

Bezvadu tīklu drošības risinājumi reāla laika lietojumiem

Aigars Riekstins, *Riga Technical University*

Kopsavilkums. Rakstā tiek sniegti 802.11 bezvadu lokālo datortīklu reāla laika parametru mērījumi saistībā ar izvēlēto kriptēšanas veidu. Tīkla parametru pētījumi veikti lauksaimniecības tehnikas darbības atbalsta tīkla kontekstā ar mērķi - aizvietot esošās vadu savienojuma sistēmas ar standarta 802.11 bezvadu risinājumu. Pēdējo gadu laikā lauksaimniecības tehnika tiek virzīta lielākas automatizācijas un ciešākas pārvaldības virzienā. Šie mērķi pieprasa liela apjoma datu komunikācijas iespēju savienojumā ar reāla laika uzdevumu atbalstu vienotā bezvadu infrastruktūrā. Dotajā darbā sniegtais tīkla reāla laika parametru novērtējums balstās uz tīkla mērījumu veikšanu kontrolētos apstākļos un tiek veikts salīdzinājums ar 802.3 Ethernet tīkla darbību līdzīgos apstākļos.

Atslēgas vārdi: bezvadu tīkli, tīkla parametri, reāla laika sistēmas, tīklu parametru mērījumi.

I. IEVADS

Modernā lauksaimniecības tehnika kļūst arvien datorizētāka. Šī datorizācija pamatā tiek veikta darbinieku darba apstākļu uzlabošanai un lauksaimniecībā izmantojamo ierīču (piemēram, traktora) vai to un apstrādes iekārtas pārvaldībai[1][2].

Šodien traktoru un to pievienoto ierīču vadība tiek veikta, izmantojot sadalītās skaitļošanas sistēmas, kuras komponentes tiek apvienotas, izmantojot standartizētas sakaru sistēmas, kas bāzētas CAN kopnes standartā.

Šīs kopnes un protokoli ir standartizēti specializētā ISOBUS reāla laika standartā [6][7]. Šāds standarts ļauj apvienot vienotā sistēmā dažādu ražotāju ierīces un pārvaldīt tās vienkopus no traktora centralizētās vadības konsoles.

Šodien ISOBUS standarts labi kalpo vienas apstrādes kompleksa ietvaros, bet tā paplašināšana uz lielākām vienībām, piemēram, vairāku traktoru vienlaicīgu vadību ierobežo CAN kopnes savienojumu sistēma.

Ņemot vērā šo attīstības tendenci un vēloties izmantot atkal jau standarta sistēmas un protokolus, šodien tiek veikts darbs pie bezvadu savienojuma sistēmas standarta izveides [3].

Šādas sistēmas balstīsies uz Wi-Fi 802.11 standarta aparatūras un Interneta protokola bāzes. Izvēlētā aparatūras standarta platforma automātiski garantē globālu sadarbības iespēju, jo spektra joslas ISM apgabalā ir rezervētas visā pasaulē. Tas ir ļoti nozīmīgi globālās ekonomikas un brīvā tirgus apstākļos, jo neprasa ražotājam piegādāt reģionam vai valstij specifisku ierīču kompleksu vai veikt tā konfigurāciju atkarībā no ģeogrāfiskā izvietojuma.

ISM joslas izmantošana nav jāsaskaņo ar valstu elektromagnētiskā spektra uzraudzības iestādēm un aparatūras saderību garantē WiFi sertifikācijas process.

Šādi definētā vidē projekta [3] ietvaros tiks izstrādāts izosinhronas pārraides protokols, kuru standartizēs globālā mērogā. Šim protokolam būs divas daļas: pirmā - reāla laika darbības režīms, un otrā - liela apjoma datu pārsūtīšanas režīms bez laika garantijām.

Otrā protokola daļa var izmantot jau esošo Interneta TCP/IP protokolu kopu, bet pirmajai daļai ir jārisina konkrētā lietošanas veida uzdevumi noteiktos laika limitos. Šos uzdevumus raksturo reāla laika un darbību drošuma garantēšanas aspekti, kas izslēdz TCP/IP protokola kopas izmantošanu tās informācijas piegādes laika nenoteiktības dēļ.

Līdz ar to tiek strādāts pie jauna lietojuma līmeņa protokola izveides, kas savu mērķu realizācijai izmantos UDP/IP protokolu kopu.

UDP protokola vājās vietas (pakešu zuduma atsekošanas un piegādes garantijas) atsvērs lietojuma līmeņa protokols.

Lai novērtētu esošās 802.11 standarta ierīču spējas nodrošināt minimāli nepieciešamos parametrus, ir jāveic to veikspējas testi scenārijiem, kas tuvināti aprakstītās sistēmas darba režīmam.

Citi pētījumi ir jau veikti šajā laukā, un dotā raksta autors vēlas atkārtot to rezultātus, lietojot jaunākas versijas Linux kodolu (2.6.33.7.2) un atbilstošu lietojuma līmeņa analogu.

II. LIETOJUMA LĪMEŅA PROTOKOLS

Standarta izstrādes procesā pieņemtais lietojuma scenārijs pieņem, ka brīvi izvēlētā laika momentā vairāki neviendabīgas konfigurācijas mezgli veido sakaru sesiju savā starpā bezvadu 802.11 tīkla ad-hock režīmā.

Lietojuma līmeņa sesijā vadītājerīces lomu izvēlas un piešķir operators. Izvēlētā vadītājerīce uzsāk sakaru seansu esošajā vidē un nodod sekotājerīcēm savu statusa informāciju un ierīču veicamo uzdevumu aprakstu. Sekotājerīces atbild ar apstiprinājuma ziņojumiem, un nepieciešamības gadījumā tās var pievienot atbildei arī savu informāciju par stāvokli un iestatījumiem dotā darba kontekstā.

Ņemot vērā iesaistīto ierīču un traktortehnikas pārvietošanās dinamiku un iesaistīto ierīču masu, šādas sistēmas komunikācijas vides latentums nedrīkstētu pārsniegt dažus simtus milisekunžu[1].

Pēc sakaru seansa izveidošanas iesaistītās ierīces turpinās apmainīties ar dažāda veida datiem ne vairāk kā 500 baitu apjomā. Šī apmaiņa prasa ievērot reāla laika intervālus ne lielākus par 50 milisekundēm.

Ņemot vērā to, ka moderna lauksaimniecības tehnika satur arī skaitļošanas komponentes, kas nodrošina to nepārtrauktu saikni ar visas saimniecības pārvaldības sistēmu, ir nepieciešams standartizēt arī šo datu plūsmas veidu. Standartā

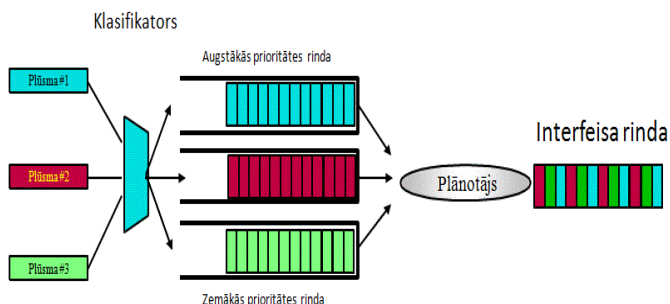
ir paredzēts tas, ka šīs komponentes saviem sakariem izmantos GPRS/UMTS liela attāluma sakaru kanālus. Līdz ar to šajā darbā standarta otrās daļas datu plūsmas netiek apskatītas. Šo datu plūsmu iespajds tiek iekļauts testa sistēmā kā fona CPU noslodze, ko radītu šādu datu nosūtīšana vai uztveršana.

III. LIETOJUMA APRAKSTS

Apskatot iespējamos tīkla lietojuma scenārijus, kā komunikācijas protokols tika izvēlēts UDP protokols. Šī izvēle balstās uz UDP protokola piemērotību reālā laika uzdevumiem [4].

UDP ziņojumi šīs sistēmas kontekstā ir nekas cits, kā atsevišķi datu bloki, kas rodas vadītājierīcē un kurus tā nosūta citām ierīcēm, izmantojot Linux standarta ligzdu (socket) interfeisu.

Linux tīkla steks pieļauj veidot prioritātes ienākošām un izejošām ziņojumu kopām [5]. Šī funkcionalitāte tiek izmantota šajā darbā, realizējot izejošās plūsmas pārvaldību, ar mērķi nodrošināt tai reālā laika prioritāti (ar klasifikatora palīdzību ievietojot UDP plūsmu augstākās prioritātes rindā atbilstoši pirmajam attēlam).



1. att. Linux tīkla plūsmu prioritāšu pārvaldība.

Ienākošās plūsmas prioritātes netika realizētas, jo mezglis, kurš strādā atbilstoši 802.11 DCF funkcijai, nespēj iespaidot sevī ienākošās plūsmas, veicot kaut kāda veida lokālu apstrādi.

Katrā ziņojumā pārsūtāmās informācijas apjoms tiek ierobežots ar 500 baitiem, ne tikai pagaidām apskatāmo lietojuma veidu prasību dēļ, bet arī tāpēc, lai nodrošinātos pret pakešu fragmentācijas iespējamo rašanos un problēmām, kas ar to saistās [8].

Visu iepriekš minēto pieņēmumu rezultātā tika izveidota sekojoša datu ziņojuma forma ziņojumiem no vadītājierīces:

1. Ziņojuma secības numurs.
2. Laiks, kad tiek uzsākts ziņojuma ģenerēšanas cikls.
3. Laiks, kad tiek izbeigts ziņojuma ģenerēšanas cikls.
4. Laiks, kad ziņojums tiek nodots OS tīkla stekam.
5. Ziņojuma ķermenis.
6. Kontrolsumma.

Lai novērstu iespēju, ka ziņojuma saturs iespaido sistēmas parametrus, tika izvēlēts gadījuma skaitļu pildīts ziņojuma ķermenis.

Sekotājierīces atbild uz ziņojumiem ar sekojoša satura apstiprinājuma ziņojumiem:

1. Ziņojuma secības numurs, kuru bija norādījusi vadītājierīce.
2. Laiks, kad tiek uzsākts atbildes ziņojuma ģenerēšanas cikls.
3. Laiks, kad tiek izbeigts atbildes ziņojuma ģenerēšanas cikls.
4. Laiks, kad atbildes ziņojums tiek nodots OS tīkla stekam.
5. Kontrolsumma.

Visi ziņojumi tiek ievietoti datu buferī un eksperimenta beigu fāzē tie tiek ierakstīti csv formāta žurnāļfailos.

IV. TESTA SISTĒMAS APRAKSTS

Sistēma, kas realizē dotā veida protokola emulāciju, 802.11 bezvadu vairākpunktu tīkla vidē tiek realizēta RTU iekšstelpās, uzstādot divus papildus personālos datorus un izmantojot jau esošo bezvadu kadru tvērēju infrastruktūru. Testa sistēmas datori tiek apgādāti ar bezvadu tīkla kartēm, kuru Linux dziņi atbalsta 802.11 b/g standartus.

Izmantotās aparatūras apraksts dots pirmajā tabulā.

1. TABULA

IZMANTOTĀS APARATŪRAS PARAMETRI

Nosaukums	CPU	RAM	Tīklu pieslēgumi
TestaPC1	Pentium 4 2,66GHz	512MB	Divi 802.3 un viens 80.11b/g
TestaPC2	Pentium 4 2,66GHz	512MB	Divi 802.3 un viens 80.11b/g
Bezvadu kadru tvērējs	BCM4704 264 MHz	32MB	Viens 802.3 un viens 80.11b/g

Aparatūras izvēle ir pamatota ar Linux kodolā esošo aparatūras dziņu esamību un iespēju to konfigurēt darbam gan infrastruktūras, gan vairākpunktu darba režīmā.

Kā OS tika izvēlēta Debian Linux 6.0.2 versijas pakotne, kurā tiek papildus uzstādīts reālā laika kodols 2.6.33.7.2-rt30-1-686 no [9]. Visu versiju kodolu ielādes parametros tiek papildus norādīti ielādes parametri, kas atslēdz ACPI un APM apakšsistēmu darbību. Tas ir nepieciešams, jo minētās pārvaldības sistēmas ļoti negatīvi iespaido reālā laika parametrus. Šo vadības sistēmu iedarbības rezultātā datorā tiek radīti ar OS resursiem nevadāmi procesora noslodzes radoši procesi, kuru nepieciešamība reālā laika kontroles sistēmā ir apšaubāma.

Reālā laika kodols ir balstīts uz RT-Preempt [10] labojumu kopas, kuras tiek virzītas uz iekļaušanu kodola pamatkodā. Šie labojumi sniedz iespēju pārvērst Linux kodolu pilnīgi pārtraucamā (preemptable) procesā, realizējot sekojošas funkcijas:

1. Kodola iekšējās slēdzes primitīvu pārveidošana, izstrādājot tos no jauna.
2. Kodola kritiskās aizsargātās koda daļas pēc noklusējuma tiek pārveidotas ar pārtraucamām. Tās daļas, kas nedrīkst tikt pārtrauktas, tiek aizvietotas ar speciālu primitīvu.
3. Kodola cikliskām slēdzēm un semaforiem tiek piešķirtas prioritātes un tiek nodrošināta to pārmantojamība.
4. Pārtraukumu apstrādes moduļi tiek pārveidoti par pārtraucamiem kodola pavedieniem.
5. Kodola taimeru API tiek papildināts ar augstas izšķiršanas spējas taimeriem.

Bez kodola izmaiņām distributīvā tika veikta programmatūras minimizācija, atsakoties no visām lietojuma līmeņa ugunsmūra un lietojumu darbības kontroles sistēmām.

Katrā testa datorā tiek realizēti trīs tīkla interfeisi - bezvadu tīkla pieslēguma interfeiss bezvadu mērījumu veikšanai, divi 802.3 Ethernet interfeisi, kas nepieciešami salīdzinošam testam vadu infrastruktūrā un visas sistēmas pārvaldībai testu veikšanas un rezultātu nolasīšanas laikā.

Testa programmatūras komponentes tika realizētas POSIX standarta C valodā un kompilētas, izmantojot gcc[11] kompilatoru. Lietojumi ir realizēti kā vairāku pavedienu lietojuma līmeņa Linux lietotnes.

Visas lietotnes dalās sūtītāja un uztvērēja versijās. Visas lietotnes versijas testu laikā tiek darbinātas ar nice -5 un 89 līmeņa reālā laika sistēmas prioritātēm. Šāda izvēle ir izdarīta tāpēc, lai varētu garantēt testa lietotnei iespēju pārtraukt jebkuru citu OS procesu savas funkcijas realizācijas laikā.

Prioritātes, kas pārsniedz norādītās, ir nepieciešamas kritisku OS sistēmas procesu darbībai un to apturēšana uz tik ilgu laiku kā testu veikšana rada sistēmas darbības nestabilitāti (piemēram, disku satura pārvaldības procesi nespēj veikt savas funkcijas, kas noved pie to satura bojājumiem).

Pašā lietojumā kā reālā laika darbības atbalstoša funkcija tiek realizēta visu nepieciešamo datu struktūru rezervēšana RAM lietotnes palaišanas brīdī. Šī funkcionalitāte dod iespēju vēl vairāk minimizēt varbūtību, ka kāda piekļuve atmiņas apgabalam izsauks pieprasījumlapaspušošanas sistēmas izsaukumu un līdz ar to daudzkārt lielāku latentumu dotās lietojuma funkcijas izpildes laikā.

Gan sūtītāja, gan uztvērēja procesi sastāv no diviem pavedieniem, no kuriem viens realizē protokola darbības, saglabājot uztvertos datus atmiņas buferī, bet otrs pavediens ar zemāku prioritāti veic uzkrāto datu saglabāšanu diskā žurnālfailu veidā pēc tam, kad sistēmas izbeidz sadarbību eksperimenta beigu fāzē.

Rezultātā iegūtie žurnālfaili tiek apstrādāti MSOffice izklājprogrammā, izmantojot tur iebūvētās varbūtības pakotnes iespējas un skriptēšanas atbalstu.

Testu laikā katra sistēma realizē 10 000 ziņojumu apmaiņu, ģenerējot tos ikkatras 20 ms. Ziņojumi tiek iekapsulēti UDP paketēs, un šie ziņojumu kadri tiek pārraidīti fiziskā tīkla vidē 10 metru attālumā, izmantojot 802.11b signalizācijas shēmu, kuras teorētiskā caurlaides spēja ir 54Mbs. Signāla kvalitātes novērojumi testa laikā norāda uz kvalitātes novērtējumu ne zemāku par 80 %.

Lai novērtētu otras sistēmas atbildes laikus, abas sistēmas sinhronizējas ar NTP protokola palīdzību, un katrs ziņojums satur augstas izšķiršanas spējas taimera vērtību par katras veiktās darbības laiku.

Lai gan NTP protokols ir pietiekami precīzs vispārējiem lietojumiem, tā precizitāte nav pietiekama nanosekunžu laika atskaites sinhronizācijai. Tāpēc analīzes fāzē tiek lietoti tikai vienas sistēmas ģenerētās laika vērtības, salīdzinot tās savā starpā, bet pārējie rezultāti tiek noapaļoti līdz milisekunžu precizitātei.

Testu rezultātos tiek aprēķināti sekojoši parametri:

1. Laiks, kas tika patērēts sūtītāja pusē (laiks starp nosūtīšanas brīdi un atbildes par dotā ziņojuma saņemšanas brīdi).

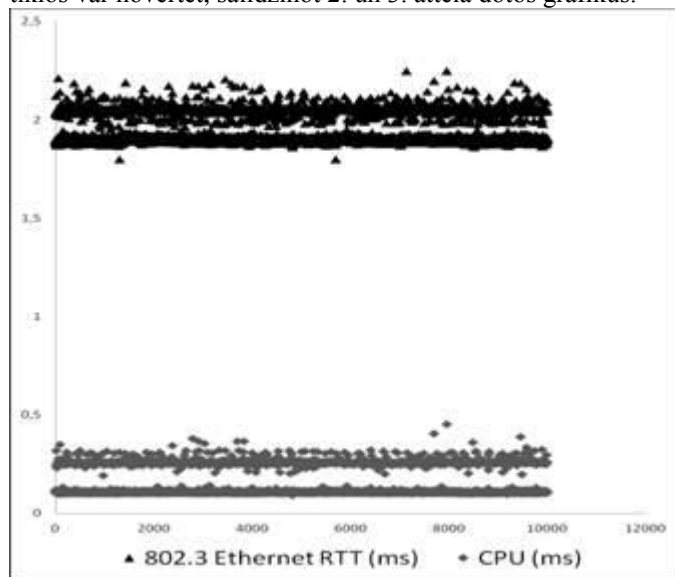
2. Laiks, kas pagājis starp diviem ziņojumiem, kas uztverti uztvērējā.

3. Standarta novirze, dispersija un vidējā vērtība visiem parametriem.

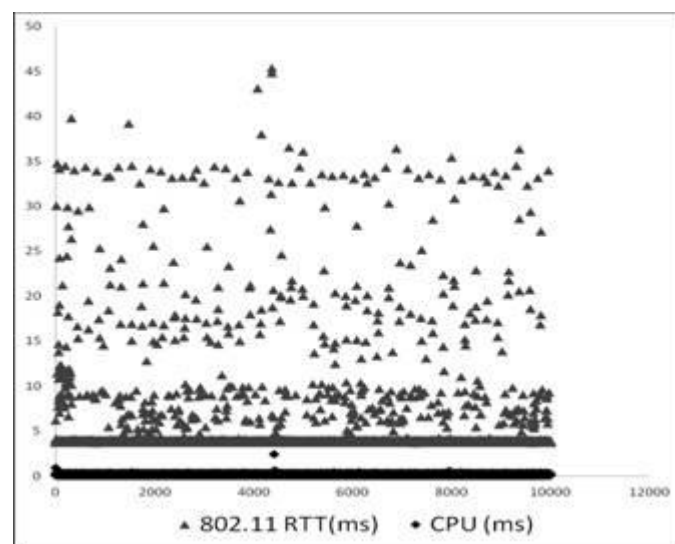
Visi testi tika veikti vispirms ar nemodificētu Linux kodolu un 802.3 vadu infrastruktūrā. Pēc pamata rezultātu ieguves tādi paši testi tiek veikti bezvadu interfeisu infrastruktūrā.

Pēc sistēmu pārstartēšanas testi tiek atkārtoti tieši tajā pašā secībā, tikai kodols saturēja jau RT labojumus.

Lokālās apstrādes un pārraides laikus vadu un bezvadu tīklos var novērtēt, salīdzinot 2. un 3. attēlā dotos grafikus.



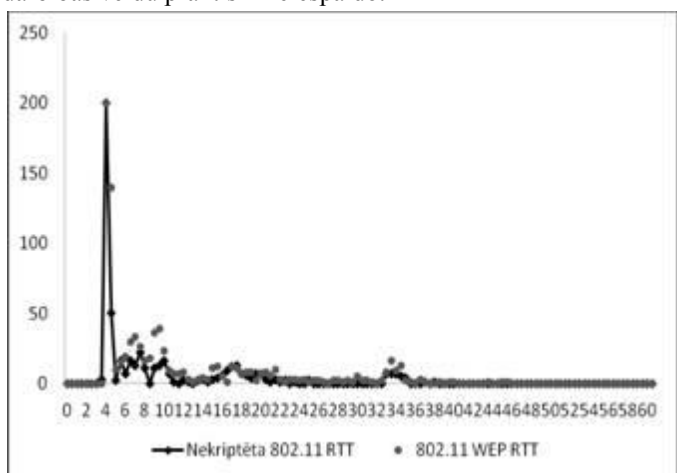
2. att. Vadu tīkla (802.3) apkārteļa un lokālās apstrādes laiki.



3. att. Bezvadu tīkla (802.11) apkārteļa un lokālās apstrādes laiki.

Šajos attēlos skaidri tiek atspoguļota bezvadu vides darbības atšķirība gan darbības laiku, gan to mainīguma ziņā. Nākamie testi tika veikti, izmainot bezvadu tīkla darbību no nekriptētas uz WEP standarta kriptēšanas veidu. Iegūtie rezultāti histogrammas formā parādīti 4. attēlā. Kā redzams,

vienkāršu bloka kriptēšanas algoritmu iespaids ir neliels un darbības veidu praktiski neiespaido.



4. att. Bezvadu tīkla (802.11) apkārtceļa laiku atkarība no kriptēšanas veida.

Lai novērtētu reālā laika kodolu labojumu un kriptēšanas iespaidu uz sistēmas parametriem, tika veikti sekojoši eksperimenti:

1. Ethernet 802.3 vadu tīkls bez RT kodola labojumiem.
2. Ethernet 802.3 vadu tīkls ar RT kodola labojumiem.
3. WiFi 802.11 bezvadu tīkls bez RT kodola labojumiem.
4. WiFi 802.11 bezvadu tīkls ar RT kodola labojumiem.
5. WiFi 802.11 bezvadu tīkls bez RT kodola labojumiem un ar WEP kriptēšanu.
6. WiFi 802.11 bezvadu tīkls ar RT kodola labojumiem un ar WEP kriptēšanu.

Reālā laika kodola labojumu iespaids un visu eksperimentu kopsavilkuma rezultāti tiek doti 2. tabulā.

2. TABULA
EKSPERIMENTU REZULTĀTU SALĪDZINĀJUMS

Ekspieriments	Vidējā RTT vērtība (ms)	Standarta novirze (ms)	Dispersija (ms)	Min. (ms)	Max. (ms)
1	1,71	0,067	0,0044	1,6	3,849
2	1,92	0,058	0,0033	1,8	2,249
3	4,37	3,228	10,4220	3,7	45,370
4	3,92	2,655	7,0472	3,4	45,896
5	5,21	4,308	18,5581	3,4	72,232
6	4,37	2,665	7,1025	3,4	37,855

No 2. tabulas ir redzams, ka RT Linux kodola labojumi sniedz daudz paredzamākus sistēmas darbības režīmus (samazināti novirzes un dispersijas rādītāji salīdzinājumā ar eksperimentiem bez reālā laika kodola labojumiem). Tāpat no šīs tabulas var novērtēt bezvadu tīkla kriptēšanas iespaidu uz sistēmas darbības režīmu, kas ir nenozīmīgs novirzes un dispersijas parametros un maznozīmīgs vidējā apkārtceļa laika ziņā.

V.SECINĀJUMI UN TURPMĀKĀ DARBA VIRZIENI

Šajā darbā tiek veikta lauksaimniecības iekārtu darbību atbalstošās bezvadu tīkla sistēmas lietojuma līmeņa analoga izstrāde un testēšana laboratorijas apstākļos. Eksperimentu rezultātā tika noskaidrotas iespējamās reālā laika sistēmas darbības robežas un šo robežu atkarība no bezvadu tīkla kriptēšanas. Esošo 802.11b standarta iekārtu un moderna Linux kodola apvienojums ar lietojuma līmeņa reālā laika lietojumu var nodrošināt pieprasīto 50 milisekunžu darbības režīmu gan kriptētā, gan nekriptētā veidā. Izmantojot 802.11g vai jaunākā 802.11n standarta aparatūru, šīs robežas būs iespējams ievērot ar vēl lielāku drošības rezervi, jo pakešu apstrādes laiks pašās sistēmās ir pietiekami zems un laika lielāko daļu veido datu noraidīšana un uztveršana fiziskajā vidē.

Dažāda standarta bezvadu iekārtu izmantošana vienā vairākpunktu bezvadu tīklā noved pie darbības režīma, kas ir līdzvērtīgs zemākās veikspējas tīkla režīmam, un tāpēc būtu nepieciešams standartā paredzēt iespēju lietot tikai viena bezvadu standarta ierīces.

Papildus apskatītajam vairākpunktu bezvadu tīkla darbības režīmam ar DCF funkciju ir nepieciešams izpētīt arī CDF funkcijas realizācijas iespaidu. Paredzams, ka hierarhiska tīkla infrastruktūra ļaus novērst bezvadu tīkla darbības nenoteiktību, samazinot sadursmju laikus bezvadu vidē.

Pirms bezvadu standarta galīgās izvēles ir nepieciešams veikt arī lauka izmēģinājumus. To ir iespējams veikt ar esošo testa sistēmu, vismaz pārvietojot to uz daudz piesātinātāku bezvadu tīklu vidi.

LITERATŪRAS SARAKSTS

- [1] Alfredo Revenaz, Massimiliano Ruggeri, Velio Tralli, *Low Latency WI-FI Real-Time Protocol for Agricultural Machines Synchronization Using Linux RT Kernel*. Proc. ISIE 2011, pp. 916 – 921.
- [2] Alfredo Revenaz, Massimiliano Ruggeri, Massimo Martelli, *Wireless Communication Protocol for Agricultural Machines Synchronization and Fleet Management*. Proc. ISIE 2010, pp. 3498 – 3504.
- [3] open System for TRAcTors' autonomouS Operations (STRATOS), [Online]. Available http://db-ictagri.eu/pub/Posting_ictagri_projects.php [Accessed: Sept. 1, 2011].
- [4] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, *RTP: A Transport Protocol for Real-Time Applications*, [Online]. Available <http://www.ietf.org/rfc/rfc1889.txt>, [Accessed: Sept. 1, 2011].
- [5] Linux Intermediate Queueing Device (IMQ) [Online]. Available <http://www.linuximq.net/> [Accessed: Sept. 1, 2011].
- [6] SAE J 1939, SAE International, [Online]. Available <http://www.sae.org/standardsdev/groundvehicle/j1939a.htm>, [Accessed: Sept. 1, 2011].
- [7] ISO 11783 Tractors and machinery for agriculture and forestry — Serial control and communications data network, 2009, ISO Geneva, Switzerland.
- [8] Kent, Christopher A.; Mogul, Jeffrey C., *Fragmentation Considered Harmful*, ACM SIGCOMM Volume 25 Issue 1, Jan. 1995 pp 75 – 87
- [9] Realtime Linux for Debian [Online]. Available http://www.ptxdist.org/software/linux-rt/debian_en.html, [Accessed: Sept. 1, 2011].
- [10] The Real Time Preempt Patch [Online]. Available www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.33.7.tar.bz2 [Accessed: Sept. 1, 2011].
- [11] GNU Compiler Collection [Online]. Available <http://gcc.gnu.org> [Accessed: Sept. 1, 2011].

Aigars Riekstiņš Received B.E. degree in electrical engineering from Riga Technical University, Latvia, in 1998, and S.M. degree in 2002. He is a doctoral student at Riga Technical University since 2003. He received a postdoctoral grant from the EU.

From March 2002 till October 2010, he was a lecturer at Riga Technical University. Current and previous research interests include network measurement and multimedia systems design.

He is a member of IEEE Computer Society and ACM since 2002.

Aigars Riekstins. Wireless Network Security in Real-Time Applications

In this article a study of a wireless network system for agricultural facilities has been carried out. The proposed system consists of standard 802.11 hardware and Linux OS, which support application-level protocol of special usage case. Such protocol is developed right now in STRATOS project and therefore a test of such system real time response is needed. This research extends previously made tests with comparison of wired and wireless infrastructure and in particular discovers system working parameters with regard of encryption in wireless networks. For such tests systems analogue design was implemented in custom made application and testing was done in laboratory conditions. As a platform of choice Linux 2.6.33.7.2 kernel with RT preempt patches was chosen as it is heading for inclusion in mainline kernel tree. Experiments revealed the potential for real-time system operating limits and dependence of these limits on the wireless network encryption. The existing 802.11b standard equipment and a modern Linux kernel with real time patches give a combination that can provide real-time applications with the required 50-millisecond round trip time for both encrypted and unencrypted mode. Future testing can be extended with regard of external influences, for example, by performing field tests. Also there can be gains in usage of coordinated wireless infrastructure in point coordination function mode. This research also shows that by using the latest 802.11g or 802.11n standard hardware, the system will comply with given time limits with an even larger margin because measured packet processing time at systems is low enough (most of the time is spent in data reception and forwarding in physical environment). Test results show that the proposed system architecture is a promising solution for low latency communication in both industrial and mobile applications.

Айгарс Риекстиньш. Безопасность беспроводной сети в приложении реального времени

В данной работе рассматриваются беспроводные сети для поддержки применения их в сельскохозяйственных объектах. Сегодня для поддержки сельскохозяйственных машин разрабатываются стандарты, которые предлагают использование оборудования стандарта 802.11 и операционной системы Линукс, которые поддерживают частную задачу в виде протокола прикладного уровня. Такой протокол прикладного уровня разрабатывается в данный момент в проекте STRATOS и, следовательно, необходимо произвести тестирование таких беспроводных систем реального времени, исходя из их времени отклика. Эта работа расширяет производившееся ранее тестирование данного протокола в сравнении с проводной и беспроводной инфраструктурой и, в особенности, с учетом параметров шифрования в беспроводных сетях. Тестовая система была реализована в виде прикладной программы собственной разработки, и тестирование было произведено в лабораторных условиях. Аппаратурная платформа тестов состоит из двух персональных компьютеров общего назначения под управлением ОС Линукс 2.6.33.7.2 ядра с патчами реального времени. Такой выбор обусловлен продвижением этих патчей в основное дерево ядра Линукс и в имеющиеся в распоряжении вычислительные и системы на борту современной сельскохозяйственной техники. Эксперименты показали, что потенциал такой системы для поддержки приложения реального времени с запросами ко времени отклика составляет не более 50мс. Существующее оборудование стандарта 802.11b и современные Линукс ядра с патчами реального времени дают комбинацию, которая может обеспечить приложения реального времени с требуемой 50-миллисекундной времени отклика для зашифрованных и не зашифрованных режимов работы. Следующие тесты будут производиться в полевых условиях. Эксперименты также показали потенциал применения новых 802.11г/н стандартов, ибо измеренное время обработки значительно ниже времени приема/передачи в среде.