Identifiering av relevanta säkerhetskrav för VANET

Torsten Blomqvist, 36132

Kandidatavhandling i datateknik

Handledare: Jerker Björkqvist

Institutionen för informationsteknologi

Åbo Akademi, 2015

Referat

I framtiden blir det allt vanligare att fordon kommunicerar med varandra. Det finns många tänkbara tillämpningar för att förbättra säkerheten på våra vägar. Dessa tillämpningar har ändå stränga säkerhetskrav eftersom de påverkar trafiksäkerheten. Denna avhandling sammanfattar kort olika tillämpningar för kommunikation mellan fordon. Därefter beskrivs de säkerhetskrav som ställs på de olika tillämpningarna och de begränsningar som finns för att verkställa dessa krav. Efter detta presenteras potentiella attacker mot kommunicerande fordon. Slutligen beskrivs metoder och krav för att förhindra eller minska effekten av sådana attacker.

Nyckelord: VANET, säkerhet, oförnekbarhet, datatillförlitlighet, autentisering, integritet, sekretess

Innehållsförteckning

1 Inledning

Trafiksäkerhet har varit en viktig angelägenhet i världen under de senaste åren. Varje år dör miljontals människor på grund av bilolyckor och många fler skadas. Många ansträngningar har gjorts för att minska dessa problem och förbättra säkerheten. Bilar har idag alltmer effektiva säkerhetsmekanismer så som anti-låssystem och elektronisk stabilitetskontroll. Samtidigt har föraren tillgång till olika hjälpmedel som navigationssystem, parkeringsradar och kameror som ska göra körningen så enkel och säker som möjligt.

Den senaste tekniska utvecklingen inom trådlös kommunikation och mobila datorer tar nu utvecklingen av intelligenta transportsystem (ITS) ett steg längre. Fordon är redan nu sofistikerade datasystem med flera sensorer och datorer, var och en tillägnad en specifik uppgift. Det nya tillägget är trådlös kommunikation. Fordon används som mobila noder för att bilda nätverk kallade VANET (Vehicular Ad hoc Network). Sammankopplade fordon samlar inte bara in information om sig själva och sin miljö utan kan också dela denna information med andra fordon (V2V) eller med närliggande infrastruktur (V2I).

Säkerhet och pålitlighet är väldigt viktiga i utvecklingen av VANET. På grund av den nära kopplingen med den fysiska miljön kan riskerna i dessa nätverk vara mycket större än i konventionella IT-applikationer. En attack mot en säkerhetskritisk applikation i en bil kan vara mycket allvarligare än en hårddisk som

förstörs av virus. I denna kandidatavhandling kommer jag att behandla olika tillämpningar för kommunikation mellan fordon och utreda säkerhetskrav och utmaningar med att trygga säkerheten i dessa system.

2 Nätverksmodell

Nätverken byggs upp av noder som kan vara installerade i fordon (OBU, on-board unit) eller bredvid vägen (RSU, roadside unit). Både OBUn och RSUn förväntas implementera DSRC [1] (dedicated short range communication) radion. DSRC är standardiserat så att IEEE 802.11p adresserar det fysiska skiktet och datalänkskiktet medan nätverksskiktet och uppåt utvecklas i IEEE P1609 [2]. Den nuvarande DSRC standarden föreslår sju kanaler i USA, alla 10Mhz breda och i 5,8Ghz frekvensspektrumet.

I Europa kallas den teknik som i USA och Asien går under namnet DSRC allmänt för ITS (intelligent transport service). Termen DSRC används ofta snävare om en uppsättning tillämpningar, däribland elektroniska vägtullar [1]. EU beslutade 2008 om att allokera 30Mhz av 5,8Ghz spektrumet till ITS [1]. Dessa 30Mhz befinner sig i mitten av det 70Mhz breda band som används av amerikanska DSRC.

ETSI (European Telecommunications Standards Institute) publicerade 2008 en standard för ITS för 8,855-5,925Ghz bandet [3], samma band som används av DSRC i USA. Standarden avser att täcka de väsentliga kraven i artikel 3.2 i R&TTE (The Radio & Telecommunications Terminal Equipment) direktiven. Artikel 3.2 avser effektiv användning av radiospektrumet för att undvika skadlig störning.

3 Tillämpningar för kommunikation mellan fordon

Om fordon direkt kan kommunicera med varandra och med infrastruktur öppnar det nya möjligheter för säkerhetstillämpningar i trafiken. Också andra icke säkerhetskritiska applikationer kan öka effektiviteten och bekvämligheten på vägarna. ”säkerhet” och ”bekvämlighet” används här för att dela in tillämpningarna enligt ändamål. Dessa kategorier kan ändå inte ses som helt oberoende varandra. Till exempel ett meddelande om en kollision kan ses som ett säkerhetsmeddelande

av närliggande fordon medan samma meddelande kan ses som en bekvämlighet av fordon längre bort, indata för att beräkna en alternativ rutt som undviker en eventuell trafikstockning olyckan orsakat.

3.1 Säkerhet

3.1.1 Säkerhetstillämpningar

Säkerhetstillämpningar för fordonskommunikation innefattar bland annat periodiskt sända broadcastmeddelanden. Dessa meddelanden kan innehålla fordonets position, hastighet, acceleration, användning av bromsar, med mera. Detta gör att intilliggande fordon kan förutspå var avsändaren av broadcastmeddelandet kommer att befinna sig i den närliggande framtiden och varna om farliga situationer uppstår.

Andra säkerhetstillämpningar kan varna om ett fordon närmar sig ett rödljus i för hög fart utan att bromsa eller om ett mötande fordon nyligen krävt ingripande av elektroniska stabilitetskontrollen.

3.1.2 Säkerhetsmål

Det är viktigt att säkerhetstillämpningar fungerar korrekt i alla situationer. Därför behövs kryptografiska protokoll som garanterar att meddelandena är autentiska. Sekretess är nödvändigtvis inte viktigt i säkerhetsapplikationer eftersom den sända informationen ofta är observerbar för alla i närheten av fordonet (t.ex. hastighet och position).

3.2 Bekvämlighet och effektivitet

3.2.1 Bekvämlighetstillämpningar

Olika bekvämlighetsapplikationer kan visa sig ha en nyckelroll i utvecklandet och ibruktagandet av trådlös kommunikation hos bilar. Säkerhetsrelaterade tillämpningar kräver standardiserad funktionalitet för att vara användbara, medan

andra icke säkerhetskritiska tillämpningar möjliggör konkurrens mellan biltillverkarna och ger motivation att investera i tekniken.

Iden om kommunikation med andra närliggande fordon har gett upphov till en mängd förslag på olika användningsändamål, till exempel för att underhålla passagerarna [4]. Frågesporter, kortspel eller rallyspel med passagerare i närliggande bilar är några exempel på underhållningstillämpningar som är möjliga med hjälp av kommunikation mellan fordon.

En enkel tillämpning för kommunikation mellan fordon och infrastruktur är olika betalningstjänster, till exempel vägtullar.

3.2.2 Säkerhetsmål

Autentisering av meddelanden krävs vanligtvis för att undvika skadlig manipulation. Sekretess behövs för sådana tillämpningar där man behöver skydda personliga data, till exempel vid finansiella transaktioner.

4 Utmaningar och begränsningar

Kommunikation över VANET kan spela en betydande roll inom trafiksäkerheten. Till exempel i eCall-projektet [5] där ett nödsamtal görs om sensorer upptäcker att en olycka har skett. Sådan information måste vara riktig och sanningsenlig eftersom liv kan stå på spel. Detta sätter strikta krav på säkerheten i systemet. Sekretess är också viktigt, det ska inte vara enkelt för obehöriga personer att spåra fordon. Det har forskats ganska mycket i datasäkerhet och säkerhetslösningar för vanliga PC-baserade miljöer, men VANET skiljer sig från dessa på en rad punkter. Därför sätts unika krav och begränsningar på säkerhetslösningar i fordon [1]:

- De inbäddade datorplattformar som används i fordon har begränsad beräkningskapacitet och begränsat minne. Fordon har en livslängd på åtminstone ett årtionde och man kan inte förutsätta att inbyggda datorer kommer att uppgraderas under fordonets livstid. Detta leder till att användningen av avancerade kryptografiska algoritmer och protokoll är begränsad.

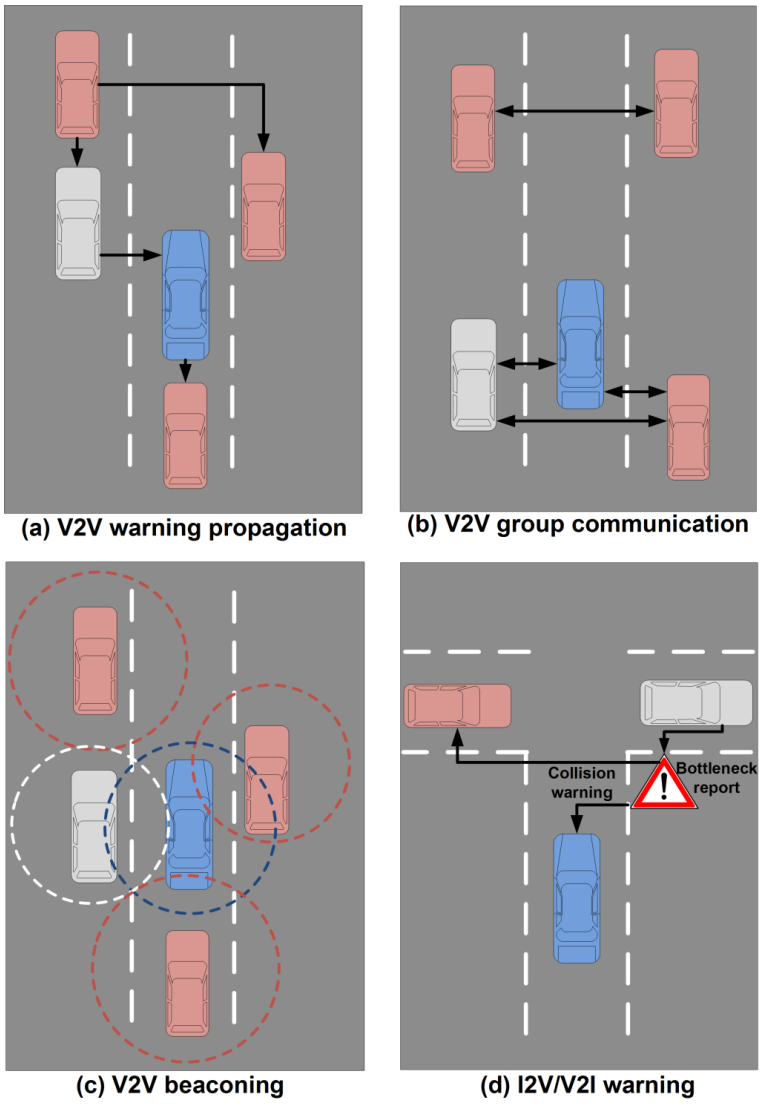
- Bandbredden för extern kommunikation är begränsad. Återigen, fordon har en begränsad livslängd och man kan inte förutsätta att bandbreddskapaciteten kommer att uppgraderas under fordonets livstid.
- Angripare av fordon har ofta fysisk åtkomst till fordonet och fordonets elektroniska kontrollenhet. Traditionella PC-attacker görs ofta över internet medan vid attacker mot fordon kan angriparen också inkludera ägaren eller tredje parter med åtkomst till fordonet, till exempel mekaniker.
- VANET har i de flesta situationer inte permanent uppkoppling till någon fast infrastruktur så som internet. Därför måste kritiska frågor som sekretess och kontroll av nätverket hanteras på andra sätt än hos traditionella PC-baserade nätverk.

Dessutom sätter slutanvändaren en rad andra krav på säkerhetslösningarna:

- Användarvänlighet. En bilägare ska inte behöva bekymra sig om datasäkerheten i fordonet. Därför borde all konfiguration ske automatiskt. Ifall ändringar behövs ska dessa göras hos en verkstad eller över datanätverk som internet eller VANET.
- Sekretess. Sekretess är redan ett stort bekymmer i konventionella IT-system. I VANET finns det ett starkt samband mellan fordon och användare. Integritetsfrågor inkluderar avslöjande av en förares position och beteende.

5 Säkerhetskrav på VANET

VANET möjliggör flera tillämpningar i trafiken, de flesta rörande trafiksäkerheten. De meddelanden som sänds över VANET har ändå olika karaktär och syfte. Med beaktande av detta kan man identifiera fyra olika kommunikationsmönster (Figur 1):



Figur 1. Kommunikationsmönster över VANET [6]

- V2V spridning av varningsmeddelanden (Figur 1-a). Ett meddelande är sänt till ett specifikt fordon eller till en grupp av fordon. Till exempel om en olycka skett kan ett meddelande sändas ut till ankommande fordon för att öka trafiksäkerheten.
- V2V gruppkommunikation (Figur 1-b). Endast fordon med vissa egenskaper kan delta i kommunikationen. Dessa egenskaper kan vara statiska (t.ex. fordon tillhörande samma företag) eller dynamiska (t.ex. fordon på samma område i ett tidsintervall).

- V2V broadcast (Figur 1-c). Broadcastmeddelanden som periodiskt sänds ut till närliggande fordon. Dessa meddelanden sänds endast till närliggande fordon (s.k. single-hop) de är inte vidarebefordrade. De är också användbara för ruttningsprotokoll eftersom de tillåter fordon att upptäcka bästa granne att dirigera ett meddelande till.
- I2V/V2I varning (Figur 1-d). Dessa meddelanden skickas antingen av infrastruktur eller ett fordon när en farlig situation upptäcks. Ett exempel kan vara en varning som sänds till fordon när de närmar sig en korsning där en eventuell kollision kan inträffa.

Varje kommunikationsmönster har en egen uppsättning säkerhetskrav där man måste ta hänsyn till vilken data som står på spel. Tabell 1 specificerar de olika säkerhetskrav som ställs på VANET i olika tillämpningar.

Tabell 1. Säkerhetskrav för VANET [6]

VANET setting / Sec. Requirement	V2V warning propagation	V2V group communication	V2V beaconing	I2V warning	V2I warning
Entity identification	✓ *(all vehicles)*	×	✓ *(sender)*	✓ *(sender)*	✓ *(sender&receiver)*
Entity authentication	✓ *(sender)*	×	✓ *(sender)*	✓ *(sender)*	✓ *(sender&receiver)*
Attribute authentication	×	✓ *(sender&receiver)*	×	×	×
Privacy preservation	✓	✓	✓	×	✓
Non-repudiation	✓ *(sender)*	×	✓ *(sender)*	✓ *(sender&receiver)*	✓ *(sender&receiver)*
Confidentiality	×	✓	×	×	×
Availability	✓	✓	✓	✓	✓
Data trust	✓	✓	✓	✓	✓

Enhets identifikation innebär att man unikt ska kunna identifiera alla enheter. Endast identifikation garanterar däremot inte att enheten är vem den utger sig för att vara, detta krav kallas enhets autentisering. I gruppkommunikation är det inte nödvändigt att kunna identifiera sig eller autentisera sin identitet. Det enda som behövs är attribut autentisering, att man kan visa att man besitter de nödvändiga attribut som krävs för att delta i gruppkommunikationen.

Genomförande av de nämnda kraven bör inte innebära minskad integritet. Bevarande av integriteten är i själva verket kritiskt inom fordonskommunikation.

Inom VANET kan integritet anses vara uppnått når två relaterade mål uppfylls [7]. Ett fordon skall inte kunna spåras till en enskild person och ett fordons åtgärder skall inte kunna kopplas ihop för att bilda in profil av användaren.

Ett annat viktigt krav är oförnekbarhet, det skall vara omöjligt för en enhet att förneka att denna sänt eller tagit emot ett meddelande. På detta sätt finns det bevis som kan användas för ansvarsändamål ifall ett fordon skickar skadlig data.

Sekretess-kravet innebär att meddelanden endast kan läsas av behöriga parter. Detta krav finns endast vid gruppkommunikation där sänd data endast är avsedd för gruppens medlemmar. De övriga kommunikationsmönstren sänder alla offentlig information.

Tillgänglighet är också ett viktigt krav, alla noder ska kunna skicka information när som helst. Eftersom de flesta meddelanden påverkar trafiksäkerheten är detta krav avgörande i denna miljö. Det sista kravet är förtroende för data. Data får inte manipuleras och måste alltid vara sanningsenlig. Detta krav innebär också att mottagen information måste vara aktuell, det vill säga att den avser det nuvarande läget i världen.

6 Attacker mot VANET

När säkerhetskraven för VANET har fastställts kan många potentiella attacker identifieras för att äventyra dem [8]. I detta avsnitt ges en översikt över attacker som kan vara attraktiva för illasinnade motståndare.

6.1 Angrepp på identifikation och autentisering

En nod är en del av nätverket när den erhållit och kan använda en identifierare. Principen är densamma som hos IP-nätverk där en nod endast kan delta i nätverket när den erhållit en giltig IP-adress. En angripare kan låtsas vara ett annat fordon genom att använda falsk identifikation. På samma sätt kan angriparen försöka visa innehav av ett attribut för att delta i gruppkommunikation eller för att få andra förmåner. Som en följd kan angriparen skicka eller ta emot meddelanden som är adresserade till eller från någon annan.

En angripare som kan förfalska eller stjäla identiteter kan också utföra så kallade Sybil-attacker. Detta innebär att angriparen samtidigt låtsas vara flera olika fordon, till exempel för att rapportera förekomsten av en falsk trafikstockning.

6.2 Angrepp på integritet

En angripare kan försöka spåra ett fordon eller koppla samman en förares identitet med ett fordon. Angriparen kan ha ett nätverk av observationsnoder eller endast placera ut en enda nod på ett strategiskt ställe. Angriparen kan också koppla ihop information de fått genom att avlyssna nätverket med annan information så som kamerabilder. Att koppla ihop en förare med ett fordon genom att observera någon starta sin bil och se en ny nod dyka upp är ett exempel.

6.3 Angrepp på oförnekbarhet

Ett angrepp på oförnekbarhet innebär att en enhet kan förneka vissa åtgärder fastän denne varit inblandad. Oförnekbarheten kan till exempel kringgås om två eller flera enheter delar samma identifikation [6]. Denna attack skiljer sig från personifieringsattacken som beskrivits tidigare, i det här fallet ingår två eller flera enheter maskopi om att använda en gemensam identitet. På detta sätt kan de inte skiljas åt, så deras handlingar kan förnekas.

6.4 Angrepp på sekretess

Avlyssning är den mest framträdande attacken mot sekretess. En angripare spelar in mottagna meddelanden för att analysera dem. Detta kan användas för att extrahera information om en förares beteende.

6.5 Angrepp på tillgänglighet

Tillgängligheten hos en nod kan förhindras med ”denial of service”-attacker. Den vanligaste angreppstypen är överbelastningsattacker som kan göras genom att konsumera all tillgänglig bandbredd eller genom att överbelasta ett fordons datorresurser genom att sända meddelanden som tvingar fordonet att utföra svåra beräkningar eller lagra mycket data. En attackerare kan till exempel översvämma mottagaren med bristfälliga meddelanden. En annan möjlig attack är att störa ut radiosändarna med en hjälp av en kraftig signal. Idag finns det inga heltäckande tekniker för att förhindra ”denial of service”-attacker, men de utgör inte heller något

betydande hot. En framgångsrik attack sänker endast säkerhetsnivån till dagens tillstånd.

6.6 Angrepp på datatillförlitlighet

Datatillförlitligheten kan äventyras på flera olika sätt. Ett enkelt angrepp vore att manipulera fordonets sensorer. Fordonets system har väldigt svårt att upptäcka en sådan attack, och det mottagande fordonet tar emot ett giltigt meddelande. Det är endast meddelandets innehåll som inte överensstämmer med verkligheten. Angriparen kan också välja att förfalska meddelanden eller att inte sända vidare meddelanden som ruttas via denne.

7 Översikt över säkerhetsförslag för VANET

Under de senaste åren har det funnits en uppsjö av forskning relaterad till VANET säkerhet. I detta avsnitt analyseras de viktigaste befintliga förslagen för att tillhandahålla säkerhet inom VANET.

7.1 Identifikation och autentisering

Till skillnad från klassiska datornätverk, där ingen central registrering existerar, kan fordon identifieras unikt redan från början [6]. Denna process utförs både av tillverkare och myndigheter. Tillverkaren ger varje fordon en unik VIN-kod (Vehicle Identification Number) medan rättsliga myndigheter kräver att varje fordon har en registreringsskylt.

Med avseende på elektronisk identifiering så har Hubaux m.fl. föreslagit en utveckling av registreringsskyltar som kallas Electronic License Plate (ELP) [9]. Dessa utfärdas av myndigheterna och tillåter att fordon både kan identifiera och autentisera sig. Eftersom dessa referenser innefattar fordonets verkliga identitet blir det dock möjligt att spåra fordon. Det behövs sålunda ett system som tillåter att fordonen förblir anonyma för de flesta andra noder, men som gör det möjligt för myndigheterna att identifiera dem vid till exempel olyckor eller skadligt beteende.

Den allmänt accepterade metoden är att implementera en PKI (Public key infrastructure) [6]. PKI gör det möjligt att binda publika nycklar till motsvarande

identiteter med hjälp av en certifikatutfärdare (CA). Användande av verkliga eller permanenta identiteter möjliggör dock spårning av fordon. Det har föreslagits två olika mekanismer för att uppfylla kraven på autentisering och sekretess i VANET [6]. Dessa är identitetsbaserad kryptografi och pseudonyma kortlivade publika nyckelcertifikat. Pseudonyma certifikat ger både autentisering och integritetsskydd [10] och är den metod som föreslås i säkerhetsstandarden för VANET, IEEE 1909.2 [2]. Identitetsbaserad kryptografi behandlas bland annat av Sun m.fl. [11].

7.2 Integritet

Många VANET tillämpningar sänder ut positionsinformation för att förbättra säkerheten eller effektivera trafikflödet. Denna information kan dock också användas av en angripare för att spåra fordonet. Det är därför nödvändigt att minimera den sända informationen och samtidigt hålla den användbar.

Sampigethava m.fl. [12] föreslår en gruppbaserad lösning där man genom att kombinera närliggande fordon i grupper kan minska antalet gånger ett fordon behöver sända fordonsdata i V2I applikationer. Andra föreslagna lösningar är ”Uncertainty-Aware Path Cloaking” [13] och aggregation [14].

7.3 Oförnekbarhet

Oförnekbarhet innebär att en enhet inte kan förneka handlingar som denne gjort. Inom datornätverk handlar det vanligtvis om att enheten skickat viss information (NRO, non-repudiation of origin) eller tagit emot den (NRR, non-repudiation of receipt). De båda tjänsterna är olika till sin karaktär och de implementeras också på olika sätt inom VANET.

7.3.1 Non-repudiation of origin

NRO implementeras traditionellt med användande av digitala signaturer. Avsändaren signerar det sända meddelandet och mottagaren kan verifiera signaturen med användande av avsändarens publika nyckel. Mottagaren har då också bevis på att det faktiskt var avsändaren som skickade meddelandet. Användandet av digitala signaturer skyddar också integriteten, eftersom en giltig digital signatur också garanterar att meddelandet inte ändrats efter att det signerats. IEEE 1909.2 standarden [2] slår fast att VANET skall använda sig av ECDSA

(elliptic curve digital signature algorithm) som är en algoritm baserad på användandet av elliptiska kurvor.

Gruppsignaturer (t.ex. Boneh m.fl. [15]) är en specifik typ av digitala signaturer som också föreslagits inom VANET. Gruppsignaturer innebär att en gruppmedlem kan signera utan att avslöja sin identitet för signaturens kontrollant. Endast en betrodd tredje part (i detta fall polis eller andra myndigheter) kan avslöja den verkliga identiteten hos undertecknaren. Denna lösning skulle garantera oförnekbarhet samtidigt som den bevarar integriteten.

7.3.2 Non-repudiation of receipt

NRR är mycket relevant i tjänster där notifieringar och andra ansvarsrelaterade meddelanden tas emot av fordon, till exempel om dynamiska hastighetsbegränsningar skickas till förbipasserande fordon. I denna situation måste det finnas bevis på att informationen faktiskt nått fordonen. Annars kan fortkörningsböter vara orättvist eftersom fordonet kan hävda att det inte tagit emot sådan information.

Det finns idag ingen ideal metod för att lösa NRR problemen [6]. För tjänster med endast några få fordon inblandade kan en lösning vara att sända mottagningskvitton. I större sammanhang kan dock skalbarhetsproblem snabbt uppstå.

7.4 Sekretess

Kryptering är en av de viktigaste säkerhetsmetoderna för att tillhandahålla sekretess och undvika avlyssning. Beträffande gruppkommunikation har tre huvudförslag gjorts hittills [6]. Det första innebär att RSU: n styr regioner [16]. Fordon inom en region skall registrera och autentisera sig hos RSU: n och får därefter en symmetrisk nyckel som används av alla fordon i regionen under en tid.

Det andra förslaget bygger på självorganiserande geografiska regioner, ett fordon blir medlem i en grupp beroende på dess plats [17]. Sedan väljs en gruppledare, t.ex. det mest centrala fordonet, som är ansvarig för att skapa och dela ut den symmetriska nyckeln. Till skillnad från föregående förslag ger det här alternativet en längre kommunikationsperiod för gruppen eftersom den inte begränsas av räckvidden hos RSU: n.

Det tredje förslaget för gruppkommunikation bygger på attributbaserad kryptering [18]. Endast fordon som besitter vissa attribut kan dekryptera skickade meddelanden. Detta förslag möjliggör även dynamiska attribut, till exempel kan ett taxibolag endast rikta meddelanden till de taxibilar som befinner sig nära flygplatsen [6].

7.5 Tillgänglighet

Det finns idag inga effektiva metoder för att möta DOS-attacker, men tillgänglighet måste ändå beaktas i de flesta säkerhetsmekanismer eftersom det också finns också andra hot som kan påverka prestandan i nätverket. Till exempel själviskt beteende hos en nod kan leda till att den överbelastar kommunikationskanalen med förfrågningar. Buttyan och Hubaux [19] har föreslagit en lösning med en elektronisk valuta, Nuglets, som delas ut när en nod deltar korrekt i nätverksfrågor. För att förhindra själviskt beteende kräver sedan vissa applikationer Nuglets av användaren.

7.6 Datatillförlitlighet

Traditionellt sett så har datatillförlitlighet etablerats genom förtroende för avsändaren [6]. Med andra ord, ju mer tillförlitlig en enhet var, desto trovärdigare var dess meddelanden. Inom VANET är det inte lätt för en enhet att bygga upp ett förtroende. Fordon kan möta varandra under en kort tid för att därefter kanske aldrig ses igen. Av denna anledning är det själva informationen som avsändaren ger som måste bevisa sin trovärdighet. Detta kallas situationsmedveten datatillförlitlighet (SAT, Situation-Aware Trust) [18].

Raya m.fl. har föreslagit ett ramverk där man jämför emottagen data med både indata från egna sensorer och iakttagelser hos andra fordon för att utvärdera tillförlitligheten hos den mottagna informationen [20]. Meddelanden som avser samma händelser grupperas sedan så att tillförlitligheten byggs upp för händelser i stället för enskilda meddelanden.

8 Avslutning

Fordon som kommunicerar med varandra kommer snart att bli verklighet. Denna utveckling drivs av krav på trafiksäkerhet och genom investeringar och forskning gjord av biltillverkare och myndigheter. Kommunikationen fordon emellan möjliggör en mängd nya tillämpningar, och omfattar många typer av tjänster med olika mål och krav, inte minst på säkerhet.

I denna avhandling har presenterats en översikt över säkerhetsfrågor inom VANET, med fokus på säker kommunikation och datasäkerhet. Här beskrevs de säkerhetskrav som är viktiga vid olika tillämpningar. Efter detta presenterades potentiella attacker mot VANET, och slutligen sammanfattades kort forskning och säkerhetsförslag för att nå de uppsatta kraven.

De identifierade kraven varierar mellan tillämpningar och typ av kommunikation (t.ex. gruppkommunikation eller broadcasting). Gemensamt för alla tillämpningar är ändå kravet på datatillförlitlighet. Eftersom många tillämpningar direkt påverkar trafiksäkerheten är det viktigt att mottagen information överensstämmer med verkligheten. Detta kan därför ses som ett av de viktigaste kraven, om informationen inte är korrekt fungerar inte säkerhetstillämpningarna. Kravet på tillgänglighet är också viktigt för att allt ska fungera.

Kraven på identifikation, autentisering och oförnekbarhet strävar alla till att åstadkomma datatillförlitlighet. Om man vet som skickat informationen, och om denne inte heller kan förneka det, stärker det tillförlitligheten. Om informationen ändå visar sig vara falsk gör kravet på oförnekbarhet det lättare att hitta den skyldiga.

De återstående kraven, sekretess och integritet, är också viktiga. Dessa krav påverkar dock inte trafiksäkerheten i lika hög utsträckning, utan finns till för att förhindra missbrukande av sänd information.

9 Referenser

[1] H. Hartenstein och K. Laberteaux, VANET: Vehicular Applications and Inter-Networking Technologies, John Wiley & Sons, 2009.

[2] ”Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages (1609.2),” IEEE Computer Society, 2006.

[3] ”Intelligent Transport Systems (ITS); Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive,” ETSI EN 302 571 V1.1.1, 2008.

[4] C. E. Palazzi, ”Fast Online Gaming over Wireless Networks,” PhD thesis University of California, Los Angeles, 2007.

[5] eSafetySupport, ”eCall Toolbox,” [Online]. Available: http://www.esafetysupport.info/en/ecall_toolbox/index.html. [Använd 8 2 2015].

[6] J. M. d. Fuentes, A. I. González-Tablas och A. Ribagorda, ”Overview of security issues in Vehicular Ad-hoc Networks,” Department of Computer Science, University Carlos III of Madrid, 2010.

[7] M. Gerlach, ”VaneSe - An Approach to Vehicular Ad Hoc Network Security,” V2VCOM, 2005.

[8] A. Aijaz, B. Bochow, F. Dötzer, A. Festag, M. Gerlach, R. Kroh och T. Leinuleer, ”Attack on Inter Vehicle Communication Systems - an Analysis,”

International Workshop on Intelligent Transportation, IEEE Communications Society, Hamburg, Germany, 2006.

[9] J.-P. Hubaux, S. Capkun och J. Luo, ”The security and privacy of smart vehicles,” *IEEE Security and Privacy magazine*, pp. 49-55, 2004.

[10] G. Calandriello, P. Papadimitratos, J.-P. Hubaux och A. Lioy, ”Efficient and Robust Pseudonymous Authentication in VANET,” *International Workshop on Vehicular Ad Hoc Networks*, pp. 19-28, 2007.

[11] J. Sun, C. Zhang och Y. Fang, ”An ID-Based framework achieving privacy and non-repudiation in vehicular ad-hoc networks,” i *Military Communications Conference*, Orlando, Florida, USA, 2007.

[12] K. Sampigethaya, L. Huangy, M. Li, R. Poovendran, K. Matsuuray och K. Sezaki, ”CARAVAN: Providing Location Privacy for VANET,” *International workshop on Vehicular ad hoc networks. ACM*, 2006.

[13] B. Hoh, M. Gruteser, H. Xiong och A. Alrabady, ”Preserving privacy in gps traces via uncertainty-aware path cloaking,” *Conference on Computer and communications security. ACM*, pp. 161-171, 2007.

[14] S. Duri, M. Gruteser, X. Liu, P. Moskowitz, R. Perez, M. Singh och J.-M. Tang, ”Framework for security and privacy in automotive telematics,” *International Workshop on Mobile Commerce. ACM*, pp. 25-32, 2002.

[15] D. Boneh och H. Shacham, ”Group signatures with verifier-local revocation,” ACM, New York, USA, 2004.

[16] M. Verma och D. Huang, ”SeGCom: Secure Group Communication in VANETs,” i *IEEE Consumer Communications and Networking Conference*, Las Vegas, NY, USA, 2009.

[17] M. Raya, A. Aziz och J.-P. Hubaux, ”Efficient Secure Aggregation in VANETs,” i *International Conference on Mobile Computing and Networking*, Los Angeles, CA, USA, 2006.

[18] X. Hong, D. Huang, M. Gerla och Z. Cao, ”SAT: Situation-Aware Trust architecture for vehicular networks,” *Mobility In The Evolving Internet Architecture. ACM*, pp. 31-36, 2008.

[19] L. Buttyan och J.-P. Hubaux, ”Nuglets: a Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks,” Laussane: Swiss Federal Institute of Technology, 2001.

[20] M. Raya, P. Papadimitratos, V. D. Gligor och J.-P. Hubaux, ”On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks,” Infocom, Phoeniz, AZ, USA: IEEE Communications Society, 2008.