فصلنامه پژوهش‌های حفاظتی ـ امنیتی دانشگاه جامع امام حسین(علیه‌السلام)
سال سوم، شماره‌ی ۱۱ (پاییز ۱۳۹۳): صص ۱۳۳ - ۱۴۴

# ارائه مدل برای ارتقاء امنیت در شبکه وایمکس

**ضرغام رستمی**[۱]
**علی ناصری**[۲]
**محمدهادی بنیادی**[۳]

تاریخ دریافت: ۱۳۹۳/۰۵/۲۵
تاریخ پذیرش: ۱۳۹۳/۰۹/۲۵

## چکیده

*یکی از مهمترین بخش‌های هر شبکه بی‌سیم امنیت و مکانیسم‌هایی است که برقراری امنیت را ممکن می‌سازد. در این مقاله به تجزیه و تحلیل ساختار معماری و پروتکل‌های ارتباطی شامل لایه و زیرلایه‌ها پرداخته شده است. فرآیند امنیتی ورود به شبکه جهت تصدیق هویت کاربر به همراه الگوریتم‌های رمزنگاری مورد بحث قرار گرفته است. از تحلیل نتایج عملی و تئوری فرآیند امنیتی شامل تاثیر طول کلیدها، زمان پردازش، نوع سیستم پردازشی در رمزنگاری ECC[۴] و RSA[۵] ، مدل ECC به‌جای RSA در راستای بالا بردن ضریب امنیت پیشنهاد شد. سپس آسیب‌پذیری پیامهای مدیریتی که در بعضی از ساختارها موجب اخلال در شبکه گردیده شناسایی شده و یک مدل جامع شناسایی حملات و انتخاب آسیب‌پذیری برای هر واحدی از شبکه وایمکس پیشنهاد گردیده است، که در دفاع سایبری برای طراحان شبکه نقاط حائز اهمیتی خواهد بود.*

**کلید واژه‌ها:** *ECC، RSA، حملات[۶]، آسیب‌پذیری[۷]*

---

۱- استادیار دانشکده فاوا-دانشگاه جامع امام حسین(ع)، Zrostami@ihu.ac.ir
۲- استادیار دانشکده فاوا-دانشگاه جامع امام حسین(ع)، anaseri@ihu.ac.ir
۳- دانشجوی کارشناسی‌ارشد مخابرات گرایش سیستم، دانشکده فاوا - دانشگاه جامع امام‌حسین(ع)، hadibonyad۵@Gmail.com

۴. Elliptic Curve Cryptography

۵. Rivest-Shamir-Adleman

۶. Atack

۷. Vulnerability

## ۱- مقدمه

با توجه به گسترش میل عمومی به استفاده از شبکه‌های بی‌سیم باند پهن این مساله در شبکه‌های بی‌سیم امروزی از اعتبار و اهمیت بیشتری برخوردار است. در شبکه‌های وایمکس به دلیل گستردگی و وسعت بالای شبکه از روش‌های خاصی برای برقراری امنیت استفاده می‌شود. شبکه‌های بی‌سیم از دو بخش اصلی شامل ایستگاه پایه (BS[۱]) و ایستگاه مشترک (SS[۲]) تشکیل شده است. کاربران از طریق SS ها می‌توانند به BS متصل شوند و همچنین سایر BSها نیز با یکدیگر در ارتباط هستند (C. Smith. , J. Meyer, ۲۰۰۴). یکی از نقاط نا امن برای شبکه، ارتباطات در فضای آزاد بوده که بایستی مکانیزیم‌های امنیتی برای آن دیده شود، اما امنیت پیاده سازی شده در لایه MAC[۳] دارای نقاط ضعف می‌باشد، یکی از مهمترین پروتکل‌های امنیتی در شبکه وایمکس پروتکل مدیریت کلید محرمانگی(PKM[۴]) بوده که وظیفه آن احراز اصالت، مجاز شناسی، توزیع و همزمان سازی کلیدها می‌باشد وبا توجه به نسخه‌های مختلف PKM مانند (PKMv۱ و PKMv۲) نسخه نهایی آن PKMv۲ که در شبکه وایمکس استفاده می‌گردد (Sanjay P. ,Nicole Collier. ,۲۰۱۰:۱۳۴-۱۳۷).

## ۲- تحلیل ساختار معماری شبکه وایمکس

معماری وایمکس از سه قسمت اصلی تشکیل شده است

۱- ایستگاه سیار که توسط کاربر نهایی دسترسی به شبکه استفاده می‌شود.

۲- شبکه دسترسی به خدمات (ASN[۵]): این شبکه از یک یا چند ایستگاه پایه و دروازه ASN تشکیل شده و دسترسی رادیویی را فراهم می‌کند.

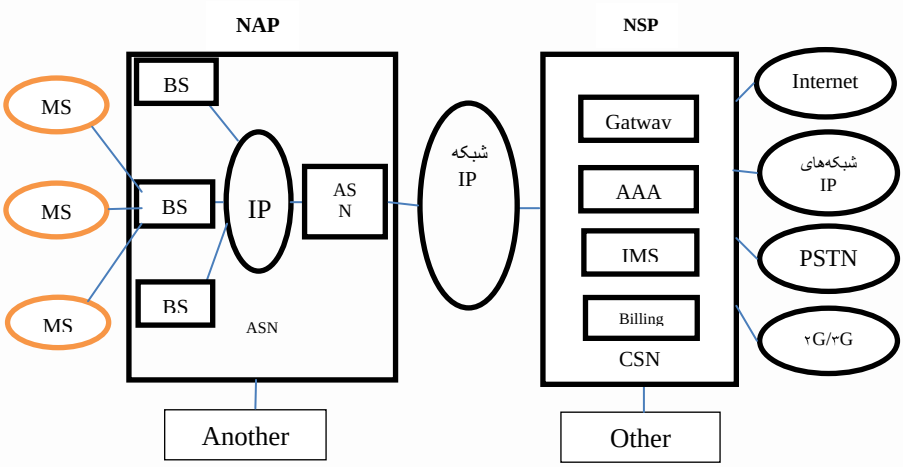
۳- شبکه اتصال به خدمات (CSN[۶]): این شبکه اتصالات IP تمام عملیات مربوط به شبکه‌های IP را فراهم می‌نماید. و همچنین ساختار این معماری به اجزای زیر تقسیم شده است:

- تامین دسترسی به شبکه NAP[۷] که ASN را تحت پوشش داردو روی آن عمل می‌کند.
- تامین خدمات[۸] NSP که خدمات وایمکس و اتصالات IP را برای مشترکین فراهم می‌کند.

---

۱. Base Station
۲. Subscriber Station
۳. Media Access Control
۴. Privacy key Management
۵. Access Service Network
۶. Connectivity Service Network
۷. Network Access Provider
۸. Network Service Provider

- تامین کننده خدمات کاربردی ASPکه می تواند خدمات ارزش افزوده و چند رسانه‌ای از طریق IMS[1] و VPN ارائه کند.
- دروازه ASN-GW به عنوان نقطه تراکم ترافیک لایه MAC در ASN عمل می کند و موارد دیگر مانند کنترل پذیرش، مدیریت منابع، مدیریت منابع رادیویی، مدیریت مکان ASN و فراخوانی، عملیات مشترکAAA[2]، ایجاد مدیریت تونل مربوط به تحرک‌پذیری با BS، کیفیت سرویس، عملیات مسیریابی به سمت CSN.
- شبکه اتصال به خدمات CSN جهت اتصال به شبکه اینترنت، و سایر شبکه‌های عمومی را فراهم می-کند. CSN در تملک NSP بوده و شامل سرورهای AAA برای عملیات تشخیص هویت وسیله و کاربر و خدمات ویژه است. CSN مدیریت سیاست‌های کیفیت خدمات و امنیت را برای هر کاربر به عهده دارد و مدیریت آدرس IP، پشتیبانی از رومینگ بین NSPهای مختلف، مدیریت مکان بین ASNها، اتصال به سایر شبکه‌ها مانند PSTN[3] و ۲G /۳G و... را به عهده دارد شکل(۱).




**شکل۱- ساختارمعماری شبکه وایمکس**

۱. IP Multimedia Subsystem
۲. Authentication Authorization and Accounting protocol
۳. Public Switched Telephone Network

## ۳- تحلیل پروتکل‌های ارتباطی وایمکس

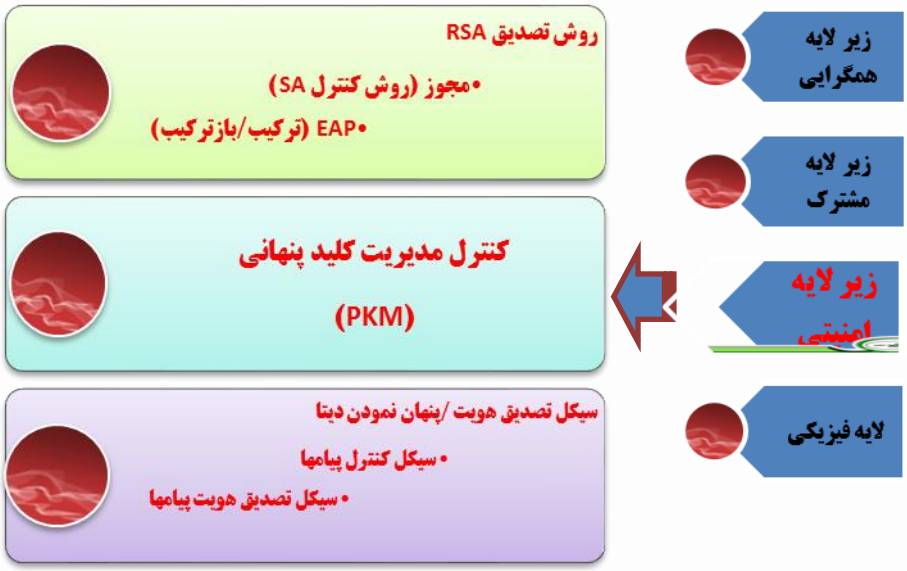
ساختار پروتکل ارتباطی در وایمکس بصورت چهار لایه بوده که شامل زیر لایه همگرایی، زیر لایه مشترک MAC، زیر لایه امنیتی و لایه فیزیکی می‌باشد، لایهMAC که وظیفه کنترل لایه فیزیکی و انتقال داده را بین ایستگاه ثابت و کاربر را به عهده دارد که قسمت اصلی شبکه وایمکس محسوب می‌شود. زیرا تمام توابع مربوط به انتقال داده از طریق لایه فیزیکی بی‌سیم اجرا می شود.

علاوه بر این، این لایه با لایه‌های بالاتر به گونه‌ای ارتباط برقرار می‌کند که انواع ترافیک‌ها را از پروتکل‌های مختلف لایه شبکه می‌پذیرد.

- **زیر لایه همگرایی[۱](CS)**: بین لایه شبکه و زیر لایه میانی واسط است. این زیر لایه بسته‌های IP,ATM[۲] و دیگر پروتکل‌ها را دریافت و طبق قالب تعریف شده برای بسته‌های لایه MAC ساماندهی می‌کند و به گونه‌ای تعریف شده که قابلیت ارتباط با پروتکل‌های متفاوت مانند پروتکل‌های صحبتE۱/T۱ و Ethernet وIP[۳] و ATM را دارد، اما بدلیل فراگیر شدن IP در عمل تنها بسته-های IP را دریافت می‌کند.
- **زیر لایه مشترک[۴](MAC CPS)**: قسمت اصلی لایه MAC محسوب می‌شود و از وظایف آن می‌توان ورود کاربران به شبکه ، اختصاص کانال ، ارائه کلاس‌های سرویس مختلف و مدیریت دست به دست دهی(handover) را نام برد.
- **زیر لایه امنیتی :**این لایه بالای لایه فیزیکی قرار دارد و وظیفه تامین امنیت داده‌های ارسال شده را در کانال بی‌سیم که به راحتی قابل شنود است را به عهده دارد. فرآیند اجرایی در این زیر لایه به طور خلاصه به شرح زیر است:

احراز هویت کاربران، توزیع کلیدهای مورد نیاز برای الگوریتم‌های رمز نگاری، رمزنگاری ترافیک داده انتقالی (Sanjay P. ,Nicole Collier, ۲۰۱۰ :۱۳۴-۱۳۷ ) و (Daniel. ,Mihai-Florentin. ,Adria, ۲۰۱۲:۹۸-۱۰۲) (Rajesh Yadav, S. Srinivasan, ۲۰۱۳:۴۴-۴۸) (Kamlesh Gupta, Sanjay Silakari, ۲۰۱۱: ۳۷۰-۳۷۵) شکل(۲).

۱. Service Specific Convergence Sublayer
۲. Asynchronous Transfer Mode
۳. Internet Protocol
۴. Mac Common Part Sublayer



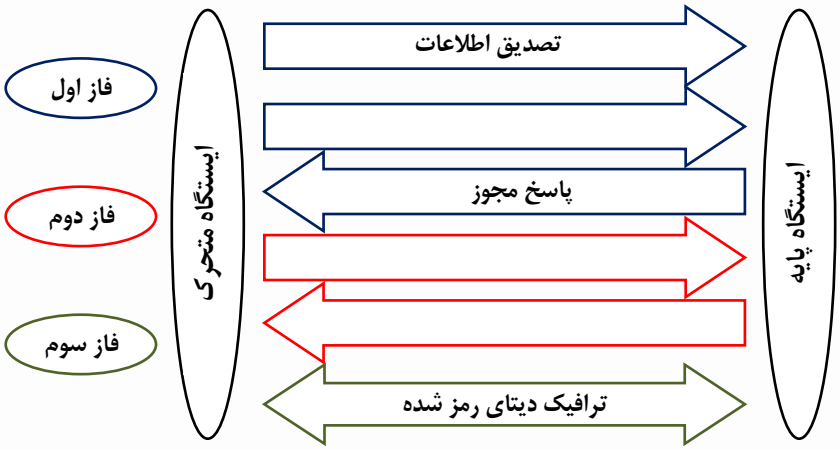

**شکل۲- ساختارامنیتی در شبکه وایمکس**

## ۴-فرآیند امنیتی در ورود به شبکه

یکی از وظایف لایه‌ی زیرین زیر لایه‌ی امنیتی، رمزگذاری ترافیک داده است. روال تصدیق هویت کاربر درشکل(۳) مشاهده می‌شود و پس از تبادل کلید الگوریتم‌های رمزنگاری بین ایستگاه ثابت(BS[۱]) و ایستگاه متحرک (SS[۲]) در نهایت ترافیک داده رمزنگاری می‌گردد.

۱. Base Station

۲. Subscriber Station




**شکل۳- فرآیندامنیتی در شبکه وایمکس**

## فرآیند امنیتی شامل:

الف) احراز هویت کاربران

ب) توزیع کلیدهای مورد نیاز برای الگوریتم‌های رمزنگاری

ج) رمزنگاری ترافیک داده انتقالی

درپروتکل مدیریت محرمانگی ابتدا استاندارد IEEE ۸۰۲,۱۶-۲۰۰۴ از نسخه اول PKMv۱ استفاده می‌شد که فرآیند احراز اصالت در آن صرفاً مبتنی بر الگوریتم رمزنگاری کلید عمومی RSA بوده و یک طرفه انجام می‌گیرد. نسخه‌ی اول این پروتکل با استفاده از پروتکل‌های اصلاح شده بهبود یافته و نسخه دوم پروتکل مدیریت کلید محرمانگی PKMv۲ معرفی گردید که مهمترین مزایای آن نسبت به نسخه اول حمایت از احراز اصالت گسترش یافته EAP[۱] است.

EAP دارای سه نوع یکی EAP-AKA[۲] مبتنی بر SIM، EAP-TLS[۳] مبتنی بر گواهینامه X.۵۰۹ EAP-TTLS[۴] مبتنی بر MS-CHAPV۲ (Sanjay P. ,Nicole Collier, ۲۰۱۰:۱۳۴-۱۳۷) و (Rakesh Kumar. ,Upena D, ۲۰۱۰:۲۵۶-۲۶۳).

۱. Extensible Authentication Protocol
۲. Authentication and Key Agreement
۳. Transport Layer Security
۴. Tunnelled Transport Layer Security

## ۵- ارائه راه کار ارتقاء امنیت

برای راه کار ارتقاء امنیتی دو مورد نتایج عملی محاسبه شده در خصوص عملکرد استفاده از مدل ECC و RSA با استفاده از سیستم‌هایی که دارای پردازشگرهای متفاوت بوده در جدول (۱) و (۲) نشان داده شده.

**جدول۱- مقایسه مدل رمزنگاری ECC وRSA**

| پردازش CPU: Celeron ۷۰۰MHz و RAM ۲۵۶M ، با حجم ۲۲بایت | | | |
|---|---|---|---|
| زمان تولید کلید (میلی ثانیه) | | طول کلید (بیت) | طول کلید (بیت) |
| RSA | ECC | RSA | ECC |
| ۳۷۰ | ۲۹۱ | ۱۰۲۴ | ۱۶۳ |
| ۴۷۳۶ | ۵۳۰ | ۲۰۴۸ | ۲۳۳ |
| ۱۰۲۲۴ | ۷۳۱ | ۴۰۹۶ | ۲۸۳ |
| ۴۱۷۳۳۰ | ۱۵۶۳ | ۸۱۹۲ | ۴۰۹ |
| ۱۶۶۹۳۲۰۰ | ۳۶۹۵ | ۱۵۳۶۰ | ۵۷۱ |

در جدول (۱) سیستمی با مشخصات RAM ۲۵۶M ، CPU :Celeron ۷۰۰MHz بر روی پیام ۲۲ بایتی اطلاعات تست شده است (Abdul-Rahman. ,Nassar۲۰۰۴:۱-۸) و ( ,Nicholas. ,Brandon ۲۰۰۴:۱-۱۱) که نتایج بهینه آنها در نمودارهای گرافیکی (۴) و (۵) نشان داده شده است.

در جدول(۲) در سیستمی با مشخصات CPU: Intel P۲,۴GHz و RAM:۵۱۲Mb برروی پیام ۱۰۰کیلو بایتی تست شده است (Rounak . ,Hemant. ,Sumita, ۲۰۱۳:۷۲۰-۷۲۵) و (Nicholas. ,Brandon, ۲۰۰۴:۱-۱۱).

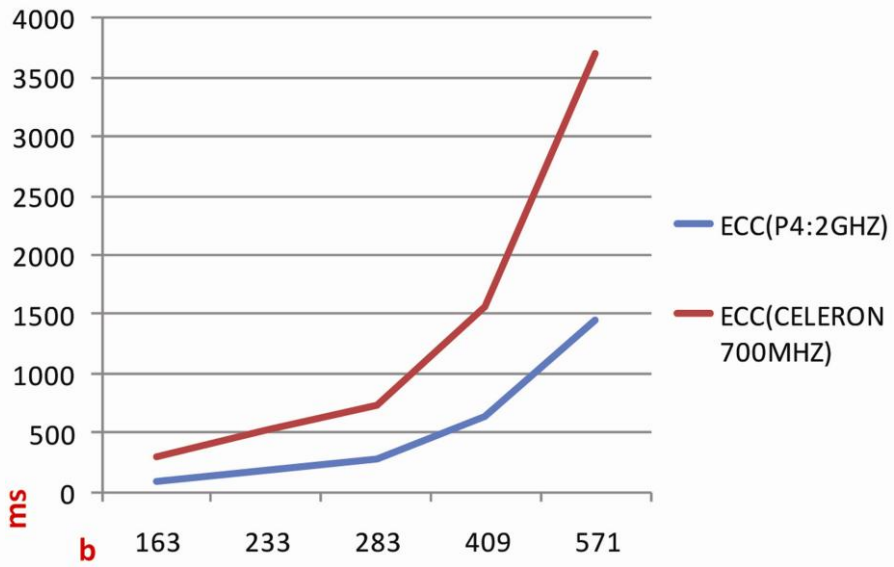
**جدول۲- مقایسه مدل رمزنگاری ECC و RSA در سیستم CPU:intel P۲,۴GHz ، RAM:۵۱۲Mb وحجم پیام ۱۰۰Kb**

| پردازش سیستم intel P۴ :۲GHz ، RAM:۵۱۲Mb وحجم پیام ۱۰۰Kb | | | |
|---|---|---|---|
| زمان تولید کلید (میلی ثانیه) | | طول کلید (بیت) | طول کلید (بیت) |
| ECC | RSA | RSA | ECC |
| ۱۶۰ | ۸۰ | ۱۰۲۴ | ۱۶۳ |
| ۷۴۷۰ | ۱۸۰ | ۲۲۴۰ | ۲۳۳ |
| ۹۸۰۰ | ۲۷۰ | ۳۰۷۲ | ۲۸۳ |
| ۱۳۳۹۰۰ | ۶۴۰ | ۷۶۸۰ | ۴۰۹ |
| ۶۷۹۰۶۰ | ۱۴۴۰ | ۱۵۳۶۰ | ۵۷۱ |

ضمناً جدول (۳) تفاوت نسبی حجم کلیدها را نشان داده شده است.که این مقدار نسبی در مدل RSA بسیار بیشتر از ECC است. در نتیجه زمان بیشتری را به خود برای پردازش اختصاص می‌دهد

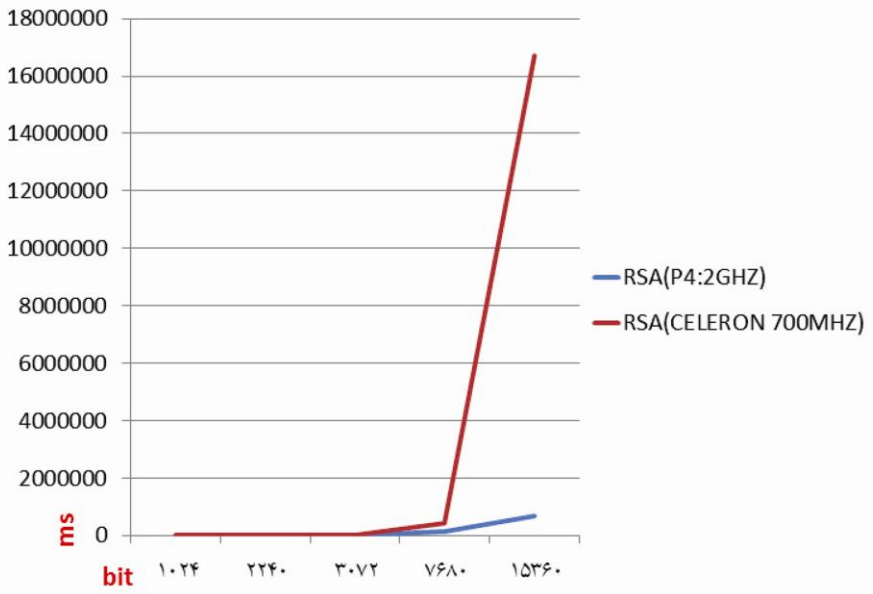
**جدول۳- نسبت بین کلیدها در روشهای ECC و RSA**

| ECC key size(bit) | RSA key size(bit) | Key size ratio(bit) |
|---|---|---|
| ۱۶۳ | ۱۰۲۴ | ۱:۶ |
| ۲۳۳ | ۲۲۴۰ | ۱:۹ |
| ۲۸۳ | ۳۰۷۲ | ۱:۱۱ |
| ۴۰۹ | ۷۶۸۰ | ۱:۱۸ |
| ۵۷۱ | ۱۵۳۶۰ | ۱:۲۶ |




**شکل ۴- مقایسه روش ECC**

در شکل(۴) مقایسه روش ECC با دو سیستم پردازشگر متفاوت CPU:Celeron۷۰۰MHz و CPU:intel P۲,۴GHz را نشان می‌دهد که در پردازشگر قوی‌تر زمان تولید کلید بصورت محسوس کاهش می‌یابد.

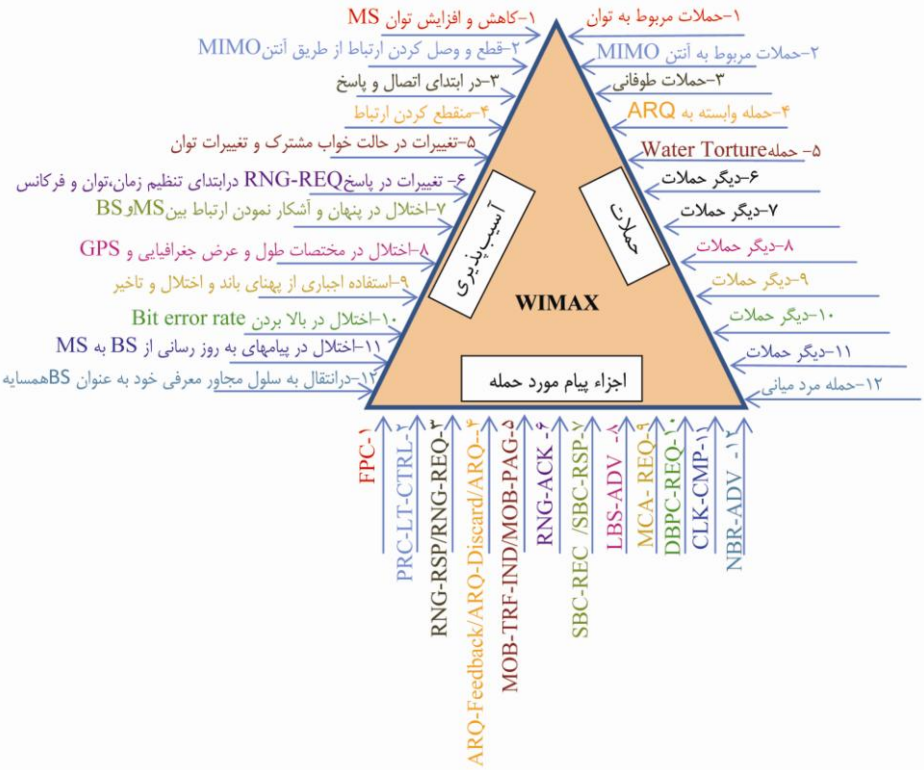



**شکل ۵- مقایسه روش RSA**

شکل(۵) نشان‌می‌دهد که روش RSA در دو سیستم پردازشگر متفاوت CPU:celeron۷۰۰MHz و CPU:intelP۲,۴GHz اندازه گیری شده که با افزایش طول کلید، زمان بصورت نمایی افزایش یافته است. که هرچه سیستم پردازشی قوی تر باشد زمان بصورت محسوس کاهش می-یابد. البته با مقایسه دو روشECC و RSA نتیجه گیری می‌گردد که در روش ECC با افزایش طول کلید زمان بصورت خطی بوده ولی در حالت RSA زمان بصورت نمایی رشد کرده است. البته استفاده از روش خم بیضوی در PDAها، کارت‌های هوشمند و موبایل بدلیل کوچک بودن اندازه کلید و ذخیره فضای حافظه و پهنای باند بدلیل محدود بودن CPU پیشنهاد شده است.

همچنین در حملاتی که بر لایه فیزیکی اعمال شده (DOS[1]) و با ایجاد نویز موجب اختلال در ارتباط می‌گردد و برای مقابله با آن استفاده از روش‌های طیف گسترده[2] دنباله مستقیم[3] و پرش فرکانسی[4] به جای مدولاسیون QAM[5] پیشنهاد می‌گردد.

## ۵-مدل جامع شناسایی حملات، اجزاء پیام‌های مورد حمله و انتخاب آسیب‌پذیری‌های شبکه وایمکس




**شکل ۶- مدل جامع شناسایی حملات و انتخاب آسیب پذیری‌های شبکه وایمکس**

۱. Denial-Of-Service
۲. Spread Spectrum
۳. Direct sequence
۴. Frequency hopping
۵. Quadratture Amplitude Modulation

در شکل(۷) مدل جامع شناسایی حملات، اجزاء پیام مورد حمله و انتخاب آسیب پذیری‌های شبکه وایمکس را نشان می‌دهد. که در آن ورودی ضلع سمت راست نوع حملات، دیگری اجزاء پیام مورد حمله و سومی نوع آسیب پذیری را به ترتیب شماره‌های متناظر توصیف می‌کند.

## ۶- نتیجه‌گیری

پس از معرفی معماری و اجزاء تشکیل دهنده، به تحلیل امنیت روش‌های رمز نگاری ECC و RSA پرداخته شد و نقاط ضعف و قوت هر کدام بررسی و در مقایسه طول کلید مدل‌های RSA ، ECC مشاهده گردید که سه پارامتر مهم اثر گذار در مدل ECC شامل افزایش سرعت، اشغال فضای کم حافظه و سایز کلید کوچکتر، برتری را نسبت به مدل RSA نشان می‌دهد، که موجب توان مصرفی کمتر در تجهیزات شده و همچنین بدلیل محدودیت CPU، تغذیه در گوشی‌های تلفن همراه و حافظه کم کارت‌های هوشمند، می‌توان از مدل ECC برای بالا بردن امنیت در شبکه وایمکس استفاده نمود.

سپس آسیب پذیری پیامهای مدیریتی که در ساختارها بدلیل رمز نشدن این پیام‌ها موجب اخلال در شبکه شده معرفی گردید. علت عدم رمزگذاری پیام‌های مدیریتی حفظ استاندارد در کنترل سریع شبکه است، چرا که رمزگذاری پیام‌ها موجب تاخیر در پردازش پیام‌های مدیریتی و تاخیر در کنترل شبکه می‌شود.

در ادامه مدل پیشنهادی جامع شناسایی حملات و انتخاب آسیب پذیری‌های شبکه وایمکس برای هر واحدی از شبکه ارائه گردید که برای طراحان شبکه مسمر ثمر خواهد بود.

## کتابنامه


Andreas Deininger, Shinsaku Kiyomoto, Jun Kurihara, Toshiaki Tanaka, ۲۰۰۷, Security Vulnerabilities and Solutions in Mobile WiMAX, International Journal of Computer Science and Network Security VOL.۷ No.۱۱, ۷-۱۵.

Abdul-Rahman Mahmood, Nassar Ikram, ۲۰۰۴, ELLIPTIC CURVE BASED SECURE MESSAGING SYSTEM, ۱-۸.

C. Smith and J. Meyer, ۲۰۰۴, ۳G Wireless with WiMAX and Wi-Fi: ۸۰۲,۱۶ and ۸۰۲,۱۱, New York: McGraw-Hill.

Daniel SIMION, Mihai-Florentin URSULEANU, Adrian GRAUR, ۲۰۱۲, An Overview on WiMAX Security Weaknesses/Potential Solutions, International Conference on DEVELOPMENT AND APPLICATION SYSTEMS, Suceava, Romania ۹۸-۱۰۲.

A.K.M. Nazmus Sakib,. Muhammad Ibrahim Khan, Mir Md. Saki Kowsar, ۲۰۱۰, IEEE ۸۰۲,۱۶e Security Vulnerability : Analysis & Solution Global Journal of Computer Science and Technology vol,۱۰،۳۵-۴۲.

Kamlesh Gupta, Sanjay Silakari,۲۰۱۱, ECC over RSA for Asymmetric Encryption: A Review, International Journal of Computer Science Issues, Vol.۸, ۳۷۰-۳۷۵.

Nicholas Jansma, Brandon Arrendondo, ۲۰۰۴, Performance Comparison of Elliptic Curve and RSA Digital Signatures,۱-۱۱.

Rakesh Kumar Jha, Upena D Dalal . ۲۰۱۰. A Journey on WiMAX and its Security Issues. International Journal of Computer Science and Information Technologies. Vol. ۱ (۴) , ۲۰۱۰, ۲۵۶-۲۶۳.

Rounak Sinha, Hemant Kumar Srivastava, Sumita Gupta, ۲۰۱۳,Performance Based Comparison Study of RSAand Elliptic Curve Cryptography, International Journal of Scientific & Engineering Research, Volume ۴, ۷۲۰-۷۲۵.

Sanjay P. Ahuja, Nicole Collier, ۲۰۱۰,An Assessment of WiMax Security, Communications and Network, ۲،۱۳۴-۱۳۷.

Scott William Hoefle, ۲۰۱۲, Survey on Cryptographic Algorithms for Securing Mobile Adhoc Networks, Engineering Universe for Scientific Research and Management

Rajesh Yadav, S. Srinivasan, ۲۰۱۳, Evolution of Wimax Technology, Security Issues and Available Solutions, Vol.۶۶, ۴۴-۴۸.