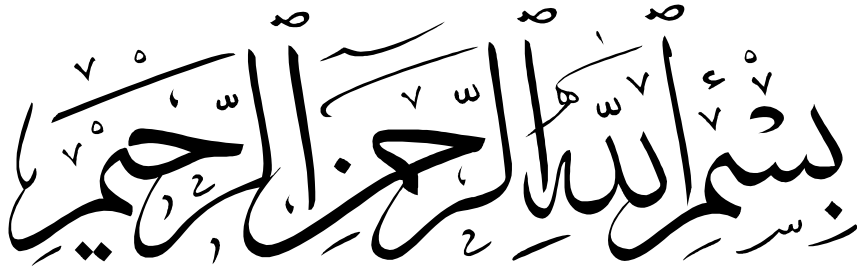

دانشگاه صنعتی امیرکبیر

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

پایان‌نامه کارشناسی ارشد مهندسی فناوری اطلاعات

گرایش امنیت اطلاعات

شناسایی مبتنی بر میزبان کرم‌واره‌ها در شبکه‌های Peer-to-Peer

نگارش:

فاطمه کاظمینی

استاد راهنما:

دکتر بابک صادقیان

استاد مشاور:

دکتر مهدی شجری

بهمن ۱۳۸۶

بسمـه تعالـــی

فرم اطلاعات پایان نامه

کارشناسی ارشد و دکترا

دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

معاونت پژوهشی

تاریخ: .....۸۷/۲/۲۴.....

پیوست: .....

نام و نام خانوادگی: فاطمه کاظمینی	**دانشجوی آزاد** ☒	**بورسیه** ☐	**معادل** ☐	
شماره دانشجوئی: ۸٤۱۳۱۰۱۱	**دانشکده:** مهندسی کامپیوتر	**رشته تحصیلی:** مهندسی فناوری اطلاعات		
نام و نام خانوادگی استاد راهنما: دکتر بابک صادقیان				
عنوان پایان نامه به فارسی: **شناسایی مبتنی بر میزبان کرم واره ها در شبکه های Peer to Peer**				
عنوان پایان نامه به انگلیسی: **Host based detection of worms in peer to peer networks**				
نوع پروژه: **کارشناسی ارشد** ☒ **دکترا** ☐	**کاربردی** ☐	**بنیادی** ☐	**توسعه ای** ☐	**نظری** ☒
تاریخ شروع: ۸۵/۷	**تاریخ خاتمه:** ۸۶/۱۱	**تعداد واحد:** ۶		
سازمان تأمین کننده اعتبار: سازمان تحقیقات مخابرات ایران				
واژه های کلیدی به فارسی: کرم‌واره‌ها (کرم های کامپیوتری)، تشخیص ناهنجاری مبتنی بر میزبان، شبکه P2P				
واژه های کلیدی به انگلیسی: Computer worms, Host-based anomaly detection, Anomaly detection, P2P network				

نظرها و پیشنهادها به منظور بهبود فعالیت های پژوهشی دانشگاه:

استاد راهنما:

دانشجو:

امضاء استاد راهنما: **تاریخ: ۸۷/۲/۱**

نسخه ۱: معاونت پژوهشی

نسخه ۲: کتابخانه و به انضمام دو جلد پایان نامه به منظور تسویه حساب با کتابخانه و مرکز اسناد و مدارک علمی

تصویب‌نامه

دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

تائیدیه هیئت داوران

عنوان:

شناسایی مبتنی بر میزبان کرم‌واره‌ها در شبکه‌های Peer-to-Peer

۱- استاد راهنما	آقای دکتر بابک صادقیان	امضاء.....
۱- استاد مشاور	آقای دکتر مهدی شجری	امضاء.....
۳- ممتحن خارجی	آقای دکتر رسول جلیلی	امضاء.....
۴- ممتحن داخلی	آقای دکتر مهران سلیمان فلاح	امضاء.....
۵- نماینده تحصیلات تکمیلی دانشکده	آقای دکتر محمد رحمتی	امضاء.....

تقدیم به پدر و مادر مهربانم

با تشکر فراوان از استاد راهنما، جناب آقای دکتر بابک صادقیان و استاد مشاور، آقای دکتر مهدی شجری که با راهنمایی های خود در طول اجرای پروژه مرا یاری دادند.

چکیده

کرم‌واره‌ها (کرم‌های کامپیوتری)، به علت قابلیت انتشار مستقل و اثرات مخربی که می‌توانند بر جای بگذارند، یکی از بزرگترین تهدیدات شبکه محسوب می‌گردند. روش‌های تشخیص کرم‌واره باید از سرعت بالایی برخوردار بوده، نرخ خطای پایینی داشته و قابلیت تشخیص کرم‌واره‌های جدید را نیز داشته باشند. شبکه‌های جدیدی مانند شبکه Peer-to-Peer (P2P) باعث به وجود آمدن زمینه جدیدی برای فعالیت کرم‌واره‌ها شده‌اند. کرم‌واره‌های P2P با سوء استفاده از ویژگی‌های این نوع شبکه‌ها، می‌توانند با سرعت بالا و با ترکیب شدن در ترافیک عادی شبکه بین گره‌ها منتشر شوند. آنها پتانسیل بالاتری برای حملات خطرناک به شبکه دارند، زیرا مکانیزم‌های فعلی تشخیص و مقابله با کرم‌واره‌ها در مقابل آنها موثر نیست. بنابراین، ساختار خاص شبکه‌های P2P، نیازمندی‌های جدیدی برای مقابله با حملات به آن مطرح می‌کند. در این پایان نامه، روشی مبتنی بر میزبان برای تشخیص کرم‌واره‌های P2P براساس تشخیص ناهنجاری ارائه نموده‌ایم. این پایان نامه شامل دو بخش است. در بخش اول، شناسایی کرم‌واره‌های P2P را تنها از روی اطلاعات یک میزبان و به کمک الگوریتم یادگیری ماشین بیزی انجام دادیم. در بخش دوم پایان نامه، برای افزایش دقت تشخیص از همکاری بین گره‌های همسایه در شبکه P2P بهره گرفتیم. این همکاری از طریق بررسی شباهت الگوی وضعیت داخلی دو گره همسایه انجام گرفته است. ما در ابتدا تاثیر زمان را توسط تبدیل فوریه سریع از الگوها حذف نموده و سپس نسبت شیب دو الگو را به منظور بررسی شباهت آنها مورد مطالعه قرار داده‌ایم. نرخ تشخیص و false positive به دست آمده در بخش اول پایان نامه به ترتیب ۸۷ و ۱۵ درصد بود. در بخش دوم پایان نامه و با در نظر گرفتن همکاری بین گره‌ها این میزان تا نرخ تشخیص ۹۵ درصد و ۵ درصد برای false positive بهبود پیدا کرد. روش ارائه شده در این پایان نامه علاوه بر دقت بالا، از هزینه محاسبات کم و سرعت نسبتاً بالایی برخوردار بوده و به سادگی روی هر گره شبکه قابل استفاده است.

کلمات کلیدی: کرم‌واره‌ها (کرم های کامپیوتری)، تشخیص ناهنجاری مبتنی بر میزبان، شبکه P2P

فهرست مطالب

فهرست اشکال

فهرست جداول

فصل ۱

مقدمه

۱ مقدمه

امنیت در شبکه‌ها و سیستم‌های کامپیوتری توسط حملات مختلفی مورد تهدید قرار می‌گیرد. یکی از رایج‌ترین حملات، حملاتی است که توسط برنامه‌های مخرب[1] صورت می‌گیرد. برنامه مخرب به یک مجموعه از دستورات گفته می‌شود که باعث نقض شدن خط مشی امنیتی سیستم می‌گردد[Bishop 2003]. کرم‌واره‌ها ، ویروس‌واره‌ها و برنامه‌های اسب ترویان، نمونه‌هایی از برنامه‌های مخرب محسوب می‌گردند که ابزار موثری برای حمله و آسیب رسانی به سیستم‌های کامپیوتری به شمار می روند. آنها با وارد شدن به سیستم و آلوده‌سازی آن، می‌توانند بسیاری از کنترل دسترسی‌های معمول در سیستم را بی اثر کرده و کنترل آن سیستم را به دست گیرند. با به دست گرفتن کنترل سیستم، برنامه مخرب می‌تواند هر گونه فعالیت مورد نظر خود را روی سیستم انجام دهد. به عنوان مثال، می‌تواند باعث افشای اطلاعات محرمانه ذخیره شده، تغییر غیر مجاز در اطلاعات سیستم و یا اختلال در فعالیت آن شود و به این شکل، تمام جنبه های مختلف امنیت در سیستم را مورد تهدید قرار دهد.

کرم‌واره‌ها، برنامه‌هایی هستند که خود را از یک کامپیوتر بر روی سیستم دیگر بازنویسی می‌کنند[Bishop 2003]. آنها به صورت مستقل عمل می‌نمایند و از این رو قدرت تکثیر و انتشار بیشتری نسبت به برنامه‌های مخرب دیگری مانند ویروس‌واره‌ها دارند. کرم‌واره‌ها یکی از بزرگترین تهدیدات شبکه و دیگر سیستم‌ها به حساب می‌آیند و قادر به آسیب رسانی جدی به آنها می‌باشند. شناسایی حمله کرم‌واره‌ها، کاری دشوار است. از مشکلات این امر می‌توان به سرعت بالای لازم برای انجام عملیات شناسایی و همچنین عدم شناخت کامل خصوصیات حمله اشاره نمود. علاوه بر سرعت عملکرد، راهکار تشخیص باید قابلیت شناسایی کرم‌واره‌ها و ویروس‌واره‌های جدید را داشته و نرخ false positive پایینی داشته باشد. روش‌های تشخیصی که مبتنی بر نشانه[2] کرم‌واره‌ها هستند، قابلیت تشخیص حملات جدید را ندارند و نمی‌توانند در مقابل این گونه حملات عکس العمل سریع انجام دهند. در ضمن، این روش‌ها برای شناسایی نشانه‌هایی که مربوط به کدهای جدید

[1] Malicious logic
[2] Signature

می‌شود، نیاز به دخالت انسان دارند. در مقابل، روش‌های شناسایی مبتنی بر ناهنجاری[1] قابلیت بهتری برای شناسایی حملات جدید و عکس العمل به موقع در برابر آنها دارند. این روش‌ها با مدل کردن رفتار عادی سیستم، می‌توانند رفتار غیر عادی آن را تشخیص دهند.

هر روزه، کرم‌واره‌های جدیدی با روش‌های عملکرد مختلف در شبکه‌های گوناگون منتشر می‌شوند. پیدایش انواع شبکه‌های کامپیوتری (مانند شبکه‌های بیسیم، سیار، Grid و P2P) با کاربردهای مختلف نیز زمینه گسترده‌تری را برای فعالیت و انتشار کرم‌واره‌ها فراهم آورده‌اند. شبکه P2P، گونه‌ای از این شبکه‌های کامپیوتری است که به علت ویژگی‌هایی که دارد، محیط بسیار مناسبی برای انتشار کرم‌واره‌ها به شمار می‌رود.

یک شبکه P2P شامل گروهی از گره‌های اینترنت است که شبکه‌ای را برای منظوری خاص بر روی شبکه اینترنت بنا کرده‌اند. این شبکه‌ها مسیر یابی را در لایه کاربرد و بالای مسیریابی IP انجام می‌دهند [Zhou, Zhang, McSherry, 2005]. به بیان دیگر، شبکه P2P یک سیستم توزیع شده خاص روی لایه کاربرد است که هر جفت از گره‌های آن می‌توانند با هم از طریق پروتکل مسیریابی در لایه P2P ارتباط برقرار کنند. هدف در این شبکه‌ها، اشتراک منابع موجود در گره‌های شبکه P2P است که به صورت اشیاء مختلفی مانند فایل‌های صوتی، تصویری، متن وغیره روی گره‌ها ذخیره شده‌اند. اعضای شبکه P2P می‌توانند، شیئ مورد نظر خود را در شبکه جستجو نموده و از گره‌ای که آن را در اختیار دارد، درخواست نمایند. شبکه‌های P2P به علت کاربردشان، هر روزه هم در بین کاربران عادی و هم در مجامع تحقیقاتی مورد استقبال بیشتری قرار می‌گیرند.

مسائل امنیتی که در ابتدای پیدایش این شبکه‌ها بیشتر مورد توجه بودند، به مسائل مربوط به اطمینان از صحت انجام عملیات در آن مانند اشتراک عادلانه منابع و حملات ممانعت از سرویس مربوط می‌شدند و دیگر حملات ممکن به شبکه نادیده گرفته شده بودند. مدتی بعد، با افزایش استفاده از شبکه‌های P2P و همین طور بالا رفتن میزان حملات روی آنها، لزوم تمرکز و تحقیق بر روی شناسایی حملاتی مانند حمله کرم‌واره‌ها ، مشخص گردید. حمله کرم‌واره‌ها یکی از مخرب‌ترین حملات روی شبکه‌های P2P محسوب می‌شود. این کرم‌واره‌ها با استفاده از خواص شبکه P2P، سریع‌تر در میان گره‌های شبکه منتشر می‌شوند. کرم‌واره‌های P2P

[1] Anomaly

از نقطه ضعف‌های معمول در میزبان‌های شبکه برای ورود و آلوده‌سازی آنها استفاده می‌کنند، ولی پس از آن، برای یافتن قربانی های بعدی خود از روش‌های متداولی که کرم‌واره‌های معمولی از آنها بهره می برند، استفاده نمی‌کنند[Zhou, Zhang, McSherry, 2005]. به علاوه، آنها با کمک خواص شبکه‌های P2P، از روش‌هایی برای انتشار بهره می‌گیرند که تشخیصشان را پیچیده‌تر و سخت‌تر از کرم‌واره‌های دیگر می‌کند. از این رو آنها می‌توانند اثر شدیدتری روی شبکه نسبت به کرم‌واره‌های عادی از خود به جای بگذارند. از ویژگی‌های شبکه P2P که کرم‌واره‌ها از آنها استفاده می‌کنند، می‌توان به موارد زیر اشاره نمود:

- تعداد زیاد گره‌های فعال عضو شبکه، که کرم‌واره می‌تواند با نفوذ به شبکه به آنها دست یابد.
- شبکه‌های محلی متفاوت مربوط به گره‌های مختلف شبکه که هر کدام ممکن است آسیب‌پذیری‌های خاصی داشته باشند و ورود کرم‌واره را به شبکه ساده کنند.
- ذخیره سازی اطلاعات گره‌های همسایه توسط هر گره عضو شبکه

در شبکه P2P، گره‌های عضو شبکه باید اطلاعاتی از گره‌های همسایه خود را نگهداری کنند تا بتوانند از طریق این اطلاعات با آنها ارتباط برقرار و درخواست های خود را منتقل کرده و یا به درخواست گره‌های دیگر پاسخ دهند. کرم‌واره‌های P2P از این خاصیت شبکه‌های P2P که گره‌های شبکه یکدیگر را می‌شناسند، استفاده می‌کنند. در این صورت کرم‌واره‌های P2P به راحتی می‌توانند اطلاعات موجود در یک گره آلوده را استخراج و قربانیان بعدی خود را شناسایی نمایند. این کرم‌واره‌ها لازم نیست به پویش شبکه یا کارهای دیگری از این قبیل، که باعث تغییر شدید در رفتار شبکه یا گره می‌شود، بپردازند تا از این طریق گره‌های فعال دیگری را که می‌توانند اهداف بعدی آلوده‌سازی باشند، شناسایی نمایند. به این ترتیب، آنها می‌توانند بدون ایجاد تغییرات ناگهانی شدید در رفتار گره یا شبکه، دیگر گره‌های شبکه را مورد حمله قرار دهند. از طرف دیگر، کرم‌واره‌های عادی در فرآیند پویش شبکه، با تعداد زیادی از خطا در ارتباط[1] با گره‌های غیرفعال رو به رو می‌شوند که باعث شناسایی آنها می‌شود. ولی کرم‌واره‌های P2P، گره‌های فعال را می‌شناسند و به همین دلیل خطایی در ارتباطات آنها رخ نمی‌دهد. در حالت کلی می‌توان گفت که کرم‌واره‌ها می‌توانند با ترافیک عادی شبکه مخلوط شوند، که

[1] Failed connection

به این دلیل، شناسایی این کرم‌واره‌ها کاری دشوار به شمار می‌آید. هدف ما در این پایان نامه، تشخیص کرم‌واره‌های P2P است، تا به این طریق میزان خطرات این کرم‌واره‌ها را کاهش داده و امنیت در شبکه‌های P2P را بالا ببریم.

سیستم‌های تشخیص ناهنجاری از دو رویکرد متفاوت از نظر اطلاعات مورد استفاده برای تشخیص، استفاده می‌کنند: رویکرد مبتنی بر میزبان[1]، که اطلاعات داخلی میزبان را مورد بررسی قرار می‌دهد و رویکرد مبتنی بر شبکه[2] که اطلاعات مورد نیاز خود را از ترافیک شبکه جمع‌آوری می‌کند. ما در این پایان نامه، رویکرد مبتنی بر میزبان را مبنای کار خود قرار داده‌ایم. دو دلیل عمده برای این انتخاب وجود دارد:

- با توجه به نوع انتشار کرم‌واره‌های P2P، این کرم‌واره‌ها باعث بروز تغییرات شدید در رفتار شبکه نمی‌شوند. به همین دلیل، داده‌های به دست آمده از شبکه نمی‌توانند اطلاعات موثری را به منظور تشخیص کرم‌واره‌های P2P در اختیار بگذارند.
- شبکه P2P یک سیستم توزیع شده است و هر گره آن می‌تواند به شبکه محلی خاصی تعلق داشته باشد. در چنین حالتی، جمع آوری اطلاعات از کل شبکه، کار دشواری است و نیاز به تمهیدات خاص دارد. بنابراین می‌توان نتیجه گرفت که در چنین شبکه‌هایی، سیستم‌های مبتنی بر میزبان، کاربرد ساده‌تر و عملی‌تری دارند. سیستم تشخیص وجود کرم‌واره را می‌توان بر روی هر گره شبکه P2P به صورت جداگانه و دلخواه نصب نمود.

علاوه بر استفاده از اطلاعات یک میزبان، ما در این پایان نامه از ایده همکاری بین گره‌ها برای بالا بردن دقت تشخیص کرم‌واره‌ها نیز استفاده نموده‌ایم. همان گونه که اشاره شد، گره‌های شبکه P2P، اطلاعات مربوط به گره‌های همسایه خود (از جمله آدرس آنها) را ذخیره می‌کنند یا به عبارت دیگر همسایگان خود را می‌شناسند. این ویژگی کمک می‌کند تا از همکاری میزبان‌های همسایه برای تشخیص کرم‌واره در شبکه P2P استفاده کنیم. برای این منظور، گره‌های همسایه اطلاعات داخلی خود را با هم مبادله می‌کنند، تا با بررسی آنها

[1] Host based
[2] Network based

به وجود فعالیت کرم‌واره پی ببرند. از آنجا که در سیستم پیشنهادی این پایان نامه، جمع آوری اطلاعات از گره‌های همسایه و به صورت توزیع شده است، می‌توان این سیستم تشخیص کرم‌واره‌های P2P را یک سیستم تشخیص نفوذ توزیع‌شده دانست. از طرف دیگر، از آنجا که پروتکل P2P روی لایه کاربرد کار می کند و ارتباطاتی که گره های P2P با هم برقرار می کنند، در این لایه صورت می گیرد، روش ارائه شده در این پایان نامه و آزمایشهای مربوطه، مختص کرم واره های P2P می باشد.

از آنجا که در اکثر موارد کرم‌واره روی گره‌های همسایه به شکل همزمان در حال اجرا است، با بررسی شباهت وضعیت عملکرد دو گره می‌توان کرم‌واره‌ها را شناسایی نمود[Malan and Smith 2005]. در این پایان نامه نیز با کمک این ایده سعی کرده‌ایم تا به نتایج بهتری در تشخیص کرم‌واره‌های P2P دست پیدا کنیم. در این روش، هرچند گره‌ها با هم همکاری می‌کنند و از اطلاعات همسایگانشان در کنار اطلاعات داخلی خود استفاده می‌کنند، ولی عملیات تشخیص کرم‌واره به طور مجزا و توسط هر گره به شکل مستقل انجام می‌گردد. در حالت کلی می‌توان روش‌های پیشنهادی در این پایان نامه را به دو بخش عمده زیر تقسیم بندی کرد:

- تشخیص کرم‌واره P2P با استفاده از اطلاعات یک میزبان
- تشخیص کرم‌واره P2P با استفاده از همکاری میزبان‌ها

این روش‌ها نتایج متفاوتی در دقت تشخیص کرم‌واره P2P و همچنین میزان اعلام خطرهای اشتباه از خود نشان دادند، ولی در مجموع در این پایان نامه ما توانستیم نتایج خوبی در تشخیص کرم‌واره‌های P2P در مقایسه با دیگر روش‌ها به دست آوریم، که در فصل های آتی جزئیات آنها را مورد بحث قرار خواهیم داد.

در این پایان نامه، پس از بخش مقدمه، در فصل۲ ابتدا به معرفی کرم‌واره‌ها ، انواع مختلف آنها و نحوه عملکردشان خواهیم پرداخت. تا به امروز، روش‌های گوناگونی در جهت تشخیص کرم‌واره‌ها و مقابله با آنها معرفی و بر روی شبکه و یا میزبان‌ها مورد استفاده قرار گرفته است. در ادامه این فصل، مروری بر روش‌های مختلف ارائه شده در این زمینه انجام گرفته است. همچنین در این بخش، دسته‌بندی‌های مختلف روش‌های تشخیص کرم‌واره‌ها را مورد بررسی قرار داده‌ایم.

از آنجا که این پایان نامه به تشخیص عملکرد کرم‌واره‌ها در شبکه‌های P2P می‌پردازد، نیاز داریم تا در ابتدا شبکه‌های P2P را بشناسیم. از این رو، فصل ۳ از این پایان نامه به معرفی شبکه‌های P2P می‌پردازد. تعریف و کاربرد این شبکه‌ها، همچنین ویژگی‌های آنها، مواردی هستند که در این فصل به آنها پرداخته شده است. در این فصل، در کنار شرح اطلاعات عمومی شبکه‌های P2P، برای روشن شدن بهتر چگونگی عملکرد آنها، یک پروتکل P2P با جزئیات بیشتری معرفی شده است.

در فصل ۴ به معرفی کرم‌واره‌های شبکه P2P پرداخته شده است. این بخش به شکل مفصلی نحوه عملکرد کرم‌واره‌های P2P را بررسی نموده و ویژگی‌های آنها را مورد کنکاش قرار می‌دهد. در ادامه فصل ۴، مروری بر تحقیقاتی که تا به امروز بر روی کرم‌واره‌ها در شبکه‌های P2P از جنبه‌های مختلف انجام شده است، صورت گرفته است.

فصول بعدی مربوط به روشهای پیشنهادی تشخیص کرم‌واره P2P در این پایان نامه می باشند. فصل ۵ به معرفی روش پیشنهاد شده برای تشخیص کرم‌واره P2P با استفاده از اطلاعات یک میزبان می‌پردازد. از جمله مواردی که در این فصل به شرح آنها پرداخته شده است، می‌توان به پارامترهای مورد استفاده در تشخیص کرم‌واره و چگونگی عملکرد الگوریتم آن، اشاره نمود. بخش انتهایی فصل نیز به نحوه پیاده سازی و تست الگوریتم پرداخته و نتایج به دست آمده را مورد بررسی قرار می‌دهد. در این روش، نرخ تشخیص، ۸۷ درصد و false positive، ۱۵ درصد بود.

ما در این پایان نامه برای تشخیص کرم‌واره‌های P2P به کمک همکاری میزبان‌ها، از روش‌هایی برای بررسی شباهت الگوها استفاده کرده‌ایم. به عبارت دیگر، در روش پیشنهادی ما گره‌های همسایه الگوهایی از وضعیت داخلی خود را با هم مبادله می‌کنند، که این الگوها باید به کمک تکنیک‌هایی با هم مقایسه شوند. از این رو، در فصل ۶، ما به بررسی پیچش پویای زمانی و تبدیل فوریه سریع که روش‌هایی هستند که برای بررسی شباهت الگوها در سیستم تشخیص کرم‌واره‌های P2P مناسب بوده و به منظور استفاده در این پایان نامه انتخاب شده‌اند، پرداخته‌ایم.

فصل ۷، روشی را که این پایان نامه برای همکاری میزبان‌ها در تشخیص کرم‌واره‌های P2P پیشنهاد کرده است، معرفی می‌کند. در این فصل نیز مانند فصل گذشته، پارامترهای تشکیل‌دهنده الگوی وضعیت میزبان‌ها که

برای تشخیص کرم‌واره مورد استفاده قرار می‌گیرند، شرح داده می‌شوند. همچنین روش‌هایی که برای بررسی تطابق الگوهای گره‌های شبکه به کاربرده شده‌اند، بحث خواهند شد. در انتهای فصل نیز چگونگی پیاده سازی روش‌ها و نتایج به دست آمده از آنها، همچنین مقایسه نتایج آنها با کارهای چاپ شده قبلی آورده شده است. در این روش، نرخ تشخیص، ۹۵ درصد و false positive، ۵ درصد بود که نشان دهنده بهبود نتایج پس از استفاده از همکاری گره‌ها می باشند.

در فصل انتهایی نیز به جمع بندی و بحث در مورد این پایان نامه و روش تشخیص کرم‌واره‌های P2P پیشنهاد شده در آن خواهیم پرداخت.

فصل ۲

کرم‌واره ها و روش‌های تشخیص آنها