ارائه روشی برای مقابله با حملات DoS ناشی از فریم‌های EAP دراستاندارد IEEE802.11i

اکرم صالح پور دهکردی[۱]
۱- دانشگاه آزاد اسلامی واحد نجف آباد، Salehpour_dd@yahoo.com

چکیده

مهم‌ترین نکته در راه استفاده از تکنولوژی‌های بی‌سیم، آگاهی از نقاط قوت و ضعف آنها است. این شبکه‌ها برای انتقال امن اطلاعات پروتکل‌های امنیتی مختلفی را تعریف کرده‌اند که IEEE802.11i جدیدترین آنها است. بررسی‌ها نشان داده‌اند که این استاندارد محرمانگی داده، جامعیت و تصدیق دوجانبه خوبی را ارائه کرده و همچنین مدیریت کلید خوبی را نیز دارا می‌باشد. با این وجود از آنجایی که در این استاندارد به دسترس‌پذیری اهمیت چندانی داده نشده و فریم‌های مدیریت و کنترل پشتیبانی نمی‌شوند، همچنان در مقابل حملات مختلف بخصوص حملات DoS آسیب‌پذیر بوده و به نفوذکنندگان اجازه اجرای انواع متفاوتی از این حملات را می‌دهد. نوعی از این تهدیدها، حملات DoS ناشی از فریم‌های *EAP* می‌باشد که ممکن است با حملات مختلف بار ترافیکی زیادی روی شبکه ایجاد کرده و موجب شود سرور یا توابعش برای ساعت‌ها بلوکه شده یا موجب عدم اجازه دسترسی به منابع برای یک کار بر مجاز گردد. در این مقاله قصد داریم حملات ناشی از این فریم‌ها را بررسی کرده و در نهایت روش مناسبی را برای مقابله با این نوع حملات ارائه دهیم.

کلید واژه

امنیت اطلاعات، رمزنگاری، حملات DoS، فریم‌های EAP، IEEE 802.11i.

۱– مقدمه

از آن جا که شبکه‌های بی‌سیم، در دنیای کنونی روز به روز در حال گسترش هستند و با توجه به ماهیت این دسته از شبکه‌ها، که براساس سیگنال‌های رادیویی‌اند، مهم‌ترین نکته در راه استفاده از این تکنولوژی، آگاهی از نقاط قوت و ضعف آنهاست. در ارتباط بی‌سیم یک شبکه محلی بی‌سیم، سه نوع فریم مدیریت، کنترلی و داده وجود دارد. هر پیاده‌سازی از این فریم‌ها به‌صورت مستقیم یا غیرمستقیم ابعاد امنیتی نظیر محرمانگی داده، جامعیت، تصدیق دوجانبه و دسترسی را به خطر می‌اندازد که از آنها به‌عنوان تهدید نام برده می‌شود در شبکه‌های بی‌سیم تهدیدها را می‌توانیم به چند دسته اصلی استراق سمع غیرمنفعل، تزریق پیام، حذف و یا ممانعت پیام، سرقت نشست، MitM[۱] و جلوگیری از سرویس[۲] که از این پس به آنDoS گفته می‌شود، تقسیم کرد. از این‌رو با گسترش شبکه‌های بی‌سیم استانداردهایی برای افزایش امنیت این شبکه‌ها نیز باید طراحی شود. متأسفانه در طراحی این استانداردها تمرکز بر انتقال امن داده‌ها است و توجه کمتری به ایمن‌سازی فریم‌های مدیریت و کنترلی شده است. در حال حاضر برای فریم‌های EAP هیچ‌گونه مکانیزمی جهت تصدیق یا محرمانگی بکار نمی‌برند. بنابراین یک نفوذکننده به‌راحتی می‌تواند حملات مختلفی مثل MitM، تغییر فریم ها، تولید فریم یا DoS را به اجراء بگذارد[1,2,3,4].

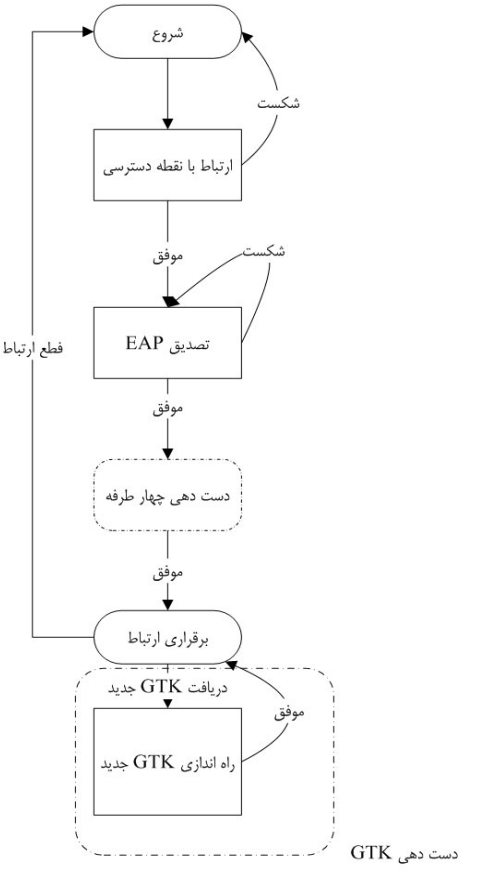
در این مقاله تهدیدات ناشی از فریم‌های EAP و تأثیر آنها روی شبکه‌های بی‌سیم معرفی شده و در ادامه روشی برای مقابله با این

تهدیدات و افزایش امنیت IEEE802.11i ارائه می‌شود که مانع از اجرای حملات معرفی شده و نفوذ حمله‌کننده به شبکه بی‌سیم می‌گردد.

در قسمت بعدی مختصری در مورد IEEE802.11i صحبت می-شود. در قسمت‌های ۳و۴ معرفی فریم‌های EAP و چگونگی اجرای حملات روی آنها مورد بررسی قرار می‌گیرد. در قسمت ۵ ارائه روش مقابله را خواهیم داشت و نهایتاً در قسمت‌های ۶و۷ ارزیابی روش ارائه شده و نتیجه‌گیری بیان خواهند شد.

۲–استاندارد IEEE802.11i

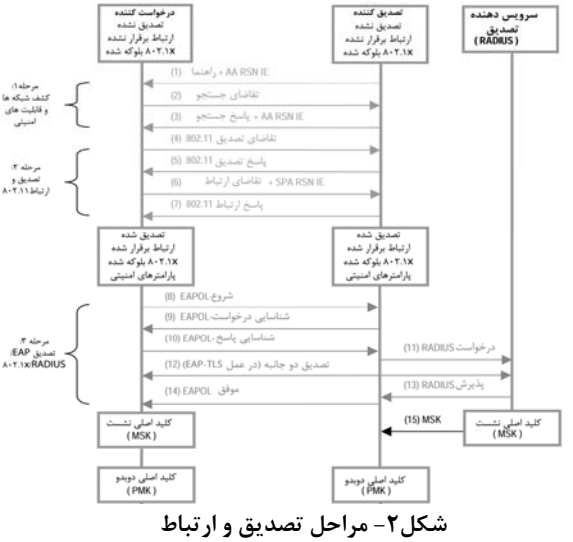
برای برقراری ارتباط در IEEE802.11i روالی باید طی شود موسوم به RSNA که شامل پروتکل‌های تصدیق، 802.1x و مدیریت کلید می‌باشد. در این روال سه موجودیت درگیر می‌باشند که درخواست‌کننده (ایستگاه‌های کاری بی‌سیم)، تصدیق‌کننده (AP)، سرویس‌دهنده تصدیق (در واقع سرویس‌دهنده RADIUS) نامیده می‌شوند. عموماً، دست‌تکانی کامل تشکیل RSNA را می‌توان به شش بخش زیر تقسیم کرد(شکل (۱)):



شکل۱- مراحل برقراری RSNA

مرحله ۱- کشف شبکه‌ها و قابلیت‌های امنیتی
مرحله ۲ – تصدیق 802.11 و ارتباط.
مرحله ۳ – تصدیق EAP/802.1x/RADIUS
مرحله ۴ – دست‌دهی چهار طرفه
مرحله ۵ – دست‌دهی کلید گروهی
مرحله ۶- ارتباط داده‌ای ایمن

در شکل (۲) مرحله تصدیق و ارتباط با نقطه دسترسی در طی تشکیل RSNA نشان داده شده است. در این دست تکانی، درخواست‌کننده و تصدیق‌کننده یکدیگر را تأیید کرده و یک نشست امن را برای انتقال داده برقرار می‌سازند [3,4,5].



شکل۲- مراحل تصدیق و ارتباط

۳– فریم‌های EAP

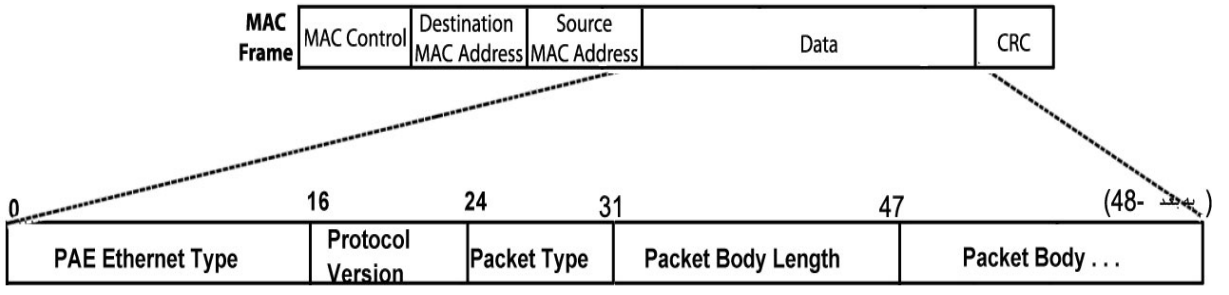
EAP یک پروتکل تصدیق توسعه یافته‌ای است که تحت RADIUS و 802.1x کار می‌کند. فرمت MPDU ی EAP در شکل (۳) [5,6] نشان داده شده است.

فریم EAP شامل قسمت‌های زیراست:

الف) PAE Ethernet Type: فیلدی به طول ۲ بایت است و مقادیر بین ۸۸ تا ۸E را دریافت می‌کند.

ب) Protocol Version: فیلدی به طول یک بایت است و حاوی یک عدد باینری بدون علامت است.

ج) Packet Type: این فیلد به طول یک بایت بوده و با یک عدد باینری بدون علامت نشان داده می‌شود. این فیلد برای تعیین نوع بسته‌های انتقالی بکار می‌رود که انواع آن در جدول (۱) نشان داده شده‌اند.



شکل۳- ساختار و محل قرار گیری فریم های EAP

جدول۱- مقادیر فیلد Packet Type

نوع بسته انتقالی	مقدار	Packet Type
بسته EAP	0000 0000	EAP-Packet
فریم EAPOL-Start	0000 0001	EAPOL-Start
فریم EAPOL-Logoff	0000 0010	EAPOL-Logoff
فریم EAPOL-Key	0000 0011	EAPOL-Key
فریم انتقال دهنده EAPOL-Encapsulated-ASF-Alert	0000 0100	EAPOL-Encapsulated-ASF-Alert

د) Packet Body Length: این فیلد به طول دو بایت و شامل یک عدد باینری بدون علامت است که طول فیلد Packet Body را تعیین می‌نماید. این فیلد می‌تواند طول Packet Body راصفر نیز نشان دهد.

ه)Packet Body: این فیلد تنها هنگامی موجود است که Packet Type یکی از مقادیر EAP-Packet، EAPOL-Key و EAPOL-Encapsulated-ASF-Alert را داشته باشد.

درجدول (۲) می‌توان محتوی Packet Body را مشاهده نمود.

جدول ۲- تعریف Packet Body بسته‌های از نوع EAP-Packet

	توضیح	
Code	۱	Request
	۲	Response
	۳	Success
	۴	Failure
Identifier	برای تطبیق Response با Request بکار می‌رود	
Length	نشان دهنده طول بسته EAP شامل فیلدهای Code,Identifier,Length,Data	
Data	این طول توسط فیلد Code تعیین می گردد.	

باید توجه داشته باشیم حداکثر طولی که یک فریم EAPOL می‌تواند داشته باشد مطابق حداکثر طولی است که توسط MAC تعریف شده است[5,6].

۴– حملات ناشی از فریم‌های EAP

این فریم ها می‌توانند تهدید خطرناکی برای شبکه‌های بی‌سیم باشند. فریم‌های EAP نوعی از فریم‌های کنترلی می‌باشند که شامل انواع تهدیدهای[1,3,4,6]:

۴–۱– بوکشی آدرس‌ها

جعل پیام شروع
جعل پیام شکست
جعل پیام قطع ارتباط
فسخ همکاری MAC

۴–۲– حملات DoS

در این حمله نفوذکننده تعداد زیادی از پیام‌های مختلف EAP را روی شبکه بی‌سیم محلی ارسال می‌کند. حمله‌کننده با بوکش آدرس‌های نقطه دسترسی و سرویس گیرنده‌ها را داشته و می‌تواند با جعل پیام‌های مختلف شروع EAP، شکستEAP، قطع ارتباط و فسخ همکاری را برای هر دو طرف ارتباطی ارسال نماید. اثرات این حمله وقتی نمایان‌تر می‌شود که پیام‌های جعلی از طرف سرویس گیرنده‌های مختلف به نقطه دسترسی ارسال شوند و نقطه دسترسی ملزم به قطع سرویس‌دهی به تمام سرویس-گیرنده‌ها شود که شبکه برای مدتی از کار می‌افتد. زمانی‌که این حملات روی سرویس گیرنده‌ها انجام شود ترافیک شبکه بالاتر رفته، عملکرد آن پایین آمده و سرویس گیرنده‌های مجاز قادر به استفاده از نقطه دسترسی و ارتباط با سایر سیستم‌ها نمی‌باشند. مثلاً پس از دریافت پیام شکست EAP، سرویس‌گیرنده مجدداً تلاش خودش را برای تصدیق

ازسرمی‌گیرد و بنا به نتیجه دریافتی به مرحله بعد ارتباط RSNA می‌رود[1,3,4].

MitM –۳–۴

در این تهدید نفوذکننده خودش را بین سرویس گیرنده و نقطه دسترسی برای بدست آوردن پیام‌های EAP قرار می‌دهد. کاری که توسط نفوذکننده انجام می‌شود قرارگیری بین نقطه دسترسی و سرویس گیرنده، بدست آوردن پیام‌های EAP، تغییر آنها و ارسال آنها به گیرنده. در تمام این مدت نفوذکننده از نظر سرویس گیرنده، نقطه دسترسی تأیید شده و از نظر نقطه دسترسی، سرویس گیرنده تأیید شده می‌باشد. هم نقطه دسترسی و هم سرویس گیرنده در تشخیص نفوذکننده شکست خورده و به ردوبدل اطلاعات ادامه می‌دهند[3,4,6].

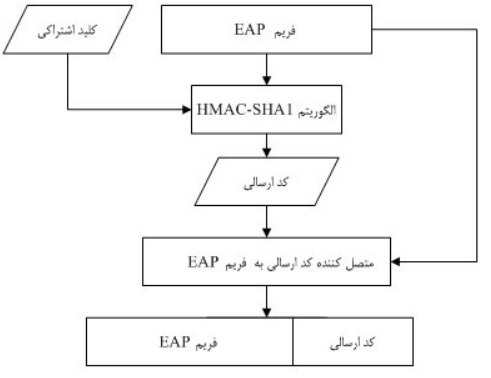
۴–۴– سرقت نشست

سرقت نشست ترکیبی از بوکشی آدرس‌ها و حملات DoS می‌باشد. عموما نفوذکننده با ارسال پیام‌های جعلی قطع ارتباط، پیام شسکت و فسخ همکاری MAC با استفاده از آدرس MAC بوکشی شده نقطه دسترسی موجب اتمام ارتباط سرویس گیرنده با نقطه دسترسی شده و نهایتاً قطع ارتباطش با شبکه بی‌سیم محلی می‌گردد. در این زمان نفوذکننده با جعل آدرس MAC سرویس گیرنده پیام شروع ارتباط را به نقطه دسترسی ارسال کرده و درنتیجه نشست را بدست می‌گیرد[1,3,4].

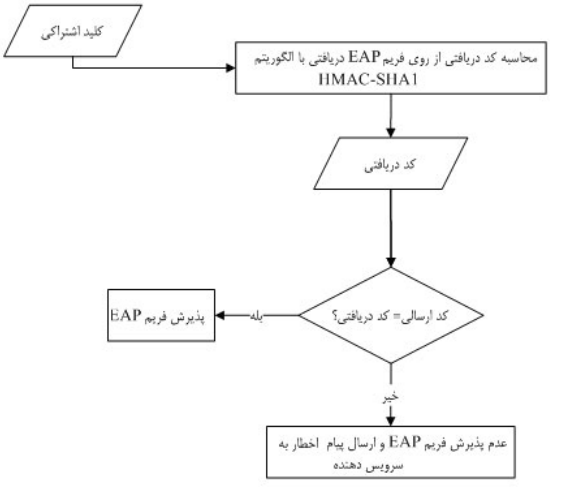
۵– طرح بهبود IEEE802.11i

در هر مرحله‌ای از برقراری روال IEEE802.11i که بتوانیم امنیت را افزایش دهیم، در واقع توانستیم امنیت را در کل روال افزایش دهیم. فریم‌های مدیریت و EAP برای بهبود امنیت باید تأیید شده و برخی از فریم‌های کنترلی در صورت لزوم نیز می‌توانند تصدیق شوند. تصدیق این فریم‌ها تا آنجایی که امکان‌پذیر است باید سریعاً انجام شود. همین که فرآیند تصدیق با موفقیت کامل شد، رمزهای مشترک بدست آمده می‌توانند برای تصدیق فریم‌های مدیریت و EAP بعدی استفاده شوند. از طریق این روش آسیب-پذیری اغلب فریم‌ها به غیر از فریم‌های راهنما و درخواست/ پاسخ جستجو که بدلیل عدم وجود رمزهای مشترک نمی‌توانند تصدیق شوند، رفع می‌گردد.

از آنجایی که بیشترین استفاده از فریم‌هایEAP در مرحله ۳ می‌باشند می‌توانیم جلوی نفوذ در مراحل بعدی را نیز به خوبی بگیریم. برای این کار باید طرحی داشته باشیم که بتواند جلوی جعل آدرس‌های MAC را گرفته، از ایجاد ترافیک کاذب در شبکه ناشی از این فریم‌ها جلوگیری نماید و در عین حال مانع از تغییر پیام‌ها یا تزریق پیام‌های مختلف توسط این نوع فریم‌ها شود. برای این منظور جلوی جعل آدرس‌های MAC را با مکانیزم تصدیق و بررسی آنها در نقطه دسترسی انجام می‌دهیم (سرند آدرس MAC). برای جلوگیری از ایجاد ترافیک کاذب از یک الگوی پخش که در واقع عمل فیلترینگ فریم‌های EAP را انجام می‌دهد، استفاده می‌کنیم و در نهایت برای جلوگیر از جعل آدرس‌ها از رمزنگاری آنها بهره می‌بریم. در شکل (۳) و (۴) می‌توانیم طرح رمزنگاری و رمزگشایی فریم‌ها در قسمت سرویس‌گیرنده و تصدیق‌کننده را مشاهده نماییم.



شکل۴- الگوریتم مدل پیشنهادی در سمت فرستنده



شکل۵- الگوریتم مدل پیشنهادی در سمت گیرنده

در این طرح از الگوریتمی که برای حفاظت فریم‌های داده در IEEE802.11i بکار می‌رود برای تصدیق فریم‌های مدیریت و EAP استفاده می‌کنیم. این الگوریتم به نام HMAC-SHA1 می‌باشد که از یک کلید عمومی برای تصدیق و رمزنگاری فریم‌های مدیریت و EAP استفاده می‌نماید.

از طرفی در سمت‌گیرنده پس از دریافت فریم، مجدداً کد حاصل از الگوریتم را روی آن محاسبه کرده و پس از مقایسه آن با کد ارسالی متوجه تغییر فریم‌ها می‌شوند. اگر دو کد محاسبه شد در فریم ارسالی و دریافتی یکسان نباشند فریم یا پیام ارسالی پذیرفته نمی‌شود ولی اگر یکسان باشند، فرض می‌شود جعل فریمی صورت نگرفته است.

اگر بتوانیم جلوی نفوذ را بگیریم که مشکلی وجود ندارد ولی اگر با تمامی تمهیدات نفوذکننده بتواند حمله کند، احتمال جعل فریم را با استفاده از الگوریتم HMAC-SHA1 کاهش می‌دهیم.

۵–۱– الگوریتم فیلترینگ ترافیک

در این روش هر سیستم فرستنده و گیرنده‌ای باید بتواند تعداد بسته‌های EAP را که در یک فاصله زمانی می‌رسد شمرده و بتواند افزایش غیرعادی نرخ ورودی را تشخیص دهد.

اگر EAP(t) را تعداد پیام‌های EAP وارد شده در بازه زمانی t و A_EAP(t) میانگین پیام‌های EAP وارد شده تا کنون در نظر بگیریم. در آن صورت اختلاف میانگین‌ها و میانگین تاریخی (میانگینی که نرخ انتقال پیام‌ها را نسبت به بازه‌های زمانی گذشته محاسبه می‌نماید) آن به‌صورت زیر محاسبه می‌شود.

$$DFA(t)=EAP(t) - A\_EAP(t) \quad (۱)$$

$$A\_EAP(t)=(1-\alpha).A\_EAP(t-1)+\alpha.EAP(t) \quad (۲)$$

که در این روابط α نشان دهنده حساسیت طولانی مدت نسبت به تغییرات جاری است. DFA(t) ورود غیرعادی پیام‌های EAP را نشان می‌دهد. اگر حمله DoSای با این پیام‌ها در حال شکل‌گیری باشد این انحراف معیار به‌صورت غیرعادی‌ای بسیار بزرگتر از نوسانات عادی تعداد پیام‌های EAP است بطوری‌که این انحراف معیار از یک حد آستانه‌ای که برای آن درنظرگرفته شده است تجاوز می‌کند و به‌عنوان یک مورد مشکوک مورد بررسی قرار می‌گیرد. اگر ما این آستانه را عددی مثل β در نظر بگیریم:

$$DFA(t)=EAP(t) - A\_EAP(t) >>\beta \quad (۳)$$

اگر بخواهیم برای فیلترینگ و تشخیص این نوع حمله الگوریتمی بنویسیم می‌توانیم به‌صورت زیر عمل کنیم:

ورودی‌ها :

EAP(t): تعداد پیام‌های ورودی در هر بازه زمانی t

A_EAP(t-1): میانگین تعداد پیام‌های EAP ورودی تا زمان t-1

خروجی:

ارسال پیام اخطار به سرویس‌دهنده

روال:

۱: محاسبه میانگین تاریخی

۲: محاسبه اختلاف میانگین‌های پیام‌های ورودی طبق رابطه (۱)

۳: در صورت برقراری رابطه (۳)

۴: تشخیص حالت مشکوک، افزایش غیرعادی پیام‌های EAP، ارسال پیام اخطار به سرویس‌دهنده

۵: درغیراین‌صورت، ادامه دریافت پیام‌ها و شرو بازه زمانی جدید

۶: بازگشت به مرحله ۱

۷: پایان

۵–۲– الگوریتم فیلترینگ آدرس MAC

عموماً برای فیلترینگ آدرس‌های MAC در نقطه دسترسی به این‌صورت عمل می‌شود که جدولی مثل جدول (۳) قرار می‌گیرد و با دریافت هر پیامی آدرس MAC آن پیام با آدرس‌های موجود در جدول مقایسه شده و درصورت عدم وجود آن آدرس در جدول MAC پیام را نادیده گرفته می‌شود.

جدول۳- مثالی از جدول کنترل MAC در نقطه دسترسی

محتوی	نام
فعال	سیاست فیلتزینگ آدرس‌های MAC
۳	تعداد آدرس‌های MAC
00:13:10:37:48:3D 00:50:8B:D0:EF:34 00:50:10:D0:EB:E8	لیست آدرس‌های MAC

حمله‌کننده می‌تواند هزاران پیام متفاوت EAP را از طرف درخواست‌کننده‌های جعلی به نقطه دسترسی ارسال کرده و نقطه دسترسی را ملزم به بررسی یکایک آدرس‌ها کند. درنتیجه منابع زیادی برای بررسی این آدرس‌ها مورد استفاده قرار گرفته و نقطه دسترسی نمی‌تواند به پیام‌های EAP کاربران مجاز رسیدگی کند. فیلترینگ آدرس‌های MAC می‌تواند به دورانداختن پیام‌های EAP جعلی کمک کرده و منابع بی‌سیم را برای سرویس‌دهی به کاربران مجاز نگهداری نماید.

مزیت این روش سادگی ومؤثر بودن آن است. شاید تنها عیب آن را بتوان عدم مقیاس‌پذیری و کارایی برای دفاتر خانگی و کوچک برشمرد.

۶– ارزیابی طرح بهبود

۶–۱– احتمال جعل فریم های EAP برای حمله

EAP: فریم اصلی انتقال

K_{EAP}: کلیدی که توسط ارسال‌کننده اصلی فرستاده می‌شود.

EAP_H: فرم جعلی که توسط حمله‌کننده ارسال می‌شود.

K_{EAP_H}: کلیدی که توسط حمله‌کننده ارسال می‌شود.

در صورتی حمله اتفاق می‌افتد که کدها و کلیدهای تولید شده از این کدها مساوی باشند یعنی:

فریم‌های حمله EAP_H∈ ,فریم‌های کاربر مجاز EAP∈

$\therefore K_{EAP}= K_{EAP\_H}$ کننده (۴)

برای انجام چنین کاری حمله‌کننده باید چندین فریم مختلف را فرستاده تا یکی از آنها با فریم EAP ارسالی یکی باشد از این‌رو اگر این فریم‌های ارسالی را در مجموعه‌ای به نام SET_H درنظر بگیریم حداقل N_H فریم در آن وجود دارد. اگر n طول کد تولید شده باشد، در روش جدید تعداد فریم‌هایی که می‌توانند تولید شوند $N=2^n$ خواهد بود. در نتیجه اگر کد تولید شده از فریم EAP کاربر مجاز را CodeEAP نامیده و کد تولید شده از کاربر غیرمجاز را CodeEAP_H بنامیم، می‌توانیم رابطه زیر را داشته باشیم:

$$P_{(CodeEAP= \ CodeEAP\_H)}= \frac{1}{N} \quad \therefore \overline{P}_{(CodeEAP\neq} \quad (۵)$$

$$=1-\frac{1}{N}_{CodeEAP\_H)}$$

از فرمول بالا می‌توانیم نتیجه‌گیری کنیم که احتمال وجود N_H فریم مستقل در SET_H به‌صورت $\overline{p}=\left(1-\frac{1}{N}\right)^{N_H}$ است. پس در نتیجه احتمال اینکه حداقل یکی از N_H فریم موجود در SET_H با $Code_{EAP}$ مساوی باشد به‌صورت زیر است:

$$p=1-\overline{p} \Rightarrow p=1-(1-\frac{1}{N})^{N_H} \quad (۶)$$

پس از ساده‌سازی فرمول بالا احتمال جعل فریم‌ها به‌صورت زیر بدست می‌آید:

$$P_{\text{جعل فریم}}=\frac{N_H}{N} \quad (۷)$$

حال N_H (تعداد فریم‌های لازم برای جعل یک فریم) را با سه احتمال معمول ۲۵٪، ۵۰٪ و ۷۵٪ برای n=32 قبل از استفاده از الگوریتم پیشنهادی (بررسی درستی با استفاده از CRC) و n=160 بیت بعد از الگوریتم پیشنهادی محاسبه‌کرده که نتایج در جدول (۴) قابل مشاهده می‌باشند.

جدول۴- تعداد فریم‌های لازم برای تولید یک فریم جعلی

تعداد N_H / امنیت	با احتمال ٪۲۵	با احتمال ٪۵۰	با احتمال ٪۷۵
بعد از تولید کد سری	3.65×10^{47}	7.3×10^{47}	1.10×10^{48}
قبل از پیاده سازی الگوریتم	1.07×10^{9}	2.15×10^{9}	3.22×10^{9}

۶–۲– سربار محاسبه فریم‌های EAP

طول فریم‌ها را با LEAP و طول فریم‌ها در روش پیشنهادی را با LEAP_P نشان می‌دهیم. سرآیند فریم‌های EAP ۲۲ بایت درنظرگرفته و طول سرآیند در EAP را ۶ بایت در نظر بگیریم، میانگین طول بدنه پیام‌های EAP را محاسبه می‌کنیم، در نتیجه:

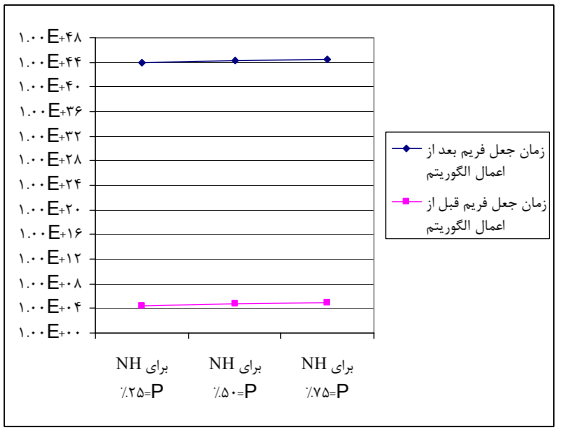
LEAP=22+6+141=169 byte = 1352 bit
LEAP_P=22+6+141+20=186 byte= 1488bit

اگر نرخ انتقال داده‌ها را 54Mbps درنظربگیریم. زمان مورد نیاز برای انتقال یک فریم در هر مورد بدست می‌آید که نتایج در جدول (۶) قابل مشاهده است.

جدول۶- مقایسه نرخ انتقال فریم‌های EAP

ردیف	طول فریم ها	نرخ فریم‌ها	زمان انتقال یک فریم
در حالت جاری	1352 bit	41880	µs۲۳
در مدل پیشنهادی	1488bit	۳۸۰۵۳	µs۲۶

همچنین زمان لازم جهت جعل فریم‌های EAP درنمودار شکل (۶) قابل مشاهده است.



شکل۷- نشان‌دهنده کارایی الگوریتم پیشنهادی

۷– نتیجه‌گیری

در این مقاله پس ازمعرفی استاندارد IEEE802.11i و فریم‌های انتقالی تحت آن پروتکل، ریسک‌های ناشی از عدم حفاظت فریم‌های EAP را مورد بررسی قرار دادیم و روشی را برای افزایش امنیت این پروتگل و رفع تهدیدهای ناشی از عدم حفاظت این فریم‌ها پیشنهاد نمودیم. روش ارائه شده مانع از اجرای حملات ترافیک کاذب، جعل آدرس‌های MAC و جعل فریم‌های EAP می‌شود. در این روش سعی شده است از مکانیزم‌هایی استفاده نماییم که اجرای آنها نیاز به حداقل تغییرات داشته و در عین حال از کارایی مناسبی نیز برخوردار باشدکه محاسبات و نمودارها این امر را به اثبات رسانده‌اند. با طرح پیشنهاد شده می‌توان حملات ناشی از فریم‌های EAP را کاهش داده و زمان مورد نیاز برای جعل یک فریم توسط نفوذکننده را افزایش داد. با اجرای این طرح نفوذ از طریق فریم‌های EAP به شبکه محلی بی‌سیم توسط نفوذکننده با مشکل مواجه می‌شود چرا که نیازمند کار بیشتر و صرف وقت و منابع بیشتری از سوی حمله کننده برای انجام این نوع حملات است.

۸– مراجع

[1] IEEE Computer Society LAN MAN Standards Committee. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications in IEEE Std 802.11. 1999.

[2] Malekzadeh M. et al. **"Security Improvement for Management Frames in IEEE 802.11 Wireless Networks",** International Journal of Computer Science and Network Security, VOL.7 No.6. 2007.

[3] C. He and J. C. Mitchell. **"Security analysis and improvements for IEEE 802.11i.",** In Proceedings of the 12th Annual Network and Distributed System Security Symposium (NDSS'05), 2005.

[4] Buttyán L. and Dóra L. **"WiFi Security – WEP and 802.11i",** Technical Report, CrySyS Lab, Budapest University of Technology and Economics, May 2006.

[5] IEEE Standard**, "Standard:802.11i™ IEEE Standard for Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements"**, Approved 24 June 2004 IEEE-SA Standards Board, ISBN 0-7381-4073-2 SH95248.

[6] IEEE Standard**, "Standard:802.1X™ IEEE Standard for Local and metropolitan area networks Port-Based Network Access Control"** ,Approved 10 March 2005 American National Standards Institute,ISBN 0-7381-4528-8 SH95298.

۹– پی‌نوشت‌ها

1- Man_in _the_Middle

2- Denial of Service