

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



دانشگاه گیلان

دانشکده‌ی پردیس بین‌الملل (انزلی)

پایان‌نامه‌ی کارشناسی ارشد

در رشته‌ی مهندسی فناوری اطلاعات – گرایش تجارت الکترونیک

طراحی سطح بالای یک سیستم تشخیص نفوذ مبتنی بر عامل و سیاست،

با قابلیت پیکربندی مجدد دینامیک برای شبکه‌های حسگر بی‌سیم

از

حسین جدیدالاسلامی

استاد راهنما

دکتر شهریار محمدی

خرداد ۱۳۹۰

**دانشکده‌ی پردیس بین‌الملل (انزلی)**

**گروه مهندسی فناوری اطلاعات**

**گرایش تجارت الکترونیک**

**طراحی سطح بالای یک سیستم تشخیص نفوذ مبتنی بر عامل و سیاست،**

**با قابلیت پیکربندی مجدد دینامیک برای شبکه‌های حسگر بی‌سیم**

**از**

**حسین جدیدالاسلامی**

**استاد راهنما**

**دکتر شهریار محمدی**

**استاد مشاور**

**دکتر رضا ابراهیمی آتانی**

**خرداد ۱۳۹۰**

تقدیم به:

# یوسف گمگشته‌ی زهرا (عج)

**تشکر و قدردانی:**

**با سپاس فراوان از زحمات بی‌دریغ اساتید گرامی  
دکتر شهریار محمدی و دکتر رضا ابراهیمی آتانی،  
که اینجانب را در انجام این پژوهش یاری نموده‌اند.**

# فهرست مطالب

## فصل ۱: کلیات تحقیق ..... ۱

۱-۱- مقدمه	۲
۲-۱- تعریف موضوع	۴
۳-۱- کارهای پیشین	۵
۴-۱- روش تحقیق	۷
۵-۱- اهداف تحقیق	۸
۶-۱- ساختار پایان نامه	۱۰

## فصل ۲: شبکه‌ی حسگر بی‌سیم (WSN) ..... ۱۱

۱-۲- مقدمه	۱۲
۲-۲- شبکه‌های حسگر بی‌سیم (تعریف)	۱۲
۳-۲- ویژگی‌های شبکه‌های حسگر بی‌سیم	۱۳
۴-۲- ساختمان نود حسگر	۱۴
۵-۲- مؤلفه‌های نرم‌افزاری شبکه‌های حسگر بی‌سیم	۱۹
۱-۵-۲- سیستم عامل Tiny OS	۲۰
۶-۲- پشته‌ی پروتکلی شبکه‌ی حسگر بی‌سیم	۲۰
۷-۲- انواع معماری‌های ارتباطی شبکه‌های حسگر بی‌سیم	۲۱
۸-۲- عوامل مؤثر در طراحی شبکه‌های حسگر بی‌سیم	۲۳
۹-۲- کاربردهای شبکه‌های حسگر بی‌سیم	۲۴
۱۰-۲- آسیب‌پذیری‌های شبکه‌های حسگر بی‌سیم	۲۸
۱۱-۲- چالش‌های شبکه‌های حسگر بی‌سیم	۲۸
۱۲-۲- مسیریابی در شبکه‌های حسگر بی‌سیم	۳۱
۱-۱۲-۲- پارامترهای مؤثر در طراحی پروتکل‌های مسیریابی در شبکه‌های حسگر بی‌سیم	۳۲

۲۵	.....	۲-۱۲-۲. انواع پروتکل‌های مسیریابی شبکه‌های حسگر بی‌سیم
۳۷	.....	۳-۱۲-۲. پروتکل‌های مسیریابی سلسله‌مراتبی (مبتنی بر خوشه‌بندی)
۳۷	.....	۴-۱۲-۲. پروتکل مسیریابی LEACH
۳۹	.....	۵-۱۲-۲. جزییات پروتکل مسیریابی LEACH
۴۱	.....	۶-۱۲-۲. مشخصات پروتکل مسیریابی LEACH

## ۴۲ ..... فصل ۳: امنیت در شبکه‌های حسگر بی‌سیم

۴۳	.....	۱-۳- مقدمه
۴۳	.....	۲-۳- لزوم امنیت در شبکه‌های حسگر بی‌سیم (چرا امنیت در WSNها)
۴۴	.....	۳-۳- مباحث امنیتی مطرح در شبکه‌های حسگر بی‌سیم
۴۴	.....	۴-۳- سرویس‌های امنیتی شبکه‌های حسگر بی‌سیم
۴۵	.....	۵-۳- مدل تهدید در شبکه‌های حسگر بی‌سیم
۴۹	.....	۶-۳- موانع امنیتی شبکه‌های حسگر بی‌سیم
۵۱	.....	۷-۳- نیازمندی‌های امنیتی شبکه‌های حسگر بی‌سیم
۵۲	.....	۱-۷-۳. نیازمندی‌های امنیتی نوعی شبکه‌های حسگر بی‌سیم
۵۳	.....	۲-۷-۳. نیازمندی‌های امنیتی منحصر بفرد شبکه‌های حسگر بی‌سیم
۵۶	.....	۸-۳- بررسی و مقایسه‌ی انواع حملات مطرح در شبکه‌های حسگر بی‌سیم
۵۸	.....	۱-۸-۳. حملات، اهداف و روش‌های آن‌ها
۶۲	.....	۲-۸-۳. دسته‌بندی حملات بر اساس مدل تهدید در شبکه‌های حسگر بی‌سیم
۶۵	.....	۳-۸-۳. حملات، روش‌های تشخیص و اقدامات متقابل در شبکه‌های حسگر بی‌سیم

## ۷۰ ..... فصل ۴: سیستم تشخیص نفوذ (IDS)

۷۱	.....	۱-۴- مقدمه
۷۱	.....	۲-۴- مفهوم نفوذ
۷۲	.....	۳-۴- سیستم تشخیص نفوذ (تعریف)
۷۳	.....	۴-۴- دسته‌بندی IDSها بر اساس معماری

۷۳	سیستم تشخیص نفوذ مبتنی بر میزبان	۱-۴-۴
۷۴	سیستم تشخیص نفوذ مبتنی بر شبکه	۲-۴-۴
۷۴	سیستم تشخیص نفوذ ترکیبی (توزیع شده)	۳-۴-۴
۷۵	دسته بندی IDSها بر اساس روش تشخیص (مکانیزم های ممیزی یا روش های تشخیص نفوذ)	۵-۴
۷۵	سیستم تشخیص نفوذ مبتنی بر رفتار غیرعادی	۱-۵-۴
۷۶	سیستم تشخیص نفوذ مبتنی بر الگویا تشخیص سوءاستفاده	۲-۵-۴
۷۷	دسته بندی IDSها بر اساس روش های تصمیم گیری	۶-۴
۷۷	دسته بندی IDSها بر اساس نحوه ی پاسخ/واکنش	۷-۴
۷۸	بررسی نقاط ضعف و آسیب پذیری های سیستم های تشخیص نفوذ	۸-۴
۷۹	راهکارهای رایج فرار از IDS	۱-۸-۴
۸۱	دسته بندی و تفکیک نقاط ضعف و آسیب پذیری های IDSها بر اساس معماری آنها	۲-۸-۴
۸۵	دسته بندی و تفکیک نقاط ضعف و آسیب پذیری های IDSها بر اساس مراحل انجام نفوذ	۳-۸-۴
۸۷	دسته بندی آسیب پذیری های IDSها بر اساس بلوک دیاگرام ساختار خود IDS	۴-۸-۴
۸۹	دسته بندی نقاط ضعف IDSها بر اساس لایه های مختلف شبکه ای در مدل TCP/IP	۵-۸-۴
۹۳	نیازمندی های عمومی سیستم تشخیص نفوذ	۹-۴
۹۳	نیازمندی های پردازشی	۱-۹-۴
۹۵	نیازمندی های عملیاتی	۲-۹-۴
۱۰۵	نیازمندی های خروجی	۳-۹-۴
۱۰۶	نیازمندی های فنی	۴-۹-۴
۱۰۸	سایر نیازمندی ها	۵-۹-۴
۱۰-۴	معرفی چند نمونه سیستم تشخیص نفوذ (بررسی و مقایسه ی ۲ سیستم تشخیص نفوذ نرم افزاری SNORT و OSSEC)	
۱۱۳		
۱۱۴	بررسی سیستم تشخیص نفوذ SNORT	۱۱-۴
۱۱۵	مشخصات عمده و متریک های SNORT	۱-۱۱-۴
۱۱۶	مدهای عملیاتی SNORT	۲-۱۱-۴
۱۲۱	طراحی SNORT (اجزاء و مشخصات)	۳-۱۱-۴



۱۲۲	.....	۴-۱۱-۴ معماری SNORT (اجزای داخلی و جریان داده‌ها)
۱۲۷	.....	۵-۱۱-۴ سیستم تشخیص نفوذ SNORT 3.0 (مشخصات و معماری)
۱۳۰	.....	۶-۱۱-۴ کاربردهای SNORT
۱۳۰	.....	۷-۱۱-۴ پلاگین‌های SNORT
۱۳۱	.....	۸-۱۱-۴ قوانین SNORT
۱۳۷	.....	۹-۱۱-۴ تحلیل‌گران SNORT
۱۳۹	.....	۱۰-۱۱-۴ SNORT و ساختار شبکه (محل استقرار SNORT در معماری شبکه)
۱۳۹	.....	۱۱-۱۱-۴ فرآیند نصب SNORT
۱۴۱	.....	۱۲-۱۱-۴ چالش‌های عمده‌ی SNORT
۱۴۲	.....	۱۲-۴ - بررسی سیستم تشخیص نفوذ OSSEC
۱۴۳	.....	۱-۱۲-۴ مدهای عملیاتی OSSEC
۱۴۴	.....	۲-۱۲-۴ مزایای کلیدی OSSEC
۱۴۵	.....	۳-۱۲-۴ مشخصه‌های اصلی OSSEC
۱۴۸	.....	۴-۱۲-۴ معماری OSSEC و اجزای داخلی آن

## **فصل ۵: تشخیص نفوذ در شبکه‌های حسگر بی‌سیم: ارائه و تشریح معماری‌های**

### **پیشنهادی شامل معماری تشخیص نفوذ (۲ سطحی) و طراحی مؤلفه-محور**

### **سیستم‌های تشخیص نفوذ پیشنهادی (CIDS و WSNIDS) برای شبکه‌های حسگر**

<b>۱۵۱</b>	<b>.....</b>	<b>بی‌سیم</b>
۱۵۲	.....	۱-۵ - مقدمه
۱۵۲	.....	۲-۵ - بررسی معماری پایه‌ی IDS در شبکه‌های حسگر بی‌سیم
۱۵۳	.....	۱-۲-۵ معماری IDS پیشنهادی
۱۵۴	.....	۲-۲-۵ روش تشخیص نفوذ IDS پیشنهادی
۱۵۶	.....	۳-۲-۵ روش تصمیم‌گیری IDS پیشنهادی
۱۵۸	.....	۴-۲-۵ روش پاسخ IDS پیشنهادی

- ۱۵۸ ..... چالش‌های عمده در طراحی سیستم تشخیص نفوذ برای شبکه‌های حسگر بی‌سیم ..... ۳-۵
- ۱۵۹ ..... نیازمندی‌های خاص سیستم تشخیص نفوذ در شبکه‌های حسگر بی‌سیم ..... ۴-۵
- ۱۶۱ ..... تشریح معماری تشخیص نفوذ پیشنهادی (۲ سطحی) ..... ۵-۵
- ۱۶۲ ..... سطح پایین: سیستم تشخیص نفوذ مبتنی بر خوشه (CIDS) ..... ۱-۵-۵
- ۱۶۷ ..... سطح بالا: سیستم تشخیص نفوذ مبتنی بر سطح کل شبکه‌ی حسگر بی‌سیم (WSNIDS) ..... ۲-۵-۵
- ۱۶۸ ..... تشریح روش کار مدل پیشنهادی ..... ۶-۵
- ۱۷۰ ..... رویکردهای تشخیص نفوذ در شبکه‌های حسگر بی‌سیم (سیستم مبتنی بر عامل و سیاست) ..... ۷-۵
- ۱۷۱ ..... روش تشخیص نفوذ مبتنی بر عامل: تعیین و طراحی عامل‌ها و مؤلفه‌ها ..... ۸-۵
- ۱۷۳ ..... عامل‌های فاز اول تشخیص نفوذ: گردآوری داده‌ها و پیش‌پردازش ..... ۱-۸-۵
- ۱۷۶ ..... عامل‌های فاز دوم تشخیص نفوذ: پردازش و تحلیل ..... ۲-۸-۵
- ۱۷۹ ..... عامل‌های فاز سوم تشخیص نفوذ: تصمیم‌گیری ..... ۳-۸-۵
- ۱۸۳ ..... عامل‌های فاز چهارم تشخیص نفوذ: ثبت و ردیابی ..... ۴-۸-۵
- ۱۸۴ ..... عامل‌های فاز پنجم تشخیص نفوذ: منابع اطلاعاتی ..... ۵-۸-۵
- ۱۸۶ ..... اعمال و فعالیت‌های مشترک عامل‌های CIDS و WSNIDS ..... ۶-۸-۵
- ۱۸۷ ..... روش تشخیص نفوذ مبتنی بر سیاست (تعریف الگو و قواعد) ..... ۹-۵
- ۱۸۹ ..... رویداد (Event) ..... ۱-۹-۵
- ۱۹۰ ..... شرایط (Conditions) ..... ۲-۹-۵
- ۱۹۰ ..... اقدامات (Actions) ..... ۳-۹-۵
- ۱۹۱ ..... قالب‌بندی قواعد ..... ۴-۹-۵
- ۱۹۲ ..... الگو و ساختار سیاست‌ها/قواعد ..... ۵-۹-۵
- ۱۹۳ ..... مراحل اتخاذ سیاست توسط سیستم تشخیص نفوذ ..... ۶-۹-۵
- ۱۹۳ ..... قواعد کشف حملات ..... ۷-۹-۵
- ۱۹۵ ..... مثال‌هایی از کاربرد قواعد کشف حملات ..... ۸-۹-۵
- ۱۹۶ ..... خصوصیات عمده‌ی منابع اطلاعاتی (پایگاه قواعد) ..... ۹-۹-۵
- ۱۹۷ ..... الگوریتم پیشنهادی استفاده شده در WSNIDS ..... ۱۰-۵
- ۱۹۸ ..... خصوصیات عمده‌ی معماری‌های پیشنهادی ..... ۱۱-۵

## فصل ۶: تحلیل و ارزیابی مدل پیشنهادی (نتایج حاصل از پرسشنامه) ..... ۲۰۲

۲۰۳	.....	مقدمه	۱-۶
۲۰۳	.....	بخش اول: دید کلی (سؤالات عمومی)	۲-۶
۲۰۴	.....	بخش دوم: جزئیات (سؤالات مربوط به خصوصیات عملکردی و غیرعملکردی)	۳-۶
۲۰۵	.....	دسته ۱: نیازمندی‌های پیش‌پردازش، پردازش، ارزیابی و مدیریتی	۱-۳-۶
۲۰۶	.....	دسته ۲: نیازمندی‌های عملیاتی (Operational)	۲-۳-۶
۲۰۷	.....	دسته ۳: سوم: نیازمندی‌های خروجی	۳-۳-۶
۲۰۷	.....	دسته ۴: چهارم: نیازمندی‌های فنی	۴-۳-۶
۲۰۸	.....	دسته ۵: پنجم: نیازمندی‌های متفرقه	۵-۳-۶
۲۰۹	.....	بخش سوم: نیازمندی‌های خاص سیستم‌های پیشنهادی در شبکه‌های حسگر بی‌سیم	۴-۶

## فصل ۷: نتایج (خلاصه و نتیجه‌گیری) ..... ۲۱۲

۲۱۳	.....	نتایج حاصل در حوزه‌ی شبکه‌های حسگر بی‌سیم و امنیت در این شبکه‌ها	۱-۷
۲۱۶	.....	نتایج حاصل در حوزه‌ی سیستم‌های تشخیص نفوذ	۲-۷
۲۱۷	.....	نتایج حاصل از تحلیل و ارزیابی پرسشنامه	۳-۷
۲۱۸	.....	نتیجه‌گیری نهایی: حوزه‌ی تشخیص نفوذ در شبکه‌های حسگر بی‌سیم و معماری‌های پیشنهادی	۴-۷
۲۲۱	.....	کارهای آتی	۵-۷

## منابع و مراجع ..... ۲۲۳

## فهرست جدول‌ها

جدول ۱-۱: برنامه‌ی زمانبندی پایان‌نامه

جدول ۱-۲: نمای کلی از ابعاد مختلف شبکه‌های حسگر بی‌سیم

جدول ۱-۳: مدل تهدید در شبکه‌های حسگر بی‌سیم

جدول ۲-۳: لایه‌های مختلف شبکه‌های حسگر بی‌سیم و حملات متناظر با آن‌ها

جدول ۳-۳: مقایسه‌ی انواع حملات شبکه‌های حسگر بی‌سیم بر اساس روش‌ها و اهداف آن‌ها

جدول ۴-۳: دسته‌بندی و مقایسه‌ی حملات شبکه‌های حسگر بی‌سیم بر اساس مدل تهدید شبکه‌های حسگر بی‌سیم

جدول ۵-۳: دسته‌بندی حملات در شبکه‌های حسگر بی‌سیم بر اساس متدهای تشخیص و دفاع در برابر آن‌ها (اقدامات متقابل

امنیتی)

جدول ۱-۴: مقایسه‌ی انواع سیستم‌های تشخیص نفوذ بر اساس معماری

جدول ۱-۶: آمار خصایص مربوط به نیازمندی‌های پیش‌پردازی، پردازشی، ارزیابی و مدیریتی سیستم پیشنهادی

جدول ۲-۶: آمار خصایص مربوط به نیازمندی‌های عملیاتی سیستم پیشنهادی

جدول ۳-۶: آمار خصایص مربوط به نیازمندی‌های خروجی سیستم پیشنهادی

جدول ۴-۶: آمار خصایص مربوط به نیازمندی‌های فنی سیستم پیشنهادی

جدول ۵-۶: آمار خصایص مربوط به نیازمندی‌های متفرقه سیستم پیشنهادی

جدول ۶-۶: آمار خصایص مربوط به نیازمندی‌های خاص و منحصر بفردهای سیستم تشخیص نفوذ پیشنهادی برای شبکه‌های

حسگر بی‌سیم

جدول ۱-۷: درصد رخداد هر یک از خصایص در دسته‌بندی‌های مختلف حملات امنیتی شبکه‌های حسگر بی‌سیم

جدول ۲-۷: مقایسه‌ی سیستم‌های تشخیص نفوذ OSSEC و SNORT

جدول ۳-۷: آمار مجموع متوسط خصوصیات مربوط به دسته نیازمندی‌های مختلف سیستم تشخیص نفوذ پیشنهادی برای

شبکه‌های حسگر بی‌سیم

## فهرست شکل‌ها

- شکل ۱-۱: معماری ارتباطی شبکه‌های حسگر بی‌سیم
- شکل ۱-۲: ساختمان و اجزای داخلی نود حسگر
- شکل ۲-۲: پشته‌ی پروتکلی شبکه‌های حسگر بی‌سیم
- شکل ۳-۲: انواع معماری‌های شبکه‌های حسگر بی‌سیم
- شکل ۴-۲: کاربردهای شبکه‌های حسگر بی‌سیم
- شکل ۵-۲: پروتکل‌های مسیریابی در شبکه‌های حسگر بی‌سیم
- شکل ۶-۲: پروتکل مسیریابی سلسله‌مراتبی LEACH
- شکل ۱-۳: ابعاد مختلف امنیت در شبکه‌های حسگر بی‌سیم
- شکل ۲-۳: درصد رخداد حملات در لایه‌های مختلف شبکه‌های حسگر بی‌سیم
- شکل ۳-۳: مقایسه‌ی حملات شبکه‌های حسگر بی‌سیم مبتنی بر ماهیت حملات
- شکل ۴-۳: مقایسه‌ی حملات شبکه‌های حسگر بی‌سیم مبتنی بر بعد امنیتی تهدید شده
- شکل ۵-۳: مقایسه‌ی حملات شبکه‌های حسگر بی‌سیم بر اساس مدل تهدید در این شبکه‌ها
- شکل ۱-۴: طبقه‌بندی سیستم تشخیص نفوذ بر اساس معماری
- شکل ۲-۴: دسته‌بندی‌های مختلف سیستم‌های تشخیص نفوذ
- شکل ۳-۴: ارتباطات مؤلفه‌های مدل CIDF
- شکل ۴-۴: نیازمندی‌های عام سیستم‌های تشخیص نفوذ
- شکل ۵-۴: معماری سیستم تشخیص نفوذ SNORT
- شکل ۶-۴: جریان داده‌ها بین مؤلفه‌های سیستم تشخیص نفوذ SNORT
- شکل ۷-۴: فاز اول: جریان بسته‌های داده‌ای شبکه در Sniffer (SNORT IDS)
- شکل ۸-۴: فاز دوم: جریان بسته‌های داده‌ای شبکه در پلاگین‌های پیش پردازنده (SNORT IDS)
- شکل ۹-۴: فاز سوم: جریان داده‌ها در موتور تشخیص و پلاگین‌های آن (SNORT IDS)
- شکل ۱۰-۴: فاز چهارم: مؤلفه Alert/Logging (اطلاع رسانی به مدیر امنیتی IDS از طریق کنسول مدیریت SNMP)
- شکل ۱۱-۴: معماری پیشنهادی برای SNORT 3.0
- شکل ۱۲-۴: نحوه‌ی عملکرد سیستم تشخیص نفوذ OSSEC

شکل ۴-۱۳: معماری سیستم تشخیص نفوذ OSSEC، حالت Local (Stand alone)

شکل ۴-۱۴: معماری سیستم تشخیص نفوذ OSSEC، حالت Server-Agent

شکل ۵-۱: مشخصات پایه‌ی مدل سیستم تشخیص نفوذ پیشنهادی

شکل ۵-۲: معماری تشخیص نفوذ پیشنهادی برای شبکه‌های حسگر بی‌سیم

شکل ۵-۳: معماری سیستم تشخیص نفوذ مبتنی بر خوشه (CIDS)

شکل ۵-۴: معماری سیستم تشخیص نفوذ مبتنی بر سطح کل شبکه‌ی حسگر بی‌سیم (WSNIDS)

شکل ۵-۵: جریان داده‌ها در سیستم تشخیص نفوذ پیشنهادی (فرآیند تشخیص نفوذ)

شکل ۵-۶: مراحل اصلی تشخیص نفوذ در سیستم تشخیص نفوذ پیشنهادی (WSNIDS)

شکل ۵-۷: فاز اول فرآیند تشخیص نفوذ در سیستم تشخیص نفوذ پیشنهادی (WSNIDS): گردآوری و پیش‌پردازش

شکل ۵-۸: فاز دوم فرآیند تشخیص نفوذ در سیستم تشخیص نفوذ پیشنهادی (WSNIDS): تحلیل و تشخیص نفوذ

شکل ۵-۹: فاز سوم فرآیند تشخیص نفوذ در سیستم تشخیص نفوذ پیشنهادی (WSNIDS): تصمیم‌گیری نهایی

شکل ۵-۱۰: فاز چهارم فرآیند تشخیص نفوذ در سیستم تشخیص نفوذ پیشنهادی (WSNIDS): ثبت و ردیابی

شکل ۵-۱۱: انواع منابع اطلاعاتی (Info-bases) موجود در سیستم تشخیص نفوذ پیشنهادی

شکل ۷-۱: مهم‌ترین و مؤثرترین خصیصه‌های حملات امنیتی در شبکه‌های حسگر بی‌سیم

شکل ۷-۲: نتایج حاصل از تحلیل و ارزیابی پرسشنامه مربوط به سیستم پیشنهادی

### طراحی سطح بالای یک سیستم تشخیص نفوذ مبتنی بر عامل و سیاست، با قابلیت پیگردینی مجدد دینامیک برای

شبکه‌های حسگر بی‌سیم

حسین جدیدالاسلامی

شبکه‌های حسگر بی‌سیم، شبکه‌هایی متشکل از تعداد زیادی نود حسگر با تراکم بالا، کاربردهای متنوع در حوزه‌های نظارت و ردیابی، منابع محدود و بدون زیرساخت هستند. این شبکه‌ها به دلایلی مانند کانال ارتباطی ناامن و ارتباطات بی‌سیم، مشکلات امنیتی فراوانی دارند. بنابراین، تأمین امنیت یک نیازمندی حیاتی برای این شبکه‌ها است. از سوی دیگر، جهت مواجهه با انواع نفوذها در حوزه امنیت اطلاعات، مکانیزم‌های امنیتی فراوانی ایجاد شده‌اند؛ یکی از مهم‌ترین این ابزارها، سیستم تشخیص نفوذ می‌باشد. سیستم تشخیص نفوذ، سیستمی نرم‌افزاری یا سخت‌افزاری است که می‌تواند بر ترافیک محیط عملیاتی مورد نظر نظارت کند، آن را تحلیل نموده و حملات را کشف نماید. بنابراین، می‌توان با بهره‌گیری از سیستم‌های تشخیص نفوذ در حوزه شبکه‌های حسگر بی‌سیم، سطح امنیت را در این شبکه‌ها افزایش داد. در این زمینه تحقیقاتی انجام شده است که غالباً ناقص و خاص-منظوره هستند و عملاً اثری از تحقیق جامعی در این حوزه دیده نمی‌شود.

این تحقیق بر آن است که با توجه به ادبیات موضوع و تحقیقات انجام شده، به بررسی موضوع حیاتی امنیت و حل مسأله‌ی تشخیص نفوذ در شبکه‌های حسگر بی‌سیم، البته با دیدی جامع و دقیق پردازد. بدین منظور با بررسی ابعاد مختلف سیستم‌های تشخیص نفوذ، شبکه‌های حسگر بی‌سیم و امنیت در این شبکه‌ها، ۳ پیشنهاد ارائه نموده است: نخست، بکارگیری یک معماری تشخیص نفوذ سلسله‌مراتبی، خوشه‌بندی، توزیعی، استاتیک و ناهمگن؛ دوم، بکارگیری پروتکل مسیریابی سلسله‌مراتبی LEACH، البته با تغییرات اندک؛ سوم، بهره‌گیری از دو نوع سیستم تشخیص نفوذ به نام‌های سیستم تشخیص نفوذ مبتنی بر سرخوشه، مستقر بر سرخوشه‌ها و سیستم تشخیص نفوذ مبتنی بر سطح کل شبکه‌ی حسگر بی‌سیم، مستقر بر روی سرور مدیریت مرکزی. بنابراین هدف این پایان‌نامه استقرار همه‌ی انواع سیستم‌های تشخیص نفوذ در قالب یک راه‌حل جامع و یکپارچه، به عنوان یک لایه‌ی دفاعی-امنیتی جدید و افزودن آن به زیرساخت امنیتی شبکه‌های حسگر بی‌سیم می‌باشد.

**کلید واژه:** شبکه‌ی حسگر بی‌سیم، امنیت، تشخیص نفوذ، سیستم تشخیص نفوذ، حمله، دینامیک، مسیریابی، عامل، سیاست، تشخیص، پاسخ، ردیابی.

## فصل ۱:

### کلیات تحقیق



پیشرفت‌ها در ارتباطات بی‌سیم، ایجاد و توسعه‌ی شبکه‌های حسگر بی‌سیم ارزان<sup>۱</sup> و با توان مصرفی پایین (منابع محدود)<sup>۲</sup> را ممکن ساخته است. شبکه‌های حسگر بی‌سیم (WSNs)<sup>۳</sup> سیستم‌هایی همگن یا ناهمگن متشکل از تعداد زیادی ابزار کوچک، به نام نودهای حسگر، هستند که محیط‌های مختلف را به صورت مشارکتی نظارت می‌کنند؛ یعنی نودهای حسگر علاوه بر عملکرد مستقل و خودمختار، با همدیگر همکاری می‌کنند و برای رسیدن به یک دید سراسری و جامع از محیط عملیاتی، داده‌های محلی‌شان را ترکیب می‌نمایند [۱ و ۲]. در شبکه‌های حسگر بی‌سیم علاوه بر نودهای حسگر، دو مؤلفه‌ی مهم دیگر به نام‌های "نقاط تجمع"<sup>۴</sup> (معادل سرخوشه‌ها و محل استقرار CIDSها) و "ایستگاه پایه"<sup>۵</sup> (معادل سرور مرکزی و محل استقرار WSNIDS) هم وجود دارند، که در مقایسه با حسگرهای معمولی منابع قوی تری دارند. نقاط تجمع اطلاعات را از حسگرهای اطراف‌شان جمع‌آوری می‌کنند، آن‌ها را مجتمع (خلاصه‌سازی)<sup>۶</sup> کرده و سپس به ایستگاه‌های پایه برای پردازش‌های بعدی ارسال می‌کنند (مطابق شکل (۱-۱)) [۱-۳]. عواملی مانند ماهیت مشترک، بی‌سیم، حفاظت نشده و ناامن کانال ارتباطی، رسانه‌ی انتقال غیرقابل اعتماد و همگانی، استقرار در محیط‌های باز و خطرناک، عملکرد خودکار و بی‌مراقب و منابع محدود، شبکه‌های حسگر بی‌سیم را برای انواع حملات مستعد و آسیب‌پذیر می‌سازد [۱ و ۴]؛ به علاوه، شبکه‌های حسگر بی‌سیم، علی‌رغم داشتن کاربردهای بسیار زیاد و متنوع (در حوزه‌های نظارت و ردیابی)، با ریسک‌های بزرگی مواجه‌اند؛ از جمله از دست دادن اطلاعات، سرویس‌ها و کنترل شبکه؛ بنابراین امنیت یک نیازمندی حیاتی برای این شبکه‌ها است. با توجه به این که استفاده از اکثر تکنیک‌های امنیتی شبکه‌های سنتی، در این نوع از شبکه‌ها غیرممکن است [۲ و ۳]؛ بنابراین مکانیزم‌های امنیتی-دفاعی که بتوانند عملیات متداول این شبکه‌ها را تضمین کنند، باید متناسب با مکانیزم‌های خودمختار و مستقل درون خود این نوع شبکه‌ها باشند. این پژوهش در جستجوی مکانیزم امنیتی کاملی برای تأمین ارکان اساسی امنیت شامل محرمانگی، یکپارچگی، دسترس‌پذیری<sup>۷</sup> و احراز هویت<sup>۸</sup>، البته با توجه به محدودیت‌ها و موانع موجود در این شبکه‌ها، می‌باشد. در حال حاضر تحقیق برای ارائه‌ی راه‌حل‌های امنیتی برای شبکه‌های حسگر بی‌سیم عمدتاً در ۳ دسته‌ی مدیریت کلید (برقراری کلیدهای رمزنگاری بین نودها برای فراهم کردن رمزنگاری و احراز هویت)، احراز هویت و مسیریابی امن (پروتکل‌هایی

<sup>1</sup> Low-cost

<sup>2</sup> Low-power

<sup>3</sup> Wireless Sensor Networks

<sup>4</sup> Aggregation points

<sup>5</sup> Base-station

<sup>6</sup> Aggregate

<sup>7</sup> Availability

<sup>8</sup> Authenticity

برای محافظت اطلاعات از افشاء غیرمجاز و تحویل کامل و درست آن‌ها به ایستگاه پایه) و خدمات امن (محلی کردن، تجمع و همزمان سازی امن) متمرکز است [۵۱]. همه‌ی پروتکل‌های امنیتی ارائه شده تاکنون، متکی بر فرضیات ویژه‌ای در باره‌ی ماهیت حملات هستند. بنابراین، با توجه به محدودیت‌های مختلف شبکه‌های حسگر بی‌سیم، لازم است که یک خط دفاعی دیگر به زیرساخت امنیتی این شبکه‌ها افزوده گردد؛ پیشنهاد ارائه شده افزودن یک لایه‌ی دفاعی-امنیتی دیگر به نام سیستم تشخیص نفوذ می‌باشد؛ که می‌تواند تلاش‌های مربوط به ایجاد ناامنی و ورود غیرمجاز را کشف کند و هنگام رخداد حملات، حتی حملات جدید (آنومالی‌ها)، هشدار داده و اقدامات لازم و عمدتاً از قبل تعیین شده را اجرا نماید.

توجه داشته باشید که رویکرد پیشنهادی روش‌های تشخیص، معماری‌ها، روش‌های تصمیم‌گیری و پاسخ‌دهی موجود را توسعه داده و مجتمع می‌کند. هم‌چنین، با اتخاذ یک رویکرد مبتنی بر عامل و سیاست برای مشاهده‌ی ترافیک، با فرآیند تشخیص چندعامله برای کشف کردن حملات با نرخ خطای پایین‌تر بطور تطبیقی، و فراهم کردن یک لایه‌ی تحلیل ضمنی کاراً برای کاربر همراه است؛ لایه‌ی تحلیل تصمیمات کاربر را در باره‌ی آنومالی‌های کشف شده، با ارائه دادن اطلاعات اضافی از منابع داده‌ای مرتبط، پشتیبانی می‌کند و مسئول بصری‌سازی و تجسم آنومالی‌ها و وضعیت لایه‌ی تشخیص<sup>۱</sup> نیز می‌باشد. سیستم تشخیص نفوذ پیشنهادی مبتنی بر تحلیل پیام‌های داده‌ای استماع شده، رویدادهای<sup>۲</sup> کشف شده (توسط سرخوشه‌ها و سرور مرکزی) و استنتاج رفتار شبکه می‌باشد. مهم‌ترین محورهای پژوهشی این پایان‌نامه عبارتند از:

- معرفی شبکه‌های حسگر بی‌سیم
- امنیت در شبکه‌های حسگر بی‌سیم و ارائه‌ی دیدی کلی از انواع حملات در این شبکه‌ها و مقایسه‌ی آن‌ها بایکدیگر از ابعاد مختلف
- بررسی سیستم‌های تشخیص نفوذ و ابعاد مختلف آن‌ها
- بررسی تشخیص نفوذ در شبکه‌های حسگر بی‌سیم
- پیشنهادیک مدل جامع، سلسله‌مراتبی و توزیع‌شده‌ی تشخیص نفوذ و معماری مؤلفه-محور سیستم تشخیص نفوذ مبتنی بر عامل و سیاست در شبکه‌های حسگر بی‌سیم

در این پایان‌نامه به تعریف نیازمندی‌ها، بررسی طرح‌های ممکن و پیشنهاد یک معماری مؤلفه-محور مناسب و اختصاصی برای تشخیص نفوذ و هم‌چنین معماری برای سیستم تشخیص نفوذ در WSN‌ها خواهیم پرداخت. به علاوه، این پژوهش ما را قادر می‌سازد تا با چالش‌های امنیتی موجود در شبکه‌های حسگر بی‌سیم، اهداف و توانایی‌های مهاجمان آشنا شویم؛ هم‌چنین روش‌ها، آثار و نتایج حملات بر روی شبکه‌های حسگر بی‌سیم را شناسایی نماییم، و بتوانیم با افزودن یک لایه‌ی امنیتی-دفاعی جدید، به نام سیستم تشخیص نفوذ، به زیرساخت امنیتی این شبکه‌ها، مشکل تشخیص نفوذ در این شبکه‌ها را تا حدودی

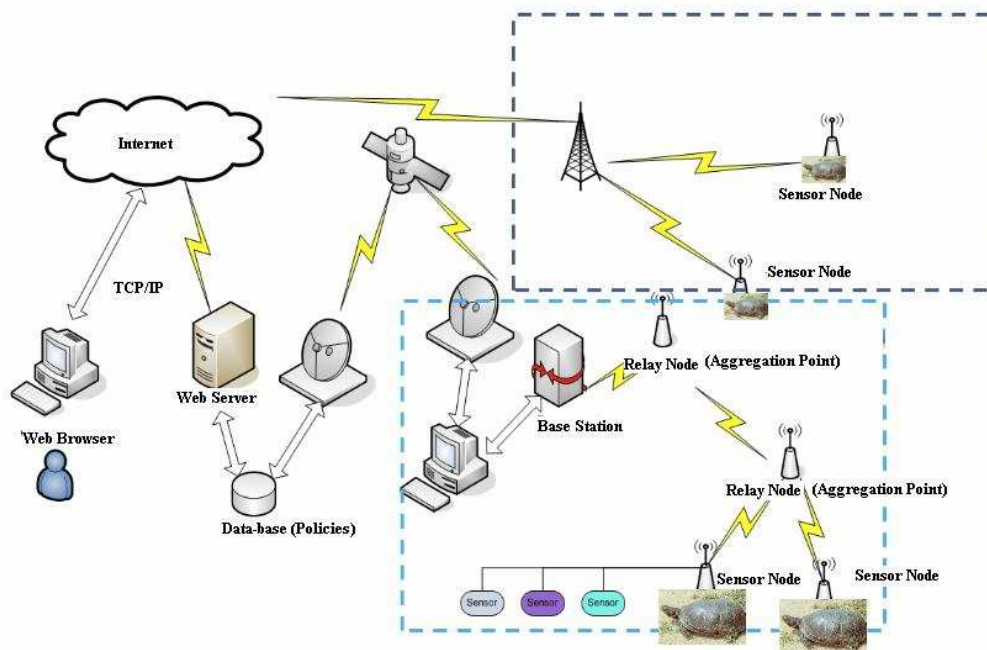
---

<sup>1</sup> Detection Layer Status

<sup>2</sup> Events

مرتفع نماییم؛ در نتیجه، حملات را کشف و مدیریت کنیم و متناسب با نوع و ماهیت حملات به آنها واکنش به موقع و متناسب نشان دهیم.

خلاصه این که، این پژوهش بر امنیت شبکه‌های حسگر بی‌سیم متمرکز است و می‌خواهد مشکل تشخیص نفوذ در شبکه‌های حسگر بی‌سیم را مرتفع نماید. در نتیجه برای رسیدن به این هدف، این پژوهش شبکه‌های حسگر بی‌سیم، ابعاد مختلف آنها و انواع حملات ممکن در این حوزه را بررسی کرده است؛ به علاوه، اهداف و توانایی‌های مهاجمان را شناسایی کرده و با آثار و نتایج حملات بر روی شبکه‌های حسگر بی‌سیم آشنا شده است. همچنین، به بررسی ابعاد مختلف سیستم‌های تشخیص نفوذ و معماری‌های پایه‌ی این سیستم‌ها، همچنین به بررسی معماری‌های دو نمونه سیستم تشخیص نفوذ (به نام‌های OSSEC و SNORT)، پرداخته است و در انتها، یک معماری تشخیص نفوذ و معماری سیستم تشخیص نفوذ متناسب با نیازها، خصوصیات و محدودیت‌های خاص این شبکه‌ها ارائه نموده است (به نام WSNIDS).



شکل ۱-۱: معماری ارتباطی شبکه‌های حسگر بی‌سیم

## ۱-۲- تعریف موضوع

مشکلی که امروزه با آن مواجه هستیم، حفاظت شبکه‌های مان در برابر انواع حملات می‌باشد. این مشکل در حوزه‌ی شبکه‌های حسگر بی‌سیم با توجه به کاربردهای فراوان و عمدتاً امنیتی-اطلاعاتی و خصوصیات ویژه‌ی این شبکه‌ها، از اهمیت بیشتری برخوردار است. تاکنون برای حفاظت از این شبکه‌ها در برابر انواع نفوذهای، معماری‌ها و مدل‌هایی ارائه شده‌اند؛ اما هیچ‌یک از

آن‌ها دیدی جامع و کلی به این مسأله نداشته‌اند و عمدتاً تک‌بعدی و خاص‌منظوره (مثلاً برای یک نوع حمله‌ی خاص) طراحی و پیاده‌سازی شده‌اند؛ اما طرح پیشنهادی در این پایان‌نامه با دیدی جامع و همه‌منظوره و با در نظر گرفتن ابعاد و خصایص مختلف شبکه‌های حسگر بی‌سیم، یک معماری جامع و کامل برای حل مشکل تشخیص نفوذ در این شبکه‌ها ارائه می‌نماید. خصیصه‌ی اصلی این معماری آن است که در ۱ یا ۲ سطح، با توجه به حوزه‌ی کاربردی و نیاز امنیتی در آن حوزه، طراحی شده است و قابل پیاده‌سازی می‌باشد. تمرکز این پایان‌نامه بر ایجاد و استقرار CIDS<sup>۱</sup>ها بر روی سرخوشه‌ها<sup>۲</sup> (سیستم تشخیص نفوذ مبتنی بر سرخوشه) و WSNIDS<sup>۳</sup> (سیستم تشخیص نفوذ شبکه‌های حسگر بی‌سیم) بر روی سرور مرکزی یا سینک می‌باشد (بنابراین، مسأله‌ی مورد بحث در این پایان‌نامه عبارت است از: تشخیص نفوذ در شبکه‌های حسگر بی‌سیم).

### ۱-۳- کارهای پیشین (تجربیات گذشته)<sup>۴</sup>

تشخیص نفوذ یک مبحث مهم در ناحیه‌ی وسیع امنیت کامپیوتر، و بطور خاص امنیت شبکه است [۶۶و۶۵] که به عنوان موضوعی مهم در شبکه‌های حسگر بی‌سیم از حساسیت و تأثیر ویژه‌ای برخوردار است. قاعده‌ی اصلی چگونگی کشف آنومالی‌های شبکه، خصوصاً بدون هیچ بازخوردی از میزبان‌های تحت تأثیر قرار گرفته، تحلیل الگوها در داده‌های شبکه و مقایسه کردن آن‌ها با داده‌های معمول است؛ سرانجام استنتاج رابطه‌های نامنظم مربوط به پروفایل یک حمله شناخته می‌شود. این رویکرد برای تشخیص نفوذ شبکه، عموماً مبتنی بر جریان اطلاعات می‌باشد. بسیاری از سیستم‌های موجود، مبتنی بر تحلیل حجم ترافیک مدل‌سازی شده توسط متدهای اصلی تحلیل مؤلفه، یا فقط تعداد جریان‌های متناظر با معیارهای منتخب، هر یک چشم انداز معتبر خاصی در باره‌ی ترافیک شبکه ارائه می‌دهد. تاکنون راه‌حل‌های زیادی برای شبکه‌های سنتی پیشنهاد شده‌اند، اما محدودیت‌های منابع شبکه‌ی حسگر بی‌سیم باعث می‌شود که آن راه‌حل‌ها برای این شبکه‌ها قابل استفاده نباشد<sup>۵</sup> [۷و۳].

در میان انواع مختلف شبکه‌ها، شبکه‌های ادهاک تشابهاتی با شبکه‌های حسگر بی‌سیم دارند. این شبکه‌ها نیز محدودیت‌های شدید منابع دارند، هر چند که مانند شبکه‌های حسگر بی‌سیم محدودکننده نیستند. در تشخیص نفوذ برای شبکه‌های ادهاک

---

<sup>۱</sup> Cluster-based Intrusion Detection System

<sup>۲</sup> در شبکه‌های حسگر بی‌سیم معمولاً فرض بر آن است که سرخوشه‌ها (دقیقاً) یکی از همان نودهای معمولی حسگر در هر یک از خوشه‌ها هستند؛ اما در معماری تشخیص نفوذ پیشنهادی ما برای شبکه‌های حسگر بی‌سیم، فرض بر آن است که یک سیستم میزبان مجزاً تحت عنوان سرخوشه با امکانات و قابلیت‌های بالاتری نسبت به حسگرهای معمولی برای استقرار CIDS در هر خوشه وجود دارد (مانند PC یا Laptop)؛ بنابراین این سیستم‌ها به عنوان سرخوشه در نظر گرفته می‌شوند، که در این صورت حتی می‌توان خوشه‌ها را ثابت/استاتیک در نظر گرفت و آن سیستم میزبان CIDS را به عنوان سرخوشه انتخاب نمود (شبکه‌ی ناهمگن).

<sup>۳</sup> Wireless Sensor Network Intrusion Detection System

<sup>۴</sup> Related work

<sup>۵</sup> In-viable