Vezetéknélküli átviteli technológiák jövője a közúti közlekedésben

Aradi Szilárd
tanársegéd, BME
Közlekedésautomatikai
Tanszék
Dr. Bécsi Tamás
adjunktus, BME
Közlekedésautomatikai
Tanszék

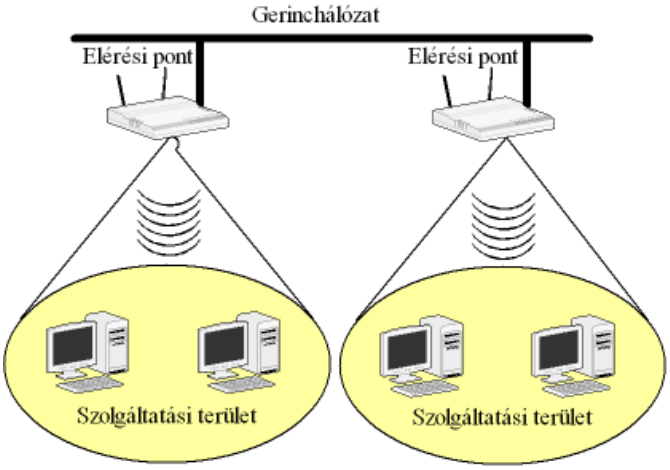
A vezeték nélküli kommunikációs technológiák és a számítástechnika rohamos fejlődésével, egyre nagyobb lehetőségek nyílnak a közúti járművek, valamint a pályamenti berendezések fejlesztésében. A folyamatosan növekvő forgalom, valamint a közúti balesetek nagy száma megteremti az igényt a hatékonyságot és biztonságot növelő berendezések iránt. A cikkben bemutatjuk, hogy milyen technológiák állnak rendelkezésre aktuálisan a járművek közötti (V2V), valamint a jármű és az útmenti berendezések közötti (V2R) kommunikációra. Kitérünk továbbá a jelenleg fejlesztés alatt álló technológiákra, alkalmazási lehetőségekre és a megoldandó problémákra. Megvizsgáljuk a mobil vezeték nélküli hálózatok (MANET) biztonsági és titkosítási kérdéseit, amelyek a tárgyalt rendszerek egyik sarokkövét jelentik.

The wireless communications technology and the rapid development of computer technology give more and more opportunities for the development of vehicle on-board units and track-side equipments. The increasing traffic and the large number of road accidents create the need for equipments, which improve safety and efficiency. The article explains the technology is currently available for vehicles-to-vehicles (V2V) and vehicle-to-infrastructure communications. We examine the mobile wireless network's (MANET) security and encryption issues, which is the most important property of the systems discussed.

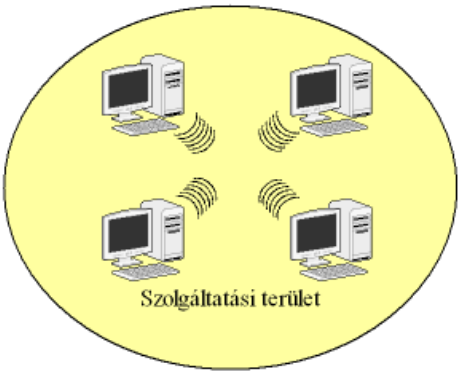
BEVEZETÉS

Az emberek életében már napjainkban is mindenütt jelen vannak a hordozható információs eszközök (PDA, mobiltelefon stb.), és ezen eszközök száma, valamint az adatátvitel sebessége folyamatosan növekszik. Működésük alapját a kommunikációs hálózatokhoz való csatlakozás képezi, ezért a vezetéknélküli hálózati technológiák egyre fontosabbak lesznek.
Általánosan kétféle lehetőség adott arra, hogy a vezetéknélküli hordozható eszközök egymással kommunikáljanak: az infrastrukturális és az ad hoc hálózat.

A mobiltelefon hálózatok hagyományosan cellákat használó technológiát alkalmaznak, emiatt erősen függnek a megfelelő infrastruktúrától (elegendő számú bázisállomás).
Az elmúlt években a vezeték nélkül kommunikáló eszközök rohamos elterjedése, arra ösztönözte a fejlesztőket, hogy olyan önszerveződő hálózatokat találjanak ki, amelyek nem igényelnek előre telepített infrastruktúrát. Ezeket hívjuk ad hoc hálózatoknak. Jellemzően önálló csomópontokból állnak és egymással együttműködve továbbítják az információkat. Általában ezek a csomópontok végpontok és hálózatirányító eszközök (pl.: routerek) is egyszerre.
Az ad hoc hálózatokat manapság két csoportba sorolják: telepített és mozgó. A telepített ad hoc hálózatokban a csomópontok nem változtatják a pozíciójukat. Ilyen például, amikor több számítógép közvetlen kapcsolatot létesít egymással Wi-Fi (Wireless Fidelity) adapter segítségével.
A mozgó ad hoc hálózatokban a rendszer elmozdulhat, melyeket angol rövidítéssel MANET-ként (Mobile Ad hoc Network) emleget a szakirodalom. A MANET vezetéknélküli mozgó csomópontok egy csoportja, amelyek hálózatot alakítanak ki információ továbbítás céljából, anélkül hogy bármilyen telepített hálózati infrastruktúrát vagy központi irányítást használnának. A legnagyobb fejlesztések a járműipar területén a MANET-ek témájában folynak, mivel ezek használata rendkívül gazdaságos, hiszen nem igényel útmenti infrastruktúrát. A járművek közötti MANET-et Vehicular Ad hoc Networknek (VANET) nevezik.



Infrastruktúrális vezeték nélküli hálózat



Ad hoc vezeték nélküli hálózat

1. ábra: Példa az infrastrukturális és ad hoc vezeték nélküli hálózatra

TECHNOLÓGIA ISMERTETÉSE

A MANET csomópontok vezetéknélküli adó-vevővel, valamint körsugárzó, vagy irányított antennával ellátott egységek. Egy adott időpillanatban, a csomópontok pozíciójának, adó-vevőjük lefedettségi területének, adóteljesítményének és a csatornák közötti interferenciáknak a függvényében kialakul egy véletlenszerű hálózat a csomópontok között. Ez a topológia időben folyamatosan változhat a csomópontok mozgása és adó-vevő paramétereik változása miatt. Ilyen környezetben – elsősorban az adatátvitel hatótávolsága miatt- szükséges, hogy egy mozgó csomópont igénybe vegye a többi csomópont segítségét, hogy az üzenete eljusson a címzetthez.
Mivel a mobil ad hoc hálózatok sűrűn és előzetes jelzés nélkül változtatják a topológiájukat, az útválasztás komoly kihívást jelentő feladat. Ezen kívül az adatátviteli típusok is egészen eltérőek, mint az infrastrukturális vezetéknélküli hálózatokban:

- Pont-pont (Peer-to-Peer): A kommunikáció a két fél között közvetlenül zajlik.
- Távoli-távoli (Remote-to-Remote): A kommunikáció a két fél között nem közvetlenül történik, de állandó adatút áll fent közöttük. Az adatok több csomópont érintésével jutnak el a címzetthez.
- Dinamikus adatátvitel (Dynamic Traffic): Akkor áll fenn, amikor a felek folyamatosan mozognak. Az adatátviteli utakat állandóan újra létre kell hozni, ami rossz minőségű kapcsolatokat és rövid lökésszerű hálózati aktivitásokat eredményez.

Értelemszerűen a mobil ad hoc hálózatokra a dinamikus adatátvitel jellemző. Az ilyen jellegű hálózatok főbb tulajdonságai a következők:

Autonóm végberendezések:
A MANET-ekben minden mozgó végberendezés egy autonóm csomópont, amely hostként (végpont) és routerként (útválasztó) is funkciónál. Azaz minden végberendezés alapvetően végpontként működik, azonban szükség esetén ellát router funkciókat is.

Megosztott irányítás
Tekintettel arra, hogy a hálózati műveletek központi irányításához nincs a háttérben hálózati infrastruktúra, ezért a hálózatkezelés és irányítás el van osztva a végberendezések között. A hálózathoz tartozó csomópontoknak együtt kell működniük, és ha szükséges átjátszó, állomásként kell funkcionálniuk, hogy elássanak egyaránt biztonsági és útválasztási feladatokat.

„Multihop routing"
Az ad hoc hálózatok használhatnak ún. singlehop és multihop routingot (útválasztás), attól függően, hogy milyen protokollt használnak a kapcsolati rétegben. A singlehop módszer a hálózati struktúra és az algoritmusok szempontjából jóval egyszerűbb, mint a multihop. Használhatósága és funkcionalitása azonban jóval korlátozottabb, mivel az egyes csomópontok, csak a velük közvetlen kapcsolatban állóknak képesek üzenetet küldeni, azaz a saját adó-vevő körzetükben lévőknek. A multihop módszer viszont, több közbenső csomópont segítségével, távolabbi célpontokhoz is képes eljuttatni az információt.

Változó hálózati topológia
Mozgó csomópontok esetén a hálózati topológia hirtelen és véletlenszerűen megváltozhat, aminek következtében az egyes terminálok összekapcsolhatósága időben változik. A MANET-eknek alkalmazkodniuk kell a változó adatforgalmi feltételekhez, valamint a csomópontok mozgási mintázatához. A csomópontoknak folyamatosan változó adatútvonalakat kell kialakítaniuk egymás között, a mozgásuk függvényében. Ezen felül előfordulhat, hogy egy felhasználó a MANET-ben nem csak az ad hoc hálózatot szeretné használni, hanem hozzáférést igényel egy nyilvános, telepített hálózathoz is.

Ingadozó hálózati kapacitás
A vezeték nélküli kapcsolatok magas bithiba arányai MANET-ekben még nagyobbak lehetnek, amelynek okai a következők. A csatorna, amelyen keresztül a berendezések kommunikálnak eleve jóval zajosabbak, valamint nagyobb a csillapítás, interferencia, és kisebb a sávszélesség, mint a vezetékes hálózatokban. Ráadásul a mobil ad hoc hálózatokban sok esetben az adatutak erősen heterogén hálózatokon keresztül jönnek létre, ami további zajszint-növekedést eredményez.

Valószínűségi Quality of Service (QoS) paraméterek
Ideális hálózatokban garantálhatóak a QoS előírásokat a hálózati kapcsolatok teljes időtartama alatt. Sajnos ez nem lehetséges az időben változó hálózati környezetben. Ennek oka, hogy a kapcsolatok véletlenszerűen megszakadhatnak, a felhasználók mozgása miatt. Sokkal célszerűbb valószínűségi QoS paramétereket meghatározni, azaz a kapcsolati hibákat egy előre meghatározott küszöbérték alatt tartani.

Egyszerű terminál
A legtöbb esetben a MANET-ek csomópontjai olyan mobil eszközök, amelyek aránylag kis processzorteljesítménnyel, kevés memóriával, és korlátos energiaforrással rendelkeznek. Az egyszerű terminálok optimalizált algoritmusokat és módszereket igényelnek a számítási és kommunikációs feladatokhoz.

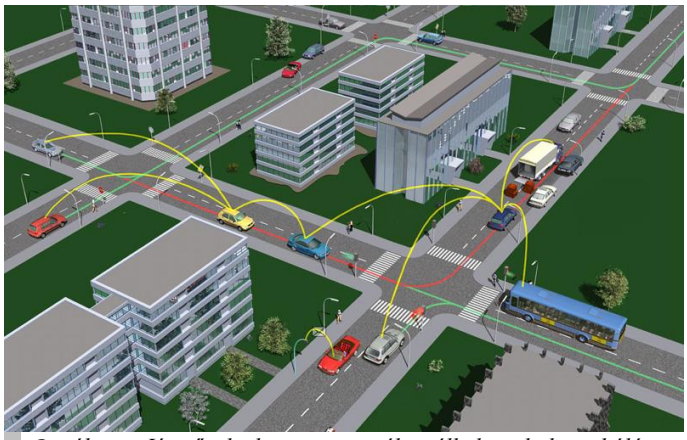
Összefoglalva, a mobil ad hoc hálózat önálló mobil csomópontok egy csoportja, amelyek egy dinamikus, célirányos, multihop, vezetéknélküli, decentralizált hálózatot alkotnak. A hálózati topológia folyamatosan változik, ahogy az egyes csomópontok csatlakoznak illetve kiválnak a hálózatból. A csomagtovábbítást, az útválasztást és más hálózati tevékenységeket a független csomópontok bonyolítják le egymással.

ALKALMAZÁSI LEHETŐSÉGEK

A mobil ad hoc hálózatok fő felhasználási területe a közúti közlekedés, ahol az ilyen fajta hálózatot Vehicular Ad hoc Networknek (VANET) nevezik. A fejlesztők távlati célja, hogy kidolgozzanak olyan egységes kommunikációs szabványokat és hálózati protokollokat, amelyek használatával a különböző gyártók járművei képesek egymással biztonságos ad hoc hálózatok kialakítására.
Több jelentős európai kutatás is indult ebben a témában az elmúlt években:

- CVIS (Cooperative Vehicle-Infrastructure Systems): alap technológiai fejlesztés.
- SAFESPOT: autógyárak fejlesztései.
- COOPERS (Co-operative Systems for Intelligent Road Safety): közút kezelők fejlesztései.

Ezeken kívül 2007-ben megalakult CAR 2 CAR Communication Consortium, amely autógyárak, egyetemek és kutatóintézetek bevonásával dolgozik egy egységes kommunikációs platform kifejlesztésén.



2. ábra: Járművek közötti vezeték nélküli ad hoc hálózat (VANET) (forrás: http://car-to-car.org)

A VANET alkalmazásai alapvetően három csoportra oszthatók:

- közlekedésbiztonságot javító alkalmazások
- közlekedés hatékonyságát növelő alkalmazások
- információs szolgáltatások

A **közlekedésbiztonság** javítására a következő alkalmazások használhatók.

Ráfutásos balesetet megelőző alkalmazás

A ráfutásos balesetek jelentős hányadát adják az összes baleseti számnak. Fő okai a vezetői figyelmetlenség és az elöl haladó jármű hirtelen fékezése. Normál körülmények között az egymás közelében haladó, hálózati eszközzel felszerelt járművek folyamatosan információkat küldenek egymásnak a pozíciójukról, sebességükről és irányukról. Ahhoz hogy a ráfutásos baleseteket elkerüljék, a járművek figyelik a sofőr tevékenységét és - a kapott információk alapján - a szomszédos járművek viselkedését. Ha a jármű veszélyes megközelítést érzékel, vagy egy másik közeli jármű vészjelzést ad, akkor hang- és fényjelzéssel figyelmezteti a vezetőt. Egy ilyen rendszer feltételezi a nagyon pontos pozícióméréset, valamint a környező járművektől érkező adatok megbízhatóságát. Az alkalmazás működéséhez elegendő lehet a singlehop üzenettovábbítás, azaz minden jármű csak a saját adó-vevő körzetében (kb. 200 m) lévő járművekkel kommunikál.

Ütközésdetektáló alkalmazás

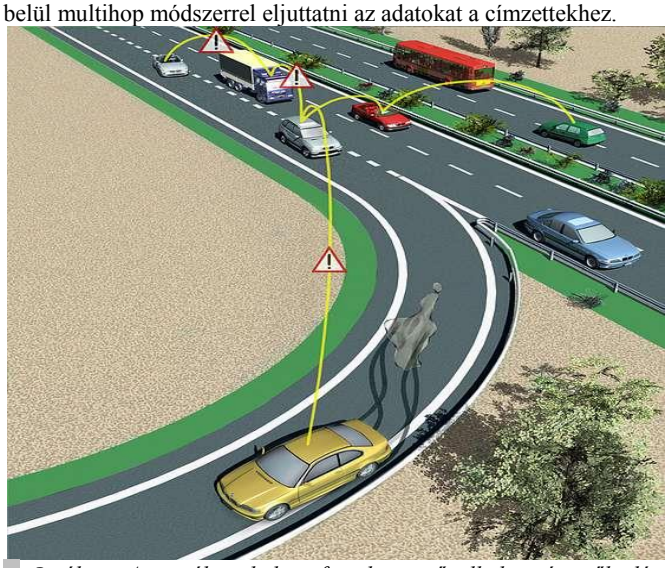
Ez az alkalmazás tulajdonképpen a ráfutásos balesteteket megelőző alkalmazás folytatásának is tekinthető. Ennek során feltételezzük, hogy az ütközés elkerülhetetlen. Hasonlóan az előzőekben leírtakhoz, itt is fontos a pozíció, irány és sebesség adatok folyamatos küldése. Amikor olyan szituáció lép fel, hogy az ütközést már semmilyen módon nem lehet elkerülni, akkor a résztvevő járműveknek végre kell hajtaniuk egy nagyon gyors és megbízható adatcserét. Ennek során pontosítják a pozícióadatokat és további járulékos adatokat (pl.: a jármű tömege) is küldenek, amelyek segítik a biztonsági berendezések megfelelő működtetését. Ezen adatok alapján mindkét jármű felkészül az ütközésre, meghatározza a légzsák, az övfeszítő és az egyéb passzív biztonsági eszközök működési paramétereit.

Az előzőhöz hasonlóan itt is nagyon fontos a pontos pozícióméres és az adatok megbízhatósága, és szintén elegendő a singlehop adatküldés.

Veszélyes útszakaszra figyelmeztető alkalmazás

Az alkalmazás célja, hogy a járművek figyelmeztessék egymást, amennyiben veszélyes útszakaszra (pl.: kátyú, csúszós út stb.) érnek. A fő feladat ebben az esetben az út tulajdonságainak meghatározása. Az egyik kiindulási alap lehet a menetstabilizáló rendszer aktivitása. Ezt az információt, a pontos pozícióval együtt szét lehet küldeni egy adott körzet járműveinek, így figyelmeztetni lehet a vezetőt a veszélyes útszakaszra. A rendszer kiterjeszthető útmenti berendezésekre is. Ezek figyelmeztethetnek többek között útépítésre, sávelhúzásra, sebességkorlátozásra.

Ennél az alkalmazásnál már nem elég a singlehop adatátvitel, mivel az adatokat néhány kilométeres körzetben érdemes továbbítani. Ezért az adatátviteli rendszernek képesnek kell lennie egy adott területen belül multihop módszerrel eljuttatni az adatokat a címzettekhez.



3. ábra: A veszélyes helyre figyelmeztető alkalmazás működése (forrás: http://car-to-car.org)

A következő nagyon fontos alkalmazási csoport a **közlekedés hatékonyságát** növeli. Hasonlóan nagy fontossággal bír, mint a biztonsági alkalmazások, hiszen a közúti közlekedés másik nagy problémáját hivatott enyhíteni. A lehetséges alkalmazások a következők.

Fejlett útvonaltervező és navigációs alkalmazás

Ez a rendszer az eddigiektől eltérően útmenti infrastruktúrát is igényel. A járművek a kihelyezett elérési pontokon keresztül letöltik a szükséges forgalmi információkat, amelyek segítik az optimális útvonal meghatározását. Egy ilyen alkalmazás feltételez egy nagyon fejlett közlekedési információs hálózatot, amely körzetekre lebontva folyamatosan friss forgalmi adatokkal rendelkezik. Természetesen itt is nagyon fontos az adatok megbízhatósága, mert rosszindulatú támadásokkal komoly torlódásokat is elő lehet idézni egy adott útszakaszon.

Intelligens kereszteződés

Ebben az esetben is részben infrastrukturális hálózatról beszélhetünk. A jelzőlámpás csomóponthoz érve a járművek kapcsolódnak a forgalomirányító berendezéshez és elküldik adataikat (pozíció, sebesség, irány stb.), valamint letöltik a kereszteződés elsőbbségi viszonyait és a jelzőlámpák állapotát. A kapott adatok és előre meghatározott kritériumok alapján a forgalomirányító berendezés előállítja a fázis-időtervet. A rendszer ezen felül képes elsőbbséget biztosítani a megkülönböztető jelzéssel ellátott járműveknek, valamint a járművek a jelzőlámpa adatai alapján segíthetnek a vezetőnek az optimális sebesség megválasztásában.

Besorolást segítő alkalmazás

Ez az alkalmazás segítséget nyújthat a járművezetőnek biztonságosan besorolni egy másik sávba anélkül, hogy az adott sáv

forgalmi áramlatát megtörné. Amikor egy a jármű például egy autópálya feljárón halad, akkor elkezd kommunikálni a közelben lévő és a manőverben érintett járművekkel. A besorolni kívánó jármű kérést küld, amely jelzésre kerül az érintett járművezetők felé, akik például a belső sávba történő behúzódással segíthetik a besoroló járművet.

Oszlopban haladó járművek

Ez az alkalmazás azt a jellegzetes forgalmi szituációt kísérlik meg automatizálás által biztonságosabbá és költséghatékonyabbá tenni, amikor több jármű, hosszú távon, azonos útszakaszon halad. Különösen tehergépjárművek (nyerges vontatók) esetében lehet hasznos a követési távolság drasztikus csökkentése, mivel így a légellenállás

Az információs szolgáltatások közé soroljuk azokat, amelyek nem közvetlenül a biztonság vagy a hatékonyság növelését szolgálják. Ezek elsősorban kényelmi és üzleti jellegű információkat szolgáltatnak. Ezek közül a főbb szolgáltatások a következők.

Internetelérés

E funkció révén bármilyen IP alapú szolgáltatás elérhetővé válhatna a járművekben. A rendszerhez szükség van útmenti internetelérési pontokra, amelyek hálózati átjáróként is funkcionálnak. Ha egy jármű nem tartózkodik egy elérési pont szolgáltatási területén sem, akkor a többi járművön keresztül multihop adatúton keresztül létesíthet internet kapcsolatot.

Hasznos helyek jelzése (Point of Interest)

A hasznos helyek jelzése (POI) nagyon sok lehetőséget rejt magában, kezdve a közeli benzinkutak felsorolástól egészen a turisztikai látnivalók bemutatásáig. Az előzőhöz hasonlóan ez is kényelmi funkció, azonban ebben nagyon sok szolgáltató cég érdekelt lehet, ami meggyorsíthatja a fejlesztést.

Távdiagnosztika

A vezeték nélküli hálózati adapterek kiválthatják a járművek diagnosztikai csatlakozóját, ami gyorsabbá és kényelmesebbé teszi a járművek szervizelését.

Díjfizetés

Ide tartozik minden olyan alkalmazás, amely pénzügyi tranzakció lebonyolítását igényli. Használható útdíj, parkolási díj és egyéb helyfüggő szolgáltatások díjának kifizetésére. Ez az alkalmazás van leginkább kitéve a rosszindulatú támadásoknak.

BIZTONSÁGI KÉRDÉSEK

Mielőtt megoldásokat keresnénk a rendszer biztonsági funkcióinak ellátására, fel kell tárnunk a lehetséges veszélyforrásokat. Fontos a tipikusan járművek közötti vezetéknélküli hálózatok esetében fennálló támadási lehetőségek feltárása, hogy a biztonsági részek tervezése során megtaláljuk az optimális megoldásokat. Az alkalmazástól függően három csoportra oszthatjuk a veszélyforrásokat:

Támadás a biztonsági alkalmazások ellen

A biztonsági alkalmazások a legfőbb ösztönzői a járművek közötti kommunikációs fejlesztéseknek. A magas fokú megbízhatóság mellett, hasonló mértékben kell figyelembe venni a biztonságot is az ilyen alkalmazások fejlesztésénél. Hiszen egy ilyen támadás nem csak kellemtelenséget okozhat (pl.: forgalmi dugók), hanem akár halálos kimenetelű balestet is okozhat.

Támadás a díjfizetést támogató alkalmazások ellen

A járművek közötti kommunikációs alkalmazások egy részét pénzügyi tranzakciók lebonyolítására fejlesztik (pl.: útdíj fizetés, helyfüggő szolgáltatások stb.). Emiatt feltétlenül számítani kell a pénzügyi rendszer elleni támadásokra, különösen a vezeték nélküli hálózatok nyitottsága miatt.

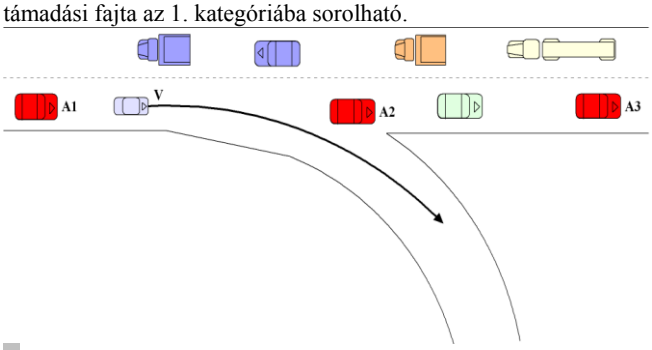
Támadások a magánszféra ellen

Az egyik legnagyobb nyugtalanságot a magánszféra védelmének kérdése váltja ki a jövőbeni járművek között hálózatokkal kapcsolatban. Tény, hogy ha megvalósul a járművek közötti információcsere, akkor könnyen lehetővé válik a járművek (és utasaik) követése.

A következőkben bemutatásra kerül néhány példa a járművek közötti hálózatokban végrehajtható támadásokról.

Hamis információ

Ebben az esetben a támadó téves információkat sugároz a hálózatban, hogy ezzel befolyásolja a járművezetők döntéseit. Például az 4. ábrán néhány sofőr összejátszik a gyorsabb haladás érdekében. Az A2-es jármű üzeneteket küld, hogy jelezze az összes őt követőnek, hogy nem messze torlódás alakult ki az úton. Ez azt eredményezi, hogy ezek a járművek megváltoztatják az útvonalukat (letérnek egy másik útra), hogy elkerüljék a torlódást.. Emiatt az A1-es jármű előtt felszabadul az út, és így gyorsabban haladhat. A fent leírt okok észszerűnek tűnnek, azonban van egy veszélyesebb támadási indok is, amit ugyanezzel a módszerrel lehet megvalósítani. Előfordulhat, hogy torlódást akarnak generálni egy adott útszakaszon bűncselekmény előkészítésének céljából. Ez a támadási fajta az 1. kategóriába sorolható.



4. ábra: Hamis információ küldésén alapuló támadás

A hálózat működésének akadályozása (Denial of Service)

Az ilyen jellegű támadások célja, hogy meggátolja a biztonsági célú funkciók működését. Nagyon sokféle módja van a támadások kivitelezésének. Akár olyan üzenetek küldésével, amely hibás működést eredményez, akár a vezeték nélküli csatorna zavarásával, ami azt eredményezi, hogy a járművek nem tudják továbbítani a biztonsági jellegű üzeneteiket. A DoS támadás annyira megzavarja a vezetéknélküli csatornát, hogy az nem képes a további kommunikációra. Ez a támadási fajta használható a biztonsági és az díjfizetést támogató alkalmazások ellen is. Ez az egyik legnagyobb biztonsági probléma a járművek közötti hálózatokban.

Azonosító, sebesség, vagy pozíció adatokkal megváltoztatása

Bizonyos baleseti szituációkban, ahol a felelősség megállapítása bonyolult, a járművezetőknek érdekében állhat meghamisítani a járművük pozíciójára vonatkozó információkat. Ezt elősegítheti a pozíció adatainak megváltoztatásával. Ahhoz, hogy az ilyen rendszerek a későbbiekben a jog által is elismertek legyenek, ezeket a biztonsági problémákat is ki kell küszöbölni. Más példa lehet az

azonosító megváltoztatása, amely a díjfizetési alkalmazások elleni támadásokkor lehetnek célra vezetők.

Azonosító feltörése

Ez esetben az ún. „Nagy Testvér” szituáció valósul, amikor egy megfigyelő követi a járműveket, hogy az így szerzett adatokat később felhasználhassa (pl.: konkurens cég utáni kémkedés). A megfigyeléshez a támadó átveszi a hatalmat az út menti infrastruktúra, vagy a járművek kommunikációs számítógépei felett vírusok vagy kémszoftverek segítségével. Ilyen formán a támadó passzív, lehallgatja a környeztében lévő járműveket, emiatt az ilyen fajta támadás, gyakorlatilag észrevehetetlen. Ez a támadás az utolsó kategóriába sorolható.

Amint a fenti példákból jól látható, nagyon sok biztonsági problémát felvet a VANET-ek használata. A vezeték nélküli hálózatok sebezhetősége hamar nyilvánvalóvá vált a személyi számítógépek közötti hálózatok esetében is. Azonban a közlekedési területen való alkalmazásuknak jóval nagyobbak a kockázatai. Alapvető elvárás az adatok megbízhatósága és biztonságos továbbítása.
További kérdést vet fel azonban a forgalomban résztvevők azonosíthatósága. A rendszer működése szempontjából megfelelőek az anonim járművek, és ennek a technikai feltételei is adottak. Azonban így nagyon nehézzé válik a támadások kivédése, valamint a rendszer alkalmatlanná válik a felelősségi kérdések megválaszolására. Ha minden jármű egyedi azonosítóval rendelkezik, akkor egy baleseti szituációt sokkal könnyebb rekonstruálni. Ez azonban minden bizonnyal társadalmi ellenállásba ütközne, hiszen így nagyon könnyen megfigyelhetővé válnak a járművek.

ÖSSZEFOGLALÁS

A cikk elsőként a mobil ad hoc vezeték nélküli hálózatok (MANET) alapvető jellemzőit tárgyalja. Kitért az ilyen hálózatok speciális tulajdonságaiból eredő megoldandó problémákra. Csoportosítja és bemutatja a közúti közlekedés területén használható MANET-et igénylő alkalmazásokat. Megvizsgálja az előre láthatólag számításba jöhető veszélyforrásokat és példákat mutat be.
Mindezekből az alábbi következtetéseket hoztuk. Funkcionálisan a legnagyobb nehézséget a dinamikusan változó hálózati topológia jelenti. Ez megnehezíti az útválasztó algoritmusok kifejlesztését,valamint csak valószínűségi QoS paraméterek meghatározását engedi.
Biztonsági szempontból a legnagyobb probléma, hogy a hálózat bárki számára hozzáférhető. Így bárki által lehallgatható, valamint könnyen korlátozni lehet a működését egyszerű DoS támadásokkal. Ezért nagyon fontos az adatok titkosítása, valamint a hálózat fizikai rétegében speciális átviteli módszerek kidolgozása a DoS támadások kivédésére. Végül nagy hangsúlyt kell fektetni a magánszféra védelmére, egyrészt a már említett titkosítással, másrészt a megfelelő azonosítási technikák kidolgozásával.

Irodalom

[1] Raya, M., and Hubaux, J-P.: "Securing vehicular ad hoc networks", Journal of Computer Security 15, 2007, pp. 39-68.
[2] Raya, M., and Hubaux, J-P.: "Security Aspects of Inter-Vehicle Communications", 5th Swiss Transport Research Conference, 2005
[3] Raya, M., Papadimitratos, P., Hubaux, J-P.: „Securing Vehicular Communications”, IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, October 2006
[4] Raya, M., and Hubaux, J-P.: „Securing vehicular ad hoc networks”, Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks, Vol. 15, Nr. 1, pp. 39 - 68, 2007
[5] Jun-Zhao Sun: „Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing”, Proc. International Conferences on Info-tech & Info -net, Beijing, China, 2001.
[6] http://car-to-car.org
[7] Car2Car Communication Consortium Manifesto, version 1.0, 21st May 2007
[8] http:// www.cvisproject.org
[9] http://www.safespot-eu.org/