Journal of Information and communication Technology in policing (JICTP)
Journal Homepage: pitc.jrl.police.ir

Vol. 2, No.4 (8), Autumn 2021

Selecting the optimal conversational algorithm on the Internet based on simulation

Received: 18 November 2021
Accepted: 15 January 2022
Article type: Research Article
PP: 25-39

DOI:
10.22034/pitc.2021.208213.1053

Behzad lak
Amin Police University, Tehran, Iran
(Corresponding author)
behzad_lak@yahoo.com

Saeid bakhtiari
Amin Police University, Tehran, Iran
saeid.bakhtiarii@chmail.ir

Seid mostafa rezvani
Amin Police University, Tehran, Iran
sm.rezvani.uni@gmail.com

Abstract

VOIP technology provides significant benefits for customers and communication service providers such as cost savings, good media services, telephone and service portability, mobility and integration with other applications. However, there are many challenges in working with VOIP technology; Such as architectural complexity, interoperability issues, service quality issues, and security challenges. Among these issues, security risks are the most important. This study provide an algorithm to improve the security of encrypted conversations based on VOIP. In this our simulation, we use the NS2 emulator with the version 2.35NS that it is under Linux. The proposed method is AES-GCM encryption, which is compared with AES-CTR in different network parameters with two factors of time and packet size. The obtained results show that the package delivery rate in AES-GCM is higher than the operating mode of AES-CTR, which is the reason for the superiority of AES-GCM in providing service quality, furthermore in this method, encryption time, decryption, power consumption, and packet loss rate in encryption are far less than operational. In another comparison, the required time to sending the package and the delay rate in transfer of package in the proposed mode of operation is far less. Therefore, in the proposed method the low rate of time and delay are required in comparison with the AES-CTR method.

Keywords: Voice over IP(VOIP), Public Switched Telephone Network (PSTN), Security, security protocols

نشریه علمی "فناوری اطلاعات و ارتباطات انتظامی"

سامانه نشریات: pitc.jrl.police.ir

سال دوم- شماره چهارم(پیاپی ۸)– زمستان ۱۴۰۰

انتخاب الگوریتم مطلوب مکالمات در بستر اینترنت مبتنی برشبیه سازی

دریافت: ۱۴۰۰/۰۳/۰۱
پذیرش: ۱۴۰۰/۰۷/۲۵
نوع مقاله: پژوهشی
صص: ۳۹-۲۵
شناسه دیجیتال(doi).
10.22034/pitc.2021.208213.1053

بهزاد لک
استادیار، گروه فناوری اطلاعات و ارتباطات، دانشگاه علوم انتظامی امین، تهران، ایران (نویسنده مسئول)
behzad_lak@yahoo.com

سعید بختیاری
استادیار، گروه فتا ، دانشگاه علوم انتظامی امین، تهران، ایران
saeid.bakhtiarii@chmail.ir

سید مصطفی رضوانی
گروه فناوری اطلاعات و ارتباطات، دانشگاه علوم انتظامی امین، تهران، ایران
sm.rezvani.uni@gmail.com

چکیده

فنآوری ویپ مزایای قابل توجهی برای مشتریان و ارائه دهندگان خدمات ارتباطی مانند صرفه جویی در هزینه، خدمات رسانه‌ای خوب، قابلیت انتقال تلفن و خدمات، تحرک و ادغام با سایر برنامه‌ها را فراهم می‌آورد. با این وجود، راه‌اندازی فناوری ویپ با چالش‌های بسیاری مواجه است؛ مانند پیچیدگی معماری، مسائل مربوط به قابلیت همکاری، مسائل مربوط به کیفیت خدمات و چالش‌های امنیتی.در این بین، خطرات امنیتی بیشترین نگرانی را با خود به همراه دارند. این تحقیق یک الگوریتم برای بهبود امنیت مکالمات رمزنگاری شده مبتنی بر ویپ پیشنهاد می دهد. پژوهش از نظر هدف کاربردی و به روش شبیه سازی اجرا شده است. ابزار مورد استفاده شبیه ساز **NS2** و نسخه **NS2.35** می باشد که تحت لینوکس و کد متن باز می‌باشد. راهکار پیشنهادی رمزنگاری **AES-GCM** می باشد که با **AES-CTR** در پارامترهای مختلف شبکه با دو فاکتور زمان و اندازه بسته مقایسه شده است. نتایج نشان می دهد، نرخ تحویل بسته در **AES-GCM** بیشتر از مد عملیاتی **AES-CTR** می باشد که این امر دلیل برتری **AES-GCM** در ارائه کیفیت سرویس می‌باشد و همچنین زمان رمزگذاری، کدگشائی، میزان مصرف انرژی و نرخ از دست رفتن بسته در رمزگذاری به مراتب کمتر از مدعملیاتی می باشد. در مقایسه ای دیگر میزان زمان مصرفی برای ارسال بسته و میزان تاخیر انتقال بسته در مد عملیاتی پیشنهادی به مراتب کمتر است. لذا میزان زمان و تاخیر کمتری در مد پیشنهادی نسبت به **AES-CTR** وجود دارد.

کلیدواژه‌ها: ویپ، شبکه تلفن سنتی، امنیت، پروتکل های امنیتی

۱- مقدمه

انتقال صدا بر روی پروتکل اینترنت (ویپ[1])، توانایی انتقال بسته‌های صوتی به‌صورت تلفنی، فکس و یا ویدیو کنفرانس بر روی یک شبکه مبتنی بر آی‌پی[2] است. علت محبوبیت بالای ویپ این است که در مقایسه با سیستم تلفن قدیمی، مزایای قابل‌توجهی از جمله صرفه‌جویی در هزینه، ارائه خدمات رسانه‌ای جدید، قابلیت حمل و ادغام با سایر برنامه‌ها را فراهم می‌کند [۱]. ویپ اساساً، به تصویری از خدمات ارتباطی مانند صوت، فکس، پیامک و پیام‌رسانی صوتی بر بستر اینترنت در مقابل شبکه تلفن سنتی اشاره دارد و شامل سیگنال دهی، راه‌اندازی کانال، دیجیتال‌سازی سیگنال‌های صوتی آنالوگ و کدگذاری می‌باشد. در بستر ویپ، اطلاعات دیجیتال به‌جای این‌که از طریق شبکه‌مدار سوییچینگ ارسال گردد، ابتدا بایستی بسته‌بندی‌شده و سپس به‌عنوان بسته‌های آی‌پی در بستر شبکه ارسال شوند. این امر باعث سادگی در گسترش، کاهش هزینه‌ها، امنیت بالاتر، ترکیب کارکردهای صدا و داده، انعطاف‌پذیری، سادگی در پیاده‌سازی، مدیریت و نگهداری آسان‌تر و صرفه‌جویی در مقایسه با شبکه تلفن عمومی گردیده است [۲]. با وجود مزایایی که فناوری ویپ دارد، باز هم از بسیاری از موانع مانند پیچیدگی معماری، مسائل مربوط به قابلیت هماهنگ‌سازی، ارائه خدمات و مسائل امنیتی رنج می‌برد. همچنین پیش‌بینی معیار کیفیت خدمات می‌تواند چالش بزرگی باشد. بر این اساس اطلاعات حساس‌تر به‌صورت دیجیتالی مبادله می‌شود و تقاضای امنیت و حریم خصوصی در خدمات مورد استفاده را با خود به همراه دارد. رمزگذاری، حریم خصوصی را فراهم می‌کند، اما پیچیدگی‌های سیستم را نیز بالا می‌برد؛ مانند اندازه-گیری و پیش‌بینی معیار کیفیت خدمات. هنگام تولید معیار کیفیت خدمات برای سیگنال‌های رمزگذاری شده باید از مدل پارامتری استفاده شود؛ زیرا دسترسی به سیگنال اولیه یا سیگنال حاصل، سخت می‌شود یا حداقل به‌روشنی متن اولیه نیست. معیار دقیق کیفیت خدمات نه‌تنها برای مشتریان سودمند است، بلکه برای سرویس‌دهنده نیز مفید می‌باشد. این معیار را می‌توان مورد استفاده قرار داد تا بتواند انتخاب‌های طراحی را ارزیابی کند و حتی می‌تواند برای تنظیم سرویس در هنگام استفاده، برای به حداکثر رساندن کیفیت خدمات ارائه شده، استفاده شود [۳].

در میان معایب ذکر شده، مسائل امنیتی ویپ جدی‌تر از بقیه است؛ زیرا دستگاه‌های امنیتی سنتی، پروتکل‌ها و معماری‌ها نمی‌توانند به‌طور مناسب از سیستم‌های ویپ در برابر حملات امنیتی محافظت کنند. امنیت ویپ، یک موضوع بسیار گسترده و مهم می‌باشد و می‌توان برای آن تعاریف مختلفی ارائه کرد؛ به‌طوری‌که هیچ‌یک از این تعاریف قطعی و ثابت نخواهند بود، چراکه امنیت در ارتباط با مسائلی است که هر روز در حال تغییر و تحول می‌باشند. البته در اینجا امنیت در سیستم‌های تلفنی مبتنی بر ویپ مطرح است. برقراری امنیت دارای لایه‌های مختلفی است؛ به‌عبارت‌دیگر در جهت امن سازی یک سیستم، باید سطوح مختلفی از امنیت را پیاده‌سازی کرد. لایه‌هایی شامل دیوار آتش[3]، احراز هویت و مانیتورینگ از جمله آن است. این معماری ساده‌ترین سطوح امنیتی را پوشش می‌دهد، به‌طوری‌که با پیاده‌سازی درست این لایه‌ها و تکنیک‌های مناسب و مرتبط با آن‌ها، می‌توان امنیت سیستم را به‌صورت قابل‌توجهی بهبود بخشید. یکی دیگر از مسائل مهمی که کمتر به آن توجه می‌شود، منشأ تهدیدات امنیتی است. معمولاً تصور می‌شود که حملات تنها منشأ اینترنتی و خارجی دارند، این در صورتی است که تهدیدات امنیتی داخلی نادیده گرفته می‌شوند؛ درحالی‌که از داخل، دسترسی به منابع سیستم راحت‌تر بوده و بسیاری از فیلترهای امنیتی وجود نخواهد داشت.

یکی از رایج‌ترین جمله‌هایی که شنیده می‌شود این است که کارمندان دانش کافی برای نفوذ به سیستم را ندارند. درحالی‌که نصب یک بدافزار با قابلیت ذخیره‌سازی نام کاربری و رمز عبور مربوط به تلفن‌ها، توسط کارمندی که از داخل به سیستم دسترسی دارد، امنیت سیستم تلفنی را به شدت تهدید کرده و امکان نفوذ به سیستم را از بیرون افزایش می‌دهد. بر این اساس، باید امنیت سیستم را از داخل و خارج شبکه موردتوجه قرار داد و همه سیاست‌های امنیتی را بر روی هر دو دامنه اعمال کرد.

بنابراین فناوری ویپ با مجموعه‌ای از آسیب‌پذیری‌ها شناخته می‌شود، به این معنی که نقص‌هایی وجود دارد که ممکن است توسط حمله کننده برای انجام حملات امنیتی مورد استفاده قرار گیرد. به‌طورکلی دو نوع آسیب‌پذیری در ویپ وجود دارد. یکی از این آسیب‌پذیری‌ها، ذاتی است که از زیرساخت می‌آید، مانند شبکه و سیستم‌عامل که در آن برنامه‌های ویپ در حال اجرا هستند. ویپ آسیب‌پذیری دیگر خود را از پروتکل‌ها و دستگاه‌هایش می‌گیرد. تمام اجزای مرتبط با استقرار سرویس ویپ، عناصر آسیب‌پذیری هستند که به‌طور مستقیم یا غیرمستقیم بر آن تأثیر می‌گذارد. اجزای آسیب‌پذیر اصلی در یک سیستم ویپ عبارتند از: سیستم‌عامل برنامه ویپ، برنامه خود ویپ، پروتکل‌های ویپ، رابط مدیریت و دستگاه‌های شبکه مانند سوییچ و روتر. آسیب‌پذیری‌های ویپ می‌تواند برای ایجاد انواع مختلف حملات مورد استفاده قرار گیرد. برای مقابله با مسائل امنیتی که اشاره شد، نیاز است تا پروتکل‌های امنیتی و الگوریتم‌های رمزنگاری مناسب با سیستم ویپ را به‌کار گرفت. لازمه به‌کارگیری الگوریتم کارآمد جهت بهبود کارایی و امنیت ویپ، ابتدا مقایسه روش‌های امنیتی مورد استفاده در ویپ و یافتن نقاط ضعف و قوت آن‌ها و نهایتاً پیاده‌سازی است [۵ و ۴]. بر اساس تحقیقات صورت گرفته، از جمله راهکارهای امنیتی پیشنهادی جهت برقراری امنیت در سرویس‌های اینترنتی استفاده از پروتکل‌های امنیتی

[1] Voice over IP(VOIP)
[2] Internet Protocol(IP)

3 Firewall

TLS[1]، SRTP[2] و IPsec[3] برای محافظت از جلسات برقراری ارتباط و RTP[4] جهت ارائه احراز هویت، یکپارچگی[5] و محرمانه بودن، برای بسته‌های مربوط به ویپ می‌باشد.

این مقاله بر اساس مقایسه مقدماتی بین استفاده از IPsec در مقابل TLS و SRTP به‌عنوان روش‌های رمزنگاری مورد استفاده برای تأمین امنیت این کانال‌های ارتباطی است. همچنین نقاط ضعف و قوت آن‌ها را موردبررسی قرار می‌دهد. هدف و نوآوری اصلی این مقاله، مقایسه، پیاده‌سازی و ارزیابی الگوریتم رمز AES-GCM[6] بعنوان یک الگوریتم کارآمد، به‌جای AES-CTR[7] در پروتکل SRTP که در حال حاضر نیز توسط ارائه‌کنندگان ویپ مورد استفاده قرار می‌گیرد، است. در حقیقت این مقاله به دنبال پاسخ دادن به این سؤال اصلی است که: "الگوریتم رمز AES-GCM چگونه می‌تواند امنیت مکالمات رمزنگاری شده مبتنی بر ویپ را افزایش دهد؟"

۲- مرور متون تحقیق (مبانی نظری، مفاهیم و تعاریف مورد نیاز در ویپ)

با مطرح شدن شبکه‌های کامپیوتری، به‌خصوص اینترنت و امکان برقراری ارتباط به‌صورت سوییچ بین بسته‌های داده، ارسال داده بر روی این شبکه‌ها به‌صورت جدی مطرح شد و در تمامی موارد موفقیت‌آمیز نمود. اگر زمانی دستگاه‌های فکس و تلکس بر روی شبکه‌های مخابراتی سنتی متن و تصویر را از جایی به‌جای دیگر منتقل می‌کردند، امروزه پست الکترونیکی و پیام‌های بین کامپیوتری این جایگاه را به دست آورده‌اند، به‌نحوی‌که صورت قدیمی ارسال اطلاعات را تحت شعاع خود قرار داده‌اند [۶].

درجایی که اطلاعات منتقل شده بر روی شبکه‌های کامپیوتری شکل صوتی به خود بگیرند، ویپ مطرح می‌شود. البته این نکته باید ذکر شود که برای داشتن یک ارتباط از نوع ویپ باید شبکه‌ای بر پایه پروتکل آی‌پی داشته باشیم. حال با توجه به این‌که بزرگ‌ترین شبکه بر پایه ویپ شبکه اینترنت است، به‌طورمعمول از فناوری ویپ به‌عنوان منتقل کننده صدا بر روی شبکه اینترنت یاد می‌شود؛ بنابراین ویپ یا انتقال صدا در بستر اینترنت که با نام آی‌پی تلفنی نیز از آن یاد می‌شود، امکان استفاده از اینترنت به‌منظور مکالمات تلفنی را فراهم می‌نماید. در مقابل استفاده از خطوط تلفن سنتی، ویپ از فناوری دیجیتال استفاده می‌نماید و نیازمند یک اتصال باند پهن[8] نظیر DSL2[9] است. شبکه‌های مبتنی بر پروتکل TCP/IP[10] از بسته‌های اطلاعاتی آی‌پی تشکیل می‌گردند که شامل یک هدر برای کنترل ارتباطات و یک پی‌لود[11] به‌منظور مبادله داده می‌باشند. فناوری ویپ از بسته‌های اطلاعاتی آی‌پی به‌منظور حرکت در شبکه و رسیدن به مقصد نهایی استفاده می‌نماید [۷]. برای ایجاد یک ارتباط مبتنی بر ویپ می‌بایست مراحل زیر را دنبال نمود و البته باید توجه داشت که تمامی مراحل باید به‌صورت بلادرنگ انجام شود.

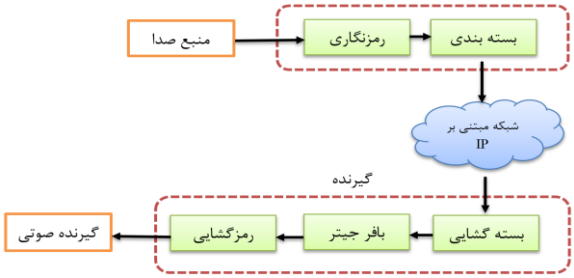
شکل (۱): مراحل ایجاد یک ارتباط با ویپ

این پنج مرحله، نحوه کامل ایجاد یک ارتباط را با ویپ مشخص می‌کند [۸]. با سیستم‌های ویپ به یکی از روش‌های مبدل تلفن آنالوگ، تلفن‌های آی‌پی و کامپیوتر به کامپیوتر می‌توان ارتباط تلفنی برقرار کرد [۹]. فناوری ویپ کاربردهای بسیاری در سیستم‌های مخابراتی دارد. از ویپ برای انتقال خطوط تلفن، اتصال دفاتر به سیستم تلفنی یکدیگر، ایجاد مرکز نوین پشتیبانی مشترکین [۱۰] جایگزینی سانترال‌های سنتی، گسترش مراکز تلفن [۱۱] اپراتورهای تلفن‌های ثابت و اپراتورهای تلفن همراه [۱۲] استفاده شده است. فناوری ویپ در این موارد باعث کاهش هزینه، افزایش امکانات و بهبود قابلیت اطمینان می‌شود. در یک نگاه سطح بالا، یک سیستم ویپ شامل سه قسمت عمده فرستنده، شبکه آی‌پی و گیرنده است که همه آن‌ها در شکل (۲) نشان داده شده است. یک کدک صوتی در فرستنده به یک سیگنال دیجیتال تبدیل می‌شود و جریان صوت دریافت شده را به قالب‌های گفتاری، فشرده می‌کند. برای جلوگیری از انبوه شدن شبکه از این قالب‌ها، چندین قالب گفتاری بسته‌بندی می‌شوند تا بتوانند بسته‌های اطلاعاتی، مانند بسته‌های RTP را شکل دهند و هدرهای مورد نیاز شبکه اضافه شوند.

پس‌ازآن، شبکه ممکن است تا زمانی که بسته به گیرنده تحویل داده می‌شود، اختلالات خاصی از قبیل از دست دادن بسته، تأخیر و تحریک را نشان دهد. بسته‌ها از هدرها جدا می‌شوند و قالب‌های گفتاری توسط جعبه یابنده استخراج می‌شوند. برای مقابله با جیتر، تغییر در تأخیر بسته، توسط شبکه یک بافر استفاده می‌شود. در

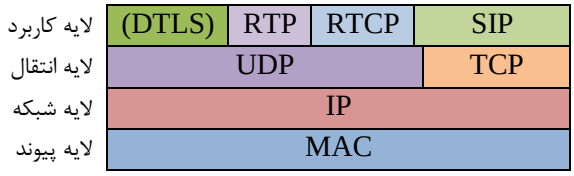
1Transport Layer Security(TLS)
2 Secure Real-time Transport Protocol(SRTP)
3 Internet Protocol Security(IPsec)
4 Real-Time Transport Protocol Flooding Attack(RTP)
5 Integrity
6 Galois/Counter Mode(GCM)
7 AES Counter Mode(CTR)
8 Broadband
9 Digital Subscriber Line 2
10 Transmission Control Protocol/Internet Protocol
11 payload

نهایت قالب‌های گفتاری کدگشائی و خارج می‌شوند [۱۳].



شکل (۲): دیاگرام توصیفی از یک سیستم ویپ [۱۳]

ویپ شامل مجموعه‌ای از فناوری‌ها و پروتکل‌هایی است که با هم به ارائه خدمات ارتباطی در اینترنت می‌پردازند و در مقابل شبکه تلفن عمومی که به‌عنوان تماس‌های صوتی معمولی استفاده می‌شود، قرار می‌گیرند. پروتکل‌های مربوطه در شکل (۳) نشان داده شده است. ویژگی اصلی این است که پروتکل آی‌پی یک هدر ۲۰ بایتی اضافه می‌کند و لایه پیوند، ۱۸ بایت برای هدر کد احراز اصالت پیام[1]، اگر از اترنت استفاده شود، اضافه می‌کند [۱۴].



شکل (۳): پروتکل‌های مربوط به معماری ویپ [۱۴]

در زمان استفاده از خطوط شبکه تلفن سنتی[2]، کاربران هزینه بیشتری جهت استفاده به شرکت ارائه‌دهنده خدمات پرداخت می‌نمایند علاوه بر این، نمی‌توان به‌طور همزمان با بیش از یک شخص گفتگو نمود.

مهم‌ترین مزیت فناوری ویپ مقرون‌به‌صرفه بودن آن است. صرفه‌جویی قابل ملاحظه‌ای در بعد هزینه‌های تماس و سخت‌افزار به‌خصوص با یک سیستم مدیریت شده اجاره‌ای در ویپ لحاظ شده است. صرفه‌جویی در زمینه سخت‌افزار که با استفاده از سخت‌افزار استاندارد کامپیوتر تأمین می‌شود و صرفه‌جویی در هزینه تماس‌ها که کاملاً وابسته به مسافت بوده و از طریق یک سیستم مدیریت شده، هزینه پرداختی نیز پشتیبانی می‌شود. سایر مزایای ویپ شامل قابلیت انعطاف، یکپارچگی، قابلیت حمل، سادگی می‌باشد. از جمله معایب تلفن‌های مبتنی بر ویپ می‌توان به مشکلات در زمان قطع برق، مشکل در تعیین اتوماتیک محل تماس‌های فوری در سرویس‌های اضطراری مانند ۱۱۰و۱۱۹، هزینه بالاتر دستگاه تلفن، مشکلات مباحث شبکه، کیفیت صوت، تأخیر، سازگاری، وابستگی، فشرده‌سازی و زمان برگرداندن داده به حالت اولیه اشاره کرد [۱۵و۱۶].

۳- رمزنگاری

هدف از رمزنگاری معمولاً چهار مفهوم محرمانگی[3]، یکپارچگی، احراز هویت[4] و انکارناپذیری می‌باشد. ازلحاظ تاریخی، رمزنگاری اغلب به‌طور مستقیم برای رمزگذاری یا کدگشائی استفاده می‌شود.

در این راستا دو نوع رمزنگاری وجود دارد: متقارن و نامتقارن.

سیستم رمزنگاری کلید متقارن به‌منظور ذخیره‌سازی، انتقال و پردازش پیام استفاده می‌شود. الگوریتم کلید متقارن عمل رمزگذاری و فرآیند کدگشائی را بر اساس یک کلید واحد انجام می‌دهد که توسط دو یا چند طرف به اشتراک گذاشته شده است. الگوریتم استاندارد رمزنگاری پیشرفته و استفاده از تابع چکیده ساز از الگوریتم‌های رمزنگاری کلید متقارن است [۱۷]. رمزنگاری کلید عمومی[5] یا نامتقارن روش مؤثری برای ارائه محرمانه بودن و احراز هویت است. در رمزنگاری کلید عمومی، یک جفت کلید عمومی و کلید خصوصی وجود دارد که کلید عمومی برای عموم قابل دسترس است و کلید خصوصی در مکانی امن نگهداری می‌شود.RSA[6]و رمزنگاری خم بیضوی[7] دو مورد از الگوریتم‌های رمزنگاری کلید عمومی برای احراز هویت هستند [۱۸]. در جدول ۱. الگوریتم‌های معمول که در رمزنگاری مورد استفاده قرار می‌گیرند به همراه برخی از خصوصیات آن‌ها آمده است.

مدهای عملیاتی مختلفی (نظیر ECB، CBC، CFB، OFB و غیره) برای رمزکننده‌های بلوکی ارائه گردیده‌اند. تمرکز این تحقیق بر روی دو مد عملیاتی GCM و CTR می‌باشد.

مد عملیاتی GCM یک الگوریتم رمزنگاری احراز هویت شده با داده‌های اضافی است که یک متن ساده را در CTR رمزگذاری می‌کند. این مد، همچنین امکان تأیید برخی از اطلاعات اضافی بدون رمزگذاری را فراهم می‌کند. از ویژگی‌های مد عملیاتی GCM بهره‌گیری از بردار اولیه وXOR نمودن بلوک‌های کلید با متن اصلی برای ایجاد بلوک‌های رمز شده بر اساس عملکرد ریاضی می‌باشد. در حقیقت GCM، ایدئال برای حفاظت از اطلاعات بسته‌بندی شده است زیرا حداقل تأخیر و حداقل سربار عملیاتی را دارا می‌باشد [۱۹].

1.Message authentication code)MAC(
2 Public Switched Telephone Network (PSTN)

3 Confidentiality
4 Authentication
5 Publick Key Cryptography
6 Rivest Shamir Adleman(RSA)
7 Elliptic Curve Cryptography(ECC)

جدول (۱): الگوریتم‌های معمول در رمزنگاری [**Error! Bookmark not defined.**]

ردیف	الگوریتم	طول بلوک (بیت)	نوع	طول کلید (بیت)	تعداد رُند	ساختار
۱	DES	۶۴	متقارن	۵۶	۱۶	FN[1] متوازن
۲	Triple DES(3DES)	۶۴	متقارن	۱۶۸،۱۱۲،۵۶	۴۸	FN
۳	Rijndael(AES)	۱۲۸	متقارن	۲۵۶،۱۹۲،۱۲۸	۱۴،۱۲،۱۰	SPN[2]
۴	Serpent	۱۲۸	متقارن	۲۵۶،۱۹۲،۱۲۸	۳۲	SPN
۵	Twofish	۱۲۸	متقارن	۲۵۶،۱۹۲،۱۲۸	۱۶	FN
۶	Blowfish	۶۴	متقارن	۴۴۸،۲۵۶	۱۶	FN
۷	Rc6	۱۲۸	متقارن	۲۵۶،۱۹۲،۱۲۸	۲۰	FN
۸	TEA[3]	۶۴	متقارن	۱۲۸	۳۲	FN
۹	XTEA[4]	۶۴	متقارن	۱۲۸	۶۴	FN
۱۰	IDEA[5]	۶۴	متقارن	۱۲۸	۸.۵	FN
۱۱	MARS	۱۲۸	متقارن	۱۲۸تا۱۰۲۴	۳۲	FN
۱۲	Kasumi[6]	۶۴	متقارن	۱۲۸	۸	SPN
۱۳	SEED[7]	۱۲۸	متقارن	۱۲۸	۱۶	FN تو در تو
۱۴	RSA	نامعلوم	نا متقارن	۱۰۲۴ تا ۲۰۴۸	-	-
۱۵	الگوریتم مبتنی بر خم بیضوی	-	نا متقارن	حداقل ۱۶۰	-	-

هنگامی‌که احراز هویت و یا رمزگذاری بر روی یک پیام انجام شود، نرم‌افزار می‌تواند دستاوردهای سرعت را با همپوشانی اجرای این عملیات به دست آورد. با بهره‌برداری از همبستگی سطح آموزش در عملیات‌های بینابینی عملکرد افزایش می‌یابد. این فرایند به نام تابع عمل[8] خوانده می‌شود [۲۰]. منلی و گرگ سهولت بهینه‌سازی هنگام استفاده از عملکرد GCM را نشان می‌دهند. آن‌ها برنامه‌ای را در نسخه C ارائه می‌دهند که یک الگوریتم رمزنگاری را می‌گیرد و کدی را تولید می‌کند که به‌درستی روی پردازنده هدف کار می‌کند [۲۱]. مد عملیاتی CTR، یک مد عملیاتی نسبتاً پایه است که اجازه دسترسی به یک بلوک تصادفی داده را می‌دهد. یک تابع شمارشی برای تولید یک توالی استفاده می‌شود که نباید خود را برای هر بلوک رمزگذاری شده تحت کلید داده شده تکرار کند. پس‌ازآن، با استفاده از CIPH و تحت کلید K و ایکس اور با متن اصلی برای تولید متن رمز شده، عملیات رمزنگاری انجام می‌شود. حالت CTR مناسب برای جریان داده‌ها از طریق انتقال بدون اتصال است؛ زیرا بلوک‌ها به اطلاعات بلوک‌های دیگر بستگی ندارد. از دست دادن یک بسته پس از کدگشائی بسته‌های دیگر تا زمانی که شمارنده در همزمان سازی نگه داشته شود، تأثیر نمی‌گذارد [۲۲].

۴- پیشینه تحقیق

برخی از حملات همراه با راهکارهای مقابله توسط باچر و همکارانش مطرح گردیده که در قالب جدول ۲. خلاصه شده است. همچنین یک نمای کلی از سیستم‌های ویپ و مسائل مربوط به امنیت آن نیز در این پژوهش، حملات موجود و بالقوه همراه با روش‌هایی که برای مقابله اتخاذ شده‌اند را به بحث گذاشته است که نتایج آن را می‌توان در قالب جدول ۳. بیان کرد [۲۳].

باربری و همکارانش نیز برای تأمین امنیت ویپ، تأثیر IPSec را موردبررسی قرار دادند؛ که نتایج نشان داد پهنای باند مؤثر IPSecدر مقایسه با SRTP در ارتباطات ویپ به میزان۵۰٪کاهش می‌یابد [۲۴].

گوپتا و همکارانش یک بحث ساختاری در مورد امنیت ویپ ارائه کردند که سه جنبه اصلی را هدف قرار می‌دهد: رسانه، سیگنالینگ و مشتق کلید. آن‌ها توصیه کردند که روش مبادله کلید محافظت شده با استفاده از SRTP صورت می‌پذیرد [۲۵]. با توجه به این‌که فناوری ویپ در ارتباط با اتصال اینترنت است و از آن استفاده می‌نماید، مشکلات و مسائل امنیتی در ارتباط با کامپیوتر متصل شده به اینترنت می‌تواند سرویس فوق را تحت تأثیر قرار دهد. مهاجمان ممکن است قادر به انجام فعالیت‌هایی نظیر قطع مکالمه تلفنی، استراق سمع، برنامه‌ریزی و هدایت حملات مبتنی بر مهندسی اجتماعی با بررسی هویت تماس گیرنده و در نهایت از کار انداختن سرویس فوق باشند. فعالیت‌هایی که مستلزم استفاده از حجم بالایی از منابع شبکه است، نظیر دریافت فایل‌های حجیم، بازی‌های آنلاین و استفاده از محتویات چندرسانه‌ای می‌تواند سرویس ویپ را تحت تأثیر قرار دهد. انواع حملات در بستر شبکه و سیستم ویپ به چهار نوع تقسیم شود: حملات علیه دسترسی،

1 Feistel Network(FN)
2 Substitution Permutation Network(SPN)
3 Tiny Encryption Algorithm(TEA)
4 eXtended Tiny Encryption Algorithm(XTEA)
5 International Data Encryption Algorithm(IDEA)
۶ این الگوریتم در سامانه‌های ارتباطات تلفن همراه Gpp ۳ وسامانه‌های UTMS، GSM و GPRS استفاده می شود.
۷ این الگوریتم از سال ۲۰۰۹ توسط مرورگر Mozilla 3.5.4 پشتیبانی شد و هم اکنون در IPSec نیز از این الگوریتم استفاده می‌شود.
8 Action function

محرمانگی، یکپارچگی و زمینه اجتماعی. برخی از حملات شامل حمله پیام‌های بی‌معنی در ویپ[1]، حمله دسته‌های ولگرد[2]، حمله تلفن تقلبی[3]، حمله رد سرویس، حمله پروتکل پیکربندی پویای میزبان[4]، حمله ازدحام ناگهانی[5]، حمله فارمینگ[6] و حمله مرد در میان[7] می‌باشند [۲۶]. برای جلوگیری از این حملات مهم از پروتکل‌های امنیتی متناسب با ویژگی‌های سیستم ویپ استفاده می‌شود.

دو پروتکل IPsec و SRTP عملیات رمزگذاری، احراز هویت و روش‌های یکپارچگی را پشتیبانی می‌کنند. به‌عنوان‌مثال، هر دو پروتکل با استفاده از رمزنگاری کلید عمومی، استاندارد رمزنگاری پیشرفته AES و الگوریتم درهم‌ساز HMAC-SHA1 پشتیبانی را انجام می‌دهند؛ بنابراین، این دو پروتکل تفاوت بسیاری در امنیت با هم ندارند. برای جلوگیری از زمان تنظیم مجدد جلسات بیشتر (از بین رفتن بسته در ابتدای یک جلسه صوتی) ضروری است که کلید رمزگذاری جریان حامل به‌عنوان بخشی از فرایند سیگنالینگ توزیع گردد. IETF با قرار دادن کلید در پروتکل (SDP[8]) پیام SIP، رویکردی را برای توزیع کلید SRTP به‌عنوان بخشی از فرایند سیگنالینگ SIP تعریف نموده است. IETF در این مرحله مکانیزمی برای SDP[9] در توزیع کلید رمز IPsec بیان نکرده است. علاوه بر این، مدل پیشنهادی در RFC 3264 ممکن است از شامل شدن اطلاعات کلیدی IPsec در پیام‌های سیگنالینگ SIP جلوگیری نماید [۲۷]. مزیت اصلی IPsec این است که پیام را در لایه IP رمزگذاری می‌کند و در ستون پروتکل پایین‌تر از TLS که در لایه انتقال رمزگذاری می‌شود، قرار می‌دهد. از آن‌جایی که امنیت در لایه IP ارائه می‌شود، می‌تواند نقطه ضعفی برای سیستم‌های ویپ که پلتفرم‌هایی را به اشتراک می‌گذارند، باشد. نکته دیگر این است که تأخیر در ارتباط با کلید مجدد انجام می‌پذیرد. برخی تحقیقات زمان تولید مجدد کلید یک جلسه TLS و یک جلسه IPsec را مقایسه نموده‌اند و نشان داده‌اند که تولید مجدد کلید جلسه در پروتکل IPsec تقریباً ۲۰ برابر زمان‌برتر از تولید کلید مجدد جلسه در پروتکل TLS (۲۶ میلی‌ثانیه در برابر ۱.۳ میلی‌ثانیه) می‌باشد. این زمان برای تولید یک کلید مجدد، زمان زیادی نیست، اما اگر هزاران ابزار نهایی به‌طور همزمان تلاش کنند تا یک کلید مجدد ایجاد نمایند، ایجاد نارضایتی و وقفه می‌نماید [۲۸. آخرین ملاحظه مربوط به شروع مجدد یک جلسه امن است. SIP با استفاده از TLS نیازمند مبادله حداقل ۶ پیام می‌باشد. SIP با استفاده از بازخورد نشست‌های IPsec عمدتاً با فرآیند کلیدی تبادل اینترنتی IKE همراه است و بستگی دارد که آیا حالت اصلی، پایه یا تهاجمی برای تبادل فاز ۱ استفاده می‌شود. با فرض این‌که حالت اصلی مورد استفاده قرار گیرد، IPsec نیاز به ۹ مبادله پیام دارد. فرض بر این است که یک تأخیر زمانی در یک منطقه تقریباً ۸۵ میلی‌ثانیه است، افزودن ۳ پیام اضافی با تأخیر ۲۵۵ میلی‌ثانیه همراه است. صنعت و جامعه علمی نیز که در حال حاضر به شدت در استانداردهای مرتبط با استفاده از TLS برای تأمین امنیت SIP و SRTP برای امنیت RTP سرمایه‌گذاری کرده‌اند، در حال حاضر در استفاده از IPsec برای محافظت از SIP و RTP سرمایه‌گذاری نکرده است. هر دو پروتکلTLS و IPsec در استاندارد (RFC 3261) SIP به‌عنوان روش امنیت مورد توجه قرار می‌گیرند. بااین‌حال، استاندارد SIP TLS را درصورتی‌که از یک مدل امنیتی hop-by hop استفاده شود را توصیه می‌کند. IPsec در استاندارد SIP وقتی توصیه می‌شود که برنامه از روش امنیتی جدا شده است. علاوه بر این، تعداد پیش‌نویس‌های اینترنتی و RFCهای مربوط به SIP و TLS، RTP و SRTP و نحوه ارتباط پروتکل SIP / TLS با RTP / SRTP به‌طور قابل‌توجهی به استفاده از IPsec برای حفاظت از هر دو SIP و RTP پرداخته‌اند. این نشانه‌ای است که دانشگاه‌ها و صنعت در حال حاضر بیشتر علاقه‌مند به کشف و حل مسائل مربوط به TLS و SRTP برای تأمین VoIP هستند. مزیت اصلی SRTP نسبت به IPsec این است که هدرهای UDP و RTP در معرض پرسنل مدیریت شبکه برای حل مشکلات مرتبط با شبکه هستند. IPsec این هدرها را رمزگذاری می‌کند که این اطلاعات را به‌عنوان یک منبع عیب‌یابی حذف می‌کند. سازوکار اصلی برای نگاه کردن به این تبعیض کننده یک ابزار اسنیفر[10] بسته است که عمدتاً برای اطمینان از اینکه بسته برای جلسه مناسب طراحی شده است استفاده می‌شود. این یک ابزار مفید است اما ممکن است در انتخاب SRTP بیش از IPsec نباشید. از منظر مدیریت شبکه، IPsec و TLS قابل مقایسه هستند [۲۹].

1 Spam
2 Rogue Sets
3 Toll Fraud
4 Dynamic Host Configuration protocol
5 Flash Crowd
6 Pharming
7 Man in The Middle
8 Session Description Protocol(SDP)
9 Session Description Protocol

10 sniffer

جدول (۲): چالش‌های ویپ و راهکارهای مقابله [**Error! Bookmark not defined.**]

چالش/حمله/تهدید/آسیب/رخنه	راهکار مقابله
حمله به لایه‌ی فیزیکی	جلوگیری از دسترسی افراد غیرمجاز به تجهیزات، سامانه‌ها و بسترهای فیزیکی شبکه
ارسال بسته‌های جعلی ARP[1] عبور ترافیک شبکه از ماشین شخص مهاجم برای دستیابی به اطلاعات	دای (بازرسی پویای آرپ)
کلاه‌برداری از طریق جعل مک آدرس تکراری	احراز هویت هنگام اتصال به درگاه شبکه
کلاه‌برداری از طریق جعل آدرس IP	جلوگیری مسیریاب از بسته‌هائی که آدرس مبدأ آن‌ها در محدوده‌ی دامنه‌ی محلی قرار ندارد. ممانعت مسیریاب از خروج بسته‌هائی که آدرس مبدأ آن‌ها در محدوده‌ی دامنه‌ی محلی قرار ندارد.
ارسال بسته‌های ناقص	جلوگیری توسط دیواره‌ی آتش
تسخیر تمام فضای بافرگره‌ی مورد حمله	پیکربندی دیواره‌ی آتش استفاده ازSYN-ACK قبل از تخصیص میان‌گیر (بافر)
دریافت و بازپخش غیر مجاز داده و صوت	به رمز در آوردن نشست‌ها با یک شماره توالی منحصربه‌فرد
ایجاد یک سرور TFTP[2] ساختگی	TLS[3] با استفاده از SSL[4]
تخلیه‌ی مخزن IP آدرس‌های DHCP با ارسال سیل‌آسای مک آدرس‌های تصادفی برای آن	IEEE 802.1x
حمله به یک گره با ارسال حجم زیادی از بسته‌های ICMP[5]	تنظیم مسیریاب برای ممانعت از بسته‌های بزرگ یا غیرضروری ICMP قرار دادن سیستم وُیپ در «LAN/VLAN» جداگانه مجهز به دیواره‌ی آتش
حمله با هدف سر ریز شدن بافر تجهیزات ویپ	استفاده از گره‌هائی با سیستم‌عامل یکسان با وصله‌های بروز
حمله به سیستم‌عامل میزبان تجهیزات ویپ	استفاده از آخرین وصله‌های ارائه شده توسط فروشنده
ویروس‌ها و نرم‌افزارهای مخرب	استفاده از ضد ویروس به روز در تمام گره‌ها
حمله به پایگاه ثبت داده‌ی تماس‌ها	جدا کردن ترافیک سیگنالینگ از پایگاه داده با قرار دادن آنها روی LAN/VLANهای جداگانه

1 Address Resolution Protocol(ARP)
2 Trivial File Transfer Protocol(TFTP)
3 Transport Layer Security(TLS)
4 Secure Sockets Layer(SSL)
5 Internet Control Message Protocol(ICMP)

جدول (۳): حملات موجود و بالقوه همراه با روش‌هائی که برای مقابله [**Error! Bookmark not defined.**]

چالش/حمله/تهدید آسیب/رخنه	راهکار مقابله	نقاط قوت و ضعف/ملاحظات
حمله به سیگنالینگ	H.235 S/MIME IPSec[6]	H.235 برای پشتیبانی از SRTP S/MIME برای پشتیبانی از SIP و SMTP[7] IPSec برای پشتیبانی از UDP و TCP[8] و SIP و RTP
حمله به قرارداد انتقال صوت	SRTP & SRTCP	ملاحظه ای یافت نشد
حمله به کاربردهای چندرسانه‌ای اینترنت مانند ویپ	MIKEY & ZRTP قراردادهای تفاهم کلید رمز	برای پشتیبانی از SRTP مستقل از سیگنالینگ از تماس‌هائی که بین شبکه‌ی VoIP و PSTN منتقل می‌شود پشتیبانی نمی‌کنند
داس ایجاد وقفه در ارائه خدمات	نظارت و جداسازی: نظارت بر کاربران مشکوک و جداسازی آنان از کاربران مشروع احراز هویت: بررسی هویت کاربر قبل از ارسال پیام او پروکسی: برای انجام سایر کنترل‌های امنیتی مانند تصدیق هویت کاربران، ثبت نام شخص ثالث و جداسازی منابع انتشار پیام‌های هرز طراحی سروری: به‌عنوان خط اول مقابله با حمله قبل از رسیدن آن به کلاینت	ملاحظه ای یافت نشد
استراق سمع	بکارگیری سخت‌افزار بی عیب و نقص اطمینان از اینکه دسترسی به بسترهای کابلی تنها به افراد مجاز محدود می‌شود پیاده‌سازی امنیت مبتنی بر مک آدرس پورت پایش منظم شبکه برای تشخیص دستگاه‌هائی که در شبکه به‌طور بی‌قاعده فعال‌اند.	ملاحظه ای یافت نشد
تغییر ظاهر	ترکیب احراز هویت و رمزنگاری	ملاحظه ای یافت نشد
تقلب در هزینه‌ی تماس	پیکربندی صحیح فایروال‌ها و محافظت پورت‌ها	ملاحظه ای یافت نشد
تماس‌ها و پیام‌های	استفاده از پازل‌های رمزنگاری	ایجاد تأخیر نامطلوب

6 Iternet Protocol security
7 Simple Mail Transfer Protocol(SMP)
8 Transmission Control Protocol(TCP)

ناخواسته		

۵- روش شناسی

ازآنجایی‌که تحقیق حاضر به دنبال ارائه راهکاری برای بهبود کارایی مکالمات رمزنگاری شده مبتنی بر ویپ می‌باشد، پژوهش ازنظر هدف کاربردی و به روش شبیه‌سازی اجرا شده است. ابزار مورد استفاده شبیه‌ساز NS2[1] و نسخه NS2.35 می‌باشد که تحت لینوکس و کد متن‌باز می‌باشد. این شبیه‌ساز با توسعه‌هایی که بر روی آن اضافه می‌شود توانایی شبیه‌سازی شبکه‌های جدید را دارا می‌باشد.

از شبیه سازها دیگری که برای شبیه سازی شبکه VOIP قابل استفاده می‌باشد، می‌توان به نرم‌افزارهای متلب[2]، OPNET و NS3 و استریسک[3] اشاره کرد. شبیه‌ساز NS2 مبتنی بر دو زبان برنامه‌سازی می‌باشد. ۱- TCL و ۲-C++ زبان C++ در شبیه‌ساز NS2، با ابزارها و کتابخانه‌های متعددی که اختیار برنامه‌نویس می‌گذارد، توان تعریف و استفاده از راهکارهای زیستی و هوش مصنوعی و پروتکل‌های مختلف شبکه را برای شبیه‌سازی امکان‌پذیر می‌کند. با استفاده از این زبان می‌توان پروتکل‌های جدیدی با قدرت بالا تعریف نمود. زبان برنامه‌سازی TCL به‌منظور تعریف توپولوژی شبکه و استفاده از پروتکل‌های تعریف شده می‌باشد. یکی از مهم‌ترین ویژگی‌های شبیه‌ساز NS2، متن‌باز بودن آن می‌باشد که در شبیه سازهای دیگر امکان تغییر و ایجاد پروتکل های جدید وجود ندارد. به‌منظور شبیه‌سازی و استفاده از راهکارهای پیشنهادی از دو پروتکل جدید با زبان C++ استفاده شده است؛ که این پروتکل‌ها وظیفه ایجاد شبکه VOIP[4]، پروتکل SRTP و رمزنگاری AES-GCM را در شبیه‌ساز NS2 فراهم می‌سازد.

۶- تجزیه‌وتحلیل

در این بخش لازم است قبل از شبیه‌سازی، ویژگی‌ها و ملاحظات امنیتی پروتکل SRTP زمانی که از الگوریتم AES-GCM استفاده‌ی شود، تشریح گردد. در رمزنگاری، مدهای کاری رویه‌هایی هستند که استفاده مکرر و امن از رمزگذاری بلوکی تحت یک تک کلید را ممکن می‌سازند. وقتی‌که یک پیغام با طول متغیر به سمت هدف ارسال می‌شود، داده ابتدا باید به بلوک‌های مجزای رمزگذاری تقسیم شود. معمولاً، آخرین بلوک باید با استفاده از طرح افزونگی بسط داده شود تا به‌اندازه طول بلوک رمزگذاری برسد. یک مد کاری، رمزگذاری هرکدام از این بلوک‌ها را توضیح می‌دهد و به‌طورکلی از تصادفی‌سازی استفاده می‌کند که برای انجام کاملاً امن این کار، مبتنی بر یک ارزش ورودی افزوده که معمولاً بردار اولیه خوانده می‌شود، می‌باشد.

در SRTP، یک کلید اصلی برای حفاظت از بسته‌های SRTP استفاده می‌شود. کلیدهای جلسه برای رمزگذاری و احراز هویت از این کلید اصلی استخراج می‌شوند. همان کلید اصلی ممکن است برای حفاظت از بسته‌های SRTCP نیز استفاده شود؛ اما کلیدهای جلسه برای بسته‌های SRTCP به‌طور جداگانه مشتق می‌شوند. AES در مد عملیاتی CTR رایج است. همچنین امکان اضافه کردن موارد جدید به این لیست پیش‌فرض پس از مشخصه ذکر شده در SRTP وجود دارد. علاوه بر این، یک تبدیل رمزنگاری معتبر وجود دارد که AES در حالت Galois / Counter (GCM) است.

تمام بسته‌های SRTP باید هم احراز هویت و هم رمزگذاری شوند. فیلدهای داده در بسته‌های RTP به داده‌های اضافی، متن اصلی و داده‌های خام تقسیم می‌شوند.

داده‌های اضافی، (که فقط باید احراز هویت شود): نسخه V (۲ بیت)، پرچم پدینگ P (۱ بیت)، پسوند فرمت X (۱ بیت)، CSRC Count CC (۴ بیت)، نشانگر M (۱ بیت)، نوع پی‌لود از نوع PT (۷ بیت)، شماره توالی (۱۶ بیت)، مهر زمانی (۳۲ بیت)، SSRC (۳۲ بیت)، شناسه منبع، اختیاری، (CSRCs، ۳۲ بیت هرکدام) و پسوند RTP، اختیاری، (طول متغیر).

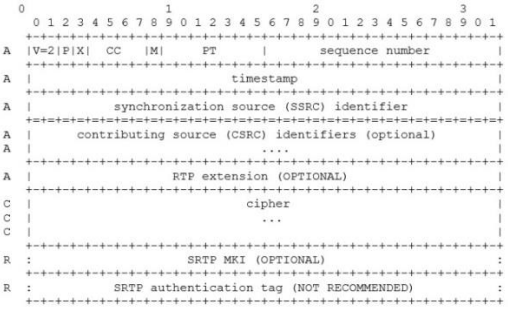
متن اصلی، (که باید رمز و احراز هویت شود): RTP payload (طول متغیر)، RTP padding (اگر استفاده شود، طول متغیر) و تعداد پد RTP (اگر استفاده شود، ۱ اکتایی).

داده‌های خام: طول متغیرهای SRTP MKI و برچسب احراز هویت SRTP.

1 Network Simulator 2
2 MATLAB
3 asterisk
4 Voice over Internet Protocol

از آن‌جایی که متن رمزنگاری AEAD بزرگ‌تر از متن اصلی یا دقیقاً طول برچسب احراز هویت AEAD است، بسته‌های رمزگذاری شده SRTP توسط یک فیلد بزرگ‌تر که حاوی متن رمز شده است، جایگزین فیلد متن اصلی می‌شوند. حتی اگر فیلد متن اصلی خالی باشد، رمزگذاری AEAD همچنان باید انجام شود، درحالی‌که متن رمز شده خروجی تنها از برچسب احراز هویت تشکیل شده است. این برچسب باید بلافاصله قبل از طول متغیر SRTP MKI و برچسب احراز هویت SRTP قرار گیرد. ساختار معرفی شده در شکل (۴) ساختار یک بسته SRTP را بعد از رمزنگاری احراز هویت شده نشان می‌دهد.

یکپارچگی و احراز هویت بسته RTP تأیید می‌شود که برچسب احراز هویت در بسته SRTP حمل می‌شود. با استفاده از الگوریتم هش SRTP از پیش تعیین شده، HMAC-SHA1، برچسب احراز هویت تولید می‌شود. اگر AES-GCM استفاده شود، برچسب احراز هویت به یک ویژگی امنیتی اضافی تبدیل می‌شود و از آن اجتناب می‌شود. علاوه بر این، هنگامی که AES-GCM به‌عنوان بخشی از پروفایل حفاظت SRTP انتخاب می‌شود کلید احراز هویت جلسه استفاده نمی‌شود.



C = متن رمزشده که هم رمزشده و هم احراز هویت شده است

A = داده اضافی که فقط احراز هویت شده است

R = نه رمزشده و نه احراز هویت شده است که بعد از رمزنگاری احراز هویت شده اضافه می‌شود

شکل (۴): ساختار یک بسته SRTP بعد از رمزنگاری احراز هویت شده.

بعد از ارائه ساختار SRTP با استفاده از الگوریتم AES-GCM و بیان ویژگی‌های آن، باید به یک نکته مهم نیز توجه کنیم. در حقیقت برای جلوگیری از استفاده مجدد از بردار مقداردهی اولیه، ما باید اطمینان حاصل کنیم که ROC SEQ، SSRC هرگز دو بار با همان کلید اصلی استفاده نشوند. دو مرحله برای این موضوع وجود دارد.

۱- مدیریت شمارش: یک فرآیند بازسازی کلید باید انجام شود تا یک کلید اصلی جدید را قبل از سیکل‌های جفت ROC، SEQ که به مقدار اصلی برمی‌گردند را تولید کند. توجه داشته باشید که به‌طور ضمنی فرض می‌شود که یا فرایند خروجی RTP این اطمینان را می‌دهد که یک مقدار (ROC، SEQ)، تکرار نمی‌شود یا اینکه فرایند رمزگذاری این اطمینان را می‌دهد که اعداد SEQ و ROC بسته‌های ارائه شده، همیشه در حال افزایش در مد مناسب هستند.

این امر برای GCM بسیار مهم است زیرا دو بار استفاده از (ROC، SEQ) یکسان، سازوکار احراز هویت را به خطر می‌اندازد. برای GCM، مقادیر (ROC، SEQ) و SSRC شود، باید توسط پیاده‌سازی SRTP یا توسط یک ماژول (مثلاً برنامه RTP) تولید یا بررسی شود که می‌تواند به‌عنوان پیاده‌سازی SRTP مورد اعتماد قرار گیرد یا نه.

۲- مدیریت SSRC: برای یک کلید اصلی داده شده، مجموعه‌ای از تمام مقادیر SSRC که با کلید اصلی مورد استفاده قرار می‌گیرند باید به دسته‌های غیر مجزا تقسیم شوند، یک فضا برای هر نقطه انتهایی با استفاده از کلید اصلی برای تولید داده‌های خروجی در نظر گرفته شده است.

هرکدام از این نقاط پایانی باید تنها مقادیر SSRC که به آن‌ها اختصاص داده شده از آن فضا را صادر کنند. علاوه بر این، هر نقطه انتهایی باید تاریخچه شناسه‌های SSRC خروجی را که در طول عمر کلید اصلی فعلی صادر کرده است را حفظ کند و هنگامی که یک منبع همگام‌سازی جدید یک شناسه SSRC را درخواست می‌کند، نباید یک شناسه‌ای که قبلاً صادر شده است را بدهد.

علاوه بر این، هویت سازنده مقادیر SSRC باید تأیید شود و یکپارچگی سیگنال SSRC بایستی حفظ شود.

بنابراین، AES-GCM از حالت AES counter برای رمزگذاری و کد Authentication Message Gaois (GMAC) برای احراز هویت استفاده می‌کند. اعضای زیر خانواده AES-GCM ممکن است با SRTP / SRTCP مورد استفاده قرار گیرند:

جدول (۴): الگوریتم‌های AES-GCM برای SRTP

نام	طول کلید	اندازه برچسب AEAD
AEAD_AES_128_GCM	16 octets	16 octets
AEAD_AES_256_GCM	32 octets	16 octets

۷- ملاحظات امنیتی

بسیاری از این توصیه‌ها برای تمام الگوریتم‌های رمزنگاری SRTP وجود دارند، اما مهم‌ترین آن‌ها شامل موارد ذیل می‌باشد:

- اگر مقدار salt اصلی باید مخفی نگه داشته شود، باید زمانی که دیگر مورد نیاز نیست به‌درستی پاک شود.

- کلید اصلی مخفی و کلیدهای حاصل از آن باید مخفی نگه داشته شود. همه کلیدها باید زمانی که دیگر مورد نیاز نیست، به‌درستی پاک شوند.

- در ابتدای هر بسته، شماره بلوک باید مجدد به یک تنظیم شود. شمارنده بلوک بعد از هر کلید بلوک که تولید می‌شود، افزایش می‌یابد اما نباید اجازه داده شود تا بیش از ۱- ^{32} ۲ برای شروع هر بسته شود. وضوح بردار مقداردهی اولیه توسط فهرست / SSRC ROC / SEQ یا SRTCP تضمین می‌شود.

- هر بار که بازسازی کلید رخ می‌دهد، مقادیر اولیه هر دو شاخص SRTCP ۳۱ بیتی و شاخص بسته SRTP ۴۸ بیتی (ROC || SEQ) باید برای جلوگیری از استفاده مجدد از بردار مقداردهی اولیه ذخیره شود.

- اگر شاخص SRTCP ۳۱ بیتی یا شاخص بسته SEQ || ROC ۴۸ بیتی به ارزش اولیه آن بازگردد، پردازش باید متوقف شود. پردازش تا زمانی که یک SRTP / SRTCP جدید با استفاده از کلید اصلی SRTP جدید ایجاد نشده است، لازم است ادامه یابد.

-لازم است تا برچسب احراز هویت AEAD به ۱۶ اکتاو برسد که به‌طور مؤثر خطر یک دشمن که با موفقیت داده‌های جعلی را تولید کرده، از بین رود.

۸- شبیه‌سازی

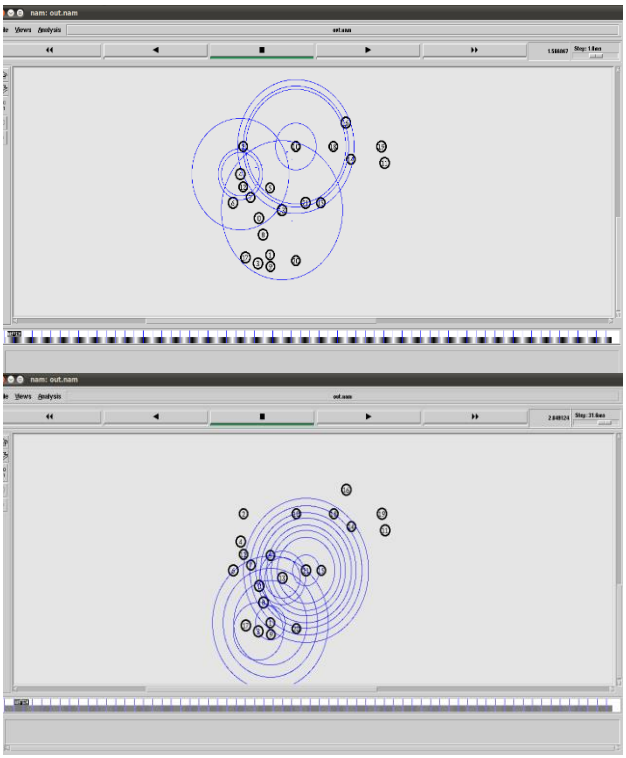
با توجه به اینکه برای شبیه‌سازی شبکه VOIP و پروتکل SRTP، ابزارهای متنوعی برای پیاده‌سازی یا شبیه‌سازی وجود دارد، به‌منظور شبیه‌سازی راهکار پیشنهادی این تحقیق، با یکی از قدرتمندترین این ابزارها برای شبیه‌سازی این شبکه که شبیه‌ساز NS2 نام دارد استفاده کردیم. پارامترها و مقادیر شبیه‌سازی در جدول (۵) نشان داده شده است.

جدول (۵): پارامترها و مقادیر شبیه‌سازی

Parameter	Value
Simulation time	**100 Sec**
Area	**2000 × 2000**
Number of Nodes	**22**
Transport layer protocol	**TCP**
Routing protocol	**AODV**
Antenna type	**Omni antenna**
Network interface	**Phy/WirelessPhy**
MAC interface	**802.11**
Extended Protocol	**VOIP**

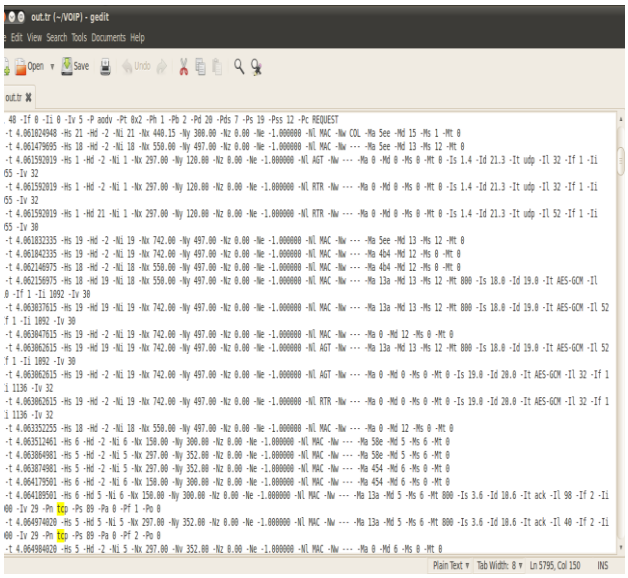
در جدول (۵) پارامترهای شبیه‌سازی راهکار پیشنهادی مشاهده می‌شود. مدل آنتن استفاده شده Omni-antenna می‌باشد. به آنتن‌های میله‌ای شکلی که تشعشات آن‌ها در تمام جهت‌ها منتشر می‌شود، آنتن‌های Omni-Directional یا همه طرفه می‌گویند، آنتن‌های دوقطبی یا Dipole یک نوع آنتن Omni-Directional هستند. پروتکل استفاده شده در لایه انتقال TCP می‌باشد. این پروتکل در انتقالات اتصال گرا استفاده می‌شود درحالی‌که پروتکل بدون اتصال UDP برای انتقالات پیام ساده مورد استفاده قرار می‌گیرد. TCP پروتکل پیچیده‌تری است و این پیچیدگی به‌واسطه طراحی وضعیت محوری است که در سرویس‌های انتقالات قابل‌اطمینان و جریان داده تعبیه شده است. در این شبیه‌سازی رابط لایه ۸۰۲.۱۱MAC می‌باشد که برای استفاده از شبکه محلی بی‌سیم در باند فرکانسی ۴/۲، ۶/۳ و ۵ گیگاهرتز مورد استفاده قرار می‌گیرد. در شبیه‌سازی NS2 زیر برنامه‌ای به نام NAM یا Network Animator وجود دارد که با استفاده از آن می‌توان شکل بصری و واقعی نودهای شبکه و نحوه ارسال اطلاعات آن‌ها را مشاهده نمود. پس از اجرای شبیه سازی، دو نوع خروجی می‌توان مشاهده نمود. خروجی NAM و خروجی TR. خروجی NAM وظیفه نمایش گرافیکی خروجی و خروجی TR که یک فایل متنی می‌باشد که وابسته به تعداد نودها، میزان ارسال اطلاعات و مدت‌زمان شبیه‌سازی حجم و طول آن متغیر می‌باشد. از این فایل TR به‌منظور دریافت و بررسی خروجی‌های شبیه‌سازی مانند مصرف انرژی، تأخیر، گذردهی یا توان عملیاتی، نرخ تحویل بسته، زمان مصرفی برای رمزنگاری و کدگشائی و... می‌توان استفاده نمود. در تحقیق جاری با توجه به رمزنگاری انجام شده علاوه بر فاکتورهای تأخیر، نرخ تحویل بسته و بسته‌های ازدست‌رفته، میزان زمان مصرفی را در فاکتورهای رمزنگاری، کدگشائی، ارسال و دریافت پیام مورد ارزیابی و مقایسه قرار داده شده است. با توجه به سناریوی موجود در شکل (۵) خروجی‌های بدست آمده استخراج و مورد ارزیابی و مقایسه قرار گرفته است. به‌منظور مقایسه و ارزیابی راهکار پیشنهادی از رمزنگاری AES-CTR استفاده شده است.

شکل (۵) نحوه استقرار گره‌ها در شبکه و چگونگی ارسال داده در شبکه VOIP بی‌سیم را بیان می‌کند. همان‌طور که در شکل (۵) مشخص می‌باشد گره‌ها در حال ارسال داده به یکدیگر می‌باشند. در این شبکه چند نوع داده در حال ارسال می‌باشد که تحت شبکه VOIP می‌باشند. دایره‌های آبی نمایان شده در شکل (۵) نشان دهنده شعاع ارسال گره‌ها در هنگام ارسال و دریافت داده می‌باشد. همان‌طور که در پارامترهای شبیه‌سازی در جدول (۵) ذکر شده است مدت شبیه‌سازی ۱۰۰ ثانیه خواهد بود که در نوار زیرین شکل (۵) مشخص است و پس از پایان ۱۰۰ ثانیه شبیه‌سازی متوقف می‌گردد.



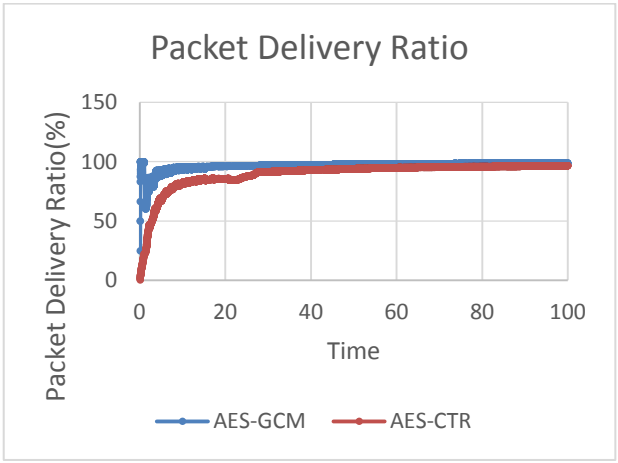
شکل (۵): خروج NAM شبکه و راهکار پیشنهادی

شکل (۶) خروجی شبیه‌ساز را در حالت فایل TR نشان می‌دهد. این فایل شامل تمامی رویدادهای اتفاق افتاده در شبیه‌سازی می‌باشد. در این خروجی می‌توان تمامی بسته‌های ارسال و دریافت شده، نوع مسیریابی، زمان ارسال و دریافت و ... مشاهده نمود. در شکل (۶) می‌توان بسته‌های ارسالی در شبکه VOIP بی‌سیم راهکار پیشنهادی را مشاهده نمود. در این راهکار ۳ بسته ارسالی مختص راهکار پیشنهادی وجود دارد. ابتدا برای برقراری اتصال ایمن بین گره‌ها بسته‌های رمزنگاری در شبکه ارسال می‌شوند که در شکل (۶) با AES-GCM مشخص شده است. در ادامه بسته‌های UDP که در شبکه وظیفه ارسال داده‌های VOIP که فایل‌های voice و چندرسانه‌ای می‌باشند ارسال می‌گردد و برای ارسال داده‌های دیگر در شبکه بی‌سیم از پروتکل TCP استفاده شده است که در شکل (۶) با بسته‌های TCP مشخص شده است. مقایسه و بررسی دو پروتکل رمزنگاری AES-GCM و AES-CTR در قالب نمودارها و ارقام به شرح ذیل می‌باشد.



شکل (۶): رویدادهای فایل **TR**

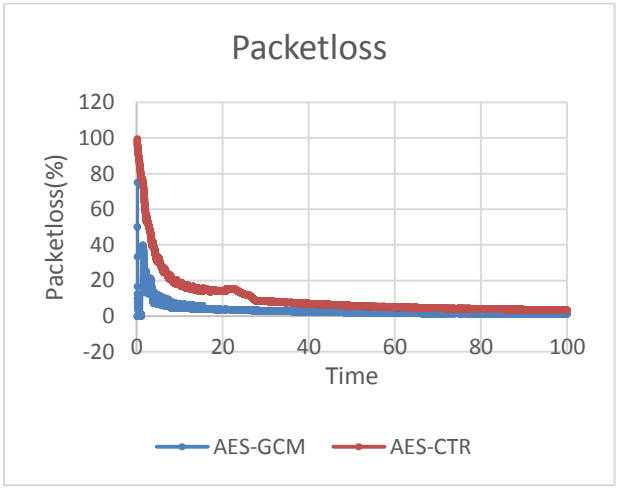
شکل (۷) نرخ تحویل بسته را در هر دو مد عملیاتی نشان می‌دهد. در شبکه نرخ تحویل بسته، تعداد بسته هایی ارسالی موفق به ازای تعداد کل بسته هایی که توسط منبع به شبکه نمایان است و با افزایش زمان، نرخ تحویل بسته‌ها افزایش می‌یابد. همان‌طور که شکل (۷) نمایان است رمزنگاری AES-CTR روند نسبتاً ثابت‌تری را در مقابل رمزنگاری AES-GCM طی می‌کند ولی نرخ تحویل بسته در راهکار پیشنهادی این تحقیق که مبتنی بر رمزنگاری AES-GCM می‌باشد از نرخ تحویل بسته بهتری برخودار می‌باشد. نرخ تحویل بسته رابطه مستقیمی با نرخ از دست رفتن بسته‌ها در شبکه دارد. درصورتی‌که سرعت رمزنگاری پایین باشد، به‌سرعت بافر گره‌ها پر شده و بسته‌ها دور ریخته خواهند شد که در نهایت باعث کاهش نرخ تحویل بسته می‌شود.



شکل (۷): نرخ تحویل بسته

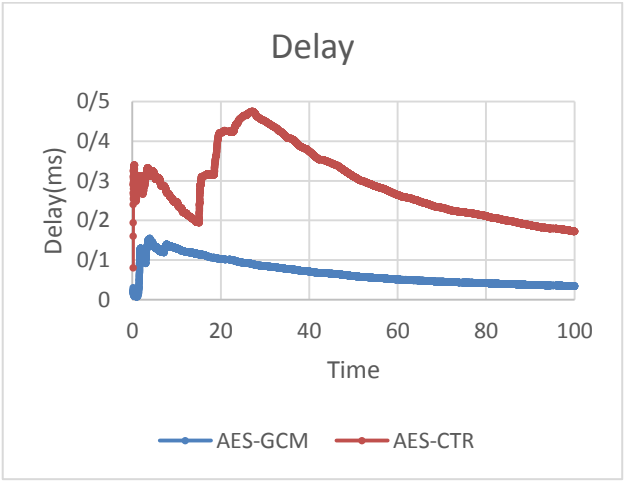
شکل (۸) نرخ از دست رفتن بسته‌ها یا حذف شدن بسته‌ها را در مد عملیاتیAES-CTR و مد عملیاتی پیشنهادی نشان می‌دهد. حذف

شدن بسته‌ها در طول عملیات مسیریابی و رمزنگاری، PacketLoss نامیده می‌شود. حذف بسته‌ها می‌تواند دلایل مختلفی داشته باشد. مثلاً اگر طول صف از حد آستانه بزرگ‌تر باشد. پر بودن حافظه صف گیرنده نیز می‌تواند باعث حذف شدن بسته شود. در بعضی مواقع ارسال خراب بسته‌ها از طرف روتر باعث حذف شدن بسته‌ها می‌گردد که باعث می‌شود مقصد درخواست ارسال مجدد اطلاعات را بدهد که این کار نیز باعث افزایش ترافیک و میزان تأخیر در شبکه می شود. همان‌طور که اشاره شد دلایل مختلفی بر نرخ از دست رفتن بسته‌ها در شبکه تأثیر می‌گذارند که در صورت از دست رفتن بسته‌ها پارامترهای دیگری نیز مانند نرخ تحویل بسته و گذردهی آسیب خواهند دید. همان‌طور که در مقایسه صورت پذیرفته مشاهده می‌شود راهکار رمزنگاری AES-GCM عملکرد بهتری در جلوگیری و مقابله با از دست رفتن بسته‌ها نشان می‌دهد.



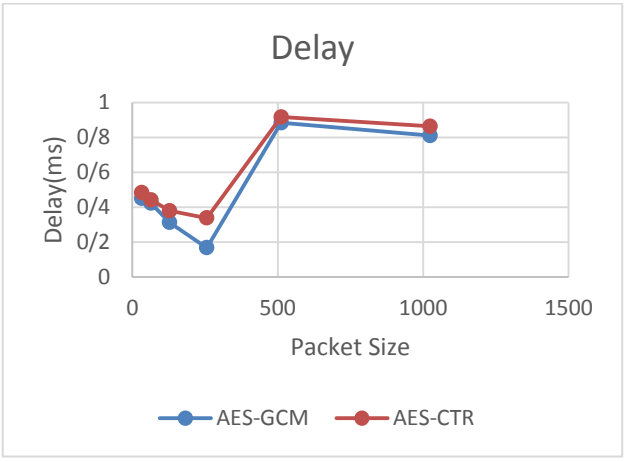
شکل (۸): نرخ از دست رفتن بسته

شکل (۹) میزان تأخیر را با توجه به زمان نشان می‌دهد. تأخیر به معنای مدت‌زمانی است یک مقدار داده در شبکه انتقال می‌یابد. فاکتورهای متعددی بر تأخیر انتقال تأثیرگذار می‌باشند؛ مانند پنهای باند، تداخل و ...همان طور که مشخص است، با افزایش زمان در روند تأخیر در شبکه تغییر ایجاد می‌شود. در ابتدا، با افزایش زمان میزان تأخیر نیز افزایش می‌یابد که در ادامه با افزایش زمان میزان تأخیر نسبتاً کاهش می‌یابد. تأخیر نیز رابطه مستقیمی با میزان تحویل بسته و گذردهی در شبکه دارد. با توجه به رمزنگاری مقایسه شده در شکل (۹)، راهکاری که میزان تأخیر کمتری را برای رمزنگاری و کدگشائی صرف کند می‌تواند تأثیر قابل‌توجهی در فاکتورهای دیگر داشته باشد. همان‌طور که در شکل (۹) به‌وضوح مشخص می‌باشد راهکار رمزنگاری AES-GCM به‌طور قابل ملاحظه‌ای تأخیر کمتری در ارسال بسته‌ها دارد. پس این مقدار تأخیر می‌تواند در فاکتورهای دیگری که ذکر شده تأثیرگذار باشد.



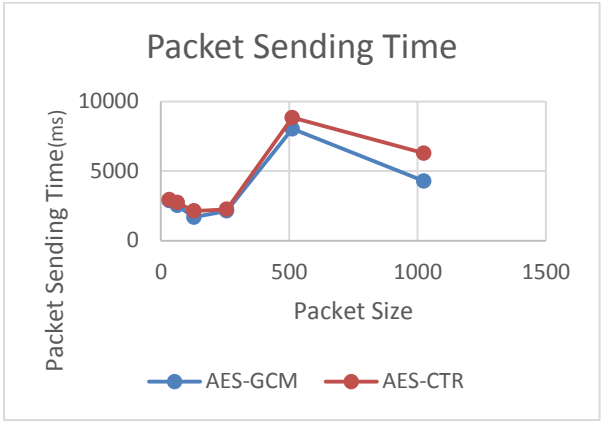
شکل (۹): تأخیر انتقال بسته

شکل (۱۰) میزان تأخیر را نسبت به‌اندازه بسته در شبکه نشان می‌دهد. به‌منظور مقایسه بهتر، علاوه بر زمان از فاکتور دیگری استفاده نمودیم. بدین منظور راهکار پیشنهادی در بسته‌های مختلف مورد ارزیابی و مقایسه قرار دادیم. بسته‌ها از ۳۲ تا ۱۰۲۴ بایت می‌باشد. میزان تأخیر ایجاد نیز برحسب میلی‌ثانیه می‌باشد. در قسمت قبل توضیح داده شده که تأخیر تأثیر قابل‌توجهی در خروجی‌های دیگر دارد. شکل (۱۰) نشان می‌دهد تأخیر با افزایش اندازه بسته‌ها، تغییر ثابتی در شبکه ندارد. تا ۲۵۶ بایت میزان تأخیر کاهشی می‌باشد و در ادامه با افزایش اندازه بسته تأخیر افزایش می‌یابد.



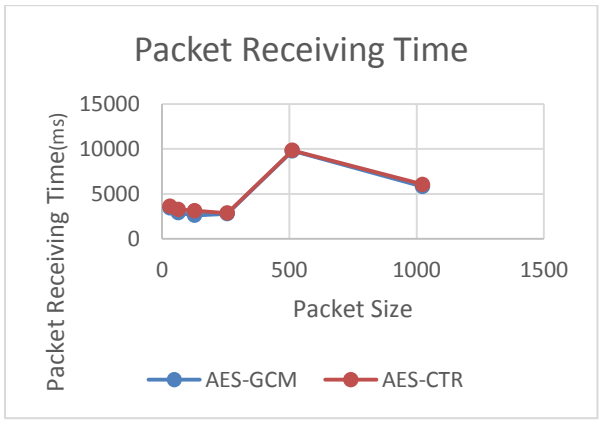
شکل (۱۰): تأخیر انتقال بسته

شکل (۱۱) زمان مصرفی برای ارسال بسته‌ها را به میلی‌ثانیه را نشان می‌دهد. این زمان رابطه مستقیمی با رمزنگاری بسته‌ها در شبکه دارد. هرچه میزان سرعت رمزنگاری پروتکل بیشتر باشد این مقدار کاهش می‌یابد. همان‌طور که مشخص است این زمان در ابتدا کاهش می‌یابد و با افزایش بسته افزایش می‌یابد.



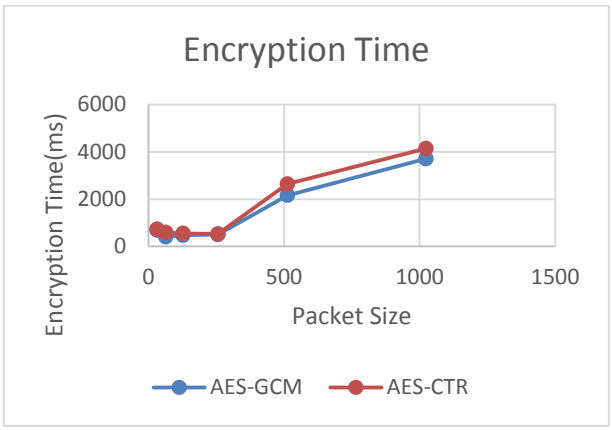
شکل (۱۱): میزان زمان مصرفی برای ارسال بسته

شکل (۱۲) زمان مصرفی برای دریافت داده به میلی‌ثانیه را نشان می‌دهد. این زمان رابطه مستقیمی با کدگشائی بسته‌ها در شبکه دارد. هرچه میزان سرعت کدگشائی پروتکل بیشتر باشد این مقدار کاهش می‌یابد. همان‌طور که مشخص است، این زمان در ابتدا کاهش می‌یابد و با افزایش بسته افزایش می‌یابد.



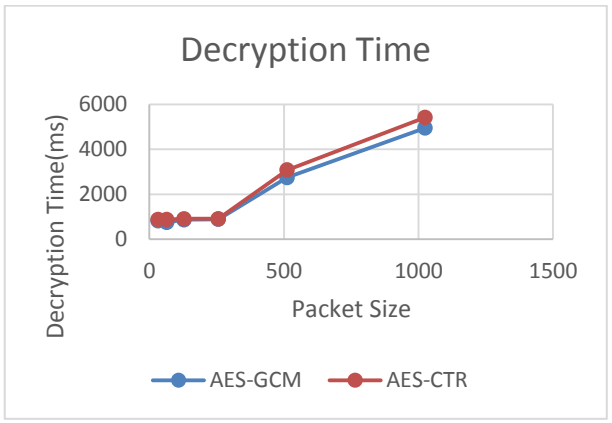
شکل (۱۲): میزان زمان مصرفی برای دریافت داده

شکل (۱۳) زمان مصرفی برای رمزنگاری بسته‌ها در شبکه راهکار پیشنهادی با رمزنگارAES-GCM و AES-CTR را نشان می‌دهد. همان‌طور که مشخص است، با افزایش اندازه بسته‌ها این زمان نیز افزایش می‌یابد. راهکار پیشنهادی نشان می‌دهد که زمان کمتری را صرف رمزنگاری می‌کند و همین عامل تأثیر مثبتی بر فاکتورهای دیگر شبکه دارد. به‌عنوان‌مثال تأثیر قابل‌توجهی بر تأخیر و زمان ارسال دارد که این عامل تأثیر مستقیمی با میزان نرخ تحویل بسته در شبکه دارد.



شکل (۱۳): زمان مصرفی برای رمزنگاری

شکل (۱۴) زمان مصرفی برای کدگشائی بسته‌ها در شبکه راهکار پیشنهادی با رمزنگاری AES-GCM و AES-CTR را نشان می‌دهد. همان‌طور که مشخص است، با افزایش اندازه بسته‌ها این زمان نیز افزایش می‌یابد. راهکار پیشنهادی نشان می‌دهد که زمان کمتری را صرف کدگشائی می‌کند و همین عامل تأثیر مثبتی بر دریافت بسته‌ها دارد.



شکل (۱۴): زمان مصرفی برای کدگشائی

۹- نتیجه‌گیری

راهکار پیشنهادی این تحقیق مبتنی بر رمزنگاری AES-GCM با AES-CTR در پارامترهای مختلف شبکه با دو فاکتور زمان و اندازه بسته مقایسه شد. نتایج مقایسه حاکی از عملکرد خوب و مناسب راهکار پیشنهادی این تحقیق می‌باشد. فناوری ویپ، از زیرساخت و قراردادهای شبکه‌های اینترنتی برای انتقال بی‌درنگ بسته‌های صوتی (نسبت به دیگر انواع بسته‌های داده) استفاده می‌کند. استفاده از این زیرساخت باعث بهره‌مندی از ضریب نفوذ و گسترش خوب این دست شبکه‌ها می‌شود و از ایجاد شبکه‌ی زیرساخت مجزا برای انجام وظایف خود اجتناب می‌نماید. این فناوری می‌خواهد از خود در جابجایی و ارائه خدمات چندرسانه‌ای به کاربران در اقصی‌نقاط شبکه‌ی داده انعطاف بیشتری نشان دهد. از سویی دیگر، به ارث

بردن مشکلات و تهدیدات مرسوم در شبکه‌های داده با چالش‌های خاصی مواجه است که متوجه قراردادهای سیگنالینگ و انتقال رسانه و همچنین تجهیزات و پایانه‌های خاص وُیپ می‌باشد. در این تحقیق سعی شده مجموعه‌ی جامعی از مشکلات و حملات چالش‌برانگیز در عملکرد سیستم‌های وُیپ که در مطالعات سنوات گذشته موردبررسی و اشاره قرار گرفته و برای آن‌ها راهکارهای ارائه گردیده، شناسایی و طبق جداول دسته‌بندی گردد.

تحقیقات نشان می‌دهد برای برقراری امنیت در ارتباطات VOIP می‌توان از سه پروتکل امنیتیIPSec و TLS و SRTP استفاده نمود. لذا این تحقیق بر اساس مقایسه مقدماتی ما بین استفاده از IPsecدر مقابل TLS و SRTP به‌عنوان روش‌های رمزنگاری مورد استفاده برای تأمین امنیت این کانال‌های ارتباطی، نقاط ضعف و قوت آن‌ها را نیز موردبررسی قرار داده است که طبق بیشتر پژوهش‌های صورت گرفته، استفاده از پروتکل‌های TLSو SRTP برای برقراری امنیت در لایه انتقال پیشنهاد شده است؛ استفاده از این پروتکل‌ها، علاوه بر سادگی، پیاده‌سازی سازگار با صنعت و سرمایه‌گذاری دانشگاهی بوده و پهنای باند کارآمدتر نسبت به پروتکل Ipsec ارائه می‌دهد؛ اما ازآنجاکه TLSبر روی TCP اجرا و اولویت ارتباط سیگنالینگ SIPدر ارتباطات صوتی استفاده از پروتکلUDP می‌باشد، لذا، استفاده از TLS سبب ضعف استفاده از مکانیزم امنیتی و افزایش ترافیک داده بدلیل تعداد زیاد اتصال بین کاربر و P-CSCF در TCP خواهد شد؛ و بنابراین بکارگیری پروتکل TLS در ارتباطات امن VoIP پیشنهاد نمی‌گردد. در حقیقت GCM یک الگوریتم توصیه شده برای رمزنگاری معتبر با داده‌هایی از یک بلوک کلید متناوب با اندازه بلوک ۱۲۸ بیتی، مانند الگوریتم پیشرفته رمزگذاری پیشرفته (AES) ساخته شده است. بنابراین، GCM حالت عملیاتی الگوریتم AES است. GCM اطمینان از محرمانه بودن داده‌ها را با استفاده از تنوع حالت عملیات رمز برای رمزگذاری اطمینان می‌دهد. GCM تضمین اعتبار داده‌های محرمانه (تا حدود ۶۴ گیگابایت در هر فراخوانی) را با استفاده از یک تابع درهم‌ساز جهانی که بر روی فیلد Galois تعریف شده است، فراهم می‌کند. GCM همچنین می‌تواند اطمینان احراز هویت داده‌های اضافی را (از عمق نامحدودی در هر فراخوانی) که رمزگذاری نشده است، فراهم کند.

با تجزیه‌وتحلیل عملکرد AES-GCM و مقایسه پارامترهای مختلف به این نتیجه رسیدیم که نرخ تحویل بسته در AES-GCM بیشتر از مد عملیاتی AES-CTR می‌باشد که این امر دلیل برتری AES-GCM در ارائه کیفیت سرویس می‌باشد.(خاصیت) همچنین زمان رمزگذاری، کدگشائی، میزان مصرف انرژی و نرخ از دست رفتن بسته در رمزگذاری به‌مراتب کمتر از مدعملیاتیAES-CTR می‌باشد.(خاصیت) در مقایسه‌ای دیگر میزان زمان مصرفی برای ارسال بسته و میزان تأخیر انتقال بسته در مد عملیاتی پیشنهادی به‌مراتب کمتر است.(خاصیت)؛ که نتایج نشان می‌دهد میزان زمان و تأخیر کمتری در مد پیشنهادی نسبت به AES-CTR را خواهد داشت.

مراجع

[1] Thermos, P. & Takanen, A., Securing VoIP networks: threats, vulnerabilities, and countermeasures. Pearson Education, 2007.

[2] Meisel, J. B. & Needles, M. Voice over internet protocol (VoIP) development and public policy implications. info, 7(3), 3-15, 2005.

[3] A.Tahir, A. Shahzad, Security Issues for Voice over IP Systems, International journal of computer and network security,2-5,41-51, 2010.

[4] De Pessemier, T. Stevens, I. De Marez, L. Martens, L. & Joseph, W. Quality assessment and usage behavior of a mobile voice-over-IP service. Telecommunication Systems, 61(3), 417-432,2016

[5] Schwartz, D. A Comparison of Peer-To-Peer and Client-Server Architectures in VoIP Systems, http://www.tmcnet.com/voip/0406/featurearticlecomparison-of-peer-to-peer. htm,2013

[6] Sun, L. & Ifeachor, E. C. Voice quality prediction models and their application in VoIP networks. IEEE transactions on multimedia, 8(4), 809-820, 2006.

[7] Andersson, M. Parametric Prediction Model for Perceived Voice Quality in Secure VoIP,2016.

[8] Bano, S. Kulkarni, V. Perigo, L. Williams, D. & Engineer, F, High-Performance and Cost-Effective VoIP Security Techniques for Operations on IPv4, IPv6, and IPv4/IPv6 Networks, 65-72, 2006.

[9] Tamási, L. Orincsay, D. & Józsa, B. G. Cost-optimal design of VoIP networks using the VPN concept. Computer Networks, 50(5), 599-614, 2006.

[10] Falk, T. H. & Chan, W. Y. Performance study of objective speech quality measurement for modern wireless-VoIP communications. EURASIP Journal on Audio, Speech, and Music Processing,, SEP, 2009.

[11] Cecere, G. & Corrocher, N. The usage of VoIP services and other communication services: An empirical analysis of Italian consumers. Technological Forecasting and Social Change, 79(3), 570-578, 2012.

[12] Kuhn, D. R. Walsh, T. J. & Fries, S. Security considerations for voice over IP systems. NIST special publication, 800, 2005.

[13] Sun, L. Speech quality prediction for voice over internet protocol networks,2004

Ethernet Working Group, InternetStandardforEthernet, "Institute of Electrical and Electronics Engineers, IEEE 802-3, Not cited, 2012.

[14] Zhang, G. Fischer-Hübner, S. Martucci, L. A. & Ehlert, S. Revealing the calling history of SIP VoIP systems by timing attacks. In 2009 International Conference on Availability, Reliability and Security (pp. 135-142), IEEE, Mar, 2009.

[15] Wahab, A. Bahaweres, R. B. Alaydrus, M. & Sarno, R. Performance analysis of VoIP client with

integrated encryption module. In 2013 1st International Conference on Communications, Signal Processing, and their Applications (ICCSPA) (pp. 1-6). IEEE. Feb,2013.
[16] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, 5280, 1-150, 2008.
[17] H. Krawczyk, M. Bellare, and R. Canetti, HMAC: Keyed-Hashing for Message Authentication, Internet Engineering TaskForce,RFC2104, updated by RFC 6151, Feb, 1997.
[18] McGrew, David A. Viega, John. "The Galois/Counter Mode of Operation (GCM)" (PDF). p. 5. Retrieved 20 July 2013.
[19] Gopal, V. Feghali, W. Guilford, J. Ozturk, E. Wolrich, G. Dixon, M. Locktyukhin, M. Perminov, M. "Fast Cryptographic Computation on Intel Architecture via Function Stitching" Intel Corp,2010.
[20] Manley, R. & Gregg, D. A program generator for intel AES-NI instructions. In International Conference on Cryptology in India (pp. 311-327). Springer, Berlin, Heidelberg,2010.
[21] Dworkin, M. Recommendation for block cipher modes of operation. methods and techniques (No. NIST-SP-800-38A). National Inst of Standards and Technology Gaithersburg MD Computer security Div, 2001.
[22] Butcher, D. Li, X. & Guo, J. Security challenge and defense in VoIP infrastructures. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 37(6), 1152-1162, 2007.
[23] Bethencourt, J. Sahai, A. & Waters, B. Ciphertext-policy attribute-based encryption. In 2007 IEEE symposium on security and privacy (SP'07), IEEE, pp. 321-334, May, 2007.
[24] Gupta, P. & Shmatikov, V. Security analysis of voice-over-ip protocols. In 20th IEEE Computer Security Foundations Symposium (CSF'07) (pp. 49-63). IEEE,2007
[25] Alshamsi, A. & Saito, T. (March). A technical comparison of IPSec and SSL. In 19th International Conference on Advanced Information Networking and Applications, IEEE (AINA'05) Volume 1 (AINA papers) (Vol. 2, pp. 395-398), Mar, 2005.
[26] Orrblad, J. Alternatives to MIKEY/SRTP to secure VoIP. Telecommunication Systems Laboratory (TSLab), Department of Microelectronics and Information Technology (IMIT). Stockholm/Kista, Royal Institute of Technology (KTH), 2005.
[27] Coulibaly, E. & Liu, L. H. Security of Voip networks. In 2010 2nd International Conference on Computer Engineering and Technology, IEEE, Vol. 3, pp. V3-104, Apr, 2010.
[28] Sweeney, B. & Wijesekera, D. Comparison of IPsec to TLS and SRTP for Securing VoIP. In WOSIS, pp. 82-92. 2007.