Study and Developing a Network Security Prototype Based on Agent Technology

Najla Badie Ibraheem **Haleema Essa Sulaiman**

College of Computer Sciences and Mathematics
University of Mosul, Mosul, Iraq

Received on: 23/10/2011 **Accepted on: 15/02/2012**

ABSTRACT

A preliminary prototype has been designed and implemented in this work to support network security that used to detect a misuse in the network environment, the events have been taken from KDD, so three types of attacks have been taken on TCP, UDP, and ICMP connections. The prototype design is based on the Agent Technology and using the JADE platform, which is a platform used as a requirement for Multi_agent systems. The used Multi_agent system is of a closed type (Closed Multi_agent System); this is due to the fact that the used agents in this system (mobile and static agents) have been defined and declared in advance, JADE Add-Ons Services have been used to provide additional features that could be used to support the proposed security prototype, like using Inter_Platform Migration Service (IPMS), and JADE Security Add-On (JADE_S).

Through the work a test has been achieved for the ability of the prototype scalability with low network latency.

Keywords: network security, misuse intrusion detection, KDD data set, agent technology, multi_agent system, mobile agent, security add_on service.

دراسة وتطوير نموذج أمنى للشبكة باستخدام تقنية الوكيل

نجلاء بديع إبراهيم ***حليمة عيسى سليمان***

كلية علوم الحاسوب والرياضيات
جامعة الموصل، الموصل، العراق

تاريخ استلام البحث: 2011\10\23 **تاريخ قبول البحث: 2012\02\15**

الملخص

تم في هذا العمل تصميم وتنفيذ نموذج أولي (Prototype) داعم لأمنية الشبكة يعمل على كشف سوء الاستخدام (Misuse Detection) في بيئة الشبكة، والأحداث قد تم أخذها من قائمة ال KDD، إذ تم اخذ ثلاث أنواع من الهجمات التي تحدث على TCP وUDP وICMP. تم تصميم النظام بالاعتماد على تقنية الوكيل (Agent Technology) وباستخدام المنصة JADE وهي إحدى متطلبات أنظمة الوكيل المتعدد (Multi_Agent Systems)، ونظام الوكيل المتعدد المستخدم هو من النوع المغلق (Closed Multi_Agent System) لكون الوكلاء المستخدمين في النظام (الوكيل المتنقل والوكلاء الثابتين) قد تم تعريفهم وتحديدهم مسبقاً ولا يجوز إدخال وكيل عشوائي إلى النظام، تم استخدام خدمات إضافية للمنصة JADE (Add-ons Services) لتوفير خصائص إضافية يمكن الاستفادة منها لدعم النموذج الأمني المقترح، مثل استخدام خدمة التنقل بين

المنصات المختلفة ((Inter_Platform Migration Service (IPMS))، وخدمة الأمنية الخاصة بالمنصة JADE ((JADE Security Add-On (JADE_S)).

من خلال العمل تم اختبار قابلية النموذج على التوسع (Scalability) وبأقل تأخير ممكن في الشبكة (Low Network Latency).

الكلمات المفتاحية: امنية الشبكة، كشف سوء الاستخدام، قائمة البيانات، تقنية الوكيل، انظمة الوكيل المتعدد، الوكيل المتنقل، خدمة الامنية الاضافية.

1- المقدمة

التطور السريع لحقل أمنية المعلومات في السنوات الأخيرة قد ازداد مع ازدياد تطور استخدام معالجة البيانات الالكترونية وتوسعها، ومع نمو التطبيقات التجارية من خلال الشبكة العنكبوتية (الانترنت) وشبكات الحاسوب الأخرى. في الوقت نفسه، فان أدوات المتطفل والمهاجم في تطور مستمر. ولمقاومة الأعداد المتزايدة من الهجمات، وللمحافظة على خدمات المعلومات المهمة، قامت مجموعات أكاديمية وتجارية بتطوير أنظمة لمراقبة الشبكات والتنبيه حال وجود فعالية أو نشاط مشتبه به. تدعى هذه الأنظمة بأنظمة كشف التطفل (Intrusion Detection Systems)(IDSs).

أنظمة كشف التطفل لا تلغي دور آليات المنع، وإنما تعمل بوصفها آلية دفاع ثانية وراء جدار النار، إذ تقوم بمراقبة الشبكة بدون التأثير في أدائها. وبالنتيجة فان نظام كشف التطفل هو العملية التي تقوم باكتشاف، ومراقبة، وتعقب، وتحديد الوصول غير المخول والفعاليات الشاذة أو الأحداث في النظام. وعند اكتشافه لإحدى هذه الحالات فانه يسجل الحدث ويعطي إنذاراً لمدير النظام للقيام بالفعل المناسب [22].

هناك العديد من الطرائق والنماذج الجديدة لأنظمة كشف التطفل قد تم تطويرها، ولكن على الرغم من التطويرات المقدمة، فإن قسماً من نقاط الضعف الموجودة في الطرائق السابقة لا تزال موجودة، مثل: دقة الكشف تكون واطئة، وانجاز الوقت الحقيقي يكون واطئاً، وقابلية التوسيع تكون محدودة. هذه المشاكل جعلت منطقة أنظمة كشف التطفل حقلاً جذابًا ومفتوحاً للبحث. وفي السنوات الأخيرة قام الباحثون بتقديم أدوات جديدة لتحسين أداء أنظمة كشف التطفل وتجاوز بعض المحددات [8,23]، وإحدى هذه الطرائق هي استخدام الوكيل المستقل (Autonomous Agent) في هذه الأنظمة [22].

يعد تطبيق الوكيل المتنقل (Mobile Agent) في تصميم أنظمة كشف التطفل تطوراً حديثاً، ويهدف إلى أن يكون كشف التطفل فعالاً في البيئة الموزعة.

الوكيل المتنقل عبارة عن كائن برمجي يعمل بصورة مستمرة ومستقلة في بيئة عملية وقادر على إنجاز الفعاليات بطريقة مرنة وذكية وقابلة للاستجابة لتغييرات البيئة.

تم استخدام الوكيل المتنقل في أنظمة كشف تطفل مختلفة، ففي عام 2004، قام الباحث محمد عايد [17]، بتقديم نظام كشف تطفل موزع بالاعتماد على الوكيل المتنقل، الذي يقوم بكشف التطفل القادم من خارج الشبكة فضلاً عن كشف التطفل الموجود داخل الشبكة. مراقبة النظام يتم السيطرة عليها من قبل نظام كشف التطفل باستخدام الوكلاء المتنقلين، إذ سيقومون بعملية جمع معلومات التطفل وإرسالها إلى المحطة الرئيسة للتحليل. النظام يظهر الأداء المتفوق مقارنة بأنظمة كشف التطفل المركزية، فضلاً عن توفيره لمصادر الشبكة مقارنة مع أنظمة كشف التطفل الموزعة التي تقوم بتوزيع آليات المراقبة مما يؤدي إلى حصول العديد من الاختناقات في الشبكة.

وفي عام 2006، قام الباحث (Asha Nagesh) [6]، بتقديم نظام تتألف معماريته الموزعة من مجموعة من الوكلاء المستقلين الذين يتنقلون من وإلى الأنظمة الأخرى بشكل انتقائي لجمع معلومات عن حركة مرور الشبكة، وتحليلها، وإرجاع النتائج التي ستعرض على واجهة مستخدم واحدة. في عام 2006، قام الباحث (محمد عويس شبلي) [19]، بتقديم نظام أمني معتمداً على الوكيل المتنقل. النظام يصور كيفية استخدام أدوات وطرائق مختلفة سوية لإنجاز المهمة المحددة للأجزاء الوظيفية للنظام الأمني أي تحليل الثغرات، وكشف التطفل، والاستجابة للتطفل، ومهمة إدارة الأمنية، على الرغم من أن هذا النظام حقق هدفه بنجاح، لكن حلوله لا تزال تعتمد على إدارة أمنية مفردة، مما يؤدي إلى مشكلة نقطة الفشل المفردة.

الوكيل المتنقل بطبيعته مستقل، ومتعاون، وينظم نفسه تلقائيا، وهذه الصفات غير موجودة في أنظمة كشف التطفل المركزية السابقة.

من أهم فوائد استخدام الوكيل المتنقل لدعم أمنية الشبكة:

- التغلب على التأخير الحاصل في الشبكة.
- تقليل الحمل على الشبكة.
- الاستقلالية والتنفيذ غير المتزامن.
- التكيف الديناميكي.
- القوة والقابلية على احتمال الخطأ.
- قابلية التوسيع [3].

يمكن إيجاز أهم الأهداف للبحث بالنقاط الآتية:

1. تناول عدد من الأدوات المستخدمة لتطوير العميل وإجراء المقارنة بينها لاختيار الأداة الأفضل من بين هذه الأدوات، ومن ثم تسخير هذه الأداة لتصميم وتنفيذ النموذج الأولي المقترح، والأداة التي تم اختيارها في العمل هي المنصة JADE [25].
2. استخدام عدد من العملاء في النظام (أي تكوين نظام عميل متعدد)، بحيث يكون لكل عميل مهمة معينة يقوم بها، بالإضافة إلى ضرورة وجود تعاون (اتصال) بين العملاء المستخدمين.
3. لحماية الرسائل التي سيتم تناقلها بين العميل المتنقل وعملاء الاسترجاع والمقارنة المستخدمين في النظام سيتم استخدام الخدمة الإضافية (خدمة الأمنية الخاصة بالمنصة JADE)، حيث سيتم استخدام خدمة التوقيع وخدمة التشفير للرسائل المتناقلة.
4. سيتم تنفيذ النظام باستخدام خدمة التنقل ضمن المنصة الواحدة، بالإضافة إلى تنفيذه باستخدام الخدمة الإضافية (خدمة التنقل بين المنصات المختلفة) ومقارنة النتائج التي سيتم الحصول عليها من خلال التجارب التي سيتم إجراءها في البحث لاختبار قابلية النظام على التوسع وبأقل تأخير ممكن في الشبكة.

2- أنواع الوكلاء

يعرض المقطع الآتي الأنواع المختلفة من الوكلاء:

أ- وكلاء التعاون Collaborative Agents

يركز وكلاء التعاون على الاستقلال والتعاون (مع وكلاء آخرين) لتحقيق مهام مالكيها. قد يتعلم الوكلاء ولكن لا يعد هذا تأكيداً نموذجياً على العملية التي يقومون بها. وللاستحواذ على إعداد مجموعة متعاونة من الوكلاء المتعاونين قد يتوجب عليهم التفاوض لكي يتم التوصل إلى اتفاقيات مقبولة على بعض الأمور.

ب- وكلاء التواصل Interface Agents

إن المفتاح المجازي لوكلاء التواصل هو المساعد الشخصي (Personal Assistant)، الذي يتعاون مع المستخدم في بيئة العمل نفسها.

ج- وكلاء المعلومات والشبكة المعلوماتية Information/Internet Agents

ظهر هذا النوع من الوكلاء بسبب الحاجة الماسة للوسائل التي تسهم في إدارة المعلومات التطورية الهائلة التي نكتسب فيها الخبرة حالياً والتي سنستمر في اكتسابها فيما بعد. ويقوم وكلاء المعلومات بدور الإدارة، والتعامل وفحص المعلومات من عدة مصادر موزعة.

د- وكلاء برمجيات التفاعل Reactive Software Agents

يمثل وكلاء برمجيات التفاعل نوعاً خاصاً من الوكلاء الذين لا يمتلكون نماذج داخلية أو رمزية من بيئاتها، وبدلا من ذلك فهم يستجيبون بطريقة تحفيزية إلى الوضع الحالي من البيئة المحيطة بهم.

هـ- الوكيل الهجين Hybrid Agents

بما أن لكل نوع من أنواع الوكيل نقاط قوة ونقاط ضعف، فان الهدف الأساس عادة هو الوصول إلى الحد الأعلى من نقاط القوة والحد الأدنى من نقاط الضعف لكل تقنية ذات علاقة لتحقيق أهداف خاصة[2,5,15,16].

و- الوكلاء المتنقلون Mobile Agents

الوكيل المتنقل عبارة عن برنامج حاسوبي مستقل يعمل على خدمة مصلحة الكائن (Entity)، ويعمل على الهجرة بين مواقع متباينة في الشبكة، وتنفيذ المهام المحلية واستمرار التنفيذ في النقطة التي توقف بها قبل عملية الهجرة. كما أن الوكيل المتنقل يمكنه أن يمتلك ميزات مثل الذكاء والقابلية على التعاون [4,10].

تعد بيئة الوكيل المتنقل نظاماً برمجياً موزعاً عبر الشبكة المكونة من حواسيب غير متجانسة. وتعد مهمتها الأساسية في تجهيز بيئة ما، إذ ينفذ الوكلاء المتنقلون وظائفهم. وتُنفذ غالبية النماذج التي يمتلكها الوكيل المتنقل.

- **دورة حياة الوكيل المتنقل**

إن دورة حياة الوكيل المتنقل تمر بالمراحل الآتية:

- التكوين (Creation): تكوين وكيل جديد وتهيئة حالته.
- الترحيل (Dispatch): انتقال الوكيل إلى مضيف جديد.
- الاستنساخ (Cloning): تكوين نسخة وتُضاعف الحالة الحالية من الوكيل الأصل في عملية الاستنساخ.
- التوقف أو عدم الفعالية (Deactivation): يكون الوكيل في وضع الرقود (Sleep) فتخزن حالته على القرص الجهاز.
- التفعيل (Activation): يسترد الوكيل حياته ويعيد تفعيل حالته من القرص.
- الاسترداد (Retraction): يعاد الوكيل من الجهاز البعيد مع حالته إلى جهاز الحاسوب الأم.
- الانتهاء (Disposal): ينتهي الوكيل وتضيع حالته إلى الأبد [9,11,12,21].

3- أدوات تطوير الوكيل Agent Toolkits

يتطلب تطوير الوكلاء واستخدامهم على نطاق واسع بنية تحتية كامنة جيدة. إن ندرة أدوات تنمية الوكيل في السنوات الأولى من البحوث حدت من استغلال هذه التكنولوجيا المفيدة. لكن اليوم هناك تشكيلة واسعة من الأدوات المتاحة لتطوير بنية تحتية متينة.

وفقاً للتقرير الذي تقدم به (Nguyen Dang) [20]، هناك أكثر من 100 نوع من المنتجات في هذه الفئة. تم التركيز على أدوات العمل الأكثر فعالية من بين الخيارات المتاحة وهي كالآتي:

- IBM-Aglet or Aglet Software Development Kit (ASDK) [14].
- Voyager [13].
- JADE [7].
- Anchor [18].
- Zeus [20][1].

يقارن الجدول الآتي الأدوات أعلاه بالاعتماد على الميزات الرئيسة التي يمكن أن توثر في تطبيقها.

جدول (1): مقارنة بين الأدوات المستخدمة لتطوير الوكيل

أدوات تطوير الوكيل ← / الميزات ↓	Aglet	Voyager	JADE	Anchor	Zeus
طبيعة المنتج	متوفر، مفتوح المصدر	تجاري	متوفر، مفتوح المصدر	متوفر في رخصة BSD	متوفر، مفتوح المصدر
تقنية الاتصال	متزامن وغير متزامن	كل الطرائق	غير متزامن	غير متزامن	غير متزامن
آلية الأمن	ضعيف	ضعيف	جيد	أمنية قوية	جيد
عامل التنقل	ضعيف	ضعيف	فيه نوع من الضعف	ضعيف	لا تتوفر
آلية الهجرة	المقبس	RMI	RMI	المقبس	لا يوجد
الاستخدامات العملية	الأسواق الالكترونية لتذاكر الطائرات في اليابان	بناء تطبيقات جافا الموزعة التي تستغل مصادر الإدخال والإخراج الرسومية المتنوعة مثل الهواتف المتنقلة iphone	عدد من الجامعات والشركات، ومختبرات الأبحاث التجارية والتقنية، والتطبيقات التجارية والالكترونية، وفي الانترنت والشبكات اللاسلكية	التطبيقات التجارية، والتطبيقات الطبية	شركات الأنظمة التجارية الذكية، وشركات التجارة الالكترونية

بعد إجراء عملية المقارنة بين خمس من الأدوات المستخدمة لتطوير الوكيل اتضح أن المنصة JADE تبدو أكثر جاذبية من البقية لاحتوائها على الميزات الأساسية والضرورية في منصات العمل، فهي مفتوحة المصدر، مصممة كلياً باستخدام الجافا، وتوفر الاتساق في API (Application Programming Interface) وتدعم أنواعاً مختلفة من الأجهزة العاملة في شبكة الإنترنت، أيضاً توفر ميزات أمنية جيدة وتدعم حركة الوكيل وتنقله، وتتفق مع FIPA (The Foundation for Intelligent Physical Agent)، فضلاً عن الاستخدامات

المتعددة لهذه المنصة في المجالات العلمية، والأعمال التجارية، والإنترنت. في حين أن الأدوات الأخرى تدعم بعض الميزات.

4- معلومات أساسية عن JADE Background to JADE

JADE هي منصة متعددة الوكلاء، ممثلة كلياً باستخدام لغة الجافا، ومطابقة لمعايير الـ FIPA لوكلاء البرمجيات الذكية. JADE يصدر مجموعة من حزم الجافا لتطوير تطبيقات الوكيل في المنصة. الفقرات الآتية تصف صفات الـ JADE وميزاتها:

- **حاويات الوكيل (Agent containers):** حاوية الوكيل توفر بيئة تنفيذية، إذ يمكن لعدد من الوكلاء أن يكونوا فعالين في الحاوية نفسها. ومنصة الوكيل ممكن أن توزع على أكثر من جهاز، وحاوية معينة أساسية (Main Container) تُعد بوصفها مسيطرة على المنصة، إذ يوفر JADE واجهة عمل رسومية للحاوية الأساسية التي من خلالها يستطيع مدير المنصة أن يدير الحاويات جميعها المحلية والبعيدة والوكلاء المتواجدون في هذه المنصة، فضلاً عن القيام ببعض الأعمال مثل إنشاء هذه المكونات أو مسحها.

توفر JADE خدمات للنظام متوافقة مع الـ FIPA مثل التسمية (Naming)، وخدمة الصفحة الصفراء (Yellow-Page)، ونقل الرسائل، والاتصال بين الوكلاء، الخ.

- **سلوكيات الوكيل (Agent Behaviours):** أعمال الوكيل تنفذ من خلال امتدادات الصنف Behaviour. وممكن أن ينفذ الوكيل عدداً من السلوكيات، كل سلوك يقابل وظيفة معينة للوكيل، ويمكن تنفيذ دالة العمل الرئيسة للسلوك عدة مرات.

يتضمن JADE جدولة تقوم بتنفيذ تلك السلوكيات بطريقة(Round-Robin) ، إذ لا يوجد أي قطع (Preemption)، لذلك كل سلوك يمتلك السيطرة بشكل صريح، وهذا ما يحدث بالفعل عن طريق وصوله إلى نهاية عمله. بمجرد عودة وظيفة العمل، سيستفسر المجدول عن الوظيفة المنجزة للسلوك لمعرفة ما إذا كان يحتاج إلى إعادة جدولته، ومن ثم يتم تنشيط سلوك آخر.

- **رسائل الوكيل (Agent Messages):** يوفر JADE تطبيق نموذج FIPA الكامل. والاتصال بين الوكلاء يكون مخفياً بشكل كبير عن المطور، ورسائل الوكيل تعرف باستخدام الصنف (ACL Message)، الذي يحتوي على مجموعة من الصفات المعرفة من قبل الـ FIPA. الرسائل التابعة للوكيل كلها توضع في طابور خاص للرسائل لكي يتم تسليمها.
- **هجرة الوكيل (Agent Migration):** إن هجرة الوكيل في السلوك تتم من خلال دالة (doMove) التي تغلف كيان الجافا وتنقله إلى الحاوية التالية. يوفر JADE التنقل الضعيف (Weak Mobility) إذ لا يمكن نقل حالة التنفيذ (Execution State). تنفيذ الوكيل في الحاوية الهدف (Destination Container) يستأنف من نقطة محددة مسبقاً (في بداية السلوك) في الوكيل [24].

5- خوارزمية العمل للنموذج المقترح Algorithm For The Proposed Prototype

الهيكل العام للنموذج الأولي يتكون من العناصر الآتية: وكلاء بناء الجداول، وكلاء الاسترجاع والمقارنة، الوكيل المتنقل. والشكل (1) يوضح كيفية استخدام هذه العناصر في العمل.

إن التنفيذ الأولي لنظام النموذج المقترح تم بالاعتماد على التنقل الأوتوماتيكي للعميل المتنقل في حواسيب الشبكة كلها، والطريقة الثانية لتنفيذ النظام تمت باعتماد أسلوب جديد للتنفيذ يكون التنفيذ السابق مضمّناً فيه، إذ سيتم اختيار الحاسوب التالي الذي سينتقل إليه العميل المتنقل يدوياً من قبل منفذ النظام.

فالتنفيذ بالاعتماد على التنقل الأوتوماتيكي للعميل وباستخدام خدمة التنقل بين المنصات المختلفة (JADE IPMS Service) سيتم بالخطوات التالية:

الخطوة الأولى: تثبيت العناوين المنطقية (IPs) لكل الحاسبات التي سينتقل إليها العميل المتنقل وهذه العناوين ستخزن في جدول يسمى itinerary والذي سيحوي على مواقع الحاسبات (المنصات) التي سينتقل إليها العميل المتنقل.

الخطوة الثانية: يتم إطلاق العميل المتنقل، والذي سينتقل إلى المنصة الأولى ثم الثانية...وهكذا حسب العناوين الموجودة في الجدول itinerary وفي كل عملية انتقال ستكون هنالك زيادة بمقدار واحد لقيمة عداد خاص بعدد المواقع التي سينتقل إليها العميل المتنقل وهذا العداد هو hopcount.

الخطوة الثالثة: فحص الحالة الحالية للعميل المتنقل ومعرفة فيما إذا كان في حالة الانتقال وجمع المعلومات أم انه في حالة عرض النتائج عن طريق مقارنة قيمة hopcount مع حجم الجدول itinerary.

أ. إذا كانت النتيجة مطابقة (أي بمعنى أن العميل المتنقل قد انتقل إلى جميع المنصات المطلوب الانتقال إليها)، ستتغير حالته إلى حالة عرض النتائج، عندئذ سيقوم العميل المتنقل بعرض النتائج على الشاشة.

ب. أما إذا كانت النتيجة غير مطابقة فان العميل المتنقل سيبقى في حالة الانتقال والمعالجة، وسيقوم بالانتقال إلى المنصة التالية، بالإضافة إلى أن قيمة العداد hopcount ستزداد بمقدار واحد وسيقوم العميل المتنقل باستلام النتائج من عميل الاسترجاع والمقارنة الموجود في المنصة الحالية.

الخطوة الرابعة: عند انتهاء العميل المتنقل من التنقل إلى جميع المنصات سيتوقف وتنتهي حياته.

أما الطريقة الثانية للتنفيذ وهي اعتماد التنقل اليدوي للعميل وباستخدام خدمة التنقل ضمن المنصة الواحدة فان خطوات تنفيذ النظام ستكون كالآتي:

الخطوة الأولى: تشغيل الوكيل المتنقل في الحاسوب الرئيس والذي عند تشغيله سيقوم بإرسال طلب إلى نظام إدارة الوكيل لغرض الحصول على قائمة بالحاويات الفعالة في النظام.

الخطوة الثانية: تشغيل الوكيلين الثابتين المسؤولين عن تكوين جداول الأحداث في كل حاسوب.

الخطوة الثالثة: تشغيل الوكيل الثابت المسؤول عن استرجاع المعلومات من الجداول المكونة في الخطوة الثانية، إذ سيقوم الوكيل بمقارنة هذه الجداول وعرض النتائج التي تم الحصول عليها على الشاشة الخاصة بكل حاسوب.

الخطوة الرابعة: قيام الوكيل المتنقل بجمع المعلومات الخاصة بالحاسوب الرئيس، إذ سيأخذ هذه المعلومات من الوكيل الثابت المسؤول عن إجراء عملية المقارنة.

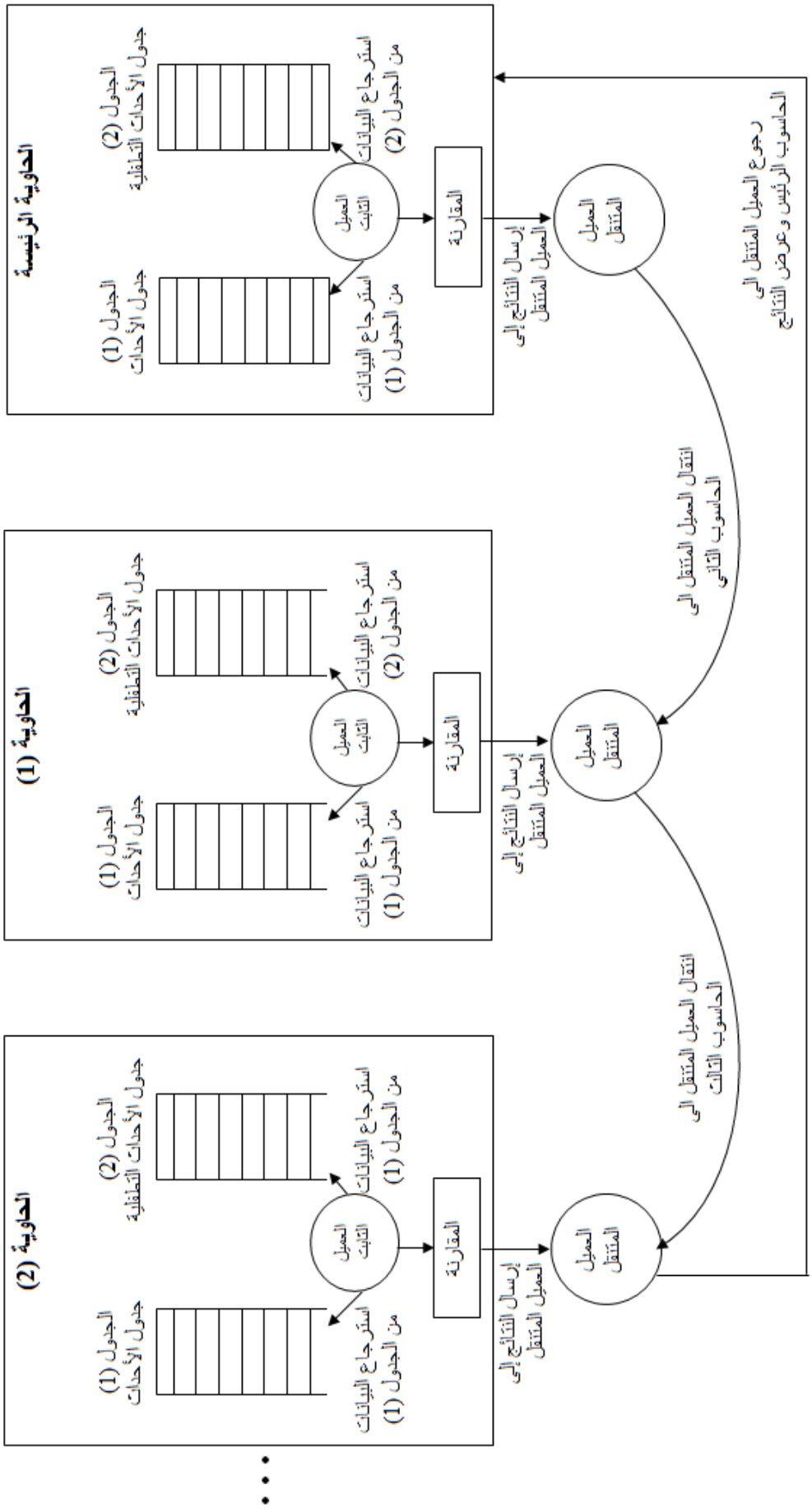
الخطوة الخامسة: إطلاق الوكيل المتنقل إلى الحاسوب التالي وسوف يقوم بجمع المعلومات من الوكيل المسؤول عن إجراء عملية المقارنة في ذلك الحاسوب.

الخطوة السادسة: تكرار الخطوة الخامسة في الحواسيب كلها الموجودة في الشبكة.

الخطوة السابعة: إرجاع النتائج المجموعة من حواسيب الشبكة كلها إلى الحاسوب الرئيس.

الخطوة الثامنة: عرض النتائج على شاشة الحاسوب الرئيس.

الخطوة التاسعة: يتوقف الوكيل المتنقل.



الشكل(1): الهيكلية العامة للنموذج المقترح

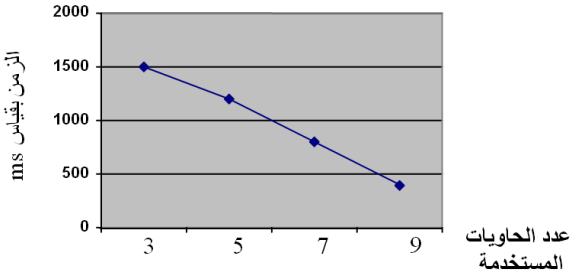
6- اختبار قابلية النموذج للتوسع Testing The Scalability of a Prototype

باستخدام تقنية الوكيل في النظام يمكن إثبات أن النظام قابل للتوسع وبأقل تأخير ممكن في الشبكة وفقاً للتجربة التالية التي اعتمدت المنصة JADE والمحرر Eclipse:

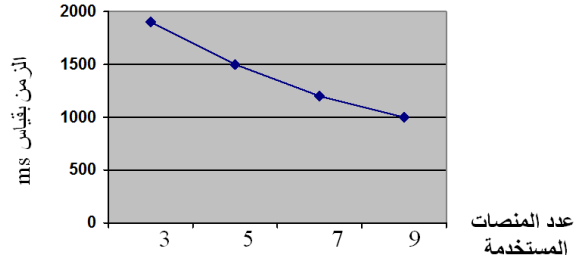
تم تنفيذ التجربة باستخدام التنقل الأوتوماتيكي للعميل حيث أن منفذ النظام لا يتدخل بتنقل العميل بين الحاويات أو بين المنصات وإنما فقط سيقوم بتجهيز العناوين للمنصات أو الحاويات التي سينتقل إليها العميل المتنقل، بعد ذلك سيقوم العميل المتنقل بالتنقل الأوتوماتيكي بين الحاويات أو المنصات المختلفة، تم تنفيذ هذه التجربة باستخدام خدمة التنقل ضمن المنصة الواحدة وباستخدام خدمة التنقل بين المنصات المختلفة.

ملاحظة: عملية تشغيل العداد الخاص بالوقت تتم في بداية كل خطوة، وعملية إيقاف العداد تتم في نهاية كل خطوة؛ وذلك للحصول على الوقت الكلي المستغرق في كل خطوة من خطوات الاختبار.

سيتم استخدام ثلاث حاويات (في حال استخدام خدمة التنقل ضمن المنصة الواحدة)، أو ثلاث منصات (في حال استخدام خدمة التنقل بين المنصات المختلفة)، ثم سيتم استخدام خمسة ثم سبعة ثم تسعة حاويات أو منصات، وسيتم حساب الوقت المستغرق لانتقال العميل بين الحاويات أو المنصات في كل مرة، والنتائج التي تم الحصول عليها موضحة في المخطط البياني –الشكل (2)– في حالة استخدام خدمة التنقل ضمن المنصة الواحدة ، والمخطط البياني –الشكل (3)– يوضح النتائج المستحصلة عند استخدام خدمة التنقل بين المنصات المختلفة.



الشكل (2): التنفيذ باستخدام خدمة التنقل ضمن المنصة الواحدة



الشكل (3): التنفيذ باستخدام خدمة التنقل بين المنصات المختلفة

7- مناقشة النتائج Results Discussion

من خلال النتائج التي تم الحصول عليها من التجارب أعلاه، يمكن استنتاج ما يلي:

1. الوقت المستغرق لانتقال العميل المتنقل في حالة تطبيق التجربة باستخدام خدمة التنقل ضمن المنصة الواحدة هو اقل من الوقت المستغرق عند تطبيقها باستخدام خدمة التنقل بين المنصات المختلفة.

2. من خلال النتائج التي تم الحصول عليها من هذه التجارب يمكن ملاحظة أن للنظام القابلية على التوسع وبأقل تأخير ممكن في الشبكة. وتُعد هذه من الفوائد المهمة لاستخدام العميل المتنقل في التطبيقات الموزعة، ولاسيما في أنظمة كشف التطفل.

8- الاستنتاجات Conclusions

من خلال تصميم النموذج الأمني وتنفيذه في البحث لغرض كشف التطفل المعتمد على الشبكة ووفق النتائج التي تم الحصول عليها، نستنتج ما يأتي:

1. بعد الاطلاع على مفاهيم تقنية الوكيل وميزاتها والفوائد التي تقدمها لأنظمة كشف التطفل اتضح أن استخدام هذه التقنية ونخص بالذكر استخدام الوكيل المتنقل الذي هو عبارة عن نوع خاص من أنواع الوكيل البرمجي يعد الأكثر ملائمة لحل مشاكل أنظمة كشف التطفل في البيئة الموزعة لما له من ميزات مهمة مثل التنقل والقابلية على التعاون مع الوكلاء الآخرين، فضلاً عن خاصية استقلاله عن مُنفذ النظام. وتقديمه فوائد عديدة لهذه الأنظمة مثل تقليل الزخم الحاصل في الشبكة، وتقليل التأخير بالوقت في الشبكة، والقابلية على التوسع، أضف إلى ذلك إعطاء الإمكانية للنظام للقدرة على احتمال الخطأ. كل هذه الميزات والفوائد جعلت من استخدام الوكيل المتنقل في أنظمة كشف التطفل تطورا هائلا يهدف إلى جعل نظام كشف التطفل فعالاً في البيئة الموزعة.
2. إن استخدام المنصة JADE كأداة لتصميم الوكيل وتنفيذه في العمل وفر الخدمات الأساسية كلها لجعل النظام يستخدم نموذج الاتصال الند_للند الموزع، إذ سيُسمح لكل وكيل باكتشاف الوكلاء الآخرين من خلال تقديم الطلبات إلى نظام إدارة العميل، والاتصال بالوكلاء باستخدام الرسائل غير المتزامنة، ويُعد نموذج الاتصال هذا بصورة عامة الأكثر قبولا في الأنظمة الموزعة.
3. باستخدام المنصة JADE والمكتوبة كلياً بلغة الجافا، يتم الاستفادة وبشكل كبير من الصنف (Behaviour) لتنفيذ مهام النظام، إذ أن كل وكيل سيمثل بمسلك واحد ويمكن للوكيل انجاز عدة مهام باستخدام هذا الصنف، فيمكن للوكيل تنفيذ أكثر من Behaviour ضمن المسلك الواحد.
4. إن استخدام الخدمة الإضافية (خدمة الأمنية الخاصة بالمنصة JADE) قد وفر الحماية للرسائل التي تم تناقلها بين عملاء النظام، إذ تم التحقق من هوية العميل المرسل (باستخدام خدمة التوقيع)، بإضافة إلى أن العميل المستلم الحقيقي هو فقط من سيستطيع قراءة الرسالة بصورة واضحة (باستخدام خدمة تشفير الرسائل).

إن تنفيذ النظام باستخدام الخدمة الإضافية (خدمة التنقل بين المنصات المختلفة)، قد أعطى الإمكانية لإجراء مقارنة بين النتائج التي تم الحصول عليها من هذا التنفيذ ونتائج تنفيذ النظام باستخدام خدمة التنقل ضمن المنصة الواحدة من خلال التجارب التي تم تنفيذها في النظام.

REFERENCES

[1] Aarti Singh, Dimple Juneja, A.K. Sharma, 2011, "Agent Development Toolkits", Y.M.C.A University of Science and Technology, Faridabad, Haryana, India, International Journal of Advancements in Technology, Vol 2, No 1.

[2] Abdelkader Outtagarts, 2009, "Mobile Agent-based Applications: a Survey", Alcatel-Lucent Bell Labs, IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.11.

[3] Adesina Simon Sodiya, 2006, "Multi-level and Secured Agent-Based Intrusion Detection System", Journal of Computing and Information Technology, p 217–223.

[4] Anand Tripathi, Tanvir Ahmed, Sumedh Pathak, Megan Carney, and Paul Dokas, 2001, "Paradigms for Mobile Agent-Based Active Monitoring of Network Systems", University of Minnesota, supported by National Science Foundation grants ANIR 9813703.

[5] Andrew S.Tanenbaum and Maarten van Steen, 2002, "Distributed Systems Principles and Paradigms" (International Edition), Prentice Hall , Inc.

[6] Asha Nagesh, Graduate Student, 2006, "Distributed Network Forensics Using JADE Mobile Agent Framework", Arizona State University, Division of Computing Studies, Sutton Hall.

[7] Bellifemine F., Caire G., Poggi A. and Rimassa G., 2003, "JADE: A White Paper", Available at http://exp.telecomitalialab.com , exp, vol. 3, No. 3.

[8] Bivens, C. Palagiri, R. Smith, B. Szymanski, and M. Embrechts, 2002, “Network-Based Intrusion Detection Using Neural Networks”, Technical Report, Rensselaer Polytechnic Institute, Troy, New York.

[9] D.G.A. Mobach, B.J. Overeinder, N.J.E. Wijngaards, and F.M.T. Brazier, 2002, "Managing Agent Life Cycles in Open Distributed Systems", IIDS Group, Department of Artificial Intelligence, Vrije Universiteit Amsterdam, de Boelelaan 1081a, The Netherlands.

[10] Emerson Ferreira de Araujo Lima, Patricia Duarte de Lima Machado, 2002, "Implementing Mobile Agent Design Patterns in The JADE Framework", http://leap.crm-paris.com/.

[11] F.M.T. Brazier, D.G.A. Mobach, B.J. Overeinder, and N.J.E. Wijngaards, 2003, "Supporting Life Cycle Coordination in Open Agent Systems", IIDS Group, Department of Artificial Intelligence, Vrije Universiteit Amsterdam, The Netherlands.

[12] Fabio Bellifemine, Giovanni Caire, Tiziana Trucco, 2010, "JADE Programmer's Guide" (TILAB, CSELT), Giovanni Rimassa (University of Parma), Telecom Italia.

[13] George J. Valentino J. G., Kniola T., Khalil S., 2007, "An Agents Toolkit to Support Distributed Simulations", Available online at http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.43.9252.

[14] Horvat D. , Cvetkovic D., Milutinovic V., Kocovic P. and Kovacevic V., 2000, "Mobile Agents and Java Mobile Agents Toolkits", Proceedings of the 33rd Hawaii IEEE International conference on System Sciences (HICSS), Maui, Hawaii, USA.

[15] Hyacinth S. Nwana, 1996, "Software Agents: An Overview", Knowledge Engineering Review, Cambridge University Press, Vol. 11, No 3, pp.1-40.

[16] Meenakshi1, Mona Sehgal2 and Payal Anand, 2010, "A Framework on Typology of Tware Agents, International Journal of Information Technology and Knowledge Management, Volume 2, No. 2, pp. 251-254.

[17] Mohamad Eid, 2004, "A New Mobile Agent-Based Intrusion Detection System Using Distributed Sensors", American University of Beirut, Department of Electrical and Computer Engineering.

[18] Mudumbai S.S., William J. and Abdelliah E., 1999, "Anchor Toolkit- A Secure Mobile Agent System", eScholarship, Available at http://escholarship.org/uc/item/2594j56c.

[19] Muhammad Awais Shibli, 2006, "Building Secure Systems Using Mobile Agents", Master Thesis, Kungl Tekniska Högskolan, Stockholm, Sweden.

[20] Nguyen G., Dang T.T., Hluchy L., Laclavik M., Balogh Z.and Budinska I., 2006, "Agent Platform Evaluation and Comparison", Supported by Institute of informatics, Slovak Academy of Sciences.

[21] Parineeth M Reddy, 2002, "Mobile Agents Intelligent Assistants on The Internet", Indian Institute of Science, India.

[22] S. Snapp, J. Brentano, and G. Dias, 1991, “DIDS (Distributed Intrusion Detection System) Motivation, Architecture, and An Early Prototype”, Proceedings of the 14th National Computer Security Conference, University of California.

[23] Safaa Zaman, 2009, "A Collaborative Architecture for Distributed Intrusion Detection System based on Lightweight Modules",Ph.D. Thesis, University of Waterloo.

[24] Vandana Gunupudi and Stephen R. Tate, 2004, "SAgent: A Security Framework for JADE", University of North Texas, research supported by NSF award 0208640.

[25] http://jade.cselt.it.