مروری جامع بر سیستم‌های شهرت و رمزنگاری به منظور برقراری امنیت و اعتماد

مهسا بیگی[۱]، بهرنگ برکتین[۲]

۱-دانشجوی کارشناسی ارشد، دانشکده مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد نجف آباد، نجف آباد، ایران

۲- استادیار، دانشکده مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد نجف آباد، نجف آباد، ایران

خلاصه

شبکه‌های اقتضائی به دلیل نوین بودن‌شان و استفاده روزافزون از این شبکه‌ها توجه پژوهشگران بسیاری را به خود جلب نموده‌اند. شبکه‌های اقتضایی متحرک به دلایل مختلفی به وجود آمدند و در زمینه‌های بی‌شماری مورد استفاده قرار گرفتند خصوصیات و محدودیت‌های خاص این دسته از شبکه‌ها باعث ایجاد مشکلات امنیتی جدید گردیده است. از این‌رونسبت به شبکه‌های سیمی حتی شبکه‌های بی‌سیم ساخت‌یافته بسیار بیشتر در معرض آسیب‌های امنیتی قرار دارند. با توجه به نبود کنترل‌کننده‌ی مرکزی، یکی از اساسی‌ترین مفاهیم و در عین حال پرچالش‌ترین مفاهیم شبکه‌های اقتضائی امر مسیریابی و ارسال اطلاعات این دسته از شبکه‌ها می‌باشد که به دلیل ویژگی‌های خاص این دسته از شبکه‌ها چهره‌ای متفاوت و عملکردی خاص دارد. با نبود این قدرت در شبکه‌های اقتضائی تبادلات شبکه به وسیله خود گره‌ها انجام می‌گیرد. در واقع در این شبکه هر گره می‌تواند هم مبدأ و هم مقصد باشد و همچنین نقش یک مسیریاب را بازی کرده که قادر است اطلاعات را از همسایه قبلی دریافت و به همسایه بعدی در مسیر مقصد ارسال نماید. بنابراین اکثر حملات جهت اختلال در روند عملیاتی شبکه در فرآیند مسیریابی و ارسال اطلاعات اتفاق می‌افتد. لذا به شدت به پروتکل‌های قابل اعتماد به ویژه در ایجاد عملکرد صحیح و امن شبکه نیاز است. راه‌کارهای پیشگیری بر مبنای گسترش همین پروتکل‌هاست. امنیت و اعتماد در شبکه‌های اقتضایی متحرک از اهمیت بالایی برخوردار است و همچنان به عنوان یکی از مباحث پر چالش امروزی در تحقیقات علمی و پژوهشگران مورد بررسی قرار می‌گیرد.در این مقاله با در نظرگرفتن اهمیت اعتماد و امنیت در بحث مسیریابی شبکه‌های اقتضایی متحرک ،هر کدام از روش‌های ارایه شده در پژوهش‌های مرتبط در حیطه‌ی سیستم رمزنگاری(امنیت) و سیستم شهرت(اعتماد) را جداگانه دسته‌بندی شده است و نتایج نشان می‌دهد که هر کدام از این سیستم‌ها، نمی‌توانند به تنهایی از حملات فعال و غیر فعال به طور همزمان جلوگیری کند.

کلمات کلیدی: شبکه اقتضایی متحرک، امنیت، اعتماد

۱. مقدمه

شبکه‌های موردی یا اقتضایی[۳] یکی از مباحث نوین و جزء زیر مجموعه شبکه‌های بی‌سیم بوده، ولی دارای تفاوت‌ها و ویژگی‌های خاص خودشان می‌باشند. پیشرفت‌های اخیر در زمینه الکترونیک و مخابرات شبکه‌های بی‌سیم امکان ساخت گره‌هایی در اندازه کوچک با قابلیت پردازش بالا را به وجود آورده که در مسافت‌های کوتاه می‌توانند با هم ارتباط برقرار نمایند. شبکه‌های اقتضائی شامل مجموعه‌ای از این گره‌ها بوده که در محیط پراکنده می‌گردند تا با همکاری یکدیگر در جهت هدف ایجاد شده عملیات خود را انجام دهند[۱]. امروزه کاربردهای بسیاری برای شبکه‌های اقتضائی مطرح گردیده

[1] Beige_mahsa1991@yahoo.com
[2] Correspondence Author : behrang_barekatain@iaun.ac.ir
3 Ad Hoc Networks

است. از جمله این کاربردها می‌توان به استفاده در میادین‌های جنگی، شناسایی محیط‌های آلوده، نظارت محیط کار و منزل، کنترل ترافیک، استفاده در جاده‌ها و بزرگراه‌های هوشمند، کاربردهای مختلف در زمینه پزشکی و غیره اشاره نمود [۲].

شبکه بی‌سیم از فناوری‌های نوینی می‌باشد که در چند ساله اخیر پا به عرصه وجود گذاشته و با توجه به خصوصیات و مزایای خود در زمینه‌های بسیاری مورد استفاده و گسترش یافته است. شبکه‌های بی‌سیم به طور کلی متشکل از سه جزء بوده که این اجزا تشکیل دهنده یک شبکه بی‌سیم می‌باشند. این اجزاء عبارتند از[۱,۳]:

۱) گره‌های شبکه بی‌سیم
۲) اتصالات شبکه بی‌سیم
۳) ایستگاه پایه[۴] و یا وجود زیرساخت

با توجه به موضوع این پژوهش هر کدام از این اجزاء به طور مستقل و وابسته به پژوهش مربوطه مورد بررسی قرار می‌گیرند. گره‌های شبکه‌های بی‌سیم، به دلیل خصوصیاتی از جمله استفاده از باتری، پهنای باند محدود، قدرت پردازشی ضعیف، حافظه ذخیره‌سازی محدود و غیره در برابر انواع حملات و آسیب‌های امنیتی بسیار آسیب‌پذیرتر از شبکه‌های سیمی می‌باشند[۴].

اتصالات بی‌سیم نیز به دلیل ماهیت بی‌سیمی بودن‌شان، تحرک گره‌ها، همبندی پویای[۵] شبکه و غیره، درمقابل حملات، بسیار آسیب‌پذیرتر از شبکه‌های سیمی می‌باشند [۲].

جز سوم، ایستگاه پایه یا زیرساخت می‌باشد که وجود این عامل در شبکه باعث گردیده تا شبکه‌های بی‌سیم به دو دسته حاوی زیرساخت[۶] و بدون زیرساخت[۷] تقسیم‌بندی شوند. آن‌چه که در این پژوهش مورد نظر محقق می‌باشد، شبکه‌های بدون زیرساخت یا به عبارتی شبکه‌های اقتضائی می‌باشند. شبکه‌های اقتضائی با توجه به نبود زیرساخت ثابت و عدم وجود سوم شخص مورد اعتماد بسیار بیشتر از شبکه‌های سیمی و حتی شبکه‌های بی‌سیم حاوی زیرساخت در برابر حملات و نفوذی‌ها آسیب‌پذیرتر بوده و به دلیل عدم ایستگاه پایه آسیب‌پذیری دوچندان می‌گردد[۳]. همچنین توزیع‌شدگی کامل شبکه باعث گردیده تا امنیت چهره‌ای متفاوت با دیگر شبکه‌ها داشته باشد. اما اساسی‌ترین خصوصیت این شبکه‌ها و یا بهتر می‌توان گفت مزیت این دسته از شبکه‌ها کاربرد این‌شبکه‌ها در زمینه‌ها متنوع می‌باشد. از جمله این زمینه‌ها می‌توان به زمینه‌های نظامی، محیط‌های آلوده و شمیایی، موارد اورژانسی و مدیریت بحران و غیره اشاره نمود. با توجه به آن‌چه بیان گردید و ویژگی‌ها و آسیب‌پذیری‌های شبکه‌های اقتضائی و همچنین با توجه به کاربرد این شبکه‌ها در موارد ویژه و حساس به شدت به مکانیزم‌های امنیتی و پروتکل‌های برقراری امنیت نیاز است تا ضرورت شبکه ایمن در کاربردهای مختلف پشتیبانی گردد [۵].

برخلاف شبکه‌های دارای زیرساخت که عناصر خاصی از شبکه، نظیر مسیریاب وظیفه مسیریابی و ارسال اطلاعات بسته‌ها را انجام می‌دهند، در شبکه‌های موردی سیار، هر یک از عناصر شبکه وظیفه مسیریابی و ارسال اطلاعات را نیز بر عهده دارد. اکثر حملات چه از جنبه دسترسی به اطلاعات شبکه و چه از جنبه مختل کردن شبکه در امر مسیریابی و ارسال اطلاعات بروز می‌دهد و در سوی مقابل روش‌های امنیتی نیز در همین راستا ارائه و پشتیبانی می‌گردد.

حملات موجود در این دسته از شبکه‌ها را می‌توان به دو نوع عمده زیر تقسیم‌بندی نمو[۶,۷]:

- حملات گره‌های بدرفتار به منظور مختل کردن عملکرد شبکه(حملات فعال)
- حملات گره‌های نفوذی به منظور شنود و دسترسی به اطلاعات شبکه (حملات غیر فعال)

[4] Base station
[5] Dynamic Topology
[6] Infrastructural
[7] Non-Infrastructural

گره های بدرفتار دو نوع می باشند : گره بدخواه[8] و گره خودخواه[9] . گره بدخواه به دسته‌ای از گره های بدرفتار گفته می‌شود که گره حمله کننده قصد دارد با عملیات مخربانه خود از جمله حذف و تغییر اطلاعات، تزریق اطلاعات نادرست یا جعل اطلاعات[10] ,سعی در ایجاد اختلال در عملکرد شبکه کند. معمولاً این دسته از حملات با مصرف باطری گره حمله‌کننده همراه می‌باشد. از سوی دیگر، یک گره خودخواه بطور مستقیم قصد وارد کردن خسارت به عملکرد شبکه را ندارد، بلکه مایل نیست که منابع خود را برای ارتباطات دیگران مصرف کند.

در حملات غیر فعال هدف گره حمله کننده استراق سمع اطلاعات و دستیابی به اطلاعات شبکه می‌باشد. این ناهنجاری بدون مزاحمت در عملیات معمول[11] شبکه انجام می‌گیرد.روش‌های ارایه شده در زمینه‌ی اعتماد در مقابل این نوع حملات ناتوان هستند.

هر کدام از حملات بیان شده در جایگاه خود بسیار مهم و پیش‌گیری از این حملات بسیار ارزشمند است. در واقع روش‌های امنیتی ارائه شده باید قابلیت این امر را داشته که به صورت کارا از هر دو نوع حملات درشبکه پیش‌گیری نمایند و حداکثر میزان امنیت و اعتماد را پیاده‌سازی نمایند.

پروتکل‌های امنیتی بسیاری به منظور پیاده‌سازی امنیت و برقراری اعتماد در این شبکه‌ها ارائه شده است. پروتکل‌های ارائه شده در این زمینه را با توجه به سابقه‌ی تحقیق می‌توان به دو دسته زیر تقسیم‌بندی کرد [۸]:

۱) برقراری اعتماد و امنیت بر اساس سیستم شهرت[12]

۲) برقراری اعتماد و امنیت بر اساس سیستم رمزنگاری[13]

مفهوم اعتماد در شبکه‌های اقتضایی به این مبحث دلالت دارد که گره‌های شبکه چه میزان اعتماد به یکدیگر دارند(برای مثال وقتی گره‌ی A بسته ای را به گره‌ی B ارسال می کندجهت رسیدن بسته به مقصد به درستی برخورد کند(اشاره به حملات فعال) .

سیستم شهرت از فراهم آوردن اعتماد بیشتر برای گره‌های خوش‌رفتار جهت پیاده‌سازی اعتماد و امنیت در شبکه استفاده می‌کند. با توجه به خصوصیات این سیستم عملکرد سیستم شهرت روشی مناسب و کارا جهت جلوگیری از حملات گره‌های بدخواه و رفتار منفی گره‌های خودخواه جهت مختل کردن عملیات شبکه می‌باشد. ولی سیستم شهرت در مقابله با حملات گره‌های نفوذی به منظور دسترسی به اطلاعات ناتوان می‌باشد. همچنین با توجه به آن‌چه در بخش پیشینه پژوهش ارائه خواهد گردید، این سیستم دارای محدودیت‌های دیگری نیز به منظور برقراری اعتماد رنج می‌برد [۹،۱۰].

هر فعالیتی که برای حفاظت از شبکه طراحی شده است را امنیت شبکه گویند،مفهوم امنیت به صورتی است که وقتی بسته ای بین دو گره ارسال میشود محتویات آن بسته از گره‌های میانی،گره‌های دشمن و نفوذی محفوظ می ماند(اشاره به حملات فعال).امنیت به عنوان یکی از ابزارهای مهم در جهت پیش‌گیری از رفتارهای منفی و افزایش کارایی شبکه-های اقتضائی می‌باشد. سیستم رمزنگاری یکی از قوی‌ترین سیستم‌ها جهت پیاده‌سازی اعتماد و افزایش امنیت در شبکه بوده و روش موثری برای مقابله با حملات گره‌های نفوذی به جهت دسترسی و شنود اطلاعات می‌باشد. سیستم رمزنگاری با استفاده از الگویتم‌های رمزنگاری و مزیت مخفی‌سازی اطلاعات اعتماد و امنیت در شبکه را ایجاد و پشتیبانی می‌کند. اما همان‌گونه که در بخش مروری بر پژوهش‌های پیشین خواهیم دید این سیستم به منظور جلوگیری از رفتارهای خودخواهانه و حملات مختل کننده گره‌های بدخواه هیچ‌گونه تدابیر امنیتی را ندارد. از طرفی بزرگترین مسئله

[8] Malicious node
[9] Selfish node
[10] Falsification
[11] Normal
[12] Reputation System
[13] Cryptography System

و مشکل این راهکارها ایجاد و توزیع امن کلید در شبکه با توجه به ماهیت شبکه‌های اقتضائی، نبود ایستگاه پایه و استفاده از امواج رادیویی جهت ارسال ودریافت اطلاعات می‌باشد[۱۱].

ساختار این مقاله به این صورت است که: در بخش دوم مروری کوتاه بر طرح‌های مبتنی بر اعتماد در سیستم شهرت شده است ،که بر اساس پروتکل‌های مبتنی بر مسیریابی OLSR[۱۶], DSR[۱۵],AODV[۱۴] و همچنین پروتکل‌های ارزیابی اعتماد با تخمین احتمالات فازی و توزیع‌های استاندارد ارایه شده است. در بخش سوم مروری بر پروتکل‌های مختلف مسیریابی امن شده است ، که شامل رمزنگاری بر اساس پروتکل‌های مبتنی بر مسیریابیDSR,AODV و همچنین پروتکل‌های امن SAFC[۱۷], SEAD[۲۰],ECCEA[۱۹],ARAN[۱۸] ارایه شده است .در بخش چهارم نتیجه‌گیری حاصل از مرور پروتکل‌های امن و قابل اعتماد بیان شده است.

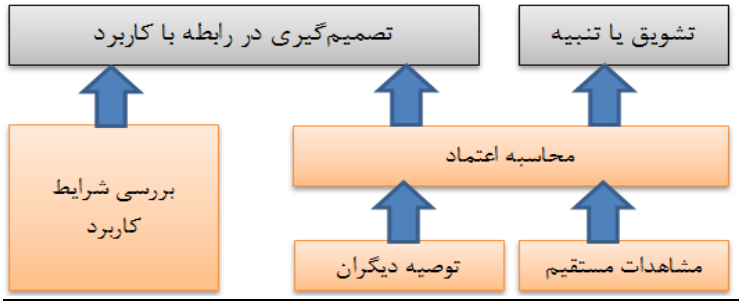
[14] Ad hoc On-Demand Distance Vector
[15] Dynamic Source Routing
[16] Optimized Link State Routing
[17] Simple Acknowledgment and Flow Conversation
[18] Authenticated Routing for Ad hoc Networks
[19] Elliptic Curve Cryptography Enabled AODV
[20] Secure Efficient Ad-Hoc Distance Vector Routing

۲. طرح های مبتنی بر شهرت

سیستم شهرت از ارائه اعتماد بیشتر برای گره‌های خوش‌رفتارتر جهت برقراری اعتماد و امنیت استفاده می‌کند. در این سیستم اعتماد گره‌ها در اثر بدرفتاری و خوش‌رفتاری کادرهم‌ساز و افزایش می‌یابد. گره‌ها با افزایش اعتماد و بهره بردن از منابع شبکه تشویق شده و در اثر بدرفتاری با کادرهم‌ساز اعتماد و قرنطینه شدن و کنار گذاشته شدن از شبکه، تنبیه می‌شوند می‌توان گفت سیستم شهرت به نوعی از نظام اعتماد حاکم بر جامعه انسانی نشأت گرفته و سعی دارد خصوصیات و ویژگی این نظام را پیاده‌سازی نماید[۸]. سیستم شهرت دارای کارایی می‌باشد. این کارایی وقتی تضمین می‌شود که مشکل عدم انگیزه درپی بالا رفتن شهرت ایجاد نشود. زیرا وقتی شهرت افزایش یابد و گره دارای اعتماد بالایی می‌شود دیگر انگیزه لازم جهت همکاریرا نداشته و دست به رفتارهای خودخواهانه‌ی خود می‌زند. به همین دلیل گره سعی می‌کند میزان اعتماد خود را حول محور آستانه نگه دارد تا هم به عنوان گره خوش‌رفتار در شبکه بماند و هم در صرفه‌جویی از منابع خود کوشا باشد. با توجه به نحوه عملکرد این سیستم، سیستم شهرت توانایی جلوگیری از گره‌های خودخواه و حملات گره‌های بدخواه را داشته و اعتماد مناسبی را در شبکه پیاده‌سازی می‌کند. ولی این سیستم و در مقابل حملات دسترسی به اطلاعات شبکه و نفوذی‌ها و عوامل دشمن، آسیب‌پذیر می‌باشد. پژوهش‌های ارائه شده با بهره‌گیری از سیستم شهرت را می‌توان به دو دسته زیر تقسیم‌بندی کرد[۱۰]:

۱) سیستم شهرت عمومی (بر مبنای توصیه گره‌های موجود در شبکه نسبت به گره مورد ارزیابی)
۲) سیستم شهرت محلی (بر مبنای مشاهدات مستقیم و اعتماد همسایگان محلی نسبت به گره‌ی موردارزیابی)

در مجموع عوامل مؤثر در محاسبه و ارزیابی اعتماد بر اساس سیستم شهرت و استفاده از این معیار را می‌توان به‌صورت شکل ۱خلاصه کرد[۱۳]. ارزیابی اعتماد برمبنای شواهد عینی و توصیه‌های دیگران و در نهایت استفاده از آن در تصمیم‌گیری‌های درون شبکه و تنبیه و تشویق برای تمام گره‌های درون شبکه می‌باشد.



شکل۱-اعتماد بر پایه سیستم شهرت در شبکه‌های اقتضائی متحرک

برخی از مهم‌ترین پژوهش‌های ارائه شده در این زمینه به همراه محدودیت‌های آن‌ها در ادامه بیان شده است:

۱- پروتکل ارزیابی اعتماد بر محوریت سوابق گره‌های شبکه و تصمیم‌گیری‌ها:
در مدل اعتماد ارائه شده محاسبه اعتماد برمبنای دریافت بسته‌ها، درستی و دقت در ارسال بسته‌ها، جواب دادن به بسته‌های مسیریابی و نیز با توجه به لیست سیاه انجام می‌شود. در این پژوهش نظریه مطلوبی ارائه شده که سنجش قابلیت اعتماد در شبکه‌های اقتضایی به صورت پویا انجام می‌شود. از محدودیت‌های این روش می‌توان به ضعف در مقابله با حملات مبتنی بر شنود و نبود تدابیر در مقابله با گره‌های نفوذی اشاره کرد[۱۲].

۲- Yan Lindsay Sun و همکاران[۱۳] برای توسعه مدل اعتماد از مباحث احتمال و به‌ویژه از توزیع‌های استاندارد استفاده شده است. از سوی دیگر جهت توسعه مدل اعتماد ارائه شده سعی بر آن است تا از یک گراف کلی در شرایط مختلف شبکه استفاده شود. در این کار معیار دیگری به‌نام اطمینان تعریف شده است که اطمینان نام برده شده از میزان اعتماد ارزیابی شده حاصل می‌شود. در این مدل از میانگین تابع اعتماد به عنوان مقدار اعتماد و از واریانس تابع به عنوان مقدار اطمینان استفاده شده است. محاسبه اعتماد در این کار بر اساس نظارت مستقیم و توصیه دیگر گره-های شبکه می‌باشد. در این مدل چارچوب اعتماد به صورت عمومی برای کل شبکه توزیع شده است. از محدودیت-های این پژوهش عدم مقابله در برابر حملات مبتنی بر شنود و کشف نکردن همه‌ی گره‌های بدرفتار می‌باشد.

۳- مدل اعتمادی با تخمین احتمالات فازی و مدل نظارت بر گره :

سازوکار ارزیابی اعتماد بر تعاملات مستقیم و آگاهی از توصیه‌ها تاکید دارد. در این کار جهت ارزیابی اعتماد از محاسبات حجیم استفاده شده است. بنابراین این محاسبات فراگیر در جاهایی که به سطوح اعتماد پایین نیاز است لازم نیست، از این‌رو فرآیند مبادله‌ی اطلاعات توصیه موجب ایجاد سربار و در نهایت بلاک شدن انتقال‌های لازم در شبکه می‌شود. از محدودیت‌های این پژوهش می‌توان به مبادله‌ی توصیه‌ها در شبکه و ایجاد سربار، کارایی پایین در برابر حملات مبتنی بر شنود و کشف نکردن همه‌ی گره‌های بدرفتار را نام برد[۱۴].

۴- پروتکل TSR[۲۱] بر پایه پروتکل مسیریابی پایه DSR[۲۲] :

در جهت ارزیابی اعتماد رفتار همسایه‌ها فقط از تعاملات مستقیم استفاده شده و از توصیه‌ها به علت سربار استفاده نمی‌شود. در این پروتکل سه نوع اعتماد گذشته گره (بر مبنای تعاملات پیشین)، اعتماد جاری گره (بر مبنای تعاملات پیشین و تعامل انجام شده کنونی با گره) و اعتماد مسیر (برمبنای اعتماد گره‌های میانی موجود در مسیر) محاسبه می‌شود. پس از ارزیابی اعتماد برای گره مورد ارزیابی اگر میزان اعتماد گره از میزان آستانه مشخص شده پایین‌تر آید گره به عنوان گره مهاجم شناخته شده و در لیست سیاه[۲۳] قرار می‌گیرد. گره اضافه شده به لیست سیاه برای مدت مشخصی (زمان قرنطینه) از شبکه کنار گذاشته می‌شود و دوباره به او با یک میزان اعتماد اولیه شانس مجدد داده می‌شود. در این روش برای محاسبه سه نوع اعتماد ذکر شده از مجموعه‌های فازی و عملیات ریاضی نسبتاً پیچیده استفاده می‌شود. از محدودیت‌های این پژوهش افزایش محاسبات و تأخیر در شبکه می‌باشد. همچنین میزان ارزیابی اعتماد به صورت محلی انجام شده که این امر خلاف ذات شبکه‌های اقتضایی متحرک می‌باشد. از طرفی آسیب‌پذیری در برابر حملات شنود و گره‌های نفوذی از دیگر محدودیت‌های این روش می‌باشد[۱۵].

۵- پروتکل RAS[۲۴] بر مبنای پروتکل پایه DSR :

اساس و زیربنای ایده آن بر مبنای انتخاب قابل اطمینان‌ترین ارسال اطلاعات به منظور افزایش اطمینان و امنیت می-باشد. در این راه‌کار بسته درخواست مسیر متناسب با برقراری قابل اطمینان‌ترین مسیر تغییر داده شده و پارامترهای مورد نیاز را در بر دارد. جهت انتخاب مسیر مطمئن، گره مبدأ حداقل اطمینان مورد نیاز به منظور ارسال بسته‌هایش را در بسته درخواست مسیر مشخص کرده و فرایند کشف مسیر شروع می‌گردد. در ادامه تنها گره‌هایی در فرایند مسیریابی شرکت می‌کنند که قابلیت اطمینانی بیشتر حد آستانه مشخص شده در بسته درخواست مسیر را دارا هستند. ازاین‌رو

[21] Trust-based Source Routing protocol
[22] Dynamic Source Routing
[23] Black list
[24] Reliable routing protocol for enhanced reliability and security in mobile Ad hoc and Sensor networks

تنها مسیرهای قابل اطمینان کشف می‌شوند. هر گره میانی مقدار قابلیت اطمینان خود را به مقدار تجمعی لحاظ شده در بسته درخواست مسیر اضافه می‌نماید. این فرایند ادامه می‌یابد تا بسته درخواست مسیر را مقصد دریافت کرده و در ادامه گره مقصد از تقسیم میزان تجمعی موجود در بسته به تعداد گره‌های مسیر، مسیری که دارای بیشترین میزان اطمینان است را به عنوان مسیر اصلی انتخاب کرده و از طریق مسیر معکوس پاسخ می‌دهد و بقیه مسیرها به عنوان مسیرهای پشتیبان ذخیره گردیده تا در هنگام بروز خطاهای امنیتی از این مسیرهای پشیتبان استفاده گردد. گرچه پروتکل ارائه شده دارای کارایی بالا در کادرهم‌ساز سربار شبکه و افزایش میزان تحمل‌پذیری خطا می‌باشد ولی بزرگترین محدودیت این پژوهش نبود تدابیر امنیتی لازم جهت مقابله با حملات و آسیب‌های امنیتی می‌باشد[۱۶] .

۶- پروتکل مسیریابی مبتنی بر اعتماد سبک وزن

مارچن و همکاران[۱۷]، یک پروتکل مسیریابی مبتنی بر اعتماد سبک وزن ارائه کردند. این برنامه سبک به این معنا است که سیستم تشخیص نفوذ (IDS[۲۵]) مورد استفاده برای برآورد اعتماد یک گره برای دیگری با مصرف منابع محاسباتی محدود همراه است. علاوه بر این، آن تنها از اطلاعات محلی استفاده می‌کند که به وسیله آن مقیاس‌پذیری برای مقاومت در برابر حمله سیاه چاله و حمله سوراخ خاکستری را تضمین می‌کند. بررسی و طبقه بندی مدل اعتماد موجود بر اساس گواهی کلید عمومی برای شبکه‌های اقتضایی پیشنهاد شده ، و سپس به بحث و مقایسه آنها با توجه به برخی از ضوابط مربوطه پرداخته شده است. همچنین، نویسندگان میان مدل‌های اعتماد با استفاده از شبکه‌های پتری تصادفی به منظور اندازه گیری عملکرد هر یک از آنها با آنچه مربوط به در دسترس بودن خدمات صدور گواهینامه است تحلیل و مقایسه انجام می‌دهند .

۷- روشی بر پایه پروتکل مسیریابی AODV، تحت عنوان TRUNCMAN[۲۶] :

معیار ارزیابی اعتماد گره‌های همسایه، براساس بسته‌های ارسال شده است. وقتی گره‌ای بسته را برای گره همسایه ارسال می‌کند، برای مدت زمان مشخصی به این گره گوش می‌دهد که آیا گره مورد نظر بسته دریافتی را ارسال می‌کند یا خیر. وقتی گره همسایه بسته دریافتی را منتشر می‌کند یک نسخه از بسته دوباره به دست گره ارسال کننده بسته می‌رسد. شناسه و شماره توالی بسته نشان دهنده‌ی هویت بسته است. گره ارسال کننده بسته با دریافت بسته‌ای با شناسه و شماره توالی مشابه متوجه می‌شود همسایه مورد نظر بسته را ارسال کرده است. اگر گره همسایه در زمان مشخص بسته دریافتی را منتشر نکند سه حالت ممکن است داشته باشد:

- ترافیک دریافتی گره دارای حجم بالایی است و به این دلیل بسته به دست آن گره نرسیده است.
- کارایی گره پایین است و بسته را در زمان دیرتری ارسال خواهد کرد.
- گره مورد نظر یک گره خودخواه است.

در این صورت ارسال کننده بسته، فیلد درخواست دلیل موجود در بسته را یک کرده و بسته را مجدداً برای آن گره ارسال می‌کند. اگر گره با کارایی پایین باشد بسته را منتشر کرده، بعد از زمان مقرر به دست ارسال کننده بسته می‌رسد. در این حالت گره مورد نظر، فیلد نشان دهنده این‌که کارایی گره پایین است را یک کرده و بسته را منتشر می‌کند. اگر ترافیک گره زیاد باشد بسته ارسالی دوم از مبدأ را دریافت کرده، فیلد مربوط در بسته را مبنای بر این‌که ترافیک گره مورد نظر زیاد است را یک کرده و بسته را منتشر می‌کند. یا این‌که بسته ارسالی دوم را ارسال نمی‌کند و به عنوان گره خودخواه در نظر گرفته می‌شود. هنگامی‌که یک گره به عنوان گره خودخواه شناخته شود یک بسته برای آگاهی گره‌های دیگر در شبکه منتشر

[25] Intrusion detection system
[26] Trust-based Routing Mechanism Using Non-Cooperative Movement in Mobile Ad-hoc Network

می‌شود و گره‌ها را از وجود گره خودخواه باخبر می‌سازد. از محدودیت‌های این پژوهش، تأخیر و کارایی پایین در برابر حملات مبتنی بر شنود و ضعف در برقراری اعتماد را می‌توان نام برد[۱۸].

۸- Mustafa و همکاران روشی سه مرحله‌ای MSR را به منظور ارزیابی و برقراری اعتماد ارائه داده‌اند که به شرح زیر می‌باشد [۱۹]:

- مسیریابی چندگانه برحسب تقاضا[۲۷]: فرآیند کشف مسیر با ارسال بسته‌های درخواست مسیر انجام می‌شود. مقصد بعد از دریافت اولین بسته درخواست مسیر برای مدت زمان مشخصی صبر می‌کند تا تمام بسته‌های درخواست مسیر برسند. سپس هر بسته دریافتی درخواست مسیر را با یک بسته پاسخ مسیر از طریق مسیر معکوس پاسخ می‌دهد.
- افزودن تأیید غیرفعال[۲۸]: اشاره دارد به این که هر گره بعد از ارسال بسته به حالت بی‌قاعده رفته و به خط گوش می‌دهد که گره دریافت‌کننده بسته، بسته را برای گام[۲۹] بعدی ارسال می‌کند یا خیر. اگر گره‌ای بسته دریافتی را ارسال نکند گره ارسال کننده بسته بعد از زمان مشخصی مجدداً بسته را برای گره مورد نظر ارسال می‌کند. اگر گره مجدداً بسته‌ی ارسالی را ارسال نکند به عنوان یک گره‌ی خودخواه در نظر گرفته خواهد شد.
- مبدأ بسته ارسالی را در n سهم کد می‌کند و از مسیرهایی مستقل از هم، سهم‌ها را برای مقصد ارسال می‌کند. مقصد با دریافت k تا از سهم‌ها، بسته اصلی را بازسازی می‌کند.

از محدودیت‌های این پژوهش به‌دنبال داشتن تأخیر و محاسبات زیاد و نبود تدابیر امنیتی در برابر حملات شنود و همچنین کشف نشدن همه گره‌های غیرقانونمند است.

۹- پروتکل اعتماد مبتنی بر AODV (TAODV):

پروتکل مسیریابی TAODV[۳۰] با اضافه کردن پارامتر اعتماد بر پیام مسیریابی، پروتکل AODV را توسعه داده است. مقدار اعتماد بعضی گره‌ها از مقدار اعتماد گره‌ی همسایه محاسبه می‌شود. دو فیلد جدید به جدول مسیریابی شامل اطلاعات اعتماد و لیست همسایه‌ها اضافه شده است. مسیرمعتمد می‌تواند از تعداد بسته‌های ارسال شده و تعداد بسته‌های دریافت شده توسط مقصد یا دیگر پارامترهای شبکه محاسبه شود .شبکه TRREP را با بهترین مقدار اعتماد و مسیر را برای ارتباطات انتخاب می‌کند. اعتماد TAODVدر [۲۰] یک معیار سه بعدی شامل اعتقاد، ناباوری و عدم قطعیت است که سه احتمال به نمایندگی این پارامترها ، با استفاده از شواهد مثبت و منفی و فرمولی خاص محاسبه می شود. برای هر عمل مسیریابی، جزئیات اعتماد پخش، ارزش اعتماد به روز شده و مسیرهای مورد اعتماد کشف می‌شوند. در جدول مسیریابی اصلی سه زمینه‌ی حوادث مثبت، منفی و عقیده اضافه شده است. TRREQ (درخواست مسیر مورد اعتماد) و TTREPs به ترتیب جایگزین RREQ وRREP شده است. در طول مسیریابی، گره A یک TRREQ به B ارسال می‌کند ،از آن‌جا که هر گره اطلاعات اعتماد گره‌ی دیگر را ندارد ، توصیه اعتماد B را به گره‌های همسایه می‌فرستد و اعتماد را محاسبه می‌کند . اگر معیار عدم قطعیت بزرگتر از مقدار آستانه باشد، سپس گره B امضای گره A را تأیید صحت می‌کند. با توجه به تایید این احراز هویت، TRREQ دوباره پخش می‌شود و یا کادرهم‌ساز یافته و ارزش اعتماد به روزرسانی می‌شوند. هر مجموعه ای از عملیات اعتماد O (162v) زمان مصرف می‌کند که در آن Vمتوسط تعداد همسایه است، در حالی که هر احراز هویت O (K3) زمان مصرف می‌کند و K طول امضاء است.TAODV با توجه به پارامتر اعتماد، می‌تواند گره‌های مخرب را در بهبود امنیت در مقایسه باAODV شبکه شناسایی کند و از حمله سیاه چاله جلوگیری کند. برای حمله سوراخ خاکستری، اعتماد همسایه ها به تدریج کادرهم‌ساز می‌یابد و گره شناسایی شده است. با این حال، TAODV نیاز به تدابیر امنیتی در برابر حملات مبتنی بر شنود دارد [۲۰] .

---

[27] On-demand Multipath Routing
[28] Enhanced Passive Acknowledgment
[29] Hop
[30] Trust base Ad hoc On-Demand Distance Vector

۱۰- پروتکل رفاقت[31] مبتنی بر AODV (FrAODV[32]):

در این پروتکل هر گره لیستی از دوستان و مقدار دوستی از آن‌ها را نگه می‌دارد. بازه‌ی دوستی از ۰ تا ۱۰۰ است که مقدار بالاتر اعتماد بالاتر در گره‌را نشان می‌دهد . برای محاسبه‌ی مسیر در FrAODV دو الگوریتم استفاده می‌شود .

- RvEvaluate: این الگوریتم مسیر معکوس از گره‌ی مقصد به منبع را می‌سازد. در اولین مرحله گره‌ی منبع RREQ را پخش می‌کند. ارسال رو به جلو می‌تواند دو موقعیت را ناشی شود.
  - گره‌ی جاری مقصد نهایی است ، اگر همسایه‌ی قبلی بک دوست نیست درخواست آن رد می‌شود. در غیر این صورت دوستی مسیر معکوس توسط مقایسه با مقدار دوستی مسیر جاری محاسبه می‌شود. این مقدار توسط رابطه‌ی ۱ به‌دست می‌آید.

$$\text{RrFrRte} = \frac{1}{h} * \sum_i^h 1^{PrFrH\,p_i} \qquad (۱)$$

اگر مقدار دوستی مسیر کمتر از مسیر قبلی باشد، مسیر رد می‌شود،در غیر این‌صورت به مسیر دوستی اضافه می‌شود.

  - اگر گره‌ی جاری یک گره‌ی میانی است درصورتی که همسایه‌ی قبلی یا بعدی در لیست دوستی نباشد آن درخواست را رد می‌کند .در غیر این صورت با اشاره به ارزیابی در مرحله‌ی قبل یک مسیر معکوس از گره‌ی جاری به منبع را می‌سازد.
- FwEvaluate :این الگوریتم مسیر ارسال روبه جلو را از منبع به مقصد می‌سازد. گره‌ی مقصد RREP مربوط به RREQ دریافت شده را تولید و به گره‌ی قبلی ارسال می‌کند . ارسال رو به جلو می‌تواند دو موقعیت را ناشی شود:
  - گره‌ی جاری منبع است. اگر گام بعدی یک دوست نبود، دوستی با درخواست رد شده تطبیق داده می‌شود. در غیر این صورت ارسال مسیر توسط مقدار دوستی مسیر جاری محاسبه می‌شود. این مقدار توسط رابطه‌ی ۲ به‌دست می‌آید.

$$\text{FwFrRte} = \frac{1}{h} * \sum_i^h 1^{FwFrHpi} \qquad (۲)$$

$FwFrHpi$ مقدار دوستی گره‌ی i ام بعدی ، h تعداد گام‌ها از مقصد به منبع است. اگر مقدار دوستی مسیر کمتر از مسیر قبلی باشد مسیر رد می‌شود. در غیر این صورت به عنوان بهترین دوست مسیر جاری اضافه می‌شود .

  - اگر گره‌ی جاری به عنوان گره‌ی میانی باشد ، اگر گام بعدی یا گام قبلی در لیست دوستان نباشد، درخواست رد می‌شود؛ در غیر این صورت با اشاره به ارزیابی در مرحله‌ی قبل یک مسیر ارسال از گره‌ی جاری به مقصد را می‌سازد.

برای محاسبه‌ی مسیر در *FrAODV* دو الگوریتم استفاده شده است. بنابراین، تاخیر پایان به پایان ناشی از محاسبه‌ی درخواست بیشتر است . در این صورت، پارامترهای QOS[33] مانند نسبت تحویل بسته در مقایسه با پروتکل AODV بهبود داده شده است [۲۱].

همان‌طور که بیان شد پروتکل‌های ارائه شده بر پایه سیستم شهرت در برابر حملات مبتنی بر شنود گره‌های نفوذی تدابیر امنیتی نداشته و با وجود این حملات کارایی شبکه بدرهم‌سازدت افت خواهد نمود. اما استفاده از سیستم شهرت در جلوگیری از رفتارهای خودخواهانه و اکثر حملات مخرب مؤثر می‌باشد. در این پیشنهادیه سعی بر آن است تا از مزایای سیستم شهرت در برقراری اعتماد استفاده و محدودیت‌های این سیستم را با استفاده از سیستم رمزنگاری برطرف کرده تا پروتکلی قابل اعتماد

[31] Friendship
[32] *Friendship based AODV*
[33] Quality of servise

جهت مسیریابی و ارسال اطلاعات شبکه‌های اقتضائی ارائه شود.در جدول ۱ کارهای ارایه شده در زمینه‌ی پروتکل‌های مرتبط به ارزیابی اعتماد در این مقاله ،به انضمام محدودیت‌ها و مزایای آن‌ها بیان شده است.

جدول۱- مربوط به کارهای انجام شده در حوزه‌ی اعتماد

نویسنده/سال	عملکرد پروتکل	محدودیت‌هاو مزایا
Jawhar, I., Z. Trabelsi, and J. Al-Jaroodi,2014	پروتکل RAS،مبتنی بر DSR ارایه شده ، اساس و زیربنای ایده آن بر مبنای انتخاب قابل اطمینان‌ترین ارسال اطلاعات به منظور افزایش اطمینان و امنیت می‌باشد. که باعث کشف مسیرهای قابل اطمینان می‌شوند.	پروتکل ارائه شده دارای کارایی بالا در کادرهم‌ساز سربار شبکه و افزایش میزان تحمل‌پذیری خطا ولی بزرگترین محدودیت این پژوهش نیاز به تدابیر امنیتی لازم جهت مقابله با حملات و آسیب‌های امنیتی می‌باشد.
H. Xia, Z. Jia, X. Li, L. Ju, and E.H.M ,2012	در پروتکل TSR برسه نوع است : اعتماد گذشته گره (بر مبنای تعاملات پیشین)، اعتماد جاری گره (بر مبنای تعاملات پیشین و تعامل انجام شده کنونی با گره) و اعتماد مسیر (برمبنای اعتماد گره‌های میانی موجود در مسیر) محاسبه می‌شود	افزایش محاسبات و تأخیر در شبکه می‌باشد. همچنین میزان ارزیابی اعتماد به صورت محلی انجام شده که این امر خلاف ذات شبکه‌های اقتضایی متحرک می‌باشد. از طرفی آسیب‌پذیری در برابر حملات شنود و گره‌های نفوذی از دیگر محدودیت‌های این روش می‌باشد
X Li, M.R Lyu, and J Liu,2004	TAOMDV با اضافه کردن پارامتر اعتماد بر پیام مسیریابی AODV توسعه داده است. دو فیلد جدید به جدول مسیریابی شامل اطلاعات اعتماد و لیست همسایه‌ها اضافه شده است.	گره های مخرب بیشتری را در بهبود امنیت شبکه در مقایسه با AODV شناسایی کند و می‌تواند حمله سیاه چاله جلوگیری کند با این حال، TAODV نیاز به تدابیرامنیتی در برابر حملات شنود دارد.
I. Jawhar, Z. Trabelsi, and J. Jaroodi,2014	در پروتکل FRAODV هر گره لیستی از دوستان و مقدار دوستی از آن‌ها را نگه می‌دارد. بازه‌ی دوستی از ۰ تا ۱۰۰ است که مقدار بالاتر، اعتماد بالاتر در گره‌را نشان می-دهد	تاخیر پایان به پایان ناشی از محاسبه‌ی درخواست بیشتر است . در این صورت، پارامترهای QOS مانند نسبت تحویل بسته در مقایسه با پروتکل AODV بهبود داده می‌شود. تدابیرامنیتی در برابر حملات شنود ندارد
] M. A. Moustafa, M.A. Youssef, and M.N. El-Derini,2011	روشی سه مرحله‌ای مبتنی بر MSR به منظور ارزیابی و برقراری اعتماد : ۱- مسیریابی چندگانه برحسب تقاضا ۲- افزودن تأیید غیرفعال ۳- بازسازی بسته فقط با دریافت k تکه از بسته	به‌دنبال داشتن تأخیر و محاسبات زیاد و نیاز به تدابیر امنیتی در برابر حملات شنود و همچنین کشف نشدن همه گره‌های غیرقانونمند است.

Yan Lindsay Sun و همکاران ۲۰۱۱	برای توسعه مدل اعتماد از مباحث احتمال و به‌ویژه از توزیع‌های استاندارد استفاده شده است.	عدم مقابله در برابر حملات مبتنی بر شنود و کشف نکردن همه‌ی گره‌های بدرفتار می‌باشد.
L. Junhai and F. Mingyu, 2011	سازوکار ارزیابی اعتماد بر تعاملات مستقیم و آگاهی از توصیه‌ها تاکید دارد. در این کار جهت ارزیابی اعتماد از محاسبات حجیم استفاده شده است.	می‌توان به مبادله‌ی توصیه‌ها در شبکه و ایجاد سربار، کارایی پایین در برابر حملات مبتنی بر شنود ناتوان است همه‌ی گره‌های بدرفتار را کشف نمی-کند.
G. Thanigaivel و **همکاران** 2013,	روشی بر پایه پروتکل مسیریابی AODV، تحت عنوان TRUNCMAN[۳۴] معیار ارزیابی اعتماد گره‌های همسایه، براساس بسته‌های ارسال شده است.	تأخیر و کارایی پایین در برابر حملات مبتنی بر شنود و ضعف در برقراری اعتماد
J. Li, R. Li, J. Kato,2012	یک چارچوب با هدف OTMF برای شبکه (OTMF) مدیریت اعتماد بر اساس هر دو اقتضایی متحرک اطلاعات مستقیم و غیر مستقیم برای مدیریت شهرت پیشنهاد دادند	عدم مقابله در برابر حملات مبتنی بر شنود و کشف نکردن همه‌ی گره‌های بدرفتار می‌باشد

۳-برقراری امنیت بر مبنای سیستم رمزنگاری:

سیستم رمزنگاری یکی از قوی‌ترین سیستم‌ها جهت پیاده‌سازی و افزایش امنیت در شبکه بوده و تنها روشی است که توانایی مقابله با حملات مبتنی بر شنود را دارد. سیستم رمزنگاری با استفاده از الگویتم‌های رمزنگاری و مزیت مخفی‌سازی اطلاعات اعتماد و امنیت در شبکه را ایجاد و پشتیبانی می‌کند. عملیات انجام شده در این سیستم بر پایه روش‌های رمزنگاری و استفاده از کلید جهت برقراری امنیت و پنهان‌سازی اطلاعات می‌باشد. در این سیستم بسته ارسالی با استفاده از الگوریتم رمزنگاری مورد استفاده و کلید تبادل شده رمز شده و برای گره مقصد ارسال می‌شود، گره‌های میانی در هنگام ارسال از محتویات بسته ارسالی آگاهی نداشته و گره‌های دشمن و نفوذی قادر به دسترسی به اطلاعات شبکه را نخواهد داشت. در واقع بزرگ‌ترین مزیتی که این روش‌های رمزنگاری فراهم می‌کنند جلوگیری از دسترسی به اطلاعات غیرمجاز شبکه می‌باشد. در ادامه روش‌های ارایه شده در زمینه امنیت و سیستم رمزنگاری طبقه بندی شده است.

۱- پروتکلی به‌نام ARAN[۳۵] :

در این کار ارائه شده که مبنای پروتکل پیشنهادی بر پایه رمزنگاری با کلید عمومی[۳۶] و همچنین استفاده از گواهی[۳۷] می‌باشد. پروتکل ARAN ملزم به استفاده از یک سرور صدور گواهی قابل اطمینان T است که کلید عمومی آن برای تمامی گره‌های

[34] Trust-based Routing Mechanism Using Non-Cooperative Movement in Mobile Ad-hoc Network
[35] Authenticated Routing for Ad hoc Networks
[36] Public Key

شبکه شناخته شده است. هر گره پیش از ورود به شبکه باید از T گواهی درخواست کند و پس از تصدیق اصالت[۳۸] خود توسط T، گواهی دریافت می‌کند. این گواهی شامل شناسه آدرس[۳۹] گره، کلید عمومی، مهر زمانی t برای زمان ایجاد شدن گواهی و e که زمان انقضاء گواهی می‌باشد، است.پروتکل ARAN برحسب تقاضا[۴۰] کار می‌کند و گره‌ها اطلاعات مسیرهای فعال را نگه‌داری می‌کنند. زمانی که هیچ نقل و انتقالی بر روی یک گره صورت نگرفته باشد، آن مسیر در جدول مسیریابی غیرفعال می‌شود. دریافت داده‌ها از یک مسیر غیرفعال باعث می‌شود که گره‌ها یک پیغام خطا (ERR[۴۱]) تولید کرده و بر روی مسیر عکس برای مبدأ ارسال کنند. در حالتی که یک گواهی باید منقضی شود، سرور صدور گواهی T پیغامی جهت اعلام انقضأ برای گروه ارسال می‌کند. هر گره پس از دریافت، مسیریابی خود را تصحیح و سپس آن‌را برای همسایه‌های خود ارسال می‌کند. این کار باعث می‌شود تا از ارتباط با گره‌های غیرقابل اطمینان خودداری شود. از محدودیت‌های این پروتکل مسئله توزیع امن کلید و وجود یک سرور صدور گواهی قابل اعتماد یا استفاده از سوم شخص قابل اعتماد برخلاف ذات شبکه‌های اقتضائی بوده و همچنین روش‌هایی که برای تصدیق اصالت ایمن به سرور گواهی لازم است در نظر گرفته نشده است و احراز صحت اطلاعات دریافتی توسط مقصد انجام نمی‌شود [۲۲].

۲- پروتکل ایمن‌سازی الگوریتم DSR[۴۲] :

در این پروتکل به‌جای استفاده از کلید عمومی از رمزنگاری متقارن استفاده می‌شود و برای تصدیق اصالت پیام‌ها از یک تابع درهم‌سازی[۴۳] بر روی پیام استفاده می‌شود. بنابراین هر گره می‌تواند از اصیل بودن پیام دریافتی اطمینان حاصل کند. مشکل عمده این الگوریتم نیاز به تولید و تبادل کلید بین گره‌های شبکه برای رمزنگاری، قبل از شروع پروتکل می‌باشد. همچنین از آن‌جایی‌که ممکن است کلید در طول عمر شبکه نامعتبر شود، ایجاد و تبادل کلید در بین گره‌های شبکه امکان‌پذیر نیست[۲۳].

۳- پروتکل SRP[۴۴] :

مبنای این پروتکل بر این اساس است که یک وابستگی امنیتی[۴۵] بین گره مبدأ و مقصد در نظر گرفته می‌شود. این وابستگی امنیتی به این صورت است که مبدا و مقصد می‌توانند به وسیله‌ی یک پروتکل تبادل کلید مانند الگوریتم دیفی هلمن[۴۶]، یک کلید خصوصی مشترک بین خود به اشتراک گذارند. گره‌های متخاصم ممکن است برای مختل کردن عملکرد شبکه رفتاری خودسرانه در پیش گیرند. آن‌ها قادر به خراب کردن، اجرای مجدد و همچنین ساختن بسته‌های مسیریابی می‌باشند و عموماً نمی‌توان انتظار داشت که پروتکل مسیریابی را به درستی اجرا کنند. این پروتکل از الگوریتم مسیریابی DSR استفاده می‌کند و یکی از مشکلات این الگوریتم عدم ایمنی در برابر حمله مردمیانی است. زیرا هیچ راهی برای پیگیری بسته‌های درون شبکه در طول مسیر وجود ندارد. اما بزرگترین محدودیت این پژوهش در توزیع امن کلید و احراز صحت اطلاعات دریافتی توسط مقصد می‌باشد. همچنین استفاده از پروتکل دیفی هلمن جهت ایجاد کلید حمله مرد میانی[۴۷] را در پی‌دارد که پروتکل پیشنهادی را کاملاً نا امن می‌کند (که درواقع این مشکل نیز از مسئله توزیع امن کلید ناشی می‌شود) [۲۴].

---

[37] Certificate
[38] Authenticate
[39] IP Address
[40] On-demand
[41] ERRor packet identifier
[42] Dynamic source routing
[43] Hash
[44] Secure Routing Protocol
[45] Secure Authenticate
[46] Diffie Hellman
[47] Man in the middle

۴- پروتکل به نام SAFC[۴۸]:

دراین پروتکل از رمزنگاری توأم با درهم‌سازی جهت ایجاد امنیت و احراز صحت اطلاعات استفاده شده است. عملکرد پروتکل به این صورت است که مبدأ در هنگام ارسال بسته، بسته ارسالی را درهم‌سازی کرده و مقدار حاصل شده را در کنار بسته قرار می‌دهد و در ادامه کل بسته را رمز می‌کند. رمز حاصل شده برای مقصد ارسال می‌شود. مقصد با دریافت بسته، آن را رمزگشایی کرده و مجدداً بسته رمز گشایی شده را درهم‌سازی می‌کند. اگر درهم‌سازی حاصل شده با درهم‌سازی دریافتی برابر نباشد از عملکرد مخرب گره‌های بدرفتار در طول مسیر آگاه شده و برای مبدأ نقض اعتبار[۴۹] ارسال می‌کند. مبدأ پس از دریافت نقض اعتبار به مسیر جایگزین تغییر جریان داده و ادامه ارسال اطلاعات را از مسیر جایگزین برای مقصد ارسال می‌کند. از محدودیت‌های این پژوهش توزیع امن کلید جهت رمزنگاری در شبکه می‌باشد[۲۵].

۵- پروتکل رمزنگاری SEAD[۵۰]:

در پروتکل SEAD، در هر گره جدول مسیریابی موجود است که در آن یک لیست از تمام اهداف احتمالی در شبکه وجود دارد. در هر جدول، آدرس اهداف را ذخیره می‌کند ، در نزدیکترین فاصله شناخته شده و گره های همسایه‌ای که می توانند با گام بعدی به هدف برسند مقیاس نامیده می‌شود . این مقیاس‌ها معمولا بر اساس تعداد گام در جداول نوشته شده است [26,27]. برای به‌روز رسانی جدول مسیریابی هر گره در بعضی مواقع یک پیام درخواست مسیر به همه‌ی همسایه‌هایش ارسال می‌کند تا قابلیت قرارگرفتن در جدول مسیر جدید را داشته باشد.در ابتدا امنیت توسعه داده شده‌ی SEAD، شماره توالی برای هر عامل جدول مسیریابی اضافه می‌کند. این شماره توالی از ایجاد حلقه جلوگیری می‌کند. تا باعث آن نشود که نتایج در خارج از زمان بروزرسانی شود. این پروتکل از یک سری درهم‌ساز یک طرفه استفاده می‌کند، برای این‌که امنیت تابع رمزنگاری نامتقارن سریع‌تر فراهم کند [26,28]. برای ساخت سری درهم‌ساز یک‌طرفه، هر گره یک شماره X به عنوان $X \in \{0.1\}$ به صورت تصادفی انتخاب می‌شود.(p تعداد بیت بازده تابع درهم‌ساز است.) و یک سری از $h_0 = h_1 . h_2 \ldots\ldots h_n$ به عنوان تساوی زیر ایجاد می‌کند.

$$h_0 = X \quad . \quad h_i = H(h_i) \qquad (۳)$$

هر گره عامل بعدی سری درهم‌ساز مهر شده، می‌تواند در پروسه‌ی به روزرسانی استفاده شود. بنابراین فرض شده محدوده‌ی آستانه برای شماره توالی و اندازه کمتر است، همچنین هر گره‌ای می‌تواند مسیر جدید با شماره توالی بالاتر یا اندازه‌گیری پایین‌تر در شبکه بسازد.این باعث شده که از اختلال در بروزرسانی شبکه جلوگیری کند. در حقیقت SEAD مانع از آن می‌شود تا دشمن انتشار داده‌ی به روزرسانی مسیر را تغییر دهد. این تغییر دادن دشمن بالغ بر شماره توالی و با اندازه‌ی بسته‌ها است، که باعث ایجاد مشکل در بروزرسانی مسیر می‌شود.پاسخ حمله همچنین در SEAD رسیدگی می‌شود. به وسیله‌ی دریافت یک بسته‌ی بروزرسانی مسیر و شماره توالی، درهم‌ساز دریافت شده‌ی قبلی، و شماره‌ی مناسب از درهم‌ساز در مقدار جدید، هر گره می‌تواند دریافت بسته‌ها را تصدیق کند .برای تصدیق درستی دریافت از گره‌ی منبع، این روش از پیام کد قابل اعتماد استفاده می‌کند. این روش برای ساختن یک کلید بین دو گره نیز ارایه شده است[۲۷].

[48] Simple Acknowledgment and Flow Conversation
[49] Confidentiality lost
[50] Secure Efficient Ad-Hoc Distance Vector Routing

۶- Neha Gupta, Manish Shrivastava [۲۹] از یک آستانه معروف به آستانه رمزنگاری[۵۱] (t,l) استفاده گردیده که کلید خصوصی CA[۵۲] به واسطه روابط چندجمله‌ای به l قسمت شکسته شده و در اخیتار l گره، که گره‌های نگه دارنده سهم[۵۳] نام برده شده‌اند، قرار داده می‌شود. هنگامی که گره جدیدی به شبکه اضافه می‌گردد لازم است تا گره مورد نظر حداقل توسط t گره گواهینامه خود را امضا کرده تا این گره احراز هویت گردد. در ادامه گره‌ای که قصد دارد به صورت امنیتی داده ارسال کند (مبدأ) ضرورت دارد تا سه مرحله زیر را انجام دهد:

۱) بازسازی کلید امنیتی توسط گره مبدأ به واسطه دریافت حداقل سهم (مشخص شده در آستانه رمزنگاری) از گره‌های نگه دارنده.۲) رمزنگاری داده با کلید به دست آمده. ۳) ارسال داده برای گره مقصد

در طرف مقابل گره مقصد عملیات زیر را انجام می‌دهد:

۱. بازسازی کلید امنیتی توسط گره مقصد به واسطه دریافت حداقل سهم (مشخص شده در آستانه رمزنگاری) از گره‌های نگه دارنده. ۲) رمزگشایی داده دریافتی با استفاده از کلید به دست آمده.

این روش اگرچه امنیت مناسبی را پیاده‌سازی می‌نماید، ولی دارای محدودیت‌های بزرگی نیز می‌باشد. از محدودیت‌های پژوهش پیشنهادی نبود قابلیت دسترسی به تعداد کافی از گره‌های نگه دارنده جهت ایجاد کلید برای تمامی گره‌های شبکه، کادرهم‌ساز سرعت شبکه بصورت نمایی با افزایش گره‌های شبکه، افزایش محاسبات و تأخیر بالا را می‌توان نام برد. همچنین در پژوهش ارائه شده مسئله توزیع امن کلید به صورت کارایی لحاظ نگردیده است.

۷- پروتکل ECCEA[۵۴]:

بر مبنای پروتکل پایه AODV ارائه شده که اساس کار این پروتکل بر مبنای استفاده از زنجیره درهم‌سازی و امضا دیجیتال به منظور برقراری اعتماد، احراز صحت و ایجاد قابلیت عدم انکار سرویس می‌باشد. توجه این پروتکل بر روی ارسال بسته‌های درخواست مسیر و پاسخ و به خصوص فیلد تعداد گام و تصدیق انتها به انتها می‌باشد و با استفاده از توابع درهم-سازی از بروز حملات در این حیطه جلوگیری می‌کند. همچنین به منظور رمزنگاری و رمزگشایی از کلید رمزنگاری استفاده گردیده و احراز صحت اطلاعات ارسالی و ایجاد قابلیت عدم انکار توسط امضا پشتیبانی می‌گردد. در این کار احراز صحت اطلاعات ارسالی و جلوگیری از حملات مربوط به تعداد گام بسته به خوبی پوشش داده شده ولی هم‌چنان پروتکل ارائه شده از ایجاد و توزیع امن کلید رمزنگاری رنج برده و تأخیر بالایی را به دنبال دارد[۳۰].

۸- پروتکل AODV امن(SAODV)

همانطور که از نام آن مشخص است، برای ایجاد امنیت بیشتر در پروتکلAODV ، ارائه شده و از توابع درهم‌ساز در آن استفاده شده است ،که در رابطه۴ نشان داده است:

$$H(n-1) = H(hn) \qquad (۴)$$

دراین رابطه ، Hتابع درهم‌ساز و h مربوط به هاپ است . در این پروتکل ، ازتعداد هاپ استفاده می‌شود برای اندازه گیری تعداد گره‌هایی از طریق آن بسته عبور می‌کند.اگر تعداد هاپ بیش از مقدار حداکثر آن شود، بسته نادیده گرفته می‌شود. برای جلوگیری از تغییرات مقدار تعداد هاپ و باید در مورد دقت مقدار آن، که استفاده شده در توابع درهم‌ساز اطمینان حاصل شود .با توجه به معادله ۴، هر گره می تواند با دریافت یک پیام و کنترل در رابطه بالا بر روی آن در مورد صحتش مطمئن شود .تعداد n حداکثر هاپ که یک بسته می تواند از طریق آن عبور کند را نشان می‌دهد[۳۱] .

همان طور که پروتکل‌های سیستم رمزنگاری و برقراری امنیت مشاهده شد ،اساسی‌ترین مشکل سیستم‌های رمزنگاری مسئله توزیع امن کلید و عدم مقابله در برابر حملات گره‌های مخرب شبکه که قصد بر هم زدن عملیات شبکه را دارند می‌باشد. در

[51] Threshold cryptography
[52] Certificate Authority
[53] share holders
[54] Elliptic Curve Cryptography Enabled AODV

جدول ۲ کارهای ارایه شده در زمینه‌ی پروتکل‌های مرتبط به امنیت در این مقاله ، به انضمام محدودیت‌های آن‌ها بیان شده است.

جدول۲- مروری بر مهمترین کارهای مرتبط با حوزه رمزنگاری

نویسنده/سال	عملکرد پروتکل	محدودیت
Y. –C. HU, and A. PERRIG,2005	پروتکل ایمن‌سازی الگوریتم DSR برای تصدیق اصالت پیام‌ها از یک تابع درهم‌سازی[55] بر روی پیام استفاده می-شود. بنابراین هر گره می‌تواند از اصیل بودن پیام دریافتی اطمینان حاصل کند.	نیاز به تولید و تبادل کلید بین گره‌های شبکه برای رمزنگاری، قبل از شروع پروتکل می‌باشد. همچنین از آن‌جایی‌که ممکن است کلید در طول عمر شبکه نامعتبر شود، ایجاد و تبادل کلید در بین گره‌های شبکه امکان‌پذیر نیست
Mamatha و همکاران در سال ۲۰۱۰	استفاده از سیستم رمزنگاری برقراری اعتماد، اضافه کردن کد درهم به بسته و ارسال آن ، مقصد برای بسته‌های نادرست نقیض اعتبار برای مبدأ ارسال و مبدأ به مسیر جایگزین تغییر جریان می‌دهد.	سربار و افزایش محاسبات کشف نکردن همهٔ گره‌های بدرفتار
Q. Gu , 2010.	یک وابستگی امنیتی[56] SRPپروتکل بین گره مبدأ و مقصد در نظر گرفته می-شود. این وابستگی امنیتی به این صورت است که مبدا و مقصد می‌توانند به وسیله‌ی یک پروتکل تبادل کلید مانند الگوریتم دیفی هلمن[57]، یک کلید خصوصی مشترک بین خود به اشتراک گذارند	عدم ایمنی در برابر حمله مردمیانی زیرا هیچ راهی برای پیگیری بسته‌های درون شبکه در طول مسیر وجود ندارد. بزرگترین‌محدودیت این پژوهش در توزیع امن کلید و احراز صحت اطلاعات است
G.S. Mamatha and S.C. sharma ,2010.	در پروتکل به نام SAFC از رمزنگاری توأم با درهم‌سازی استفاده شده است. مبدأ در هنگام ارسال بسته، بسته ارسالی را درهم‌سازی کرده و مقدار حاصل شده را در کنار بسته قرار می-دهد و در ادامه کل بسته را رمز می‌کند. رمز حاصل شده برای مقصد ارسال می-شود. مقصد با دریافت بسته، آن را	توزیع امن کلید جهت رمزنگاری در شبکه می‌باشد.

[55] Hash
[56] Secure Authenticate
[57] Diffie Hellman

	رمزگشایی کرده و مجدداً بسته رمز گشایی شده را درهم‌سازی می‌کند.	
Sanzgiri.K و همکاران ۲۰۱۲	بر پایه رمزنگاری با ARANپروتکل کلید عمومی[58] و همچنین استفاده از گواهی[59] می‌باشد. این گواهی شامل شناسه آدرس[60] گره، کلید عمومی، مهر برای زمان ایجاد شدن گواهی و tزمانی که زمان انقضاء گواهی می‌باشد است.e	مسئله توزیع امن کلید و وجود یک سرور صدور گواهی قابل اعتماد یا استفاده از سوم شخص قابل اعتماد برخلاف ذات شبکه‌های اقتضایی بوده و همچنین روش‌هایی که برای تصدیق اصالت ایمن به سرور گواهی لازم است در نظر گرفته نشده است و احراز صحت اطلاعات دریافتی توسط مقصد انجام نمی‌شود
N. Guptal, & M. Shrivastava March-2013	پیاده سازی امنیت مناسب در شبکه با استفاده از یک مقدار استانه و کلید CAخصوصی	نبود قابلیت دسترسی به تعداد کافی از گره‌های نگه دارنده جهت ایجاد کلید برای تمامی گره‌های شبکه، کادرهم‌ساز سرعت شبکه بصورت نمایی با افزایش گره‌های شبکه، افزایش محاسبات و تأخیر بالا
B. Reddy, and M. N. Prasad, March-2014.	بر مبنای استفاده از زنجیره درهم‌سازی و امضاء دیجیتال به منظور برقراری اعتماد، احراز صحت و ایجاد قابلیت عدم انکار سرویس می‌باشد.	توزیع امن کلید رمزنگاری رنج برده و تأخیر بالایی را به دنبال دارد

۴- نتیجه‌گیری

شبکه‌های اقتضائی به دلیل نوین بودن‌شان و استفاده روزافزون از این شبکه‌ها توجه پژوهشگران بسیاری را به خود جلب نموده‌اند. یکی از اساسی‌ترین مفاهیم و در عین حال پرچالش‌ترین مفاهیم شبکه‌های اقتضائی امر مسیریابی و ارسال اطلاعات این دسته از شبکه‌ها می‌باشد ،که به دلیل ویژگی‌های خاص این دسته از شبکه‌ها چهره‌ای متفاوت و عملکردی خاص دارد. با توجه به اهمیت شبکه‌های اقتضائی در کاربردهای امروزی به ویژه در موارد حساس، امنیت و اعتماد در مسیریابی و ارسال اطلاعات این دسته از شبکه‌ها، امری حایز اهمیت است. در این مقاله به مروری بر کارهای انجام شده و طبقه‌بندی آنها در زمینه‌ی برقراری امنیت در سیستم رمزنگاری و برقراری اعتماد در سیستم شهرت پرداخته و بررسی شد که هر کدام از این سیستم‌ها به تنهایی توانایی مقابله با حملات فعال و غیرفعال توام با یکدیگر را ندارند .در واقع برای مقابله با هر دو حمله به طور همزمان ترکیب سیستم شهرت در جهت مقابله با حملات غیرفعال (مبتنی بر شنود) با سیستم رمزنگاری در جهت مقابله با حملات فعال نیاز است.

[58] Public Key
[59] Certificate
[60] IP Addr

منابع

[1] L. Abusalah, A. Khokhar, and M. Guizani, "A survey of secure mobile ad hoc routing protocols," *Communications Surveys & Tutorials, IEEE*, vol. 10, no. 4, pp. 78-93, 2008.

[2] R. Haboub and M. Ouzzif, "Secure and reliable routing in mobile adhoc networks," *International Journal of Computer Science & Engineering Survey (IJCSES)*, vol. 3, no. 1, pp. 53-64, 2012.

[3] S. Aghaie, and F. Adibnia, "A Novel Approach for Anonymous Secure Routing in Mobile Ad Hoc Network Using Cryptography," *IJCSNS International Journal of Computer Science and Network Security*, Vol.13, pp. 63-71, January 2013.

[4] Cheng, X., X. Huang, and D.-Z. Du, Ad hoc wireless networking. Vol. 14. 2013: Springer Science & Business Media.

[5] J. Li, R. Li, J. Kato, Future trust management framework for mobile ad hoc networks: security in mobile ad hoc networks, IEEE Communications Magazine 46 (4) (2008) 108–114

[6] R.H. Jhaveri, S.J. Patel, and D.C. Jinwala, "Dos attacks in mobile ad hoc networks: A survey," in *Advanced Computing & Communication Technologies (ACCT), Second International Conference on*, 2012, pp. 535-541.

[7] Y.C. Hu, A. Perring, D.B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," Proceedings of the 2003 ACM workshop on Wireless security,San Diego, USA, pp. 30-40, 2003.

[8] Narula, P., et al., Security in mobile ad-hoc networks using soft encryption and trust-based multi-path routing. Computer Communications, 2008. 31(4): p. 760-769.

[9] S. Sutariya, and P. P. Modi, "A Review of Different Reputation Schemes to Thwart the Misbehaving Nodes in Mobile Ad Hoc Network," *International Journal of Computer Science and Information Technologies*, Vol. 5, pp. 4599-4603, 2014.

[10] Jin-Hee Cho, Member, IEEE, Ananthram Swami, Fellow, IEEE, and Ing-Ray Chen, Member, IEEE, "A Survey on Trust Management for Mobile Ad Hoc NetworksIEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 13, NO. 4, FOURTH QUARTER 2011.

[11] Isa Maleki1, Ramin Habibpour2, Majid Ahadi3, Amin Kamalinia4, "SECURITY IN ROUTING PROTOCOLS OF AD-HOC NETWORKS: A REVIEW," International Journal of Mobile Network Communications & Telematics (IJMNCT) Vol. 3, No.4, August 2013.

[12] A.A. Pirzada and C. McDonald, "Trust establishment in pure ad-hoc networks," Wireless Personal Communications, vol. 37, no. 1-2, pp. 139-168, 2006.

[13] Y.L. Sun, Z. Han, W. Yu, and K.J.R. Liu, "A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense Against Attacks," INFOCOM, 2006.

[14] L. Junhai and F. Mingyu, "A Subjective Trust Management Model Based on Certainty-Factor for MANETs," Journal of Computer Research and Development, vol. 47, pp. 515-523, 2010.

[15] H. Xia, Z. Jia, X. Li, L. Ju, and E.H.M. Sha, "Trust prediction and trust-based source routing in mobile ad hoc networks," Ad Hoc Networks,Vol. 13, pp. 1-19, 2012.

[16] Jawhar, I., Z. Trabelsi, and J. Al-Jaroodi, *Towards more reliable and secure source routing in mobile ad hoc and sensor networks.* Telecommunication Systems, 2014. 55(1): p. 81-91.

[17] N. Marchang, R. Datta, Light-weight trust-based routing protocol for mobile ad hoc networks, IET Information Security 6 (2) (2012) 77–83.

[18] G. Thanigaivel, N.A. Kumar, and P. Yogesh, "TRUNCMAN: Trust based routing mechanism using non-cooperative movement in mobile ad-hoc network," in Digital Information and Communication Technology and it's Applications (DICTAP), Second International Conference on, IEEE, 2012, pp. 261-266.

[19] M. A. Moustafa, M.A. Youssef, and M.N. El-Derini, "MSR: A multipath secure reliable routing protocol for WSNs," in Computer Systems and Applications (AICCSA), 9th IEEE/ACS International Conference on, 2011, pp. 54-59.

[20] X Li, M.R Lyu, and J Liu, "A trust model based routing protocol for secure ad hoc networks," Aerospace Conference, 2004. Proceedings. 2004 IEEE , vol.2, pp.1286,1295 2004

[21] I. Jawhar, Z. Trabelsi, and J. Jaroodi, "Towards More Reliable and Secure Routing in Mobile Ad Hoc and Sensor Networks," Telecommunication Systems Springer, Vol. 16, pp. 1-10, 2014.

[22] K. Sanzgiri, D. LaFlammey, B. Dahilly, "Authenticated Routing for Ad hoc Networks," IEEE Security and Privacy 2004,Vol. 2, No. 3, PP. 94-105, May/June 2005.

[23] Y. –C. HU, and A. PERRIG, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Springer Science Wireless networks 2005,Vol. 2, No. 3, PP. 94-105, May/June 2005.

[24] Q. Gu, Secure Routing Protocols, Encyclopedia of Cryptography and Security (2ndEd.), H. Tilborg and S. Jajodia Ed., Springer, 2010.

[25] G.S. Mamatha and S.C. Sharma, "A robust approach to detect and prevent network layer attacks in MANETS," International Journal of Computer Science and Security, vol. 4, no. 3, pp. 275-284, 2010.

[26] Y.C. Hu, A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy 2004,Editorial Calendar, Vol. 2, No. 3, pp. 94-105, May/June 2004.

[27] C.H. Lin, W.S. Lai, Y.L. Huang, M.C. Chou, "I-SEAD: A Secure Routing Protocol for Mobile Ad Hoc Networks", International Conference on Multimedia and Ubiquitous Engineering, pp. 102-107, April 2008.

[28] S. Basagni, M. Conti, S. Giordano, I. Stojmenovic, "Mobile Ad-hoc Networking", IEEE press, John Wiley and Sons publication, pp. 329-354, 2004.

[29] N. Guptal, M. Shrivastava, "Securing Routing Protocol by Distributed Key Management and Threshold Cryptography in Mobile Ad hoc Network ", International Journal of Advanced Computer Research, Vol-3, pp. 13-18, March-2013.

[30] B. Reddy, and M. N. Prasad, "Efficient Lightweight Hybrid Cryptography Solution to Secure Mobile Ad hoc Networks," International Journal of Research in Computer and Communication Technology, Vol. 3, pp. 325-332, March-2014.

[31] F. Maan, Y. Abbas, N. Mazhar, "Vulnerability assessment of AODV and SAODV routing protocols against network routing attacks and performance comparisons", Wireless Advanced (WiAd), London, pp. 36-41, June 2011.