فصلنامه علمی - پژوهشی فرماندهی و کنترل، سال دوم، شماره سه، پاییز ۱۳۹۷

مفاهیم و چالش‌های امنیتی اینترنت اشیاء نظامی با محوریت مکانیزم MIoT ایالات متحده آمریکا

محمد بهشتی آتشگاه[۱]، مرتضی براری[۲]، مجید بیات[۳]، محمدرضا عارف[۴]

تاریخ دریافت: ۱۳۹۷/۰۳/۱۵ **تاریخ پذیرش: ۱۳۹۷/۰۹/۱۲**

چکیده

اینترنت اشیاء **(IoT)** پتانسیل بالقوه‌ای برای تبدیل‌شدن به مهمترین مفهومی را دارد که در طی دهه‌های اخیر انقلاب عظیمی در عرصه فناوری اطلاعات و ارتباطات به راه انداخته است. در حقیقت، مفهوم اینترنت اشیاء، شبکه‌ای جهانی مبتنی بر اینترنت تعریف می‌کند که در آن تمامی اشیاء قابلیت اتصال به یکدیگر، تبادل اطلاعات و انجام فعالیت‌های هوشمند خواهند داشت. این مفهوم جدید هم کاربردهای غیرنظامی (شهری) و هم کاربردهای نظامی را تحت تأثیر مفاهیم جدید خود قرار داده است. با ورود بحث اینترنت اشیاء و همچنین قابلیت متصل‌شدن سیستم‌های مختلف سلاح به شبکه، فرصت تسهیل کنترل سلاح‌ها توسط فرماندهان و نیز ارتقاء سرعت عمل در واکنش‌ها پدید می‌آید. در این میان و نسبت به کاربردهای غیرنظامی، کاربردهای نظامی اینترنت اشیاء که تحت عنوان حوزه اینترنت اشیاء نظامی معرفی می‌گردد بیشتر حائز اهمیت است چرا که می‌تواند تأثیرات مستقیم مثبت یا مخربی را در صحنه‌های نبرد به دنبال داشته باشد. از این رو، مسائل امنیتی مرتبط با بخش‌های مختلف اینترنت اشیاء نظامی بسیار حیاتی می‌باشند. در این مقاله، ابتدا به مفاهیم و معماری اینترنت اشیاء نظامی اشاره نموده و مکانیزم اینترنت اشیاء نظامی را با تمرکز بر روی اینترنت اشیاء نظامی ایالات متحده آمریکا مرور می‌نماییم. سپس به بحث و بررسی چالش‌ها و نگرانی‌های امنیتی پرداخته و نهایتاً نیز به طرح ملزومات امنیتی اینترنت اشیاء نظامی می‌پردازیم.

کلمات کلیدی: اینترنت اشیاء نظامی، جنگ شبکه-محور، فرماندهی و کنترل، امنیت و حریم‌خصوصی، رمزنگاری.

[۱] دانشجوی دکتری، دانشکده مهندسی برق و کامپیوتر، دانشگاه صنعتی مالک اشتر، *m_beheshti_a@mut.ac.ir*

[۲] دانشیار، مجتمع دانشگاهی برق و کامپیوتر؛ دانشگاه صنعتی مالک اشتر، *m.barari@mut.ac.ir*

[۳] استادیار، دانشکده مهندسی کامپیوتر؛ دانشگاه شاهد، *mbayat@shahed.ac.ir*

[۴] استاد تمام، دانشکده مهندسی برق، دانشگاه صنعتی شریف، *aref@sharif.edu*

۱. مقدمه

۱-۱. مرور مختصری بر IoT

در یک نگاه کلی، مفهوم اینترنت اشیاء[1] (IoT) به صورت شبکه‌ای از دستگاه‌های (یا اشیای) متصل در نظر گرفته می‌شود. در قالب تجسم امروزه، IoT شامل انواع مختلفی از دستگاه‌ها همانند حسگرها، فعال‌کننده‌ها[2]، برچسب‌های RFID، تلفن‌های هوشمند یا سِرورهای پشت‌خط می‌شود که به طور واضح در مقیاس اندازه[3]، قابلیت[4] و عاملیت[5] با هم متفاوت می‌باشند. چالش اصلی این است که چطور چنین شبکه‌ای را تطبیق دهیم تا در محیط و زیرساخت اینترنت مرسوم فعلی پیاده‌سازی شده و فعالیت نماید. تحقیقاتی که اخیراً صورت پذیرفته‌اند عموماً بر روی طراحی، استفاده و تطبیق پروتکل‌های اینترنتی استاندارد در حوزه‌ی IoT متمرکز بوده‌اند[1]. IoT فرصت‌های بالقوه عظیمی در بسیاری از حوزه‌های کاربردی همانند توزیع توان الکتریکی، حمل و نقل هوشمند، کنترل صنعتی، کشاورزی صنعتی، مانیتورینگ محیطی و پیرامونی، خرده‌فروشی کالا و غیره ارائه می‌دهد[2,3]. ایده‌های کلیدی IoT، حوزه‌های نظامی و دفاعی جدید بسیاری را به ارمغان آورده است که در آن‌ها چابکی و امنیت لجستیک نظامی تا حد زیادی بهبود یافته است[4]. با توسعه فناوری‌های IoT و کاربردهای آن، کاربردهای نظامی IoT تنها به حوزه لجستیک محدود نمی‌شود و IoT اهمیت و ارزش فوق‌العاده‌ای برای شناسائی‌های نظامی، نظارت و کنترل محیطی و پیرامونی، استفاده در جنگ‌افزارهای بدون سرنشین و غیره به ارمغان می‌آورد[5].

به وضوح، IoT می‌تواند انقلاب اطلاعاتی-نظامی جدیدی را در امور نظامی مُدرن ایجاد کرده و به روند پیشرفت آن شتاب بدهد. البته IoT آن‌طوری که اینترنت عمومی امروزه کامل و پیاده‌سازی‌شده است، ایده‌آل نبوده و مسائل و مشکلات بسیاری در مورد کاربردهای آن باقی مانده است که باید حل شوند[5,6].

هر چند که ارزش‌های مهم IoT در حوزه نظامی در حال گسترش روزافزون می‌باشند، اما تقریباً تمامی تحقیقات کنونی در چارچوب مثال‌ها و ایده‌های ساده نظامی باقی مانده‌اند. بنابراین نیاز است تا تحقیقات اصولی و بنیادین در حوزه کاربردهای نظامی IoT (یعنی MIoT[6]) در جهت کاربردهای نظامی IoT صورت بگیرد. یکی از بزرگترین چالش‌های تحقق و پیاده‌سازی گسترده IoT، موضوع امنیت و چالش‌های مرتبط با آن است. امنیت اینترنت اشیاء تبدیل به یک موضوع برجسته تحقیقاتی در سال‌های اخیر شده است که شامل چندین پروژه تحقیقاتی می‌گردد که توسط اتحادیه اروپا و DARPA حمایت مالی می‌شوند[7].

ادامه این مقاله بدین صورت سازمان‌دهی شده است: در بخش بعد مفهوم کلی و معماری اینترنت اشیاء نظامی را مرور کرده و در یکی از زیربخش‌ها، به مرور اینترنت اشیاء نظامی ایالات متحده آمریکا می‌پردازیم. در بخش۳، نقش IoT در کاربردهای نظامی را معرفی می‌نماییم. در بخش٤، تهدیدهای امنیتی IoT را بررسی نموده و به طور خاص، آسیب‌پذیری‌ها و ریسک‌های MIoT ایالات متحده آمریکا را بررسی می‌نماییم. سپس در بخش۵، به ملزومات امنیتی اینترنت اشیاء نظامی می‌پردازیم. نهایتاً با نتیجه‌گیری در بخش٦ به این مقاله پایان می‌دهیم.

۱-۲. اینترنت اشیاء نظامی با محوریت ایالات متحده آمریکا

علیرغم این که مفهوم اینترنت اشیاء در حوزه‌های غیرنظامی یک مفهوم جدید و تأثیرگذار به شمار می‌رود، اما برای حوزه نظامی، اینترنت اشیاء در عمل مبحث جدیدی به شمار نمی‌رود. در دهه ۱۹۹۰ میلادی، رهبران و فرماندهان نظامی ایالات متحده دورنمایی جدید از نحوه انتقال داده و نحوه ارائه معماری شبکه‌ها در میدان‌های نبرد ارائه دادند[8]. این مطلب، مفهوم

[1] *Internet of Things*
[2] *Actuators*
[3] *Size*
[4] *Capability*
[5] *Functionality*
[6] *Military Internet of Things*

پایه‌ای و اساس جنگ شبکه-محور[1] را پایه‌ریزی کرده و قالب آن را شکل داد[9]. آن‌ها مدلی از جنگ مبتنی بر تجمیع و یکپارچه‌سازی سه حوزه مربوطه را توصیف نمودند: ۱) حوزه فیزیکی که در آن حوادث فیزیکی اتفاق افتاده، عملیات صورت می‌پذیرد و داده از حسگرها و مشاهدات انسان تولید می‌گردد؛ ۲) حوزه اطلاعات که در آن داده ارسال شده و ذخیره می‌گردد؛ و ۳) حوزه شناختی که در آن، داده پردازش و تحلیل می‌گردد. سه حوزه جنگ شبکه-محور یعنی ترکیب حسگرها و دستگاه‌های تعبیه‌شده، اتصال اینترنت و فناوری پایگاه داده و تحلیل نرم‌افزاری بسیار به مفهوم مُدرن اینترنت اشیاء نزدیک هستند. در حقیقت، می‌توان گفت که جنگ شبکه-محور کاربرد فناوری‌های IoT در مأموریت‌های نظامی را حتی قبل از پیدایش مفهوم اینترنت اشیاء توصیف می‌نماید.

امروزه، توسعه فناوری‌های مربوط به IoT در حوزه نظامی در وهله اول بر روی کاربردهای سیستم‌های فرامین و کنترل، ارتباطات، رایانه، اطلاعات، جاسوسی و شناسایی (C4ISR) و سیستم کنترل-آتش متمرکز شده است. این توسعه توسط یک نگاه غالب در حوزه نظامی برگرفته می‌شود که حسگرها و شبکه‌ها در درجه نخست به عنوان ابزاری به منظور جمع‌آوری و تسهیم (به اشتراک‌گذاری) داده در میدان جنگ دیده می‌شوند تا فرامین و کنترل موثرتری از دارایی‌های نظامی داشته باشند. فناوری‌های IoT همچنین در برخی از کاربردها برای مدیریت لجستیک، آموزش و شبیه‌سازی تطبیق یافته‌اند؛ اما به هر حال، گسترش IoT در حوزه نظامی محدود بوده و به طور ضعیفی یکپارچه‌سازی شده است. شکل ۱ کلیات معماری اینترنت اشیاء نظامی آمریکا را نشان می‌دهد.

۱-۲-۱. فرامین، کنترل، ارتباطات، رایانه، اطلاعات، جاسوسی و شناسایی

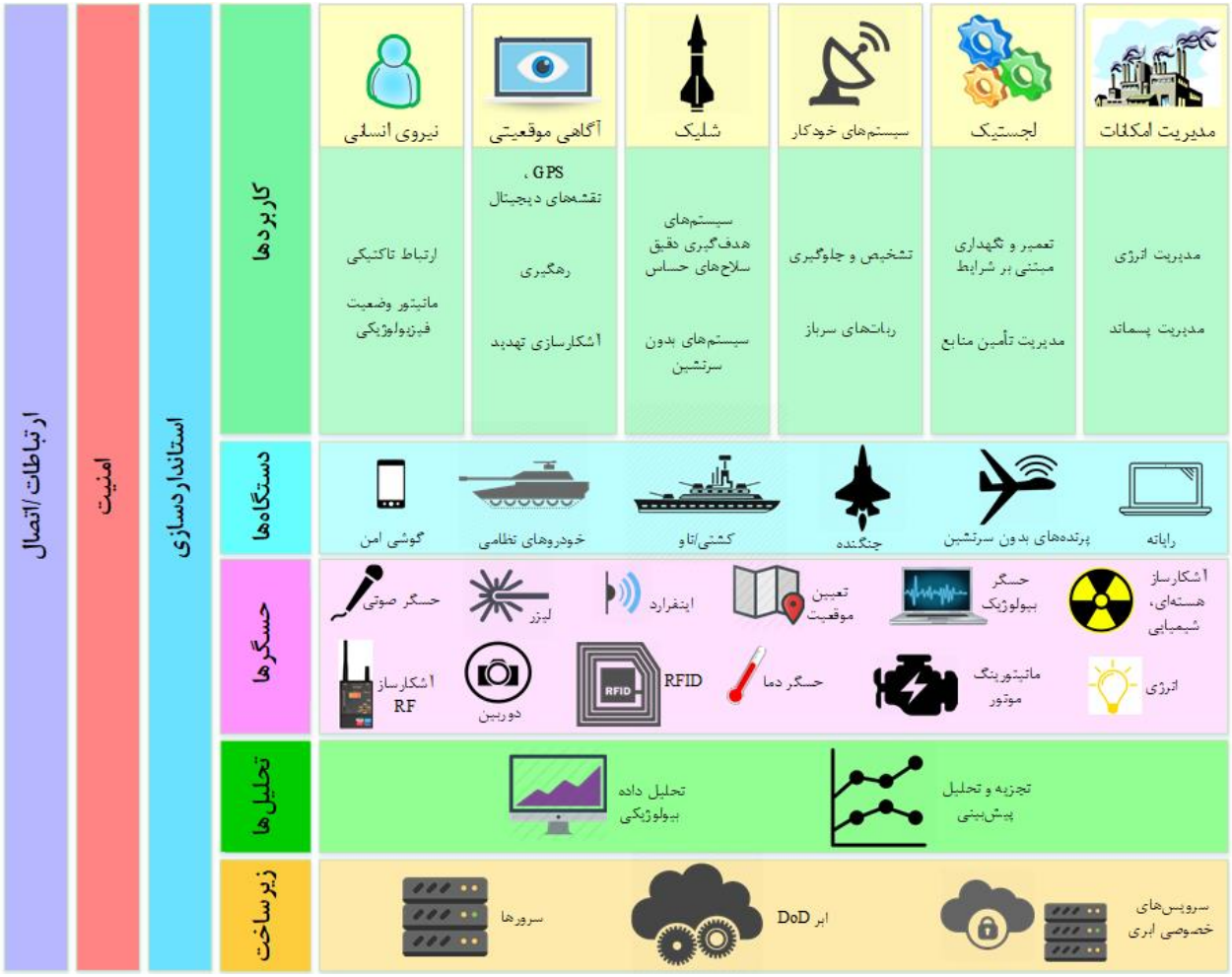
به منظور جمع‌آوری داده‌های نظامی، میلیون‌ها حسگر بر روی حوزه وسیعی از پلتفرم‌ها پیاده‌سازی و توسعه داده شده‌اند. رادار، سونار، ویدئو، فناوری اینفرارد و داده آشکارسازی RF توسط پلتفرم‌های حسگری هوابرد، ماهواره‌های جاسوسی و پرنده‌های بدون سرنشین (UAV)، ایستگاه‌های زمینی و دریایی، سربازان در میدان نبرد، سیستم‌های زمینی متداول توزیع‌شده[2] (DCGS) و پلتفرم اصلی یکپارچه‌سازی-داده C4ISR نظامی جمع‌آوری می‌گردند. DCGS داده مربوط به اطلاعات بالایی و پایینی زنجیره فرامین را بررسی و تحلیل می‌نماید. این سیستم، تصویر جامعی از موقعیت و وضعیت نیروهای خودی و دشمن ارائه داده و امکان بهبود فرآیند تعیین موقعیت و کنترل فضای نبرد را فراهم می‌سازد.

فرماندهان ارشد از طریق مراکز عملیات مرکزی که داده را از پلتفرم‌ها جمع‌آوری می‌نمایند، می‌توانند آگاهی موقعیتی جامعی از وضعیت میدان نبرد داشته باشند. همچنین جنگنده‌ها نیز به داده مربوط به فضاها و نواحی عملیاتی آن‌ها دسترسی دارند. خلبانان جنگی، داده اولویت‌بندی‌شده را از طریق خطوط داده تاکتیکی[3] (TDLs) دریافت می‌کنند که این داده اولویت‌بندی‌شده با داده‌ای که آن‌ها توسط سیستم حسگرهایشان جمع‌آوری نموده‌اند یکپارچه می‌شود تا خلبانان بتوانند تمامی تهدیدات و اهداف را از طریق مانیتورهای موجود در اتاقک کابین (کاکپیت) خود مشاهده نمایند.

۱-۲-۲. سیستم‌های کنترل آتش

سیستم‌های کاملاً اتوماسیون‌شده در حوزه نظامی در بحث‌های کنترل آتش متمرکز می‌باشند. این سیستم‌ها از داده مربوط به حسگرهای مختلف استفاده می‌کنند تا به سرعت واکنش نشان داده و دقت نشانه‌گیری جنگ‌افزارها را فراهم نمایند. برای مثال، سیستم نظارتی نیروی دریایی آمریکا که یک سیستم کنترل-آتش یکپارچه برای کشتی‌های سطحی می‌باشد، امکان ترکیب (عملکردی) کامل با سیستم‌های کنترل آتش اتوماسیون‌سازی‌شده را داراست.

[1] *Network-Centric Warfare*
[2] *Distributed Common Ground System*
[3] *Tactical Data Links*



شکل ۱. معماری اینترنت اشیاء نظامی آمریکا.

این سیستم امکان فرماندهی و کنترل را به صورت کنترل تجهیزات سلاح‌ها در کشتی‌های جنگی سطحی ایالات متحده از توپخانه دریایی و اژدر گرفته تا موشک‌های کروز هدایت‌شونده علیه سلاح‌های ضدموشک فراهم می‌نماید. سیستم راداری AN/SPY می‌تواند مهمات هدایت‌شونده را تشخیص داده، رهگیری نموده و هدایت نماید به گونه‌ای که در یک زمان قادر است تا به طور کاملاً خودکار یکصد هدف را تعقیب و رهگیری نماید[10].

نیروهای نظامی به طور گسترده‌ای بر روی استفاده از پرنده‌های بدون سرنشین (UAV) سرمایه‌گذاری کرده‌اند تا با اهداف ارزشمند دشمن درگیر شوند. خلبانان ایستگاه زمینی از دوربین‌ها و حسگرهای موجود بر روی بدنه هواپیمای بدون سرنشین پریدیتور[14] استفاده می‌کنند تا بتوانند آن را به گونه‌ای پرواز دهند که گویا در داخل کابین آن نشسته‌اند. با استفاده از ترکیب حسگرهای موجود بر روی بدنه پرنده (جنگنده) و اطلاعات به دست آمده از DCGS، پریدیتور اهداف خود را شناسایی نموده و می‌تواند با استفاده از موشک‌های Hellfire و هدایت لیزری با آن‌ها درگیر شود.

همچنین، در مفهوم جنگ شبکه-محور یا مُدل جدیدتر آن یعنی اینترنت اشیاء نظامی، مهمات نیز قابلیت شبکه‌شدن را خواهند داشت و این امر از طریق اجازه دادن به سلاح‌های هوشمند به منظور ردیابی و رهگیری اهداف سیار یا هدایت پرواز قابل تحقق و انجام است. یک نمونه اولیه و مقدماتی، موشک حمله زمینی تام‌هاوک[15] یا همان TLAM می‌باشد که سلاح برتر نیروی دریایی ایالات متحده آمریکا به شمار می‌آید. نوع قالب TLAM 4 یک خط ارتباطی ماهواره‌ای دو-طرفه دارد که اجازه می‌دهد تا بتوان مسیر موشک را به سمت یک هدف جدید هدایت نمود یا این که موشک به آرامی به سمت یک

[14] *Predator*

[15] *Tomahawk Land Attack Missile*

هدف پیش برود در حالی که توسط دوربینی که بر روی آن نصب شده است فیلم صحنه نبرد مربوطه را به کماندوها ارسال می‌کند و آن‌ها می‌توانند اهداف جدیدی را به آن اختصاص دهند و میزان تخریب ناشی از برخوردهای دیگر را ارزیابی نمایند[11]. TLAM همچنین می‌تواند به منظور حمله به هر هدف از پیش تعیین‌شده به خدمت گرفته شود یا اینکه از مختصات جدید GPS به منظور حمله خود استفاده نماید.

۱-۲-۳. لجستیک

حوزه‌های نظامی، فناوری‌های IoT را برای مدیریت لجستیک (تدارکات) در یک سطح و مرتبه محدود به خدمت گرفته‌اند. آژانس لجستیک دفاعی[16] (DLA) و فرمان حمل و نقل[17] (USTRANSCOM) که در آن‌ها مدیریت تدارکات به شاخه‌های سرویس متصل می‌شود، از دستگاه‌های IoT همانند RFID استفاده می‌کنند تا روند حمل و مدیریت موجودی را رهگیری نمایند. برای نمونه، پالت‌ها به وسیله RFID های فعال و غیرفعال مجهز می‌شوند تا فرآیند انتقال منابع و تجهیزات بین مراکز عمده رهگیری و دنبال شوند. همچنین DLA از کارتخوان‌های دیجیتال استفاده می‌کنند تا سطح سوخت مخزن‌ها را کنترل نمایند. سپس این سیستم از نرم‌افزارهای تحلیلی استفاده می‌کند تا شرایط محیطی موثر بر میزان و حجم سوخت مصرفی همانند دما را تنظیم نماید. داده لجستیکی به یک سیستم باطنی با یک واسط ارسال می‌شود تا کاربران بتوانند سفارشات خود را رهگیری کرده و فهرست مواد را که در محیط داده یکپارچه‌شده[18]/همگرائی شبکه حمل و نقل جهانی[19] (IGC) نامیده می‌شود، مانیتور نموده و کنترل نمایند[12].

۱-۲-٤. آموزش و شبیه‌سازی

فناوری مربوطه-IoT همچنین در بحث آموزش و شبیه‌سازی نظامی مورداستفاده قرار می‌گیرند. برای مثال، آموزش زنده شلیک‌خانه که از دوربین‌ها، حسگرهای حرکتی و حسگرهای آکوستیکی به منظور ردیابی و رهگیری سربازان در حین تمرین‌های آموزشی استفاده می‌کند، و داده را به دستگاه‌های سیار و برای آموزش‌دیدگان ارسال می‌کند تا پس از تمرین بتوانند فعالیتشان را بازبینی نموده و اشکالات احتمالی را برطرف نمایند. مثال دیگر، سیستم درگیری لیزری یکپارچه‌شده چندگانه (MILES) می‌باشد که جنگ پیاده‌نظام را با استفاده از فشنگ‌های مشقی و لیزر شبیه‌سازی می‌کند. همانند بازی لیزر-تگ که کودکان و نوجوانان بازی می‌کنند، لیزرها بر روی سلاح‌ها سوار شده و سیگنال‌های کُدشده‌ای را ارسال می‌کنند و زمانی که سرباز یک فشنگ مشقی را در شبیه‌سازی شلیک می‌کند، اگر حسگرهای تعبیه‌شده بر روی لباس و تجهیزات سرباز یک سیگنال لیزری مربوط به یک اصابت گلوله ثبت نماید، با فعال‌کردن یک صدای هشدار می‌توان سرباز کشته‌شده را مشخص کرد. نسخه‌های جدیدتر MILES از مُدل‌کردن رایانه و اتصال استفاده می‌کنند تا تمرین‌های آموزشی جامع‌تری با امکان شبیه‌سازی هر چیز از آتش توپخانه گرفته تا سلاح‌های کشتار جمعی و امکان مانیتورکردن تمرینات به صورت بلادرنگ ارایه دهند.

۱-۲-۵. تحرک

DoD پروژه‌ای در وزارت دفاع ایالات متحده آمریکا آغاز نموده است که فناوری‌های سیار لازم برای جنگنده‌های نظامی و همچنین حتی موارد غیرنظامی را پیاده‌سازی می‌کند. برنامه‌های موبایل مجزا از طریق سرویس‌ها و آژانس‌های انفرادی DoD و با استفاده از پلتفرم‌ها، پروتکل‌ها و ملزومات متفاوت توسعه داده می‌شوند. این برنامه‌ها تحت نظر افسر ارشد اطلاعات DoD[20] (CIO) با یک کارگروه هماهنگ شده و می‌توانند اطلاعات را میان خود به اشتراک گذاشته و در مواقع موردنیاز بهترین واکنش و عمل را انجام دهند.

بیش از یک دهه است که مبحث تحرک و سیاربودن تاکتیکی در حوزه نظامی توسعه داده شده است. برنامه جنگجوی ارتش Nett با نام اختصاری NW و برنامه جنگجوی زمینی که قبلاً به انجام رسیده است، چندین سال زمان صرف توسعه دستگاه‌های ایمن اندرویدی برای پیاده‌نظام و با استفاده از یک نسخه اختصاصی از سیستم عامل اندروید نموده است. این دستگاه‌ها که نسخه‌های اصلاح‌شده گوشی‌های هوشمند

[16] *Defense Logistics Agency*
[17] *Transportation Command*
[18] *Integrated Data Environment*
[19] *Global Transportation Network Convergence*
[20] *Chief Information Officer*

COTS Samsung Note می‌باشند به رادیوی تفنگدار با قابلیت–اتصال داده متصل می‌شوند و هدفشان اتصال سربازان میدان نبرد به امکانات و برنامه‌هایی همچون نقشه‌های سه–بُعدی، ردیابی نیروها، ترجمه زبان‌ها و پروفایل اهداف ارزشمند[21] (HVTs) می‌باشد. امروزه، این برنامه‌ها در پایگاه‌های محدودی به صورت آزمایشی (پایلوت) اجرا شده‌اند اما توسعه گسترده‌تر آن به دلیل ضعف ارتباط و اتصال، عاملیت محدود و تجربه اندک کاربران مختل شده است.

در این زمینه، نیروی هوایی ایالات متحده رویکرد بسیار متفاوتی اتخاذ نموده است: توسعه برنامه‌ها بر روی آی‌پد[22] تجاری به منظور پشتیبانی از طیف وسیعی از کاربردها. برنامه‌نویسان پایگاه هوایی اسکات آمریکا، به منظور برنامه‌ریزی بارگیری‌ها و مهمات هواپیماهای باری KC-10 یک برنامه کشیدن–و–انداختن[23] را توسعه داده‌اند و به دلیل توسعه این برنامه جایزه دولتی نوآوری در تکنولوژی ایالات متحده را از آن خود کرده‌اند. همچنین نیروی هوایی درصدد است تا با استفاده از آی‌پدها دستورالعمل‌های تجهیزات الکترونیکی را به پرسنل تعمیر و نگهداری ارائه دهد و این آی‌پدها جایگزین لپ‌تاپ‌های لمسی سنگین و زمختی می‌شوند که محدودیت طول عمر کم و باطری محدود دارند[13].

در حال حاضر، پنتاگون برنامه تحرک آژانس سیستم اطلاعات دفاعی[24] **(DISA)** را در حال اجرا دارد که شامل پیاده‌سازی یک بسته نرم‌افزاری برای دستگاه‌های اندرویدی مورد تأیید آژانس امنیت ملی آمریکا[25] **(NSA)** می‌باشد تا بخش‌های اجرایی DoD[26] بتوانند به سرویس‌های تجاری IT مثل ایمیل DoD متصل شوند. این برنامه شامل دستگاه‌های امنی می‌شوند که قادرند تا به شبکه طبقه‌بندی‌شده محرمانه DoD که SIPRNet نام دارد، دسترسی یابند. مهندسان همچنین بر روی راهکارهای احرازاصالت و امنیتی کار می‌کنند تا به رهبران DoD امکان اتصال به اطلاعات حساس محرمانه سازمان از طریق دستگاه‌های موبایلشان فراهم نماید؛ به طوری که آن‌ها قادر خواهند بود تا این اطلاعات حساس را بر روی دستگاه‌های موبایل خود مشاهده نمایند[14].

۲. مفهوم و معماری MIoT

۲-۱. مفهوم MIoT

جنگ مبتنی بر اطلاعات به طور عمده از جنگ مُدرن شکل می‌گیرد و جنگ(افزار) شبکه–محور NCW[27] فرض استراتژیک نیروها و قوای نظامی ایالات متحده آمریکا است که در آن، مفهوم جدیدی از جنگ مطرح است و با پلتفرم (بستر) جنگ–محور سنتی قابل مقایسه می‌باشد. در پلتفرم جنگ–محور، اطلاعاتی که در روند جنگ تسهیم و به اشتراک گذاشته می‌شود، خیلی اندک است. NCW می‌تواند تمامی انواع نیروها (زمینی، هوائی، دریایی) را به هم متصل نموده، پلتفرم‌های سلاح در میدان نبرد را به یک شبکه اطلاعات واحد وصل نماید و یک شبکه یکتا تشکیل دهد که در آن تسهیم (به اشتراک‌گذاری) بلادرنگ اطلاعات، کوتاه‌شدن زمان اخذ تصمیم، و زمان اعلام فرامین و افزایش بهره‌وری عملیات مشترک را توسعه خواهد داد. ایده کلیدی NCW این است که سلاح‌ها می‌توانند تنها با اتصال به سیستم واحد مزیت‌های بیشتر داشته باشند و این مطلب به طور ذاتی مربوط به ایده کلیدی IoT است. با استفاده از ایده کلیدی IoT، تمامی انواع نیروهای عملیاتی، واحدها و عناصر برای تحقق بخشیدن به جامعه اطلاعاتی و تسهیم آن‌ها میان موجودیت‌ها متصل می‌شوند که این امر باعث بهبود عملکرد سیستم و کارآیی آن می‌شود[15].

با توسعه سریع ارتباطات، فناوری‌های نرم‌افزاری و شبکه، فناوری‌های نظامی جدید مختلفی چون فناوری تشخیص و شناسائی حسی، فناوری ادغام اطلاعات، فناوری شبکه ارتباطات، فناوری محاسباتی پیشرفته، فناوری تصمیم‌گیری فرامین و فناوری امنیت اطلاعات قابل دسترسی و عملی‌شدن خواهند داشت. این فناوری‌ها تأثیرات مهمی بر روی پردازش اطلاعات، معماری سیستم و مشخصه فناوری IoT دارند. به

[21] *High-Value Targets*
[22] *iPad*
[23] *Drag-and-Drop*
[24] *Defense Information System Agency's (DISA) Mobility Program*
[25] *National Security Agency*
[26] *Department of Defense*
[27] *Network Centric Warfare*

طور مشابهی این فناوری‌ها پشتیبانی برای کاربردهای نظامی IoT را ارائه می‌نمایند[14].

MIoT می‌تواند زیرساخت فیزیکی نظامی و زیرساخت اطلاعات را به طور عمیقی با هم بیامیزد و قابلیت اتصال اشیاء نظامی را به یکدیگر فراهم نماید. MIoT می‌تواند امور متنوع نظامی را با دقت بیشتر و پویاتری پیاده‌سازی نموده و مدیریت نماید تا بحث هوشمندی تجهیزات محقق گردد، که این امر باعث استفاده کامل از منابع نظامی شده و میزان کارآیی عملیات نظامی را افزایش خواهد داد. MIoT قابلیت استفاده و به کاربردن در C2[۲۸]، ISR[۲۹]، لجستیک نظامی، پشتیبانی سلاح و مانیتورینگ محیطی را دارد تا روی هم‌رفته قابلیت استفاده از سیستم مبتنی بر اطلاعات را تقویت نماید[16].

۲-۲. معماری MIoT

توسعه و گسترش فناوری‌های IoT و گشایش ملزومات کاربردهای نظامی، مفهوم MIoT را معنی داده و تعریف می‌کند. معماری MIoT، مشخصه‌ها و ملزومات تمامی انواع کاربردهای نظامی را ترکیب کرده و در هم می‌آمیزد، سرویس کلی MIoT را توصیف کرده و در یک کلام، یک نمایش ساختاری از تابع، رفتار و نقش موجودیت‌ها در MIoT می‌باشد. با ترکیب وضعیت تحقیقات کنونی IoT، یک معماری پنج لایه از MIoT شامل لایه‌ی سنجش[۳۰]، لایه دسترسی[۳۱]، لایه شبکه[۳۲]، لایه سرویس[۳۳] و لایه کاربرد[۳۴] ارائه شده است که در شکل۲ قابل مشاهده می‌باشد[17].

لایه سنجش از مجموعه تجهیزات و حسگرهای مختلف اطلاعات شامل رادار، سونار، حسگر، RFID و غیره تشکیل شده است. داده مربوط به این لایه اساساً بحث حسگری و سنجش داده را محقق نموده و همچنین پیاده‌سازی MIoT را کنترل می‌کند. لایه دسترسی از گره‌های ایستگاه پایه و گره‌های حوزه یا سینک تشکیل شده است که از طریق سیستم‌های سیمی و بی‌سیم به یکدیگر متصل می‌شوند تا کنترل شبکه و ترکیب اطلاعات گره‌های انتهائی محقق گردد. در همان زمان، لایه دسترسی همچنین می‌تواند انتقال اطلاعات گره‌های انتهایی را پیاده‌سازی نماید. لایه شبکه از شبکه ارتباطی سیمی، شبکه ارتباطی بی‌سیم و شبکه‌های LAN خاص و غیره تشکیل می‌شود. لایه شبکه هسته اصلی شبکه برای بارگذاری اطلاعات منتقل‌شده به شمار می‌رود و شبکه انتقال و ارسال پایه را برای کاربردها و سرویس‌های عظیمی فراهم می‌نماید[17].

لایه سرویس از سرویس ذخیره‌سازی داده، سرویس محاسبه داده، سرویس جستجوی داده، سرویس امنیت سیستم، سرویس پشتیبانی کاربرد و غیره تشکیل می‌شود که می‌تواند قابلیت ذخیره‌سازی محاسبات اساسی و قابلیت سرویس اطلاعات عمومی برای سیستم کاربردی و کاربر MIoT را فراهم نماید. اساساً لایه کاربرد به منظور پشتیبانی حوزه کاربردهای مختلف همچون C2، ISR، پشتیبانی لجستیک، مدیریت‌کردن توزیع فیزیکی و غیره مورد استفاده قرار می‌گیرد. بر اساس لایه سرویس، لایه کاربرد راه‌حل‌های کاربردی نظامی جزئی و تفصیلی همچون فرامین و دستور نیروها، کنترل سلاح، مانیتور میدان جنگ، پشتیبانی تجهیزات، نظارت و شناسائی، لجستیک نظامی، درمان‌های پزشکی و نجات در میدان جنگ پیشنهاد می‌شود[17].

این معماری سیستم می‌تواند یک راه‌حل غیرتجسمی و متمرکز MIoT در نظر گرفته شود و همین‌طور می‌تواند یک ساختار قابل استفاده مجدد برای توسعه و کاربرد MIoT فراهم نماید که در اصل مشخصه‌های کاربردهای MIoT را نشان می‌دهد[17].

۲-۳. چالش‌های اینترنت اشیاء نظامی آمریکا

به طور کلی، چالش‌های عملیاتی‌شدن اینترنت اشیاء نظامی ایالات متحده آمریکا به صورت زیر می‌باشد؛ البته توجه شود که چالش‌های امنیتی نیز در کنار این دسته از چالش‌ها قرار می‌گیرند که در بخش‌های دیگر مقاله به آن‌ها پرداخته خواهد شد[8].

۱. وابستگی فرآیند جمع‌آوری داده به ورودی دستی اطلاعات: بسیاری از سیستم‌های یکپارچه جمع‌آوری داده DoD به ویژه در حوزه‌های لجستیکی متکی به ورود داده به

[28] *Command and Control*
[29] *Intelligent, Surveillance and Reconnaissance (ISR)*
[30] *Sense layer*
[31] *Access layer*
[32] *Network layer*
[33] *Service layer*
[34] *Application layer*

صورت دستی هستند. زنجیره تأمین توسط DLA و USTRANSCOM مابین هاب‌های اصلی با استفاده از برچسب‌های RFID رهگیری می‌شوند، اما زمانی که زنجیره شکسته شده و فراتر از هاب‌های مرکزی توزیع شوند، بحث رهگیری تبدیل به یک کار دستی می‌شود. افسران تأمین، سفارشات را بر روی کاغذ امضا نموده و اعداد سریال قطعات را با دست وارد ترمینال‌های کامپیوتری می‌نمایند. این رویکرد در میدان نبرد برای افسران لجستیکی سنگین بوده و احتمال بروز خطر انسانی به طور معنی‌داری محل تهدید می‌باشد[14].

۲. پردازش محدود داده موجود: یکی از بزرگترین خلأها در اکوسیستم داده وزارت دفاع ایالات متحده (DoD) بحث تحلیل دیجیتال می‌باشد. حسگرهای تعبیه‌شده در دستگاه‌ها مقدار و حجم بسیار زیادی از اطلاعات را جمع‌آوری می‌نمایند اما اغلب، داده‌ها هرگز پردازش یا تحلیل نمی‌شوند. به عنوان یک نتیجه، بسیاری از اطلاعات هرگز مورد استفاده قرار نمی‌گیرند؛ آن قسمتی هم که استفاده می‌شوند اغلب توسط یک انسان و به صورت دستی تحلیل می‌شود و نهایتاً تبدیل به داده قابل استفاده برای کاربران-نهایی می‌گردد. هرچند که انجام پردازش‌ها توسط انسان می‌تواند در یک نگاه امنیت سیستم را نسبتاً افزایش دهد، اما وابسته‌بودن به پردازش دستی می‌تواند منجر به بروز تأخیرهای معناداری در گرفتن اطلاعات مهم توسط آن دسته از افرادی شود که می‌توانند بر روی آن اطلاعات عمل نمایند، و این می‌تواند باعث شکست مأموریت‌ها گردد، و یا رهبران و فرماندهان را بدون داشتن آگاهی از تمامی حقایق مربوطه مجبور به اتخاذ تصمیمات نماید[18].

۳. فقدان اتوماسیون: می‌توان گفت که خودکارسازی و اتوماسیون هدف نهایی IoT است؛ بدین معنی که در مفهوم اینترنت اشیاء، دستگاه‌های هوشمند مختلف به صورت خودکار و بدون دخالت انسان با یکدیگر ارتباط برقرار نموده و فعالیت می‌نمایند. کاربرهای نهایی IoT از حسگرها، RFID ها و تحلیل‌های دیجیتال استفاده می‌کنند تا پاسخ‌های اتوماسیون‌شده و خودکار را تولید نمایند. فناوری‌های مربوط به-IoT **که** توسط حوزه نظامی توسعه داده شده‌اند فاقد اتوماسیون می‌باشند. برای مثال، اکثر سیستم‌های بدون سرنشین، خودمختار (خودکار) نیستند و به صورت از راه دور و توسط اپراتورهای انسانی هدایت و کنترل می‌شوند. اتوماسیون فرآیند صدای موج می‌تواند به طور معناداری کُشندگی و بقای جنگ‌افزارها و همچنین کارآیی عملیات‌های DoD را افزایش داده و در مقابل تعداد نفرات موردنیاز برای اتمام یک مأموریت و احتمال بروز خطای انسانی را کاهش داده و زمان واکنش را بهبود بخشد[8].

٤. معماری تکه‌تکه IT: بزرگترین مشکل در رابطه با سیستم‌های فناوری نظامی، تکه‌تکه[35] بودن آن است. حوزه نظامی فاقد یک معماری منسجم IT است که بتواند از کاربردهای IoT که کارآمد و قابل دفاع باشند، پشتیبانی نماید. سیستم‌های IT از طریق سرویس‌های مسلح نظامی و آژانس‌های DoD به شبکه‌های DoD متصل می‌شوند، اما در عین حال به طور مستقل و با توجه به ملزومات متفاوت توسعه داده می‌شوند. اغلب، چندین سرویس در یک عملیات درگیر می‌شوند یا چندین آژانس در یک فرآیند درگیر می‌گردند اما اطلاعات باید میان سیستم‌ها به صورت دستی عبور داده شوند که هم ناکارآمد است و هم اینکه احتمال بروز خطای انسانی را افزایش می‌دهد. بحث تکه‌تکه بودن معماری IT مربوط به DoD، توسعه و استفاده امنیتی متداول را مشکل می‌سازد[19].

۳. نقش IoT در کاربردهای نظامی

چندین حالت استفاده و کاربرد با تأثیر- بالا به منظور پیاده‌سازی و استفاده از IoT در محیط‌های نظامی وجود دارد. برخی از این کاربردها در ادامه به اختصار توصیف می‌شوند. مباحث کاربردی جزئی‌تر IoT در عملیات‌های نظامی در مرجع [8] قابل مطالعه می‌باشد.

۳-۱. تجهیزات هوشمند

اینترنت اشیاء برای تجهیزات گوناگون و گسترده نظامی همانند وسایل نقلیه، سیستم‌های پشتیبانی و حتی سلاح‌ها قابل استفاده می‌باشد. بسیاری از چنین اشیاء فعال شبکه قابل اشاره هستند که رخنه‌های معنی‌دار و آسیب‌پذیری‌های مسأله‌ساز و جدی دارند. به‌ویژه، چندین آسیب‌پذیری جدی در وسایل نقلیه شناسایی شده است که منجر به فراخوانی‌های گسترده این

[35] *Fragmentation*

خودروها شده است[23-20]. همچنین نمونه‌هایی از سوءاستفاده و بهره‌برداری‌های دشمن از نقاط ضعف موجود در امنیت سیستم‌های سایبری- فیزیکی نظامی وجود دارد[24]. به طور مشابه، محققین نیز اخیراً آسیب‌پذیری‌های امنیتی مهمی در سلاح‌های هوشمند موجود تجاری شناسایی نموده‌اند[25].

۳-۳. لجستیک

استفاده از IoT شامل حسگرها و RFID، پایه‌ای‌ترین الزام برای بهبود کارآیی و اثربخشی عملیات لجستیکی به شمار می‌رود. این الزام شامل قابلیت همکاری با سیستم‌های لجستیکی بخش-سوم می‌شود، چرا که تجهیزات پشتیبانی موردنیاز در خلال عملیات‌های نظامی تنها شامل تجهیزات نظامی نمی‌گردد، بلکه همچنین مواد غذایی و پزشکی برای نیروها را نیز در بر می‌گیرد. استفاده از سیستم‌های IoT در لجستیک همچنین می‌تواند به ایمنی بیشتر عملیات لجستیکی بیانجامد. برای مثال به وسیله جلوگیری از حمل و نقل مشترک برخی کالاها و محصولات همچون اجزای شیمیایی که می‌تواند منجر به واکنش‌های شیمیایی خطرناک شوند یا بخش‌های تجهیزات رمزنگاشتی که نباید به هیچ وجه توسط یک دشمن شنود گردند[26]. به هر حال، در گذشته نشان داده شده که تجمیع نامناسب راه‌حل‌های ردیابی RFID با دیگر سیستم‌ها می‌تواند منجر به مسیرها و روش‌های جدید حمله به سیستم‌های اطلاعاتی گردد[27].

همچنین فقدان یک محافظت مناسب از محرمانگی می‌تواند مهاجم را قادر به اجرای بهتر حملات هدف‌دار بر روی کاروان‌های حمل و نقل یا استفاده از اطلاعات به عنوان یک کانال جانبی برای استدلال در مورد عملیات نظامی برنامه‌ریزی شده می‌نماید. به طور مشابه، محافظت از یکپارچگی و دسترس‌پذیری می‌تواند توسط یک مهاجم به منظور تأثیر عملیات لجستیکی مورد بهره‌برداری قرار گیرد؛ برای مثال به وسیله مسیریابی مجدد بداندیشانه کالاها و تجهیزات. تمامی این ریسک‌ها باید زمانی به حساب آورده شوند که کاربردهای لجستیکی IoT- فعال برای مقاصد نظامی طراحی می‌گردند.

۳-٤. مراقبت پزشکی

کمک در درمان‌های پزشکی در شرایط اضطراری و جراحی‌های حین نبرد و عملیات یکی از مهمترین و متداول‌ترین کاربردهای سیستم‌های IoT ایستا و تجهیزات هوشمند پوشیدنی در محیط نظامی محسوب می‌شود. به هر حال، در کنار پتانسیل بالا برای بهبود سرعت و صحت حمل و نقل اشیاء، نجات افراد و درمان پزشکی سربازان، سیستم‌های مراقبت پزشکی هوشمند و سیستم‌های مانیتورینگ سلامت نوعاً با تجهیزات بی‌سیم و با قابلیت برقراری ارتباط میان دستگاه‌ها و سیستم‌های پزشکی مختلف مستقر تجهیز می‌شوند. این تجهیزات و سیستم‌های پوشیدنی یا تعبیه‌شونده برخی آسیب‌پذیری‌های امنیتی دارند که نمونه‌هایی از آن‌ها در مراجع [28-30] نشان داده شده‌اند.

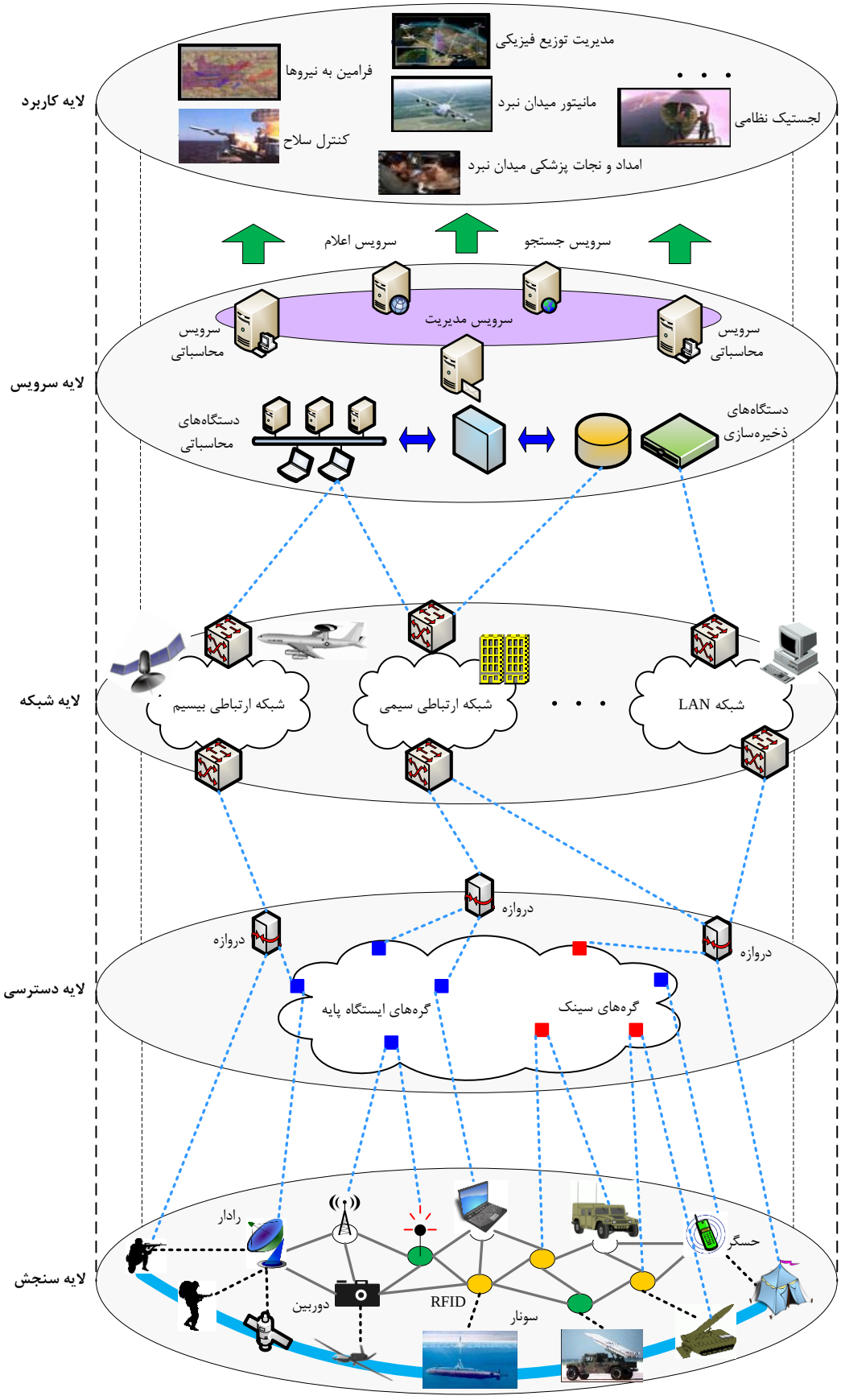
٤. MIoT و تهدیدهای امنیتی

همانند هر فناوری جدید، IoT نیز یکسری حملات جدید در سیستم‌های IT نظامی با خود به همراه دارد. برخی از معروف‌ترین تهدیدات و حملات شامل موارد زیر می‌شود[14]:

۱. دستگاه‌های IoT (شامل سنسورها و عملگرها)
۲. کانال‌های ارتباطی میان دستگاه‌ها و همچنین میان دستگاه‌ها و سیستم‌های انتهایی- پشتی
۳. امنیت شبکه
٤. ذخیره‌سازی داده
۵. امنیت و حریم‌خصوصی حین پردازش داده
٦. حملات داخلی (سوء استفاده کاربران)
۷. حملات مربوط به کاربردهای خاص IoT

٤-۱. آسیب‌پذیری‌ها

مطالعه اخیر [31] بر روی ۵۰ دستگاه هوشمند که عموماً هم در حوزه کاربردی خانه هوشمند قرار دارند، نشان داد که هیچ یک از دستگاه‌ها از کلمه عبور قوی و احرازاصالت متقابل استفاده نمی‌کنند یا از حساب‌های کاربری محافظت‌شده در برابر حملات جستجوی کور استفاده نمی‌کنند.



شکل۲. معماری سیستم MIoT.

تقریباً دو دستگاه از هر ده دستگاه از برنامه‌های کاربردی موبایل به منظور کنترل دستگاه‌های IoT استفاده می‌کردند که این برنامه‌های موبایلی از پروتکل امنیتی SSL به منظور امن‌نمودن و رمزگذاری ارتباطات با ابر بهره نمی‌برند. به ویژه، برخی از پُرتال‌های وِب مورداستفاده به منظور کنترل دستگاه‌های IoT آسیب‌پذیری‌های جدی داشتند که اجازه دسترسی غیرمجاز به سیستم انتهایی- پشتی را می‌دهد.

پروژه امنیت نرم‌افزار وِب متن باز (OWASP) فهرستی از ده آسیب‌پذیری جدی اینترنت اشیاء ارائه نموده [32] که سطح حمله کاربردهای IoT را تعریف می‌کند:

۱. واسط وب ناامن
۲. احرازاصالت/مجازشناسی ناکافی
۳. سرویس‌های ناامن شبکه‌ای
٤. فقدان رمزگذاری انتقال
۵. نگرانی‌های حریم خصوصی
٦. واسط ابری ناامن
۷. واسط موبایلی ناامن
۸. قابلیت پیکربندی امنیتی ناکافی
۹. نرم‌افزار/میان‌افزار ناامن
۱۰. امنیت فیزیکی ضعیف

٤-۲. ریسک‌های امنیتی MIoT ایالات متحده

مهمترین چالش برای پیاده‌سازی IoT در حوزه نظامی، امنیت است. IoT می‌تواند به منظور جمع‌آوری و ارسال داده مربوط به موقعیت، وضعیت و تحرک نیروها، مواد و تجهیزات مورد استفاده قرار بگیرد. همان‌طور که هیئت مدیره علوم دفاعی آمریکا در گزارش سال ۲۰۱۳ میلادی اشاره نموده، اگر شبکه‌های DoD با خطر مواجه شده و فاش شوند، اسلحه‌ها، موشک‌ها و بمب‌های ایالات متحده شلیک نمی‌کنند یا ممکن است بر سر نیروهای خودی فرود آیند. ممکن است در زمان و مکانی که موردنیاز است، تأمین غذا، آب، دارو و سوخت به موقع به انجام نرسد[33].

نگرانی اصلی این است که شبکه‌هایی که به طور کافی امن‌سازی نشده‌اند، می‌توانند اطلاعات مفیدی در مورد وضعیت نیروها، روند استقرار و گسترش تجهیزات و تأمین‌ها و غیره را در اختیار دشمن قرار دهند که این اتفاق به دشمن اجازه می‌دهد تا تحرکات نیروهای ایالات متحده را پیش‌بینی نماید. همچنین، نگرانی دیگری در مورد دستکاری‌های احتمالی یا قطع احتمالی جریان‌های داده مابین واحدها، یا تغییر داده به منظور دادن اطلاعات غلط به فرماندهان، و یا جلوگیری از اینکه واحدها مأموریت خودشان را به درستی انجام دهند نیز وجود دارد.

امنیت شبکه و دستگاه: بخش بزرگی از ارزش IoT از خاصیت و ویژگی همه‌جا حاضربودن دستگاه‌ها و کاربردهای IoT و همچنین ارتباطات میان آن‌ها ناشی می‌شود. این مطلب فضای وِب وسیعی از نقاط ورودی بالقوه برای مهاجمان سایبری فراهم می‌کند. این سیستم‌ها همچنین بسته به اتصال، ذخیره‌سازی و پردازش، نقاطی آسیب‌پذیر برای استفاده مهاجم تولید می‌کند.

یکی از بهترین راه‌ها برای افزایش امنیت شبکه‌های پیچیده، محدودکردن نقاطی (گره‌هایی) است که یک مهاجم می‌تواند از هر نقطه ورودی مشخصی به آن‌ها دسترسی داشته باشد. به هر حال، اساساً این رویکرد برای امن‌سازی معماری شبکه با مفهوم IoT که بیشترین ارزش خود را از یکپارچه‌سازی سیستم‌ها و داده کسب می‌کند در تضاد است. امن‌سازی دستگاه‌های IoT نیز کار دشواری است. بسیاری از دستگاه‌های IoT به لحاظ فیزیکی کوچک بوده و ظرفیت محاسباتی و ذخیره‌سازی محدودی دارند، هیچ واسط کاربری انسانی و یا هیچ تعامل انسانی ندارند و به یکپارچه‌سازی بلادرنگ داده وابسته می‌باشند. این مطلب، رویکردهای مرسوم برای امنیت همانند معماری جزءشدن، رمزگذاری پیشرفته و فرآیندهایی همچون احرازاصالت چندگانه را که به کندی انجام داده یا از تبادل داده میان دستگاه‌ها و سیستم‌ها بر روی شبکه جلوگیری می‌نمایند، چرا که نیاز به توان محاسباتی بیشتری بر روی دستگاه‌ها دارند تا داده را رمزگشایی نموده یا احرازاصالت را انجام دهند یا این که نیاز به ورودی انسانی برای احرازاصالت دارند[14].

تهدیدات داخلی و خطای کاربر: با وجود بیش از ۳ میلیون کارمند در DoD، تهدیدات داخلی یک نگرانی اصلی برای آن به شمار می‌رود. تمرین سایبری خوب برای کارکنان همواره یک چالش بزرگ برای تمامی سازمان‌های بزرگ محسوب می‌شود. برنامه‌ها برای آموزش کاربران در مورد ریسک‌های سایبری

می‌تواند کمک کند اما تنها با یک اشتباه از سوی یک کاربر، یک مهاجم می‌تواند با روش‌هایی نه چندان پیچیده امکان دسترسی به سیستم را پیدا کند[34].

جنگ الکترونیک: چالش دیگر پیاده‌سازی IoT این است که اینترنت اشیاء سیستم‌ها را در برابر جنگ الکترونیک آسیب‌پذیر می‌سازد. اکثر فناوری‌های IoT از ارتباطات بی‌سیم بر روی فرکانس‌های رادیویی استفاده می‌نمایند. مهاجمان می‌توانند تکنیک‌های نه چندان پیچیده مثل مسدودسازی سیگنال RF[۳۶] را استفاده نمایند تا این سیگنال‌ها را مسدود نمایند، و باعث شوند تا دستگاه‌ها نتوانند با زیرساخت خود در شبکه ارتباط داشته باشند. ارتباطات بی‌سیم همچنین تهدید افشای موقعیت مکانی نیروهای ایالات متحده را به واسطه ارسال‌های RF بالا می‌برند. اساساً دستگاه‌های ارسال‌کننده می‌توانند توسط هر گیرنده رادیویی که در حوزه فرکانسی آن باشد، تشخیص داده شده و آشکار شوند. ارسال مختصات سه‌گانه از فرستنده‌ها نیز می‌تواند موقعیت مکانی سربازان یا وسائط نقلیه فاش نماید[14].

اتوماسیون، عامل افزاینده تهدیدها: IoT با مباحث همه‌جا حاضر بودن و اتوماسیون عجین است و این ویژگی‌ها باعث تشدید چالش‌های امنیت DoD می‌گردند. حجم دستگاه‌ها، شبکه‌ها، زیرساخت و داده شامل IoT باعث می‌شود تا امنیت یک چالش اصلی به حساب آید. در کل، اتوماسیون‌سازی تجهیزات و وسایل نقلیه باعث گسترش تهدیدات سایبری به حوزه فیزیکی شده و احتمال بروز صدمات فیزیکی به دستگاه‌ها را افزایش می‌دهد[17].

٤-۲. حریم‌خصوصی

پیامدهای حریم‌خصوصی IoT تبدیل به موضوعی برای تحقیقات و زمینه مورد علاقه در اروپا [35] و آمریکا [36] شده است. هرچند که حریم‌خصوصی در خلال عملیات‌های نظامی جزء نگرانی‌های اولیه و جدی محسوب نمی‌شود اما NATO و کشورهای عضو آن مجبورند تا از قوانین حریم‌خصوصی ملی لازم‌الاجرا نسبت به پرسنلشان پیروی نمایند. بنابراین توجه به این نکته اهمیت دارد که راه‌حل‌های پیاده‌سازی شده IoT به هیچ وجه نباید تهدیدی علیه حریم‌خصوصی پرسنل اعمال نمایند و تمامی اطلاعات شخصی جمع‌آوری شده باید به اندازه کافی هم در انتقال و هم در ذخیره‌سازی محافظت گردند.

۵. ملزومات امنیتی برای MIoT

ملزومات امنیتی برای سیستم‌های IoT نظامی متفاوت از ملزومات امنیتی برای دیگر سیستم‌های IT که در محیط‌های نظامی مورداستفاده قرار می‌گیرند، نیستند. به طور کلی همان نگرانی‌ها پیرامون محرمانگی، یکپارچگی و دسترس‌پذیری وجود دارد که در ادامه به آن‌ها می‌پردازیم. البته به اختصار به روش‌های رمزنگاری مطرح برای رفع نگرانی‌های مطرح نیز اشاره‌ای می‌نماییم.

۵-۱. محرمانگی

محرمانگی یک رویکرد مهم از هر عملیات نظامی به شمار می‌رود. در حالت استفاده از سیستم‌های IoT، محافظت محرمانگی برای تمامی کانال‌های ارتباطی، ذخیره‌سازی و پردازش داده هم در گره‌های انتهایی مهم در سیستم انتهایی-پشتی موردنیاز می‌باشد. برای مثال، در حالت شبکه‌های حسگر بی‌سیم یا وسایل نقلیه بدون سرنشین، افشای محرمانگی ممکن است به وسیله سرنخ دادن در مورد نقشه‌های نظامی و فراهم‌نمودن پشتیبانی غیرعمدی به دشمن از طریق دادن اطلاعات به او و افزایش آگاهی‌های موقعیتی و مکانی دشمن هم نیروهای خودی و هم اهداف عملیات را به خطر بیاندازد. یک نمونه از دنیای واقعی مصداق چنین تهدیدی در دسامبر ۲۰۰۹ و زمانی بود که نظامیان عراقی به لینک ارسال ناامن که توسط پرنده‌های بدون سرنشین آمریکا مورداستفاده قرار می‌گرفت دسترسی پیدا کردند[23].

در این حوزه، رمزنگاری متقارن در هر دو بخش رمزهای قالبی و رمزهای جریانی مورد توجه قرار دارد. با توجه به این که عموماً در فضای اینترنت اشیاء با دستگاه‌هایی با منابع انرژی محدود و همچنین توان محاسباتی پایین سروکار داریم، رویکردهای رمزنگاشتی سبک‌وزن بیشتر مورد توجه می‌باشند. از این رو، در میان رمزهای قالبی الگوریتم‌های CLEFIA، PRESENT و AES و نیز در حوزه رمزهای جریانی

[۳۶] *Jamming*

الگوریتم‌های Grain v1، MICKEY v2 و Trivium کاندیدهای اصلی می‌باشند[37].

۵-۲. یکپارچگی

یکپارچگی برای بسیاری از رویکردهای سیستم‌های IoT نظامی ضروری می‌باشد. به وضوح، اهمیت دارد که اطلاعات ارسالی به مرکز فرماندهی و کنترل توسط اشیای هوشمند نباید در میان راه دچار تغییر و دستخوردگی گردد و به عبارت دیگر باید اعتماد و اعتبار کافی برای استفاده در تصمیمات فرامینی را داشته باشد. به هر حال، به همان اندازه هم اهمیت دارد که دستور و اطلاعات مکانی فراهم‌شده توسط اشیای هوشمند نیز دارای یکپارچگی مناسب باشند.

برای مثال در دسامبر ۲۰۱۱ میلادی، جمهوری اسلامی ایران توانست به طور موفقیت‌آمیزی UAV شناسایی آمریکا به نام RQ-170 را از طریق ارسال سیگنال‌های فریب GPS[۳۷] که پرنده RQ-170 دریافت کرده بود تا به محل پرتابش بازگردد و فرود آید، پایین آورد. یکپارچگی تنها یک ویژگی از اطلاعات نیست، بلکه یک ویژگی از کل یک سیستم است که در آن یکپارچگی اشاره به حصول اطمینان از دست نخوردن پیکربندی یک سیستم می‌نماید[7].

نقض یکپارچگی یک سیستم ممکن است تأثیر مصیبت‌باری بر روی محرمانگی، یکپارچگی و دسترس‌پذیری داده پردازش‌شده توسط چنین سیستمی داشته باشد. اهمیت این حوزه منجر به توسعه برنامه تحقیقاتی DARPA در حوزه سیستم‌های نظامی سایبری با قابلیت اطمینان بالا شد[38-39].

ابزاری که برای حفظ یکپارچی مورد استفاده قرار می‌گیرند توابع چکیده‌ساز می‌باشند. آخرین استاندارد توابع چکیده‌ساز، SHA-3 می‌باشد که در سال گذشته میلادی استانداردسازی شد. البته این تابع چکیده‌ساز خیلی هم سبک‌وزن محسوب نمی‌شود و به نظر می‌رسد که می‌توان از جایگزین‌هایی استفاده نمود که مبتنی بر رمزهای قالبی سبک‌وزن طراحی و پیاده‌سازی شده‌اند[40].

۵-۳. دسترس‌پذیر بودن

اگر دسترسی موردنیاز به اطلاعات ارسالی از حسگرها و دستگاه‌ها وجود نداشته باشد، استفاده از پتانسیل کامل اینترنت اشیاء در محیط‌های نظامی قابل دستیابی نخواهد بود. به طور مشابه، اطلاعات فرمان و کنترل باید در مواقع لزوم برای عملگرها و دستگاه‌های هوشمند قابل دسترسی باشد. یک رویکرد مشخص از دسترسی مرتبط با IoT به حمله خواب-محرومیت[۳۸] معروف است. این نوع حمله به طور مشخص دستگاه‌های دارای باطری را هدف قرار می‌دهد که در میان دستگاه‌ها و اشیای هوشمند متداول است؛ این حمله از ورود این دستگاه‌ها به حالت صرفه‌جویی در مصرف انرژی جلوگیری می‌کنند. این عمل به تخلیه باطری دستگاه منجر می‌شود و این در حالی است که شارژ مجدد باطری دستگاه ممکن است در شرایط نبرد و حمله، بسیار سخت و حتی به لحاظ عملی ناممکن باشد. بنابراین فناوری توان-صفر و صرفه‌جویی در مصرف انرژی ممکن است برای بقای حیات سیستم‌های IoT مهم باشد. این موضوعات بخش عظیمی از برنامه‌های تحقیقاتی اخیر DARPA را در بر می‌گیرد[32]. به طور جزیی‌تر، در سال ۲۰۱۲ میلادی DARPA برنامه سیستم‌های نظامی سایبری با ضریب اطمینان بالا (HACMS)[۳۹] را اعلام نمود، که در آن سعی بر این است آسیب‌پذیری‌های امنیتی IoT برطرف گردد. این موسسه می‌خواهد مطمئن شود که وسایل نقلیه نظامی، تجهیزات پزشکی و بهداشتی و حتی هواپیماهای بدون سرنشین از طرف محیط و مهاجمین بیرونی قابل نفوذ و هَک‌شدن نمی‌باشند. HACMS سعی دارد تا خوراک لازم برای پروتکل‌های امنیتی آتی را فراهم نماید، که در نهایت امنیت و استانداردسازی‌های کافی را برای IoT به ارمغان آورد[41].

۵-۴. احراز اصالت و صدور مجوز

در فضای اینترنت اشیاء، طرفین ارتباط باید قادر به بررسی اصالت/هویت یکدیگر باشند. به بیان ساده‌تر، گیرنده باید قادر باشد تا بتواند اصالت پیام‌های تبادلی را تأیید (و یا رد) نماید. علاوه بر آن، دستگاه‌های IoT باید بتوانند تأیید کنند که آیا موجودیت‌های خاص مجاز به دسترسی به داده‌های مربوطه هستند یا نه؟. در لایه شبکه، تنها دستگاه‌های مجاز باید قادر

[37] *Spoofing attack*
[38] *Sleep-deprivation attack*
[39] *High Assurance Cyber Military Systems program*

باشند تا به شبکه IoT دسترسی یابند. دستگاه‌های غیرمجاز نباید بتوانند تا پیام‌هایشان را به دیگر دستگاه‌های مجاز IoT ارسال نمایند، چرا که ممکن است هدفشان تخلیه و یا پایین آوردن انرژی باتری دستگاه‌های مجاز باشد[1].

برای پاسخ به این نگرانی‌ها، نیاز به استفاده از پروتکل‌های احرازصالت/هویت و مجازشناسی می‌باشد. بدین منظور از اولیه‌های رمزنگاری همچون امضاهای دیجیتال، توابع چکیده‌ساز، پروتکل‌های مدیریت کلید و طرح‌های تسهیم‌راز استفاده می‌شود.

٦. نتیجه‌گیری

کاربرد IoT در حوزه‌های نظامی جزء جدانشدنی و اضطراری توسعه اطلاعاتی بخش نظامی محسوب می‌گردد. IoT توسعه حوزه نظامی را به طور عمده‌ای پیش خواهد برد و به نظر می‌رسد که به زودی شاهد شبکه‌های اینترنت اشیاء نظامی باشیم که در آن نقش انسان کمرنگ‌تر از قبل شده و دستگاه‌ها و جنگ‌افزارهای هوشمند با تکیه بر ارتباطات گسترده و متعاقباً توانایی تصمیم‌گیری و انجام فعالیت‌های تصمیم‌گیرانه، نقش‌آفرینی قابل ملاحظه‌ای داشته باشند. با توجه به دامنه کاربردهای اینترنت اشیاء نظامی و اهمیت خروجی آن‌ها، شاید بتوان گفت که همانند مفهوم اصلی اینترنت اشیاء، حوزه امنیت اصلی‌ترین چالش اینترنت اشیاء نظامی (MIoT) محسوب می‌گردد. وجود یک آسیب‌پذیری در هر یک از بخش‌ها و اجزای اینترنت اشیاء نظامی می‌تواند به بروز خسارت‌های جبران‌ناپذیری منجر گردد. در این مقاله سعی بر این بود تا در وهله اول کلیاتی از مفاهیم و معماری MIoT و همچنین مکانیزم اینترنت اشیاء نظامی با محوریت بررسی مکانیزم ایالات متحده آمریکا مطرح گردد. در ادامه و در کنار ارایه کاربردها، به مبحث تهدیدهای مطرح امنیتی این حوزه پرداخته شد که در این رابطه نیز، آسیب‌پذیری‌ها و ریسک‌های MIoT ایالات متحده آمریکا به طور خاص بررسی گردید. در نهایت ملزومات امنیتی موردنیاز اینترنت اشیاء نظامی معرفی و مورد بررسی قرار گرفت.

همانند مفهوم اصلی اینترنت اشیاء که کاربردهای جدیدی را در حوزه‌های کاربردی مختلف معرفی نموده است، حوزه نظامی نیز با ورود این مفهوم کاربردهای جدیدی را خواهد داشت که معادلات نبردهای آینده را دستخوش تغییرات اساسی خواهد نمود. اما باید توجه داشت که در کنار ارایه کاربردهای جدید، تهدیدات امنیتی نیز برجسته‌تر می‌گردد. با توجه به این که دامنه و عواقب تهدیدات امنیتی مرتبط با حوزه اینترنت اشیاء نظامی بسیار حساس و بعضاً جبران‌ناپذیر می‌باشد نیاز است تا به برقراری ملزومات امنیتی مختلف کاربردهای این حوزه توجه ویژه‌ای گردد.

سپاس‌گزاری

این مقاله توسط بنیاد ملی علمی ایران (INSF) به شماره قرارداد ۹٦/۵۳۹۷۹ حمایت شده است.

۷. منابع

[1]. K.-T. Nguyen, M. Laurent, N. Oualha, "Survey on secure communication protocols for the Internet of Things", Ad-hoc Networks, pp.1-15, 2015.

[2]. L. Atzori, A. Iera, G. Morabito, "The Internet of Things: A survey," Computer Networks, 2010, doi:10.1016/j.comnet.2010.05.010, 2010.

[3]. F. A. Ian and M. J. Josep, "The Internet of NANO-THINGS," IEEE Wireless Communications, pp. 58-64, 2010.

[4]. M. Micheal and M. Darianian, "Architectural solutions for mobile RFID services for the internet of things," IEEE Congress on Services-Part 1, pp. 71-74, 2008.

[5]. D. Wobschall D, "Networked Sensor Monitoring Using the Universal IEEE 1451 Standard," IEEE Instrumentation & Measurement Magazine, vol. 11, no. 2, pp. 18-22, 2008.

[6]. Dennis, Matthias, Dominik, H. Picker, "Key Problems and Instantiations of the Internet of Things (IoT)," Seminar on Internetworking, pp. 1-7, 2010.

[7]. K. Wrona, "Securing the Internet of Things A Military Perspective," IEEE 2nd World Forum on Internet of Things (WF-IoT), 2015, pp.

[8]. D.-E. Zheng and W.-A. Carter, "Leveraging the Internet of Things for a More Effective and Effective Military", A Report of the CSIS Strategic Technologies Program, SEPTEMBER 2015.

[9]. Wayne P. Hughes, "Naval Operations: A Close Look at the Operational Level of War at Sea," Naval War College Review 65, no. 3, 2012, pp. 23–47.

[10]. "Aegis Combat System," Navysite.de, accessed June 29, 2015, http://navysite.de/weapons/aegis.htm.

[11]. Naval Air Systems Command, "Tomahawk Data Sheet," accessed June 29, 2015, http://www.navair.navy.mil/index.cfm?fuseaction=home.display&key.

[12]. Defense Logistics Agency, "IDE/GTN Convergence," accessed June 29, 2015, http://www.dla.mil/informationoperations/pages/IGC.aspx.

[13]. U.S. Air Force: Programmers Earn Award for Innovative Tablet App. Available online: http://www.af.mil/ News/ArticleDisplay/tabid/223/Article/518660/programmers-earn-award-for-innovative-tablet-app. aspx (accessed on 12 September 2016).

[14]. P. Fraga-Lamas, T.-M. Fernández-Caramés, M. Suárez-Albela, L. Castedo and M. González-López, "A Review on Internet of Things for Defense and Public Safety," Sensors, doi:10.3390/s16101644, 2016.

[15]. Tunnell, H.D. "The U.S. Army and network-centric warfare a thematic analysis of the literature." In Proceedings of the Military Communications Conference, Tampa, FL, USA, pp. 889–894, 2015.

[16]. Tunnell, H.D. "Network-centric warfare and the data-information-knowledge-wisdom hierarchy". Mil. Rev, 92, pp. 43–50, 2014.

[17]. L. Yushi, J. Fei, Y. Hui. "Network Study on application modes of military Internet of Things (MIOT)". IEEE International Conference on Computer Science and Automation Engineering (CSAE) 3 (2012): pp. 630-634, 2012.

[18]. G. Singh. "Internet of Things Advancement in Defence". International Journal of Scientific Research Engineering & Technology (IJSRET), pp. 28-36, 2015.

[19]. NATO Parliamentary Assembly, Science and Technology Commitee, "The Internet of Things: Promises and Perils of a Disruptive Technology", www.nato-pa.int, 2017.

[20]. I. Roufa, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Grutser, W. Trappe, and I. Seskar, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in Proc. of the 19th USENIX conference on Security, 2010.

[21]. S. Checkoway, D. Mccoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," in SEC'11 Proceedings of the 20th USENIX conference on Security, 2011.

[22]. C. McCarthy, K. Harnett, and A. Carter, "Characterization of Potential Security Threats in Modern Automobiles: A Composite Modeling Approach," National Highway Traffic Safety Administration, Washington, Tech. Rep. October, 2014.

[23]. C. Miller and C. Valasek, "A Survey of Remote Automotive Attack Surfaces," Tech. Rep., 2014.

[24]. J. A. Marty, "Vulnerability Analysis of the MAVLink Protocol," Ph.D. dissertation, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, 2014.

[25]. A. Greenberg, "Hackers can disable a Sniper Rifle - or change its target," Wired, Jul. 2015.

[26]. A. Sorniotti, L. Gomez, and K. Wrona, "Secure and trusted in-network data processing in wireless sensor networks: a survey," Journal of Information Assurance and Security, vol. 2, no. 4, 2007. [27]. M. Rieback, B. Crispo, and A. Tanenbaum, "Is your cat infected with a computer virus?" in Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications (PERCOM),

[28]. D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, "Security and Privacy for Implantable Medical Devices," IEEE Pervasive Computing, vol. 7, no. 1, Jan. 2008.

[29]. D. Halperin, T. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses," in Symposium on Security and Privacy, 2008.

[30]. W. H. Maisel and T. Kohno, "Improving the security and privacy of implantable medical devices." The New England journal of medicine, vol. 362, no. 13, Apr. 2010.

[31]. M. B. Barcena and C. Wueest, "Insecurity in the Internet of Things," Symantec, Tech. Rep., 2015.

[32]. D. Miessler, "Securing the Internet of Things: Mapping Attack Surface Areas Using the OWASP IoT Top 10," in RSA Conference, 2015.

[33]. Defense Science Board, "Resilient Military Systems and the Advanced Cyber Threat," Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, January2013,http://www.acq.osd.mil /dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

[34]. D. Desail, H. Upadhyay, "Security and Privacy Consideration for Internet of Things in Smart Home Environments", International Journal of Engineering Research and Development, Volume 10, Issue 11, PP.73-83, 2014.

[35]. M. van den Berg, P. de Graaf, P. O. Kwant, and T. Slewe, "Mass surveillance-Part 2: Technology Foresight," European Parliament, Tech. Rep., 2015.

[36]. E. Markey, "Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk," Tech. Rep., 2015.

[37]. eStream ciphers, http://www.ecrypt.eu.org/stream/

[38]. K. Fisher, "HACMS: High Assurance Cyber Military Systems," HILT'12 Proceedings of the ACM SIGAda annual conference on High integrity language technology, 2012.

[39]. L. Pike, P. Hickey, J. Bielman, T. Elliott, E. Hamberg, and T. Dubuisson, "Building a High-Assurance Unpiloted Air Vehicle," in MEMOCODE' 13 Eleventh ACM-IEEE International Conference on Formal Methods and Models for Codesign, 2013.

[32]. NIST FIPS 180-4, "Secure Hash Standards", https://doi.org/10.6028/NIST.FIPS.1804, 2015.

[40]. U.S. Defense Advanced Research Projects Agency, "N-ZERO Envisions' Asleep-yet-Aware' Electronics That Could Revolutionize Remote Wireless Sensors," Communications of the ACM, Apr. 2015.

[41]. HACMS Project (High Assurance Cyber Military Systems program). http://www.defenseone.com/technology.