دانشگاه صنعتی امیرکبیر
(پلی‌تکنیک تهران)
دانشکده مهندسی کامپیوتر

گزارش کتبی درس
روش پژوهش و ارائه

بررسی و مقایسه الگوریتم‌های رمزنگاری شبکه بی‌سیم در مقابله با حمله‌های سایبری

نگارش
محمدمهدی نظری

استاد درس
دکتر مهدی صدیقی

بهار 1402


بسم الله الرحمن الرحيم

سپاس‌گزاری

وظیفه خود می‌دانم که از تلاش‌های مستمر و بی‌وقفه استاد بزرگوار دکتر مهدی صدیقی در راستای آموزش نگارش این گزارش صمیمانه سپاس‌گزاری کنم.

محمدمهدی نظری

بهار 1402

چکیده

در این گزارش به‌صورت کلی درباره روش‌های رمزنگاری شبکه بی‌سیم که شامل الگوریتم‌های WEP، WPA، WPA2 می‌شود، صحبت می‌شود و شیوه رمزنگاری هرکدام را شرح داده و از نظر عملکردی مقایسه می‌شود. در ادامه در هر کدام از روش‌ها به حمله‌هایی که در برابر آن‌ها آسیب‌پذیرند اشاره خواهد شد.

واژه‌های کلیدی

WEP, WPA, WiFi, Authentication

فهرست مطالب

عنوان **صفحه**

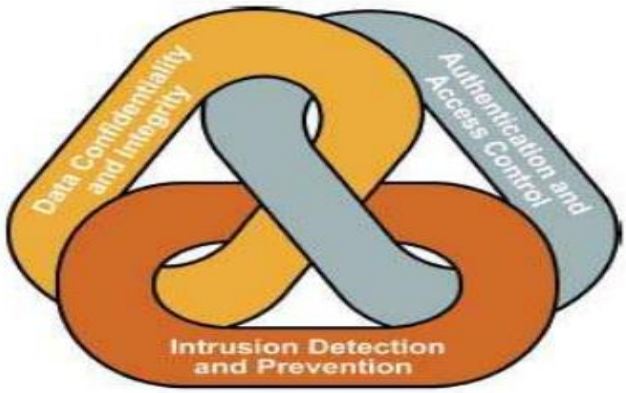
فصل اول – مقدمه

مقدمه

با معرفی شبکه‌های کامپیوتری انقلابی در انتقال و تبادل اطلاعات به وجود آمد و باعث پیشرفت و افزایش سرعت صنایع مختلف شد. اولین نسخه این شبکه‌ها به‌صورت سیمی و محلی بودند که به LAN [1]معروف هستند. باگذشت زمان و پیشرفت تکنولوژی شبکه‌های بی‌سیم تحت عنوان WLAN [2]هم وارد بازار شدند.

این شبکه‌ها که تحت عنوان استاندارد IEEE 802.11 یا تکنولوژی Wi-Fi[3] هم معروف هستند که به‌سرعت محبوبیت زیادی در بین مردم و شرکت‌ها و مؤسسه‌ها کسب کردند. از دلایل این شهرت می‌توان به هزینه کم و سادگی ایجاد شبکه بی‌سیم و تأمین سرعت و کیفیت انتقال داده اشاره کرد. به دلیل رواج بالای استفاده از این شبکه‌ها مسئله امنیت شبکه‌های بی‌سیم ارزش دوچندانی می‌یابد.

امنیت در شبکه‌های بی‌سیم رعایت سه شرط کلی در برقراری ارتباط و انتقال داده تعریف شده است. رعایت محرمانگی و یکپارچگی به معنی محافظت از داده در برابر تهدیدهای هکرها و حفظ صحت داده در فرایند انتقال. مورد دوم دارابودن سیستم احراز هویت مناسب و کنترل دسترسی کاربران به شبکه. در نهایت هم این سیستم باید بتواند نفوذ بدون اجازه به شبکه را تشخیص دهد و از آن جلوگیری کند. سه مورد گفته شده در شکل 1-1 قابل‌مشاهده هستند:



شکل 1-1 سه فاکتور اصلی برقراری امنیت شبکه‌های کامپیوتری [*1*] .

[1] Local Area Network
[2] Wireless Local Area Network
[3] Wireless Fidelity

فصل دوم - معرفی کلی الگوریتم‌ها

WEP -1-2

2-1-1- معرفی کلی الگوریتم

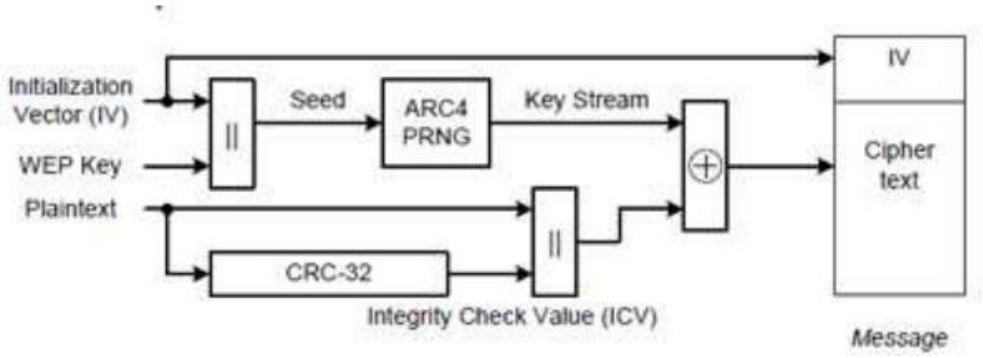
اولین الگوریتم رمزنگاری برای شبکه‌های بی‌سیم WEP نام داشت که در سال 1999 میلادی عرضه شد و شکل کامل آن Wired Equivalent Privacy است . همان‌طور که از نحوه نام‌گذاری آن مشخص است هدف اصلی آن استفاده از الگوریتم‌های امنیتی سیمی بر روی شبکه‌های بیسیم بود که نتوانست نیاز به محرمانگی و یکپارچگی و احراز هویت این شبکه‌ها را فراهم کند و خیلی زود کنار گذاشته شد.

WEP از مکانیزم رمزگذاری کلید مشترک برای شبکه بی‌سیم استفاده می‌کند. بااین‌حال، در عمل، WEP به دلیل نقص در طراحی و اجرای آن ضعیف بود و به‌راحتی قابل هک بود. مهاجمان می‌توانند از ابزارهایی مانند Aircrack-ng برای جمع‌آوری داده‌های کافی برای شکستن کلیدهای رمزگذاری WEP در عرض چند دقیقه استفاده کنند. به دلیل این مسائل امنیتی، WEP دیگر به‌عنوان وسیله‌ای امن برای ارتباط بی‌سیم توصیه نمی‌شود.

2-1-2- شیوه رمزنگاری

از الگوریتم RC4[4] برای حفظ محرمانگی و از الگوریتم CRC-32[5] برای حفظ یکپارچگی استفاده می‌شود. علاوه بر این دو الگوریتم نیاز به دو متغیر دیگر به نام‌های IV[6] و PSK[7] نیاز است که به‌عنوان ورودی به الگوریتم داده می‌شوند.

IV یک بردار ثابت 24 بیتی و PSK یک کلید مشترک بین تمام کاربران شبکه است که می‌تواند 40 بیت یا 104 بیت باشد. روند اجرای رمزنگاری را در شکل 2-1-1 مشاهده می‌شود:



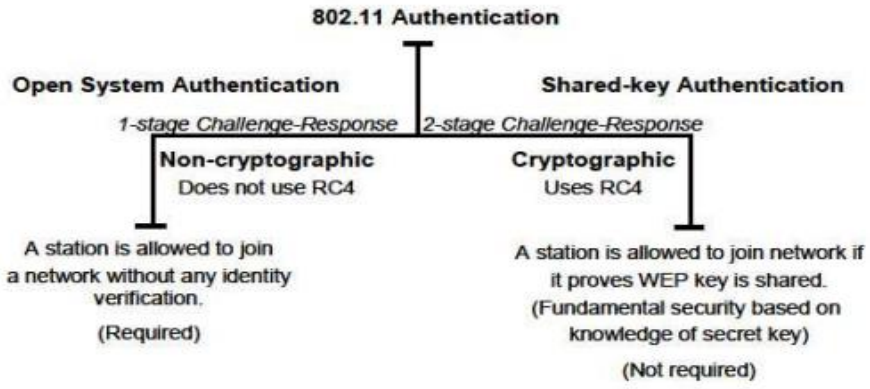
شکل 2-1-1 نحوه کپسوله‌سازی و رمزنگاری الگوریتم *WEP [1]* .

همان‌طور که در شکل مشاهده می‌شود ابتدا IV و کلید مشترک باهم Hash (در اینجا کانکت[8]) شده و یک Seed 64 یا 128 بیتی می‌سازند که به‌عنوان ورودی به الگوریتم RC4 داده می‌شود و در داخل خود از یک Random Number Generator به نام PRNG استفاده می‌کند . به‌صورت موازی Plaintext که ورودی خام از کاربر یا Access Point است همراه با خروجی الگوریتم CRC-32 که دیتا 32 بیتی به نام ICV است Hash شده و خروجی این قسمت با خروجی قسمت بالا باهم XOR می‌شوند و دیتای رمزنگاری شده را می‌سازند. مجموعه فعالیت‌های گفته شده کپسوله‌سازی نامیده می‌شود که در فرستنده انجام شده و به گیرنده ارسال می‌شود. عکس همین عمل در گیرنده انجام می‌شود که Decapsulation نام دارد.

[4] Rivest Cipher 4
[5] Cyclic Redundancy Code
[6] Initialization Vector
[7] Pre Shared Key
[8] Concat

2-1-3- سیستم احراز هویت

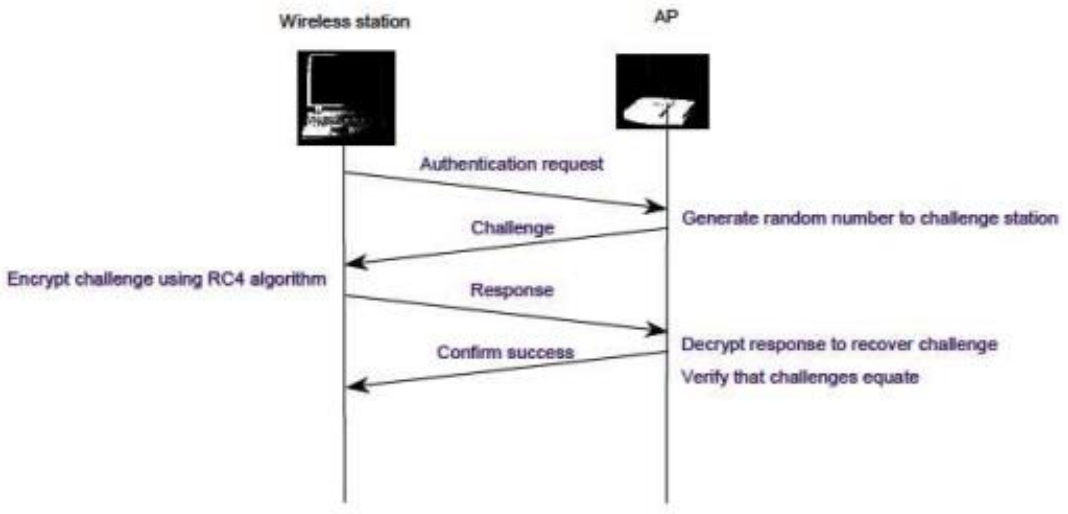
برای شبکه‌هایی که از WEP استفاده می‌کنند دو سیستم احراز هویت Open System و Shared-key وجود دارد که در شکل 2-1-2 قابل‌مشاهده است:



شکل 2-1-2 تقسیم‌بندی روش‌های احراز هویت شبکه با امنیت *WEP [1]* .

در روش Open System فقط از یک مرحله برای احراز هویت استفاده می‌شود که آن هم با استفاده از MAC Address سیستم کاربر است. بدین صورت که دستگاه مشتری که می‌خواهد به شبکه بی‌سیم متصل شود، به‌سادگی یک درخواست احراز هویت را به نقطه دسترسی بی‌سیم ارسال می‌کند. اگر نقطه دسترسی درخواست را دریافت کند، با یک تأیید پاسخ می‌دهد و به مشتری اجازه می‌دهد با شبکه ارتباط برقرار کند. در این روش از رمزنگاری و الگوریتم‌های اشاره شده استفاده نمی‌شود.

اما در روش Shared-key از دو مرحله درخواست و چالش استفاده می‌شود که طی آن Access Point یک عدد تصادفی یا متن خام را به دستگاه کاربر می‌فرستد و کاربر در پاسخ با استفاده از این Plaintext و کلید مشترک شبکه و الگوریتم RC4 متن رمزنگاری شده را تولید کرده و به سرور یا Access Point می‌فرستد و در آنجا رمزگشایی می‌شود و اگر با داده ارسالی اولیه یکسان بود، اجازه وصل‌شدن به شبکه را به کاربر می‌دهد؛ اما در غیر این صورت اجازه دسترسی را به کاربر نمی‌دهد. در شکل 2-1-3 روند گفته شده ملاحظه می‌شود:



شکل 2-1-3 روند احراز هویت با روش کلید مشترک در معماری *WEP [1]* .

2-1-4- نقاط ضعف

این سبک رمزنگاری همان‌طور که در ابتدا هم اشاره کردیم نقاط ضعف زیادی داشت که از جمله آن می‌توان به موارد زیر اشاره کرد:

1. رمزگذاری ضعیف: WEP از یک کلید مخفی مشترک 40 بیتی یا 104 بیتی برای رمزگذاری ترافیک بی‌سیم استفاده می‌کند که مهاجمان با استفاده از ابزارهایی مانند Aircrack-ng به‌راحتی می‌توانند آن را شکست دهند. علاوه بر این، یکپارچگی داده‌های رمزگذاری شده تضمین نمی‌شود و مهاجمان می‌توانند به‌راحتی بسته‌های جدید را تغییر داده یا به شبکه تزریق کنند.

2. عدم احراز هویت: WEP از Open System Authentication استفاده می‌کند، مکانیزم احراز هویت ساده و ضعیف که هیچ‌گونه امنیت واقعی در برابر دسترسی غیرمجاز را ارائه نمی‌دهد. مهاجمان می‌توانند به‌راحتی بسته‌های داده را در شبکه بی‌سیم ضبط کنند و کلید رمزگذاری را بشکنند و به آنها دسترسی کامل به شبکه بدهند.

3. کوتاه‌بودن بردار اولیه: WEP از یک مکانیسم ضعیف تولید IV استفاده می‌کند که منجر به استفاده مکرر از IVها می‌شود و این امر را قادر می‌سازد تا بسته‌های کافی برای شکستن کلید رمزگذاری را با استفاده از brute-force و سایر حملات تحلیل رمزی جمع‌آوری کنند.

4. بدون مدیریت کلید: WEP هیچ مکانیزم داخلی برای مدیریت کلیدها ندارد و در صورت به‌خطرافتادن کلید، تغییر کلیدها و برقراری مجدد ارتباطات ایمن را دشوار می‌کند.

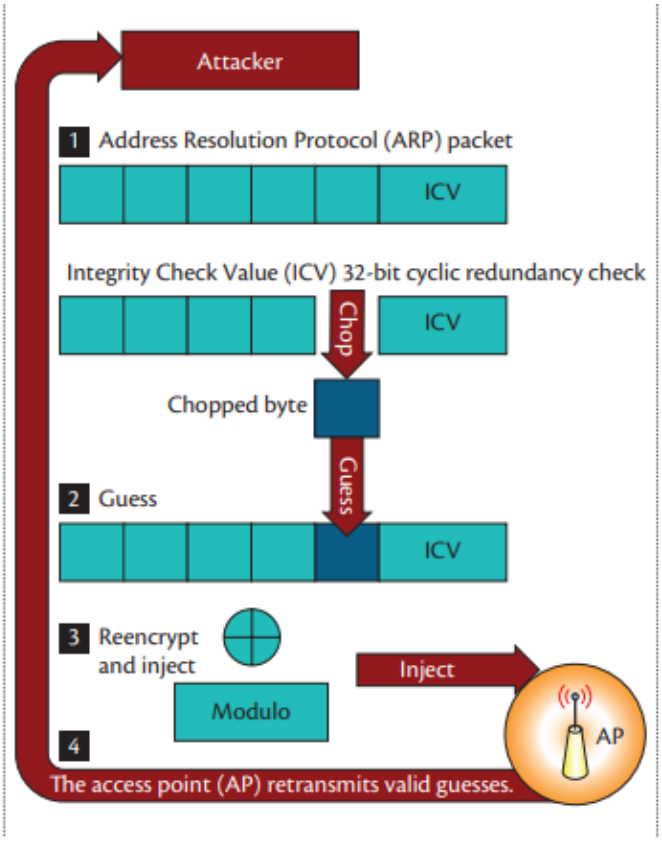
از جمله از نقطه‌ضعف‌های دیگر می‌توان به موارد زیر در شکل 2-1-4 اشاره داشت:

Security Issue or Vulnerability	Remarks
1. Security features in vendor products are frequently not enabled.	Security features, albeit poor in some cases, are not enabled when shipped, and users do not enable when installed. Bad security is generally better than no security.
2. IVs are short (or static).	24-bit IVs cause the generated key stream to repeat. Repetition allows easy decryption of data for a moderately sophisticated adversary.
3. Cryptographic keys are short.	40-bit keys are inadequate for any system. It is generally accepted that key sizes should be greater than 80 bits in length. The longer the key, the less likely a comprise is possible from a brute-force attack.
4. Cryptographic keys are shared.	Keys that are shared can compromise a system. As the number of people sharing the key grows, the security risks also grow. A fundamental tenant of cryptography is that the security of a system is largely dependent on the secrecy of the keys.
5. Cryptographic keys cannot be updated automatically and frequently.	Cryptographic keys should be changed often to prevent brute-force attacks.
6. RC4 has a weak key schedule and is inappropriately used in WEP.	The combination of revealing 24 key bits in the IV and a weakness in the initial few bytes of the RC4 key stream leads to an efficient attack that recovers the key. Most other applications of RC4 do not expose the weaknesses of RC4 because they do not reveal key bits and do not restart the key schedule for every packet. This attack is available to moderately sophisticated adversaries.
7. Packet integrity is poor.	CRC32 and other linear block codes are inadequate for providing cryptographic integrity. Message modification is possible. Linear codes are inadequate for the protection against advertent attacks on data integrity. Cryptographic protection is required to prevent deliberate attacks. Use of noncryptographic protocols often facilitates attacks against the cryptography.
8. No user authentication occurs.	Only the device is authenticated. A device that is stolen can access the network.
9. Authentication is not enabled; only simple SSID identification occurs.	Identity-based systems are highly vulnerable particularly in a wireless system because signals can be more easily intercepted.
10. Device authentication is simple shared-key challenge-response.	One-way challenge-response authentication is subject to "man-in-the-middle" attacks. Mutual authentication is required to provide verification that users and the network are legitimate.
11.The client does not authenticate the AP.	The client needs to authenticate the AP to ensure that it is legitimate and prevent the introduction of rogue APs.

شکل 2-1-4 نقاط ضعف الگوریتم *WEP [1]* .

5-1-2- حمله‌های مورد بررسی

اولین حمله مورد بررسی در این سیستم جمله خردکن یا ChopChop است .در این حمله مهاجم با استراق سمع بسته‌های انتقالی پروتکل ARP[9] در شبکه از بایت آخر همه‌ی حالت‌های آن بسته که از 0 تا 255 است را حدس زده و بسته را دوباره رمزنگاری می‌کند و به Access Point می‌فرستد و در صورت درست بودن بسته ارسالی، Access Point دوباره بسته را در شبکه ارسال می‌کند که مهاجم در این صورت می‌فهمد که حدس درست بوده است. این مراحل به ترتیب برای همه بایت‌ها انجام می‌دهد تا کل بسته را حدس بزند. این مراحل در شکل 5-1-2 به‌نمایش‌درآمده است:



شکل 5-1-2 نحوه اجرای حمله ChopChop *[2]* .

به‌طورکلی حمله به این شبکه‌ها به دودسته Key-recovery و Packet-building تقسیم می‌شوند که در دسته اول هدف اصلی پیداکردن کلید شبکه است و در دسته دوم هدف ساخت بسته‌های ردوبدل شده در شبکه است.

[9] Address Resolution Protocol

انواع این حمله‌ها در شکل‌های 2-1-6 و 2-1-7 قابل‌مشاهده است:

10.1 Key-recovery attacks

Name	Type	Year	Packets	Ratio
FMS	statistical	2001	6,000,000 (64 bit WEP)	86
KoreK	statistical	2004	200,000 (64 bit WEP)	3
PTW	statistical	2007	70,000 (64 bit WEP)	1

شکل 2-1-6 حملات مبتنی بر پیداکردن کلید *[3]* .

10.2 Packets-building attacks

Name	Type	Year	Packets
Chop chop	fake ARP	2004	1 at begin (later: injection-capture)
Fragmentation	fragmentation	2005	1 at begin (later: injection-capture)
Google replay	replay	2010	1 at begin (later: injection-capture)
Coolface	man-in-the-middle	2010	0 at begin (later: injection-capture)

شکل 2-1-7 حملات مبتنی بر پیداکردن بسته‌های داخل شبکه *[3]* .

2-2- **WPA**

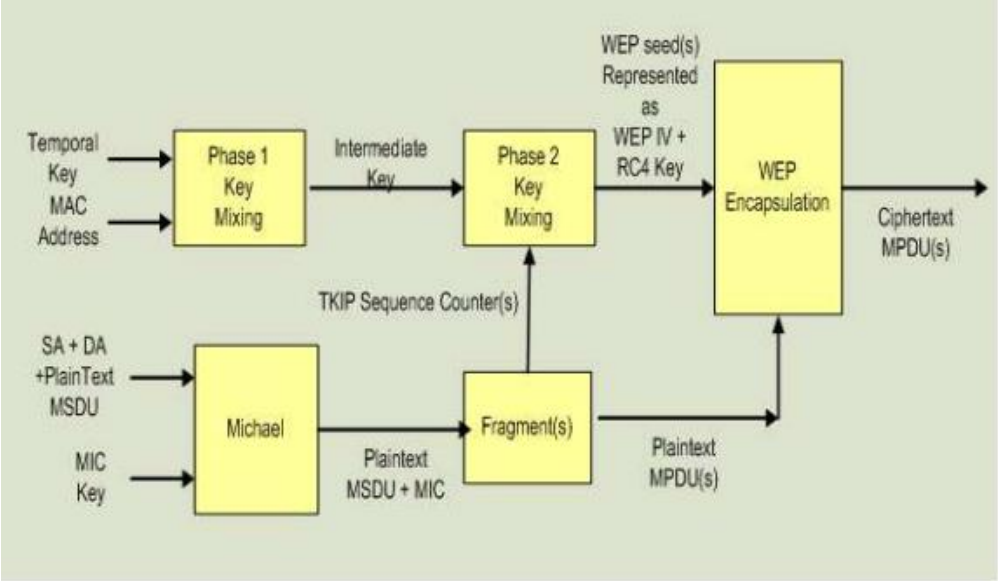
2-2-1- معرفی کلی الگوریتم

این الگوریتم با نام کلی Wi-Fi Protected Access در سال 2002 به‌عنوان راه‌حل برای نقص‌های WEP عرضه شد. از جمله ویژگی‌های این الگوریتم تطابق سخت‌افزاری با نسخه‌های پیشین بود برای اینکه کاربران قبلی هم بتوانند از این الگوریتم‌ها استفاده کنند. برای رمزنگاری هم تنها به‌روزرسانی نرم‌افزاری بر روی WEP صورت گرفت. شیوه اجرایی این الگوریتم به دو صورت WPA-PSK و Enterprise است. حالت اول برای خانه‌ها یا اداره‌های کوچک استفاده می‌شود (SOHO[10]) و مورد دوم برای سازمان‌ها استفاده می‌شود که از سروری بر پایه پروتکل‌های 802.1X و EAP استفاده می‌کند.

2-2-2- شیوه رمزنگاری

در این الگوریتم برای حفظ محرمانگی از الگوریتم TKIP[11] و برای حفظ یکپارچگی از الگوریتم MIC[12] معروف به Michael استفاده می‌شود. این الگوریتم بر روی رمزنگاری WEP پیاده شده و علاوه بر TKIP و MIC در درون خود از RC4 و CRC-32 استفاده می‌کند. علاوه بر اضافه‌شدن و پیچیده ترشدن الگوریتم‌های رمزنگاری نسبت به نسخه قبلی پارامترهای کلید و بردار اولیه هم ارتقا پیدا کرده‌اند و کلید 128 بیت و بردار اولیه 48 بیتی به‌عنوان ورودی به الگوریتم داده شده‌اند. مراحل رمزنگاری در شکل 2-2-1 قابل‌مشاهده است:

[10] Small office/ Home office
[11] Temporal Key Integrity Protocol
[12] Message Integrity Check



شکل 2-2-1 روند کپسوله‌سازی در الگوریتم *WPA [1]* .

ابتدا در فاز اول سه عبارت کلید 128 بیتی و بردار اولیه 48 بیتی و MAC Address باهم ترکیب شده و کلید میانی 80 بیتی را می‌سازند. در مرحله بعدی 16 بیت کم‌ارزش IV با آن ترکیب شده و یکی از ورودی‌هایWEP- Encapsulation را می‌سازد . به‌صورت موازی Plaintext و کلید مایکل 64 بیتی خروجی موردنیاز برای حفظ یکپارچگی را می‌سازند و ورودی دوم بلوک WEP ساخته می‌شود.

2-2-3- سیستم احراز هویت

احراز هویت WPA با استفاده از یک کلید Pre-Shared (PSK) یا یک روش احراز هویت مبتنی بر سرور، معروف به WPA-Enterprise، کار می‌کند که از یک سرور احراز هویت، مانند RADIUS، برای تأیید هویت مشتری استفاده می‌کند.

با WPA-PSK، یک کلمه عبور یا کلید مشترک برای احراز هویت مشتریان در شبکه استفاده می‌شود. این تضمین می‌کند که فقط کسانی که رمز عبور یا کلید را می‌دانند، می‌توانند به شبکه متصل شوند. از طرف دیگر، WPA-Enterprise به مکانیزم احراز هویت قوی‌تری مانند IEEE 802.1X یا EAP[13] نیاز دارد که احراز هویت متقابل بین مشتری و سرور را فراهم می‌کند و امکان استفاده از اعتبارنامه‌های پیچیده‌تر را فراهم می‌کند.

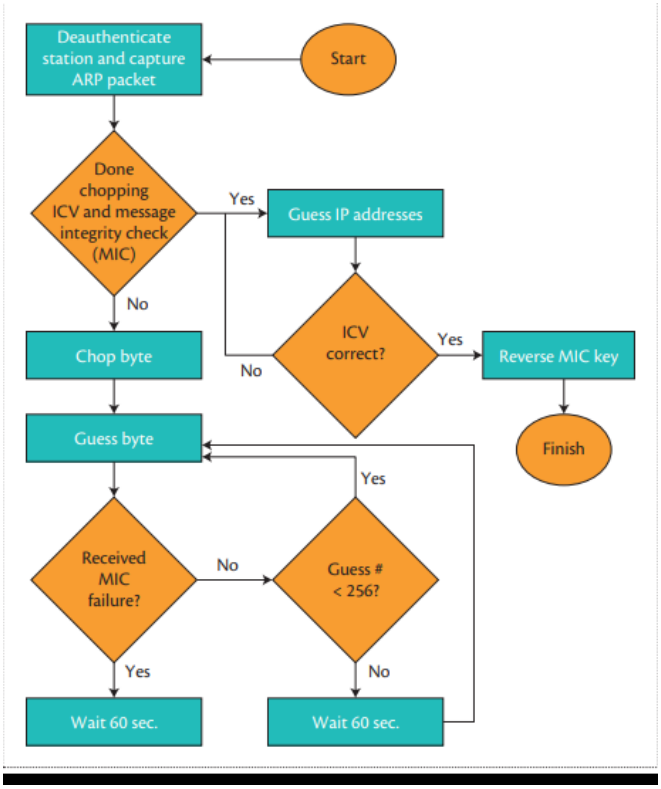
[13] Extensible Authentication Protocol

2-2-4- حمله‌های مورد بررسی

اولین حمله مورد بررسی حمله Beck-Tews است که نسخه پیشرفته‌تر ChopChop است. حمله Beck-Tews نوعی حمله به شبکه‌های بی‌سیم است که از ضعف پروتکل رمزگذاری WPA-TKIP سوءاستفاده می‌کند. اولین‌بار توسط محققان امنیتی آلمانی مارتین بک و اریک توس در سال 2009 نشان داده شد.

این حمله با تزریق بسته‌های ساخته شده ویژه به شبکه بی‌سیم کار می‌کند که به مهاجم اجازه می‌دهد تا کلید مخفی مورداستفاده برای رمزگذاری داده‌های بی‌سیم را کشف کند. هنگامی که کلید بازیابی شد، مهاجم می‌تواند تمام ترافیک بی‌سیم عبوری از شبکه را رمزگشایی کند و به طور بالقوه به اطلاعات و منابع حساس در شبکه دسترسی پیدا کند.

فرق این حمله در WPA با WEP در این است که در سیستم WPA ازReplay attack با استفاده از معیاری به نام MIC countermeasures جلوگیری می‌کند. اگر بسته اشتباهی از طرف کاربر به Access Point ارسال شود یک MIC Failure رخ می‌دهد اگر در فاصله کمتر از 60 ثانیه بعد از اولین MIC Failure یک MIC Failure دیگر رخ بدهد Access Point کل شبکه را به مدت 60 ثانیه خاموش می‌کند و کلید موقت را تغییر می‌دهد مهاجم برای جلوگیری از این اتفاق بعد از اولین MIC Failure باید 60 ثانیه صبر کرده و دوباره بسته ارسال کند. این روند اجرایی در شکل 2-2-2 قابل‌مشاهده است:



شکل 2-2-2 شیوه انجام حمله *Beck-Tews* بر روی شبکه‌های رمزنگاری شده با الگوریتم *WPA [2]* .

از جمله حمله‌های دیگر برای این شبکه می‌توان موارد شکل 2-2-3 را مثال زد:

Name	Year	Utility	Ratio
Beck and Tews	2008	inject traffic (QoS features)	24
Ohigashi-Morii	2009	inject traffic (in all modes)	2
Michael	2010	inject traffic (in all modes)	1
Hole196	2010	man-in-the-middle, inject traffic, DoS attack	-
Dictionary attack		key-recovery	-

شکل 2-2-3 انواع حملات به شبکه با امنیت *WPA [3]* .

WPA2 -2-3

2-3-1- معرفی کلی الگوریتم

WPA2 (Wi-Fi Protected Access II) یک نسخه بهبودیافته از پروتکل امنیتی اصلی WPA است که برای برقراری امنیت شبکه‌های بی‌سیم استفاده می‌شود. در سال 2004 برای رفع نقاط ضعف موجود در WPA و ایجاد امنیت قوی‌تر برای شبکه‌های بی‌سیم معرفی شد.

مانند WPA، WPA2 از یک Pre-Shared Key (PSK) یا روش احراز هویت مبتنی بر سرور برای احراز هویت و رمزگذاری ترافیک شبکه بی‌سیم استفاده می‌کند. بااین‌حال، از یک روش رمزگذاری قوی‌تری به نام AES [14] به‌جای رمزگذاری ضعیف‌تر TKIP استفاده شده در WPA استفاده می‌کند.

WPA2 امنیت قوی‌تری را برای شبکه‌های بی‌سیم فراهم می‌کند و حملاتی مانند حمله Beck-Tews یا شکستن رمز عبور شبکه را برای مهاجمان سخت‌تر می‌کند. این پروتکل در حال حاضر پروتکل توصیه شده برای برقراری امنیت شبکه‌های بی‌سیم است و تا حد زیادی جایگزین WPA از نظر پذیرش و استفاده شده است.

WPA2 دارای دو نسخه است: WPA2-Personal که از یک Pre-Shared Key (PSK) برای احراز هویت کلاینت‌ها در شبکه استفاده می‌کند و WPA2-Enterprise که به مکانیزم احراز هویت مبتنی بر سرور مانند IEEE 802.1X/EAP برای تأیید هویت مشتریان نیاز دارد.

2-3-2- شیوه رمزنگاری

در این روش از الگوریتم AES برای حفظ محرمانگی و از CCMP [15]برای حفظ یکپارچگی استفاده می‌شود. AES یک الگوریتم رمزگذاری متقارن است، به این معنی که از یک کلید برای رمزگذاری و رمزگشایی داده‌ها استفاده می‌شود. پس از تکمیل احراز هویت، دستگاه مشتری و شبکه از کلید جلسه برای رمزگذاری و رمزگشایی داده‌های بی‌سیم ارسال شده بین آنها استفاده می‌کنند. رمزگذاری AES با استفاده از یک کلید رمزگذاری قوی که شکستن آن دشوار است، امنیت بالایی را فراهم می‌کند. سیستم احراز هویت CCMP دارای دو مدل کاری Counter Mode برای رمزنگاری و مدل CBC-MAC برای حفظ یکپارچگی است.

[14] Advanced Encryption Standard
[15] Counter Mode- Cipher Block Chaining MAC Protocol

2-3-3- سیستم احراز هویت

از دو نوع اصلی احراز هویت برای برقراری امنیت شبکه‌های بی‌سیم با رمزنگاری WPA2 استفاده می‌شود:

1. WPA2-Personal: از احراز هویت Pre-Shared Key (PSK) استفاده می‌کند، که در آن همه کلاینت‌ها و Access Point رمز عبور یا کلید یکسانی را به اشتراک می‌گذارند که برای احراز هویت و رمزگذاری ترافیک شبکه بی‌سیم استفاده می‌شود.

2. WPA2-Enterprise: از احراز هویت مبتنی بر سرور، به‌ویژه IEEE 802.1X/EAP استفاده می‌کند، که برای احراز هویت کلاینت‌ها در شبکه به یک سرور RADIUS نیاز دارد.

در WPA2-Enterprise، هنگامی که یک دستگاه مشتری برای اولین‌بار به شبکه متصل می‌شود، درخواستی را برای ایجاد اتصال شبکه به Access Point ارسال می‌کند. سپس نقطه دسترسی پیامی به سرور RADIUS می‌فرستد و از آن می‌خواهد دستگاه مشتری را احراز هویت کند. سپس دستگاه سرویس‌گیرنده و سرور RADIUS یک سری پیام را مبادله می‌کنند تا هویت مشتری را مشخص کرده و اطمینان حاصل کنند که مجاز به دسترسی به شبکه است.

فرایند احراز هویت در WPA2-Enterprise می‌تواند از مکانیسم‌های مختلف احراز هویت، از جمله گواهی‌های دیجیتال، ترکیب نام کاربری و رمز عبور، یا احراز هویت کارت هوشمند، بسته به پیکربندی خاص شبکه، استفاده کند.

4-3-2- حمله‌های مورد بررسی

مهم‌ترین حمله برای این شبکه‌ها حمله DoS[16]است. هدف از حمله DoS این است که سیستم یا شبکه را برای کاربران موردنظر از دسترس خارج کند و اغلب سیستم را پاسخگو نمی‌کند یا آن را به طور کامل خاموش می‌کند.

انواع مختلفی از حملات DoS وجود دارد، از جمله:

1. حملات سیل: شامل ارسال حجم زیادی از ترافیک به سیستم یا شبکه موردنظر، غلبه بر منابع آن و عدم پاسخگویی آن است.

2. حملات سیل SYN[17]: به طور خاص اتصالات TCP [18](پروتکل کنترل انتقال) را با ارسال تعداد زیادی درخواست SYN هدف قرار می‌دهند، اما به پاسخ‌های SYN-ACK [19]سرور پاسخ نمی‌دهند و باعث می‌شود که سرور منتظر تأیید نهایی بماند و در نهایت خراب شود.

3. حملات سیل پینگ: شبکه هدف را با درخواست‌های پینگ پر می‌کند تا پهنای باند آن را مصرف کند و آن را برای درخواست‌های قانونی از دسترس خارج کند.

4. Distributed Denial of Service (DDoS): شامل استفاده از تعداد زیادی رایانه در معرض خطر (به نام بات نت) برای انجام یک حمله هماهنگ به یک شبکه یا سیستم هدف است.

حملات DoS می‌تواند عواقب جدی داشته باشد، از جمله اختلال در عملیات تجاری، ازدست‌دادن درآمد، و به طور بالقوه قراردادن داده‌های حساس در معرض دسترسی غیرمجاز. مدیران شبکه اغلب از فایروال‌ها، سیستم‌های تشخیص نفوذ و سایر اقدامات امنیتی برای کاهش تأثیر حملات DoS و جلوگیری از وقوع آنها در وهله اول استفاده می‌کنند.

[16] Denial of Service
[17] Synchronization
[18] Transmission Control Protocol
[19] Acknowledgement

برای مقایسه گذرداد داده بین روش‌های مختلف از یک سناریو تست استفاده شده که طی آن یک فایل بین دو کلاینت فرستاده شده و زمان این انتقال اندازه‌گیری شده است. حاصل تقسیم اندازه این فایل بر زمان انتقال برون‌داد را نتیجه می‌دهد.

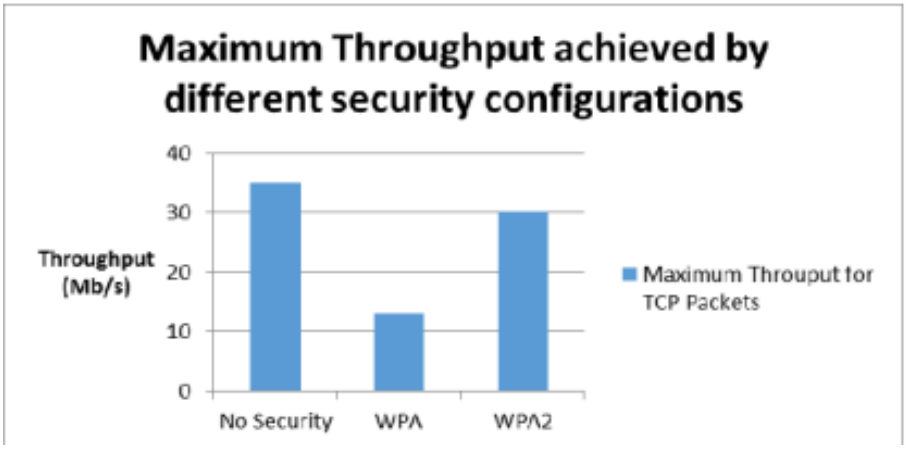
سه حالت برای اندازه‌گیری برون‌داد در این تست انجام شده است:

الف) بدون امنیت

ب) WPA با احراز هویت PSK و رمزگذاری RC4

ج) WPA2 با احراز هویت PSK و رمزگذاری AES

نتایج در شکل 3-1 قابل‌مشاهده است:



شکل 3-1 نتایج آزمایش برون‌داد بر روی دو کلاینت در سه حالت گفته شده *[4]* .

همان‌طور که در نتایج شکل مشاهده می‌شود بیشترین گذرداد برای حالت بدون امنیت است چون‌که هیچ پردازشی روی داده‌های انتقالی انجام نمی‌شود با گذر به رمزنگاری با WPA کاهش شدیدی در برون‌داد مشاهده می‌شود که دلیل آن پیچیدگی‌های الگوریتم‌های TKIP و MIC است که سرعت انتقال داده را پایین می‌آورد در WPA2 با معرفی الگوریتم‌های جدید و بهینه‌سازی پردازش‌ها به گذرداد خیلی بهتری رسیدیم؛ اما هنوز از حالت بدون امنیت کمتر خواهد بود.

[20] Throughput

فصل چهارم - جمع‌بندی و نتیجه‌گیری

جمع‌بندی و نتیجه‌گیری

در این گزارش ابتدا درباره شبکه‌های بی‌سیم و ویژگی‌های آن‌ها صحبت کردیم سپس وارد بحث امنیت در شبکه‌ها دلیل نساز به آن و فاکتورهای مورد بررسی آن صحبت شد. در بخش بعدی سه الگوریتم اصلی رمزنگاری شبکه‌های بی‌سیم را از نظر تاریخچه شیوه رمزنگاری نحوه احراز هویت و حملات متداول به آن‌ها بررسی کردیم. در آخر هم یک مقایسه بین گذرداد بین الگوریتم‌ها صورت داده شده است.

مراجع و منابع

[1] G. Georgios ,“WiFi security and testbed implementation for WEP/ WPA cracking demonstration,” Ph.D. dissertation, College of Eng. and Sc. and Comp, Kingston Univ., London, 2014. [Online]. Available: https://www.academia.edu/7438337/Dcom_00234

[2] F. T. Sheldon, J. M. Weber, S. -M. Yoo and W. D. Pan, "The Insecurity of Wireless Networks," in IEEE Security & Privacy, vol. 10, no. 4, pp. 54-61, July-Aug. 2012, doi: 10.1109/MSP.2012.60.

[3] M. Caneill, J. Gilis, “Attacks against the WiFi protocols WEP and WPA,” . October - December. 2010.. [Online]. Available: https://matthieu.io/dl/papers/wifi-attacks-wep-wpa.pdf

[4] A. H. Adnan et al., "A comparative study of WLAN security protocols: WPA, WPA2," 2015 International Conference on Advances in Electrical Engineering (ICAEE), Dhaka, Bangladesh, 2015, pp. 165-169, doi: 10.1109/ICAEE.2015.7506822.

[5] B. Potter, "Wireless security's future," in IEEE Security & Privacy, vol. 1, no. 4, pp. 68-72, July-Aug. 2003, doi: 10.1109/MSECP.2003.1219074.

[6] Rana, Muhammad Ehsan & Abdulla, Mohamed & Arun, Kuruvikulam. (2021). Common Security Protocols for Wireless Networks: A Comparative Analysis. 10.2991/ahis.k.210913.080.