اداره تحصیلات تکمیلی	**بسمه‌تعالی** **فرم تصویب پیشنهادیه پایان‌نامه دانشجوی دوره کارشناسی ارشد در شورای گروه و دانشکده** (ویرایش بهار ۱۳۹۳)	**شناسه: ب/ک/۱** **شماره:** **تاریخ:** **پیوست:**

مشخصات دانشجو :

نام و نام خانوادگی: احمد حقیقی **شماره دانشجویی:** ۹۲۰۸۵۰۴ **دوره: نوبت اول** ☑ **نوبت دوم** ☐

رشته/ گرایش تحصیلی: فناوری اطلاعات/ مخابرات امن **گروه:** مهندسی کامپیوتر **دانشکده:** مهندسی برق و کامپیوتر

نشانی و تلفن : خراسان جنوبی، فردوس

- مشخصات پایان‌نامه:

۱- عنوان :

فارسی : مقابله با حملات انکار سرویس در شبکه‌های موردی سیار از طریق بهبود مسیریابی

انگلیسی : Defending against Denial of Service (DoS) attacks in MANETs by improving routing

نوع پایان‌نامه: کاربردی ☑ بنیادی☐ توسعه‌ای ☑ اولین نیمسال اخذ واحد پایان‌نامه: نیمسال اول ۹۴-۹۳ تعداد واحد: ۶ واحد

- مشخصات استادان راهنما و مشاور:[1]

مسئولیت	نام و نام خانوادگی	آخرین مدرک تحصیلی /مرتبه علمی	گروه/دانشکده/ دانشگاه یا موسسه	امضاء
استاد راهنمای اول	کیارش میزانیان	دکتری / استادیار	کامپیوتر / برق و کامپیوتر / یزد	
استاد مشاور اول	قاسم میرجلیلی	دکتری / دانشیار	برق مخابرات/ برق و کامپیوتر / یزد	
استاد مشاور دوم				

این پیشنهادیه در شورای تحصیلات تکمیلی/ شورای گروه به تاریخ موردبررسی و تصویب قرار گرفت.

نام و امضای مدیر گروه مهدی رضائیان

این پیشنهادیه در شورای تحصیلات تکمیلی دانشکده به تاریخ موردبررسی و تصویب قرار گرفت و اطلاعات مربوط به آن در سامانه پژوهشگاه علوم و فنآوری اطلاعات ایران ثبت و تأییدشده است.

نام و امضای رئیس / معاون آموزشی دانشکده

اصل پیشنهادیه تأییدشده باید به اداره تحصیلات تکمیلی دانشگاه ارسال گردد.

[1] امضای اساتید راهنما و مشاور الزامی است و امضای "از طرف" پذیرفته نمی شود. درصورتی که هریک ازاساتید یاد شده عضو هیات علمی دانشگاه یزد نباشند، ضمن درج نشانی و شماره تلفن آنان، آخرین حکم کارگزینی آن‌ها ضمیمه گردد.

۲- شرح پایان‌نامه:

الف) تعریف موضوع(تعریف مسئله، هدف از اجرا و کاربرد نتایج تحقیق):

در سال‌های اخیر محبوبیت و فراوانی دستگاه‌های سیار و اتصالات بی‌سیم به‌طور چشم‌گیری افزایش یافته است. عدم نیاز به وجود زیرساخت جهت ارتباط، قابلیت سیار بودن دستگاه‌ها، خود پیکربندی و بی‌سیم بودن اتصالات، از بارزترین خصیصه‌های شبکه‌های موردی سیار است که خود دلیلی بر افزایش روزافزون محبوبیت و کاربرد این نوع از شبکه‌ها می‌باشد. از مهم‌ترین کاربردهای شبکه‌های موردی سیار می‌توان به کاربرد آن در امور نظامی برای ارتباط سربازان و ادوات جنگی با یک‌دیگر و مراکز فرماندهی، عملیات نجات در مواردی مانند زلزله، سیل، آتش‌سوزی و ... که بسترهای ارتباطی از بین می‌روند، کاربردهای محلی مانند کنفرانس‌ها، کلاس‌های درس و ... که در آن‌ها شرکت‌کنندگان از طریق اتصال گوشی‌ها و لپ‌تاپ‌ها و سایر تجهیزات خود به یک‌دیگر، به تبادل اطلاعات می‌پردازند، سیستم‌های رأی‌گیری و یا کاربرد آن در موارد شبکه‌های خانگی برای اتصال دستگاه‌ها به یک‌دیگر اشاره نمود.

برخی از خصیصه‌ها و چالش‌های شبکه‌های موردی سیار:[1]

- پهنای باند محدود: اتصالات بی‌سیم معمولاً پهنای باند کم‌تری نسبت به نوع سیمی دارند.
- هم‌بندی پویا: ماهیت پویایی هم‌بندی در این شبکه‌ها مسئله اعتماد بین گره‌ها را مشکل می‌سازد و در مواردی که در شبکه وجود گره‌هایی بدخواه[1] شناسایی می‌شود این اعتماد به‌کلی متزلزل می‌شود.
- سربار مسیریابی: در شبکه‌های موردی سیار گره‌ها متحرک بوده و مکان آن‌ها تغییر می‌کند، لذا مسیرها فقط برای مدتی معین معتبر بوده و پس از جابجایی گره‌ها و خارج شدن از محدوده یک‌دیگر، مسیرهای قبلی از اعتبار ساقط می‌شوند.
- مشکل‌ترمینال مخفی: این مشکل مربوط به حالتی است که بسته‌ها در گره دریافت‌کننده دچار تصادم می‌شوند، دلیل تصادم این است که گره‌های فرستنده برای مقصد، در شعاع دید یک‌دیگر نیستند و لذا هم‌زمان اقدام به ارسال می‌کنند.
- گم‌شدگی بسته: وجود مواردی هم‌چون مشکل‌ترمینال مخفی، تداخل[2]، پیوندهای یک‌طرفه[3] و شکستن مسیرها به دلیل سیار بودن گره‌ها، منجر به بالا رفتن نرخ گم‌شدگی بسته‌ها در شبکه‌های موردی سیار می‌شود.
- محدودیت انرژی: دستگاه‌هایی که در شبکه استفاده می‌شوند هرکدام متناسب با اندازه و وزن آن‌ها، دارای مقدار مشخصی ظرفیت ذخیره‌سازی انرژی هستند.
- مشکلات امنیتی: ماهیت بی‌سیم بودن شبکه‌های موردی سیار چالش‌های امنیتی جدیدی را به وجود آورده است. برای مثال یک رسانه بی‌سیم در برابر استراق سمع آسیب‌پذیر می‌باشد. مهم‌تر اینکه به دلیل وابستگی این شبکه به همکاری بین گره‌ها، شبکه در برابر مسائل زیادی آسیب‌پذیر می‌شود که در ادامه بیش‌تر توضیح داده خواهد شد.

به دلیل ماهیت سیار بودن گره‌ها و مواردی مانند محدودیت منابع انرژی گره‌ها، پروتکل‌های مسیریابی متداول، برای این‌گونه شبکه‌ها مناسب به نظر نمی‌رسد و لذا محققان را بر آن داشت تا پروتکل‌های مسیریابی جدیدی را ارائه دهند. دو نمونه بسیار مشهور این پروتکل‌ها AODV[4] [2] (RFC3561) و DSR[5][3] (RFC4728) است. هر دو نوع پروتکل از نوع براساس-تقاضا[6] می‌باشند، به‌این معنی که عمل یافتن مسیر جدید و معتبر به گره مقصد زمانی انجام می‌شود که گره مبدأ قصد ارتباط با گره مقصد را داشته باشد.[4]

همان‌طور که در بالا به‌آن اشاره شد به دلیل نبود زیرساخت در شبکه‌های موردی سیار، عمل مسیریابی و هدایت بسته‌ها توسط خود گره‌های تشکیل‌دهنده شبکه انجام می‌شود و لذا نیاز به همکاری امری حیاتی است. بنابراین وقتی گرهی عمداً از همکاری امتناع ورزد، می‌تواند بر شبکه اثری سوء داشته باشد و عملکرد شبکه را مختل و بازدهی را کاهش دهد. برای مثال در هر دو پروتکل مسیریابی یادشده (DSR , AODV) وقتی گره مبدأ قصد ارسال دارد، اگر از قبل مسیری برای رسیدن به مقصد نداشته باشد، فاز

---

[1] Malicious
[2] Interference
[3] Uni-directional
[4] Ad hoc On-Demand Distance Vector
[5] Dynamic Source Routing
[6] On-demand

تشخیص مسیر[1] را اجرا می‌کند. در این فاز، گره بسته‌ای RREQ[2] ارسال می‌کند؛ این بسته در کل شبکه فراپخشی[3] می‌شود تا مسیری به مقصد یافت شود، روش پاسخ دادن و یافتن مسیر در DSR با AODV تفاوت دارد، ولی در هر دو روش اعتماد به گره‌های میانی امری اجتناب‌ناپذیر است، چراکه پاسخ به این RREQ می‌تواند توسط گره‌های میانی صورت گیرد. حال اگر یک یا شماری از گره‌های میانی بدخواه باشند می‌توانند عملکرد شبکه را تهدید کنند و باعث اختلال در ارتباط گره‌ها شوند. دو نمونه مشهور ازاین‌گونه خراب‌کاری‌ها حملات چاله سیاه[4] و چاله خاکستری[5] می‌باشند که توسط گره‌های بدخواه میانی صورت می‌گیرد. این حملات در ردیف حملات انکار سرویس[6] قرار می‌گیرند چراکه با قطع کردن ارتباط و یا اخلال در آن موجب می‌شوند تا مشتری[7] نتواند سرویس موردنظر خود را از کارگزار[8] دریافت کند.

در زیر به‌اختصار به معرفی حملات چاله سیاه و چاله خاکستری می‌پردازیم.

حملات چاله سیاه:

در این نوع از حملات وقتی بسته‌ای RREQ توسط گره بدخواه دریافت می‌شود، بلافاصله یک بسته پاسخ (RREP[9]) جعلی ارسال می‌کند و ادعا می‌کند که نزدیک‌ترین مسیر به مقصد را می‌داند. این بسته‌ی RREP جعلی به مبدأ می‌رسد و لذا مبدأ مسیر اعلام‌شده توسط گره بدخواه را انتخاب کرده و شروع به ارسال بسته‌هایش می‌کند. حال وقتی بسته‌های داده به گره بدخواه می‌رسد، گره تمامی بسته‌ها را دور ریخته[10] و لذا موجب می‌شود هیچ بسته‌ای به مقصد نرسد، به عبارتی ارتباط بین مبدأ و مقصد از دید طرفین قطع است. به همین دلیل این حمله از نوع انکار سرویس به شمار می‌آید. [5]

حملات چاله خاکستری:

این حمله در پاسخ دادن به RREQ ها به دو طریق عمل می‌کند، حالت اول این حمله کاملاً شبیه حمله چاله سیاه است یعنی گره به تمامی RREQ ها پاسخ می‌دهد و خود را گرهی جا می‌زند که کوتاه‌ترین مسیر را دارد، در حالت دوم گره در فاز تشخیص مسیر به بسته‌های RREQ مانند سایر گره‌های شبکه عمل می‌کند و رفتار بدخواه گونه از خود بروز نمی‌دهد.

تفاوت عمده این حمله با چاله سیاه در نحوه برخورد با بسته‌های داده است، در این نوع حملات وقتی گره برای عبور بسته‌ها توسط مبدأ انتخاب شد، گره بدخواه تمامی بسته‌ها را دور نمی‌ریزد، بلکه آن‌ها به‌صورت تصادفی و یا طبق الگویی خاص دور می‌ریزد[5] مثلاً بسته‌ها با مقصد خاص یا شرایطی خاص را در زمان‌هایی معین دور می‌ریزد، این امر سبب می‌شود که تشخیص این‌گونه حملات بسیار مشکل‌تر از نوع چاله سیاه باشد، چراکه گره گاهی رفتار بدخواه و گاهی مانند سایر گره‌های معمولی رفتاری عادی از خود نشان می‌دهد و همین امر، به‌کارگیری روش‌های مبتنی بر اعتماد را نیز دچار مشکل می‌سازد.

لازم به ذکر است که حتی در صورت عدم وجود گره بدخواه در شبکه، RREP فرستاده شده توسط گرهی میانی، همواره مسیری معتبر را نشان نمی‌دهد؛ چرا که به دلیل سیار بودن گره‌ها، مسیرها شکسته شده، و اعتبار خود را از دست می‌دهند و بایستی بین این نوع از RREP ها و آن‌هایی که توسط گره‌های بدخواه ارسال می‌شوند تمایز قائل شد. به عنوان مثال پروتکل اولیه DSR فاقد مکانیزمی مناسب جهت حذف مسیرهای کهنه بود، لذا این گونه مسیرها در حافظه گره باقی می‌ماند و این خود نرخ ارسال RREP های نامعتبر (شامل مسیر کهنه) را افزایش می‌داد. البته امروزه این مشکل با وجود راهکارهای پیشنهاد شده[6] تا حد زیادی حل شده به نظر می‌رسد، و هرچند که مشکل به طور کامل رفع نشده است، ولی می‌توان با به‌کارگیری روش‌های موجود، به میزان قابل قبولی درمورد تازه بودن مسیرها اطمینان حاصل کرد.

از آنجایی که برخی از کاربردهای شبکه‌های موردی سیار در مواردی حساس و حیاتی مانند نظامی یا امداد و نجات می‌باشد اهمیت امنیت در آن بسیار بیشتر به چشم می‌خورد، چراکه خسارات وارده می‌تواند فراتر از خسارات مادی باشد. آنچه ما می‌خواهیم انجام دهیم ارائه بهبودی در پروتکل مسیریابی است تا بتوان آن را در برابر حملات انکار سرویس مقاوم سازد.

ب) سابقه تحقیق:

---

[1] Route discovery
[2] Route Request
[3] Broadcast
[4] Black hole
[5] Gray hole
[6] Denial of Service
[7] Client
[8] Server
[9] Route Reply
[10] Drop

در سال ۲۰۰۳ Ramaswamy و همکارانش روشی را برای مقابله با حملات چاله سیاه با استفاده از پروتکل AODV ارائه دادند که علاوه بر جدول مورد استفاده در پروتکل AODV، یک جدول دیگر به نام DRI[1] را به کار بردند که سه ستون دارد، ستونی برای نام گره، ستون From که مقدار ۱ در این ستون مشخص می‌کند گره ما بسته‌اش را از این گره دریافت کرده است و ستون Through که مقدار ۱ در این ستون به معنی این است که گره ما بسته‌هایش را از طریق این گره ارسال کرده است، سپس وقتی گرهی میانی RREP می‌فرستد، فرستنده در صورت نیاز یک بسته RREQ اضافی[2] می‌فرستد و در بسته‌ی RREP اضافی[3] گره مربوطه جدول DRI خود را می‌فرستد، سپس گره مبدأ با مقایسه این جدول‌ها با یک‌دیگر می‌تواند در مورد بدخواه بودن گره‌ها تصمیم‌گیری نماید.[7] پس از آن در سال ۲۰۱۲ Singh Bindra و همکارانش این روش را بهبود دادند و جدول جدید خود را EDRI نامیدند[8] و در سال ۲۰۱۳ Hiremani و همکارش روش EDRI را بهبود داده و آن را MEDRI نامیدند[9].

در سال ۲۰۱۳ R. Jhaveri روش قبلی خود و همکارانش با نام R-AODV را ارتقا داد. در روش MR-AODV هر گره بر اساس مشاهده‌هایش و RREQ و RREP هایی که دریافت کرده است مقداری به نام PEAK را محاسبه می‌کند، سپس هر RREP ی که دریافت می‌کند شماره ترتیب[4] آن را با این مقدار PEAK مقایسه کرده و درصورتی که بیشتر از این مقدار باشد گره فرستنده بسته را به‌عنوان گره بدخواه شناخته و لیست گره‌های بدخواه شناسایی شده را در RREQ خود قرار می‌دهد تا سایر گره‌ها را مطلع سازد. لازم به ذکر است که PEAK حداکثر مقداری است که شماره ترتیب بسته RREP می‌تواند داشته باشد، و از آنجایی که گره بدخواه برای تازه[5] نشان دادن RREP خود بیشترین شماره ترتیب را در بسته قرار می‌دهد، این روش می‌تواند گره‌های بدخواه را شناسایی کند.[10]

در سال ۲۰۱۴ Mohanapriya و همکارانش برای مقابله با حملات چاله خاکستری، بهبودی در پروتکل DSR ایجاد نمودند که در آن داده‌ها به‌صورت بلوکه‌ای ارسال می‌شود و طول هر بلوک در ابتدای ارسال توسط مبدأ به مقصد اعلام می‌شود، سپس وقتی مقصد کاهش قابل ملاحظه‌ای را در داده‌های دریافتی مشاهده می‌کند اقدام به اجرای فاز تشخیص گره بدخواه می‌کند. در این فاز از گره با فاصله ۲ گام عقب‌تر سؤال می‌شود تا بسته‌های دریافتی و ارسالی‌اش را اعلام کند و این روال را تکرار می‌کند و اطلاعات دریافت شده را مقایسه می‌کند، وقتی تفاوت در داده‌های رسیده مشاهده شد، گره‌های IDS موجود به نظارت بر گره‌های مشکوک می‌پردازند و در صورت مشاهده رفتار بدخواه از گره تحت نظر، آن گره را به‌عنوان گره بدخواه معرفی می‌کنند.[11]

در سال ۲۰۱۴، J. Chang و همکارانش الگوریتم قبلی خود با نام CBDS[6] را که در سال ۲۰۱۲ ارائه نموده بودند ارتقا دادند، در روش CBDS گره مبدأ قبل از اقدام به ارسال بسته RREQ (برای یافتن آدرس مقصد)، با یکی از همسایه‌های خود همکاری می‌کند و آدرس همسایه‌اش را در یک بسته‌ی RREQ که به بسته طعمه[7] مشهور است قرار می‌دهد و آن را ارسال می‌کند، حال از آنجایی که گره‌های بدخواه به هر RREQ دریافتی پاسخ می‌دهند، وقتی گره بدخواه به این بسته پاسخ می‌دهد با استفاده از سازوکاری که در CDBS تعبیه‌شده، گره مبدأ می‌تواند گره بدخواهی که RREP را فرستاده شناسایی کند و سپس در مرحله بعدی این گره را در مسیریابی شرکت نمی‌دهند. روش پیشنهادی این قابلیت را دارد که در حین ارسال داده وقتی گم‌شدگی بسته‌ها از حد آستانه عبور می‌کند، فاز تشخیص گره بدخواه را دوباره اجرا کند تا گره بدخواه ای که ابتدا کشف نشده است را شناسایی کند.[12]

ج) کلمات کلیدی:

فارسی: شبکه‌های موردی سیار، مسیریابی، حملات چاله سیاه، حملات انکار سرویس

انگلیسی: Mobile ad-hoc networks, routing, black hole attacks, Denial of Service (DoS) Attacks

[1] Data Routing Information
[2] Further Request
[3] Further Reply
[4] Sequence number
[5] Fresh
[6] Cooperative Bait Detection Scheme
[7] Bait

د) فرضیات (یا سئوالات پژوهشی):

۱. چگونه می‌توان حملات انکار سرویس را در شبکه‌های موردی سیار تشخیص داد؟
۲. چگونه می‌توان سازوکاری تعبیه نمود تا بتوان گره بدخواه در شبکه را شناسایی کرد؟
۳. چگونه می‌توان با کم‌ترین تغییرات در پروتکل‌های مسیریابی موجود، آن‌ها را در برابر حملات انکار سرویس مقاوم‌تر ساخت؟

هـ) روش تحقیق (مخصوص دانشکده‌های علوم انسانی، منابع طبیعی و هنر و معماری):

و) مراحل اجرای پروژه و زمان‌بندی:

مراحل اجرا / زمان‌بندی	آبان ۹۳	آذر ۹۳	دی ۹۳	بهمن ۹۳	اسفند ۹۳	فروردین ۹۴	اردیبهشت ۹۴	خرداد ۹۴	تیر ۹۴	مرداد ۹۴	شهریور ۹۴
جستجوی و بررسی منابع	■										
شبیه‌سازی پروتکل‌های پایه	■	■									
تجزیه‌وتحلیل روش پیشنهادی			■	■	■	■					
طراحی، پیاده‌سازی و اجرای روش پیشنهادی					■	■	■	■	■		
جمع‌بندی و نگارش پایان‌نامه							■	■	■	■	■

ز) فهرست منابع ومآخذ:

[1] Aarti and D. S. S. Tyagi, “Study of MANET : Characteristics , Challenges , Application and Security Attacks,” *Int. J. Adv. Res.*, vol. 3, no. 5, pp. 252–257, 2013.

[2] S. R. Das, E. M. Belding-Royer, and C. E. Perkins, “Ad hoc On-Demand Distance Vector (AODV) Routing,” 2003.

[3] D. A. Maltz and D. B. Johnson, “The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4,” 2007.

[4] M. Abolhasan, T. Wysocki, and E. Dutkiewicz, “A review of routing protocols for mobile ad hoc networks,” *Ad Hoc Networks*, vol. 2, no. 1, pp. 1–22, Jan. 2004.

[5] R. H. Jhaveri, S. J. Patel, and D. C. Jinwala, “DoS Attacks in Mobile Ad Hoc Networks: A Survey,” in *2012 Second International Conference on Advanced Computing & Communication Technologies*, 2012, pp. 535–541.

[6] N. A. Husieen, O. B. Ghazali, S. Hassan, and M. M. Kadhum, “Route Cache Update Mechanisms in DSR Protocol – A Survey,” vol. 4, pp. 136–141, 2011.

[7] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, “Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks,” in *International Conference on Wireless Networks (ICWN’03), Las Vegas, Nevada, USA*, 2003, vol. 2003, pp. 1–7.

[8] G. Singh Bindra, A. Kapoor, A. Narang, and A. Agrawal, “Detection and removal of co-operative blackhole and grayhole attacks in MANETs,” in *2012 International Conference on System Engineering and Technology (ICSET)*, 2012, pp. 1–5.

[9] V. A. Hiremani and M. M. Jadhao, “Eliminating co-operative blackhole and grayhole attacks using modified EDRI table in MANET,” in *2013 International Conference on Green Computing, Communication and Conservation of Energy (ICGCE)*, 2013, pp. 944–948.

[10] R. H. Jhaveri, “MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV Based MANETs,” in *2013 Third International Conference on Advanced Computing and Communication Technologies (ACCT)*, 2013, pp. 254–260.

[11] M. Mohanapriya and I. Krishnamurthi, “Modified DSR protocol for detection and removal of selective black hole attack in MANET,” *Comput. Electr. Eng.*, vol. 40, no. 2, pp. 530–538, Feb. 2014.

[12] J.-M. Chang, P.-C. Tsou, I. Woungang, H.-C. Chao, and C.-F. Lai, “Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach,” *IEEE Syst. J.*, vol. PP, no. 99, pp. 1–11, 2014.

۳- مواد، وسایل و دستگاه‌های مورد نیاز و منبع تأمین:

نام ماده یا دستگاه	محل تامـین
دسترسی به اینترنت پر سرعت در محیط دانشگاه	

۴- تعهد نامه دانشجو:*

اینجانب **احمد حقیقی** متعهد می‌شوم که با توجه به مفاد این پیشنهادیه به‌طور تمام وقت، زیر نظر اساتید راهنما و مشاور انجام وظیفه نمایم. ضمنا با اطلاع از اینکه کلیه حقوق مادی و معنوی مترتب بر نتایج حاصل از پایان‌نامه (اعم از چاپ مقاله، کتاب، ارائه به بخش صنعت و ...) متعلق به دانشگاه یزد خواهد بود از انتشار نتایج حاصل از آن بدون مجوز دانشگاه خودداری نمایم.

تاریخ و امضای دانشجو

*موارد مهم که دانشجویان محترم باید به آن توجه داشته باشند:

۱ – دانشجو موظف است با نظر استاد/اساتید راهنما پیشنهادیه پایان‌نامه خود را حداکثر تا ۸ هفته پس از شروع نیمسال سوم به گروه آموزشی تحویل دهد. همچنین دانشجو باید با اعمال تغییرات موردنظر گروه و دانشکده، پیشنهادیه پایان‌نامه خود را حداکثر تا ۱۰ هفته پس از شروع نیمسال سوم به تصویب شورای گروه و حداکثر تا ۱۴ هفته پس از شروع نیمسال سوم به تصویب شورای دانشکده برساند.

۲ - پس از تصویب پیشنهادیه در دانشکده، اطلاعات مربوطه توسط دانشجو باید در سامانه پژوهشگاه علوم و فناوری اطلاعات ایران به آدرس www.irandoc.ac.ir ثبت و توسط مدیر گروه /استادراهنما تأیید گردد.

۳ - پس از تصویب پیشنهادیه پایان‌نامه، باید نسخه اصلی پایان‌نامه و تاییدیه ثبت پیشنهادیه در پژوهشگاه علوم و فناوری اطلاعات ایران جهت بایگانی در پرونده دانشجو به حوزه تحصیلات تکمیلی دانشگاه ارسال شود.