اهداف دو مقاله:

هدف مقاله اول بهبود امنیت شبکه از طریق شبکه سازی تعریف شده توسط نرم افزار (SDN) است در حالی که هدف مقاله دوم شناسایی عناصر اصلی مربوط به امنیت شبکه و مروری بر تهدیدات بالقوه، آسیب پذیری ها و اقدامات لازم برای مقابله با آنها مرتبط با تکنولوژی طراحی شده به استاندارد LAN بی سیم IEEE 802.11 می باشد.

شبکه سازی تعريف شده از طريق نرم افزار (SDN) تکنولوژی در حال ظهوری است که اخيرا توجه بسیاری را در صنعت و دانشگاه به خود جلب کرده است. با جدا کردن منطق کنترلی از پیاده سازی بسته و اختصاصی دستگاه های شبکه رایج، محققان و نوآوران قادر به طراحی توابع / پروتکل های شبکه نوین به روشی بسیار انعطاف پذیرتر، قدرتمند تر و ساده تر شدند. اعتقاد نویسنده بر این است SDN فرصت های تحقیق جدیدی را برای امنیت فراهم می کند و می تواند تا حد زیادی به تحقیقات امنیتی شبکه تاثیر گذار باشد. اما به خاطر اینکه جامعه امنیت شبکه تا کنون چندان به بررسی و آزمایش این روش نپرداخته است، متد SDN به اندازه کافی توسعه پیدا نکرده است.

به منظور حفاظت از اطلاعات اختصاصی، مالکیت معنوی، مالی و یا هر گونه اطلاعات خصوصی دیگر موجود در شبکه یک سیستم، محرمانه بودن، یکپارچگی و دسترسی، سه اقدام کنترل امنیتی اصلی هستند که باید با استاندارد IEEE 802.11 اجرا شود. استفاده از روش CIA Triad برای اطمینان از آگاهی در برابر تهدیدات و مدیریت ریسک ها ضروری است. به منظور جایگزینی TCP / IP و برآورده کردن این پیش شرط، مدل مرجع شبکه باز سیستم (OSI) به عنوان مدل مرجع شبکه ای برای تحلیل داده ها بین سخت افزار و نرم افزار در یک سیستم هفت لایه معرفی شد. در این مقاله بیان شده با پیشرفت تکنولوژی مردم تقاضا سیستم های قابل حمل و بی سیم بیشتری دارند. در حالی که استفاده از این سیستم ها به دلیل محدوده گسترده تری که دارند، امکان سو استفاده و افشا شدن اطلاعات را به هکرها و مهاجمان می دهد. از این رو به منظور حفاظت از اطلاعات اختصاصی، مالکیت معنوی، مالی و یا هر گونه اطلاعات خصوصی دیگر موجود در شبکه یک سیستم، محرمانه بودن، یکپارچگی و دسترسی، سه اقدام کنترل امنیتی اصلی هستند که باید با استاندارد IEEE 802.11 اجرا شود.

**ویژگی های SDN**

1- کنترل جریان دینامیک

کنترل جریان شبکه به صورت دینامیکی امکانات بسیاری در توابع امنیتی شبکه فراهم می کند.

2- قابلیت مشاهده شبکه­ای با کنترل جریان مرکزی

نظارت شبکه فعالیت مهم و ضروری در امنیت شبکه است. به طور رایج، برای نظارت بر کلیه زیر شبکه ها (از جمله ترافیک کلی و ترافیک داخلی)، نیاز به نصب یا راه اندازی سنسورهای نظارت و جمع آوری اطلاعات شبکه در هر دستگاه شبکه یا لینک داریم، که به نظر می رسد درک اینها در شبکه های بزرگ در دنیای واقعی آسان نیست.

3- برنامه پذیر بودن شبکه

توابع امنیت شبکه عموما با استقرار برخی از واسطه های سخت افزاری یا نصب برخی از برنامه های نرم افزاری ساخته می شوند.

4- صفحه داده ساده شده

در مقایسه با دستگاه های نسل قبلی، سخت افزار (مثلا صفحه نمایش داده) برای SDN میتواند به راحتی تغییر کند، زیرا از مدول های سخت افزاری نسبتا ساده­ای تشکیل شده و مدول های صفحه کنترل پیچیده را به حرکت وا می دارد.

5- اظهار نهایی

با وجود این که ما هر یک از ویژگی ها را به صورت جداگانه بحث می کنیم، اما اذعان داریم که در واقع سخت است که آنها را برای برنامه های امنیتی خاص جدا سازیم.

**مدل هفت لایه OSI**

این مدل بر اساس پروتکلی مشخص و استانداردهای منحصر به فرد خاص خودشان طراحی شده اند. در حین انجام وظایف بسیار متمایز، در مدل OSI هفت لایه به گونه ای قرار گرفته اند که هر لایه از لایه بالایی خود پشتیبانی کند و به لایه پایینی خود سرویس دهد. لایه ها 1-4 به لایه های پایین تر از ستون های پروتکل تعلق دارند و لایه های رسانه ای مسئول انتقال و انتقال داده ها هستند. لایه های 5-7 به عنوان لایه های میزبان بالایی در نظر گرفته می شوند و با داده های سطح برنامه ارتباط دارند. این لایه ها عبارتند از: که در مدل OSI هفت لایه به گونه ای قرار گرفته اند که هر لایه از لایه بالایی خود پشتیبانی کند و به لایه پایینی خود سرویس دهد.

*1- لایه فیزیکی*

لایه فیزیکی (لایه 1) در انتها قرار دارد و به توپولوژی فیزیکی و اجزای سخت افزاری مکانیکی مرتبط با شبکه که برای انتقال و دریافت ارتباطات مرتبط هستند، اطلاق می شود. الزامات سیم، خط و کابل مخصوص مانند اترنت، فیبر نوری، RS232، T1، 802.x، RJ45 و سایرین، لایه فیزیکی را تشکیل می دهند. داده ها در این لایه به صورت دوتایی مشخص می شوند و به شکل بیت به لایه 2 ارسال می گردند.

*2- لايه لینک داده*

لايه لینک داده (لايه 2) از لایه های کنترل لینک لوجیکال (LLC) و کنترل دستیابی به مدیا (MAC) تشکيل شده است که با استفاده از IEEE براي شناسايي و جدا کردن مسئوليت هاي فردي در اين سطح اجرا می شوند. اهمیت این لایه، قابلیت پیوند سیستم ارائه شده توسط LLC بین لایه فیزیکی و لایه های بالایی است تا بتوانند به طور موثر با یکدیگر ارتباط برقرار کنند. زیرلایه فرعی MAC مسئول ارائه سیستم با یک شناسه ی منحصر به فرد (آدرس MAC) است که اجازه تشخیص شبکه بین کامپیوترهای مرتبط در سراسر شبکه را می دهد.

*3- لایه شبکه*

لایه شبکه (لایه 3) مسیریابی بسته های مستقل اطلاعات از منبع به مقصد را با استفاده از آدرس های IP مربوطه مدیریت می کند

*4- لایه حمل و نقل*

لایه حمل و نقل (لایه 4) بر کیفیت خدمات ارائه شده و همچنین ارائه حمل و نقل میزبان به میزبان تمرکز می کند. علاوه بر این، این بسته های اطلاعات به عنوان «بخش ها» شناخته می شوند. پروتکل های مرتبط با این لایه مبتنی بر اتصال هستند مانند TCP و ACK ، به استثنای UDP که در آن ACK لازم نیست.

*5- لایه جلسه ای*

لایه جلسه ای (لایه 5) ارتباط بین برنامه های شبکه را مدیریت و کنترل می کند. پروتکل های این لایه عبارتند از جلسات NFS، SQL و ISO.

*6- لایه ارائه*

لایه ارائه (لایه 6) یا «لایه Syntax» همانطور که معمولا ذکر می شود رمزگذاری را ارائه می دهد، داده های اصلاح شده را از لایه های پایین تر نشان می دهد تا این لایه در لایه برنامه قابل نمایش باشد. طرح های کد گذاری مانند HTML و ASCII و همچنین پسوند های فایل مانند .PNG، .JPG و .gif در این سطح آماده می شوند.

*7- لایه برنامه*

لایه برنامه (7) که در بالا قرار دارد، به تعاملات و پردازش کاربر پایان می دهد. احراز هویت کاربر در این سطح اتفاق می افتد و همچون هر پردازش دیگری، این کار به رابط کاربر با برنامه های کامپیوتری مربوط می شود. این فعالیت ها شامل ایجاد فایل ها، ایمیل، انتقال اسناد و یا فایل ها، حتی جستجو در اینترنت می باشد.

در ادامه مقاله 1، اینکه چگونه SDN می تواند موجب افزایش امنیت اطلاعات شود، پرداخته شد. به این منظور سه ویژگی پیشگیری، تشخیص و پاسخ بررسی شدند. این سه ویژگی، خصوصیات لازم برای بهبود امنیت اطلاعات شبکه هستند. بر اساس تجزیه و تحلیل عمیق ویژگی های SDN و برنامه های کاربردی مورد بحث در این مقاله، نویسنده ادعا کرده است که SDN می تواند به وضوح عملکرد توابع امنیت شبکه را بهبود بخشد.

1- پیشگیری

پیشگیری فرایند متوقف کردن مهاجمان از تماس با اهداف به منظور حفاظت است، و معمولا با تنظیم برخی سیاست های امنیتی تعیین می کنند که چه کسی (یا چه چیزی) می تواند (یا نمی تواند) به آنها دسترسی داشته باشد. این فرآیند نیاز به برنامه ریزی دقیق و تحقیق برای به حداقل رساندن اشتباهات دارد، زیرا ممکن است سیاست های امنیتی کاربران را مسدود کنند و یا حالات مخرب را بپذیرد. بنابراین، تعیین سیاست های امنیتی مهم ترین کار است، سیاست های امنیتی معمولا پس از تصمیم گیری تغییر نمی کنند. با این حال، بسیاری از معماری های موجود در شبکه کاملا پیچیده و متغیر هستند، و در نتیجه کنترل دسترسی بر اساس سیاست های استاتیک ممکن است برای حفاظت و مدیریت یک شبکه بزرگ و دینامیک کافی نباشد

2- تشخیص

تشخیص یک فرایند امنیتی مهم به منظور کشف شبکه های نفوذی است و معمولا از دو روش تشخیص استفاده می شود: (i) تشخیص سوء استفاده و (ii) تشخیص غیر متعارف. تشخیص سوء استفاده، حملات مبتنی بر الگوهای شناخته شده را تشخیص می دهد و تشخیص غیر متعارف با شناسایی الگوهای مخرب در ترافیک شبکه که با رفتارهای معمول طبیعی مطابقت ندارند، حملات را پیدا می کند.

3- پاسخ

پاسخ به حملات (به عبارتی دیگر، مقابله با حمله) بخش مهمی در چارچوب امنیت دفاعی قوی است. با این حال، با توجه به مطالعات انجام شده سخت ترین بخش امنیت شبکه این قسمت می باشد. به طور رایج، برای پاسخ دادن به حملات، ممکن است میدل باکس هایی را نصب کنیم تا آزمایشات حمله یا انزوا یا قربانی کردن میزبان را برای محافظت از میزبان های دیگر در شبکه انجام دهند. ویژگی کنترل جریان دینامیک SDN می تواند به طور قابل توجهی برای افزایش این فرایند مورد استفاده قرار گیرد. این آزمایشات می تواند به راحتی توسط این ویژگی کاهش یابد و همچنین انزوای شبکه یا قرنطینه را می توان به راحتی با SDN اجرا کرد.

**نتیجه گیری**

* در این ارائه روش SDN و مدل OSI به منظور برقراری امنیت شبکه با یکدیگر مقایسه شده اند.
* با توجه به مطالب بیان شده، SDN می تواند یکی از تاثیر گذارترین فن آوری ها برای ایجاد نوآوری های مختلف در امنیت شبکه باشد.
* از طرفی با توجه به نیاز روز افزون مردم به تکنولوژی های بیسیم، باید پیشرفت های بیشتری در این زمینه صورت گیرد. با شناخت استانداردها و محدودیت هایی که بر تکنولوژی اعمال می شود، قابلیت های نرم افزاری و سخت افزاری و برنامه های کاربردی مورد نیاز در مدل OSI و IEEE 802.11 فراهم می شود تا از این طریق بتوان اطلاعات با ارزش­ را ایمن و خصوصی نگه داشت.