پژوهشگاه فضایی ایران

ISRC

مرکز تحقیقات فضایی

عنوان اختصاری پروژه: اینترنت اشیاء کشاورزی
کد پروژه: ۰۱-۹۹۹۷CNS
کد فعالیت: ۰۷-۰۱-۹۹۹۷CNS

تحلیل نیازمندی‌های کارکردی پلتفرم اینترنت اشیا (پروتکل‌های ارتباطی با اشیا– LAN)

کد سند: ۰۷/۰۶-۰۱/۹۹۹۷MSRI-CNS
شماره ویرایش: ۱/۱
طبقه‌بندی: عادی
تاریخ: ۹۷/۰۴/۱۶

تعداد کل صفحات: ۱۸ صفحه

(با احتساب برگ روی جلد)

استفاده از این سند صرفا توسط گیرندگان مجاز است.

بسم الله الرحمن الرحيم

شناسنامه سند

۱- مشخصات پروژه

عنوان کامل پروژه	**انجام مطالعات امکانسنجی و پیاده سازی ایده اینترنت اشیاء در حوزه کشاورزی**			**مدیر پروژه**	-
کد پروژه	CNS**۹۹۹۷-۰۱**	**پژوهشکده (حوزه) مجری**	مرکز تحقیقات فضایی	**تاریخ شروع پروژه**	۹۵/۰۲/۰۱
کد فعالیت	CNS**۹۹۹۷-۰۱-۰۷**			**تاریخ خاتمه پروژه**	۹۵/۰۹/۰۱

۲- مشخصات سند

عنوان سند	تحلیل نیازمندی‌های کارکردی پلتفرم اینترنت اشیا (پروتکل‌های ارتباطی با اشیا- **LAN**)			**تعداد صفحات**	
				کل سند	۱۸
طبقه‌بندی سند	عادی	**کد سند**	MSRI-CNS**۹۹۹۷-۰۱**/R-**۰۷/۰۶**		
ویرایش	۱/۱	**تاریخ ویرایش**	**۹۷/۰۴/۱۶**	**پیوست‌ها**	**۱۱**

۳- جدول تهیه، تایید و تصویب در پژوهشکده (حوزه) مجری

	سمت*	**نام و نام‌خانوادگی**	**امضا**	**تاریخ**
تهیه‌کننده(گان)	**رییس بخش طراحی و پیاده سازی نرم افزار**			
تاییدکننده(گان)	**رییس اداره برنامه ریزی**			
تصویب‌کننده	**رییس مرکز**			

*** برای مواردی که مجری، حوزه دیگری غیر از پژوهشکده است، مثل مراکز یا گروه‌های پژوهشی مستقل و ... از سمت‌های معادل بر اساس نظر رییس حوزه استفاده شود.**

شناسنامه سند (ادامه)

۴- جدول تایید و تصویب در پژوهشگاه

	سمت	نام و نام‌خانوادگی	امضا	تاریخ
تاییدکننده(گان)	مدیران مرکز طراحی و توسعه سامانه‌های فضایی یا مدیر پژوهش و فناوری (برحسب مورد)			
	سایر افراد (مانند معاون تضمین کیفیت، بهره‌بردار و ... براساس قرارداد یا نظر تصویب‌کننده و مدیریت کنترل پروژه)			
تصویب‌کننده	رییس مرکز طراحی و توسعه سامانه‌های فضایی یا معاون پژوهش و فناوری(برحسب مورد)			

۵- جدول توزیع نسخ (گیرندگان)

عنوان واحد	توزیع	عنوان واحد	توزیع
ریاست پژوهشگاه فضایی ایران		مدیریت راهبرد و طراحی ماموریت	
دفتر ریاست، روابط عمومی و امور بین الملل		مدیریت مهندسی سامانه‌های فضایی	
مدیریت حراست		مدیریت آزمون و عملیات میدان	
اداره امور حقوقی		**معاونت اجرایی**	
مدیریت نظارت و ارزیابی و پاسخگویی به شکایات		مدیریت توسعه منابع انسانی	
مدیریت بازرگانی خارجی		مدیریت پشتیبانی	
مدیریت طرح و برنامه	●	مدیریت امور مالی	
معاونت پژوهش و فناوری		اداره تشکیلات و بهبود روش‌ها	
مدیریت آموزش و تحصیلات تکمیلی		**سازمان فضایی ایران**	
مدیریت پژوهش و فناوری	✓	**پژوهشکده سامانه‌های حمل‌ونقل فضایی**	
مدیریت دانش		**پژوهشکده سامانه‌های ماهواره**	
معاونت تضمین کیفیت و ایمنی		**پژوهشکده مکانیک**	
مدیریت مهندسی تضمین کیفیت		**پژوهشکده مواد و انرژی**	
مدیریت کالیبراسیون و استاندارد		**پژوهشکده رانشگرهای فضایی**	
مدیریت ایمنی و محیط زیست		**مرکز تحقیقات فضایی**	✓
مرکز طراحی و توسعه سامانه‌های فضایی			
سایر گیرندگان:			

***توزیع نسخ بر اساس علامت‌های زیر انجام می‌شود:**

✓: سند برای این واحدها ارسال می‌شود.

●: سند برای این واحدها ارسال نمی‌شود و صرفا اطلاع‌رسانی می‌شود.

۶- تایید مرکز اسناد

مدیریت دانش (مرکز اسناد) پژوهشکده مجری
نام و نام‌خانوادگی: .....
تاریخ: .....
مهر و امضا

مدیریت دانش (مرکز اسناد) پژوهشگاه فضایی ایران
نام و نام‌خانوادگی: .....
تاریخ: .....
مهر و امضا

شناسنامه سند (ادامه)

۷- جدول مشخصات و شرح وظایف دست‌اندرکاران تدوین سند*

ردیف	نام و نام‌خانوادگی	آخرین مدرک تحصیلی	رشته تحصیلی	مرتبه علمی**	محل کار	شرح وظایف	درصد مشارکت
۱	دانشگاه امیرکبیر				دانشگاه امیرکبیر		۱۰۰
۲							
۳							
۴							
۵							
۶							
۷							
۸							
۹							
جمع							۱۰۰

*منظور کلیه افرادی است که در انجام فعالیت‌های مرتبط با این سند نقش اصلی داشته‌اند.

**برای اعضای هیات علمی از عناوین مربوط (استاد، دانشیار، استادیار، مربی) و برای دیگر پژوهشگران از عنوان کارشناس استفاده شود.

۸- دیگر همکاران تدوین سند*

ردیف	نام و نام‌خانوادگی	آخرین مدرک تحصیلی	رشته تحصیلی	مرتبه علمی	محل کار	نقش

* منظور کسانی است که ضمن مطالعه سند، نظرات قابل توجهی را در خصوص سند ارائه کرده‌اند. ویراستاران ادبی نیز در این جدول ذکر می‌شوند.

شناسنامه سند (ادامه)

۹- جدول مشخصات ناظر(ان)

ردیف	نام و نام‌خانوادگی	آخرین مدرک	رشته	مرتبه علمی	محل کار	توضیحات
۱	احسان پناهی	فوق لیسانس		کارشناس	مرکز تحقیقات فضایی	

۱۰- جدول سوابق ویرایش و تغییرات

ویرایش	تاریخ	شرح تغییرات	علت/مرجع تغییر	واحد تهیه‌کننده مسئول
۱/۱	۹۶/۰۴/۱۶	نگارش سند	-	-

چکیده

گزارش حاضر حاوی سند دریافتی از دانشگاه امیرکبیر (پیمانکار پژوهشگاه فضایی ایران در قرارداد "طراحی و پیاده سازی پلتفرم اینترنت اشیاء) با عنوان " تحلیل نیازمندی‌های کارکردی پلتفرم اینترنت اشیا (پروتکل‌های ارتباطی با اشیا- LAN)" می باشد.

واژه‌های کلیدی:

اینترنت اشیا، پلتفرم، کشاورزی هوشمند

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

ISRC

آزمایشگاه اینترنت اشیاء

گروه پلتفرم

عنوان سند:

تحلیل نیازمندی‌های کارکردی پلتفرم اینترنت اشیا (پروتکل‌های ارتباطی با اشیا– LAN)

کد سند:

IoT-IMP-LAN-v۱.۰

تاریخ:

۹۷/۰۱/۱٤

کلیه حقوق هر نوع استفاده از این سند نزد آزمایشگاه اینترنت اشیاء دانشکده مهندسی کامپیوتر و فناوری اطلاعات دانشگاه صنعتی امیرکبیر محفوظ می‌باشد.

بسم الله الرحمن الرحیم

اطلاعات سند

نام پروژه:	طراحی و پیاده‌سازی پلتفرم اینترنت اشیاء
نام سند:	تحلیل نیازمندی‌های کارکردی پلتفرم اینترنت اشیا (پروتکل‌های ارتباطی با اشیا-LAN)
کد سند:	IoT-IMP-LAN-v۱,۰
وضعیت:	نهایی
تاریخ انتشار نهایی:	---
نوع طبقه‌بندی سند:	محرمانه

تاریخچه بازبینی‌ها

ردیف	نام بازبینی کننده	تاریخ بازبینی	تغییرات
۱	تیم فنی	۹۶/۱۱/۱۰	بر اساس نظرات کارفرما در جلسه ۹۶/۱۱/۷
۲	تیم فنی	۹۷/۰۱/۱۴	ویرایش ادبی و فنی
۳			
۴			

چکیده

این سند در راستای شناسایی نیازمندی‌ها و طراحی پروتکل LAN برای اتصال اشیا، تنظیم و گردآوری شده است. با توجه به نیاز کارفرما علاوه بر پروتکل ارتباطی LoRaWAN، پیاده‌سازی پروتکل LAN نیز جز مواردی است که در توسعه پلتفرم اینترنت اشیا در نظر گرفته شده است.

فهرست مطالب

فصل ۱: طراحی پروتکل LAN ٦
۱-۱- مقدمه ٦
۱-۲- پروتکل پیشنهادی ۷
۱-۳- پوشش نیازمندی‌ها ۹

فهرست جداول

جدول (۱-۱) پوشش نیازمندی‌های پروتکل LAN..... ۹

فصل ۱:
طراحی پروتکل LAN

۱-۱- مقدمه

پلتفرم اینترنت اشیاء قابلیت اتصال اشیاء از طریق پروتکل LAN (خانواده IEEE ۸۰۲ و مشخصا IEEE ۸۰۲,۳، IEEE ۸۰۲,۱۱ و ...) را فراهم می‌کند. برای این منظور، پروتکل لایه کاربرد پیشنهادی در این مستند دو دسته‌ی کلی نیازمندی‌ها به شرح زیر را برآورده می‌کند:

۱. تبادل داده

۱,۱. ارسال داده از اشیاء به پلتفرم (Up-Link)

۱,۲. ارسال داده از پلتفرم به اشیاء (Down-Link)

۲. امنیت

۲,۱. احراز هویت پلتفرم توسط اشیاء (Platform Authentication)

۲,۲. احراز هویت اشیاء توسط پلتفرم (Thing Authentication)

۲,۳. محرمانگی (Confidentiality)

۲,۴. تمامیت (Integrity)

لازم به ذکر است که این پروتکل علاوه بر پلتفرم بر روی اشیاء نیز باید پیاده‌سازی گردد، بنابراین استفاده از پروتکل‌های استاندارد موجود برای این منظور (در عمل) الزامی است. در ادامه این سند، در ابتدا پروتکل پیشنهادی شرح داده شده و سپس نحوه تامین نیازمندی‌ها مشخص خواهد شد.

۱-۲- پروتکل پیشنهادی

پروتکل پیشنهادی از سه مرحله اصلی تشکیل می‌گردد:

۱. برقراری نشست (Session Establishment)
۲. احراز هویت اشیاء (Thing Authentication)
۳. تبادل داده (Data Communication)

هر یک از این مراحل در ادامه این بخش تشریح می‌گردد.

- **برقراری نشست**

در مرحله اول، با درخواست اشیاء برای اتصال به پلتفرم یک تونل SSL/TLS مابین شی و پلتفرم برقرار می‌گردد. در ایجاد این تونل موارد زیر در نظر گرفته شده است:

۱. الگوریتم‌های رمزنگاری متقارن (برای رمز داده) و الگوریتم‌های رمزنگاری نامتقارن (برای تبادل کلید) الگوریتم‌هایی است که در RFC ۵۲۴۶ و RFCهای مرتبط مشخص شده است.
۲. از گزینه اختیاری "Client Certificate Request" استفاده نشده است بنابراین اشیاء نیاز به داشتن Certificate ندارند که برای توسعه دهندگان اشیاء مزیت محسوب می‌شود.
۳. در زمان استفاده از این پلتفرم در محیط واقعی، Certificate استفاده شده برای پلتفرم باید توسط یک CA امضاء شده باشد که اشیاء یک کپی از Certificate آن CA را داشته باشند یا به نحوی امکان صحت‌سنجی آن Certificate توسط اشیاء (مثلا زیرساخت PKI) امکان‌پذیر باشد که جزییات آن خارج از محدوده این پروتکل پیشنهادی است.

- **احراز هویت اشیاء**

بعد از ایجاد تونل TLS، مرحله دوم این پروتکل اجرا می‌شود که در آن، هویت اشیاء توسط پلتفرم مورد تایید قرار می‌گیرد. برای احراز هویت اشیاء، در این پروتکل از jwt استفاده می‌شود که یک روش مبتنی بر

token می‌باشد که هم در پلتفرم و هم در شی پیکربندی می‌شود. شی می‌بایست از این token در تمام ارتباط‌های بعدی خود استفاده کند. همانگونه که ذکر شد، این فرایند بعد از ایجاد تونل TLS و با استفاده از پروتکل HTTP (به عبارت دیگر بر روی پروتکل https) انجام می‌گیرد. در ساخت این token از مقدار hash آدرس IP شی استفاده می‌شود. با توجه به این که هر شی در پلتفرم می‌بایست توسط یک شناسه یکتا مشخص شود، پیشنهاد می‌شود برای اشیایی که توسط این پروتکل به پلتفرم متصل میشوند، اشیا توسط آدرس IP و آدرس سخت افزاری MAC به صورت منحصر به فرد مشخص گردد.

در صورت احراز هویت موفق شی، طی یک سری پیغام handshake، شی به یک کانال socket.io مشخص شده توسط پلتفرم، subscribe می‌کند. جهت تامین امنیت این بخش، ارتباطات socket.io نیز بر روی تونل TLS ارسال می‌گردد (در حقیقت از مکانیزم wss استفاده می‌شود)

- **تبادل داده: ارسال داده‌ها از اشیاء به پلتفرم**

برای ارسال داده‌ها در این پروتکل از لایه‌ی انتقال TCP و پروتکل HTTP استفاده می‌شود. Gateway متصل به پلتفرم هیچ پردازشی روی داده‌ها صورت نمی‌دهد و آن‌ها را مستقیما به لایه‌ی بالاتر انتقال می‌دهد. در این بین تنها token شی از نظرت صحت بررسی می‌گردد. شی با استفاده از تقاضا POST داده را به endpoint پیشنهادی data/ بر روی پورت ۸۰ Gateway ارسال می‌کند. در ازای این تقاضا یک پاسخ مبنی بر دریافت gateway به شی ارسال خواهد شد.

- **تبادل داده: ارسال داده از پلتفرم به اشیاء**

سرور داده‌ها را از طریق ارتباط socket.io که پیشتر در فاز احراز هویت شکل گرفته است برای شی مورد نظر ارسال می‌کند. با توجه به اینکه این ارتباط در داخل یک تونل TLS انجام می‌گیرد، داده‌ها قابل شنود توسط سایرین نیستند علاوه بر آن ساختار این داده‌ها از منظر Gateway پنهان می‌باشد و توسط لایه‌ی بالاتر عمل encoding صورت پذیرفته است. همانگونه که ذکر شد، شی در مرحله احراز هویت با استفاده از http و پورت ۸۰ Gateway ارتباط socket.io را با سرور شکل می‌دهد و در ادامه داده‌ها در channelای با نام پیشنهادی data برای شی منتشر خواهند.

- **راه کارهای پیشنهادی**

در این پروتکل می‌توان جهت کاهش حجم داده‌ی انتقالی در صورت توافق با کارفرما از روش‌های compression استفاده کرد یا به جای استفاده از پروتکل HTTP از پروتکل سبکتر CoAP بهره برد.

۱-۳- پوشش نیازمندی‌ها

پروتکل پیشنهادی در مرحله قبلی، نیازمندی‌های ذکر شده در بخش ۱ را به شرح زیر پوشش می‌دهد.

جدول (۱-۱) پوشش نیازمندی‌های پروتکل LAN

ردیف	نیازمندی	نحوه پوشش
۱	تبادل داده Up-Link	ارسال بسته POST به End-Point مشخص شده
۲	تبادل داده Down-Link	تبادل داده بر روی socket.io
۳	Platform Authentication	Verify کردن Certificate پلتفرم توسط شی با استفاده از CA
۴	Thing Authentication	استفاده شناسه و رمز عبور در درخواست اول، استفاده از token در درخواستهای بعدی
۵	Confidentiality	الگوریتم رمزنگاری استفاده شده از TLS که هم بسته‌های HTTP و هم ارتباطات socket.io بر روی آن بستر انجام می‌شود.
۶	Integrity	الگوریتم HMAC استفاده شده از TLS