علوم رایانش و فناوری اطلاعات
نشریه علمی انجمن کامپیوتر ایران
مجلد ۱۳، شماره ۱، ۱۳۹۴
صفحات ۶۵-۷۲
**مقاله عادی**

نشریه علوم رایانش و فناوری اطلاعات

# مقابله با حمله لاپوشانی در سیستم‌های شهرت با استفاده از نظریه‌ی بازی‌ها

شبنم سراجی  مهران سلیمان فلاح

دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی امیرکبیر، تهران، ایران

## چکیده

سیستم‌های شهرت به عنوان یک روش برای تشویق همکاری میان گره‌های شبکه‌های سیار موردی و سیستم‌های همتا به همتا مورد استفاده قرار می‌گیرند. در این روش، گره‌هایی که از شهرت مطلوبی برخوردار هستند، مورد اعتماد در نظر گرفته می‌شوند و در تراکنش‌های خود با گره‌های دیگر براساس شهرت خود خدمات دریافت می‌کنند. به دلیل وجود آسیب‌پذیری‌هایی در سیستم‌های شهرت، از جمله دسترس‌پذیری شناسه‌های ارزان و همچنین انتساب شهرت اولیه به گره‌های تازه وارد، بروز برخی از حملات از جمله حمله لاپوشانی در آنها امکان‌پذیر می‌شود. در این مقاله بر روی حمله‌ی لاپوشانی تمرکز می‌کنیم و به منظور بهبود پژوهش‌های انجام شده، با استفاده از نظریه‌ی بازی به ارائه‌ی یک مدل بازی که تراکنش دو گره داخلی شبکه را نشان دهد، می‌پردازیم. برای این منظور، از مدل بازی‌های بیزین استفاده کرده و با در نظر گرفتن نوع خودخواه و عادی برای هر گره، بازی میان دو گره داخلی شبکه را گسترش می‌دهیم. در ادامه، یک تعادل نش بیزین کامل بازی را به‌دست می‌آوریم. تحلیل تعادل به‌دست آمده نشان می‌دهد که با در نظرگرفتن هزینه‌ی شناسه‌ی مناسب، از حمله‌ی لاپوشانی جلوگیری می‌شود به‌طوری‌که گره‌های عادی نیز برای ورود به شبکه از انگیزه‌ی کافی برخوردار خواهند بود.

**کلمات کلیدی:** حمله لاپوشانی، شبکه‌های سیار موردی، سیستم‌های همتا به همتا، سیستم‌های شهرت، مدیریت اعتماد، نظریه‌ی بازی.

## ۱- مقدمه

همکاری میان گره‌ها به منظور عملیاتی موفق در شبکه‌های سیار موردی خود سازمان‌دهی شده و یا شبکه‌های همتا به همتا بسیار حائز اهمیت است. به منظور همکاری، یک گره باید منابع خود را برای فراهم آوردن خدمات به دیگران اختصاص دهد. اگر گره‌ها دارای انگیزه لازم برای همکاری با سایر گره‌ها نباشند، به علت در دست داشتن منابع محدود، ممکن است رفتار خودخواهانه از خود نشان دهند و بدون فراهم کردن خدمت برای سایر گره‌ها، از خدمات شبکه استفاده کنند.

مکانیزم‌هایی که تاکنون برای تشویق گره‌های شبکه به همکاری ارائه شده‌اند، براساس پرداخت هزینه برای دریافت خدمات شبکه [۱، ۲] و یا براساس مدیریت اعتماد و سیستم‌های شهرت هستند [۳، ۴، ۵، ۶، ۷].

در حقیقت، شهرت به موجودیت‌ها اجازه می‌دهد که اعتماد و یا درجه اطمینان به یک موجودیت دیگر در یک زمینه‌ی خاص ارزیابی کنند. در شبکه‌های سیار موردی و یا شبکه‌های نظیر به نظیر، اعتماد یک گره به سایر گره‌ها نشان دهنده میزان تمایل آن گره به فراهم آوردن خدمات برای سایر گره‌ها است. بنابراین، با استفاده از سیستم‌های شهرت، گره‌ها قادر خواهند بود که گره‌های بدرفتار را شناسایی کنند و آنها را از دریافت خدمات محروم نمایند.

به دلیل وجود برخی از آسیب‌پذیری‌ها در سیستم‌های شهرت، از جمله دسترس پذیری شناسه‌های ارزان، امکان بروز برخی از تهدیدات از جمله Sybil و لاپوشانی برای گره‌های خودخواه فراهم می‌شود [۸]. حمله Sybil در سیستم‌های شهرت زمانی رخ می‌دهد که حمله کننده برخی از شناسه‌ها را به منظور توصیه خودش به عنوان یک گره خوش رفتار جعل می‌کند [۹]. در حمله لاپوشانی از طرف دیگر، یک گره خودخواه همکاری نمی‌کند و تا زمانی که شهرتش پایین نیامده از خدمات شبکه سوء استفاده می‌کند و سپس برای فرار از مجازات که عدم دریافت خدمات شبکه است، شبکه را ترک کرده و با شناسه‌ای جدید وارد شبکه می‌شود. در صورت انجام این حمله، در عملکرد روش‌های مدیریت اعتماد مبتنی بر سیستم‌های شهرت اخلال ایجاد می‌شود. بنابراین، تحلیل این حمله و ارائه راه حل برای مقابله با آن ضروری خواهد بود که در این مقاله به آن پرداخته‌ایم.

دو راه حل کلی برای مقابله با حمله‌ی لاپوشانی وجود دارد. راه حل اول آن است که شناسه‌ها دائمی باشند و هر گره تنها بتواند یک بار از شبکه شناسه دریافت کند. این راه حل با مسئله حریم خصوصی گره‌ها در تضاد است. در این صورت، یک راه برای حفظ حریم خصوصی گره‌ها استفاده از یک مرجع مرکزی معتبر است که به گره‌های شبکه شناسه‌های معتبر و دائمی اعطا کند. این راه حل با طبیعت غیرمتمرکز شبکه‌های سیار موردی و یا شبکه‌های نظیر به نظیر در تضاد است که در آنها همه گره‌ها به صورت خودمختار و مستقل بدون وجود مرجع مرکزی عمل می‌کنند.

اگر شناسه‌ها در شبکه دائمی نباشند، راه حل دوم اعمال جریمه بر گره‌های تازه وارد به شبکه است. در این رابطه، برخی از مقالات برای حل مسئله لاپوشانی به گره‌های تازه وارد شهرت اولیه صفر و یا شهرت اولیه کمتر از حد آستانه ای که بتوانند به وسیله‌ی آن از شبکه خدمت دریافت کنند، نسبت می‌دهند. این در حالی است که انتساب شهرت اولیه صفر و یا شهرت اولیه کمتر از حد آستانه دریافت خدمت به گره‌های تازه وارد سبب می‌شود که گره‌های قانونی و خوش رفتار نیز برای ورود به شبکه انگیزه‌ای نداشته باشند. از طرف دیگر، برخی از مقالات برای دریافت شناسه از شبکه هزینه در نظر می‌گیرند و یا برای اعمال جریمه به تازه واردان، از استراتژی احتمالی استفاده می‌کنند [۱۰، ۱۱]. منظور از استراتژی احتمالی آن است که با گره‌های تازه وارد به صورت احتمالی همکاری شود. همچنین، منظور از هزینه شناسه، میزان منابعی است که یک گره تازه وارد زمان ورودش به شبکه باید مصرف نماید.

هدف از نگارش این مقاله تحلیل و مقابله با حمله‌ی لاپوشانی، یکی از حملات مهم به سیستم‌های شهرت است. از آنجا که به علت عدم وجود مرجع معتبر مرکزی در شبکه‌های سیار موردی و یا همتا به همتا، گره‌ها خودشان در تراکنش با هم براساس معیار شهرت تصمیم‌گیری می‌نمایند و در تصمیم‌گیری خود مصالحه می‌کنند، از نظریه‌ی بازی می‌توان در ارائه یک طرح برای مدیریت اعتماد در این شبکه‌هابهره گرفت. بنابراین، در این مقاله برای بررسی و مقابله با حمله‌ی لاپوشانی از نظریه‌ی بازی استفاده می کنیم. راهکار پیشنهادی برای مقابله با این حمله بر پایه‌ی اخذ هزینه‌ی شناسه از تازه واردان است. برای این منظور، از بازی‌های چند مرحله‌ای با اطلاعات ناکامل برای مدل کردن تراکنش‌های بازیکنان استفاده می‌کنیم. به منظور تشویق گره‌ها برای پیوستن به شبکه، یک شهرت اولیه به گره‌های تازه وارد نسبت داده می‌شود. این مقدار کمترین میزان شهرتی است که به گره تازه وارد امکان دریافت خدمات شبکه را پس از ورودش به شبکه می‌دهد. هزینه‌ی شناسه طوری در نظر گرفته شده‌است که گره‌های خودخواه انگیزه‌ای برای انجام لاپوشانی نداشته باشند.

## ۲- کارهای مرتبط

با حمله لاپوشانی به طور کلی با استفاده از شناسه‌های غیر قابل تعویض و یا جریمه گره‌های تازه وارد به شبکه مقابله می‌شود. راه حل اول نیازمند استفاده از مرجع معتبر مرکزی است که به گره‌های شبکه شناسه‌های معتبر و دائمی اعطا کند. این راه حل نیز با طبیعت غیرمتمرکز شبکه‌های سیار موردی و یا همتا به همتا در تضاد است. راه حل دیگر، تعیین یک مکانیزم جریمه برای بازداشتن گره‌های خودخواه به انجام لاپوشانی است.

در مقاله [۱۲]، یک مکانیزم مبتنی بر توکن ارائه می شود که براساس آن هر گره تازه وارد به شبکه از یک گره موجود در شبکه تقاضای دریافت توکن شهرت می کند که براساس آن توکن بتواند با گره‌های دیگر تراکنش‌های خود را آغاز کند. گرهی که به یک تازه وارد توکن شهرت ارائه کرده است و به عبارتی وی را به شبکه معرفی کرده است تا زمانی که تازه وارد در مرحله‌ای به نام مرحله نهفتگی قرار دارد، در مقابل اعمالش مسئول است. براساس مقاله فوق، ارائه توکن به یک گره تازه وارد و معرفی وی به شبکه به معنای تضمین خوش رفتاری آن است. این در حالی است که در شبکه‌های سیار موردی و یا همتا به همتا گره‌ها بدون وجود انگیزه لازم تضمینی برای خوش رفتار بودن یک گره تازه وارد نمی‌دهند.

در مقاله [۱۳]، یک مدل اقتصادی برای رفتار گره‌ها به منظور بررسی مسئله سواری رایگان در سیستم‌های همتا به همتا ارائه شده‌است. هم چنین، یک مکانیزم جریمه که سواره‌های رایگان را با فراهم کردن خدمات کمتر تنبیه می‌کند، معرفی شده‌است. در ادامه، یک مدل کلی پویا به منظور محاسبه هزینه اجتماعی که در اثر وجود شناسه‌های ارزان به شبکه تحمیل می‌شود، بیان شده‌است. کارایی سیستم در دو حالت شناسه‌های دائمی و شناسه‌های رایگان ارزیابی شده‌است. در نهایت، از ارزیابی انجام شده نتیجه گیری می‌شود که جریمه کردن همه تازه واردان به شبکه تنها در صورت نرخ بالای ورود و خروج به شبکه، سبب کاهش کارایی اجتماعی می‌شود. در مقاله [۱۴]، ادعا شده‌است که یک گره لاپوشانی‌کننده حتی پس از انجام لاپوشانی، رفتارهای مشخصی را دنبال کرده و ادامه می دهد و بنابراین یک لاپوشانی‌کننده با مشاهده و مقایسه رفتارهای انجام شده توسط یک تازه وارد شناسایی می‌شود. از پیش ترتیب مشاهده برای شناسایی لاپوشانی‌کننده‌ها و کم کردن اثر لاپوشانی استفاده می کند. قابل ذکر است که راه حل ارائه شده برای شناسایی لاپوشانی‌کننده‌ها ممکن است منجر به تولید هشدارهای نادرست شود.

مدیریت اعتماد و سیستم‌های شهرت می‌توانند به منظور تحلیل و مقابله با لاپوشانی مورد تستفاده قرار بگیرند. در مقاله [۱۵]، یک مدل اعتماد چند سطحی برای مقابله با سواره‌های رایگان ارائه شده‌است که همتاها را به سطوح اعتماد دسته بندی می‌کند. یک همتا تنها در صورتی می‌تواند از همتای دیگر که مالک یک فایل است، آن فایل را دریافت کند که سطحش از سطح مالک فایل کمتر نباشد. در مقاله [۱۶]، یک طرح مبتنی بر شهرت برای شبکه‌های سیار موردی برای جلوگیری از حمله‌ی لاپوشانی ارائه شده‌است. در طرح ارائه شده، هر گره تنها در صورتی برای گره مقابل خود خدمات فراهم می‌آورد که شهرت وی از یک حد آستانه بالاتر باشد. یک سیستم شهرت دیگر در مقاله [۱۷] معرفی شده‌است که در آن امتیاز شهرت یک همتا که حداقل یک بار همکاری کرده است، از امتیاز شهرت تازه واردان بیشتر است. به علاوه، امتیاز شهرت یک گره همکاری کننده به صورت تدریجی افزایش می‌یابد و شهرت یک گره خودخواه به سرعت کاهش می‌یابد. همه مقاله‌های فوق، یک شهرت اولیه بسیار کم به تازه واردان اختصاص می‌دهند به طوریکه آنها قادر به دریافت خدمات شبکه پس از ورودشان به شبکه نخواهند بود مگر آنکه در چندین دور اول پس از ورود به شبکه، همکاری کرده و شهرت خود را به میزان لازم برای دریافت خدمات شبکه افزایش دهند. به عبارت دیگر، انگیزه لازم برای ورود گره‌های خوش رفتار به شبکه در نظر گرفته نشده‌است.

در مقاله [۱۸]، یک مکانیزم شهرت به منظور مقابله با حمله pollution ارائه شده‌است. این مکانیزم شهرت، به تازه واردن یک شهرت اولیه کمینه نسبت می‌دهد. به‌طوری‌که آنها بتوانند پس از ورودشان به شبکه از سایر گره‌ها خدمات دریافت کنند. در حالی که تازه واردان به شبکه انگیزه لازم برای ورود به شبکه را دارا هستند، از حمله لاپوشانی جلوگیری نمی‌شود. در حقیقت، لاپوشانی‌کننده‌ها تنها قادر به انجام سواری رایگان در تعداد مراحل محدودی پس از ورودشان به شبکه خواهند بود.

سیستم شهرت ارائه شده در مقاله [۱۹]، دو نوع شهرت بارگیری و بارگزاری را در نظر گرفته است. یک گره جریمه می‌شود اگر بارگیری بیشتری انجام دهد و همکاری اش در بارگزاری فایل ها از حد استانه مورد نظر کمتر باشد. در ادامه یک پارامتر براساس زمان صرف شده برای بارگزاری فایل‌ها که تعیین کننده رفتار گره است، تعریف می‌شود. اگر پارامتر تعریف شده از یک حد آستانه تعیین شده برای چندین تراکنش متوالی کمتر باشد، آن گره به عنوان یک لاپوشانی‌کننده احتمالی در نظر گرفته می‌شود و شهرتش به سطح کمتر بعدی به روزرسانی می‌شود.

شناسایی لاپوشانی‌کنندگان به این صورت، ممکن است منجر به تولید هشدارهای نادرست توسط سیستم شود.

نظریه‌ی بازی یک ابزار قدرتمند است که می‌تواند به منظور مدل کردن و تحلیل رفتار گره‌های شبکه مورد استفاده قرار گیرد. برخی از راه حل‌های مقابله با لاپوشانی از نظریه‌ی بازی به منظور تحلیل دقیق‌تر استفاده کرده اند. در مقاله [۲۰]، تراکنش میان گره‌های بدخواه و عادی شبکه سیار موردی به منظور تحلیل رفتارهای گره‌های بدخواه و قانونی بررسی شده‌است. برای این منظور، از مدل بازی‌های سیگنالینگ بیزین پویا استفاده شده‌است. گره‌های قانونی برای ارائه خدمات، با توجه به باور خود نسبت به گره مقابلشان تصمیم‌گیری می‌نمایند و زمانی که باور آنها نسبت به گره مقابل از یک حد آستانه بگذرد، گره مقابل را به عنوان گره بدخواه به شبکه گزارش می‌کنند. از طرف دیگر، گره‌های بدخواه ریسک ماندن خود در شبکه را سنجیده و با توجه به آن تصمیم به ماندن و یا فرار از شبکه می‌گیرند. در حقیقت، گره‌های بدخواه برای فرار از مجازات و گزارش شدن به عنوان گره بدخواه، به نقطه‌ای دیگر از شبکه فرار می‌کنند و راه‌حلی برای مقابله با این فرار ارائه نشده‌است. این در حالی است که در مدل بازی ارائه شده در این مقاله، گره‌های خودخواه به منظور دستیابی به بهره بیشتر دست به لاپوشانی می‌زنند و هم‌چنین راه‌حلی برای مقابله با این رفتار ارائه می‌شود.

حملات علیه سیستم‌های شهرت از جمله لاپوشانی، توصیه نادرست و Sybil در مقاله [۲۱] بررسی شده‌اند. برای مقابله با حمله‌ی لاپوشانی تراکنش‌های بازیکنان به صورت یک بازی چند مرحله‌ای مدل می‌شود. هر گره تازه وارد برای ورود به شبکه باید هزینه ای بپردازد. استراتژی پرداخت هزینه به این صورت تعریف می‌شود که در برابر هر بازیکن قدیمی که تا کنون از این استراتژی تخطی نکرده است، همکاری شود و با مشاهده اولین تخطی تا پایان بازی با او همکاری نشود. همچنین در مقابل هر بازیکن تازه وارد همکاری نشود مگر آنکه بازیکن تصمیم گیرنده خودش تازه وارد باشد. به منظور بهبود این طرح بیشترین تعداد بازیکنانی که در هر مرحله می‌توانند تازه وارد باشند، ضریبی از تعداد کل بازیکنان در نظر گرفته می‌شود. از آنجا که این استراتژی سخت گیرانه است، زیرا تنها یک تخطی سبب می‌شود که بازیکنان همواره عدم همکاری کنند، در ادامه مقداری نویز نیز به مدل افزوده می‌شود.

در مقاله [۱۰] نشان داده می‌شود در صورت در نظر گرفتن هزینه شناسه مناسب، استراتژی (TFT) و نسخه دیگر آن TFT احتمالی سبب تنبیه رفتار لاپوشانی می‌شوند. نویسندگان مقاله هم چنین، مدل عمل متقابل غیرمستقیم را به صورتی توسعه داده اند که در آن، تمییزدهندگان، همتاهایی که براساس توصیف سیستم همتا به همتا عمل می‌کنند و با تازه واردان به صورت احتمالی همکاری می‌کنند، برنده بازی شوند. این مسئله با در نظر گرفتن احتمال همکاری کم با تازه واردان محقق می‌شود که منجر به کاهش کارایی اجتماعی خواهد شد.

در مقاله [۱۱]، برای مقابله با لاپوشانی‌کننده‌ها یک مکانیزم جریمه در مقابل گره‌های تازه وارد ارائه شده‌است. سیستم ذخیره یابی همتا به همتا به عنوان یک بازی تکاملی مدل می‌شود. در ادامه، دو نوع استراتژی تعریف می‌شود. در استراتژی اول، همتاهایی که تمییزدهنده نامیده می‌شوند، به صورت احتمالی با یک مقدار مشخص با تازه واردان همکاری می‌کنند. در استراتژی دوم، همتاهایی که فراری نامیده می‌شوند، همواره همکاری نمی‌کنند و به صورت احتمالی لاپوشانی می‌کنند. بهره کلی برای تمییزدهندگان و فراری‌ها محاسبه شده‌است. در نهایت، نشان داده می‌شود که کارایی اجتماعی با در نظر گرفتن مقدار خاصی برای احتمال همکاری با تازه واردان بیشینه می‌شود. قابل ذکر است که در دو مقاله [۱۰] و [۱۱]، مدل تراکنش گره‌های تمییزدهنده و لاپوشانی‌کننده ساده در نظر گرفته شده است. این در حالی است که در این مقاله مدل تراکنش گره‌های داخلی شبکه را به صورتی که هر گره بتواند نوع عادی و یا خودخواه داشته باشد، گسترش داده‌ایم.

## ۳- مدل بازی

گره‌های یک شبکه را می‌توان بازیکنان یک بازی تصور نمود که اعمال خود را به صورت استراتژیک انتخاب می‌کنند. یک گره ممکن است بسته دریافتی از گره دیگر را برای گره‌های دیگر ارسال کند و یا آن بسته را به دور بیندازد. هر گره هم چنین می‌داند که سایر گره‌ها اعمال انتخابی وی را مشاهده کرده و بر آن اساس یک سطح اعتماد به وی اختصاص می‌دهند و در این صورت، گره‌های بدرفتار از دریافت خدمات شبکه محروم خواهند شد.

### ۳-۱- فرضیات

هر گره در شبکه می‌تواند نوع خودخواه و یا عادی را داشته باشد. هر گره در شبکه دارای یک شناسه است و می‌تواند هر زمانی که بخواهد از شبکه شناسه جدید دریافت کند. هر گره با یک شناسه جدید به عنوان یک تازه وارد تلقی می‌شود. هم چنین، به منظور تشویق گره‌های تازه وارد برای پیوستن به شبکه، یک شهرت اولیه به هر گره تازه وارد تخصیص داده می‌شود.

جدول ۱- جدول علائم به کار رفته

| معنا | علامت به کار رفته |
|---|---|
| هزینه همکاری یک گره عادی در برابر گره عادی دیگر | $C_C$ |
| هزینه همکاری یک گره خودخواه در برابر گره دیگر | $C''_C$ |
| هزینه همکاری یک گره عادی در برابر گره خودخواه دیگر | $C'_C$ |
| هزینه‌ی شناسه تازه وارد | $C_I$ |
| بهره‌ی گره عادی در اثر لاپوشانی | $-C_W$ |
| سود حاصل از عدم همکاری گره عادی در برابر گره خودخواه دیگر | $G$ |
| سود حاصل از دریافت خدمات | $G_C$ |
| بهره‌ی حاصل از لاپوشانی | $G_W$ |
| احتمال ورود تازه وارد به شبکه | $P_e$ |

فرض می‌کنیم که شبکه از سیستم شهرت بتا استفاده می‌کند که براساس تابع توزیع بتا از مشاهدات صورت گرفته است [۲۲، ۲۳]. مقدار شهرت به صورت یک زوج مرتب $(\alpha, \beta)$ نشان داده می‌شود که در آن $\alpha$ و $\beta$ به ترتیب نشان دهنده تجربیات مثبت و منفی هستند. قابلیت اعتماد یک گره با شهرت $(\alpha, \beta)$، براساس مقدار امید متغیر تصادفی $p$ با توزیع بتا با پارامترهای $\alpha$ و $\beta$ محاسبه می‌شود. این مقدار برابر با $E(p) = \frac{\alpha}{\alpha+\beta}$ است.در این مقاله، منظور ما از شهرت یک گره، قابلیت اعتماد آن گره در فراهم آوردن خدمات برای سایر گره‌ها است. هر گره لیستی از شناسه‌های گره‌های دیگر شبکه را در اختیار دارد و از شهرت گره‌هایی که قبلا با آنها تراکنش داشته است، مطلع است.

تراکنش میان دو گره به صورت یک بازی چند مرحله‌ای با اطلاعات ناکامل مدل شده‌است. هر گره می‌تواند نوع خودخواه (SF) و یا عادی (NR) را داشته باشد. منظور از باور یک گره نسبت به گره مقابل دیگر، مقدار احتمالی است که وی برای نوع گره مقابل خود براساس نوع خودش و تاریخچه اعمال مشاهده شده از گره مقابل در نظر میگیرد. باور گره $i$ در آغاز مرحله $t$نسبت به اینکه گره مقابلش دارای نوع $\theta_{-i}$ باشد با $\mu_i(\theta_{-i}|\theta_i, h^t)$ نشان داده می‌شود. بازیکنان بهره کل را با استفاده از معیار میانگین زمانی محاسبه می‌کنند.

نوع هر گره ترجیحات وی را برای فعالیت در شبکه نشان می‌دهد که نزد خودش محرمانه باقی می‌ماند. گره‌های خودخواه متمایل به دریافت هر چه بیشتر خدمات شبکه و فراهم آوردن خدمات هر چه کمتر به شبکه هستند. این در حالی

است که گره‌های عادی به طور کلی متمایل به همکاری هر چه بیشتر با سایر گره‌های شبکه هستند.

پیش از آنکه دو گره اعمال خود را در یک تراکنش انتخاب کنند، ابتدا به شناسایی یکدیگر می‌پردازند. هر گره شناسه گره مقابل خود را در جدول شهرتش جستجو می‌کند. در صورت وجود شناسه گره مقابل در جدول شهرت خود، براساس باورش نسبت به قابلیت اعتماد گره مقابل عمل می‌کند. اگر یکی از دو گره شناسه گره مقابل خود را در جدول شهرتش در اختیار نداشته باشد، گره مقابل را یک گره تازه وارد در نظر می‌گیرد و یک شهرت اولیه به وی نسبت می‌دهد و هم چنین شهرت اولیه به همراه شناسه جدید وی را در کل شبکه توزیع می‌کند. همچنین فرض می‌کنیم دو گره تازه وارد با هم تراکنشی انجام نمی‌دهند. جدول ۱، نمادهای به کار رفته شده در این مقاله را نشان می‌دهد.

## ۳-۲- بازی بیزین چند مرحله‌ای

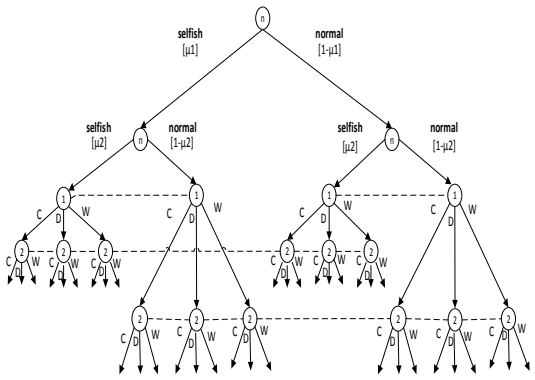
شکل ۱ فرم گسترده بازی بیزین ایستا میان دو گره داخلی شبکه را نشان می‌دهد. گره داخلی اول را با $i$ و گره داخلی دوم را با $j$ نشان می‌دهیم.برای هر گره دو نوع خودخواه و عادی در نظر می‌گیریم. نوع گره داخلی اول را با $\theta_1$ و نوع گره داخلی دوم را با $\theta_2$ نشان می‌دهیم.

$\theta_1 = \theta_2 \in \{SF, NR\}$

هر گره نوع خود را می‌داند و هیچ گره‌ای از نوع گره دیگر مطلع نیست. طبیعت تعیین می‌کند که کدام دو گره و با چه نوعی با یکدیگر بازی کنند.

هر بازی به شکل فوق در مراحل $t = 0,1,2,\dots T$ انجام می‌شود با این ویژگی که بازیکنان به صورت هم‌زمان اعمال خود را انتخاب می‌کنند و اعمال انتخابی آنها در انتهای مرحله مربوطه آشکار می‌شوند. $a_i^t \in A_i(h^t)$ نشان‌دهنده عمل انتخابی بازیکن $i$ در مرحله $t$ است.هر گره اعمال خودش و سایر گره‌ها را که از تراکنش‌های قبلی صورت گرفته میان خودشان مشاهده کرده است، در یک تاریخچه در اختیار دارد.

در بازی فوق، عمل $C$ از سوی هر بازیکن نشان دهنده همکاری و ارائه خدمات و عمل $D$ نشان دهنده عدم همکاری و عدم ارائه خدمات به گره مقابل است. گره $j$ هنگام انتخاب عملش در رویارویی با گره $i$ ، با توجه به تراکنش‌های مستقیم قبلی که با وی داشته است، باورش را براساس رابطه‌ی بیز نسبت به $i$ شکل می‌دهد. احتمال آنکه $i$ از دیدگاه $j$ خودخواه باشد را با $\mu_1$ نشان می‌دهیم. به همین ترتیب، احتمال آنکه $j$ از دیدگاه $i$ خودخواه باشد را با $\mu_2$ نشان می‌دهیم. $\mu_1$ نسبت تعداد عدم همکاری‌های صورت گرفته از جانب $i$ در برابر $j$ به




شکل ۱- بازی تک مرحله بیزین میان دو گره داخلی شبکه

تعداد کل همکاری‌ها و عدم همکاری‌های وی در برابر $j$ است. $\mu_2$ نیز به همین ترتیب تعریف می‌شود. در اثر سپری شدن زمان و صورت گرفتن تراکنش‌های مختلف، این احتمالات با استفاده از قانون بیز به‌روزرسانی می‌شوند.

بهره‌های بازیکنان در اثر انتخاب اعمالشان در هر مرحله در شکل‌های ۲، ۳ و ۴ نشان داده شده‌است. صرف نظر از نوع گره‌ها، همکاری تنها یک گره در یک تراکنش به معنای فراهم شدن خدمات برای گره مقابل است. گره داخلی خودخواه گره‌ای است که تمایل به دریافت خدمات بیشتر و ارائه خدمات کمتر دارد. بنابراین، این گره تمایل زیادی به تراکنشی دارد که نتیجه آن عدم‌همکاری از جانب خودش و همکاری از جانب گره مقابلش است و از این تراکنش بیشترین سود خود را می‌برد. از آنجا که گره خودخواه تمایل کمتری برای همکاری دارد، بنابراین هزینه همکاری یک گره خودخواه در برابر گره دیگر را چه عادی و چه خودخواه باشد، بیشتر از هزینه همکاری یک گره عادی در برابر یک گره عادی دیگر در نظر می‌گیریم و آن را با $C''_C$ نشان می‌دهیم.

| | C | D | W |
|---|---|---|---|
| C | $(G_C - C''_C, G_C - C''_C)$ | $(-C''_C, G_C)$ | $(-C''_C, G_W)$ |
| D | $(G_C, -C''_C)$ | $(0,0)$ | $(0, G_W)$ |
| W | $(G_W, -C''_C)$ | $(G_W, 0)$ | $(G_W, G_W)$ |

شکل ۲- بهره‌های بازی تک مرحله‌ای در صورتیکه هر دو بازیکن سطری و ستونی خودخواه باشند

| | C | D | W |
|---|---|---|---|
| C | $(G_C - C''_C, G_C - C'_C)$ | $(-C''_C, G_C + G)$ | $(-C''_C, -C_W)$ |
| D | $(G_C, -C'_C)$ | $(0, G)$ | $(0, -C_W)$ |
| W | $(G_W, -C'_C)$ | $(G_W, G)$ | $(G_W, -C_W)$ |

شکل ۳- بهره‌های بازی تک مرحله‌ای در صورتیکه بازیکن سطری خودخواه و بازیکن ستونی عادی باشند

| | C | D | W |
|---|---|---|---|
| C | $(G_C - C_C, G_C - C_C)$ | $(-C_C, 0)$ | $(-C_C, -C_W)$ |
| D | $(0, -C_C)$ | $(0,0)$ | $(0, -C_W)$ |
| W | $(-C_W, -C_C)$ | $(-C_W, 0)$ | $(-C_W, -C_W)$ |

شکل ۴- بهره‌های بازی تک مرحله‌ای در صورتیکه هر دو بازیکن سطری و ستونی عادی باشند

هنگامی که میانگین شهرت گره خودخواه از یک حد آستانه کمتر شده‌است و دیگر عدم همکاری ممکن است برایش سودآور نباشد، ممکن است تصمیم به لاپوشانی (W) بگیرد. گره خودخواه باید ریسک لاپوشانی را در نظر بگیرد و با مقایسه بهره‌ی حاصل از ماندنش در شبکه و بهره‌ی حاصل از لاپوشانی تصمیم‌گیری نماید. ریسک لاپوشانی را عدم ورود به شبکه و یا دستیابی به بهره‌ای کمتر یا مساوی بهره‌ی ماندن در شبکه تعریف می‌کنیم.

گره داخلی عادی از طرف دیگر گره‌ای است که به طور کلی تمایل به همکاری دارد. بهره‌ی یک گره عادی در اثر عدم همکاری با گره عادی دیگر، خواه آن گره همکاری کرده باشد یا نکرده باشد، صفر خواهد بود. این در حالی است که عدم همکاری گره عادی در برابر گره خودخواه برای وی سودآور است، زیرا گره عادی بیشتر متمایل به عدم همکاری در برابر گره خودخواه است و در صورت همکاری با گره خودخواه، به‌طوری‌که گره خودخواه نیز همکاری کرده باشد، سودی کمتر از همکاری با گره‌های عادی به‌دست می‌آورد. بنابراین، هزینه همکاری یک گره عادی با گره خودخواه دیگر را بیشتر از هزینه همکاری وی با گره عادی دیگر در نظر می‌گیریم و این هزینه را با $C'_C$ نشان می‌دهیم. همچنین با توجه به آنکه گره

عادی تمایل به هر چه همکاری بیشتر و عدم همکاری کمتر دارد و تمایلی به انجام لاپوشانی ندارد، انجام عمل لاپوشانی برای یک گره عادی یک عمل مغلوب محسوب می‌شود.

## ۴- محاسبه تعادل نش بیزین

تعادل مطلوب ما برای بازی چند مرحله‌ای توصیف شده در بخش قبل، آن است که در آن از عمل لاپوشانی جلوگیری شود. در این بخش، به دنبال یافتن چنین تعادلی هستیم.

میزان بهره‌ی یک لاپوشانی‌کننده از یک بار عمل لاپوشانی به صورت زیر است:

$$G_W = P_e.(E'(R_{ini}) + (1 - P_e).(0) = P_e.(E'(R_{ini}))$$

همچنین، میزان بهره‌ی یک تازه وارد قانونی که آن را با $G_{NC}$ نشانمی‌دهیم، به صورت زیر است:

$$G_{NC} = P_e.(E(R_{ini}) + (1 - P_e).(0) = P_e.(E(R_{ini}))$$

منظور از $E'(R_{ini})$ بهره‌ای است که گره خودخواه لاپوشانی‌کننده در اثر ورودش به شبکه به‌دست می‌آورد. این بهره‌ی شامل دریافت خدمات شبکه و پرداخت هزینه‌ی شناسه است. همچنین، $E(R_{ini})$ نیز بهره‌ای است که گره تازه وارد قانونی که نوعش عادی باشد، در اثر ورودش به شبکه به‌دست می‌آورد. این بهره نیز شامل دریافت خدمات شبکه و پرداخت هزینه‌ی شناسه است.

**لم ۱.** پروفایل استراتژی ((D, D), (D, D)) درصورتی‌که $G_W \le 0$ تعادل نش بیزین خالص است.

**اثبات.** ابتدا فرض می‌کنیم که اعمال نوع‌های گره اول ثابت هستند و به بررسی بهترین پاسخ‌های هر یک از دو نوع گره دوم می‌پردازیم. اگر نوع گره دوم عادی باشد، با توجه به جداول بهره، عمل D برای نوع عادی گره دوم بهترین پاسخ است.

اگر نوع گره دوم خودخواه باشد، با توجه به جداول بهره، درصورتی‌که $G_W \le 0$ باشد، عمل D برای نوع خودخواه گره دوم بهترین پاسخ است.

اکنون فرض می‌کنیم که اعمال نوع‌های گره دوم ثابت هستند و به بررسی بهترین پاسخ‌های هر یک از دو نوع گره اول می‌پردازیم. اگر نوع گره اول عادی باشد، با توجه به جداول بهره، عمل D برای نوع عادی گره اول بهترین پاسخ است. اگر نوع گره اول خودخواه باشد، با توجه به جداول بهره، درصورتی‌که $G_W \le 0$ باشد، عمل D برای نوع خودخواه گره اول بهترین پاسخ است.

**لم ۲.** پروفایل استراتژی ((W, D), (W, D)) درصورتی‌که $G_W > 0$ تعادل نش بیزین خالص است.

**اثبات.** همانند اثبات لم ۱. به راحتی بررسی می‌شود.

**لم ۳.** پروفایل استراتژی ((D, C), (D, C)) تحت برقراری روابط (۱)، (۳)، (۴) و (۶) تعادل نش بیزین خالص است.

**اثبات.** اگر نوع گره دوم عادی باشد، با توجه به جداول بهره، بهره‌ی گره عادی دوم وابسته به نوع گره اول است و از آنجا که با توجه به پروفایل استراتژی فوق می‌خواهیم عمل C برای گره عادی دوم بهترین پاسخ باشد، باید بررسی کنیم که تحت چه شرایطی عمل C بهترین پاسخ خواهد بود. با بررسی به نتیجه زیر می‌رسیم:

$$\text{If } E_2(C) \ge E_2(D), \mu_1 \le \frac{G_C - C_C}{G_C - C_C + C'_C + G} \quad (۱)$$

$$\text{If } E_2(C) \ge E_2(W), \mu_1 \le \frac{G_C - C_C + C_W}{G_C - C_C + C'_C} \quad (۲)$$

از آنجا که $(C_W > C'_C)$ رابطه‌ی (۲) همواره برقرار است.

اگر نوع گره دوم خودخواه باشد، عمل D همواره از عمل C بهتر است. همچنین داریم:

$$\text{If } G_W \le 0, E_2(D) \ge E_2(W)$$

$$\text{If } G_W > 0, \mu_1 \le \frac{G_C - G_W}{G_C} \quad (۳)$$

اگر نوع گره اول عادی باشد، همانند بررسی‌های فوق برای گره عادی دوم، می‌خواهیم عمل C برای گره عادی اول بهترین پاسخ باشد. بنابراین:

$$\text{If } E_1(C) \ge E_1(D), \mu_2 \le \frac{G_C - C_C}{G_C - C_C + C'_C + G} \quad (۴)$$

$$\text{If } E_1(C) \ge E_1(W), \mu_2 \le \frac{G_C - C_C + C_W}{G_C - C_C + C'_C} \quad (۵)$$

از آنجا که $(C_W > C'_C)$ رابطه‌ی (۵) همواره برقرار است.

اگر نوع گره اول خودخواه باشد، ، عمل D همواره از عمل C بهتر است. همچنین داریم:

$$\text{If } G_W \le 0, E_1(D) \ge E_1(W)$$

$$\text{If } G_W > 0, \mu_2 \le \frac{G_C - G_W}{G_C} \quad (۶)$$

**لم ۴.** پروفایل استراتژی ((C, C), (C, C)) تعادل نش بیزین خالص نیست.

**اثبات.** اگر نوع گره دوم خودخواه باشد، با توجه به جداول بهره، عمل D برای گره خودخواه دوم بهترین پاسخ است. قابل ذکر است که سایر پروفایل‌های استراتژی خالص همانند پروفایل استراتژی ((C, C), (C, C)) قابل بررسی هستند و هیچ یک تعادل نش بیزین خالص نیستند.

**لم ۵.** برای بازی دو گره داخلی شبکه تعادل نش بیزین ترکیبی وجود ندارد.

**اثبات.** با بررسی روابط میان بهره‌ها، مشاهده می‌شود که امکان یکسان‌سازی بین بهره‌ها وجود ندارد.

با توجه به بررسی‌های فوق، دو پروفایل استراتژی زیر برای گره عادی اول و گره خودخواه اول به صورت زیر دست می‌آیند. قابل ذکر است که پروفایل استراتژی گره‌های عادی دوم و خودخواه دوم نیزبه صورت متقارن به دست می‌آیند.

**Algorithm 1** Normal-type player 1's PBE strategy

**if** $\mu_2 \le \frac{G_C - C_C}{G_C - C_C + C'_C + G}$ and $\mu_1 \le \frac{G_C - C_C}{G_C - C_C + C'_C + G}$ **then**
    Choose C
**else**
    Choose D
**end if;**

**Algorithm 2** Selfish-type player 1's PBE strategy

**if** $G_W < 0$
    Choose D
**else**
    **if** $\mu_2 \le \frac{G_C - C_C}{G_C - C_C + C'_C + G}$ and $\mu_1 \le \frac{G_C - C_C}{G_C - C_C + C'_C + G}$
        Choose D
    **else**
        Choose W
    **end if;**
**end if;**

**قضیه ۱.** استراتژی پروفایل‌های ارائه شده تعادل بیزین کامل هستند.

**اثبات.** ابتدا نشان می‌دهیم که چهار شرط بیزین برقرار هستند [۲۴].

۱. با استفاده از شهرت بتا، از رابطه‌ی بیز برای به روزرسانی باور $\mu_i(\theta_j|h^t)$ به باور $\mu_i(\theta_j|h^{t+1})$ استفاده شده‌است.

۲. باورهای پسین مستقل هستند و در صورت آنکه تاریخچه اعمال انتخاب شده یکسان باشد، هر گره صرف نظر از نوعش باور یکسانی نسبت به نوع گره دیگر دارد.

۳. فرایند به روزرسانی باور $\mu_i(\theta_j|h^t)$ به باور $\mu_i(\theta_j|h^{t+1})$ تنها متاثر از اعمال بازیکن $j$ است.

۴. همه بازیکنان باید باور یکسانی نسبت به نوع بازیکن دیگر داشته باشند. از آنجا که تنها دو بازیکن داریم، این شرط نیز برقرار است.

با برقراری چهار شرط فوق و همچنین با توجه به استراتژی پروفایل‌های تعادلی به‌دست آمده (لم‌های ۱ تا ۵)، این قضیه اثبات می‌شود.

## ۴-۱- مقابله با لاپوشانی

با استفاده از الگوریتم‌های ارائه شده در قسمت قبل می‌خواهیم بهره‌ی میانگین یک لاپوشانی‌کننده را در اثر لاپوشانی محاسبه کنیم. قابل ذکر است که شهرت اولیه‌ای که به یک تازه وارد تخصیص می‌دهیم به گونه ای است که با انجام یک بار عدم همکاری در مرحله‌ی بعد دیگر نتواند از خدمات شبکه استفاده کند. پس از ورود تازه وارد به شبکه جداول شهرت گره‌ها با شناسه تازه وارد به همراه شهرت اولیه‌اش به‌روزرسانی می‌شوند. در آغاز ورود تازه وارد به شبکه از دیدگاه وی همه گره‌های خوشه دارای شهرت $\frac{1}{2}$ هستند.

بهره‌ی یک لاپوشانی‌کننده از انجام یک بار لاپوشانی به صورت زیر خواهد بود:

$$E'(R_{ini}) = \frac{-C_I+\frac{G_C}{2}+0}{3}, G_W = P_e.E'(R_{ini})$$

قابل ذکر است که احتمال ورود لاپوشانی‌کننده به شبکه پس از هر بار لاپوشانی ممکن است متفاوت باشد، اما بهره‌ی میانگین لاپوشانی‌کننده به صورت زیر به دست می‌آید:

$$G_W = P_e.E'(R_{ini})$$

اکنون اگر بهره‌ی لاپوشانی‌کننده را برابر صفر قرار دهیم، برای یک گره خودخواه انگیزه ای برای لاپوشانی باقی نمی‌ماند. بنابراین هزینه‌ی شناسه یک تازه وارد را به صورت زیر تنظیم می‌کنیم:

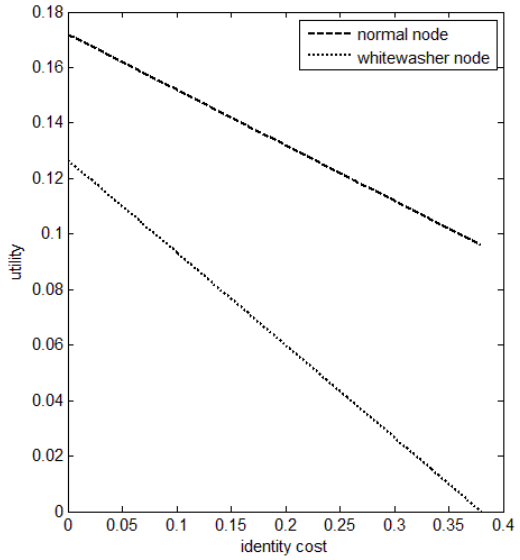
$$C_I = \frac{G_C}{2} \quad (۷)$$

قابل ذکر است که با در نظر گرفتن هزینه شناسه طبق رابطه (۷)، گره‌های تازه وارد قانونی که نوعشان عادی باشد بهره‌ی میانگین مثبت خواهند داشت و بنابراین برای ورود به شبکه دارای انگیزه خواهند بود.

## ۵- نتایج عددی

در بخش قبل مشاهده کردیم که با در نظر گرفتن هزینه‌ی شناسه براساس رابطه‌ی (۷)، گره‌های خودخواه لاپوشانی نمی‌کنند و همچنین گره‌های عادی برای ورود به شبکه انگیزه‌ی کافی را خواهند داشت. در این بخش بررسی می‌کنیم که در صورت در نظر گرفتن هزینه‌ی شناسه‌ی کمتر از رابطه‌ی (۷)، گره‌های خودخواه برای انجام لاپوشانی انگیزه خواهند داشت اما بهره‌ی گره‌های عادی همواره بیشتر از گره‌های لاپوشانی‌کننده است. در شکل ۵ چگونگی تغییرات بهره‌ی گره‌های عادی و لاپوشانی‌کننده براساس تغییر هزینه‌ی شناسه مشاهده می‌کنیم.پارامترهای شبکه را به صورت زیر درنظر می‌گیریم:

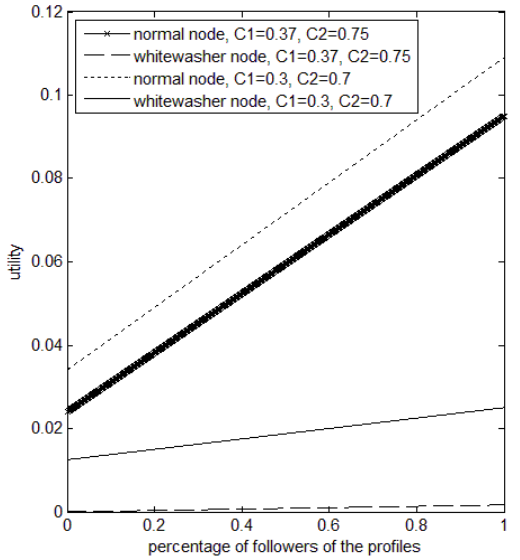
$$G_C = .75, G = .3, C_C = .15, C'_C = .2$$




شکل ۵- بهره گره‌های عادی و لاپوشانی‌کننده براساس هزینه شناسه

با توجه به شکل فوق مشخص است که گره‌های عادی همواره بر لاپوشانی‌کنندگان برتری دارند.

در شکل‌های ۶ و ۷ چگونگی تغییر بهره‌ی گره‌های عادی و لاپوشانی‌کننده براساس افزایش درصد گره‌هایی که از پروفایل‌های نش استراتژی ارائه شده در بخش قبل پیروی می‌کنند، نشان‌داده‌شده‌است. در این دو شکل، عدم پیروی بازیکنان از پروفایل‌های استراتژی قبلی را با انتخاب آستانه‌ای بیشتر برای ارائه‌ی خدمات به گره‌ها در نظرمی‌گیریم. به طور دقیق‌تر به جای در نظر گرفتن مقدار آستانه‌ی $\frac{G_C-C_C}{G_C-C_C+C'_C+G}$ به منظور ارائه‌ی خدمات، از مقدار بیشتری استفاده می‌کنیم که در نتیجه‌ی آن گره‌های خودخواه بتوانند نسبت به بخش قبلی تا یک مرحله بیشتر از خدمات شبکه بهره‌مند شوند و سپس بهره‌ی گره‌های عادی و لاپوشانی‌کننده را همانند بخش قبل محاسبه می‌کنیم.




شکل ۶- بهره گره‌های عادی و لاپوشانی‌کننده براساس درصد پیروی‌کنندگان از پروفایل استراتژی نش بیزین

پارامترهای شبکه را در شکل ۶ و ۷ به ترتیب به صورت زیر درنظر می‌گیریم:

$G_C = .75, G = .3, C_C = .15, C'_C = .2$

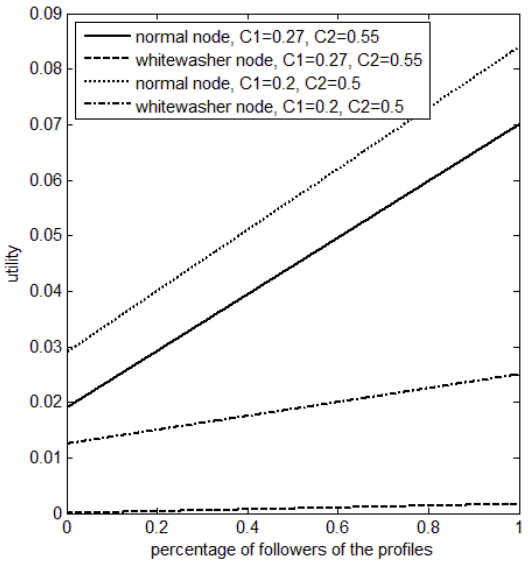
$G_C = .55, G = .2, C_C = .1, C'_C = .15$

قابل ذکر است که $C_1$ هزینه‌ی شناسه با توجه به پیروی از پروفایل‌های بخش قبلی است و $C_2$ هزینه‌ی شناسه با توجه به عدم پیروی از پروفایل‌های بخش قبلی است. این دو هزینه را یکبار طوری درنظرگرفته‌ایم که حمله‌ی لاپوشانی رخ ندهد و بار دیگر طوری درنظرگرفته‌ایم که حمله‌ی لاپوشانی رخ دهد.

با توجه به دو شکل ۶ و ۷ مشخص است که با افزایش درصد گره‌های پیروی کننده از پروفایل‌های استراتژی ارائه شده در بخش قبل، بهره‌ی گره‌های عادی و بهره‌ی لاپوشانی‌کنندگان نیز افزایش می‌یابد. همچنین با مقایسه دو شکل ۶ و ۷ درمی‌یابیم که با افزایش سود حاصل از همکاری، بهره‌ی گره‌های عادی نیز افزایش می‌یابد.

## ۶- نتیجه‌گیری

در این مقاله، با استفاده از نظریه‌ی بازی ابتدا نحوه تراکنش گره‌های داخلی شبکه با استفاده از بازی‌های بیزین مدل شده و سپس با به‌دست آوردن تعادل نش بیزین، پروفایل استراتژی گره‌های خودخواه و گره‌های عادی ارائه شد. براساس پروفایل‌های استراتژی، گره عادی باور خود را نسبت به گره مقابلش شکل می‌دهد و براساس این باور همکاری و یا عدم همکاری را برمی‌گزینند. گره خودخواه نیز درصورتی‌که بهره‌ی حاصل از لاپوشانی بیشتر از بهره‌ی ماندنش در شبکه باشد، لاپوشانی می‌کند.




شکل ۷- بهره گره‌های عادی و لاپوشانی‌کننده براساس درصد پیروی‌کنندگان از پروفایل استراتژی نش بیزین با سود همکاری کمتر

به منظور مقابله با حمله‌ی لاپوشانی هزینه‌ی دریافت شناسه از شبکه را به میزانی در نظر گرفتیم که در نتیجه‌ی آن گره‌های خودخواه برای انجام حمله‌ی لاپوشانی انگیزه‌ای نداشته باشند و همچنین گره‌های عادی نیز برای ورود به شبکه از انگیزه‌ی کافی برخوردار خواهند بود. در نهایت، با تحلیل پارامترهای شبکه مشاهده کردیم که حتی در صورت انجام شدن حمله‌ی لاپوشانی، بهره‌ی گره‌های عادی همواره بیشتر از بهره‌ی گره‌های لاپوشانی‌کننده است. با افزایش درصد پیروی‌کنندگان از پروفایل‌های نش بیزین، بهره‌ی گره‌های عادی و لاپوشانی‌کنندگان نیز افزایش می‌یابد.

در این مقاله، الگوی تحرک گره‌ها و ورود و خروج آنها به شبکه در نظر گرفته نشده‌است. همچنین تحرک گره‌ها در شبکه می‌تواند استراتژیک باشد که در این صورت تحلیل رفتار حمله کنندگان می تواند به عنوان یک پژوهش آتی در نظر گرفته شود. همچنین فرض می‌شود که در بازی دو گره داخلی، هر دو گره با احتمال یکنواخت با یکدیگر وارد تراکنش می‌شوند که این مسئله نیز می‌تواند استراتژیک در نظر گرفته شود و رفتار حمله‌کنندگان در پی آن بررسی و تحلیل شود. در این مقاله، امکان تبانی گره‌های خودخواه با یکدیگر نیز در نظر گرفته نشده‌است و این در حالی است که گره‌های خودخواه می‌توانند برای گرفتن خدمات از شبکه با یکدیگر تبانی کنند. بنابراین، در نظر گرفتن مسئله تبانی میان گره‌ها و بررسی و تحلیل حمل لاپوشانی نیز به عنوان یک پژوهش آتی می‌تواند مطرح شود.

## مراجع

[1] L. Buttyan, and J. Hubaux,"Nuglets: avirtual currency to stimulate cooperation in self-organized mobile ad hoc networks," Technical Report DSC/2001/001., EPFL, Lausanne, 2001.

[2] C. J. Zhong, S. and Y. Yang, "Sprite: Asimple, cheat-proof, credit-based system for mobilead-hoc networks," 22nd IEEE Int. Conf. ComputerCommunications (IEEE INFOCOM03), San Francisco, CA, USA, March-April, pp. 1987-1997, 2003.

[3] J. Cho, A. Swami, and I. Chen, "A surveyon trust management for mobile ad hoc net works," Communications Surveys & Tutorials, vol. 13, no. 4, pp. 562-583, 2011.

[4] P. Michiardi, and R. Molva, "Core: Acollaborative reputation mechanism to enforce nodecooperation in mobile ad hoc networks," 6th IFIP Communications and Multimedia Security Conf., Portorosz, Slovenia, September, pp. 107-121. Kluwer Academic Publishers, 2002.

[5] S. Buchegger, and J. Le Boudec, "A robustreputation system for p2p and mobile ad-hoc networks," 2nd ACM SIGCOMM Workshop on Economics of Peer-to-Peer Systems, Cambridge, MA, USA, June, pp. 119-123. ACM, 2004.

[6] J. Liu, and V. Issarny, "Enhanced reputationmechanism for mobile ad hoc networks," 2nd Int. Conf. on Trust Management, Oxford, UK, March-April, pp.48-62. Springer, 2004.

[7] F. Hendrikx, K. Bubendorfer, and R. Chard, "Reputation systems: A survey and taxonomy," Journalof Parallel and Distributed Computing, vol. 75, pp. 184-197, 2015.

[8] K. Homan, D. Zage, and C. Nita-Rotaru, "Asurvey of attack and defense techniques for reputationsystems," ACM Computing Surveys (CSUR), vol. 42, no. 1, pp. 1:1-1:31, 2009.

[9] M. Fallah, and M. Mouzarani, "A game-based sybil-resistant strategy for reputation systems in self organizing manets," The Computer Journal, Oxford Univ. Press, vol. 54, no. 4, pp. 537-548, 2011.

[10] M. Feldman, and J. Chuang, "The evolution of cooperation under cheap pseudonyms," Proceedings of the Seventh IEEE International Conference on E-Commerce Technology, Washington, DC, USA, July, vol. 24, no. 5, pp. 284-291, 2005.

[11] N. Oualha, and Y. Roudier, "A game theoreticalapproach in securing P2P storage against whitewashers," 18th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises. WETICE'09., Groningen, June, pp. 128-133. IEEE, 2009.

[12] A. M. Kudtarkar, and S. Umamaheswari, "Avoiding whitewashing in P2P networks," *First International Communication Systems and Networks and Workshops, COMSNETS*, 2009.

[13] M. Feldman, C. Papadimitriou, J. Chuang, and I. Stoica, "Free-riding and whitewashing in peer-to-peer systems," IEEE Journal on Selected Areas in Communications, pp. 1010-1019, 2006.

[14] J. Chen, H. Lu, and S. Bruda, "Asolution for whitewashing in P2P systems basedon observation preorder," International Conferenceon Networks Security, Wireless Communications and Trusted Computing, NSWCTC'09., Wuhan, Hubei, April, pp. 547-550, 2009.

[15] C. Zuo, J. Zhou, and H. Feng, "A novelmulti-level trust model to improve the security of P2Pnetworks," 3rd IEEE International Conferenceon Computer Science and Information Technology (ICCSIT), Chengdu, July, pp. 100-104, 2010.

[16] S. Abbas, M. Merabti, and D. Llewellyn-Jones, "Deterring whitewashing attacks in reputation basedschemes for mobile ad hoc networks," Wireless Days(WD), IFIP, Venice, October, pp. 1-6, 2010.

[17] X. Yu, and S. Fujita, "Whitewash-awarereputation management in peer-to-peer file sharingsystems," The 18th International Conference on Parallel and Distributed Processing Techniques andApplications (PDPTA 2012), Las Vegas, January, (WorldComp), 2011.

[18] R. Barra de Almeida, M. Natif, J. Augusto, A. Couto daSilva, and A. Borges Vieira, "Pollutionand whitewashing attacks in a P2P live streamingsystem: Analysis and counter-attack," IEEEInternational Conference on Communications (ICC), Budapest, June, pp. 2006-2010, 2013.

[19] W. Luo, J. Liu, J. Xiong, and L. Wang, "Defending against whitewashing attacks in peer-to-peer file-sharing networks," Proceedings of the 4th International Conference on Computer Engineering and Networks, pp. 1087-1094, 2015.

[20] F. Li, Y. Yang, and J. Wu, "Attack and flee: game-theory-based analysis on interactions among nodes in manets," IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, vol. 40, no. 3, pp. 612-622, 2010.

[21] E. Friedman, P. Resnick, and R. Sami, "Manipulation-resistant reputation systems," In Nisan, N., Roughgarden, T., Tardos, E., and Vazirani, V. (eds.), Algorithmic Game Theory, pp. 677-697, 2007.

[22] A. Jsang, and R. Ismail, "The beta reputation system," Proceedings of the 15th bled electronic commerce conference, June, pp. 2502-2511, 2002.

[23] J. Liu, and V. Issarny, "An incentive compatible reputation mechanism for ubiquitous computing environments," International Journal of Information Security, vol. 6, no. 5, pp. 297-311, 2007.

[24] D. Fudenberg, and J. Tirole, Game theory. Cambridge, Massachusetts, 1991.

**شبنم سراجی** فارغ‌التحصیل رشته مهندسی فناوری اطلاعات گرایش امنیت اطلاعات از دانشکده مهندسی کامپیوتر و فناوری اطلاعات دانشگاه صنعتی امیرکبیر درسال ۱۳۹۳ است. رمزنگاری، امنیت شبکه، شبکه‌های بی‌سیم و استفاده از نظریه بازی در تحلیل موضوعات امنیتی و نرم‌افزاری از زمینه‌های تحقیقاتی مورد علاقه ایشان است.

آدرس پست‌الکترونیکی ایشان عبارت است از:

shabnam.seradji@aut.ac.ir

**مهران سلیمان فلاح** دانشیار مهندسی کامپیوتر در دانشگاه صنعتی امیرکبیر است. موضوعات پژوهشی مورد علاقه او در حوزه تحلیل و راستی آزمایی سیستم‌های امنیت اطلاعات است. استفاده از نظریه بازی در تحلیل و طراحی سیستم‌های مقاوم در مقابل حمله‌های امنیتی و نیز امنیت مبتنی بر زبان‌های برنامه‌سازی محور اصلی پژوهش او در سال‌های اخیر بوده است.

آدرس پست‌الکترونیکی ایشان عبارت است از:

msfallah@aut.ac.ir

**اطلاعات بررسی مقاله:**

تاریخ ارسال: ۱۳۹۴/۰۳/۲۷

تاریخ اصلاح: ۱۳۹۴/۰۴/۰۱

تاریخ قبول شدن: ۱۳۹۴/۰۴/۲۰

نویسنده مرتبط: شبنم سراجی، دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی امیرکبیر، تهران، ایران.