استفاده از اینترنت اشیا در محیط شبکه نظامی: چالش‌ها و راه‌حل‌ها

نیره قدیمی
فارغ التحصیل دکترای مهندسی برق، گرایش الکترونیک، دانشگاه تبریز

چکیده
فناوری اینترنت اشیا (IoT) با گسترش روزافزون خود، پتانسیل عظیمی برای تحول در عملیات نظامی دارد. با تبدیل دارایی‌های میدان جنگ به موجودیت‌های شبکه‌ای از طریق حسگرهای متعدد محیطی و شخصی، حجم وسیعی از اطلاعات دقیق و ظریف جمع‌آوری می‌شود. این اطلاعات می‌تواند به طور چشمگیری کارایی عملیات نظامی را در زمینه‌هایی مانند اطلاعات، نظارت و شناسایی (ISR)، خودکارسازی زنجیره تامین، و عملیات شهری در محیط‌های پیچیده کلان شهرها افزایش دهد. با این حال، دستیابی به این مزایا مستلزم پرداختن به چالش‌های کلیدی است. این چالش‌ها شامل سازگاری الگوهای معماری تجاری IoT با ساختارهای شبکه‌های نظامی، اطمینان از قابلیت همکاری بین سامانه‌های مختلف IoT، مدیریت و پردازش حجم عظیم داده‌ها، و توسعه راهکارهای میان‌افزار IoT با بازدهی بالا در مصرف منابع است. محیط شبکه‌بندی تاکتیکی که با محدودیت منابع دست و پنجه نرم می‌کند، این دستور کار تحقیقاتی را نه تنها چالش‌برانگیزتر، بلکه از نظر نیاز به نوآوری در میان‌افزار ضروری می‌سازد. این مقاله بر لزوم تحقیق و توسعه در این زمینه‌ها برای بهره‌برداری کامل از پتانسیل IoT در عرصه نظامی تاکید دارد.

واژگان کلیدی: کاربردهای سایبرفیزیکی، ارتباطات نظامی، اینترنت اشیا

مقدمه

اصطلاح "اینترنت اشیا" نسبتاً جدید است، اما ریشه عمیقی در زمینه‌های تحقیقاتی مختلف دیگر از جمله سامانه‌های سایبرفیزیکی، محاسبات فراگیر و همه‌جا حاضر، سامانه‌های تعبیه‌شده، شبکه‌های بی‌سیم اختصاصی تلفن همراه، شبکه‌های حسگر بی‌سیم، شبکه‌های تلفن همراه، محاسبات پوشیدنی، محاسبات ابری، تحلیل داده‌های بزرگ و همچنین عامل‌های هوشمند دارد [۱]. علاوه بر این، پیشرفت‌های اخیر در کوچک‌سازی، شناسایی فرکانس رادیویی(RFID) ، محاسبات کم مصرف و ارتباطات ماشین به ماشین (M۲M) رشد اینترنت اشیا را بیشتر تقویت کرده است و بخش‌های تجاری و صنعتی از قبل توجه قابل توجهی به این زمینه نشان داده‌اند. به عنوان یک فناوری عمدتاً تجاری، نوآوری‌ها در اینترنت اشیا ناشی از حوزه نظامی و مرتبط با آن تحت حوزه‌های موضوعی گسترده‌تر سامانه‌های سایبرفیزیکی و محاسبات تعبیه‌شده است. با این حال، تأثیر پیشرفت‌ها در اینترنت اشیا تجاری به دلیل رابطه ارتش با شرکای تجاری و صنعتی و فرآیندهای مربوطه، به طور فزاینده‌ای بر ارتش تأثیر خواهد گذاشت [۲].

ما انتظار داریم که پذیرش گسترده اینترنت اشیا حداقل در چهار حوزه کلیدی تأثیر بسزایی بر ارتش داشته باشد:

۱) پلتفرم‌های حسگری و محاسباتی جدید با ادغام در فرآیندهای نظامی
۲) پیشرفت‌ها در فعال‌کننده‌های اساسی اینترنت اشیا
۳) افزایش اطلاعات در دسترس
۴) تغییرات در دکترین (اصول و مبانی) مرتبط با در دسترس بودن و قابلیت‌های اینترنت اشیا

نخست، با توجه به محرک‌های بازار رقابت و صرفه‌جویی در مقیاس، اینترنت اشیا تجاری مدرن، پلتفرم‌های ارزان و قوی ارائه می‌دهد که می‌تواند برای تکمیل و گسترش قابلیت‌های حسگری و محاسباتی ارائه شده توسط تجهیزات درجه نظامی مورد استفاده قرار گیرد. بنابراین، انتظار داریم استقرار مشترک و همزیستی فناوری‌های تجاری اینترنت اشیا در مجاورت فناوری‌های نظامی سنتی را شاهد باشیم.

دوم، انتظار داریم که فعال‌کننده‌های اساسی اینترنت اشیا (به عنوان مثال، کوچک‌سازی، حسگرها، بهره‌وری انرژی و غیره) برای تجهیزات نظامی سنتی استفاده شوند. مجموعه پلتفرم‌ها، از کشتی‌ها گرفته تا هواپیما، وسایل نقلیه زمینی، ربات‌ها و سامانه‌های تسلیحاتی، تحت تأثیر فناوری‌های اینترنت اشیا قرار خواهند گرفت. علاوه بر این، با فراگیرتر شدن فناوری‌های اینترنت اشیا، تعداد "چیزهای" متصل می‌تواند افزایش یابد و شامل لوازم پزشکی، غذا، آب، مهمات و سایر مواد مصرفی و قطعات نیز بشود. تأثیر آن قابل توجه خواهد بود، از تعمیر و نگهداری به موقع گرفته تا کاهش زمان خرابی تا بهینه‌سازی در تدارکات و فرآیندهای زنجیره تأمین [۳].

سوم، انتظار داریم که اینترنت اشیا به منبع مهمی از اطلاعات برای عملیات نظامی، به ویژه در زمینه محیط‌های شهری مانند شهرهای هوشمند و کلان‌شهرها تبدیل شود. در واقع، سامانه‌های زیرساختی شهری، مانند سامانه‌های نظارت بر ترافیک، شبکه‌های هوشمند ابزار، سامانه‌های حمل و نقل عمومی، شبکه‌های نظارت تصویری و سایر خدمات ارائه شده توسط شهرها به منظور تأمین رفاه ساکنان، منبع ارزشمندی از اطلاعات و جایگزینی برای حسگرهای اختصاصی ساخته و مستقر خواهند بود [۴].

در نهایت، انتظار داریم که مفاهیم اساسی اینترنت اشیا به طور اساسی دکترین و تکنیک‌ها، تاکتیک‌ها و رویه‌های (TTP) میدان نبرد آینده را تغییر دهد، که یک محیط عملیاتی بسیار متصل، با استقرار خاص و گسترده سامانه‌های حسگر محیطی و شخصی با تراکم بالا خواهد بود. چشم‌انداز اینکه همه چیز در میدان نبرد یک موجودیت شبکه‌ای باشد، صرف‌نظر از اینکه چقدر کوچک یا بزرگ باشد، به

طور قابل توجهی پتانسیل آگاهی از موقعیت بهبود یافته در سطوح مختلف را افزایش می‌دهد، اما چالش‌های بسیاری را نیز ایجاد می‌کند که بعداً مورد بحث قرار خواهند گرفت [۵].

درست همانطور که ظهور شبکه‌های ارتباطی سرآغاز عصر جنگ شبکه‌محور بود، انتظار داریم که اینترنت اشیا سرآغاز عصر جدیدی از عملیات فعال شده توسط اینترنت اشیا باشد، با ظهور برنامه‌های سایبرفیزیکی نوآورانه و پیچیده. برنامه‌های خاصی که مطمئناً شامل نظارت بیومتریک سربازان، ارتباطات پیشرفته حرکتی، حسگری مشارکتی و جمعی، تهیه اطلاعات هوشمند از طریق واقعیت افزوده و تدارکات و اتوماسیون زنجیره تأمین خواهد بود [۶].

با این حال، پذیرش فناوری‌های اینترنت اشیا در زمینه نظامی چالش‌های تحقیقاتی خاصی را به وجود می‌آورد، از جمله قابلیت همکاری سامانه‌های نظامی با دستگاه‌های تجاری اینترنت اشیا و زیرساخت‌های اطلاعاتی شهری، فیلتر کردن و اولویت‌بندی اطلاعات برای اطمینان از پردازش و انتشار به موقع ارزشمندترین اطلاعات، و تجزیه و تحلیل داده‌های تولید شده توسط اینترنت اشیا برای اهداف آگاهی از موقعیت. همزیستی و استقرار مشترک سخت‌افزار تجاری اینترنت اشیا و نظامی نگرانی‌های امنیتی و تضمین اطلاعات را افزایش می‌دهد. بهره‌گیری از اطلاعات زیرساخت‌های تجاری مستقر شده در شهرهای هوشمند و سایر محیط‌های کنترل نشده، مسائل مربوط به فریب در اطلاعات جمع‌آوری شده را افزایش می‌دهد.

این مقاله یک نمای کلی از چگونگی تشدید چالش‌های تحقیقاتی مرتبط با اینترنت اشیا در محیط‌های تاکتیکی توسط محدودیت‌های منابع سخت‌گیرانه ارائه می‌دهد. به ویژه از نظر ارتباطات و قدرت، بلکه تا حدی با قابلیت‌های محاسباتی و ذخیره‌سازی نیز محدودیت وجود دارد. بخش‌های بعدی این نمای کلی، نیاز به راهکارهای میان‌افزار اختصاصی اینترنت اشیا را توصیف می‌کنند که ویژگی‌های خاصی را برای تسهیل توسعه و استقرار برنامه‌های اینترنت اشیا ارائه می‌دهند که به چالش‌های تحقیقاتی مرتبط با اینترنت اشیا در داخل و برای اهداف عملیات نظامی می‌پردازند. با توجه به اینکه موضوع کلی اینترنت اشیا در عملیات نظامی بسیار گسترده است و برای محدود کردن بحث، و همچنین ارائه تمرکز برای یک راهکار میان‌افزار پیشنهادی، این مقاله بر جنبه‌های ارتباطات و مدیریت اطلاعات چالش‌های اینترنت اشیا متمرکز است.

مزایای اینترنت اشیا تجاری برای سامانه‌ها و عملیات نظامی

همزیستی و استقرار مشترک فناوری‌های تجاری اینترنت اشیا و سامانه‌های نظامی بر بسیاری از جنبه‌های عملیات نظامی فعال شده توسط اینترنت اشیا تأثیر خواهد گذاشت. به منظور نشان دادن تأثیر این انقلاب، این بخش یک نمای کلی از آخرین وضعیت در راهکارهای تجاری اینترنت اشیا ارائه می‌دهد و پتانسیل‌های پذیرش آنها در محیط‌های نظامی را تجزیه و تحلیل می‌کند.

بررسی اجمالی فناوری‌های تجاری اینترنت اشیا

رشد تصاعدی بازارهای تجاری اینترنت اشیا، انبوهی از دستگاه‌های قدرتمندتر و با بازدهی انرژی بیشتر تولید می‌کند. اکثر این دستگاه‌ها بر روی پلتفرم‌های سخت‌افزاری سنتی ساخته شده‌اند که یا ریزپردازنده (به عنوان مثال، ARM Cortex A) یا انواع میکروکنترلر (به عنوان مثال، ARM Cortex M یا Atmel AVR) هستند. با این حال، راهکارهای سخت‌افزاری بسیار نوآورانه مبتنی بر پردازنده‌های نورومورفیک (مانند تراشه True North IBM)، CPU چند هسته‌ای هیبریدی (مانند برد Parallela Adapteva) یا معماری‌های CPU/FPGA (مانند Xilinx۷۰۰۰ SoC Zynq-) نیز در حال ظهور هستند. قابلیت‌های این پلتفرم‌ها امکان اجرای خدمات پیچیده و پرمصرف محاسباتی را در عین حال با بازدهی انرژی نسبتاً بالا فراهم می‌کند.

علاوه بر این، دستگاه‌های اینترنت اشیا با حسگرها و محرک‌های به طور فزاینده پیشرفته جفت می‌شوند. دستگاه‌های پوشیدنی مانند Myo Armbandقادر به تشخیص حرکات انسان و استفاده از آنها برای تعامل با سامانه‌های خودکار هستند. حسگرهای زیستی تجاری که به طور گسترده‌ای برای برنامه‌های تناسب اندام و مراقبت‌های بهداشتی مورد استفاده قرار می‌گیرند، همچنین امکان جمع‌آوری معیارهای بیولوژیکی مهم مانند ضربان قلب را فراهم می‌کنند تا تصویر جامعی از وضعیت سلامت فرد ارائه دهند. در حالی که تلاش‌های اولیه در دستگاه‌های شیشه هوشمند مانند Google Glass موفقیت‌آمیز نبود، به نظر می‌رسد نسل جدیدی از دستگاه‌ها مانندMicrosoft Hololens ، آماده ارائه اطلاعات مهم به صاحبان خود به شیوه‌ای مختصر، زمینه‌ای و غیر مزاحم از طریق فناوری‌های واقعیت افزوده است. این قابلیت‌های جدید امکان توسعه محیط‌های غوطه‌وری پیشرفته را فراهم می‌کند که در آن انسان‌ها می‌توانند با دستگاه‌های اینترنت اشیا و سامانه‌های خودکار به روشی طبیعی و مؤثر تعامل داشته باشند [۹-۱۰]

راهکارهای تجاری اینترنت اشیا همچنین نوآوری‌های جالبی را از منظر شبکه‌سازی به ارمغان می‌آورند. چندین استاندارد جالب برای ارتباطات برد کوتاه با توان کم در سال‌های اخیر پدیدار شده‌اند، از جملهIEEE ۸۰۲.۱۵.۴ و Bluetooth LE. تراشه‌های ارتباطی تجاری مدرن مانند فرستنده گیرندهTexas Instruments CC ۱۱۲۰۰، همچنین امکان پیوندهای دستیابی مجدد با برد بسیار طولانی (بیش از ۲۰ مایل دید مستقیم) را با وجود پهنای باند کم (کمتر از ۱۰ کیلوبیت بر ثانیه) فراهم می‌کنند. جفت شده با راهکارهای انطباق مانند ۶LoWPANوBNEP ، این استانداردها با فعال کردن ارتباطات مبتنی بر IP در بالای دستگاه‌های اینترنت اشیا، دامنه جدیدی از امکانات را باز می‌کنند، بنابراین قابلیت همکاری با برنامه‌های شبکه‌سازی را که برای دستگاه‌های کمتر محدود و زیرساخت‌های سیمی طراحی شده‌اند، تضمین می‌کنند.

در نهایت، توجه داشته باشید که تعداد فزاینده‌ای از دستگاه‌های اینترنت اشیا در بازار برای محیط‌های صنعتی سخت طراحی شده‌اند. در حالی که مشخصات آنها کاملاً مطابق با استانداردهای نظامی نیست، اما جایگزین‌های بسیار بهتری را برای پذیرش مستقیم در محیط‌های نظامی نسبت به دستگاه‌های درجه تجاری معمولی ارائه می‌دهند.

پتانسیل‌ها برای پذیرش نظامی

پذیرش در مقیاس بزرگ فناوری‌های اینترنت اشیا در سناریوهای نظامی، راه را برای عملیات فعال شده توسط اینترنت اشیا هموار می‌کند، جایی که نسل جدیدی از برنامه‌های سایبرفیزیکی وعده می‌دهد که اثربخشی رزمی را به طور قابل توجهی بهبود بخشد. ما می‌توانیم دو رکن اساسی برای توسعه برنامه‌های سایبرفیزیکی شناسایی کنیم: حسگری و اتوماسیون.

حسگری مستقیماً تحت تأثیر فناوری‌های اینترنت اشیا قرار می‌گیرد. هزینه کم آنها امکان استقرار حسگرهای تجاری اینترنت اشیا در مقیاس بزرگ را برای گسترش و تکمیل سامانه‌ها و شبکه‌های حسگری نظامی فراهم می‌کند. استقرارهای مویرگی و/یا با تراکم بالا حسگرهای اینترنت اشیا، از طریق جمع‌آوری مقادیر زیادی از داده‌های محیطی، آگاهی از موقعیت بسیار دقیق‌تر و جامع‌تری را ممکن می‌سازد، در حالی که در عین حال بستر را برای یک پلتفرم قابل استقرار و مصرفی سریع فراهم می‌کند.

در سناریوهای امداد و نجات بشردوستانه و بلایای طبیعی (HADR) با عملیات در محیط‌های شهری، ادغام سامانه‌های نظامی با زیرساخت‌های اطلاعاتی غیرنظامی می‌تواند مزایای حسگری قابل توجهی را به ارمغان بیاورد. در واقع، استفاده از قابلیت‌های حسگری زیرساخت‌های موجود اینترنت اشیا، مانند سامانه‌های نظارت بر ترافیک و شبکه‌های نظارت تصویری، از قبل نشان داده شده است که یک مزیت حیاتی از نظر آگاهی از شرایط زمینه‌ای ارائه می‌دهد. توجه داشته باشید که در این موارد، معمولاً مهندسان وقت ندارند که یکپارچه‌سازی برنامه‌ریزی شده را انجام دهند و اغلب نیاز به انجام یکپارچه‌سازی موردی بین ارتش و سامانه‌های تجاری اینترنت اشیا دارند.

راهکارهای حسگری شخصی، امکان ضبط وضعیت و زمینه سربازان از طریق قرائت‌های بیومتریک و راهکارهای تشخیص حرکات خودکار و همچنین نظارت بر وضعیت فیزیکی (و روانی) پرسنل نظامی در حین فعالیت در میدان را فراهم می‌کند. این به فرماندهان اجازه می‌دهد تا نیات خود را به طور مؤثرتر و قابل اعتمادتری به نیروهای خود منتقل کنند، اطلاعات به روز شده در مورد وضعیت نیروهای خود را برای بهبود تصمیم‌گیری دریافت کنند و به طور خودکار درخواست تدارکات و/یا تقویت نیرو کنند. همچنین، ارزیابی پس از عمل داده‌های نظارت بیولوژیکی می‌تواند توسعه اصول تاکتیکی مؤثرتری را که عملکرد پرسنل انسانی را در نظر می‌گیرد، امکان‌پذیر کند.

به طور کلی، فناوری‌های اینترنت اشیا نشان دهنده یک نقطه عطف مهم در جهت تحقق چشم‌انداز یک طیف پیوسته از حسگری است، از سطح کشور گرفته تا شهر، تا میدان نبرد و حتی سرباز انفرادی، که یک فناوری کلیدی برای عملیات C٤ISR آینده است. در واقع، اطلاعات دقیق و ظریفی که توسط دستگاه‌ها و سامانه‌های بسیاری که از طریق فناوری‌های اینترنت اشیا پیاده‌سازی می‌شوند، پس از مراحل همبستگی و تحلیل، می‌تواند منجر به آگاهی از موقعیت به طور قابل توجهی بهبود یافته شود.

به نوبه خود، دانش ارزشمندی که از طریق آگاهی از موقعیت پیشرفته ارائه شده توسط ادغام سامانه‌های نظامی و تجاری اینترنت اشیا به دست می‌آید، اطلاعات قابل اجرا را ارائه می‌دهد. چنین اطلاعاتی می‌تواند به طور مؤثر از طریق توسعه راهکارهای خودکار برای حمایت از رزمندگان، در سطح تصمیم‌گیری و همچنین برای تدارکات زنجیره تأمین مورد بهره‌برداری قرار گیرد. به عنوان مثال، راهکارهایی که دانش میدان نبرد را ایجاد می‌کنند می‌توانند برای ارائه پیشنهاداتی به رهبران نظامی برای تصمیم‌گیری استفاده شوند. یا آنها می‌توانند به طور خودکار به دارایی‌های بدون سرنشین (ربات‌های زمینی، پهپادها و غیره) دستور دهند تا اقدامات مناسب را در حمایت از اهداف مأموریت فعلی انجام دهند. آگاهی از موقعیت غنی شده همچنین می‌تواند تدارکات زنجیره تأمین خودکار را فعال کند و پتانسیل قابل توجهی برای بهینه‌سازی تحویل به موقع تدارکات دارد. مزایای ناشی از آن شامل رهایی پرسنل از کارهای حسابداری و اداری تکراری و مستعد خطا است.

چالش‌های تحقیقاتی فعلی

اینترنت اشیا در آینده بسیار نزدیک بر عملیات نظامی تأثیر خواهد گذاشت، و چالش‌های بسیاری را ایجاد می‌کند، اما مزایای بالقوه بسیاری را نیز ارائه می‌دهد. با این حال، تعیین چگونگی ادغام فناوری‌های اینترنت اشیا در اکوسیستم نظامی و چگونگی استفاده کارآمد از آنها هنوز هم سوالات تحقیقاتی باز را نشان می‌دهد.

از منظر C٤ISR ، می‌توانیم شش دسته از چالش‌های پیش روی توسعه و کاربردهای عملیات فعال شده توسط اینترنت اشیا را شناسایی کنیم: ارتباطات، همزیستی همگرا، قابلیت همکاری بین سامانه‌های نظامی و تجاری اینترنت اشیا، فیلتر کردن و اولویت‌بندی اطلاعات برای اطمینان از پردازش و ارتباطات ارزشمندترین اطلاعات در محیط‌های تاکتیکی با محدودیت منابع، تجزیه و تحلیل داده‌های تولید شده توسط اینترنت اشیا برای اهداف آگاهی از موقعیت و راهکارهای میان‌افزار اینترنت اشیا که به طور خاص برای تسهیل توسعه و استقرار برنامه‌های اینترنت اشیا طراحی شده‌اند.

ارتباطات

بسیاری از سامانه‌ها و اجزای اینترنت اشیا که در محیط تجاری توسعه یافته‌اند، فرضیات متعددی را در مورد دسترسی و ثبات پیوندهای شبکه برای ارتباطات ایجاد می‌کنند، و اغلب فرض می‌کنند که WiFi ، Insteon ، Z-Wave، ZigBee و غیره و همچنین درگاه‌هایی وجود دارد که به اینترنت متصل می‌شوند. به طور مشابه، حسگرهای پوشیدنی فرض می‌کنند که یک شبکه منطقه شخصی (PAN) مانند بلوتوث یا ANT وجود دارد، و از طریق PAN ، دستگاه می‌تواند به یک تلفن همراه دسترسی پیدا کند، که سپس اتصال قابل

اعتمادی به اینترنت از طریق شبکه‌های تلفن همراه فراهم می‌کند. دستگاه‌های شهر هوشمند وجود خطوط انتقال برق، WiFiیا تلفن همراه برای اتصال به اینترنت را فرض می‌کنند. اتومبیل‌ها سلولی یا استانداردهای آینده مانند p۸۰۲,۱۱ را فرض می‌کنند. حتی دستگاه‌های محاسباتی تعبیه شده مستقل نیز معمولاً با استفاده از نوعی ارتباطات تلفن همراه توسعه یافته و شبکه‌سازی می‌شوند.

یک چالش مهم در هنگام پذیرش اینترنت اشیا تجاری در عملیات نظامی این است که شبکه‌های نظامی، به ویژه شبکه‌های تاکتیکی، معمولاً به اینترنت متصل نیستند یا دسترسی به اینترنت محدود، محدود و گران (به عنوان مثال، با استفاده از SATCOM) دارند. این با رویکرد پردازش اطلاعات اتخاذ شده توسط اکثر دستگاه‌های تجاری اینترنت اشیا مغایرت دارد، که متکی به دستگاه‌های متصل به زیرساخت‌های ابری متمرکز برای تجزیه و تحلیل است، که معمولاً توسط سازنده اداره می‌شود. در این حالت، جریان داده معمولاً از دستگاه به یک درگاه یا تلفن همراه و سپس به سرورهای سازنده (از طریق WiFi یا تلفن همراه) است، جایی که داده‌های خام به طور مرکزی تجزیه و تحلیل شده و سپس به کاربر برگردانده می‌شود. علاوه بر این، برخی از دستگاه‌های اینترنت اشیا نیاز دارند که صاحبان با سازنده ثبت نام کنند و حتی اگر نتوانند به زیرساخت متمرکز سازنده دسترسی پیدا کنند، فعال نمی‌شوند. این الگوها به دلایل امنیتی و همچنین دسترسی، در محیط نظامی قابل دفاع نیستند.

همزیستی و عملیات همگرا

با پذیرش مفاهیم و فناوری‌های اینترنت اشیا در شبکه‌های نظامی، یک چالش مهم، همزیستی و استقرار مشترک دستگاه‌ها و شبکه‌های تجاری اینترنت اشیا و دستگاه‌ها و شبکه‌های نظامی با دقت ساخته شده، با دقت تأیید شده و با دقت کنترل شده است [۲]. به عنوان مثال، دستگاه‌های تجاری اینترنت اشیا ممکن است نیاز داشته باشند ترافیک خود را از طریق شبکه‌های نظامی سوار کنند، که مشکل‌ساز است. علاوه بر این، با توجه به ماهیت همزیستی آنها، دستگاه‌های تجاری اینترنت اشیا ممکن است قادر به تشخیص (و به طور تصادفی نشت) اطلاعات حساس یا تداخل در عملکرد عادی تجهیزات نظامی باشند. و در محیط‌های غیر سنتی مانند شهرهای هوشمند، مسائلی مانند فریب حیاتی خواهند بود، زیرا دستگاه‌های اینترنت اشیا و خدمات شهری به منابع ارزشمندی از اطلاعات برای عملیات نظامی تبدیل می‌شوند و نیاز به رویکردهای جدیدی برای ردیابی نسب، تعیین اعتماد و انتقال اطلاعات قابل اجرا به سربازان دارند.

قابلیت همکاری

همانطور که در تلاش‌های تجاری اینترنت اشیا منعکس شده است، ناهمگونی قابل توجهی در دستگاه‌ها، زیرساخت‌ها و استانداردهای ارتباطی پشتیبانی کننده وجود دارد [۳]. چنین تنوع طراحی، موانعی را برای یکپارچه‌سازی برنامه‌ریزی شده و موردی سامانه‌های اینترنت اشیا ایجاد می‌کند. برای کاربردهای نظامی، قابلیت همکاری به یک نکته کلیدی برای یکپارچه‌سازی سامانه‌های بین ائتلافی و همچنین یکپارچه‌سازی بین زیرساخت‌های نظامی و تجاری تبدیل می‌شود.

تغییر در استانداردهای ارتباطی بین سامانه‌های نظامی و تجاری، مانند کانال‌های رادیویی مورد استفاده، تا حدی ناشی از ملاحظات امنیتی، مانند تمایل به کاهش رهگیری ارتباطات نظامی توسط دشمنان است. این امر مستلزم توسعه خدماتی است که برای ایجاد پل ارتباطی بین استانداردهای از قبل موجود طراحی شده‌اند.

فیلتر کردن و اولویت‌بندی اطلاعات

همانطور که داده‌های تولید شده توسط زیرساخت‌های اینترنت اشیا به طور تصاعدی رشد می‌کنند، روش‌هایی برای محدود کردن مقدار داده‌های خام برای پردازش و اولویت‌بندی انتقال بیشترین اطلاعات تولید شده توسط تحلیل‌ها به طور فزاینده‌ای ضروری می‌شوند [۴].

از دیدگاه خدمات تجاری، محدودیت‌های شبکه فراتر از محدودیت‌های اعمال شده توسط خدمات مصرف‌کننده، مانند محدودیت‌های داده در برنامه‌های تلفن همراه، نگرانی چندانی ندارند. همانطور که قبلاً اشاره شد، استفاده از شبکه نظامی نیاز به روش‌هایی برای اولویت‌بندی انتقال محتوا، بر اساس کیفیت ذاتی اطلاعات و نیازهای سربازان دارد.

برای سامانه‌های نظامی، یک چالش اضافی از مدیریت بار شناختی برای سربازان ناشی می‌شود. در صورتی که اطلاعات گیج کننده یا نامربوط (یا بدتر از آن، فریبنده) به آنها منتقل شود، ممکن است بر عملکرد سرباز تأثیر منفی بگذارد یا منجر به اقدامات نادرست شود. در نهایت، محدودیت‌های قابل توجه در منابع شبکه و اهمیت حیاتی چند عملکرد اساسی، مانند آگاهی از موقعیت، در رابطه با بسیاری از عملکردهای دیگر پیاده‌سازی شده توسط کاربردهای نظامی، اولویت‌بندی اطلاعات مربوطه را به یک عنصر ضروری در کاربردهای نظامی آینده تبدیل می‌کند [۵].

تجزیه و تحلیل

مقیاس رو به رشد استقرار دستگاه‌های اینترنت اشیا به مجموعه‌داده‌های رو به رشدی منجر شده است که باید از خدمات مصرف‌کننده گرا استفاده شود [۶]. در کاربردهای نظامی، به ویژه آنهایی که به سمت درک زمان واقعی میدان نبرد گرایش دارند، ترکیب اطلاعات قابل اجرا از مجموعه‌داده‌ها در زمان واقعی نزدیک به زمان واقعی به یک الزام مهم تبدیل می‌شود. برای کاربردهای تجاری، این مجموعه‌داده‌ها اغلب به خدمات مبتنی بر ابر برای پردازش بعدی منتقل می‌شوند. این برای کاربردهای نظامی که تحت شبکه‌های با محدودیت منابع فعالیت می‌کنند، کمتر عملی می‌شود. در اینجا، دو ملاحظه برای پردازش داده‌ها وارد عمل می‌شوند: اول، نیاز به قابلیت‌هایی برای فیلتر کردن مجموعه‌داده‌ها برای ویژگی‌های جالب تا حد امکان نزدیک به منابع آنها [۷]. دوم، توانایی تولید نمایش‌های اطلاعات مختصر برای مجموعه‌داده‌ها، که برای استفاده بهینه از منابع شبکه طراحی شده‌اند.

میان‌افزار اینترنت اشیا

پذیرش فناوری اینترنت اشیا در ارتش مستلزم راهکارهای میان‌افزار است که هدف آن تعریف و مدیریت آسان برنامه‌های سایبرفیزیکی است. به طور کلی، میان‌افزار اینترنت اشیا باید با توزیع پردازش اطلاعات مورد نیاز بر روی پلتفرم‌های سخت‌افزاری ناهمگن، به طور مؤثر از منابع محاسباتی موجود استفاده کند. به ویژه، راهکارهای میان‌افزار باید پردازش داده‌های جمع‌آوری شده از دستگاه‌های اینترنت اشیا را در امتداد مسیرهای ارتباطی فعال کنند، احتمالاً در لبه بین شبکه‌های تاکتیکی و اینترنت اشیا (گره‌های درگاه یا گره‌های اختصاصی که منابع محاسباتی را در مجاورت نزدیک با درگاه‌ها فراهم می‌کنند)، و نیاز به خدمات مبتنی بر ابر را به حداقل می‌رسانند. علاوه بر این، میان‌افزار اینترنت اشیا متمرکز بر ارتش باید با میان‌افزار ارتباطات تاکتیکی ادغام شود تا انتشار اطلاعات حیاتی را مطابق با نیازهای مصرف‌کنندگان و اولویت نسبی که آنها به اطلاعات نیاز دارند، اولویت‌بندی کند. در نهایت، تعریف و نمونه‌سازی پویای خدمات پردازش اطلاعات برای پرداختن به سناریوهای یکپارچه‌سازی برنامه‌ریزی شده و ویژه و پشتیبانی از نیازهای پویای سربازان ضروری است.

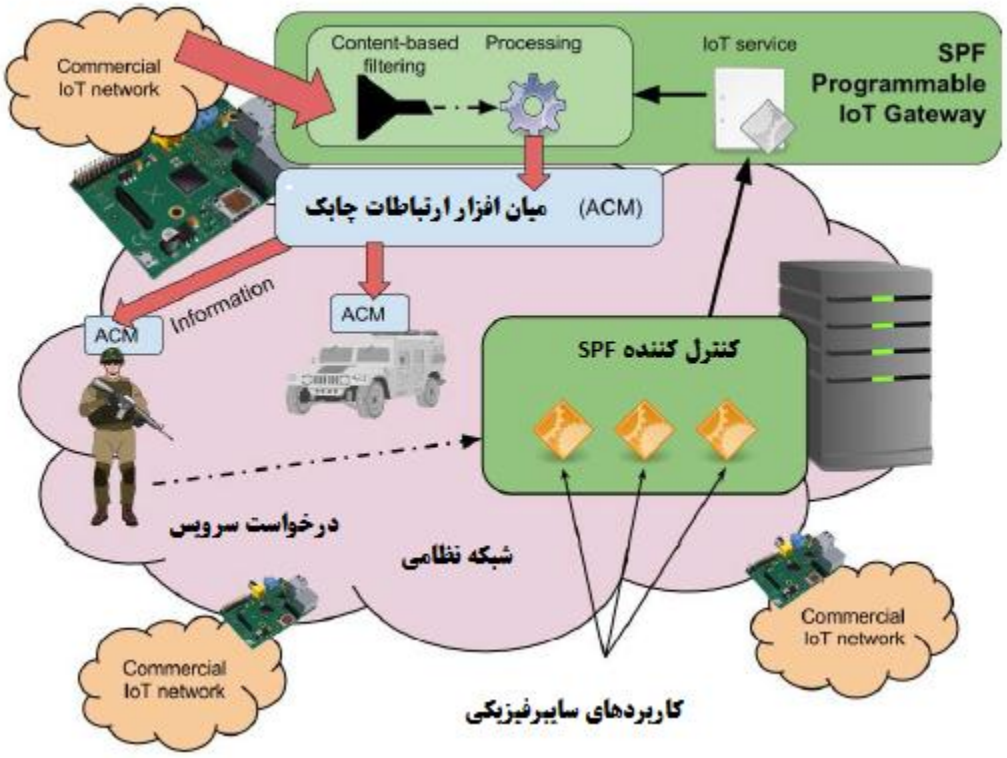
پشتیبانی از عملیات نظامی فعال شده توسط اینترنت اشیا

برنامه‌های سایبرفیزیکی برای عملیات نظامی فعال شده توسط اینترنت اشیا نیاز به پشتیبانی از میان‌افزار شبکه تاکتیکی دارند، که باید به چالش‌های شرح داده شده در بخش قبلی بپردازد. به این منظور، میان‌افزار باید روش‌ها و ابزارهایی را برای پیاده‌سازی جمع‌آوری و تجزیه و تحلیل داده‌های خام اینترنت اشیا، انتشار اطلاعات پردازش شده و تسهیل تعریف، استقرار و مدیریت برنامه‌های سایبرفیزیکی فراهم کند، در حالی که با در دسترس بودن منابع محدود از نظر پهنای باند ارتباطی، انرژی، محاسبات و ذخیره‌سازی کنار می‌آید.

تجربیات نویسندگان در این زمینه از قبل منجر به تحقق Agile Computing Middleware شده است، یک راهکار ارتباطی جامع برای شبکه‌های تاکتیکی [۹-۸]، و اساس کار ارائه شده در اینجا برای رسیدگی به برخی از مسائل تحقیقاتی اولیه است. به طور خاص، این مقاله SPF را ارائه می‌دهد، یک طراحی میان‌افزار جدید که به سمت اولویت‌بندی انتشار اطلاعات، بر اساس ارزش درک شده اطلاعات برای مصرف‌کنندگان، هدایت می‌شود.

یک پارادایم جدید برای فیلتر کردن، پردازش و انتشار اطلاعات یکپارچه

به منظور پشتیبانی از برنامه‌های سایبرفیزیکی در محیط‌های نظامی، Agile Computing Middleware(ACM) [۵] روش‌های جدیدی را برای ارتباطات شبکه در محیط‌های لبه تاکتیکی معرفی می‌کند. نکته کلیدی برای استفاده ACM از منابع شبکه، مفهوم ارزش اطلاعات (VoI) است - معیاری از ابزار درک شده اطلاعات برای مصرف‌کنندگان بر اساس زمینه موقعیتی آنها. از طریق روال‌های محاسبهVoI ACM ، یک اولویت خاص برای هر شی اطلاعاتی (پویا و خاص مصرف‌کننده) محاسبه می‌شود و برای سفارش انتقال اعمال می‌شود. SPF بر اساس ACM ساخته شده است، پلتفرم (Sieve, Process, and Forward) برای ارائه فیلتر یکپارچه داده‌های اینترنت اشیا (الک)، استخراج اطلاعات (پردازش) و توابع انتشار (ارسال) برای زمینه‌های محاسباتی تاکتیکی و شهری توسعه یافته است. در اصطلاح‌شناسیSPF ، یک کاربرد اینترنت اشیا مجموعه‌ای از خدماتی است که توابعی را برای فیلتر کردن، اولویت‌بندی و تجزیه و تحلیل اطلاعات فراهم می‌کنند که می‌توان آنها را به صورت درخواستی فعال کرد. خدمات در بالای گره‌های اختصاصی در لبه اینترنت اشیا / شبکه تاکتیکی، به نام(Programmable IoT Gateways (PIGs ، اجرا می‌شوند. همانطور که در شکل ۱ نشان داده شده است، توابع تعریف، نمونه‌سازی و مدیریت خدمات توسط یک جزء کنترل کننده متمرکز ارائه می‌شوند، که خدمات اینترنت اشیا را بر اساس درخواست‌های کاربران به صورت درخواستی نمونه‌سازی می‌کند و در صورت لزومPIG ها را دوباره برنامه‌ریزی می‌کند.



شکل ۱. عملیات مبتنی بر اینترنت اشیا همانطور که توسط SPF و ACM پیاده‌سازی شده است.

توسعه‌دهندگان می‌توانند به راحتی کاربردها و خدمات اینترنت اشیا را با استفاده از یک(Domain Specific Language (DSL اختصاصی تعریف کنند DSL .دستورالعمل‌هایی را برای استفاده از مجموعه‌ای از توابع فیلتر کردن، پردازش و ارتباطات پیاده‌سازی شده توسط پلتفرم نرم‌افزاری نشان می‌دهد. به طور خاص، SPF با اجازه دادن به اجرای حداقل مقدار تفاوت بین محتوای پیام‌ها، برای جلوگیری از انتقال‌های زائد، فیلتر کردن مبتنی بر محتوا قابل تنظیم را فراهم می‌کند. همچنین، توسعه‌دهندگانی که از SPF استفاده می‌کنند، می‌توانند به راحتی خدمات اینترنت اشیا را بر اساس رویه‌های پیچیده دستکاری اطلاعات تعریف کنند، که از مجموعه‌ای از توابع اساسی پردازش و دستکاری داده‌ها، و قوانینی که مشخص می‌کنند چگونه اطلاعات مشتق شده باید منتشر شوند، استفاده می‌کنند. برای انتشار اطلاعات در محیط تاکتیکی، SPF از توابع ارائه شده توسط جزء DisService ACM استفاده می‌کند [۹].

نتایج تجربی

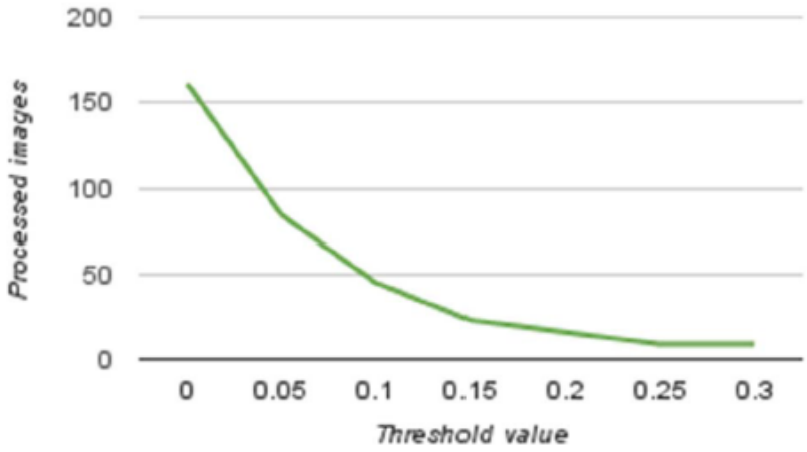
به منظور نشان دادن قابلیت SPF برای توسعه و استقرار خدمات اینترنت اشیا که می‌توانند با توجه به منابع در دسترس در دستگاه‌هایی کهPIG ها را اجرا می‌کنند مقیاس شوند، ما یک ارزیابی تجربی از عملکرد فیلتر کردن مبتنی بر محتوا SPF ارائه می‌دهیم. نتایج در این بخش با استفاده از پیاده‌سازی نمونه اولیه SPF جمع‌آوری شده است، که ما با استفاده از پلتفرم JRuby توسعه دادیم و تحت مجوز MIT به عنوان منبع باز[2] منتشر کردیم.

به طور خاص، ما یک فیلتر مبتنی بر محتوا را برای خدمات اینترنت اشیا تجزیه و تحلیل تصویر در نظر می‌گیریم، که تفاوت بین تصاویر متوالی را که از زیرساخت اینترنت اشیا می‌آیند محاسبه می‌کند. الگوریتم فیلتر کردن تفاوت بین هر جزء RGB از هر جفت پیکسل واقع در یک موقعیت یکسان در دو تصویر را محاسبه می‌کند. خروجی یک عدد بین ۰ و ۱ است، که به عنوان مجموع تمام مقادیر به دست آمده در مرحله قبل، نرمال شده بر تعداد پیکسل‌ها در تصاویر و سه جزء رنگ محاسبه می‌شود. بنابراین، می‌توان یک آستانه تفاوت را مشخص کرد که زیر آن SPF PIG از پردازش تصویر صرف نظر می‌کند و با تغییر آن آستانه، می‌توان تلاش محاسباتی رویPIG ها را کنترل کرد. بدین ترتیب، فیلتر کردن مبتنی بر محتوا، تنظیم مقدار پردازش انجام شده با توجه به منابع موجود درPIG ها را ممکن می‌سازد، که SPF را به یک راهکار مقیاس‌پذیر تبدیل می‌کند که با طیف وسیعی از ماشین‌ها سازگار است، از سرورهای قدرتمندی که روی پهپادها و وسایل نقلیه زمینی نصب شده‌اند گرفته تا دستگاه‌های COTS کوچک، ارزان و کم مصرف.

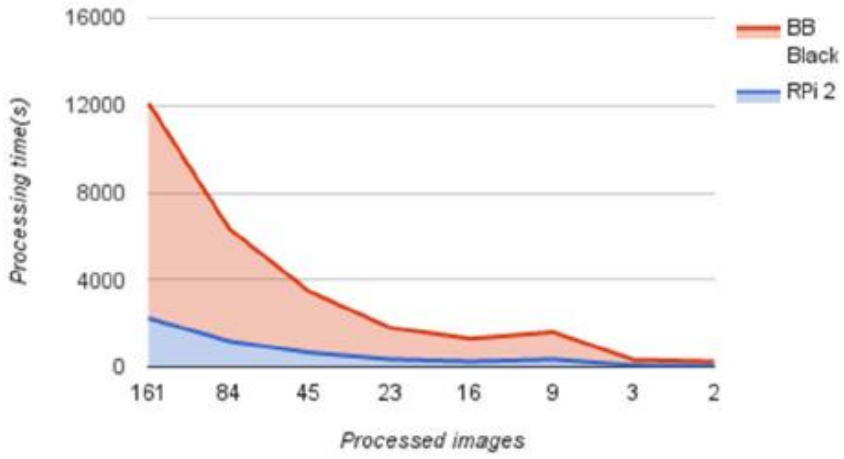
برای نشان دادن تأثیر فیلتر کردن مبتنی بر محتوا بر گره‌های با منابع محدود، ما دو دستگاه COTS را برای آزمایش‌های خود انتخاب کرده‌ایمBeagleBone Black Rev.C :. مجهز به پردازنده ۱ گیگاهرتزیARMSitara AM ۳۳۵ xو ۵۱۲ مگابایتRAM ، و Raspberry Pi۲ مدلB ، که دارای یک پردازنده چهار هسته‌ای ۹۰۰ مگاهرتزی ARM Cortex با ۱ گیگابایت RAM است. با توجه به ویژگی‌های این دستگاه‌ها، ما آنها را برای آزمایش نمونه اولیه خود و مقایسه نتایج به دست آمده در دو سیستم مناسب می‌دانیم. هر دو دستگاه سیستم عامل Linux Debian ۸ Jessie را اجرا می‌کنند، که روی آن Java OpenJDK ۷ و کتابخانه‌های OpenCV۳ و Tesseract را با اتصالات Java مربوطه نصب کرده‌ایم. برای اجرای آزمایش‌های خود، از یک مجموعه داده ۱۶۰ تصویری مشتق شده از ویدیوی یک چهارراه شلوغ استفاده کرده‌ایم که ترافیک جاده‌ای و افرادی را نشان می‌دهد که در پیاده‌رو راه می‌روند، که معتقدیم بسیار نزدیک به یک سناریوی واقعی است. تمام تصاویر دارای وضوح ۷۳۸x۱۲۸۰ پیکسل هستند، در فرمت PNGرمزگذاری شده‌اند و اندازه آنها حدود ۱ مگابایت است. شکل ۲ در زیر تعداد تصاویر پردازش شده را نشان می‌دهد، که با افزایش آستانه تفاوت به طور تصاعدی کاهش می‌یابد.

همچنین جالب است که عملکرد پردازش تصویر را بین Raspberry Pi ۲ و BeagleBone Black مقایسه کنیم، که به صورت زمان لازم برای اجرای یک خط لوله خاص روی یک مجموعه از تصاویر بیان می‌شود. شکل ۳ مجموع زمان پردازش را هنگامی که SPF PIG از OCR با استفاده از موتور Tesseract روی مجموعه داده تصویری فیلتر شده ما استفاده می‌کند، نشان می‌دهد. تصاویر کمتر در

مجموعه مربوط به آستانه تفاوت بالاتر است. نمودار نشان می‌دهد که نمونه اولیه SPF عملکرد بالاتری را روی Raspberry Pi ۲ در مقایسه با BeagleBone Black به دست می‌آورد.



شکل ۲. تعداد تصاویر پردازش شده در برابر مقدار آستانه تفاوت



شکل ۳. مجموع زمان پردازش (به ثانیه) در برابر تعداد تصاویر در مجموعه داده فیلتر شده.

نتیجه‌گیری

پیشرفت‌های اخیر در فناوری اینترنت اشیا، همانطور که در این مقاله بررسی شد، هم عملیات نظامی موجود را به میزان زیادی تغییر می‌دهد و هم از آن سود می‌برد. تا حدی، انتظار می‌رود این مزایا از استفاده ترکیبی از دستگاه‌های تجاری (COTS) و راهکارهای میان‌افزار تخصصی ناشی شود. با این حال، استقرار مشترک و همزیستی اینترنت اشیا تجاری و سامانه‌های نظامی چالش‌های بسیاری را ایجاد می‌کند. یک موضوع مشترک برای این چالش‌ها در مدیریت منابع محاسباتی و شبکه‌بندی محدود، در مقایسه با خدمات تجاری

موجود نهفته است. ما در مورد رابطه این چالش‌های تحقیقاتی با زمینه‌های نظامی بحث کردیم و بحثی را ارائه دادیم در مورد اینکه چگونه راهکارهای میان‌افزار، مانند ACM وSPF ، قصد دارند از طریق روش‌های جدید توسعه و استقرار برای کاربردهای سایبرفیزیکی و اولویت‌بندی اطلاعات، بسیاری از این چالش‌ها را برطرف کنند.

گسترش اطلاعات تولید شده توسط اینترنت اشیا به حدی زیاد خواهد بود که نیاز به معماری‌ها و چارچوب‌هایی که اطلاعات را فیلتر می‌کنند، اولویت‌بندی می‌کنند و به طور هوشمندانه از پشتیبانی تصمیم‌گیری حساس به زمینه و هدف استفاده می‌کنند را اجباری می‌کند. ما نشان می‌دهیم که راهکارهای میان‌افزار می‌توانند قابلیت‌هایی را ارائه دهند که برخی از اثرات منفی کاربردهای نظامی فعال شده توسط اینترنت اشیا را کاهش می‌دهند. به ویژه آنهایی که در محیط‌های تاکتیکی عمل می‌کنند. ما انتظار داریم که در آینده نزدیک، راهکارهای میان‌افزار مانند SPF به طور فزاینده‌ای به سمت اطلاعات گرایش پیدا کنند - و به سمت استفاده بیشتر از فناوری‌هایی مانند ارزش اطلاعات و محتوای فعال شده معنایی که با فراداده‌های اعتماد و منشأ غنی شده است، همگرا شوند.

منابع

A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications”, IEEE Communications Surveys & Tutorials, Vol. ١٧, No. ٤, pp. ٢٣٤٧-٢٣٧٦, Fourth quarter ٢٠١٥.

D. Zheng, W. Carter, “Leveraging the Internet of Things for a More Efficient and Effective Military”, CSIS/Rowman & Littlefield, ٢٠١٥.

M. Nitti, V. Pilloni, G. Colistra, L. Atzori, “The Virtual Object as a Major Element of the Internet of Things: a Survey”, IEEE Communications Surveys & Tutorials, in press.

E. Kovacs, A. Papageorgiou, B. Cheng, “Real-Time Data Reduction at the Network Edge of Internet-of-Things Systems”, in Proceedings of ١١th International Conference on Network and Service Management (CNSM ٢٠١٥), ٩-١٣ November ٢٠١٥, Barcelona, Spain.

N. Suri, G. Benincasa, R. Lenzi, M. Tortonesi, C. Stefanelli, L. Sadler, “Exploring Value of Information-based Approaches to Support Effective Communications in Tactical Networks”, IEEE Communications Magazine, Vol. ٥٣, No. ١٠, pp. ٣٩-٤٥, October ٢٠١٥.

J. Stankovic, “Research Directions for the Internet of Things”, IEEE Internet of Things Journal, Vol. ١, No. ١, pp. ٣-٩, ٢٠١٤.

K. Velasquez, D. P. Abreu, M. Curado, E. Monteiro, “Service Placement for Latency Reduction in the Internet of Things”, Annals of Telecommunications, in press.

N. Suri, E. Benvegnù, M. Tortonesi, C. Stefanelli, J. Kovach, J. Hanna, “Communications Middleware for Tactical Environments: Observations, Experiences, and Lessons Learned”, IEEE Communications Magazine, Vol. ٤٧, No. ١٠, pp. ٥٦-٦٣, October ٢٠٠٩.

N. Suri, G. Benincasa, M. Tortonesi, C.Stefanelli, J. Kovach, R. Winkler, R. Kohler, J. Hanna, L. Pochet, S. Watson, “Peer-to-Peer Communications for Tactical Environments: Observations, Requirements, and Experiences”, IEEE Communications Magazine, Vol. ٤٨, No. ١٠, pp. ٦٠-٦٩, October ٢٠١٠.

M. Tortonesi, J. Michaelis, N. Suri, M. A. Baker, “Softwaredefined and Value-based Information Processing and Dissemination in IoT Applications”, in Proceedings of the ١٤th IEEE/IFIP Network Operations and Management Symposium (NOMS ٢٠١٦), ٢٥-٢٩ April ٢٠١٦, Istanbul, Turkey.

Leveraging the Internet of Things in a Military Network Environment: Challenges and Solutions

Natereh Ghadimi
Ph.D. Graduate in Electrical Engineering, Electronics, University of Tabriz

Abstract

The Internet of Things (IoT) technology, with its continuous expansion, holds immense potential for transforming military operations. By converting battlefield assets into networked entities through numerous environmental and personal sensors, a vast amount of precise and nuanced information is collected. This information can significantly enhance the efficiency of military operations in areas such as Intelligence, Surveillance, and Reconnaissance (ISR), supply chain automation, and urban operations in complex metropolitan environments. However, achieving these benefits necessitates addressing key challenges. These challenges include reconciling the differences between commercial IoT architectural patterns and military network structures, ensuring interoperability between various IoT systems, managing and processing the massive volume of data, and developing resource-efficient IoT middleware solutions. The resource-constrained tactical networking environment makes this research agenda not only more challenging but also essential in terms of the need for middleware innovation. This paper emphasizes the need for research and development in these areas to fully harness the potential of IoT in the military domain.

Keywords: Cyber-Physical Applications, Military Communications, Internet of Things