مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
سال ششم، شماره ۲، تابستان ۱۳۹۷، ص ۱۴۶-۱۳۵

ارتباطات زیرآبی پنهان و امن مبتنی بر سوت دلفین و درخت مرکل

سید محمدرضا موسوی میرکلایی[1*]، مسعود کاوه[2]

۱- استاد، ۲- دانشجوی دکتری، دانشکده مهندسی برق، دانشگاه علم و صنعت ایران

(دریافت: ۹۶/۰۴/۳۱، پذیرش: ۹۶/۱۱/۱۸)

چکیده

شرایط و چالش‌های منحصربه‌فرد موجود در کانال‌های زیرآبی موجب می‌شود تا ارتباطات در این محیط در مقابل حملات بدخواهانه بسیار آسیب‌پذیر باشند. لذا در سال‌های اخیر استفاده از سیگنال‌های زیستی مانند سوت دلفین به‌منظور ایجاد ارتباطات پنهان و همچنین به‌منظور استفاده از خواص فرکانسی بسیار مناسب این سیگنال‌ها در زیر آب، پیشنهاد شده است. اما در این روش نیز نمی‌توان به ارتباطات امن کامل در محیط زیر آب رسید، زیرا این سیگنال‌های در همه آب‌ها موجود نبوده و یا در حالتی بدتر، ممکن است دشمن به تجهیزاتی مجهز باشد که به هر طریقی قادر به آشکارسازی این سیگنال‌ها در زیر آب شود. لذا در این مقاله، روشی مبتنی بر درخت مرکل به هدف فراهم نمودن ارتباطی امن در همه حالت‌ها متناسب با ویژگی‌های محیط زیرآبی ارائه می‌شود تا در مقابل حملات ممکن در این محیط از جمله حمله بازپخش، حمله ارسال پیام‌های جعلی، حمله تحلیل پیام و حمله اصلاح پیام مقاوم باشد. تحلیل‌های امنیتی، نشان می‌دهند که روش ارائه‌شده در این مقاله در برابر همه حملات ذکرشده امن کامل بوده و سه شرط مهم تصدیق صحت، محرمانگی و بی‌عیبی پیام را برآورده می‌سازد. همچنین در بخش ارزیابی عملکرد این روش ثابت می‌شود که روش ارائه‌شده با توجه به محدودیت‌های محیط زیرآب، بسیار مناسب بوده و نسبت به روش‌های سنتی رمزنگاری، عملکرد بهینه‌تری را در دو مولفه سربار مخابراتی و هزینه‌های محاسباتی از خود به‌جای می‌گذارد.

واژه‌های کلیدی: ارتباطات زیرآبی پنهان و امن، سیگنال‌های زیستی، سوت دلفین، تهدیدات زیرآبی، درخت مرکل

۱- مقدمه[1]

ارتباطات زیرآبی همواره با چالش‌های بیشتری نسبت به ارتباطات در هوا روبه‌رو بوده است. به دلیل جذب بالای انرژی توسط آب، باید از سیگنال‌های آکوستیکی به‌جای سیگنال‌های رادیویی یا نوری در زیر آب استفاده نمود که این امر سبب رویارویی با مشکلاتی از قبیل تداخل‌های چندمسیره [۲-۱]، پهنای باند بسیار محدود [۳]، تاخیرهای بسیار زیاد [۴]، نرخ خطای بیت بزرگ [۶-۵] و محیط بسیار نویزی در زیر آب [۸و۷] می‌شود. به دلیل وجود این چالش‌ها و ویژگی‌های منحصربه‌فرد، ارتباطات زیرآبی می‌تواند به‌راحتی در معرض حملات بدخواهانه قرار گیرد. بنابراین در سال‌های اخیر تلاش‌های زیادی در راستای ایجاد ارتباطی امن به دور از انواع مختلفی از حملات ممکن در زیر آب صورت گرفته است.

ارتباطات زیرآبی پنهان[1] به منظور عدم آشکارسازی پیام توسط شنودگر از اولین اقدامات امنیتی در محیط زیر آب بوده‌اند [۱۰-۹]. روش‌های زیادی در سال‌های اخیر جهت رسیدن به ارتباطات زیرآبی امن پیشنهاد شده‌اند که از جمله آن‌ها می‌توان به سوارسازی تقسیم فرکانسی متعامد[2] [۱۳-۱۱]، طیف گسترده چندحامله[3] [۱۴] و طیف گسترده با توالی مستقیم[4] اشاره نمود [۱۶-۱۵]. روش OFDM در واقع یک مدولاسیون باند پایه است که استفاده از تقسیم فرکانس به‌صورت عمودی عمل می‌نماید. در این روش بازه فرکانسی به چندین فرکانس حامل یا به عبارت دیگر زیرحامل تقسیم شده و بر روی هر یک از این زیرحامل‌ها بخشی از اطلاعات ارسال می‌گردد. از مزیت‌های این روش ارسال داده به صورت موازی و غلبه بر محوشدگی در فرکانس مورد نظر است. در روش‌های طیف گسترده، توان سیگنال ارسالی در یک طیف فرکانسی پخش می‌شود. این روش باعث می‌شود تا آشکارسازی سیگنال توسط دشمن کار پیچیده‌ای باشد، زیرا در این روش، سیگنال پیام با یک سیگنال دیگر که دارای فرکانس

* رایانامه نویسنده مسئول: M_Mosavi@iust.ac.ir

1- Covert Underwater Acoustic Communication

2- Orthogonal Frequency Division Modulation (OFDM)
3- Multicarrier Spread Spectrum (MC-SS)
4- Direct Sequence Spread Spectrum (DSSS)

بالاتری از سیگنال اصلی می‌باشد، رمز شده و فقط گیرنده آن سیگنال دیگر را به‌منظور آشکارسازی پیام اصلی در اختیار دارد. اما این روش‌ها با دو مشکل اساسی روبه‌رو می‌باشند. ابتدا اینکه آن‌ها به نسبت، سیگنال به نویز[1] بالایی برای ایجاد ارتباطی موفق نیاز دارند. لذا احتمال آشکارسازی پیام در سطوح SNR بالاتر افزایش یافته و سامانه در معرض حمله قرار می‌گیرد. از طرفی با توجه به ویژگی‌های کانال زیرآبی، کار در SNR پایین بسیار مشکل خواهد بود. همچنین شکل موج سیگنال‌های مورد استفاده در این روش‌ها از دیگر نقاط ضعف آن‌ها می‌باشند. چرا که این شکل موج‌ها دارای ویژگی‌های مشخصی بوده که به راحتی توسط سونارهای دشمن قابل آشکارسازی است. وجود این مسائل، تلاش‌ها را به سمت استفاده از سیگنال‌های زیستی رهنمون ساخته است که می‌توانند میزان پنهانی بسیار مناسبی را به همراه داشته باشند. در واقع به‌جای پایین آوردن SNR به یک سطح کمینه، می‌توان از سیگنال‌هایی برای مخابرات زیرآبی استفاده نمود که به‌صورت طبیعی در زیر آب وجود دارند [۱۷]. این یک روش جدید و بسیار مناسب برای دستیابی به ارتباطات زیرآبی پنهان می‌باشد که از سیگنال‌های مورد استفاده جانداران دریایی مانند شیر دریایی [۱۸] و دلفین‌ها استفاده می‌نماید [۱۹].

در سال‌های اخیر تحقیقات بسیار زیادی بر روی استفاده از صوت دلفین در ارتباطات زیرآبی صورت گرفته است [۲۶-۲۰]. ویژگی‌های فرکانسی و همبستگی خاص مولفه‌های صوت دلفین مانند سوت‌ها[2] و کلیک‌ها[3]، موجب شده تا استفاده از آن‌ها به نتایج بسیار مثبتی در ارتباطات زیرآبی پنهان ختم شود. به این منظور، در این مقاله یک سوت دلفین [۲۷] از نظر خواص فرکانسی و همبستگی زیر مورد تحلیل قرار می‌گیرد.

- این روش موجب دستیابی به میزان پنهانی خوب حتی در سطوح SNR بالا می‌گردد.
- انرژی این سوت به میزان قابل توجهی در بازه فرکانسی ۱ تا ۹ هرتز متمرکز شده است که برای ارتباطات زیرآبی بسیار مناسب می‌باشد.
- به دلیل مشخصه‌های فرکانسی پایین، این روش می‌تواند برای ارتباطات در مسافت‌های بسیار طولانی مورد استفاده قرار گیرد.
- به دلیل خواص همبستگی متقابل بسیار مناسب بین نمونه‌های[4] مختلف، نرخ خطای بیت در این روش به طور قابل توجهی کاهش می‌یابد.

اما مساله مهمی که باید مورد توجه قرار گیرد این است که این سوت‌ها ممکن است در همه محیط‌های زیرآبی پنهان نبوده و یا در حالتی بدتر، دشمن ممکن است به تجهیزاتی مجهز باشد که بتواند سوت‌های ارسالی را آشکار نماید. از طرفی دیگر، هنوز هم تمایل به استفاده از سوت‌های دلفین به دلیل ویژگی‌های بسیار مناسب دیگرشان وجود دارد. لذا این مقاله سعی در ارائه روشی امن و بهینه متناسب با محدودیت‌های کانال زیرآبی مبتنی بر استفاده از سوت دلفین و روش‌های رمزنگاری دارد. در سال‌های اخیر برخی روش‌ها به منظور امنیت سامانه‌های ارتباطات زیرآبی و سامانه‌های سونواری صورت گرفته‌اند [۳۰-۲۸] که از قبیل این سامانه‌ها می‌توان به شبکه‌های حسگر زیرآبی اشاره نمود [۳۵-۳۱] که چالش‌ها و راه‌کارهای امنیتی در لایه‌های مختلف این شبکه‌ها توسط دانشمندان مورد بررسی قرار گرفته و هنوز هم یک زمینه تحقیقاتی باز می‌باشد [۴۰-۳۶]. سامانه‌ای که در این مقاله مورد بررسی قرار می‌گیرد، شامل تعداد مشخصی از زیرسطحی‌ها شامل AUV[5] و زیردریایی‌های خودی می‌باشد که گزارش‌های زیرآبی را به یک مرکز فرماندهی سطحی[6] می‌فرستند. هر یک از AUVها می‌تواند خود اطلاعات زیرآبی را به دست آورده و یا اطلاعات از حسگرهای زیرآبی جمع‌آوری نماید [۴۲-۴۱] و سپس برای SCC بفرستد. همچنین یک حمله‌گر بیرونی[7] نیز در سامانه وجود دارد که می‌تواند حمله‌های بازپخش[8]، حمله ارسال پیام‌های جعلی[9]، حمله تحلیل پیام[10] و حمله اصلاح پیام[11] را انجام دهد.

هدف این مقاله ارائه یک روش امن و بهینه با توجه به حمله‌ها و محدویت‌های موجود در محیط زیرآب می‌باشد. امن به این معنا که روش پیشنهادی در برابر حملات مذکور مقاوم بوده و سه شرط تصدیق صحت، محرمانگی و بی‌عیبی پیام را ارضا نماید. بهینه نیز به این معنا است که روش‌های امنیتی اضافه شده بر سامانه دارای کمترین میزان سربار مخابراتی و کمترین میزان مصرف منابع محاسباتی باشند. لذا یک روش تصدیق صحت مبتنی بر درخت هش مرکل[12] [۴۵-۴۳] در این مقاله ارائه می‌گردد. همچنین برای محرمانگی و بی‌عیبی پیام از الگوریتم AES[13] استفاده می‌شود. همچنین میزان بهینه بودن این روش در دو مولفه سربار مخابراتی و هزینه‌های محاسباتی با روش RSA[14] مورد مقایسه قرار می‌گیرد. تحلیل امنیتی نشان می‌دهد که روش پیشنهادی در برابر حملات مذکور مقاوم بوده و سه شرط اصلی

1- Signal To Noise Ratio (SNR)
2- Whistles
3- Clicks
4- Symbol

5- Autonomous Underwater Vehicles
6- Surface Command Center (SCC)
7- External Adversary (EA)
8- Replay Attack
9- Fabricated Message Attack
10- Analyst Attack
11- Message Modification Attack
12- Merkle Hash Tree
13- Advanced Encryption Standard
14- Rivest–Shamir–Adleman

امن بودن پیام را برآورده می‌سازد. همچنین در بخش ارزیابی عملکرد این روش ثابت می‌شود که روش ارائه شده با توجه به محدودیت‌های محیط زیرآب، بسیار مناسب بوده و نسبت به روش RSA، عملکرد بهینه تری را در دو مولفه سربار مخابراتی و هزینه‌های محاسباتی از خود به جای می‌گذارد. سازمان‌دهی مقاله به شرح زیر است:

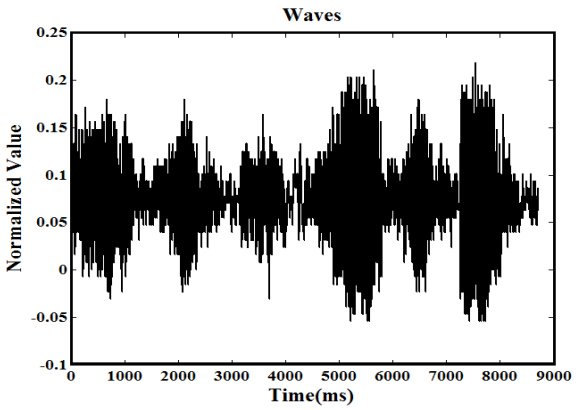
بخش دوم به تحلیل سوت دلفین مورد استفاده در این مقاله می‌پردازد. بخش سوم مدل سامانه تهدیدات را نشان داده و بخش چهارم روش ارائه شده را مورد بررسی قرار می‌دهد. همچنین تحلیل امنیتی و ارزیابی عملکرد روش پیشنهادی به ترتیب در بخش‌های پنجم و ششم قرار گرفته و در انتها نیز یک نتیجه‌گیری صورت می‌گیرد.

این مقاله، یک پروتکل ارتباطی نوین برای ارتباطات زیرآبی "امن" و "بهینه" مبتنی بر درخت هش مرکل و سوت دلفین ارائه می‌دهد که برای اولین بار از روش‌های رمزنگاری در این سامانه‌ها استفاده می‌نماید. نحوه استفاده از درخت هش مرکل و الگوریتم AES در این پروتکل موجب گشته تا روش پیشنهادی علاوه بر امنیت کامل و مقاومت در برابر حملات موجود، دارای بهینگی قابل توجهی در سربار مخابراتی و محاسباتی متناسب با محدودیت‌های موجود در سامانه‌های زیرآبی گردد. همچنین استفاده از سوت دلفین به عنوان حامل، علاوه بر افزودن خاصیت پنهانی پیام، سبب آشکارسازی مناسب و اجتناب از به‌کارگیری روش‌های کدگذاری و کدگشایی با افزایش سربار مخابراتی در گیرنده و فرستنده می‌شود.

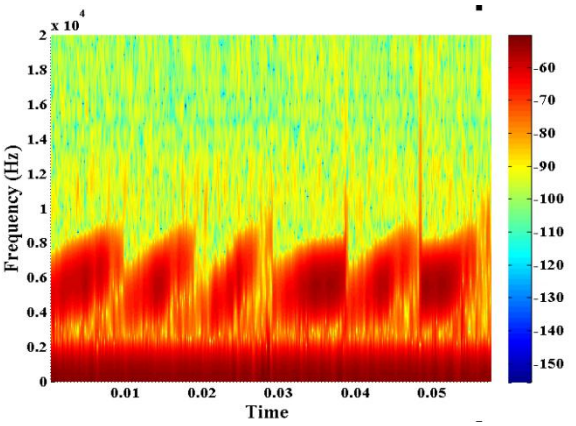
۲- تحلیل سوت دلفین

سوت دلفین به دو دسته کلی سوت‌ها و کلیک‌ها تقسیم می‌شود که دلفین‌ها از آن‌ها به ترتیب برای مخابرات و مکان‌یابی استفاده می‌کنند. سوت‌ها سیگنال‌های FM باند باریک و دارای بازه زمانی چند صد ms تا چند ثانیه بوده، اما کلیک‌ها دارای بازه زمانی چند ده ms تا چند صد ms می‌باشند. در این مقاله از سوت دلفین آمده در [۲۷] برای ارسال اطلاعات استفاده می‌شود. شکل (۱) سوت ضبط شده را در زمان نشان می‌دهد. شکل (۲) نشان‌دهنده طیف زمان- فرکانس سوت می‌باشد.

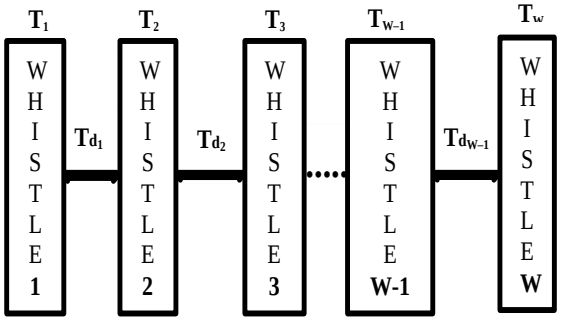
با توجه به این شکل می‌توان مشاهده نمود که اکثر انرژی سوت در بازه ۱ تا ۹ هرتز متمرکز شده است. لذا می‌توان نتیجه گرفت که این سوت به دلیل مشخصه‌های فرکانسی پایین، برای ارتباطات زیرآبی در زیرآب بسیار مناسب می‌باشد. شکل (۳) کدینگ تاخیر در زمان سوت را نشان می‌دهد. T_i بیان‌گر میزان بازه زمانی هر سوت و T_{d_i} بیان‌گر فاصله زمانی یک سوت تا سوت بعدی می‌باشند.



شکل (۱): نمونه‌های موجود در بازه زمانی سوت دلفین.



شکل (۲): تحلیل زمان- فرکانس سوت دلفین.



شکل (۳): تاخیرهای زمانی موجود در یک سوت دلفین

با توجه به شکل (۱)، هر سوت شامل شش نمونه با اطلاعات مختلف بوده، به طوری که می‌توان فرض کرد در شکل (۳)، $W = 6$ باشد. بنابراین، نمونه‌های موجود در سوت ضبط شده در شکل (۱) به ترتیب و به صورت زیر فرض می‌شوند:

$W_1(t), W_2(t), W_3(t), W_4(t), W_5(t), W_6(t)$

جدول (۱) مقادیر توابع خودهمبستگی و همبستگی متقابل هر یک از نمونه‌ها را نشان می‌دهد. با توجه به این جدول می‌توان مشاهده نمود که مقادیر همبستگی متقابل نمونه‌ها در سوت دلفین بسیار کم بوده (نزدیک به صفر) و در واقع این موضوع،

کلید اصلی مخابرات زیرآبی به‌وسیله سوت دلفین می‌باشد. شکل (۴) بلوک دیاگرام انتهای فرستنده را در روش پیشنهادی نشان می‌دهد. در ابتدای بیت‌های سریال به فرم موازی در آمده و سپس بر پایه اینکه خروجی قسمت موازی‌ساز چه مقداری باشد، سوت مورد نظر برای ارسال انتخاب می‌شود. در شکل (۵) بلوک دیاگرام مربوط به انتهای گیرنده سوت دلفین نمایش داده شده است. در سمت گیرنده W بخش محاسبه همبستگی وجود دارد که همبستگی سوت دریافتی را با سوت‌های ذخیره شده در خود محاسبه می‌نماید. با توجه به خواص همبستگی سوت مورد نظر در جدول (۱)، W–1 مقدار همبستگی نزدیک به صفر بود و یک مقدار نزدیک به یک می‌باشد که این سوت همان سوت ارسالی از طرف فرستنده است. در واقع در این روش، تابع خودهمبستگی سوت‌ها باید تیز بوده و مقدار تابع همبستگی بین آنان باید به سمت صفر میل نماید. در غیر این‌صورت خطای بیت اتفاق افتاده و تصمیم‌گیری غلط صورت می‌گیرد.

جدول (۱). ضرایب همبستگی مربط به سوت دلفین.

سیگنال ها	$w_1(t)$	$w_2(t)$	$w_3(t)$	$w_4(t)$	$w_5(t)$	$w_6(t)$
$w_1(t)$	1.00	-0.16	0.08	-0.03	-0.18	0.00
$w_2(t)$	-0.16	1.00	-0.06	-0.20	0.14	0.04
$w_3(t)$	0.08	-0.06	1.00	0.02	-0.08	0.09
$w_4(t)$	-0.03	-0.20	0.02	1.00	0.16	0.00
$w_5(t)$	-0.18	0.14	-0.08	0.16	1.00	-0.08
$w_6(t)$	0.00	0.04	0.09	0.00	-0.08	1.00

در این روش چهار نمونه‌ای که دارای کمترین مقدار همبستگی متقابل می‌باشند یعنی: $W_1(t)$، $W_3(t)$، $W_4(t)$ و $W_6(t)$ برای ارسال اطلاعات و دو سوت دیگر جهت برای استفاده‌های دیگر مانند ایجاد هم‌زمانی انتخاب می‌شوند. بر اساس بیت‌های ارسالی، هر یک از سوت‌های $W_1(t)$، $W_3(t)$، $W_4(t)$ و $W_6(t)$ انتخاب شده و ارسال می‌گردند. لذا مقدار اطلاعاتی را هر سوت حمل می‌کند برابر دو بیت می‌باشد، زیرا $\log_2 4 = 2$. اگر فرض شود که هر یک سوت‌ها، اطلاعات را به فرم زیر حمل کنند:

دیتا	سوت
00	$W_1(t)$
01	$W_3(t)$
10	$W_4(t)$
11	$W_6(t)$

آن‌گاه برای فرستادن کلمه‌ای مانند hi با مقدار بیت‌های '01 01 10 10 00 01 10 10 01' باید به ترتیب سوت‌های زیر ارسال شوند:

$W_3(t), W_4(t), W_4(t), W_1(t), W_3(t), W_4(t), W_4(t), W_3(t)$

در قسمت گیرنده نیز با توجه به مطالبی که ذکر شد هر یک از سوت‌ها با توجه به مقدار همبستگی‌شان آشکار می‌شوند.

در این نوع از ارسال پیام، استفاده از روش‌های بازخوردی سنتی برابرسازی کانال مناسب نیست. لذا می‌توان از الگوریتم MP[1] برای تخمین کانال استفاده نمود. الگوریتم MP یک روش تکرارپذیر است که می‌تواند به طور پیوسته کانال غالب را شناسایی و ضرایب مربوط به آن را تخمین بزند. در هر تکرار، MP یک ستون از نمونه‌های ارسالی S را انتخاب می‌کند که با تقریب تکرار قبلی هم‌خوانی دارد. اگر فرض شود که داده‌ها از یک کانال چندمسیره زیرآبی عبور نمایند، نمونه‌های سیگنال دریافتی (Y) می‌توانند به صورت رابطه زیر بیان گردند:

$$Y_{N\times 1} = S_{N\times L} \times h_{L\times 1} + W_{N\times 1} \qquad (۱)$$

که در آن، h تپ کانال و W سیگنال نویزی می‌باشند.

۳- مدل سامانه و تهدیدهای موجود

شکل (۶) یک سامانه ارتباطات آکوستیک زیرآبی شامل چند AUV و زیردریایی خودی، یک مرکز فرماندهی سطحی (SCC) و یک حمله‌گر (EA) را نشان می‌دهد. در این سامانه هر یک از زیرسطحی‌ها دارای محدودیت انرژی و محاسباتی می‌باشند، زیرا منابع انرژی و محاسباتی آن‌ها (خصوصا AUV) محدود می‌باشد. SCC گزارشات هر یک از زیرسطحی‌ها را جمع‌آوری نموده و به تحلیل آن‌ها می‌پردازد. به دلیل رسیدن پیام‌های بسیار زیاد به SCC توسط همه زیرسطحی‌ها، در نظر گرفتن هزینه‌های محاسباتی برای SCC نیز یک مساله چالش‌برانگیز محسوب می‌گردد. هرچند که فرض می‌شود SCC هیچ‌گونه محدودیتی در مصرف منابع انرژی نداشته باشد. همچنین ذکر این نکته ضروریست که تمام اطلاعات و گزارش‌هایی که زیرسطحی‌ها برای SCC می‌فرستند در یک فرمت خاص بوده و البته SCC این فرمت را می‌داند.

و یک حمله‌گر (EA) را نشان می‌دهد. در این سامانه هر یک از زیرسطحی‌ها دارای محدودیت انرژی و محاسباتی می‌باشند، زیرا منابع انرژی و محاسباتی آن‌ها (خصوصا AUV) محدود می‌باشد. SCC گزارشات هر یک از زیرسطحی‌ها را جمع‌آوری نموده و به تحلیل آن‌ها می‌پردازد. به دلیل رسیدن پیام‌های بسیار زیاد به SCC توسط همه زیرسطحی‌ها، در نظر گرفتن هزینه‌های محاسباتی برای SCC نیز یک مساله چالش‌برانگیز محسوب می‌گردد. هرچند که فرض می‌شود SCC هیچ‌گونه محدودیتی در مصرف منابع انرژی نداشته باشد. همچنین ذکر این نکته

1- Matching Pursuit

ضروریست که تمام اطلاعات و گزارش‌هایی که زیرسطحی‌ها برای SCC می‌فرستند در یک فرمت خاص بوده و البته SCC این فرمت را می‌داند.

همچنین این سامانه می‌تواند توسط EA مورد حمله قرار گرفته که در مورد محیط زیرآبی و ارتباطات در آن شناخت کاملی داشته می‌تواند پیام‌های ارسالی را در بین راه ضبط کرده و یا به دام بیندازد. حال فرض می‌شود که EA حملات زیر را به سامانه اعمال کند:

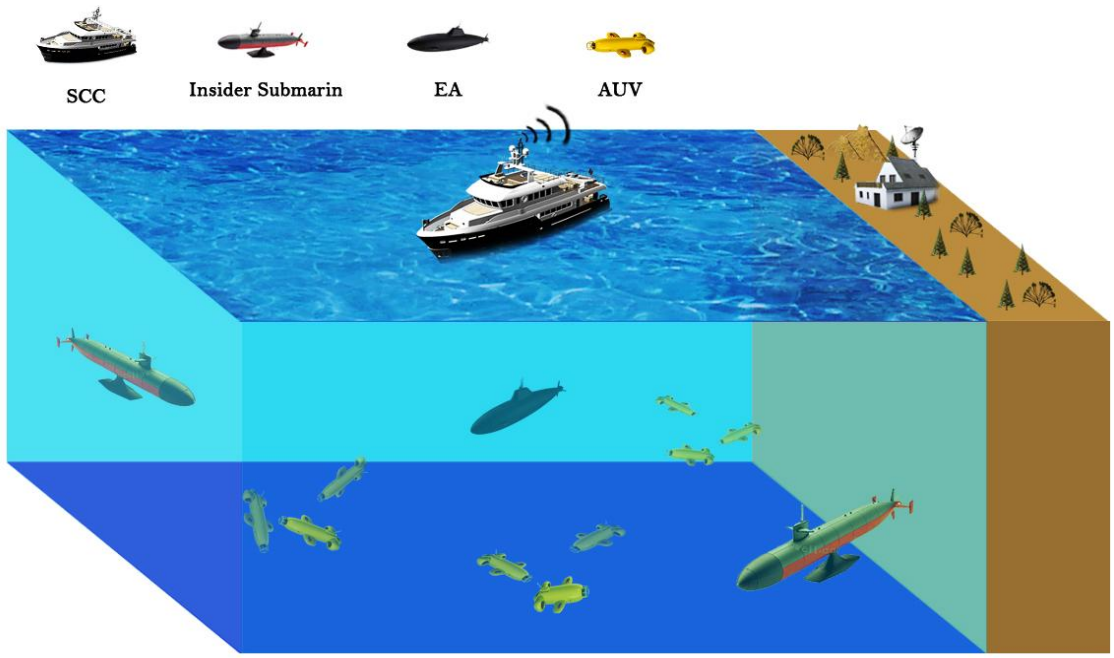
۱) **حمله بازپخش:** در این نوع از حمله، EA می‌تواند پیام‌های ارسال شده توسط زیرسطحی‌ها را ضبط کرده و دوباره برای SCC ارسال نماید. در واقع SCC پیام‌هایی را دریافت می‌کند که از تاریخشان گذشته است. لذا در نظر گرفتن یک روش تصدیق صحت برای آشکارسازی پیام‌های منقضی ضروریست.

۲) **حمله ارسال پیام جعلی:** در اینجا SCC یک پیام جعلی از EA دریافت کرده که با توجه به نوع پیام دریافتی و در صورت عدم آشکارسازی می‌تواند موجب گرفتن تصمیماتی به نفع دشمن گردد. بنابراین تدوین روشی مبتنی بر تصدیق صحت برای آشکارسازی فرستنده پیام‌های دریافتی در SCC ضروری می‌باشد.

۳) **حمله تحلیل پیام:** در این روش EA پیام ارسالی را دریافت کرده و به گشودن و تحلیل آن برای یافتن جزییات هر چه بیشتر اهتمام می‌ورزد. بنابراین استفاده از روش‌های رمزنگاری جهت مقابله با حمله‌های ضدمحرمانگی لازم است.

۴) **حمله اصلاح پیام:** پیام‌های ارسالی در کانال ممکن توسط EA گیر افتاده و مورد تغییر و اصلاح قرار گیرند. در این صورت SCC امکان دستیابی به پیام‌های صحیح را از دست می‌دهد. لذا باید از روش‌های حفظ بی‌عیبی پیام استفاده شود.

در ادامه توضیح مدل سامانه و تهدیدات موجود، به بررسی اهداف طراحی پرداخته می‌شود. در واقع همان‌طور که قبلا اشاره گردید، هدف از ارائه روش پیشنهادی در این مقاله، طراحی یک پروتکل "امن" و "بهینه" برای سامانه مورد نظر است.



شکل (۶): مدل سامانه ارتباطات زیرآبی و تهدیدات موجود در این مقاله.

۴- روش امن پیشنهادی در این مقاله

روش امن و بهینه ارائه شده در این مقاله بر پایه درخت هش مرکل شکل می‌گیرد. درخت‌های هش مرکل روشی بر پایه توابع هش رمزنگاری می‌باشند که به شکل یک درخت، به درهم ساختن پیام‌ها از گره‌های پایین‌تر تا بالاترین گره می‌پردازند. در این درخت‌ها، هر گره برگ[1] (پایین‌ترین گره) به عنوان یک فرزند در نظر گرفته شده و هر گره غیر برگ بالایی از هش شدن فرزندهای پایینی حاصل می‌گردد. این درخت یک عامل از فاکتور

1- Leaf Node

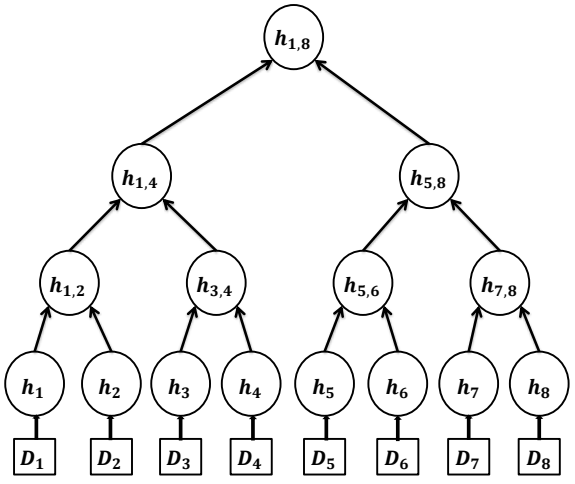
دو دارد، یعنی برای یک درخت با ارتفاع n، 2^n گره برگ به وجود می‌آید. اطلاعات مسیر تصدیق صحت[1]، یکی از مهم‌ترین مفاهیم مطرح شده در درخت مرکل می‌باشد که در واقع کلید اصلی تصدیق صحت بر پایه درخت مرکل بوده و گره‌های برگ به وسیله آن اعتبار می‌یابند. شکل (۷) یک درخت مرکل با هشت گره برگ را نشان می‌دهد. با توجه به شکل، هر گره بالایی از هش شدن دو گره پایینی به دست می‌آید. برای مثال اگر داشته باشیم $h_i = Hash\ (D_i)$، آنگاه مقدار $h_{5,6}$ از رابطه زیر به دست می‌آید:

$$h_{5,6} = Hash\ (h_5|h_6) \qquad (۲)$$

همچنین گره ریشه[2] (بالاترین گره) نیز از رابطه زیر به دست می‌آید:

$$h_{1,8} = Hash\ (h_{1,4}|h_{5,8}) \qquad (۳)$$

نکته مهمی که باید در نظر گرفته شود این است که هر گره برگ به وسیله API مربوط به خود و گره ریشه تصدیق می‌شود. برای مثال، اگر SCC گره ریشه ($h_{1,8}$) را ذخیره کند، پنجمین پیام ارسالی (D_5) از یک زیرسطحی با $API_j = \{h_6, h_{7,8}, h_{1,4}\}$ می‌تواند به این صورت تصدیق شود: ابتدا SCC طبق رابطه (۲) مقدار $h_{5,6}$ را محاسبه می‌نماید. سپس طبق درخت مرکل در شکل (۷)، همین روند را تا ریشه محاسبه نموده و به مانند رابطه (۳) تکرار می‌کند. حال SCC مقدار گره ریشه به دست آمده را با مقداری که خود ذخیره کرده بود، مقایسه می‌نماید. اگر دو مقدار با هم برابر باشند، پیام مورد قبول واقع شده و در غیر این‌صورت رد می‌گردد.



شکل (۷): یک درخت هش مرکل با ارتفاع سه و تعداد برگ هشت.

در حالت کلی می‌توان یک درخت مرکل را با ارتفاع n و تعداد ریشه برگ 2^n در نظر گرفت. تعدادی پیام رمز شده‌ای که هر درخت در هر شرایطی باید تولید کند، مقادیر ارتفاع و متعاقبا تعداد ریشه برگ را مشخص می‌نماید. برای مثال اگر فرض شود که SCC باید به طور میانگین در هر دوازده دقیقه یک پیام از هر زیرسطحی دریافت نماید، لذا در هر روز ۱۲۰ پیام در قالب متن رمز شده بین SCC و هر زیرسطحی مخابره شده که در این صورت به درختی با ارتفاع هفت و تعداد ریشه برگ‌های ۱۲۸ نیاز است.

به دلیل استفاده از توابع رمزنگاری هش، لازم است تا در اینجا ثابت شود که هیچ گونه تصادمی[3] صورت نمی‌گیرد. یعنی اگر $hi = Hash\ (Di)$، آنگاه نتوان پیام جعلی D'_i پیدا کرد که در آن داشته باشیم: $hi = Hash\ (D'i)$. به عبارت دیگر باید ثابت نمود که احتمال اتفاق یک تصادم تقریب برابر صفر است. اگر h یک تابع هش بوده که بتواند خروجی هش رمز شده‌ای برابر z-bit $(z = 2^q,\ q \in \{1, 2, \dots\})$ تولید نماید، بنابراین برای یک پیام تصادفی D، 2^z پیام هش شده مختلف توسط h(D) تولید می‌شود. در اینجا می‌توان ثابت نمود که چند پیام جعلی باید توسط EA ساخته و فرستاده شود تا در SCC یک تصادم رخ دهد. اگر فرض شود که P(l) احتمال رخ دادن یک تصادم بعد فرستادن l پیام جعلی باشد، داریم:

$$Pr[E_i] = \frac{i-1}{2^z} \qquad (۴)$$

$$P(l) = \Pr[E_1 \vee E_2 \vee \dots \vee E_l]$$
$$\leq \Pr[E_1] \vee \Pr[E_2] \vee \dots \vee \Pr[E_l]$$
$$\leq \frac{0}{2^z} + \frac{1}{2^z} + \cdots + \frac{l-1}{2^z} = \frac{l(l-1)}{2^{z+1}} \qquad (۵)$$

که در آن، E_i احتمال رخ دادن iامین تصادم بعد از فرستادن D_i می‌باشد. طبق رابطه (۵)، باند بالایی P(l) با $O(2^{-z-1}l^2)$ رشد می‌کند. برای مثال اگر P(l) = 0.5 و z = 128-bit، آنگاه برای تولید یک تصادم با شانس ۵۰٪ (که خود شانس بالایی محسوب می‌شود)، EA نیاز دارد تا 2^{64} پیام جعلی را برای SCC بفرستد! اما D_i در دوره تناوب‌های زمانی کوتاه تغییر می‌کند که با این شرایط، احتمال روی دادن یک تصادم، به اندازه بسیار بزرگی کافی، قابل صرف نظر کردن است.

با توجه به شکل (۸)، هر زیرسطحی S_j یک درخت مرکل با تعداد 2^n گره برگ در پایگاه داده خود می‌سازد. هر S_j نیز به تعداد گره‌های برگ خود، پیام‌های رمز شده‌ای به صورت رابطه زیر تولید می‌نماید:

$$C_i = Enc_{K_j}(m_i|TS_i) \qquad (۶)$$

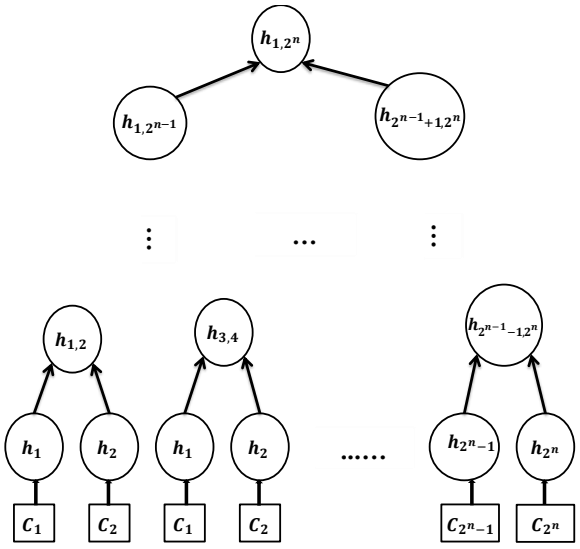
که در آن، m_i و TS_i به ترتیب متن اصلی و مهر زمانی[4] و به

1 Authentication Path Information (API)
2 Root Node

3- Collision
4- Time Stamp

معنای رمزنگاری توسط الگوریتم AES تحت کلید K_j با توزیعی مانند توزیع کلید دفی- هلمن می‌باشد. حال S_j به تشکیل گره‌های برگ با استفاده از به دست آوردن تابع هش هر یک از پیام‌های رمز شده مبتنی بر رابطه (۷) می‌پردازد:

$$h_i = \text{Hash}\ (C_i) \qquad (۷)$$



شکل (۸): یک درخت مرکل را با ارتفاع n و تعداد ریشه برگ 2^n.

به دلیل جمع و ارتباطات بلادرنگ، وجود مهر زمانی برای هر پیام ضروریست. همچنین در ادامه مشاهده خواهد شد که با کمک مهر زمانی، می‌توان اثر بعضی از تهدیدات را خنثی نمود. در حالت کلی، هر پیام ارسالی توسط S_j می‌تواند با توجه به ثانیه، دقیقه، روز، ماه و سال ارسال آن پیام تاریخ‌گذاری شده و به‌وسیله این تاریخ، مهر زمانی منحصربه‌فرد برای هر پیام تولید گردد. ذکر این نکته ضروریست که میانگین فاصله زمانی بین ارسال دو پیام متوالی توسط S_j و یا نوع مهر زمانی مورد استفاده، مقدار n و متعاقبا تعداد گره‌های برگ درخت مرکل مرتبط را مشخص می‌کند. برای مثال اگر SCC هر پیام را با فاصله میانگین ۱۲ دقیقه از هر زیرسطحی دریافت نماید، آن‌گاه در طول یک روز ۱۲۰ پیام دریافت نموده که در نتیجه هر S_j باید یک درخت مرکل با ارتفاع ۷ و تعداد گره‌های برگ ۱۲۸ در هر روز تولید نماید. پس از به‌دست آمدن تمام گره‌های برگ، گره‌های بالایی نیز از هش کردن دو گره پایینی خود با توجه به شکل (۸) به‌دست آمده و این روند تا گره ریشه ادامه می‌یابد. حال S_j می‌تواند یک مجموعه برای هر پیام رمزشده به‌صورت $[C_i, API_i]$ بسازد.

علاوه بر مجموعه ذکرشده، هر زیرسطحی C_{root_j} را به‌صورت رابطه زیر به‌دست می‌آورد:

$$C_{root_j} = Enc_{K_j}(H_{1,2^n}) \qquad (۸)$$

که در آن، $H_{1,2^n}$ گره ریشه می‌باشد. در سمت دیگر SCC C_{root_j} را دریافت نموده و گره ریشه ارسالی را طبق رابطه زیر می‌گشاید:

$$h_{1,2^n} = Dec_{K_j}(C_{root_j}) \qquad (۹)$$

که در آن، Dec_{K_j} الگوریتم رمزگشایی AES با کلید فصلی K_j می‌باشد. سپس SCC گره ریشه هر زیرسطحی را ذخیره می‌کند. پس ارسال C_{root_j}، S_j می‌تواند با استفاده از سوت دلفین، $[C_i, API_i]$ را برای SCC بفرستد. در ادامه منظور دریافت معتبر پیام‌ها، SCC می‌تواند مراحل زیر را به اجرا برساند:

۱) SCC می‌تواند حمله بازپخش را با مقایسه مجموعه هش پیام‌های دریافتی قبلی و هش پیام دریافت‌شده آشکار نماید. برای مثال فرض شود که C_i S_1 را برای SCC می‌فرستد که مقدار هش C_i برابر با Hash $(C_i) = d$ می‌باشد. سپس به پایگاه داده خود رجوع کرده و تمامی مقادیر هش‌های رسیده شده قبل را فراخوانی می‌نماید. اگر d عضو مجموعه هش‌های دریافتی قبلی تا آن لحظه باشد، آن‌گاه حمله بازپخش آشکار شده و پیام دریافت‌شده رد می‌گردد. برای مثال فرض شود که مجموعه پیام‌های هش‌شده دریافتی قبلی برابر با {c, d, e, f} باشد. حال با توجه به اینکه d عضوی از این مجموعه است، لذا پیام دریافتی یک پیام بازپخش شده بود و SCC آن را رد می‌کند.

۲) همچنین SCC برای اعتباربخشی به پیام، باید بتواند منبع فرستنده پیام را نیز شناسایی نماید. به عبارت دیگر SCC باید بداند که پیامی که دریافت می‌کند از سمت یکی از زیرسطحی‌ها ارسال شده و یا EA آن را ارسال نموده است. همان‌طور که قبلا ذکر شده است، SCC C_{root_j} و $[C_i, API_i]$ را به ترتیب دریافت می‌نماید. حال با استفاده از این مقادیر، SCC می‌تواند طبق روندی که در مثال زیر طی خواهد شد، منبع پیام دریافتی را تصدیق صحت کند.

فرض شود که S_1 $[C_i, API_i]$ را برای SCC می‌فرستد. همچنین می‌دانیم که قبلا SCC همه C_{root_j}های مربوط به زیرسطحی‌ها را دریافت نموده است. لذا SCC $H_{1,2^n}$ مربوط به S_1 را در اختیار دارد. حال SCC با استفاده از $[C_i, API_i]$ و رابطه (۹) به محاسبه گره ریشه دریافتی پرداخته و مقدار حاصله را با مقدار $H_{1,2^n}$ ذخیره‌شده مقایسه می‌نماید. اگر دو مقدار با هم برابر باشند پیام معتبر بوده و

پذیرفته می‌شود. در غیر این‌صورت، پیام دارای منبع نامعتبر بوده و رد می‌گردد.

$$\begin{aligned} h_{1,2} &= h_1 \oplus h_2 \\ h_{1,4} &= h_{1,2} \oplus h_{3,4} \\ h_{1,8} &= h_{1,4} \oplus h_{5,8} \\ &\vdots \\ h_{1,2^{n-1}} &= h_{1,2^{n-2}} \oplus h_{2^{n-2}+1,2^{n-1}} \\ h_{1,2^n} &= h_{1,2^{n-1}} \oplus h_{2^{n-1}+1,2^n} \end{aligned} \quad (۱۰)$$

۳) علاوه بر اعتبار، روش پیشنهادی باید محرمانگی و بی‌عیبی پیام را نیز برآورده سازد. برای حمله ضدمحرمانگی، فرض شود که EA پیام رمزشده را در اختیار داشته و به باز کردن و یافتن جزییات بیشتری از پیام، اهتمام بورزد. به دلیل اینکه الگوریتم AES یک الگوریتم امن می‌باشد [۴۶]، لذا EA بدون داشتن کلید نمی‌تواند آن را شکسته و به پیام دسترسی داشته باشد. بنابراین روش فوق علاوه بر معتبر بودن، شرط محرمانگی پیام را نیز در بر دارد.

۴) در طرف دیگر فرض شود که SCC پیام رمزشده C_i را دریافت نموده و با الگوریتم رمزگشایی AES متن اصلی $m_i|TS_i = Dec_{K_j}(C_i)$ را بگشاید. به دلیل تاخیر انتشار موجود در کانال آکوستیک زیرآبی، ابتدا SCC تازگی پیام را با توجه به رابطه زیر مورد بررسی قرار می‌دهد:

$$|TS_i - TS_{local}| \leq \theta \quad (۱۱)$$

که در آن، TS_{local} مهر زمانی محلی در SCC و θ یک مقدار آستانه از پیش تعریف‌شده می‌باشد. اگر رابطه (۱۱) برقرار نباشد، SCC پیام را رد می‌کند. در غیر این‌صورت متن اصلی m_i را با فرمتی که در پایگاه داده خود ذخیره دارد، مقایسه می‌نماید. اگر فرمت پیام‌ها یکی بود، پیام پذیرفته‌شده و در غیر این‌صورت رد می‌گردد. به این ترتیب، روش ارائه‌شده در این مقاله، بی‌عیبی پیام را نیز ارضا می‌نماید.

۵- تحلیل امنیتی

ویژگی‌های امنیتی روش پیشنهادی در این مقاله، در این بخش مورد بررسی قرار می‌گیرد. به عبارتی دیگر، میزان مقاوم بودن این روش در مقابل حملات بازپخش که خود نوعی از حمله فریب محسوب می‌شود [۵۰]، ارسال پیام جعلی، تحلیل پیام و اصلاح پیام مورد ارزیابی قرار می‌گیرد.

۵-۱- مقاومت در برابر حمله بازپخش

با توجه به توضیحات ارائه‌شده در قدم اول بررسی اعتبار پیام، SCC می‌تواند حمله بازپخش را با پس از دریافت $[C_i, API_i]$ آشکار نماید. برای توضیح بیشتر، ابتدا SCC مقدار $Hash\ (C_i)$ را محاسبه نموده و سپس آن را با مقادیر هش دریافتی در پایگاه داده خود مقایسه می‌نماید. اگر هیچ یک از اعضای مجموعه هش دریافتی قبلی، برابر با هش پیام دریافتی جدید نباشند، آن‌گاه می‌توان به این نتیجه رسید که حمله بازپخش صورت نگرفته است، در غیر این‌صورت حمله بازپخش آشکار شده، بنابراین روش پیشنهادی در برابر حمله بازپخش مقاوم است.

۵-۲- مقاومت در برابر حمله ارسال پیام جعلی

همان‌طور که در رابطه (۱۰) مشاهده شد، SCC می‌تواند منبع پیام را با دریافت $[C_i, API_i]$ و متعاقبا با محاسبه گره ریشه پیام دریافتی شناسایی نماید، زیرا SCC قبلا گره ریشه هر زیرسطحی را از رابطه (۹) در پایگاه داده خود ذخیره نموده و می‌تواند آن را با گره ریشه به‌دست آمده از رابطه (۱۰) مقایسه نماید. اگر دو مقدار برابر باشند، پیام پذیرفته می‌شود، اما در غیر این‌صورت، منبع پیام نامعتبر بوده و پیام رد می‌گردد.

ذکر این نکته ضروریست که EA هیچ گونه دسترسی به پایگاه داده ذخیره شده در هیچ یک از زیرسطحی‌ها نداشته و دانشی در مورد اطلاعات محرمانه موجود در آن‌ها چیزی نمی‌داند. همچنین با توجه به رابطه (۵) ثابت شد که احتمال وقوع یک تصادم قابل چشم‌پوشی بوده و EA قادر به تولید پیام جعلی که $Hash\ (C_i) = Hash\ (C_i')$ نمی‌باشد. با توجه به موارد و روابط ذکرشده، روش پیشنهادی در این مقاله در برابر حمله ارسال پیام جعلی مقاوم است.

۵-۳- مقاومت در برابر حمله تحلیل پیام

در روش پیشنهادی، هر زیرسطحی پیام مورد نظر خود ابتدا با استفاده از الگوریتم رمزنگاری AES رمز نموده (رابطه (۶)) و سپس پیام رمزشده را برای SCC می‌فرستد. اگر EA پیام رمزشده را در اختیار داشته باشد، بدون داشتن کلید سری، هرگز به متن اصلی دست نخواهد یافت، زیرا همان‌طور که قبلا ذکر شده است، الگوریتم AES امن می‌باشد. بنابراین روش پیشنهادی در برابر حمله تحلیل پیام امن می‌باشد.

۵-۴- مقاومت در برابر حمله اصلاح پیام

پس از تصدیق صحت پیام و منبع آن، SCC رمز C_i را گشوده و $m_i|TS_i$ را با توجه به رابطه زیر به‌دست می‌آورد:

$$m_i|TS_i = Dec_{K_j}(C_i) \quad (۱۲)$$

همان‌طور که قبلا ذکر شد، تمام پیام‌هایی که زیرسطحی‌ها برای SCC می‌فرستند در قالب یک فرمت بوده و این فرمت در

پایگاه داده SCC قرار دارد. حال SCC پس از گشودن رمز پیام طبق رابطه (۱۲)، متن اصلی به‌دست آمده را با فرمت موجود در پایگاه داده خود مقایسه می‌نماید. اگر پیام گشوده‌شده در قالب فرمت ذخیره‌شده در SCC بود، آنگاه پیام پذیرفته می‌شود، در غیر این‌صورت پیام به‌نحوی دچار تغییر شده و بی‌عیبی آن زیر سوال می‌رود. به این ترتیب حمله اصلاح پیام آشکار شده و SCC پیام را رد می‌کند. بنابراین روش پیشنهادی در این مقاله در برابر حمله اصلاح پیام مقاوم می‌باشد.

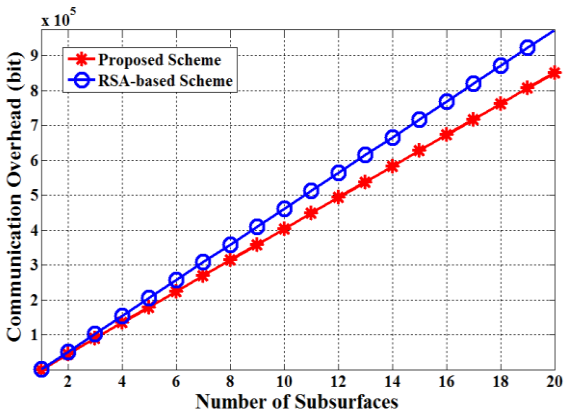
۶- ارزیابی عملکرد و میزان بهینگی

در قسمت قبل ثابت شد که روش ارائه شده امن بوده و در مقابل همه تهدیدات مقاوم است. اما میزان بهینگی روش ارائه‌شده نیز با توجه به محدودیت‌های موجود در سامانه‌ها و کانال‌های زیرآبی از اهمیت به‌سزایی برخوردار است. لذا در این بخش ارزیابی عملکرد و بهینگی روش پیشنهادی در دو مولفه سربار مخابراتی و هزینه محاسباتی با روش RSA مقایسه می‌شود.

۶-۱- سربار مخابراتی

به دلیل پهنای باند کم در ارتباطات آکوستیک زیرآبی، در نظر گرفتن سربار مخابراتی مساله‌ای بسیار مهم می‌باشد. در واقع یک رابطه مستقیم بین سربار مخابراتی که روش ارائه‌شده به سامانه اضافه می‌کند و تعداد سوت‌هایی که هر زیرسطحی برای ارسال هر پیام به SCC نیاز دارد، وجود خواهد داشت. بنابراین سربار مخابراتی اضافه شده به سامانه توسط روش امن ارائه‌شده در این مقاله با روش RSA مقایسه می‌شود.

همان‌طور که در قسمت‌های قبل اشاره گردید، SCC برای تصدیق صحت منبع پیام، نیاز به دریافت API_i مربوطه دارد. هر API از n پیام z بیتی تشکیل شده که در آن n ارتفاع درخت و یک تابع رمزنگاری هش z بیتی می‌باشد. بنابراین مقدار سربار مخابراتی روش مبتنی بر درخت مرکل در حالت کلی برابر $n \times z$ بیت است. برای مثال اگر فرض شود که $n = 7$ و $z = 128$، آنگاه سربار مخابراتی روش پیشنهادی برابر با $7 \times 128 = 896$ خواهد بود. در روش RSA که در آن S_j یک امضا RSA برای SCC می‌فرستد، مقدار سربار مخابراتی به‌طور معمول برابر ۱۰۲۴ بیت می‌باشد. اما این اختلاف با افزایش تعداد زیرسطحی‌ها محسوس‌تر خواهند شد، زیرا در یک سامانه مخابرات آکوستیک زیرآبی، هر SCC با تعداد زیادی از زیرسطحی‌ها در ارتباط است. شکل (۹) برتری عملکرد روش پیشنهادی نسبت به روش RSA را با افزایش تعداد زیرسطحی‌ها نشان می‌دهد.



شکل (۹): مقایسه سربار مخابراتی بین روش پیشنهادی و روش RSA.

۶-۲- هزینه محاسباتی

در این بخش، هزینه محاسباتی بین دو روش مذکور در زیرسطحی‌ها و در SCC آورده می‌شود. جدول (۲) نتایج مشاهدات حاصل از اجرای یک تابع رمزنگاری هش، یک امضا RSA و یک تصدیق امضا RSA را نشان می‌دهد که در ماشین Intel Pentium IV 3.0-GHz به اجرا در آمده اند [۴۹]. در روش پیشنهادی، تعداد تابع هشی که هر زیرسطحی برای یک درخت تولید می‌کند را می‌توان از رابطه زیر به دست آورد:

$$N = 2^n + 2^{n-1} + \cdots + 2^1 + 1 = 2^{n+1} - 1 \qquad (۱۳)$$

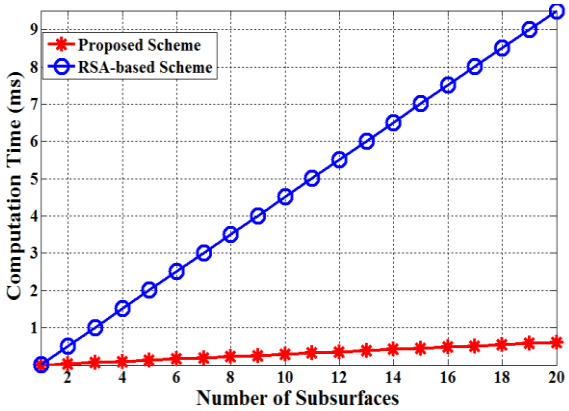
که در آن، N تعداد مقادیر هش تولید شده در یک درخت و n ارتفاع درخت‌های تولید شده می‌باشد. حال با توجه به جدول (۲) با فرض $n = 7$ مقدار زمان مورد نیاز برای تولید یک درخت در هر زیرسطحی برابر با 0.02346 ms می‌باشد. همچنین هر امضا الگوریتم نیز طبق جدول (۲) به ۲/۲۵ ms زمان نیاز دارد. در حالی که برای ارسال هر پیام در فرستنده، هزینه محاسباتی برای هر زیرسطحی در روش درخت مرکل نسبت به روش RSA مقداری قابل چشم‌پوشی است. روش ارائه‌شده در این مقاله دارای هزینه محاسباتی بسیار کمتری نسبت به روش RSA در زیرسطحی‌ها می‌باشد.

اما در گیرنده، برای اینکه منبع پیام توسط SCC تصدیق گردد، نیاز است تا API آن محاسبه شده که در این‌صورت SCC باید هفت تابع هش را محاسبه نماید. بنابراین میزان هزینه محاسباتی صرف شده برای هر پیام در روش ارائه‌شده برابر 0.000644 ms می‌باشد. در حالی که طبق جدول (۲) و در روش اعتبار بخشیدن به امضا RSA، پیچیدگی محاسباتی برابر ۰/۱ ms خواهد بود. شکل (۱۰) هزینه محاسباتی در SCC را با استفاده از دو روش ارائه‌شده در این مقاله و RSA نشان می‌دهد. با توجه به نتایج مشخص است که روش ارائه‌شده در این مقاله

دارای هزینه محاسباتی بسیار کمتری نسبت به روش RSA در SCC می‌باشد.

جدول (۲): زمان اجرای عملگرهای رمزنگاری.

عملگر رمزنگاری	زمان مورد نیاز برای اجرا
تابع هش یک‌طرفه	۰/۰۰۰۰۹۲ ms
یک امضا RSA	۲/۲۵ ms
یک تصدیق امضا RSA	۰/۱ ms



شکل (۱۰): هزینه محاسباتی در روش پیشنهادی و روش RSA در SCC.

۷- نتیجه‌گیری

در این مقاله پروتکلی امن و بهینه مبتنی بر درخت هش مرکل و با استفاده از سوت دلفین برای ارتباطات آکوستیک زیرآبی ارائه شده است. شبیه‌سازی بخش دو نشان می‌دهد که به دلیل ویژگی‌های مناسب سوت دلفین مانند ضرایب فرکانسی پایین و خواص همبستگی عالی، می‌توان از آن به عنوان حامل اطلاعاتی استفاده نمود که علاوه بر پنهانی و آشکارسازی مناسب پیام، میزان خطای بیت موجود در کانال زیرآبی را بدون استفاده از روش‌های کدینگ کانال تا حد بسیار زیادی کاهش دهد. همچنین برای بخشیدن امنیت کامل به سامانه، از روشی مبتنی بر درخت هش مرکل و الگوریتم AES استفاده شده است. تحلیل امنیتی نشان می‌دهد که پروتکل پیشنهادی با مقاومت در برابر همه تهدیدات موجود در کانال زیرآبی (حملات بازپخش، ارسال پیام جعلی، تحلیل پیام و اصلاح پیام)، سه شرط مهم تصدیق صحت، محرمانگی و بی‌عیبی را برآورده می‌سازد. همچنین ارزیابی عملکرد و میزان بهینگی نشان می‌دهد که روش پیشنهادی با توجه به محدودیت‌های موجود در محیط زیرآب، در دو مولفه سرریز مخابراتی و هزینه محاسباتی و پردازشی دارای عملکردی مناسب و سبک‌وزن بوده که آن را برای پیاده‌سازی در سامانه‌های زیرآبی، عملی می‌سازد.

۸- مراجع

[1] A. Falahati, B. Woodward, and S. C. Bateman, "Underwater Acoustic Channel Models for 4800 b/s QPSK Signals," IEEE J. Oceanic Engineering, vol. 19, no. 1, pp. 12-20, 1991.

[2] A. Zielinski, Y. Yoon, and L. Wu, "Performance Analysis of Digital Acoustic Communication in a Shallow Water Channel," IEEE J. Oceanic Engineering, vol. 20, no. 4, pp. 293-299, 1995.

[3] P. A. Walree and R. Otnes, "Ultrawideband Underwater Acoustic Communication Channels," IEEE J. Oceanic Engineering, vol. 38, no. 4, pp. 678-688, 2013.

[4] A. C. Singer, J. K. Nelson, and S. S. Kozat, "Signal Processing for Underwater Acoustic Communications," IEEE Communication Magazine, vol. 47, no. 1, pp. 90-96, 2009.

[5] T. C. Yang, "Correlation-Based Decision-Feedback Equalizer for Underwater Acoustic Communications," IEEE J. Oceanic Engineering, vol. 30, no. 4, pp. 865-880, 2005.

[6] S. Hwang and P. Schniter, "Efficient Multicarrier Communication for Highly Spread Underwater Acoustic Channels," IEEE J. Selected Areas in Communications, vol. 26, no. 9, pp. 1674-1683, 2008.

[7] M. Stojanovic and J. Preisig, "Underwater Acoustic Communication Channels: Propagation Models and Statistical Characterization," IEEE Communication Magazine, vol. 47, no. 1, pp. 84-89, 2009.

[8] M. khishe, M. R. Mosavi, and M. Kaveh, "Improved Migration Models of Biogeography-Based Optimization for Sonar Dataset Classification by using Neural Network," J. Applied Acoustics, vol. 118, no. 3, pp. 15-29, 2017.

[9] J. Ling, H. He, J. Li, and W. Roberts, "Covert Underwater Acoustic Communications: Transceiver Structures, Waveform Designs and Associated Performances," IEEE Conf. Oceans 2010 MTS/IEEE Seattle, pp. 1-10, 2010.

[10] J. Ling, H. He, J. Li, and W. Roberts, "Covert Underwater Acoustic Communications," J. Acoust. Soc. Am., vol. 128, no. 5, pp. 2898-2909. 2010.

[11] G. Leus and P. A. Walree, "Multiband OFDM for Covert Acoustic Communications," IEEE J. Selected Areas in Communications, vol. 26, no. 9, pp. 1662-1673, 2008.

[12] G. Leus, P. Van Walree, J. Boschma, C. Fanciullacci, H. Gerritsen, and P. Tusoni, "Covert Underwater Communications with Multiband OFDM," IEEE Conf. Oceans, pp. 1-8, 2008.

[13] Z. Hijaz, and V. S. Frost, "Exploiting OFDM Systems for Covert Communication," in Military Communications Conference, pp. 2149-2155, 2010.

[14] P. Van Walree, E. Sangfelt, and G. Leus, "Multicarrier Spread Spectrum for Covert Acoustic Communications," IEEE Conf. Oceans, pp. 264-271, 2008.

[15] T. C. Yang and W. B. Yang, "Low Probability of Detection Underwater Acoustic Communications using Direct-Sequence Spread Spectrum," J. Acoust. Soc. Am, vol. 124, no. 6, pp. 3632-3647, 2008.

[16] T. C. Yang and W. B. Yang, "Performance Analysis of Direct-Sequence Spread-Spectrum Underwater Acoustic Communications with Low Signal-to-Noise-Ratio Input Signals," J. Acoust. Soc. Am, vol. 123, no. 2, pp. 842-855, 2008.

[17] S. Liu, G. Qiao, and A. Ismail, "Covert Underwater Acoustic Communication using Dolphin Sounds," J. Acoust. Soc. Am, vol. 133, no. 4, pp. 300-306, 2013.

[18] Y. Jia, G. Liu, and L. Zhang, "Bionic Camouflage Underwater Acoustic Communication based on Sea Lion Sounds," International Conf. Control, Automation and Information Sciences, pp. 1-5, 2015.

[19] X, Han, J, Yin, P. Du, and X. Zhang, "Experimental Demonstration of Underwater Acoustic Communication Using Bionic Signals," J. Applied Acoustics, vol. 78, no. 2, pp. 7-10. 2014.

[20] B. K. Branstetter, J. S. Trickey, K. Bakhtiari, A. Black, and H. Aihara, "Auditory Masking Patterns in Bottlenose Dolphins (Tursiops Truncatus) with Natural, Anthropogenic, and Synthesized Noise," J. Acoust. Soc. Am, vol. 133, no. 3, pp. 1811-1819, 2013.

[21] C. Capus, A. Y. Pailhas, K. Brown, and D. M. Lane, "Bio-Inspired Wideband Sonar Signals based on Observations of The Bottlenose Dolphin (Tursiops Truncatus)," J. Acoust. Soc. Am, vol. 121, no. 1, pp. 594-605, 2007.

[22] S. Liu, G. Qiao, Y. Yu, L. Zhang, and T. Chen, "Biologically Inspired Covert Underwater Acoustic Communication using High Frequency Dolphin Clicks," IEEE Conf. Oceans, pp. 1-5, 2013.

[23] L. Songzuo, M. Tianlong, and Q. Gang, "Bionic Communication by Dolphin Whistle with Continuous-Phase based on MSK Modulation," International Conf. Signal Processing, pp. 1-5, 2016.

[24] R. Aubauerb and W. W. L. Au, "Phantom Echo Generation: A New Technique for Investigating Dolphin Echolocation," J. Acoust. Soc. Am, vol. 104, no. 3, pp. 1164-1169, 1998.

[25] M. W. Muller, J. S. Allen, and W. W. L. Au, "Time-Frequency Analysis and Modeling of The Backscatter of Categorized Dolphin Echolocation Clicks for Target Discrimination," J. Acoust. Soc. Am, vol. 124, no. 1, pp. 656-665, 2008.

[26] R. M. López and C. Bazúa, "Who Is Whistling? Localizing and Identifying Phonating Dolphins in Captivity," J. Applied Acoustics, vol. 71, pp. 1057-1062, 2010.

[27] https://www.macaulaylibrary.org/

[28] Y. Huang, S. Zhou, Z. Shi, and L. Lai, "Channel Frequency Response based Secret Key Generation in Underwater Acoustic Systems," IEEE Trans. Wireless Communications, vol. 15, no. 9, pp. 5875-5888, 2016.

[29] H. Kulhandjian, T. Melodia, and D. Koutsonikolas, "Securing Underwater Acoustic Communications through Analog Network Coding," Proc. SECON, pp. 1-9, 2014.

[30] B. G. Mobasseri and R. S. Lynch, "Information Embedding in Sonar by Modifications of Time-Frequency Properties," IEEE J. Oceanic Engineering, vol. 41, no. 1, pp. 139-154, 2016.

[31] M. C. Domingo, "Securing Underwater Wireless Communication Networks," IEEE Communication Magazine, vol. 8, no. 1, pp. 22-28, 2011.

[32] G. Han, J. Jiang, N. Sun, and L. Shu, "Secure Communication for Underwater Acoustic Sensor Networks," IEEE Communication Magazine, vol. 53, no. 8, pp. 54-60, 2015.

[33] G. Dini and A. L. Duca, "A Secure Communication Suite for Underwater Acoustic Sensor Networks," Sensors- Basel, vol. 12, no. 11, pp. 133-58, 2012.

[34] Y. Chen, Y. Lin, and S. Lee, "A Mobicast Routing Protocol in Underwater Sensor Networks," IEEE Conf. Wireless Communications and Networking, pp. 510-515, 2011.

[35] S. Misra, S. Dash, M. Khatua, A.V. Vasilakos, and M. S. Obaidat, "Jamming in Underwater Sensor Networks: Detection and Mitigation," IET Commun., vol. 6, no. 14, pp. 2178-88, 2012.

[36] X. Lu and Z. Yonghua, "Modeling The Wormhole Attack in Underwater Sensor Network," IEEE 8th International Conf. Wireless Communications, Networking and Mobile Computing, pp. 1-4, 2012.

[37] Y. Luo, L. Pu, Z. Peng, and Z. Shi, "RSS-Based Secret Key Generation in Underwater Acoustic Networks: Advantages, Challenges, and Performance Improvements," IEEE Communication Magazine, vol. 54, no. 2, pp. 32-38, 2016.

[38] C. Lal, R. Petrocci, M. Conti, and J. Alves, "Secure Underwater Acoustic Networks: Current and Future Research Directions," IEEE 3th Conf. Underwater Communications and Networking, pp. 1-5, 2016.

[39] H. Li, Y. He, X. Cheng, H. Zhu, and L. Sun, "Security and Privacy in Localization for Underwater Sensor Networks," IEEE Communication Magazine, vol. 53, no. 11, pp. 56-62, 2015.

[40] G. Ateniese, et al., "SecFUN: Security Framework for Underwater Acoustic Sensor Networks," IEEE 3th Conf. Oceans, pp. 1-9, 2015.

[41] M. Ahmed, M. Salleh, and M. Channa, "Routing Protocols Based on Node Mobility for Underwater Wireless Sensor Network: A Survey," J. Network and Computer Applications, vol. 78, pp. 242-252, 2017.

[42] Y. Chen, and Y. Lin, "Mobicast Routing Protocol for Underwater Sensor Networks," IEEE Sensors Jounal, vol. 13, no. 2, pp. 737-749, 2013.

[43] R. Merkle, "Protocols for Public Key Cryptosystems," in Proc. IEEE Symp. Security and Privacy, pp. 122-134, 1980.

[44] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, "An Efficient Merkle-Tree-Based Authentication Scheme for Smart Grid," IEEE Systems Journal, vol. 8, no. 2, pp. 655-663, 2014.

[45] Y. Liu, C. Cheng, T. Gu, T. Jiang, and X. Li, "A Lightweight Authenticated Communication Scheme for Smart Grid," IEEE Sensors Jounal, vol. 16, no. 3, pp. 836-842, 2015.

[46] N. Ferguson, R. Schroeppel, and D. Whiting, "A Simple Algebraic Representation of Rijndael," in Proc. Sel. Areas Cryptogr., pp. 103-111, 2001.

[47] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," Commun. of the ACM, pp. 120-126, 1978.

[48] W. Diffie, and M. E. Hellman, "New Directions in Cryptography," IEEE Trans. Information Theory, vol. 22, no. 6, 1976.

[49] W. Dai, Crypto++ 5.6.2 Benchmarks 2013. [Online]. Available: http:// www.cryptopp.com/.

[50] E. Shafiee, M. R. Mosavi and M. Moazedi, "Detection of Spoofing Attack Based on Multi-Layer Neural Network in Single-Frequency GPS Receivers", Journal of Electronical & Cyber Defence, Vol. 3, No. 1, pp.69-80, 2015. (in persian).

Journal of Electronical & Cyber Defence
Vol. 6, No. 2, 2018, Serial No. 22

Covert and Secure Underwater Acoustic Communication using Merkle Hash Tree and Dolphin Whistle

M. R. Mousavi*, M. Kaveh

*Department of Electrical Engineering, Iran University of Science and Technology, Tehran, Iran

(Received: 03/04/2016, Accepted: 06/06/2017)

ABSTRACT

The unique characteristics of the Underwater Acoustic Communication (UWAC) channel cause the UWAC systems to be very vulnerable to the malicious attacks. So, the bionic-based UWAC has been used due to its good covert performance, and its suitable frequency and correlation properties. It may not be covert in all the underwater environments, or an adversary can detect the message anyway. Therefore, this paper aims at proposing an improved Merkle hash tree based secure scheme that can resist the current possible underwater attacks, i.e., the replay attack, the fabricated message attack, the message altering attack, and the analyst attack. The security analysis indicates that the proposed scheme is resilient to the mentioned attacks. Also, the performance evaluations show that the proposed scheme is proportional to the UWAC limitations due to its efficiency in terms of energy consumption, communication overhead, and computation cost.

Keywords: Bionic Signals, Covert and Secure UWAC, Dolphin Whistle, Malicious Attacks, Merkle Hash Tree

* Corresponding Author Email: M_Mosavi@iust.ac.ir