sätt på hur datatrafiken ska vara organiserad beroende på applikationen som nätverket har. I den första mäter sensorerna fysiska fenomen kontinuerligt och då styrs dataflödet av en nätverkskontroller eller en router. I den andra sättet börjar sensorerna mäta efter ett händlese som kan antingen vara ett externt fenomen eller styrt av applikationen. Datatrafiken styrs då genom routernoder. Den tredje sättet har och göra med kommunikation som ske inom en viss tidsram. Trafiken för den styrs av IEEE 802.15.4 definierade avfrågningsbaserade ramstrukturen. ZigBee standarden innehåller ett flexibelt sätt för att ge adresser för noder.

Highway Addressable Remote Transducer (HART) är det mest använda kommunikationsprotokollet inom automations- och industriapplikationer enligt Akyildiz och Vuran [3]. Standarden fungerar enligt ett primär/sekundär kommunikationsprincip och anänvds för att styra och övervaka applikationer med ungefär 20 miljoner apparater. WirelessHART är den trådlösa versionen av HART. Enligt Akyildiz och Vuran [3] har WirelessHART fem olika komponenter. WirelessHART field devices (WFD) är sensorer som är kopplade till maskiner. Gatewayn används för att för att ge ett gränssnitt för den trådlösa delen av nätverket och den trådbaserade nätverksinfrastrukturet. Gatewayn möjliggör också kommunikationen mellan värdapplikationen och WFDn. Nätverkshanteraren (eng. network manager) hanterar kommunikationen mellan apparater och övervakar nätverkets hälsa. WirelessHART adapters sköter integreringen av äldre HART apparater till det trådlösa nätverket. WirelessHART innehåller också bärbara meddelare som ska ge tillgång till nätverket och WFD gränssnittet på plats.

I de flesta WSN klarar inte sensornoderna att kommunicera med externa nätverk som internet och gör det i stället med hjälp av gatewayn. Gatewayn blir då en systemkritisk felpunkt. IPv6 over Low-power Wireless Personal Area Network (6LoWPAN) standarden utvecklades för att möjliggöra ett effektivare sätt för ett WSN att kommunicera med internet. Enligt Akyildiz och Vuran [3] definierar 6LoWPAN hur man implementerar stacken för IPv6 ovanpå IEEE 802.15.4. Det möjliggör kommunikation mellan internet och alla noder inom WSN. 6LoWPAN innehåller ett anpassningslager där radio- och IPv6 kommunikationen kan operera samtidigt. För att kunna anpassa IPv6 kommunikation inom ett WSN behöver också paketerna som skickas vara fragmenterade. Det beror på att sändtagare inom WSN använder IEEE 802.15.4 där den maximala nyttolasten (eng. payload) är 102 byte och inte klarar av att ta emot hela nyttolasten från källor som skickar med IPv6 som har den maximala nyttolasten av 1280 byte.

* 1. Exempelanvändningsområden

Sensorer används för att mäta flera olika saker, vilket också betyder att WSN används i flera olika områden. Akyildiz och Vuran [3] definierar fem kategorier för användningsområden för WSN: militären, miljön, hälsovården, hemmet och industrin.

WSN är väldigt användbara inom militären på grund av att nätverket kan fortsätta fungera även om en del av sensornoderna förstörs av till exempel fienden. WSN har flera olika användningar inom militären. De används till exempel för att övervaka utrustning, fiendens styrkor, terrängen eller för att detektera användningen av kemiska-, biologiska- eller kärnvapen. Akyildiz och Vuran [3] går vidare in på tre olika typer av WSN inom militären: Smart Dust, detektering av prickskyttar och VigilNet. Smart Dust teknologin hade som mål att utveckla WSN med små sensornoder för militär användning. Nodernas storlek är ungefär 100 kubikmillimeter och de används för flera olika saker inom militären, som övervakningen av slagfält eller transportövervakning. Smart Dust har också fått kommersiell användning i till exempel virtuella tangentbord och övervakning inom köttproduktion. Prickskyttsdetektering fungerar med antingen en samling mikrofoner som är monterad på ett fordon eller buren av en person eller med ett nätverk av sensorer som tar upp ljudet och sedan räknas det ut varifrån skottet blivit avfyrat. Dessa system används förutom militären också för att till exempel öka säkerheten under evenemang som till exempel tal. VigilNet är ett storskaligt övervakningsnätverk som använder magnetiska sensorer som märker magnetfält när till exempel fordon kommer nära sensorn. VigilNet är ett energieffektivt som klarar av övervakning inom ett stort område och är därför väldigt användbar för slagsfältsövervakningsapplikationer där minimeringen av risker för militärpersonal är viktigt.

WSN har väldigt många olika användningar inom miljön. Nätverken används för att spåra djur och att mäta flera olika fenomen som sker i naturen. Akyildiz och Vuran [3] ger som exempel bland annat Great Duck Island projektet, ZebraNet och Vulkanövervakning. På ön Great Duck Island (GDI) används WSN för att övervaka fåglarnas häckningsområden och för att mäta mikroklimatiska faktorer inom ön. Data som samlas används för att till exempel studera hur ändringar i miljön påverkar fåglarnas häckande. WSN som används i GDI har därför två olika typer av sensornoder. Den första typen är placerad i ställen var fåglarna lagar deras bon och mäter temperatur för att veta om bon är i användning. Den andra typen av sensornoderna mäter mikroklimatet i området. ZebraNet är ett exempel på ett WSN som används för att spåra djur. I ZebraNet hängs sensorn runt halsen på en zebra och med hjälp av den kan man hålla koll på var den är. ZebraNet är ett exempel på ett WSN där sensornoderna inte kan kommunicera med basstationen hela tiden på grund av att noden är hela tiden i rörelse och kan vara för långt borta från basstationen. ZebraNet använder därför två protokoll för att kringgå fördröjningen i överförandet av data. I den första sänder noderna deras information och data till en grannod när de möter en ny grannod. I den andra ges noderna en hierarki, där en nod får ett högre nivå inom hierarkin då den just kommunicerat med en annan nod. När noderna kommer ikontakt med varandra är det noden som är högre i hierarkin som tar emot data från den andra noden. När noden sedan kommer i kontakt med basstationen delar den med sig all data, både vad den själv mätt och vad den fått från andra noder. Vulkanövervakning är ett exempel på var WSN kan användas för att mäta fenomen i områden som kan vara farliga för människor. Dessa WSN har enligt Akyildiz och Vuran [3] bara blivit använt två gånger i början av 2000-talet och de användes för att få data från aktiva vulkaner. I vulkanövervakning har WSN ofta bara liten mängd noder. Dessa noder mäter seismiska aktiviteter som händer i vulkanen runt utbrottet.

WSN användning inom hälsovården är ganska omfattande. Akyildiz och Vuran [3] fokuserar på WSN användniung i övervakningen av patienter och artificiella näthinnor, men det finns också andra användningar inom hälsovården. Projektet för artificiella näthinnor har som mål att implantera en konstgjord näthinna till människor med synskador. Målet med projektet är att ersätta skadade fotoreceptorer med mikrosensorer. WSN används också för att övervaka patienter och deras hälsa. Sensorer kan mäta till exempel deras puls, blodtryck och muskelaktivitet.

Enligt Akyildiz och Vuran [3] används WSN i flera hushållsapplikationer. De ger som exempel dammsugare, DVD spelare och kylskåp som apparater som kan innehålla WSN. WSN kan ge applikationen möjligheten att vara lättare hanterat, både lokalt och på distans. Applikationernas sammankoppling kan också möjliggöras av WSN.

Sensornätverk med tråd har använts länge inom industrin för till exempel automering av produktionen. Enligt Akyildiz och Vuran [3] är dock dessa nätverk väldigt dyra att både installera och förbättra. WSN är både lättare att implementera, upprätthålla och de har större noggrannhet. Ett användning för WSN inom industrin är förebyggande underhåll. Sensornoderna mäter vibrationer i maskinen och från det kan man avgöra i vilket skick maskinen är.

1. Nätverkstopologier – en jämförelse (4-6 sidor)

En nätverkstopologi beskriver hur ett nätverk är uppbyggt. Topologin innehåller både den fysiska och logiska placeringen av noderna och hur kopplingarna inom nätverket är arrangerade. En topologi hjälper med att ge en bild på hur nätverket ska byggas upp och kan ge en bild av hur man implementerar det mest optimala dataflödet inom nätverket. Nätverkstopologier kan också användas för att hitta och fixa problem inom nätverket. Det finns olika typer av topologier och valet av topologin kan ha en stor och fixa problem inom nätverket. Det finns olika typer av topologier och valet av topologin kan ha en stor och fixa problem inom nätverket. Det finns olika typer av topologier och valet av topologin kan ha en stor påverkan på till exempel effektiviteten och energianvändningen av nätverket.

* 1. Olika strukturer – star network, mesh network, o.d.

ZigBee stödjer tre olika typer av nätverkstopologier. Topologierna är star-, tree, och mesh. En ZigBee nätverk består av tre olika typer av noder: koordinator, router och slutenhet. Enligt Ata Elahi och Adam Gschwender [4] är det koordinatorn som ansvarar för initieringen och hanteringen av nätverket och motsvarar basstationen/sinken inom WSN. Routern används inom mesh och tree topologierna och har som uppgift att söka efter den bästa rutten för en meddelande att ta. Slutenheten är noden med minst funktionaliteter och har som uppgift att sända och ta emot paketer. Eftersom en sensornod inom WSN klarar av att både att mäta fysiska fenomen, bearbeta den och skicka och ta emot data, borde en sensornod kunna sköta en zigbee routers uppgift. Vissa noder inom ett WSN kan förstås ha nedsatta funktionaliteter och därför klassificeras som en slutenhet jämfört med en nod med mera funktionaliteter.



Figur 4: Star topologin (bildkälla: <https://www.e-spincorp.com/zigbee-network-topology/>)

Star topologin är en enkel single hop topologi med en central basstation som är kopplad med alla sensornoderna inom nätverket, vilket man kan se i Figur 4. Sensornoderna är inte kopplade med varandra och klarar bara av att kommunicera med basstationen. Enligt Elahi och Gschwender [4] har star topologin fördelen att den är enkel och att paketerna i nätverket inte behöver gå igenom flera hopp för att komma fram till basstationen. Star topologin har dock flera svagheter. Enligt Elahi och Gschwender samt andra [4,5,6,7] kan basstationen fungera som flaskhals på grund av att all trafik måste gå igenom den. I star topologin klarar inte nätverket att göra ett ny kommunikationsrutt mellan sensornoden och basstationen om något blockerar kommunikationen mellan dem. Det beror på att topologin är single hop. Sercan Vançin och Ebubekir Erdem [6] nämner också att WSN med star topologin använder mera energi och är inte så effektiva i stora nätverk med flera noder.



Figur 5: Tree topologin (bildkälla: <https://www.e-spincorp.com/zigbee-network-topology/>)

Figur 5 visar hur tree topologin är byggt upp. Basstationen fungerar som en rotnod till ett multi hop nätverk. Ett nätverk med tree topologin fungerar med en förälder-barn hierarki. Enligt Elahi och Gschwender och andra studier [4,5,6] kan basstationen och routers vara kopplad till både routers och slutenheter. En barnnod klarar bara av att kommunicera med sitt föräldernod medan föräldrar klarar också av att kommunicera med deras barnnod. En föräldernod kan förstås vara en barnnod till en annan nod. Det kan enligt Boris Mihajlov och Mitko Bogdanoski [7] leda till problem om en nod med barn blir oansluten från nätverket. Då kommer alla barn till noden också att bli oanslutna från resten av nätverket. Enligt Vançin och Erdem [6] är tree topologin en lågkostnads topologi med låg energiförbrukning.



Figur 6: Mesh topologin (bildkälla: <https://www.e-spincorp.com/zigbee-network-topology/>)

Mesh topologin är den mest flexibla av topologierna som ZigBee stöder. Figur 6 ser väldigt lika figur 5, men det finns vissa viktiga skillnader mellan mesh och tree topologierna. Mesh topologin använder multi hop kommunikation mellan noderna så som i tree topologin, men noderna i mesh topologin klarar av att kommunicera med varandra utan en hierakisk ordning. I en ZigBee nätverk är slutenheterna kopplade med en router, men kan koppla sig med en annan router om problem uppkommer i den förra kopplingen vilket Elahi och Gschwender och andra [4,5,6,7] visar. I en WSN kan en sensornod fungera både som en router och en slutenhet på grund av dess kommunikationsförmåga. Elahi och Gschwender [4] samt Omojokun G. Aju [5] lägger märke på att mesh topologin möjliggör ett självorganiserande nätverk. Nätverket klarar av att använda olika vägar föra paket fram till basstationen. Självorganiseringen gör också tillägningen eller borttagningen av sensornoder lätt och sensornodernas energibesparingsmetod av att stänga av sig ibland fungerar bra i meshnätverk. Elahi och Gschwender [4] samt Omojokun G. Aju [5] poängterar dock att flexibilittetet kommer i kostnad på att mesh topologin är den mest komplexa av topologierna och behöver större pålägg (eng. overhead).

* 1. prestanda

En viktig aspekt när man bygger upp ett WSN är prestandan på nätverket. De olika topologierna kommer att ha olika prestanda. Sigit Soijoyos och Ahmad Asharis [8] studie jämför topologierna i ett fysiskt WSN med fem sensornoder som mäter temperatur. Studien mäter fördröjningen, dataflödet och paketförlust (eng. packet loss). Susan G. Varghese, Ciji Pearl Kurian, V.I. George, Anupriya John, Varsha Nayak och Anil Upadhyay [9] studie handlar om att jämföra topologierna för ett WSN för användning inom ett IoT (Internet of Things) baserat ljuskontrollsystem. Studien använder simuleringprogrammet Qualnet och nätverket består av 21 noder. Studien jämför också två olika dirigerings protokoll (eng. routing protocol), Adhoc on-demand distance vector (AODV) och dynamic source routing (DSR). Studien jämför bland annat end-to-end fördröjningen, dataflödet och jitter i nätverket. Chenyan Zhang och Wenguang Luo [10] studie jämför topologiernas dataflöde och fördröjning både med antalet noder och olika paketstorlekar med programmet OPNET.

Med dataflöde menas hur många packet data som sänds genom nätverket och lyckas komma fram. I studierna med ett fixat antal noder [8,9] är det star topologin som har den största dataflödet följt av tree topologin. Mesh topologin hade den minsta dataflödet. Soijoyos och Asharis [8] mätte dataflödet i avseende på distans och kom fram till att i mesh topologin minskas paketstorleken mest då distansen paketet måste föras mellan noder ökas. Varghese et al. [9] visade dock att dirigering (eng. routing) protokollet har en stor påverkan på topologins dataflöde. Studiens resultat visar att mesh hade ett bättre dataflöde än tree med DSR, men inte med AODV. Zhang och Luo [10] mäter dataflödet i förhållandet med antal noder. Zhang och Luos mätning hålls konsistent med hur studierna [8,9] med ett fixat antal noder. Mesh topologin hade den minsta dataflödet med star den största. Det intressanta är att tree topologin har dock den största dataflödet vid det största antalet (50) noder. Deras mätning med olika paketstorlekar ger också likande resulatat. Från dessa mätningar kan man dra slutsatsen att star topologin har den största dataflödet, åtminstone i mindre nätverk med 50 eller mindre noder.

Paketförlust sker då en eller flera paket av data förloras under kommunikation av noder. Soijoyos och Asharis [8] jämförelse om paketförlust ger en likadan bild av topologierna som jämförandet av dataflödet. Mesh topologin har den största förlusten, följd av tree topologin. Mesh topologins paketförlust ökar med distansen och går upp till 3% vid 5 meter. Tree topologins paketförlust ökar också med distansen och går upp till 2.5% vid 5 meter. Star topologin har den överlägset minsta paketförlustet med 0,5% från 2 meter framåt och den ökar inte. Det beror på att i star topologin behöver inte paketen gå igenom flera noder för att nå basstationen och därför är risken mindre för ett paket att inte komma fram.

Med End-to-end fördröjning menas hur länge det tar för ett paket att komma från ursprungsnoden till slutdestinationen. Enligt Soijoyos och Asharis [8] studie är det mesh topologin som har den största fördröjningen med ungefär 0.2 sekunder vid distansen 5 meter. Star och tree topologiernas fördröjning mättes att vara nästan lika, med båda mellan 0.1 och 0.15 sekunder. Star topologin hade dock lite mindre fördröjning. Varghese et al. [9] visar liknande resultater. Mesh har överlägset störst fördröjning både med AODV och DSR. Studien visar igen vikten på dirigeringsprotokollet. Tree topologin hade över en sekund mindre fördröjning än star topologin när AODV användes, medan Star hade nästan en sekund mindre när DSR användes. Zhang och Luo [10] visar att fördröjningen ökar när antalet noder ökar. Zhang och Luo [10] visar att ökningen är större i star och tree topologierna jämfört med mesh topologin och att både star och tree har mindre fördröjning än mesh när det finns mindre noder. Studien visar också att en ökad paketstorlek ökar på fördröjningen och att mesh klarar av ett större paketstorlek med mindre fördöjningar.

 Jitter är variationen i latens som ett nätverk har. Varghese et al. [9] studie visar att dirigeringsprotokollet påverkar jitter i en stor grad. Star topologin har mest jitter med AODV med mesh- och tree topologierna ganska nära varandra. Tree har dock lite mindre jitter med AODV jämfört med mesh. Däremot har star topologin minst jitter än de två andra topologierna med DSR. Med detta protokoll har mesh mest jitter och skillnaden mellan mesh och tree är ungefär lika stor som med AODV. Eftersom jittervärdet för samma topologi hade en stor skillnad mellan de två protokollen, kan man dra slutsatsen att topologin inte har en så stor betydelse på jittret som dirigeringsprotokollet har.

* 1. Energiförbrukning

Energiförbrukningen är en viktig statistik som man måste tänka på när man bygger ett WSN. WSN kan operera långa tider utan mänsklig kontakt och måste därför kunna hållas i gång länge. Därför har utvecklingen på WSN teknologier haft ett stort fokus på att förbättra energiförbrukningen. Varghese et al. [9] studie jämför energiförbrukningen mellan topologierna när noderna är inaktiva, sänder data och när de tar emot data. Studien jämför också dirigeringsprotokollen AODV och DSR.



Figur 7: energinförbrukning mellan topologierna (bildkälla: <https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/iet-wss.2018.5065>)

Figur 7 visar resultaten på Varghese et al. [9] simulering av energiförbrukningen. Från figuren kan man se att mesh topologin har den minsta energiförbrukningen oberoende av vilken aktivitetsläge noderna har eller vilket dirigeringsprotokoll används. Star topologin använder mest energi då noderna är inaktiva, men har mindre energiförbrukning jämfört med tree topologin då noderna tar emot eller sänder data. Studien visar att AODV har större energikonsumtion än vad DSR har med alla topologierna. Ur resultaten kan man dra slutsatsen att dirigeringsprotokollet påverkar energiförbrukningen och att mesh topologin är den mest energisnålaste topologin.

1. Sammanfattning (1-2 sidor)

Källförtecking:

|  |  |
| --- | --- |
| [1]  | L. Peterson and B. Davie, Computer Networks: A Systems Approach, Elsevier, 2012.  |
| [2]  | R. Sheldon, ”What is a sensor?,” TechTarget.com, 2022. |
| [3]  | I. F. Akyildiz ja M. C. Vuran, Wireless Sensor Networks, WILEY, 2010.  |
| [4]  | A. Elahi ja A. Gschwender, ZigBee Wireless Sensor and Control Network, Pearson, 2009.  |
| [5]  | O. G. Aju, "A Survey of ZigBee Wireless Sensor Network Technology: Topology, Applications and Challenges," *International Journal of Computer Applications,* vol. 130, no. 9, pp. 47 - 55, 2015.  |
| [6]  | S. VANÇİN ja E. ERDEM, ”Design and Simulation of Wireless Sensor Network Topologies Using the ZigBee Standard,” International Journal of Computer Networks and Applications, vol. 2, no. 3, pp. 135 - 143, 2015.  |
| [7]  | B. Mihajlov and M. Bogdanoski, "Overview and Analysis of the Performances of ZigBee-based Wireless Sensor Networks," International Journal of Computer Applications, vol. 29, no. 12, pp. 28 - 35, 2011.  |
| [8]  | S. Soijoyo and A. Ashar, "Analysis of Zigbee Data Transmission on Wireless Sensor Network Topology," nternational Journal of Advanced Computer Science and Applications, vol. 8, no. 9, pp. 145 - 151, 2017.  |
| [9]  | S. G. Varghese, C. P. Kurian, V. George, A. John, V. Nayak and A. Upadhyay, "Comparative study of zigBee topologies for IoT-based lighting automation," IET Wireless Sensor Systems, vol. 9, no. 4, 2019.  |
| [10]  | C. Zhang and W. Luo, "Topology Performance Analysis of Zigbee Network in the Smart Home Environment," in 5th International Conference on Intelligent Human-Machine Systems and Cybernetics, Hangzhou, 2013.  |
| [11]  | K. Devadiga, "EEE 802.15.4 and the Internet of things," Aalto University School of Science. |