**شناسایی تهاجم کرم چاله در شبکه حسگر بی سیم**

**جواد سلمانیان**

**دانشجوی دکتری تخصصی مهندسی کامپیوتر-نرم افزار**

**Javadsalmanian80@yahoo.com**

**سمیه ارمند پیشه**

**Noonoosh59@gmail.com**

**دانشجوی کارشناسی ارشد برنامه ریزی درسی**

**مرجان سلمانیان**

**Noonooosh93@gmail.com**

**کارشناسی مهندسی برق –دانشگاه آزاد اسلامی واحد کرج**

چکيده : شبکه­های حسگر بی سیم، متشکل از گره­های متعددی بوده که به همراه خود خصیصه­های آسیب پذیری همچون انتقال در فضای باز، خودسازمان دهی بدون ساختار اصلاح شده، محدودیت منبع، حافظه و قابلیت­های محاسباتی دارند. این مشخصه­ها، شبکه را مستعد ایجاد حملات مخربی همچون کرم چاله، سیاه چاله، سیبیل، غرقه سازی می نماید. حملات کرم چاله که از لحاظ ساختاری به سه نوع باز، بسته و نیمه باز تقسیم می شوند، با هدف تخریب مسیریابی ایجاد می­شوند. در سناریو حملات کرم چاله، گره مخرب بسته­های داده­ای را در هنگام انتقال بسته فیمابین ایستگاه­های پایه جذب می نماید. در این حملات دو یا چند گره مخرب، تونلی مجازی را برای هدایت ترافیک داده­ای کشف شده، ایجاد می نمایند. این نوشتار تشخیص حمله کرم چاله را با استفاده از ارزیابی نتایج شبیه سازی برای ایجاد سطوح امنیتی بالاتر در شبکه حسگر ارائه نموده است.

كليد واژه­ها: امنیت، شبکه حسگر، شبیه ساز NS-2،تهاجم کرم چاله،

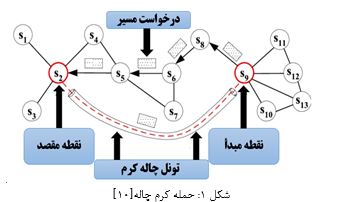
1.مقدمه

با رشد و توسعه سیستم­های توزیع شده فراگیر ، شاهد تکنولوژی­های نوین و کارآمدی همچون سیستم­های خانگی ، سیستم­های الکترونیکی مراقبت از سلامت و شبکه­های­ حسگر هستیم. سیستم­های فراگیر توزیعی کوچک، سیار و مبتنی بر باتری هستند. ویژگی مهم در سیستم­های فراگیر، عدم وجود کنترل و سرپرستی انسانی است. این عامل منجر به کاربرد شبکه حسگر در محیط­های مخاطره آمیز و پرهزینه­ای برای حضور انسان، همچون محیط­های نظامی و نظارت میدان جنگ، سیستم­های تشخیص سیل، نظارت محیط زیست، تشخیص صدا و لرزش، تشخیص زمین لرزه، نظارت پزشکی و تشخیص آتشفشان­های فعال می گردد[1]. علیرغم اینکه شبکه­های حسگر بی سیم در بعد عملیاتی ویژگی­های قابل توجهی همچون هزینه نصب پایین و نیز عدم مراقبت عملیات شبکه را دارا هستند، ولی بعلت فضای خالی تدافعی فیزیکی(عدم وجود دروازه یا سوییچ برای مشاهده و نظارت بر جریان اطلاعات) و همچنین ذات آسیب پذیر این شبکه­ها مبنی بر محدودیت منبع انرژی، امنیت این شبکه­ها همواره مواجه با مخاطرات، حملات مضّر و خطرآفرین علی الخصوص در شبکه­هایی با درجه اهمیت بالاتر ایجاد می نماید[2,3]. به منظور اجرای شبکه حسگر بی سیم در حالت امن، هر نوع دسترسی غیر­مجاز و یا دستکاری اطلاعات گره­ها و ترافیک عبوری می بایست با نرخ صحیح بالا به شکلی کارآمد تشخیص داده شود. در راستا مراقبت و محافظت از شبکه حسگر بی سیم با در نظر گرفتن ماهیت شبکه مذکور و نیز چالش مصرف انرژی، خطوط اول و دوم دفاعی(رمزنگاری و سیستم تشخیص نفوذ ) مورد استفاده قرار خواهند گرفت. بدیهی است خطوط دیگر دفاعی همچون سیستم ممانعت از نفوذ و ظرف عسل و سایر روش­های مرسوم نیازمند الگوریتم­های کاراتر جهت کمینه کردن مصرف انرژی در شبکه­های با اهمیت هستند. شبکه­ حسگر بی سیم، مصون از مخاطرات اتلاف و انهدام نیست. برخی از این مخاطرات با شبکه­های موردی سیار یکسان و مابقی بطور خاصه برای شبکه­های حسگر هستند. پژوهشگران متعددی نسبت به پژوهش پیرامون راهکارهای مسیریابی و حملات امنیتی اقدام نموده اند[3,4,5,6,7,8,9].

از طرفی دیگر، پژوهش­های متعددی پیرامون ایجاد محدودیت در مواجهه با حملات کرم چاله انجام شده که، عمده این روش­ها به دو مکانیزم تشخیص و ممانعت پرداخته اند. از اینرو، راهکارهای متعددی همچون راهکارهای مبتنی بر زمان-مکان، تحلیل ایستا، تحلیل گراف و نیز راهکارهای مبتنی بر همسایگان برای مقابله با حمله کرم چاله وجود دارد.

# 2-حمله کرم چاله

حمله کرم چاله، حمله ای مسیریابی است که بازخورد حمله در لایه شبکه صورت می پذیرد[,1110]. این حمله مستلزم درج حداقل دو گره مخرب است. این دو گره توسط یک ارتباط قوی کم تأخیر به یکدیگر، متّصل هستند. به این ارتباط که منجر به ایجاد اختلال و انحراف در پروتکل مسیریابی می گردد، تونل نیز گفته می شود. برای مثال، می توان به یک اتّصال سیمی، اتّصال نوری، اتّصال اِتِرنِت و انتقال بدون سیم برد بالا، برای ارتباط قوی اشاره داشت. گره مخرّب، در بخشی بسته­ها را از شبکه دریافت نموده و سپس با توجه به ارتباط قوی خود با گره ای در بخش دیگری از شبکه، بسته­ها را هدایت و ارسال می نماید . ساخت اتصال و یا ارسال مجدد بیت­ها می تواند بصورت انتخابی، صورت پذیرد. حمله مذکور، در زمانیکه گره­ها نسبت به کشف اطلاعات همسایه خود مبادرت می ورزند، انجام می گیرد. شایان ذکر است برای این سناریو خطرناک، نیاز به هیچگونه سازشی با حسگر­ها نیست. بطور عمومی حملات کرم چاله، در پروتکلAODV در فاز کاوش مسیر، بواسطه ساخت مسیر همسایه جعلی ایجاد شده توسط گره نفوذی کرم چاله، صورت می پذیرد[12]. آسیب پذیری در حملات کرم چاله بعلّت نوع غیر فعّال حمله و عدم نیاز به اطلاعات پیرامون تأسیسات رمزنگاری شبکه، بسیار بالاست. از اینرو منجر به ایجاد قطع و تداخل کامل در سیستم می گردند[10،11،12].



حملات کرم چاله، به دسته­های زیر تقسیم می گردند[12].

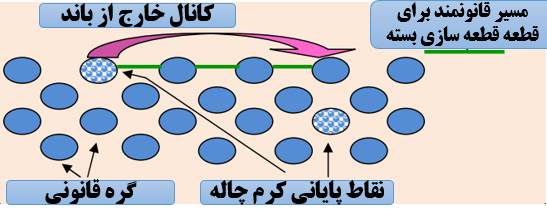
\* حمله کرم چاله با استفاده از کانال خارج از باند : در این کرم چاله، پهنای باند بالای اختصاصی در نقاط پایانی به منظور ایجاد اتّصال کرم چاله ایجاد می گردد.

\* حمله کرم چاله با استفاده از قطعه قطعه سازی بسته­ها (هر بسته از مسیر قانونی، مسیریابی می گردد.)

\* حمله کرم چاله با استفاده از انتقال با قدرت بالا ،(تنها یک گره مخرّب با قابلیّت انتقال بالا وجود داشته که بسته­ها را به منظور دنبال نمودن مسیر عبور از آن، جذب می کند.)

\* حمله کرم چاله با استفاده از تقویت بسته (تنها یک گره مخرّب که بسته را بین 2 گره دور از هم بازپخش نموده و همسایگان جعلی ساخته می شوند).

\* حمله کرم چاله با استفاده از جعل و انحراف پروتکل گره­ مخرّب (کرم چاله را توسط هدایت بسته­ها بدون حمایت و نیز برخلاف گره قانونی، ایجاد می نمایند).



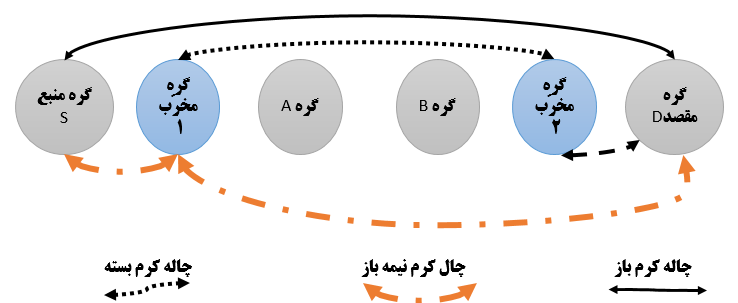
شکل 2: کرم چاله با استفاده از کانال خارج از باند و قطعه قطعه سازی [10]

رفتار هدایت بسته نقاط پایانی کرم چاله و همچنین تمایل آنها به مخفی سازی و نمایش هویّت­ها، سه مدل مجزا را پدید می آورد. در زیرD,S,M1,M2 به ترتیب، منبع و مقصد و دو گره مخرّب هستند[13].

\* کرم چاله باز (منبع، مقصد گره­ها و همچنین هر دو گره مخرّب نمایان هستند. هویّت گره­های B و A در مسیر پیمایش شده، مخفی نگه داشته می شود.)

\* کرم چاله نیمه باز (گره مخرّب اوّل در کنار منبع قابل مشاهده است، در حالیکه گره مخرّب دوم مخفی نگه داشته شده است. در نتیجه مسیر پیمایش S,M1,Dبازای بسته­های ارسالی از S به D است.)

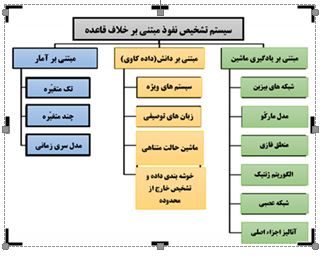
\* کرم چاله بسته (در این مدل حمله، هویّت­ها از منبع به مقصد پنهان بوده و منجر به ایجاد این سناریو می گردد که منبع و مقصد خود را در یک گذر همدیگر ببیند، از اینرو همسایه­های جعلی ایجاد خواهند شد).



شکل 3: کرم چاله­های باز، نیمه باز و بسته]10-11[

## 2-1تشخیص کرم چاله با استفاده از شبیه سازی

سیستم­های تشخیص نفوذ بر اساس عملکرد، به سه گروه تشخیص مبتنی بر خلاف قاعده، تشخیص مبتنی بر بد رفتاری و تشخیص مبتنی بر خصوصیات طبقه بندی می گردند. راهکار خلاف قاعده، مبتنی بر مدلسازی رفتاری آماری است. رفتار عادی عملیاتی اعضاء برای سیستم تشریح گشته و مقدار قطعی انحراف از رفتار عادی، تحت عنوان پرچم خلاف قاعده بیان می گردد. از معایب این روش می توان به این موضوع اشاره داشت که پروفایل های عادی باید در فواصل زمانی معین به علت تغییر سریع رفتار شبکه، بروزرسانی گردند. از مزایای این روش می­توان به کاربرد آن در جهت تشخیص حملات ناشناخته و یا حملاتی که با آن مواجه شده اشاره نمود[15] . تشخیص خلاف قاعده بر پایه طیبعت پردازشی ایجاد شده در مدل رفتاری به سه دسته مبتنی بر آمار، تشخیص مبتنی بر دانش و مبتنی بر یادگیری ماشینتقسیم می گردند. شکل2- طبقه بندی سیستم های تشخیص نفوذ مبتنی بر خلاف قاعده را بر اساس الگوریتم های تشخیص آنها، تشریح ساخته است.



در طی شبکه،ترافیک خروجی ظبط گردیده و پروفایلی که رفتار اتفاقی و ناگهانی آنرا بازنمایی کند، تولید می گردد. هنگامیکه شبکه در شرایط عادی(فاقد جریان حمله) به سر می برد، پروفایل مرجعی نیز ساخته می شود. بعد از آنکه شبکه مورد نظارت قرار خواهد گرفته و پروفایل­ها در فواصل زمانی معین تولید می­گردند. از اینرو با مقایسـه پروفایل مرجع، یک رتبه خلاف قاعده تولید خواهد گشت. اگر این رتبه از آستانه مشخصی عبور نماید، سیســتم تشخیص نفوذ، پرچـم وقـوع بدرفتاری را به آن تخصیص خواهد داد.

## 2-2تشخیص کرم چاله با استفاده از شبیه سازی

پروتکل­های مسیریابی بواسطه ارزیابی کیفیت اتصال با استفاده از تخمین کیفیت بسته داده­ای دریافتی و دسترسی به اطلاعات مقصد، کمک شایانی در تشخیص حملات می نمایند. در این نوشتار، کیفیت بسته­های دریافتی و تعداد کل بسته­های تولید شده در طی 2 شبکه امن و نا امن با ایجاد سناریو کرم چاله و همچنین سایر پارامترهای اساسی همچون توان عملیاتی، میزان تأخیر، ناپایداری در تأخیر و ... ارزیابی شده است.

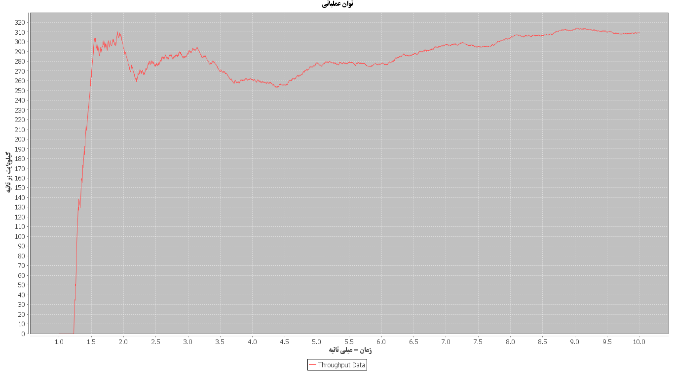
بسته­های داده­ای انتقالی در شبکه حسگر بی سیم، بر فراز رسانه انتقال بدون سیم منتقل می گردند. از اینرو هر گره توانایی دریافت و تحلیل بسته داده­ای گره­های مجاور خود را داراست.

شبیه سازی تشخیص حمله کرم چاله، با استفاده از شبیه ساز NS-2 و تحت کد TCL ایجاد شده است جدول- 1 بیانگر پارامترهای مورد کاربرد است. [14-18]

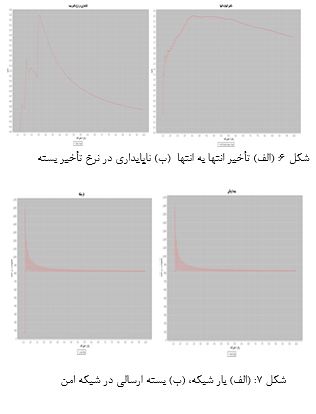
جدول 1: پارامترهای شبکه

|  |  |
| --- | --- |
| 21 | تعداد گره |
| 500 m2\*500 | ابعاد شبکه |
| AODV | پروتکل مسیریابی |
| 50 ms | بیشینه بسته در IFQ |
| 10.0 | زمان خاتمه شبیه سازی |

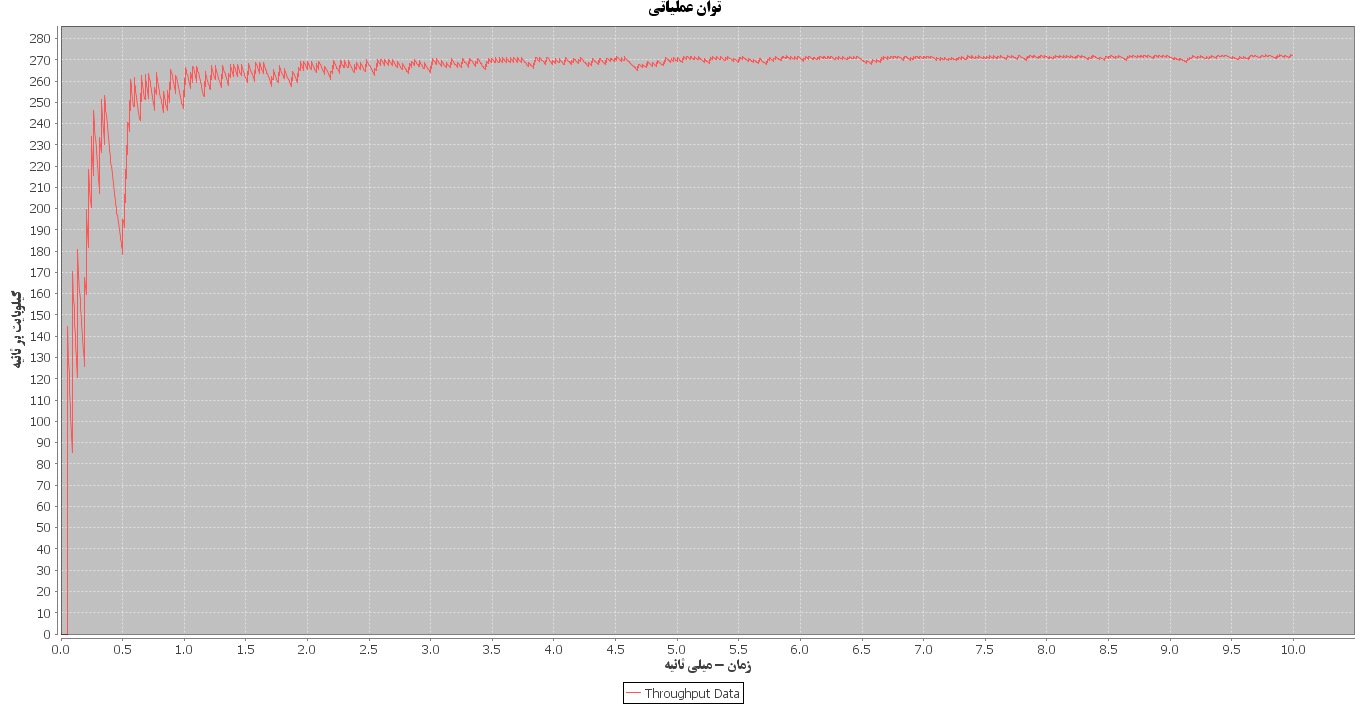
بعد از ایجاد نیازمندی­های حمله، با ارزیابی نتایج در دو حالت امن و نا امن، توانایی تشخیص حمله کرم چاله میسور خواهد گشت. شایان ذکر است که نتایج در دو سطح شبکه(مسیریابی و عامل)، گردآوری شده است. از اینرو نتایج بدست آمده در حالت امن با ردیابی در سطح عاملین از قرار زیر است:



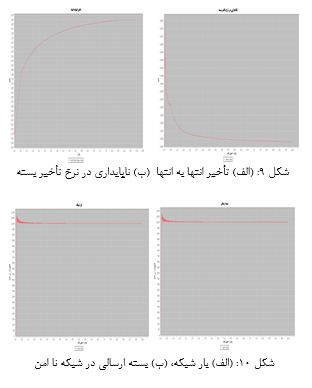
شکل 5: توان عملیاتی در حالت امن



در سویی دیگر با وجود حمله کرم چاله نیمه باز، نتایج زیر بدست آمده است.



شکل 8: توان عملیاتی در حالت نا امن و ایجاد سناریو مخرب کرم چاله



در تحلیل و اخذ خروجی شبکه در مدل ردیابی عامل AGT مشاهده می شود کهتوان عملیاتی در حالت حمله بصورت ثابت در پیک زمانی خاصی در حال افزایش است. این در حالیست که در حالت امن شبکه، توان عملیاتی بصورت گسسته در پیک­های زمانی متفاوت در حال ازدیاد است.

تأخیر انتها به انتها در طی حمله بصورت نمایی در حال فزونی یافتن است و این درحالیست که در حالت امن شبکه، این نرخ در حال کاهش است.

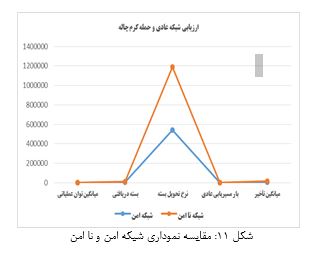
در وضعیت امن شبکه، پارامتر ناپایداری نرخ تأخیر در بازه زمانی 1 تا 3 میلی ثانیه افزایش و بعد کاهش یافته است. این در حالیست که در حالت نا امن، در نیم میلی ثانیه آغازین شبیه سازی، ناپایداری شدیدی در نرخ تأخیر بسته داریم که خود بیانگر رخداد حمله است.

در حالت امن، بار شبکه بعد از تناوب تا 3 میلی ثانیه آغاز شبیه سازی، جریان پیوسته­ای از بار شبکه را دنبال می کند. در حالت نا امن، بار شبکه در نیم میلی ثانیه آغازین، فزونی یافته است.

در نمودار بسته ارسالی، شاهد آن هستیم که در حالت امن بعد از گذشت 3 میلی ثانیه، تناوب به حالت پایدار خود رسیده و ادامه می یابد و این در حالیست که در حالت حمله در ابتدای نیم میلی ثانیه آغاز شبیه سازی، بسته های انبوهی انتقال یافته اند.

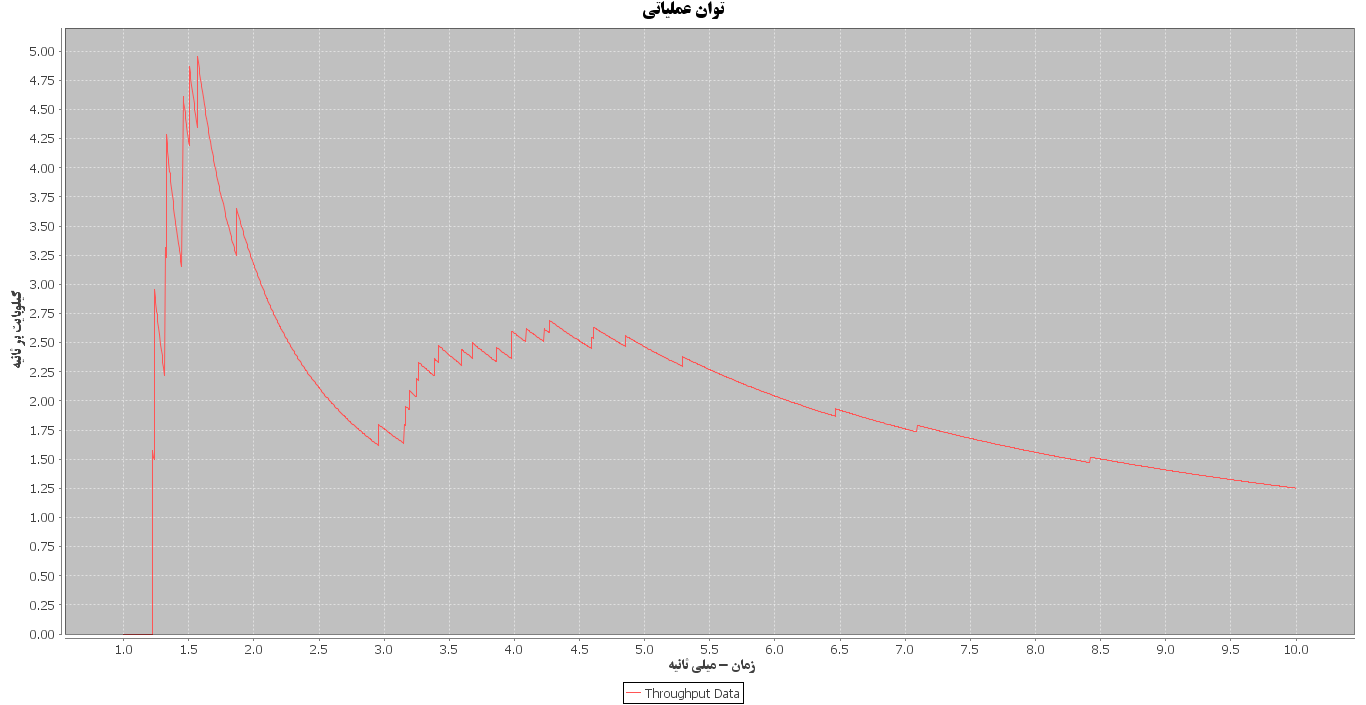
جدول 2: ارزیابی پارامترهای اساسی شبکه

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| میانگین تأخیر | بار مسیریابی عادی | نرخ تحویل بسته |  | بسته دریافتی | میانگین توان عملیاتی | نوع شبکه |
| 8996.44 | 0.618 | 539900 |  | 5399 | 2174.19 | امن |
| 6667 | 0.054 | 648900 |  | 6489 | 1354.91 | نا امن |

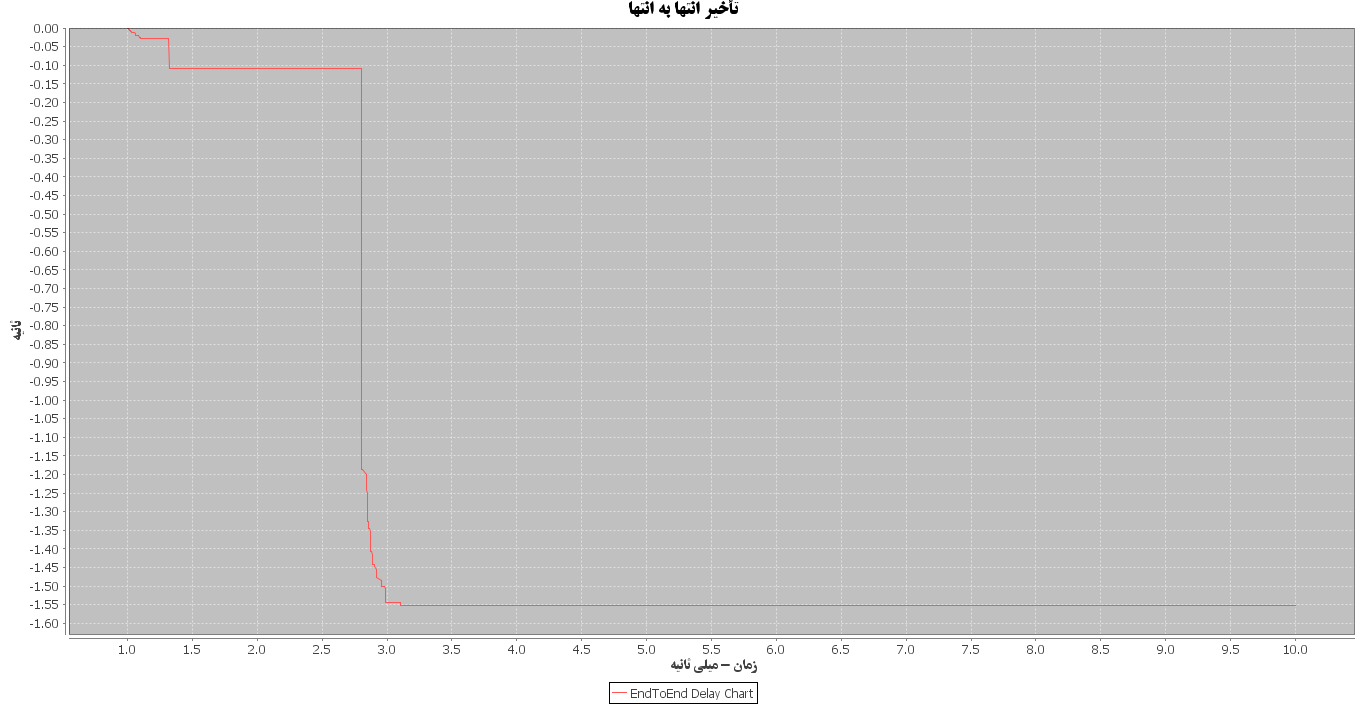


شکل 11: مقایسه نموداری شبکه امن و نا امن

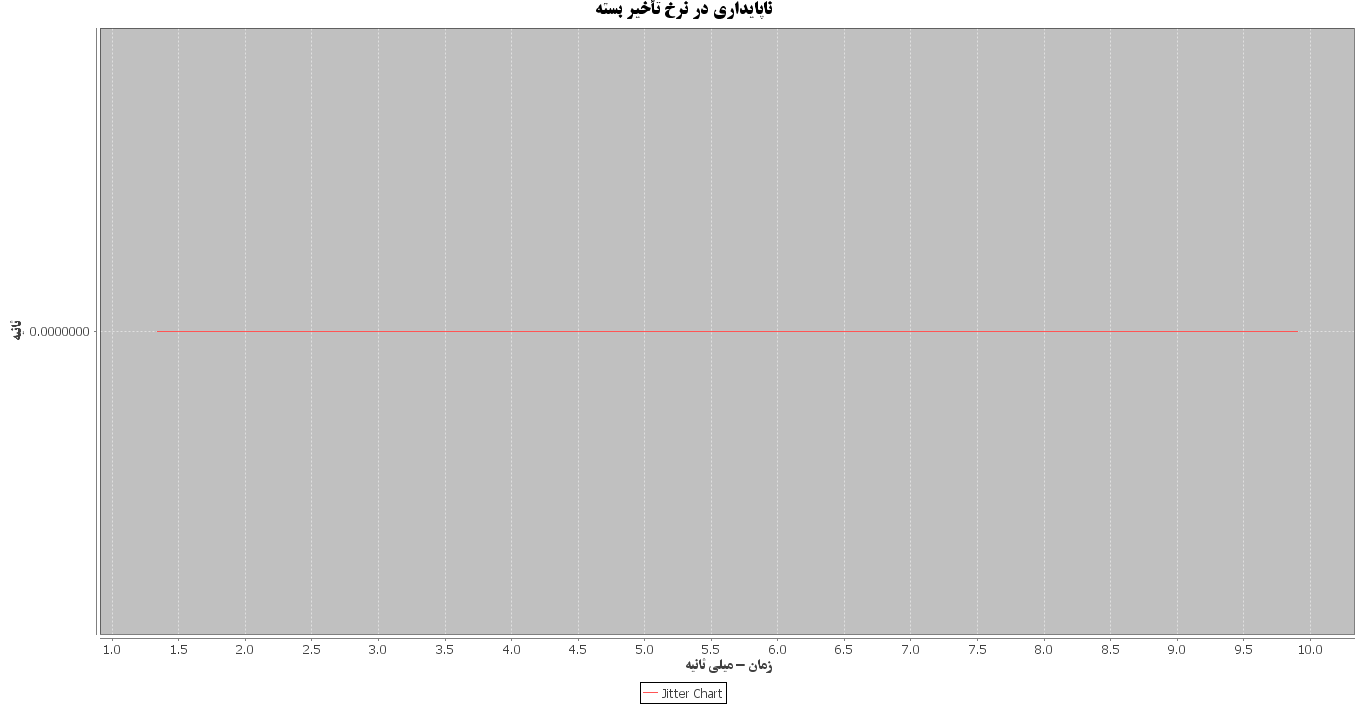
از سویی دیگر برای اطمینان از نتایج و پربارتر بودن تحلیل نتایج، و استخراج بواسطه تحلیل و ردیابی سطح مسیریابی شبکه یا RTR صورت پذیرفته که نتایج آن از قرار زیر است:



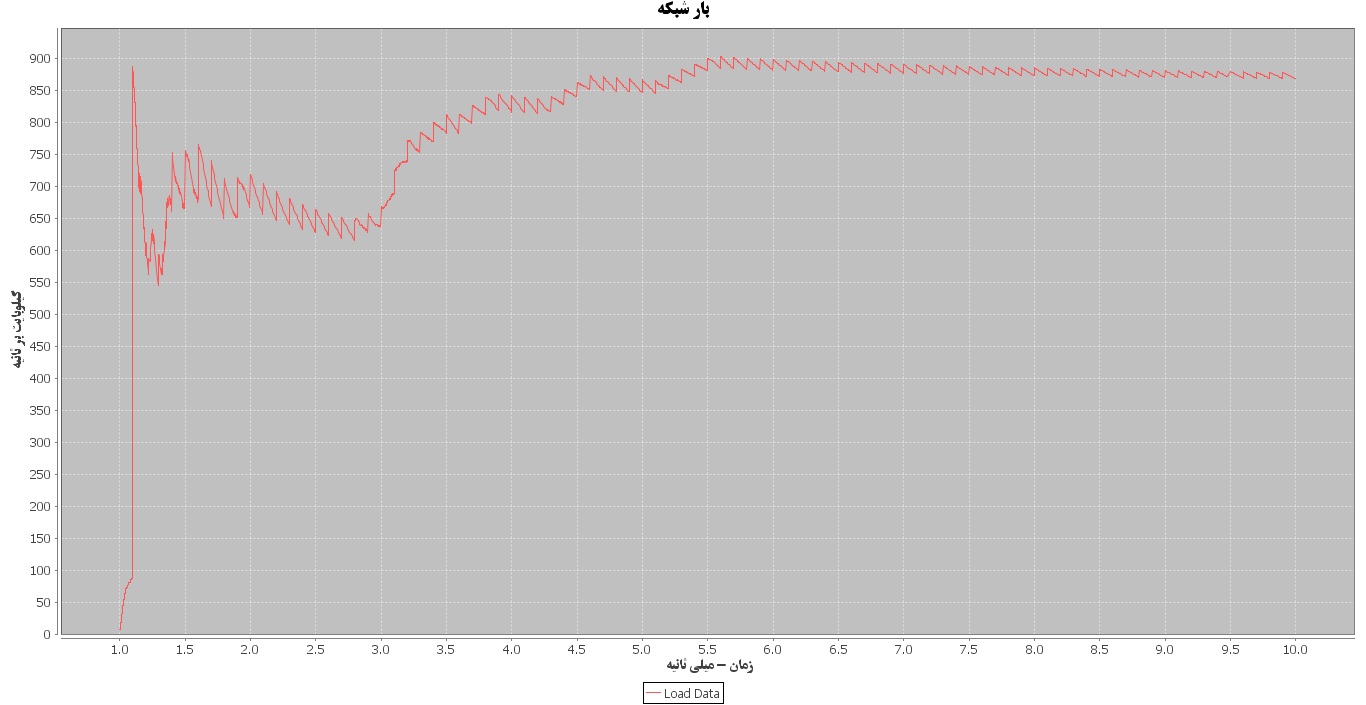
شکل 12: توان عملیاتی در حالت امن، معیار RTR



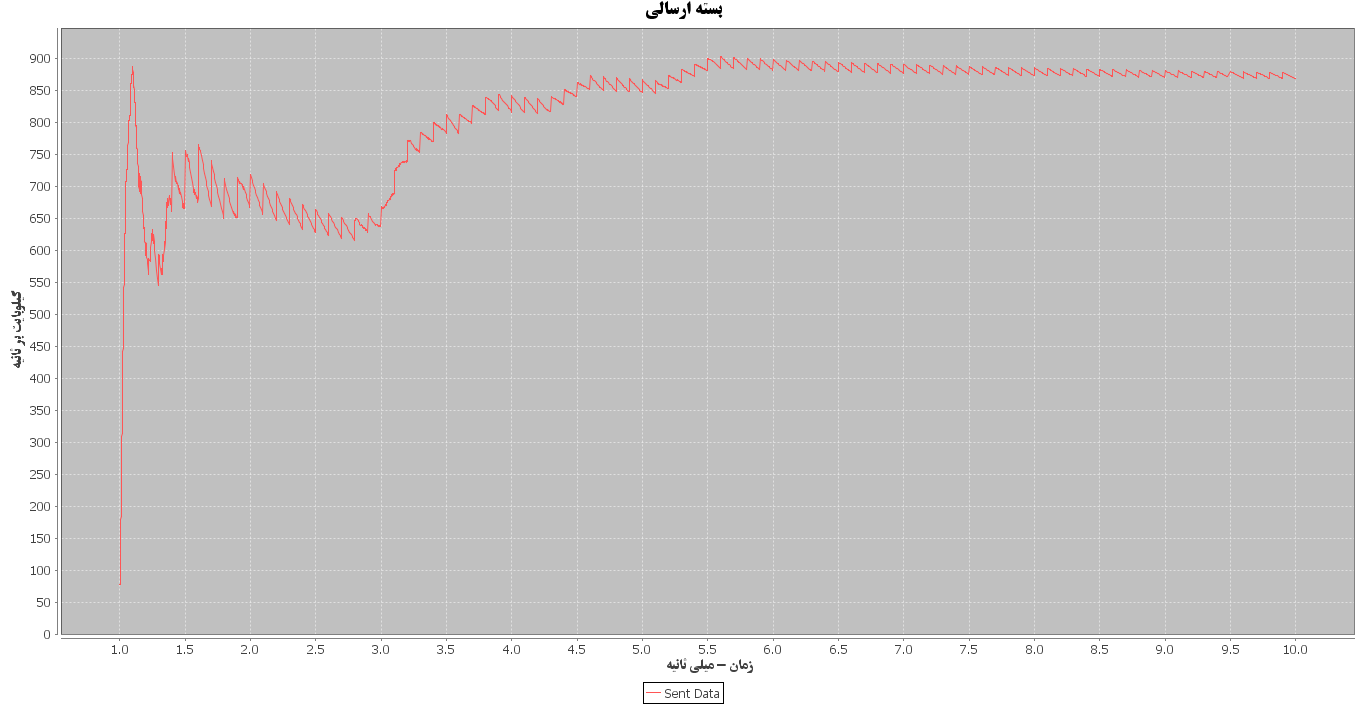
شکل 13: تأخیر انتها به انتها



شکل 14: ناپایداری در نرخ تأخیر بسته

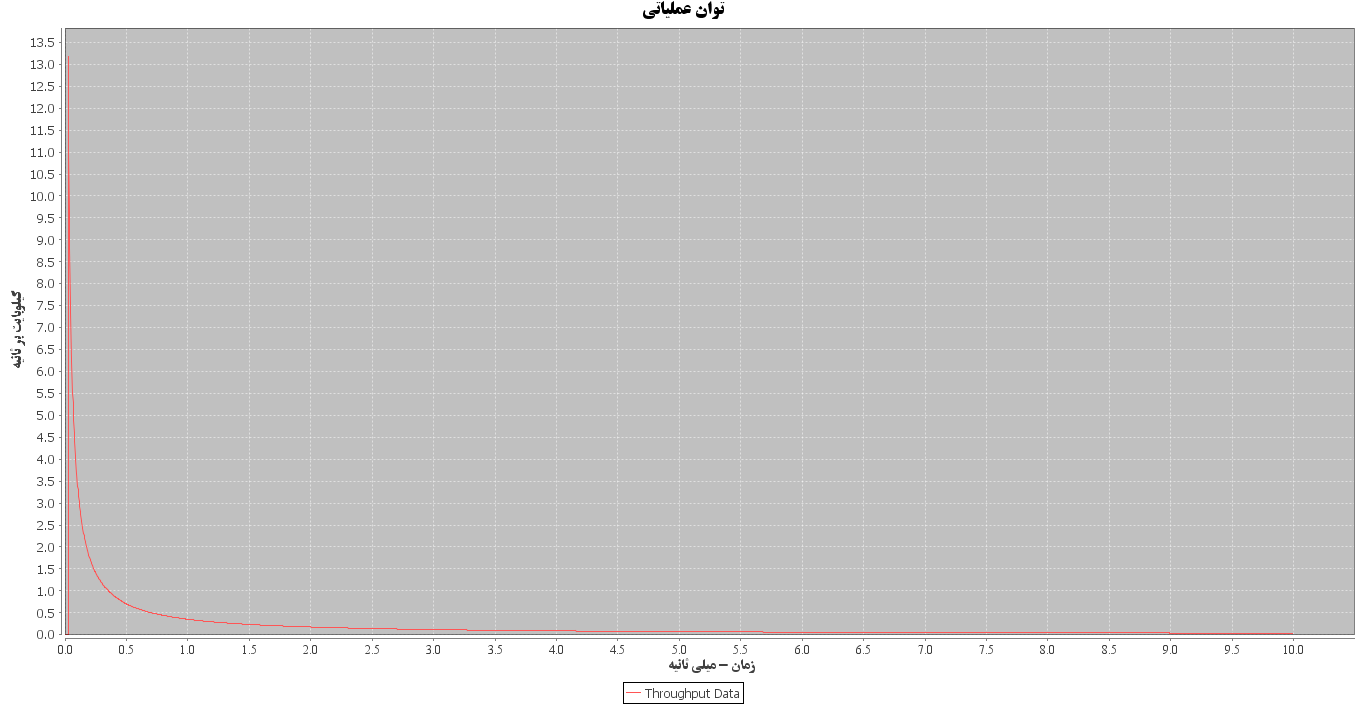


شکل 15: بار شبکه

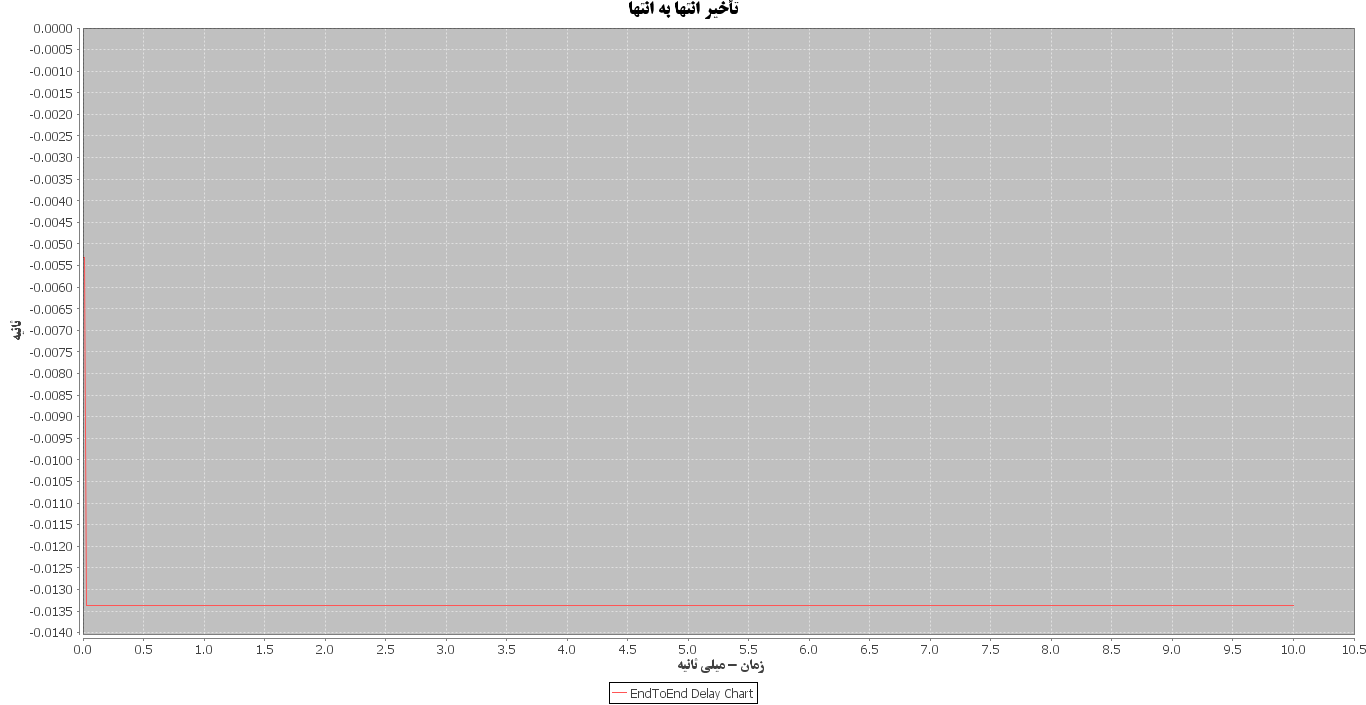


شکل 16: بسته ارسالی

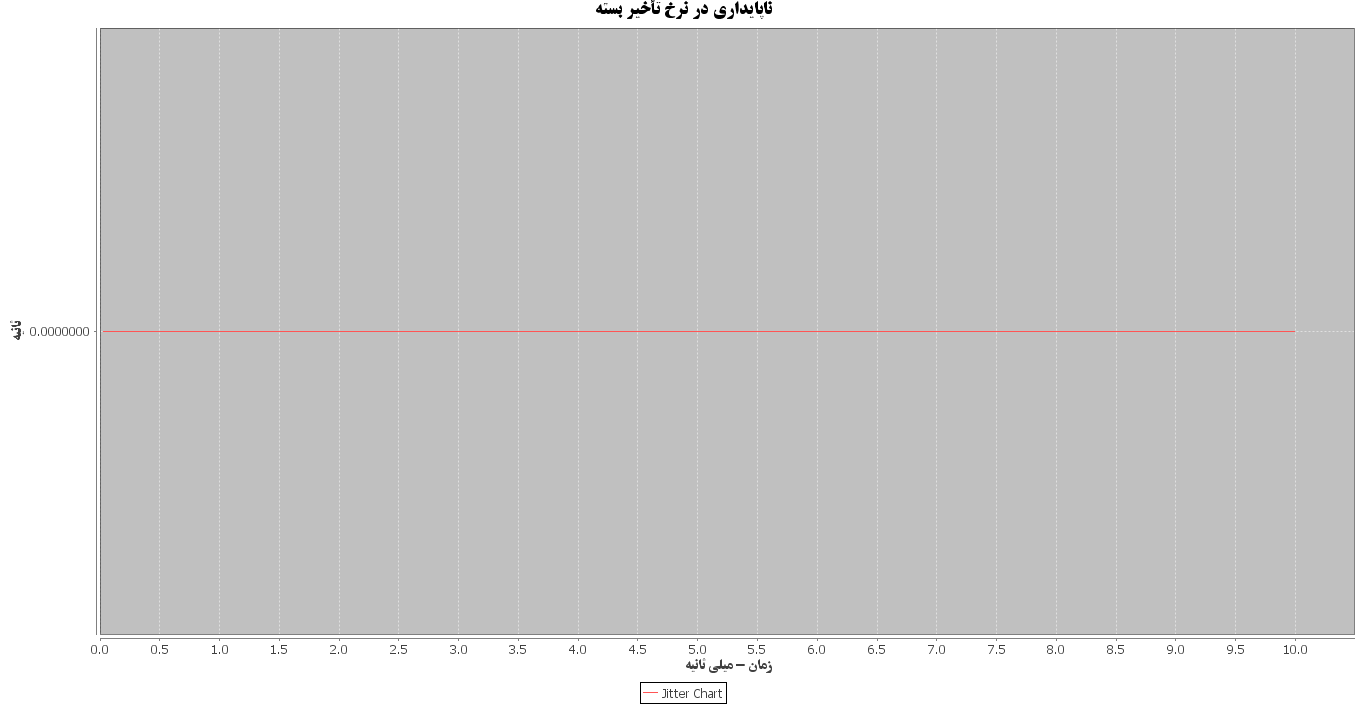
خروجی مدل ردیابی مسیریابی RTR عبارتست از:



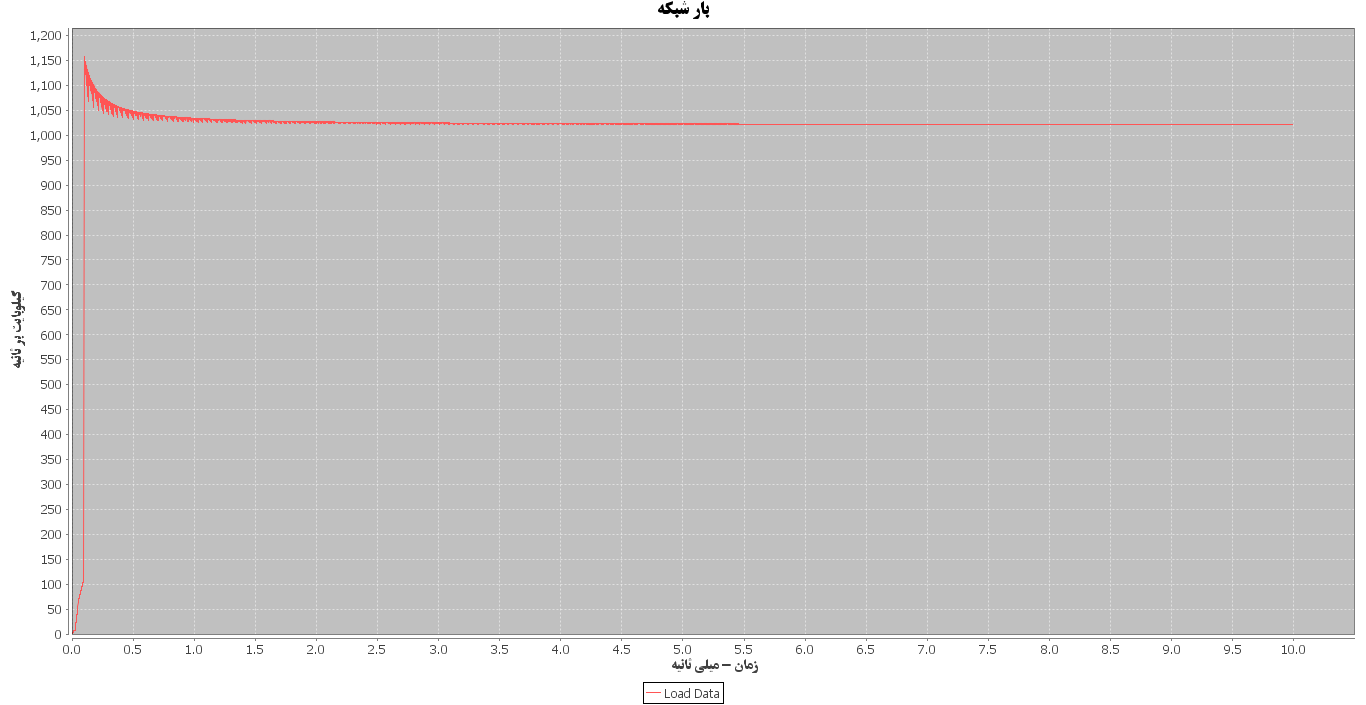
شکل 17: توان عملیاتی در حالت نا امن، مدل ردیابی شبکه RTR



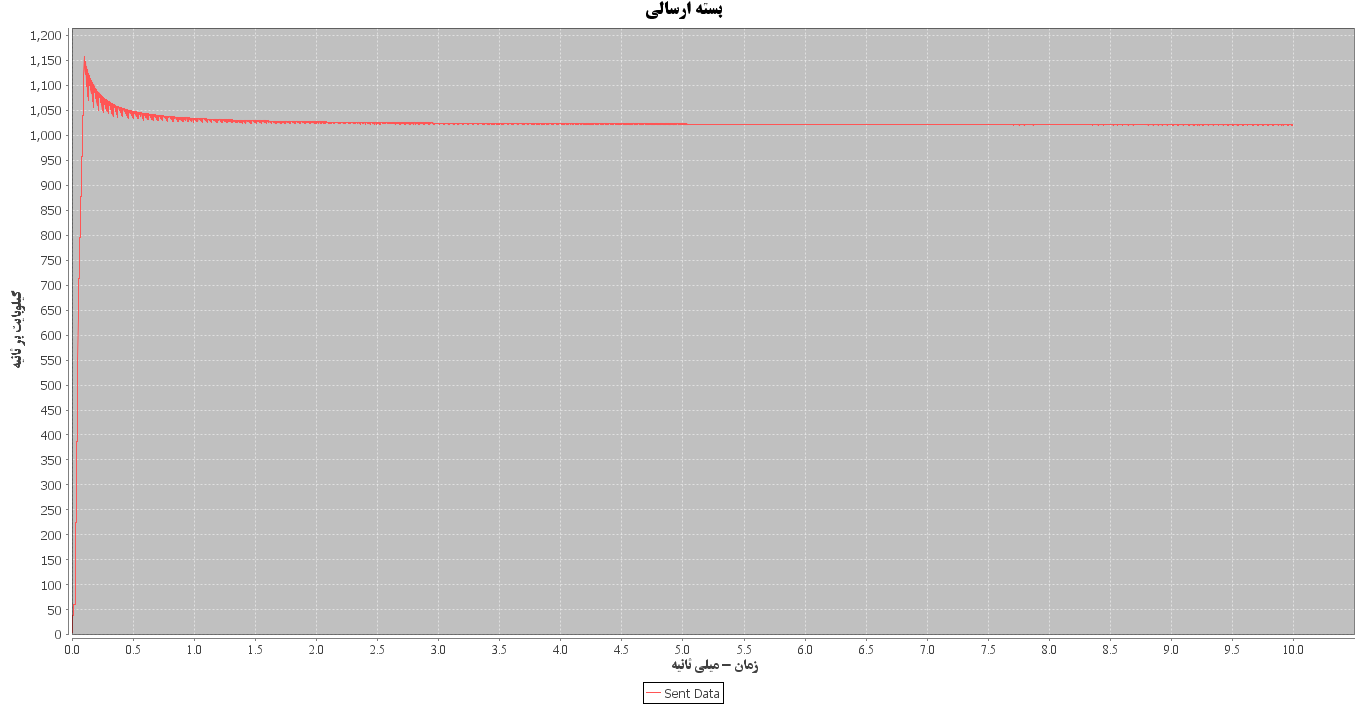
شکل 18: تأخیر انتها به انتها، مدل ردیابی شبکه RTR



شکل 19: ناپایداری در نرخ تأخیر بسته



شکل 20: بار شبکه، مدل ردیابی شبکه RTR



شکل 21: بسته ارسالی، مدل ردیابی شبکه RTR

همانطور که از نتایج قابل درک است، توان عملیاتی در سطح ردیابی مسیریابی و در حالت امن بصورت گسسته در طی زمان تنزل یافته و این در حالیست که، حالت نا امن در آغاز نیم میلی ثانیه نخست شبیه سازی کاهش شدیدی یافته است.

در حالت امن تأخیر انتها به انتها، ترافیک بصورت دوره­ای در طی زمان در حال کاهش بوده و این نقطه مقابل ترافیک نا امن است که ترافیک به یکباره کاهش یافته است.

نرخ ناپایداری در تأخیر بسته در هر دو شبکه برابر است. بار شبکه در ترافیک ایمن بطور پیوسته در حال فزونی است و لیکن در حضور حمله کرم چاله، ترافیک بصورت پیوسته در حال تنزل است. نرخ بسته ارسالی در حالت امن بصورت گسسته در حال افزایش بوده ولی در حالت نا امن، بصورت پیوسته تنزل می یابد.

# 3-نتيجه‌گيري

در این نوشتار، پیاده­سازی و تشخیص حمله کرم چاله مورد بحث قرار گرفته است. یکی از نقاط قوت حمله کرم چاله، استراق تمامی بسته­های داده­ای و نیز جعل و تغییر بسته داده­ای است. نتایج شبیه سازی و ارزیابی پارامترهای توان عملیاتی، نرخ تأخیر­، تأخیر انتها به انتها و نرخ بسته ارسالی بیانگر تشخیص حمله کرم چاله است. از اینرو شبکه حسگر با استخراج این نتایج توانایی تشخیص و ممانعت از این حمله را توسط متدلوژی تشخیص خلاف قاعده مبتنی بر آمار، داراست.

# مراجع

1. Tanenbaum, A. S. (1995). *Distributed operating systems, Pearson Education India.*
2. Iyengar, S. S. and R. R. Brooks (2016). *Distributed sensor networks: sensor networking and applications*, CRC press.

Mohanty, P., S. Panigrahi, N. Sarma and S. S. Satapathy (2010). *SECURITY ISSUES IN WIRELESS SENSOR NETWORK DATA*

1. *GATHERING PROTOCOLS: A SURVEY*. Journal of Theoretical & Applied Information Technology
2. Kazemitabar Amirkolaei, M. (2013). *Enhancing Bio-inspired Intrusion Response in Ad-hoc Networks*, Edinburgh Napier Unversity.
3. Kolias, C., et al. (2011). *Swarm intelligence in intrusion detection: A survey*. computers & security 30(8): 625-642.
4. Maleh, Y., & Ezzati, A. (2014). *A review of security attacks and Intrusion Detection Schemes in Wireless Sensor Networks*. arXiv preprint arXiv:1401.1982.
5. Meisel, M., et al. (2010). *A taxonomy of biologically inspired research in computer networking*. Computer Networks 54(6): 901-916.
6. Chaitanya, K., & Ghosh, A. (2010). *Analysis of Denial-of-Service attacks on Wireless Sensor networks using simulation*. Middlesex University, 1-13
7. Malhotra, J. (2015). *Review on Security Issues and Attacks in Wireless Sensor Networks*. International Journal of Future Generation Communication and Networking 8(4): 81-88.
8. امیر اکبری فر، حمید عباسی نیشابوری "تحلیل امنیت در شبکه حسگر بی سیم" همایش ملی علوم و مهندسی کامپیوتر، دانشگاه خاوران 1395.
9. امیر اکبری فر، حمید عباسی نیشابوری "مروری بر سیستم­های تشخیص نفوذ در شبکه حسگر بی سیم" همایش ملی علوم و مهندسی کامپیوتر، دانشگاه خاوران 1395.

Gupta, N. and S. N. Singh (2016). *Wormhole attacks in MANET.* Cloud System and Big Data Engineering (Confluence), 2016 6th

1. Maulik, R. and N. Chaki (2011). *A study on wormhole attacks in MANET*. International Journal of Computer Information Systems and Industrial Management Applications ISSN: 2150-7988.
2. A. Vani and D.Sreenivasa Rao(2011),”*A simple Algorithm for detection and Removal of wormhole attacks for secure Routing in Ad-hoc Wireless Networks*”, International Journal on Computer Science and Engineering, Vol.3,No.6,PP2377-2384.
3. Haghighi, A., Mizanian, K., & Mirjalily, G. (2016).” *Improved MCBDS for defending against gray hole and black hole attacks in MANETs”*. Advances in Science and Technology Research Journal, 10(30).
4. Somasundaram, K. (2016).” *An Effective CBHDAP Protocol for Black Hole Attack Detection in Manet*”. Indian Journal of Science and Technology, 9(36).
5. Nitnaware, D., & Thakur, A. (2016). “*Black hole attack detection and prevention strategy in DYMO for MANET*”. Paper presented at the Signal Processing and Integrated Networks (SPIN), 2016 3rd International Conference on.
6. Khan, F. A., Imran, M., Abbas, H., & Durad, M. H. (2017). “*A detection and prevention system against collaborative attacks in Mobile Ad hoc Networks*”. Future Generation Computer Systems, 68, 416-427.
7. Ns-2,”*http://www.isi.edu/nsnam/ns*/,”