
بسم الله الرحمن الرحيم

دانشگاه قم

دانشکده فنی و مهندسی

پایان‌نامه دوره کارشناسی ارشد

عنوان:

چارچوب خودمختار برای مسیریابی بر مبنای اعتماد در شبکه های بی سیم خودسازمانی

استاد راهنما:

دکتر زینب موحدی

نگارنده:

فهیمه بیان

تابستان/ ۱۳۹۲

«صورتجلسه دفاع از پایان‌نامه کارشناسی ارشد»

با تأییدات خداوند متعال و با استعانت از حضرت ولی عصر (عجل الله تعالی فرجه الشریف)

جلسه دفاع از پایان‌نامه کارشناسی ارشد خانم: فهیمه بیان رشته: مهندسی فناوری اطلاعات – تجارت الکترونیک تحت عنوان: چارچوب خودمختار برای مسیریابی بر مبنای اعتماد در شبکه های بی سیم خودسازمانی با حضور هیأت داوران در محل دانشگاه قم در تاریخ ۱۳۹۲/۰۷/۱۱ تشکیل گردید.

در این جلسه، پایان‌نامه با نمره (به عدد:.....، به حروف:.....) و با درجه عالی بسیار خوب خوب قابل قبول مورد دفاع قرار گرفت.

نام و نام خانوادگی	سمت	مرتبه علمی	امضاء
دکتر زینب موحدی	استاد راهنما	استادیار	
دکتر یعقوب فرجامی	استاد ناظر	استادیار	
دکتر فرانک فتوحی	استاد ناظر	استادیار	
دکترعفت گلپر رابوکی	نماینده کمیته تحصیلات تکمیلی	استادیار	

معاون آموزشی و پژوهشی دانشکده

نام و امضاء

مدیر امور آموزش و تحصیلات تکمیلی

نام و امضاء

تقدیم به:

پدر و مادر و همسر عزیزم که با محبت و صبر خود از من حمایت نمودند.

تشکر و قدردانی:

حمد و سپاس خدای را که توفیق کسب دانش و معرفت را به ما عطا فرمود .در اینجا برخود لازم می دانم از تمامی اساتید بزرگوار، به ویژه اساتید دوره کارشناسی ارشد که در طول سالیان گذشته مرا در تحصیل علم و معرفت یاری نموده‌اند تقدیر و تشکر نمایم.

از استاد گرامی و بزرگوار سرکار خانم دکتر زینب موحدی که راهنمایی اینجانب را در انجام تحقیق و پژوهش این پایان نامه تقبل نموده‌اند نهایت تشکر و سپاسگزاری را دارم. بنده، حضور ایشان را در تمام طول دوره راهنمایی، همچون یاوری در کنار خود حس کرده و علاوه بر استفاده از علم ایشان، از فضائل و کرامات اخلاقی بیشمار ایشان بهره بردم.

چکیده

شبکه های بی سیم خودسازمانی با ویژگی های پویایی، تحرک و منابع محدود مشترک شناخته می شوند. کارایی این شبکه ها وابسته به همکاری بین نودهای توریع شده است. درنتیجه این شبکه ها به یک چارچوب مدیریت اعتماد نیازمند هستند که اعتماد را در شبکه استقرار دهد و رفتار نودها با یکدیگر را مدیریت کند.

در این پایان نامه یک چارچوب خودمختار برای مسیریابی بر مبنای اعتماد در شبکه های بی سیم خودسازمانی ارائه می شود که در فرایند مسیریابی شبکه، از مقادیر اعتماد محاسبه شده توسط سیستم اعتماد استفاده می کند. این چارچوب خودمختار با استفاده از یک آستانه تطبیق پذیر که با توجه به محتوای اساسی شبکه تنظیم شده است، نودهای نرمال و بدرفتار شبکه را شناسایی می کند. مدل پیشنهادی دو هدف اصلی دارد. اول، یک چارچوب تنبیهی در مقابل نودهای بدرفتار ارائه کرده و از سرویس دهی به آن ها خودداری می کند. در نتیجه نودها برای دریافت خدمات از شبکه به رفتار نرمال ترغیب می شوند. دوم، مدل ارائه شده برای ارسال داده، مسیری با بیشترین اعتبار را انتخاب می کند تا اثر حذف بسته ها توسط نودهای بدرفتار را کاهش دهد. این ویژگی ها طول عمر شبکه را افزایش داده و منابع شبکه را به صورت کارا به مصرف می رساند.

برای نشان دادن اثر بخشی مدل ارائه شده، ATRS بر روی پروتکل مسیریابی DSR پیاده سازی شده و عملکرد آن در حضور تعداد متفاوت نودهای بدرفتار، با عملکرد DSR مقایسه شده است. نتایج کسب شده توسط ATRS در مقابل DSR بهبود مناسبی را از جهت نرخ حذف نودهای بدرفتار، تأخیر و نرخ بسته های ارسالی نشان داد.

همچنین در این پایان نامه، یک دسته بندی جدید برای حملات فریبنده مقدار اعتماد، ارائه شد. علاوه بر این طبقه بندی جدیدی برای معیارهای ارزیابی معرفی شد تا بتوان چارچوب های مدیریت اعتماد را به طور یکسانی سنجید.

کلمات کلیدی: چارچوب خودمختار برای مسیریابی بر مبنای اعتماد، شبکه های بی سیم خود سازمانی، موتور خودمختار تعیین آستانه، کشف مسیر، انتخاب مسیر

فهرست مطالب

عنوان **صفحه**

فصل اول : مقدمه ۱

۱-۱ محتوا ۱

۱-۲ اهداف ۵

۱-۳ نوآوری ها ۶

۱-۴ ساختار پایان نامه ۹

فصل دوم : دسته بندی چارچوب های مدیریت اعتماد و معیارهای ارزیابی ۱۰

۲-۱ مقدمه ۱۰

۲-۲ کارهای پیشین ۱۲

۲-۳ طبقه بندی ارائه شدهٔ ما از حملات تحریف اعتماد ۱۴

۲-۳-۱ حملات دروغ گویی ۱٤

۲-۳-۲ حملات دو چهره ۱۵

۲-۴ چارچوب های مدیریت اعتماد مقاوم در برابر حملات تحریف اعتماد ۱۷

۲-۴-۱ چارچوب های مقاوم نسبت به حملهٔ دو چهره ۱۷

۲-۴-۱-۱ بلا ۱۷

۲-۴-۱-۲ چارچوب خود مختار نظارت دانش اعتماد (ATMS) ۲۰

۲-۴-۱-۳ المتیری ۲۲

۲-۴-۱-۴ دیتاکلاس ۲٤

۲-۴-۲ چارچوب های مدیریت اعتماد مقاوم نسبت به حملهٔ دروغ گویی ۲٦

۲-۴-۲-۱ AFStrust ۲٦

۲-۴-۲-۲ ترودی ۲۸

۲-۴-۲-۳ اعتبار مشارکتی (CORE) ۳۱
۲-۴-۲-۴ انگیزه برونی و امن برمبنای اعتماد (SORI) ۳۳
۲-۵ دسته بندی پیشنهادی ما از معیارهای ارزیابی چارچوب های مدیریت اعتماد .. ۳۶
۲-۶ بحث و مقایسه ۴۳
فصل سوم : ارائه چارچوبی خودمختار برای مسیریابی بر مبنای اعتماد(ATRS) ۴۶
۳-۱ مقدمه ۴۶
۳-۲ انگیزه ۴۷
۳-۳ مراحل فرایند مسیریابی ۴۸
۳-۳-۱ کشف مسیر ٤٨
۳-۳-۲ انتخاب مسیر ٤٨
۳-۴ تاثیر اعتماد بر مراحل مسیریابی ۴۸
۳-۴-۱ کشف مسیر بر مبنای اعتماد ٤٩
۳-۴-۲ انتخاب مسیر بر مبنای اعتماد ٤٩
۳-۵ بررسی بخش استقرار اعتماد در مقالات مطرح شده ۴۹
۳-۵-۱ چارچوب های مدیریت اعتمادی که مقادیر اعتماد را در فاز کشف مسیر به کار بستند ۵۰
۳-۵-۲ چارچوب های مدیریت اعتمادی که از مقادیر اعتماد در فاز انتخاب مسیر استفاده کرده اند ۵۱
۳-۵-۳ چارچوب های مدیریت اعتمادی که از مقادیر اعتماد در هردو فاز کشف و انتخاب مسیر استفاده کرده اند ۵۲
۳-۶ ارائه ی چارچوبی خودمختار برای مسیریابی بر مبنای اعتماد(ATRS) ۵۳
۳-۶-۱ موتور خودمختار برای تشخیص سطح اعتبار نودها ٥٤
۳-۶-۲ کشف مسیر مبتنی بر اعتماد ٥٥
۳-۶-۳ انتخاب مسیر ٥٩

۳-۷ نتیجه گیری ۵۹
فصل چهارم : ارزیابی چارچوب خودمختار برای مسیریابی بر مبنای اعتماد(ATRS) ۶۱
۴-۱ مقدمه ۶۱
۴-۲ ویژگی های محیط شبیه سازی ۶۲
۴-۳ معیارهای مورد استفاده ۶۳
۴-۴ نتایج و تحلیل آن ها ۶۴
۴-۴-۱ تحلیل نتایج ۷۰
۴-۶ بحث ۷۱
۴-۷ نتیجه گیری ۷۲
فصل پنجم : نتیجه گیری ۷۳
۵-۱ ساختار ۷۳
۵-۲ خلاصه دستاوردها ۷۳
۵-۳ کارهای آینده ۷۵
منابع و مآخذ به ترتیب ارجاع در متن ۷۷
پیوست الف: واژه نامه انگلیسی به فارسی ۸۲

فهرست جدول ها

عنوان **صفحه**

جدول ۲-۱ مقایسه چارچوب های مدیریت اعتماد..... ۴۱
جدول ۴-۱ پارامتر های اصلی شبیه سازی ۶۳

فهرست شکل‌ها و نمودارها

عنوان **صفحه**

شکل ۲-۱ دسته بندی حملات تحریف اعتماد ۱۴
شکل ۲-۲ چارچوب خود مختار نظارت دانش اعتماد ۲۰
شکل ۲-۳ معیار های ارزیابی چارچوب های مدیریت اعتماد ۳۷
شکل ۳-۱ معماری ATRS ۵۴
شکل ۴-۱ تاثیر درصد حمله کننده و تغییر تعداد نود بر ATRS و DSR. ms=۵m/s و nc=۲۰ ..... ۶۵
شکل ۴-۲ تاثیر درصد حمله کننده و تغییر سرعت نودها بر ATRS و DSR. nn=۵۰ و nc=۲۰ ..... ۶۷
شکل ۴-۳ تاثیر درصد حمله کننده و تعداد ارتباط نودها بر ATRS و DSR. nn=۳۰و ms=۵m/s ۶۹

فهرست علائم و اختصارات (Abbreviations)

MANET	Mobile Ad hoc NETwork
ATRS	Autonomic Trust based Routing Scheme
NS-۲	Network Simulator -۲
DSR	Dynamic Source Routing
NRT	Neighbor Reputation Table
GRT	Global Reputation Table
ATMS	Autonomic Trust Monitoring Scheme
MAEP-K	Monitor Analyze Execution Planning-Knowledge
LTT	Local Trust Table
GTT	Global Trust Table
PDR	Packet Delivery Ratio
MDR	Malicious Drop Ratio
CPU	Central Processing Unit
AHP	Analytical Hierarchy Process
CFStrust	Certainty-Factor trust
CORE	COllaborative REputation
SORI	Secure and Objective Reputation-based Incentive
RF	Request-for-Forwarding
HF	Has-Forwarded
LER	Local Evaluation Record
AE۲ED	Average End To End Delay
MAC	Media Access Controller
MDP	Malicious Detection Performance
CBR	Constant Bit Rate
AODV	Ad-hoc On demand Distance Vector
AOMDV	Ad-hoc On demand Multiple path Distance Vector
AOTDV	Ad-hoc On demand Trusted Distance Vector
TAODV	Trusted AODV
LARS	Locally Aware Reputation System
OCEAN	Observation-based cooperation enforcement in ad hoc networks

فصل اول : مقدمه

۱–۱ محتوا

درسال های اخیر استفاده از سیستم های کامپیوتری و تکنولوژی های ارتباط به طور چشم گیری تکامل داشته است. فراهم کردن رنج وسیعی از سرویس ها برای صدها میلیون کاربر که به شبکه متصلند، تنوع و ناهمگونی ابزارها، تفاوت در تکنولوژی های پایگاه داده و سیستم های ذخیره سازی و بسیاری از دشواری های دیگر، مدیریت سیستم های کامپیوتری و شبکه ها را پیچیده کرده است.

هزینه مدیریت اطلاعات، بخش مهمی از هزینه های سازمان ها را به خود اختصاص می دهد. به علاوه درصد زیادی از شکست های سیستم به علت خطاهای انسانی است. در نتیجه خطاهای مدیریتی انسان هزینه های سنگینی به سازمان ها و به دنبال آن به اقتصاد جهان تحمیل می کند. راه حل این مشکل، ایجاد سیستم های خودمختار بدون نیاز به دخالت انسان است. سیستم های خودمختار مانند شبکه عصبی انسان، باید خود را با شرایط مختلف و تغییرات درونی و محیطی تطبیق دهند.

ایجاد سیستم های خود مختار که خود را مدیریت می کنند مزایای زیادی را فراهم می کند. این سیستم ها حوادث مهم اطراف خود را شناسایی کرده و بدون هیچ دخالت خارجی و انسانی، نسبت به آن ها عکس العمل نشان می دهند. آگاهی از شرایط درونی و محیطی و

تطبیق پذیری از ویژگی های این سیستم هاست. همچنین سیستم های خود مختار از تجربیات گذشته درس گرفته و رفتار خود را در طول زمان بهبود می دهند.

یک شبکه خود خودسازمانی، یک شبکه بی سیم است که به وسیله مجموعه ای از ابزارهای متحرک[۱] تشکیل شده است. این ابزارها بدون وجود هیچ زیرساختی به هم متصل شده اند. در این شبکه ها به علت توزیعی بودن[۲]، برای حمایت از فعالیت ها و بقای شبکه، نودها باید با هم مشارکت کنند.

ایده خود مختاری بیش از هر نوع از مدل های شبکه، در شبکه های خود سازمانی کاربرد دارد و علت آن اهمیت مصرف کارای منابع و پویایی قابل توجه در این شبکه هاست.

شبکه های خود مختار در انواع مختلف شبکه های خودسازمانی از قبیل شبکه های اقتضایی سیار [۳]، شبکه های حسگر بی سیم[۴]، شبکه های بدون زیرساخت وسایل نقلیه[۵] و غیره کاربرد دارد.

بی سیم بودن و تحرک شبکه های خودسازمانی، محدودیت های از قبیل محدودیت در منابع و انرژی را به شبکه تحمیل می کند. در نتیجه نودها به بدرفتاری و عدم مشارکت ترغیب می شوند. که این امر، انقراض شبکه را به دنبال دارد. ایمن سازی این شبکه ها در مقابل انواع بدرفتاری، تنها از طریق رمزنگاری[۶] میسر نخواهد بود. برای برقراری امنیت در چنین شبکه هایی، مکانیزمی مورد نیاز است که نودها را وادار به همکاری کند. به کمک این مکانیزم -که همان اعتماد است- نودهای بدرفتار شناسایی می شوند و از مقادیر اعتبار نودها در تصمیم گیری های شبکه استفاده می شود. بنابرین انگیزه حمله کاهش یافته و کارایی شبکه افزایش می یابد.

مفهوم اعتماد به طور گسترده در حوزه های مختلف علوم کامپیوتر به خصوص در شبکه های کامپیوتری مورد مطالعه قرار گرفته است. شبکه های بدون زیرساخت[۷] از مزایای چارچوب های اعتماد سود می برند. در یک شبکه بدون زیرساخت، هیچ نود مرکزی وجود ندارد تا مسئولیت پیکربندی، مدیریت و تعمیر ایستگاه ها را به عهده بگیرد. با توجه به ویژگی های شبکه های خود مختار، یک نود باید بتواند خود را پیکربندی و مدیریت کند و با استفاده از

---

۱ Mobile
۲ Distribution
۳ Mobile ad hoc networks (MANET)
٤ Wireless sensor networks
٥ Vehicular ad hoc networks (VANET)
٦ Cryptography
۷ Ad hoc

جمع آوری اطلاعات محلی و تبادل آن با همسایه ها، از تجربیات گذشته درس بگیرد. بنابرین هر نود فقط باید با همسایه های مورد اعتمادش تعامل داشته باشد زیرا تبادل اطلاعات با همسایه های غیر نرمال، می تواند خود مختاری شبکه های بدون زیر ساخت را به خطر بیندازد. پس یک سیستم اعتماد باید به نودها کمک کند تا در مورد همسایه های خود تصمیم بگیرند.[۱]

یکی از سیاست های شبکه که می تواند با کمک سیستم اعتماد ارتقا یابد، فرایند مسیریابی است. هدف ما انجام مسیریابی بر مبنای اعتماد در شبکه های خود سازمانی، بخصوص در MANET هاست.

امروزه استفاده از MANET روز به روز در حال گسترش است. بعضی از کاربردهای آن ارتش، بعد از جنگ یا زلزله که زیرساخت های ارتباطی ازبین رفته است، هواشناسی، راهنمایی و رانندگی و بسیاری کاربردهای دیگر است.

در نگاه کلی دو دسته عملیات مرتبط با اعتماد در فرایند مسیریابی اتفاق می افتد: کشف مسیر و انتخاب مسیر. همه سیستم های استقرار اعتماد[۱] به این دو فاز مربوط می شوند. بنابرین سیستم های استقرار اعتماد موجود را می توان با توجه به نوع استفاده از مقادیر اعتماد، به دو دسته تقسم کرد. دسته اول از اطلاعات اعتماد در فاز کشف مسیر و دسته دوم در فاز انتخاب مسیر استفاده می کنند.

کشف مسیر مجموعه تلاش هایی است که یک شبکه برای یافتن مسیر به سمت مقصد انجام می دهد تا داده ای را به او ارسال کند. این فرایند شامل انتشار درخواست مسیر[۲] توسط مبدا، تکرار انتشار آن توسط نودهای میانی، تحویل آن به مقصد و ارسال بسته پاسخ مسیر[۳] از سوی نود مقصد است. در فاز کشف مسیر، اطلاعات اعتماد نودها برای تصمیم گیری در مورد تکرار انتشار یک بسته درخواست مسیر در شبکه مورد استفاده قرار می گیرد.

فرایند انتخاب مسیر، شامل انتخاب بهترین مسیر به سمت مقصد، از بین مسیرهای موجود و با توجه به معیارهای مسیریابی است. به منظور اطمینان از انتقال صحیح بسته های داده، اطلاعات اعتماد نودها به عنوان یک معیار برای انتخاب مسیری با معتبر ترین نودهای میانی، مورد استفاده قرار می گیرد.

---

۱ Trust establishment systems
۲ Route request
۳ Route reply

چارچوب ها استقرار اعتماد که در دسته اول قرار می گیرند، فقط به نودهای نرمال سرویس داده و از انجام درخواست نودهای بدرفتار خودداری می کنند. در مدل همکاری برمبنای مشاهده(OCEAN[1]) [۲] یک لیست اجتناب تعریف می شود که شامل نودهای بدرفتار است. در این مدل، ترافیک رسیده از سوی یک نود بدرفتار که در لیست اجتناب ثبت شده است، نادیده گرفته می شود. مدل انگیزه برونی و امن برمبنای اعتماد (SORI[2]) [۳] نودهای بدرفتار موجود در همسایگی خود را با حذف احتمالی بسته هایشان تنبیه می کند. در مدل اعتبار مشارکتی (CORE[3]) [۴] فقط بسته های درخواست مسیر دریافت شده از سوی یک مبدا معتبر سرویس دهی می شوند. در مدل بردار فاصله مورد تقاضای موردی بر مبنای اعتماد(TAODV[4]) [۵] هر نود میانی از انجام فرایند مسیریابی مربوط به نودها نا معتبر، سر باز می زند. چارچوب های موجود در این دسته، بسته های دریافت شده را به صورت انتخابی سرویس می دهند؛ بنابرین آن ها در مصرف منابع محدود شبکه صرفه جویی می کنند. اما در این مدل ها به علت استفاده از نودهای بدرفتار در فرایند ارسال داده و عدم انتقال بسته از مسیر امن، احتمال حذف بسته افزایش می یابد.

مدل های استقرار اعتماد متعلق به گروه دوم، اطلاعات اعتماد را تنها در فاز انتخاب مسیر استفاده می کنند. در المتیری [۶] و لیندسی [۷] مبدا از بین مسیرهای موجود منتهی به مقصد، معتبر ترین مسیر را انتخاب می کند. این چارچوب ها صحت ارسال بسته را به وسیله ارسال آن ها از مسیر امن، ضمانت می کنند؛ اما این مدل ها از بدرفتاری جلوگیری نمی کنند. به علاوه، در مواردی که نوع حمله خودخواهی، شبکه را تهدید می کند، این سیاست، نه تنها نودهای بدرفتار را تنبیه نکرده بلکه آن ها را به استفاده آزادانه از منابع شبکه و عدم مشارکت تشویق می کند.

تعدادی از چارچوب های مدیریت اعتماد، مسیریابی را از طریق ایمن سازی هر دو فاز کشف مسیر و انتخاب مسیر انجام می دهند. در مدل بردار فاصله مسیر امن مورد تقاضای موردی (AOTDV[5]) [۸]، دیتاکلاس [۹] و سیستم اعتبار آگاه محلی (LARS[6]) [۱۰] ترافیک دریافت شده از نودهای بدرفتار در فاز کشف مسیر توسط همسایه های آن ها، نادیده

---

۱ Observation-based Cooperation Enforcement in Ad hoc Networks
۲ Secure and Objective Reputation-based Incentive
۳ COllaborative REputation
٤ Trusted AODV
٥ Ad hoc On-demand Trusted-path Distance Vector
٦ Locally Aware Reputation System

گرفته می شود. در فاز انتخاب مسیر، نود مبدا برای انتخاب مسیر مناسب برای ارسال داده تصمیم گیری می کند. چارچوب های موجود در این دسته، نودهای نامعتبر موجود در همسایگی خود را با خودداری از انجام درخواست هایشان تنبیه می کنند. همچنین این مدل ها ارسال داده را از طریق مسیرهای امن انجام می دهند؛ بنابرین امنیت به طور تقریبی محقق می شود. هیچ یک از مدل های بررسی شده در این دسته، نفع نود مقصد از دریافت بسته را در نظر نگرفته و بسته را حتی درصورت بدرفتار بودن مقصد، ارسال می کنند. به علاوه، نقش نود بعدی[۱] بدرفتار در هیچ یک از مدل ها مورد توجه قرار نمی گیرد و بسته به شرط معتبر بودن مبدا آن، برای یک نود بعدی نامعتبر ارسال می شود.

در این پایان نامه، یک چاچوب خودمختار برای مسیریابی بر مبنای اعتماد در شبکه های بی سیم خودسازمانی ارائه می شود که مقادیر اعتماد را در فرایندهای کشف مسیر و انتخاب مسیر به کار می بندد. این مدل خودمختار، نودهای نرمال و بدرفتار را با استفاده از یک آستانه تطبیق پذیر که با توجه به شرایط شبکه تنظیم شده است، شناسایی می کند. چارچوب پیشنهادی، نقش تمام نودهای منتفع را در صورت بدرفتار بودن، برای تنبیه در نظر می گیرد. از ویژگی های چارچوب خودمختار برای مسیریابی برمبنای اعتماد (ATRS[۲]) می توان به عملکرد خودمختار، عدم وابستگی به پروتکل، انعطاف پذیری، خود تطبیقی، سهولت در محاسبه و پایین بودن سربار محاسباتی اشاره کرد.

به منظور تنظیم رفتار یک نود در مقابل نودهای دیگر، ATRS با استفاده از موتوری خودمختار برای مدیریت قابل تطبیق با مقادیر اعتماد نودهای شبکه، آستانه ای تنظیم می کند. این آستانه با توجه به شرایط موجود و نودهای حاضر در شبکه، نودها را در رده قابل اعتماد و غیرقابل اعتماد دسته بندی می کند. همچنین ATRS مکانیزمی تنبهی برای از بین بردن انگیزه بدرفتاری ارائه می کند. بنابرین نودها در صورت تمایل به استفاده از منابع شبکه، وادار به مشارکت می شوند. به منظور کاهش نرخ بسته های حذف شده توسط نودهای بدرفتار، ATRS ماژولی برای ارسال بسته های داده ازمسیر امن پیشنهاد می کند.

۱-۲ اهداف

با توجه به محدودیت پهنای باند و انرژی در شبکه های بی سیم خود سازمانی، باید تا حد ممکن از ارسال مجدد بسته ها جلوگیری کرد. از سوی دیگر، نودها به علت محدودیت های

---

۱ Next node

۲ Autonomic Trust based Routing Scheme

ذکر شده، تمایلی به همکاری و ارسال بسته های دیگران ندارند؛ بنابرین بسته ها، حذف شده و مبدا مجبور به ارسال مجدد این بسته ها می شود. هدف این پایان نامه ارائه یک چارچوب مدیریت خودمختار اعتماد برای شبکه های بی سیم است که فرایند مسیریابی را با توجه به مقادیر اعتماد انجام دهد. بنابرین نودها، نتیجه مشارکت در شبکه را دریافت کرده و این مساله انگیزه ای برای همکاری آن ها خواهد بود.

برخی از چارچوب های ارائه شده برای مدیریت اعتماد در شبکه های بی سیم خودسازمانی، مولفه سوم مکانیزم اعتماد، که همان مولفه استقرار اعتماد است را پیاده سازی ننموده اند. همچنین بعضی از مدل های دارای مولفه سوم، یا از بین بردن انگیزه بد رفتاری را در طراحی قرار نداده و یا نرخ حذف بسته ها را با انتخاب مسیری امن برای ارسال، کاهش نمی دهند. مدل هایی که در هر دو زمینه فعالیت کرده اند، نفع نود مقصد را از دریافت بسته مورد نظر قرار نداده و نقش نود بعدی بدرفتار را در ارسال صحیح بسته ها نادیده گرفته اند. همچنین آن ها آستانه ای غیر پویا و نامطابق با شرایط شبکه را برای دسته بندی نودها مورد استفاده قرار داده اند.

این کار، یک نگرش جامع به چارچوب های موجود مدیریت اعتماد داشته واین چارچوب ها را از جنبه های مختلف بررسی می کند. با توجه به مرورهای انجام شده، مدل ATRS در این پایان نامه طراحی می شود که هدف آن استقرار اعتماد در شبکه و استفاده از مقادیر اعتماد در فرایند مسیریابی است. مدل ATRS بر روی پروتکل مسیریابی DSR[۱] پیاده سازی شده و با استفاده از نرم افزار NS-۲[۲]شبیه سازی شده است. در پایان، چارچوب معرفی شده، ارزیابی و با DSR بی دفاع مقایسه می شود تا کارایی آن در حضور سناریوهای مختلف بررسی شود.

۱-۳ نوآوری ها

امور انجام شده در این پایان نامه به صورت خلاصه به این شرح است:

- انجام یک مرور جامع بر چارچوب های مدیریت اعتماد در شبکه های اقتضایی متحرک

این مرور، نگرش جامعی بر چارچوب ها مختلف مدیریت اعتماد که برای MANET طراحی شده اند، ارائه می کند که مولفه های مختلف، معیارهای ارزیابی، ویژگی های منحصر به فرد و نقاط مثبت و منفی هر مدل را موشکافی می کند. این مرور، حمله

[۱] Dynamic Source Routing
[۲] Network Simulator-۲

هایی را مورد مطالعه قرار می دهد که محاسبه اعتبار را تحریف می کند. در این بررسی، چارچوب ها با توجه به مقاومتشان در مقابل هر یک از این حمله ها مورد تحلیل قرار می گیرند.

- ارائه یک طبقه بندی جدید برای حمل های تحریف اعتماد

در این تحقیق، حمله های تحریف اعتماد دسته بندی شده و توضیح مفصلی از هر یک از انواع حمله ارائه می شود. ما حمله های تحریف اعتماد را به دو دسته دروغگویی[۱] و دوچهره[۲] تقسیم می کنیم. این تقسیم بندی با توجه به این که حمله چگونه تخمین اعتماد یک نود در مورد نودهای دیگر را تحریف می کند، صورت می گیرد. یک نود دروغ گو، می تواند با انتشار تهمت علیه یک نود خوش رفتار، او را مخرب معرفی کند. نودهای دوغگو با توجه به این که فقط به انتشار دروغ پرداخته و یا این که علاوه بر دروغ، فعالیت خرابکارنه دیگری را به طور همزمان انجام می دهند، به دو دسته دروغگوی محض[۳] و دروغگوی خرابکار[٤] تقسیم بندی می شوند. یک نود دوچهره حمله خود را زمان بندی کرده و برای فریفتن درک یک نود از رفتار نودهای دیگر، عملکرد خود را بین رفتار خوب و بد به صورت متناوب تغییر می دهد. ما حمله دوچهره را با توجه به موقت یا دائمی بودن تهدید، به دو دسته روشن-خاموش[٥] و رفتار متناقض[٦] تقسیم می کنیم.

- ارائه یک دسته بندی جدید برای معیارهای اصلی ارزیابی

در این پایان نامه، طبقه بندی جدیدی برای معیارهای اندازه گیری استفاده شده در چارچوب های مدیریت اعتماد مورد مطالعه در ادبیات معرفی شده است. همچنین تعدادی معیار دیگر به این معیارها اضافه شده تا بتوان نگاه جامعی برای ارزیابی چارچوب های مدیریت اعتماد استفاده کرد. اهمیت این دسته بندی، بررسی یکسان چارچوب های مدیریت اعتماد است.

دستیافت های سه گانه مطرح شده با همکاری خانم ها موحدی و حسینی انجام شده است.

- ارائه یک چارچوب خودمختار برای مسیریابی بر مبنای اعتماد(ATRS)

---

۱ Bad mouthing
۲ Double-face
۳ Liar
٤ Subversive
٥ On-off
٦ Conflicting behavior

در این پایان نامه، یک چارچوب استقرار اعتماد با ویژگی های زیر برای شبکه های متحرک بدون زیرساخت ارائه می شود:

- این مدل یک موتور خودمختار به عنوان آستانه را مورد استفاده قرار می دهد تا با توجه به شرایط اساسی شبکه، نودهای نرمال و بدرفتار را شناسایی کند.
- مدل پیشنهادی انگیزه حمله را از نودهای بدرفتار گرفته و آن ها را وادار به همکاری می کند.
- ATRS نرخ حذف را از طریق ارسال بسته های داده از مسیرهای مناسب و امن کاهش می دهد.
- این چارچوب، به وسیله کاهش نرخ حذف و نیاز به ارسال مجدد، کارایی و طول عمر شبکه را افزایش می دهد.
- مدل پیشنهادی شانس مجدد حضور در شبکه را برای نودهای بدرفتار فراهم کرده تا بتوانند به شبکه باز گردند. این امکان نودها را به همکاری در شبکه ترغیب می کند؛ در حالی که اکثر مدل ها، یک نود بدرفتار را برای همیشه در لیست سیاه قرار داده و از شبکه حذف می کنند.[۲]
- ATRS با همه چارچوب های جمع آوری و محاسبه اعتماد، قابل همگام سازی بوده و می تواند اطلاعات اعتماد مورد استفاده را از طریق این چارچوب فراهم کند.
- این مدل به صورت مستقل از پروتکل های مسیریابی عمل می کند.

- پیاده سازی ATRS

برای نشان دادن کارایی مدل پیشنهادی، ATRS با استفاده از شبیه ساز NS-۲ پیاده سازی می شود، مجموعه ای از شبیه سازی ها روی آن انجام شده و با نتایج به دست آمده از DSR در حضور نودهای حمل کننده مقایسه می شود. انتظار می رود که نتایج شبیه سازی ها رشد چشمگیری در کارایی شبکه نشان داده و نرخ حذف نودهای بدرفتار(MDR[۱])، تأخیر متوسط مبدا به مقصد[۲] و نرخ دریافت بسته (PDR[۳])، بهبود یابد.

۱Malicious Drop Ratio
۲End to End Delay
۳Packet Delivery Ratio