مروری بر مهم‌ترین و اخیرترین پژوهش‌های حوزه امنیت و تشخیص نفوذ در شبکه‌های حسگر بی‌سیم

سمیه میرزاوند[1*]، محسن چکین[2]

۱- دانشگاه آزاد اسلامی واحد دزفول، گروه مهندسی کامپیوتر، دزفول، ایران،
Mirzavand.somayeh@yahoo.com

۲- دانشگاه آزاد اسلامی واحد دزفول، گروه مهندسی کامپیوتر، دزفول، ایران،
mcheghin@gmail.com

چکیده

شبکه‌های حسگر بی‌سیم از جمله شبکه‌های نوین امروزی بوده که در کاربردها و عرصه‌های مختلفی مورد استفاده و بهره‌برداری قرار گرفته‌اند. شبکه‌های حسگر بی‌سیم از سنسورهایی تشکیل شده است که وظیفه جمع‌آوری اطلاعات از محیط اطراف را بر عهده دارند. این شبکه‌ها به دلیل بی‌سیم بودن، محدودیت منابع، تحرک و پویایی و وظایف مهم و بحرانی که دارند نسبت به شبکه های دیگر دارای آسیب‌پذیری نسبتا بالایی هستند. ساختار توزیع‌شدگی کامل شبکه‌های حسگر و نبود قدرت کنترل‌کننده مرکزی و کاربردهای حساس و ویژه شبکه، این دسته از شبکه‌ها را مستعد اعمال حملات مختلف می‌سازد. به‌دلیل ویژگی‌های خاص شبکه‌های حسگر بی‌سیم و محدودیت‌های ذاتی که در منابع دارا هستند، برقراری امنیت و قابلیت اطمینان در این شبکه‌ها به یک چالش تبدیل شده است. لذا در این مقاله، به تجزیه و تحلیل برخی از مهم‌ترین مقالات و تحقیقاتی که تاکنون در حوزه پشتیبانی از اعتماد در شبکه‌های حسگر بی‌سیم ارائه گردیده پرداخته شده و این پژوهش‌ها را نقد و بررسی خواهیم نمود.

کلمات کلیدی: شبکه حسگر بی‌سیم، امنیت، تشخیص نفوذ

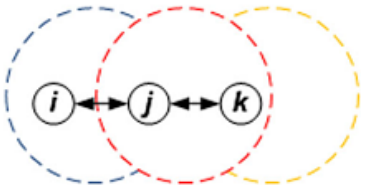
۱–مقدمه

شبکه‌های حسگر بی‌سیم از جمله شبکه‌های نوین امروزی بوده که در کاربردها و عرصه‌های مختلفی مورد استفاده و بهره‌برداری قرار گرفته‌اند. ساختار توزیع شدگی کامل شبکه‌های حسگر و نبود قدرت کنترل‌کننده مرکزی از یک‌سو نمایان‌گر آسیب‌پذیری بالای شبکه در قبال آسیب‌های امنیتی می‌باشد، و از سوی دیگر کاربردهای حساس و ویژه شبکه به خصوص در عرصه‌های نظامی و خاص این دسته از شبکه‌ها را مستعد اعمال حملات مختلف می‌سازد. ازاین‌رو وجود راه‌کارهایی در جهت پشتیبانی و پیاده‌سازی امنیت و تشخیص نفوذ در این دسته از شبکه‌ها به عنوان یکی از ملزومات شبکه به شمار رفته و اساسی‌ترین ابزار در جهت افزایش کارایی شبکه می‌باشند [۱]. سیستم تشخیص نفوذ به عنوان یکی از سازوکارهای مهم و کارامد در جهت برقراری امنیت در بستر شبکه‌های حسگر به شمار می‌رود. با توجه به اهمیت بالای مبحث امنیت در شبکه‌های حسگر و شایستگی‌های مکانیزم تشخیص نفوذ تاکنون پژوهش‌های مختلفی به ویژه در سال‌های اخیر مبتنی بر عملکرد این مکانیزم توسعه یافته‌اند که به نوعی اهمیت موضوع پژوهش را در میان سایر موضوعات پژوهشی نمایش می‌دهد [۲].

۳– مروری بر پژوهش‌های حوزه امنیت و تشخیص نفوذ در شبکه‌های حسگر بی‌سیم

تا به‌حال پژوهش‌های بسیاری در راستای بهبود پیاده‌سازی امنیت و تشخیص نفوذ در شبکه‌های حسگر بی‌سیم با کار کردن برروی معماری‌ها و پروتکل‌های مسیریابی و مکانیزم‌های پیاده‌سازی امنیت ارائه گردیده که نشان دهنده اهمیت بالای این موضوع در شبکه‌های حسگر بی‌سیم می‌باشد. در این قسمت از فصل به بررسی و تحلیل برخی از اخیرترین و معتبرترین پژوهش‌های ارائه شده، پرداخته خواهد شد و آن‌ها را از دیدگاه ضرورت ارائه پژوهش جاری با توجه به چگونگی نحوه عملکردشان آنالیز و ارزیابی خواهیم نمود. هدف از این امر در وهله اول نمایش اهمیت و ارزش موضوع و مسئله پژوهشی به عنوان چالشی باز در میان پژوهش‌های گذشته، و در وهله دوم تحلیل عملکرد، و مزایا و معایب پژوهش‌های انجام شده با هدف بهره‌گیری از مزایای سوابق پژوهش در ارائه روش پیشنهادی، و پوشش محدودیت‌های موجود در ارائه راه‌کاری کارآمد می‌باشد. در ادامه به بررسی سوابق پژوهش و تحلیل هر پژوهش وابسته به مسئله پژوهشی پرداخته شده است.

از جمله پژوهش‌های مهمی که در حوزه بهبود تشخیص نفوذ در شبکه‌های حسگر بی‌سیم ارائه و معرفی گردیده می‌توان به پژوهش ادنن و همکاران در سال ۲۰۱۶ اشاره کرد [۳]. ادنن و همکاران در این پژوهش پروتکلی با نام TERP معرفی نمودند. TERP در جهت پشتیبانی از امنیت و تشخیص نفوذ بر مبنای نظارت مستقیم، نظارت غیرمستقیم، و عاملی تحت عنوان افزایش دقت محاسبات امنیت گسترش یافته است. بدین جهت در وهله اول تشخیص نفوذ و اعتبار گره‌ها بر محوریت حالت بی‌قاعده ارزیابی و دنبال می‌گردد. شکل (۱) نمایی از این فرایند نظارت را مبتنی بر عملکرد حالت بی‌قاعده نمایش می‌دهد.



شکل ۱ - بهره‌بری از حالت بی‌قاعده در جهت تشخیص نفوذ [۳]

در ادامه نتیجه ارزیابی‌ها و نظارت‌های مستقیم با نظارت‌های غیرمستقیم (توصیه‌های تبادلی) از حسگرهای همجوار ترکیب می‌گردد. به‌طوری‌که اطمینان از توصیه‌های به اشتراک گذاشته شده بر محوریت ارزش‌گذاری گره درخواست کننده و بر اساس اعتبار گره‌های پاسخ دهنده سنجیده و در محاسبات نهایی تشخیص نفوذ شرکت داده می‌شود. در انتها این دو شاخص با شاخص دیگری تحت عنوان افزایش دقت محاسبات امنیت، ترکیب و تشخیص نفوذ نهایی را مبتنی بر رابطه (۱) تشکیل می‌دهند.

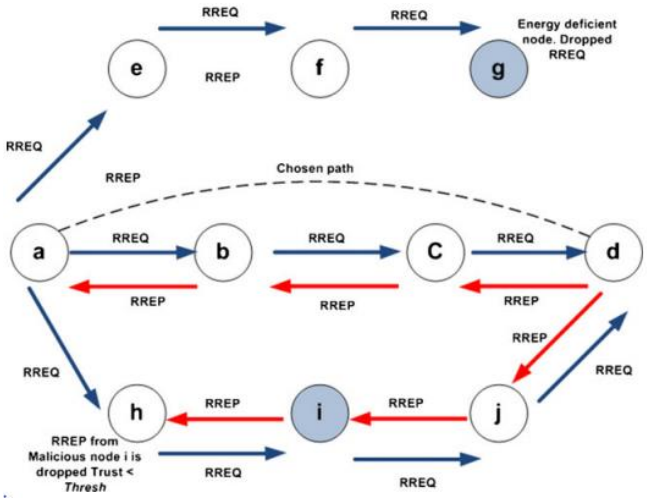
$$T_{i,j}(t) = w_1 DT_{i,j}(t) + w_2 \frac{IT_{i,j}^{k}(t)}{N_j} + w_3 E(p)_{i,j}(t) \qquad (1)$$

مقدار اعتماد نهایی حاصل از تشخیص نفوذ با دو شاخص انرژی و تأخیر مسیرهای میانی با هدف پشتیبانی از مفهوم اطمینان در شبکه، ترکیب و انتخابات نهایی گره‌ها و مسیرهای میانی مبتنی بر رابطه (۲) صورت می‌پذیرد. از چالش‌های مرتبط با TERP می‌توان به افزایش سربارهای ناشی از اشتراک‌گذاری توصیه‌ها، آسیب‌پذیری در برابر گره‌های نفوذی، افزایش سربارها و ناتوانی در کشف برخی حملات را اشاره نمود.

$$T_{i,j}(t) = \alpha * Trust + \beta * Energy + \gamma * Hopcount \qquad (2)$$

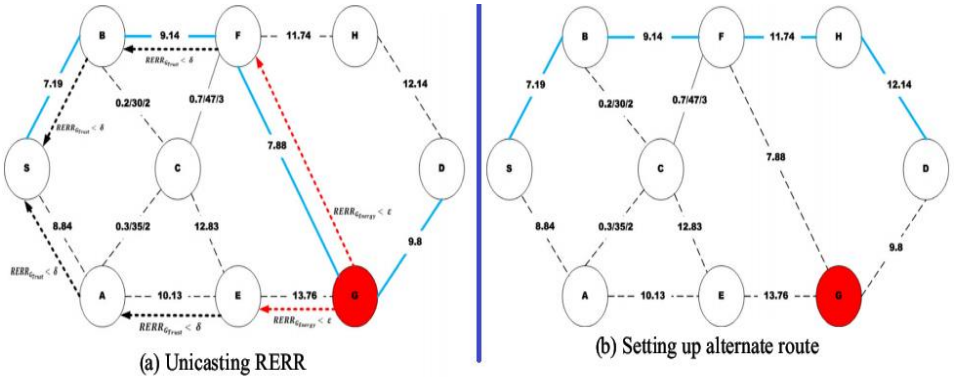
از جمله پژوهش‌های مهم دیگری که در حوزه بهبود تشخیص نفوذ در شبکه‌های حسگر بی‌سیم ارائه و معرفی گردیده می‌توان به پژوهش دیگر ادنن و همکاران در سال ۲۰۱۶ اشاره کرد [۴]. ادنن و همکاران در این پژوهش پروتکل دیگری تحت عنوان TESRP با هدف عملکرد پروتکل TERP ارائه و معرفی نمودند. عملکرد این پروتکل به منظور بهبود چالش‌ها و آسیب‌پذیری‌های پروتکل TERP بر مبنای توزیع بتا توسعه یافته است. توزیع بتا در کنار تشخیص نفوذ به‌کار رفته تا امنیت با دقت بالاتری سنجیده شده و از آسیب‌های گره‌های بدخواه تا حد امکان پیش‌گیری گردد. همچنین به منظور بهبود پیاده‌سازی اطمینان از تعاملات TESRP در حین مسیریابی از شرکت گره‌هایی با انرژی و کارایی پایین در پروسه مسیریابی پیش‌گیری

نموده و در نتیجه مسیرهایی با انرژی و کارایی بالا کشف خواهند شد تا اطمینان نیز به صورت مطلوب‌تر توسعه و پشتیبانی گردد. شکل (۲) نمایی از این فرایند را در ارتباط با پروتکل TESRP نمایش می‌دهد. از چالش‌های مرتبط با پروتکل TESRP می‌توان به آسیب‌پذیری‌های امنیتی در مقابله حملات نفوذی‌ها با قصد فریب سیستم تشخیص نفوذ، مغایرت ارزیابی‌های اعتماد با اطمینان، و افزایش سربار و تأخیر فرایند مسیریابی را اشاره نمود.



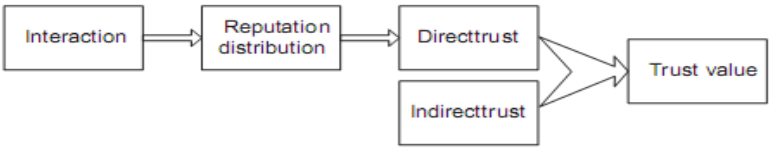
شکل ۲ - نمایی از فرایند مسیریابی پروتکل TESRP [٤]

از جمله پژوهش‌های مهم دیگری که در حوزه بهبود تشخیص نفوذ در شبکه‌های حسگر بی‌سیم ارائه و معرفی گردیده می‌توان به پژوهش دیگر ادنن و همکاران در سال ۲۰۱۷ اشاره کرد [۵]. ادنن و همکاران در این پژوهش پروتکل دیگری با نام ESRT با هدف بهبود عملکرد پروتکل TERP و TESRP ارائه و معرفی نمودند. تشخیص نفوذ پروتکل ESRT به منظور دستیابی به اهداف معین شده و بهبود مسائل دو پروتکل اشاره شده (و مرتبط)، بر محوریت عملکرد همان دو پروتکل با افزدن معیار بازه‌های زمانی تراکنش‌ها در ارزیابی‌های تشخیص نفوذ توسعه یافته است. همچنین به منظور بهبود پیاده‌سازی اطمینان و پشتیبانی از خطاهای مسیرهای تعاملات در ارتباط با عملکرد نامطلوب TESRP همروند با پشتیبانی از اطمینان، از انتشار تک‌پخشی بسته‌های شکست مسیر تنها در مسیرهای به سمت مبدأ و مسیریابی چندمسیری با هدف استفاده از مسیرهای پشتیبان بهره برده شده است. شکل (۳) نمایی از این فرایند را در ارتباط با عملکرد ESRT نمایش می‌دهد. از چالش‌های مرتبط با این پروتکل می‌توان به افزایش تأخیر مسیریابی چندمسیری، افزایش سربارهای تشخیص نفوذی (اشتراک‌گذاری توصیه‌ها)، و عدم وجود تدابیر کافی در جهت مقابله با حملات گره‌های نفوذی را عنوان نمود.



شکل ۳- پروسه مسیریابی و بازیابی خطا در مسیرها تعاملات مبتنی بر عملکرد ESRT [٥]

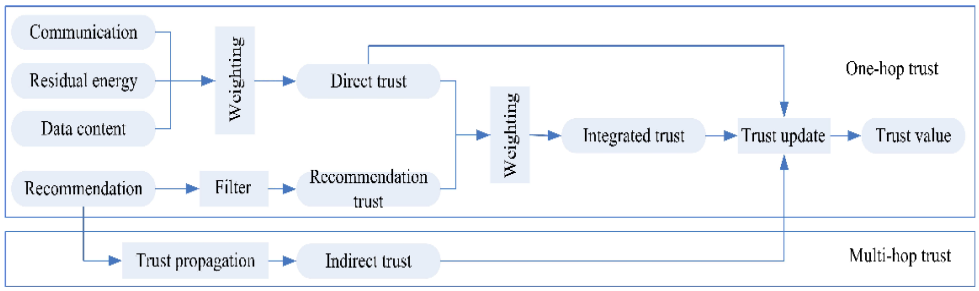
از جمله پژوهش‌های مهم دیگری که در حوزه بهبود تشـخیص نفوذ در شـبکه‌های حسـگر بی‌سـیم ارائه و معرفی گردیده می‌توان به پژوهش دیگر فنگ و همکاران در سـال ۲۰۱۶ اشـاره کرد [۶]. فنگ و همکاران در این پژوهش پروتکل با نام BTRES با هدف بررسی و شناسایی حملات داخلی و ارائه روشی به منظور پیش‌گیری از این دسته از حملات معرفی نمودند. BTRES بر مبنای عملکر سیستم تشخیص نفوذ توسعه یافته و بر اساس مزایا این سیستم و استفاده از قابلیت‌های تابع توزیع بتا عملکرد خود را در شـبکه‌های حسـگر بی‌سـیم گسـترش می‌دهد. تشخیص نفوذ در این روش مبتنی بر نظارت مستقیم و غیرمسـتقیم بر پایه قابلیت‌های توزیع بتا صـورت پذیرفته (توزیع بتا قابلیت افزایش دقت محاسـبات را فراهم می‌نماید) و بر اسـاس نتیجه نهایی محاسـبات، در ارتباط با حسـگرها نتیجه‌گیری می‌شود. شکل (۴) نمایی از عملکرد BTRES را در جهت تشخیص نفوذ نمایش می‌دهد. از چالش‌های مرتبط با BTRES می‌توان به آسیب‌پذیری پروتکل در مقابله با نفوذی‌ها با قصد فریب سیستم تشخیص نفوذ و افزایش سربارهای تحمیلی به شبکه به منظور اشتراک‌گذاری توصیه‌ها را اشاره نمود.



شکل ٤- نمایی از اجزای عملیاتی BTRES [٦]

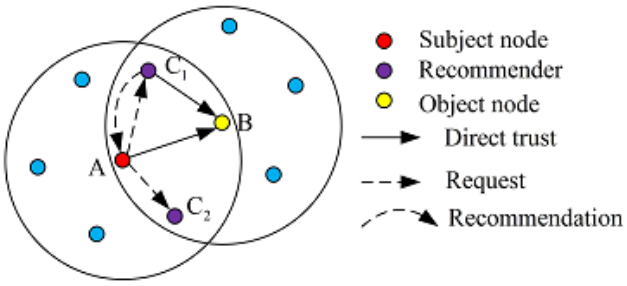
از جمله پژوهش‌های مهم دیگری که در حوزه بهبود تشـخیص نفوذ در شـبکه‌های حسـگر بی‌سـیم ارائه و معرفی گردیده می‌توان بـه پژوهش دیگر یـا و همکـاران در سـال ۲۰۱۶ اشـاره کرد [۷]. یـا و همکـاران در این پژوهش پروتکـل با نام TeAOMDV معرفی و ارائه گردیده اسـت. TeAOMDV بر مبنای توسـعه پروتکل پایه AOMDV و منطق فازی گسـترش یافته اسـت. منطق فازی کاربردی در این پروتکل در سـنجش اعتبار گره‌های شـبکه مورد استفاده قرار گرفته و تصمیم‌گیری تشـخیص نفوذ به واسـطه روابط خطی انجام می‌گیرد. عملکرد TeAOMDV مبتنی بر دو شـاخص، ارزش اعتماد مسـیر و مسـیریابی کم‌تأخیر گسـترش یافته است. به‌طوری‌که در وهله اول اعتبار مسیر احراز گردیده و سپس از میان مسیرهای امن، مسـیر با تأخیر کمینه انتخاب خواهد گردید. در جهت تشـخیص نفوذ پروتکل TeAOMDV بر پایه ارزیابی نظارت مستقیم با قابلیت تفکیک بسته‌های تعاملی و ارزش‌گذاری متغیر وابسته به اهمیت بسته، و تابع محوشدگی عمل می‌نماید. TeAOMDV از نظارت‌های سایرین به صورت محلی با هدف کاهش سربارها بهره برده و به جهت افزایش دقت محاسبات این نظارت‌ها را اعمال ضـریب دقت ارزیابی می‌نماید. از مزایای این پروتکل می‌توان به پیش‌گیری از حملات انکارسرویس اشاره نمود. اما از چالش‌های مرتبط با پروتکل TeAOMDV می‌توان به آسـیب‌پذیری در برابر گره‌های نفوذی و عدم قابلیت شـناسـایی همه گره‌های مخرب را می‌توان اشاره نمود.

از جمله پژوهش‌های مهم دیگری که در حوزه بهبود تشـخیص نفوذ در شـبکه‌های حسـگر بی‌سـیم ارائه و معرفی گردیده می‌توان به پژوهش دیگر جنگ و همکاران در سـال ۲۰۱۵ اشـاره کرد [۸]. جنگ و همکاران در این پژوهش پروتکل با نام EDTM معرفی و ارائه نمودند. EDTM در وهله اول تشـخیص نفوذ را بر پایه تعاملات مسـتقیم گسـترش داده و محاسـبات مربوط به نحوه عملکرد حسـگرها را بر اسـاس نظارت‌های مسـتقیم توسعه می‌دهد. در ادامه این محاسبات با عقاید گره‌های دیگر (توصـیه‌ها) به جهت تشـخیص نهایی ترکیب می‌گردد. همچنین در EDTM از تمایز بسته‌های کنترلی و داده، و میزان کارایی حسـگر در تعاملات نیز به جهت تصـمیم‌گیری‌ها اسـتفاده گردیده اسـت. معماری کلی پروتکل EDTM در شکل (۵) نمایش و ارائه گردیده است.



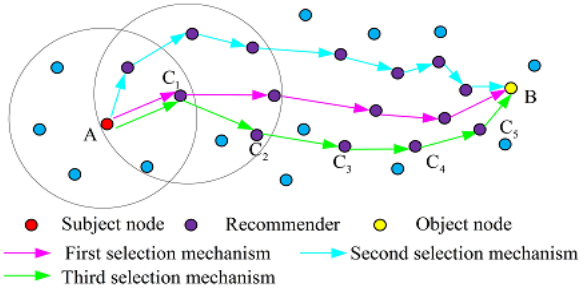
شکل ۵ - معماری کلی پروتکل EDTM [۸]

نحوه تشـخیص نفوذ بر محوریت مشاهدات مستقیم و عقاید حسگرهای دیگر در پروتکل EDTM در شکل (۶) نمایش و ارائه گردیده است. در این شکل چگونگی محاسبات تشخیص محلی نمایش داده شده است.



شکل ٦ - تشخیص نفوذ مبتنی بر ارزیابی‌های محلی EDTM [۸]

همچنین به جهت اسـتفاده از عقاید سـایرین در ارتباط با مسـیرهای تعاملات از اشـتراک‌گذاری توصیه‌های گره‌های فعال در مسـیر بهره برده شـده اسـت. این پروسـه با هدف افزایش دقت تشخیص نفوذ مرتبط با مسیرهای فعال و تعاملات گره‌های میانی آن صورت می‌پذیرد. شکل (۸) نمایی از این اشتراک‌گذاری را نمایش می‌دهد.



شکل ۸ - سنجش اعتبار مسیرهای فعال در پروتکل EDTM [۸]

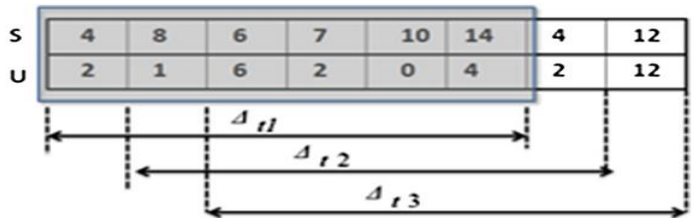
از چالش‌های مرتبط با EDTM می‌توان به آسـیب‌پذیری پروتکل در برابر گره‌های نفوذی با قصـد فریب سـیسـتم، کاهش سرعت پروتکل به صورت نمایی با افزایش تعداد گره‌ها، و تأخیر بالای تعاملات در این پروتکل را اشاره نمود.

از جمله پژوهش‌های مهم دیگری که در حوزه بهبود تشـخیص نفوذ در شـبکه‌های حسـگر بی‌سـیم ارائه و معرفی گردیده می‌توان به پژوهش دیگر سـنگ و همکاران در سـال ۲۰۱۵ اشـاره کرد [۹]. سنگ و همکاران در این پژوهش پروتکل با نام DT-WSN-BM ارائه نمودند. تشـخیص نفوذ در این DT-WSN-BM به صـورت پویا و بر اساس معیارهای متعددی مبتنی بر عملکرد حسـگرها در بسـتر شبکه صورت می‌پذیرد. پروتکل ارائه شده در این پژوهش به منظور تشخیص نفوذ یک روش دو مرحله‌ای مبتنی بر نظارت مسـتقیم و غیرمسـتقیم ارائه می‌نماید. در گام ابتدایی تشـخیص نفوذ بر محوریت تعاملات مستقیم حسگر ارزیاب با حسگر مورد ارزیابی محاسبه و منظور می‌گردد که نتیجه‌ای از عملکرد حسگر مورد ارزیابی حاصل خواهد آمد. در گام دوم از DT-WSN-BM از نظارت غیرمسـتقیم به منظور ارزیابی‌های اعتماد عمومی اسـتفاده می‌نماید که تلاش بر آن

بوده تا این نظارت با اطمینان از توصیه‌های دریافتی محاسبه و ملاحظه گردد. در نهایت تشخیص صورت پذیرفته به واسطه دو عامل اشاره شده با یکدیگر ترکیب و مقدار نهایی اعتبار هر گره مشخص می‌گردد. این ارزیابی‌ها در تعاملات مختلف به صورت پویا محاسبه و منظور می‌گردد. در انتها پروتکل ارائه شده تحت شبیه‌ساز ns2 مورد ارزیابی و آزمایش قرار گرفته تا میعارهای تأثیرپذیر تحلیل و نتایج مورد مقایسه قرار گیرد. از چالش‌های مرتبط با DT-WSN-BM می‌توان به عدم ارزیابی مطلوب با توجه به تاریخچه گذشته حسگرها، فریب سیستم در مقابله با حملات نفوذی‌ها، و عدم پاسخ‌گویی در شرایط مختلف شبکه را اشاره نمود.

از جمله پژوهش‌های مهم دیگری که در حوزه بهبود تشخیص نفوذ در شبکه‌های حسگر بی‌سیم ارائه و معرفی گردیده می‌توان به پژوهش دیگر لابروی و همکاران در سال ۲۰۱۵ اشاره کرد [۱۰]. لبری و همکاران در این پژوهش پروتکل با نام RARTrust معرفی و ارائه نمودند. RARTrust به آسیب‌پذیری‌های مدل‌های سنتی تشخیص نفوذ اشاره نموده و به‌طور تخصصی‌تر به آسیب‌پذیری این مدل‌ها در برابر حملات تغییر در بسته پرداخته شده است. به طوری‌که چارچوب RARTrust مبتنی بر عملکرد سیستم تشخیص نفوذ توسعه یافته، و تلاش بر استفاده از ترکیب شاخصی تحت عنوان اعتبار کوتاه مدت با ارزیابی اعتبار سنتی در راستای بهبود تشخیص نفوذ بوده است. در انتها مقدار حاصل از ارزیابی‌های مستقیم با تبادلات توصیه‌های حسگرهای تک‌گامی ترکیب و به جهت تشخیص نفوذ حاصل می‌گردد. شکل (۸) نمایی از عملکرد RARTrust را نمایش می‌دهد. همچنین نحوه محاسبه اعتبار کوتاه مدت و چگونگی ترکیب آن با اعتبار تاریخچه در شکل (۹) ارائه و نمایش داده شده است. این نحوه محاسبات تشخیص نفوذ به ارزیابی عملکرد حسگر در بازه‌های زمانی متفاوت با توجه به ارزش بازه زمانی اشاره مینماید. از چالش‌های مرتبط با RARTrust می‌توان به عدم مقابله در برابر گره‌های نفوذی، و سربارهای ناشی از اشتراک‌گذاری توصیه‌ها اشاره نمود.

شکل ۸ – تشخیص نفوذ مبتنی بر اجزای RARTrust [۱۰]



شکل ۹ – محاسبه اعتبار کوتاه مدت و ترکیب آن با اعتبار تاریخچه در RARTrust [۱۰]

از جمله پژوهش‌های مهم دیگری که در حوزه بهبود تشخیص نفوذ در شبکه‌های حسگر بی‌سیم ارائه و معرفی گردیده می‌توان به پژوهش دیگر ادنن و همکاران در سال ۲۰۱۵ اشاره کرد [۱۱]. ادنن و همکاران در این پژوهش پروتکل با نام TB-AODV معرفی نمودند. پروتکل معرفی شده در این پژوهش مبتنی بر نظارت‌های مستقیم و غیرمستقیم بر محوریت توالی رفتارهای خوب و بد گره‌ها، صحت در انجام تعاملات و دنباله‌ای از خوش‌رفتاری گره‌ها توسعه یافته است. در این پروتکل به نسبت تعاملات مثبت و منفی گره‌ها تشخص نفوذ اعمال گردیده و در صورت خوش‌رفتاری، گره خیرخواه با افزایش اعتبار تشویق و در صورت بروز رفتارهای منفی گره مخرب با کاهش اعتبار و حذف از شبکه تنبیه خواهد گردید. شاخص‌های رفتارهای منفی مورد ارزیابی در این پژوهش شامل، حذف بسته، تغییرات در بسته، جعل و فریب فرایند مسیریابی می‌باشند. در

این پژوهش از ارزش‌گذاری متغیر به مشاهدات مستقیم و غیرمستقیم به جهت افزایش دقت در محاسبات تشخیص نفوذ استفاده گردیده و نتیجه ارزیابی‌ها در جدول مسیریابی گره‌ها به عنوان درجه اعتبار گره‌های همسایه به جهت تصمیم‌گیری‌های بعدی ذخیره خواهد گردید. از چالش‌های مرتبط با این پژوهش می‌توان به عدم مقابله در برابر گره‌های نفوذی و ضریب بالای اشتباه در تصمیم‌گیری‌ها، را اشاره نمود.

از جمله پژوهش‌های مهم دیگری که در حوزه بهبود تشخیص نفوذ در شبکه‌های حسگر بی‌سیم ارائه و معرفی گردیده می‌توان به پژوهش دیگر اندرسن و همکاران در سال ۲۰۱۵ اشاره کرد [۱۲]. اندرسن و همکاران در این پژوهش پروتکل با نام MC-Trust معرفی گردیده است. پروتکل ارائه شده در این پژوهش بر مبنای سه شاخص امنیتی تشخیص نفوذ را اعمال می‌نماید. این سه شاخص عبارتند از کارایی گره، یکپارچگی در انجام توالی رفتار مثبت و نوع رفتار. به‌طوری که عامل کارایی گره به کارایی و میزان انرژی باقمانده گره اشاره می‌نماید، عامل یکپارچگی به نرخ یکپارچگی در توالی رفتار مثبت و منفی گره‌ها اشاره نموده و نوع رفتار به چگونگی عملکرد گره مورد ارزیابی بر مبنای نظارت‌های مستقیم اشاره دارد. در زمانی که فرایند مسیریابی صورت می‌پذیرد، هر گره شاخص‌های سه گانه را در مورد گره‌های همسایه‌ها بر پایه نظارت مستقیم و غیرمستقیم بررسی نموده و با توجه به بررسی‌های انجام شده تصمیم‌گیری می‌نماید که داده را از طریق همسایه مورد نظر ارسال گردد یا خیر. اگر عامل یکپارچگی یک گره پایین باشد ممکن است حمله در راه بوده و مسیریابی حدالامکان از طریق این گره نباید انجام گردد. اگر عامل یکپارگی برای یک گره میانگین یا متوسط باشد، در این صورت در رابطه با گره مورد نظر از دیگر همسایه‌ها توصیه دریافت شده و گره از روند مسیریابی کنار گذاشته نخواهد شد، بلکه مجدداً به صورت فعالانه گره مورد نظر در فرایند مسیریابی شرکت نموده تا مجدداً رفتارش آنالیز و بررسی گردد. شاخص نوع رفتار شاخصی است که به عملکرد گره در تعاملات اشاره می‌نماید. بر اساس سه شاخص ذکر شده معیار انتخاب گره بعدی انجام گرفته و مسیریابی بر این اساس ادامه می‌یابد. از چالش‌های مرتبط با این پژوهش می‌توان به افت کارایی روش در مقابله با حملات نفوذی‌ها و عدم کشف همه گره‌های مخرب را در تعاملات میان گره‌ها و آسیب‌پذیری در ارتباط با حملات توصیه‌ها را عنوان نمود.

۳- نتیجه‌گیری

این پژوهش دلالت بر این دارد که شبکه‌های حسگر بی‌سیم شبکه‌ای بسیار آسیب‌پذیر در پشتیبانی از امنیت و مقابله با آسیب‌های امنیتی می‌باشند. در ادامه و در پی بررسی عرصه‌های کاربردی شبکه‌های حسگر، مشخص گردید که کاربردهای حساس و مهم این دسته از شبکه‌ها در زمینه‌های نظامی، صنعتی، و غیره، حاکی از انگیزه بالا اعمال حملات مختلف به شبکه، با هدف اختلال در روند عملیاتی شبکه است. در واقع بخش بزرگی از کاربردهای شبکه‌های حسگر را کاربردهای حساس و کلیدی نظامی، هسته‌ای، تجاری و اقتصادی تشکیل می‌دهد که این کاربردها به شدت مستعد اعمال حملات مختلف با اهداف مختلف هستند. ازاین‌رو امنیت و پیاده‌سازی آن با توجه به آسیب‌پذیری شبکه و بنابر کاربردهای مهم شبکه، یکی از ارکان اساسی و اجتناب‌ناپذیر این دسته از شبکه‌ها به شمار می‌رود. اما با توجه به بررسی‌های انجام شده، زمانی راه‌کارهای امنیتی و پیاده‌سازی امنیت کارآمد و مؤثر خواهند بود که متناسب با خصوصیات و ماهیت محدود شبکه‌های حسگر توسعه و گسترش یابند.

۴- مراجع

[1]. Muneebahmdhyiddeen, M., Mohan, R., Anupama, B. L., & Nair, A. V. (2016). Recent Survey on Security in Wireless Sensor Network. *Wireless Communication*, *8*(7), 270-273.

[2]. Shabana, K., Fida, N., Khan, F., Jan, S. R., & Rehman, M. U. (2016). Security issues and attacks in Wireless Sensor Networks. *International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE)*, *5*(7), pp-81.

[3]. Ahmed, A., Bakar, K. A., Channa, M. I., Haseeb, K., & Khan, A. W. (2016). A trust aware routing protocol for energy constrained wireless sensor network. *Telecommunication Systems*, *61*(1), 123-140.

[4]. Ahmed, A., Bakar, K. A., Channa, M. I., & Khan, A. W. (2016). A secure routing protocol with trust and energy awareness for wireless sensor network. Mobile Networks and Applications, 21(2), 272-285.
[5]. Ahmed, A., Bakar, K. A., Channa, M. I., Khan, A. W., & Haseeb, K. (2017). Energy-aware and secure routing with trust for disaster response wireless sensor network. Peer-to-Peer Networking and Applications, 10(1), 216-237.
[6]. Fang, W., Zhang, C., Shi, Z., Zhao, Q., & Shan, L. (2016). BTRES: Beta-based Trust and Reputation Evaluation System for wireless sensor networks. Journal of Network and Computer Applications, 59, 88-94.
[7]. Xia, H., Yu, J., Tian, C. L., Pan, Z. K., & Sha, E. (2016). Light-weight trust-enhanced on-demand multi-path routing in mobile ad hoc networks. Journal of Network and Computer Applications, 62, 112-127.
[8]. Jiang, J., Han, G., Wang, F., Shu, L., & Guizani, M. (2015). An efficient distributed trust model for wireless sensor networks. IEEE Transactions on Parallel & Distributed Systems, (1), 1-1.
[9]. Song, J., Li, X., Hu, J., Xu, G., & Feng, Z. (2015, August). Dynamic trust evaluation of wireless sensor networks based on multi-factor. In Trustcom/BigDataSE/ISPA, 2015 IEEE (Vol. 1, pp. 33-40). IEEE.
[10]. Labraoui, N., Gueroui, M., & Sekhri, L. (2016). A risk-aware reputation-based trust management in wireless sensor networks. Wireless Personal Communications, 87(3), 1037-1055.
[11]. Ahmed, A., Bakar, K. A., Channa, M. I., & Haseeb, K. (2015). Countering Node Misbehavior Attacks Using Trust Based Secure Routing Protocol. TELKOMNIKA (Telecommunication Computing Electronics and Control), 13(1), 260-268.
[12]. Anderson, G., & Dorsey, D. J. (2015, May). Ternary trust metric for mobile ad-hoc networks. In Computational Intelligence for Security and Defense Applications (CISDA), 2015 IEEE Symposium on (pp. 1-9). IEEE.