عنوان مقاله:
انتخاب الگوریتم مطلوب مکالمات در بستر اینترنت مبتنی برشبیه سازی

محل انتشار:
فصلنامه فناوری اطلاعات و ارتباطات انتظامی, دوره 2, شماره 8 (سال: 1400)

تعداد صفحات اصل مقاله: 17

نویسندگان:
بهزاد لک - *استادیار، گروه فناوری اطلاعات و ارتباطات، دانشگاه علوم انتظامی امین، تهران، ایران*

سعید بختیاری - *استادیار گروه فتا، دانشگاه علوم انتظامی امین- تهران -ایران*

سید مصطفی رضوانی - *گروه فناوری اطلاعات و ارتباطات، دانشگاه علوم انتظامی امین، تهران، ایران*

خلاصه مقاله:
فنآوری ویپ مزایای قابل توجهی برای مشتریان و ارائه دهندگان خدمات ارتباطی مانند صرفه جویی در هزینه، خدمات رسانه ای خوب، قابلیت انتقال تلفن و خدمات، تحرک و ادغام با سایر برنامه ها را فراهم می آورد. با این وجود، راه اندازی فناوری ویپ با چالش های بسیاری مواجه است؛ مانند پیچیدگی معماری، مسائل مربوط به قابلیت همکاری، مسائل مربوط به کیفیت خدمات و چالش های 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 NS۲ و نسخه NS۲.۳۵ می باشد که تحت لینوکس و کد متن باز می باشد. 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 می باشد و همچنین زمان رمزگذاری، رمزگشایی، 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.

کلمات کلیدی:
ویپ, شبکه تلفن سنتی, امنیت, پروتکل های امنیتی