# الدليل السيبراني المستمد من الذكاء الاصطناعي

الباحث/ حمد عبد الله علي مطر النيادي

(ISSN: 2537 - 0758)

# الدليل السيبراني المستمد من الذكاء الاصطناعي

الباحث/ حمد عبد الله علي مطر النيادي

## المقدمة

### ١. التعريف بموضوع البحث

يتطور مجال الذكاء الاصطناعي بسرعة مذهلة، فى منتصف الخمسينات ظهر الذكاء الاصطناعي جرى تعريفه على أنه "علم وهندسة تصنيع الآلات الذكية"، ومن الناحية النظرية فإن الذكاء الاصطناعي هو قدرة الآلة على إدراك بيئتها والاستجابة لها بشكل مستقل وأداء المهام التي تتطلب عادة الذكاء البشرى وعمليات صنع القرار، ولكن دون تدخل بشرى مباشر. أحد جوانب الذكاء البشرى هو القدرة على التعلم من تجربة، والتعلم الآلي هو تطبيق الذكاء الاصطناعي الذى يحاكى هذه القدرة ويمكن الآلات وبرامجها من التعلم، وهو أمر مهم بشكل خاص من منظور العدالة الجنائية حيث ضرورة التعرف على الأنماط، فالبشر بارعون فى التعرف على الأنماط، ومن خلال التجربة، نحن نتعلم كيف نميز كلا من الأشياء، والناس، والإنسان بعواطفه المعقدة، والمعلومات، والظروف، وكل هذا يتم بشكل يومي. يسعى الذكاء الاصطناعي لتكرار هذه القدرة البشرية فى البرمجيات والخوارزميات وأجهزة الكمبيوتر، على سبيل المثال، تستخدم خوارزميات التوضيح الذاتي مجموعات البيانات لفهم كيفية تحديد الأشخاص على أساس صورهم، وفهم عاداتهم وأنماطهم على الإنترنت، واكتشاف سمات طبية من خلال المسح الإشعاعى المعقدة[١].

يمكن تطبيق الذكاء الاصطناعي- التعرف على الوجه- فى كل مكان فى كل من القطاعين العام والخاص، وغالبًا ما يعتمد محللو الاستخبارات على صور الوجه للمساعدة فى تحديد هوية الفرد ومكان وجوده، وتعد دراسة الحجم الكبير للصور ومقاطع الفيديو ذات الصلة بطريقة دقيقة وفى الوقت المناسب مهمة تستغرق وقتًا طويلاً ومضنية، مع احتمال حدوث خطأ بشرى بسبب التعب وعوامل أخرى، وعلى عكس البشر لا تتعب الآلات، لقد نجح الباحثون فى إجراء تجارب على استخدام الخوارزميات التي يمكن أن تتعلم كيفية التمييز بين شخص وآخر عن طريق استخدام ميزات الوجه

[1] John Searle, 'Can Computers Think?' in David J Chalmers (ed), Philosophy of Mind: Classical and Contemporary Reading, Oxford University Press, 2002, p. 669.

بنفس طريقة المحلل البشرى، وجرى تطبيق الذكاء الاصطناعي فى مجال الكشف التلقائى عن مخالفات المرور، كما يتم استخدام خوارزميات الذكاء الاصطناعي فى الطب لتفسير الصور الإشعاعية، والتي قد يكون لها آثار مهمة على العدالة الجنائية والطب الشرعى كما فى حالات تأسيس سبب وطريقة الوفاة، كما تم استكشاف خوارزميات الذكاء الاصطناعي فى مختلف التخصصات فى علوم الطب الشرعى، بما فى ذلك تحليل الحمض النووى، وأصبح الذكاء الاصطناعي تقنية مهمة سريعة فى كشف الاحتيال عبر الإنترنت، حيث جرى استخدام كميات كبيرة من البيانات لتدريب خوارزميات على الكشف عن الاحتيال بشكل مستمر، وعلى التنبؤ بالأنماط الشاذة والتعرف عليها وتعلم كيفية التعرف على الأنماط الجديدة[٢].

وقد أدخلت العديد من الدول نظام الذكاء الاصطناعي فى مجال العدالة الجنائية مثل الولايات المتحدة والمملكة المتحدة وعدد لا بأس به من دول الاتحاد الأوربى، وأنشأت دولة الإمارات العربية وزارة للذكاء الاصطناعي وبدأت فى تطبيقه فى المجال الشرطى، بينما منح القانون المصرى للأدلة الرقمية ذات الحجية الممنوحة للأدلة المادية.

**٢. أهمية الدراسة**

ترجع أهمية دراسة هذا الموضوع إلى التطور الذى طرأ فى إثبات الجرائم ومعرفة هوية مرتكبيها، وذلك فى مواكبة التطور الهائل فى الجرائم المستحدثة لاسيما الجرائم السيبرانية، لذا كان هذا البحث مهما فى التعرف على الوسائل الحديثة المستخدمة فى كشف مرتكبى الجرائم التي تقع عبر شبكات الإنترنت والجريمة المنظمة العابرة للحدود.

**٣. إشكالية الدراسة وتساؤلاتها**

الإشكالية الرئيسية فى هذه الدراسة هى هل يعول على الذكاء الاصطناعي فى **إثبات الجرائم السيبرانية؟** وينبثق عن هذه الإشكالية التساؤلات الآتية:

**١- كيفية إثبات الجرائم السيبرانية بواسطة الجيل الأول من الذكاء الاصطناعي**

**٢- كيفية إثبات الجرائم السيبرانية بواسطة الجيل الثاني من الذكاء الاصطناعي**

---

(2) Christopher Rigano, using artificial intelligence to address criminal justice needs, NIJ Journal / Issue No. 280 January 2019, P. 3

(ISSN: 2537 - 0758)

**٤. منهجية الدراسة**

يعتمد الباحث على المنهج الوصفى فيما يتعلق ببيان وسائل الذكاء الاصطناعي، والمنهج التحليلى فيما يتعلق بالتطبيق القانونى للذكاء الاصطناعي فى **إثبات الجرائم السيبرانية**

**٥. خطة الدراسة**

سيتم تقسيم هذا البحث إلى مبحثين ويليهما خاتمة بها النتائج التي يتم التوصل إليها والمقترحات، وجاءت خطة البحث على النحو التالى:

**المبحث الأول: إثبات الجرائم السيبرانية باستخدام الجيل الأول من الذكاء الاصطناعي**

**المبحث الثاني: إثبات الجرائم السيبرانية باستخدام الجيل الثاني من الذكاء الاصطناعي**

## المبحث الأول

## إثبات الجرائم السيبرانية باستخدام الجيل الأول من الذكاء الاصطناعي

بمراجعة الموارد الأكاديمية المتاحة يتلاحظ وجود العديد من تطبيقات تقنيات الذكاء الاصطناعي التي يمكن الاستعانة بها في إثبات الجرائم السيبرانية، ومن ذلك، أن يتم تطبيق الشبكات العصبية لإثبات جرائم الاختراق، واستخدام الشبكات العصبية فى إثبات رفض تقديم الخدمة، وإثبات وتصنيف البرامج الضارة، كما تستخدم تقنيات الذكاء الاصطناعي مثل الأساليب البحثية، واستخراج البيانات، والشبكات العصبية، ونظام المعلومات الإدارية، في إثبات ما يتعلق بالفيروسات، ويكمن مستقبل تكنولوجيا إثبات جرائم الفيروسات فى تطبيق يعرف باسم تقنية تكنولوجيا الحدس **Heuristic Technology** والتي تعني "المعرفة والمهارات التي تستخدم بعض الأساليب لتحديد وتحليل الرموز بذكاء لإثبات فيروس غير معروف بواسطة بعض القواعد أثناء المسح"(٣).

(3) Selma Dilek, Hüseyin Çakır and Mustafa Aydın, applications of artificial intelligence techniques to combating cyber-crimes: a review, DOI: 10.5121/ijaia.2015.6102, International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, No. 1, January 2015, P. 21

ونتناول في هذا المبحث إثبات الجرائم السيبرانية باستخدام الشبكات العصبية في مطلب أول، ثم إثبات الجرائم السيبرانية باستخدام العميل المحقق الذكي في مطلب ثان، وذلك على النحو الآتي:

## المطلب الأول

## إثبات الجرائم السيبرانية باستخدام الشبكات العصبية

الشبكات العصبية عبارة عن آلية إلكترونية تحاكي الجوانب الهيكلية والوظيفية للشبكات العصبية الموجودة فى النظم العصبية البيولوجية، وتؤتي نتائج كبيرة فى حالات التنبؤ أو التصنيف أو التحكم فى البيئات السيبرانية الحيوية والمعقدة، ومن تطبيقات استخداماتها فى إثبات الجرائم السيبرانية[٤]:

- شبكة **NeuroNet** (٢٠٠٨) وهي عبارة عن نظام شبكة عصبية يجمع المعلومات الموزعة ويعالجها، وتثبت المخالفات السيبرانية، وتصدر تنبيهات وفي الوقت ذاته بل تبدأ التدابير المضادة، وأظهر الواقع العملي فعالية هذه الشبكة فى إثبات ومكافحة جرائم هجمات حجب الخدمة، وقد تم تصميم مُعرِّفات هوية عصبية قائمة على الشبكات يمكنها على الفور إثبات وتصنيف مختلف الهجمات وذلك فى عام (٢٠١١)[٥].
- شبكة **IDS-NNM**: عبارة عن نظام تم استحداثه عام ٢٠٠٩، وذلك لإثبات جرائم الاختراق الإلكتروني باستخدام الشبكة العصبية المعتمدة على النمذجة، وقد أثبتت التجارب العملية فعاليتها في إثبات جميع محاولات الاقتحام فى اتصالات الشبكة دون إعطاء أي تنبيهات خاطئة، وفي العام ٢٠٠٩ أيضا تم تصميم بنية تفصيلية تحتوي على نظام إثبات لنفس الجرائم على أساس الشبكة العصبية الاصطناعية من أجل تعزيز إثبات جرائم اختراق الشبكات، وفى العام التالي مباشرة تم استحداث أنظمة أخرى لإثبات جرائم الاختراق الإلكتروني مع التركيز بشكل خاص على

---

(4) Selma Dilek, applications of artificial intelligence techniques to combating cyber-crimes: a review, op, cit, P. 25

(5) Y. Chen, "NeuroNet: Towards an Intelligent Internet Infrastructure", 5th IEEE Consumer Communications and Networking Conference (CCNC 2008), pp. 543 547; S. T. F. Al-Janabi, H. A. Saeed, "A Neural Network Based Anomaly Intrusion Detection System", Developments in E-systems Engineering (DeSE), (2011), pp. 221– 226.

(ISSN: 2537 - 0758)

الأنظمة التي تستخدم شبكات عصبية اصطناعية لإثبات حركة المرور المشبوهة والتي قد تشكل جريمة[٦].

- فى عام (٢٠٠٩) واستنادا إلى الانتشار الخلفي للشبكات العصبية تم تقديم طريقة هجينة لإثبات وتصفية البريد المزعج، وأثبتت تلك المقاربة أنها أكثر قوة مقارنة بالطرق الأخرى للإثبات غير المنظم أو العشوائي للبريد التي تستخدم الكلمات الرئيسية، بسبب التغير المستمر للسلوك الإجرامي للبريد العشوائي[٧].
- فى عام (٢٠٠٩) استُخدِمت الشبكة العصبية في إثبات وتحليل جرائم هجمات حجب الخدمة، وأظهرت التجارب دقة وفعالية استخدام الشبكة العصبية أكثر من الطرق الأخرى[٨].
- فى عام (٢٠٠٩) تم استخدام طريقة جديدة لإثبات وجود الزومبي بواسطة الشبكات العصبية، وبعد التجارب تبين فاعلية هذه المقاربة وسهولة استخدامها فى حالة التطبيق على شبكة حقيقية وتحقيق نتائج جيدة فى إثبات الزومبي[٩].
- فى عام (٢٠١٢) تم تطوير معرفات الهوية القائمة على أنظمة الشبكات العصبية، وبعد الاستخدام العملي والفعلي تبين أن هذا النظام له معدلات إثبات لجرائم الاختراق الإلكتروني مماثلة للمعرفات المتاحة الأخرى، وفضلا عن هذا، ثبت أنه أسرع ٢٠ مرة على الأقل فى إثباته لجرائم هجمات حجب الخدمة[١٠].

---

(6) C. Bitter, D.A. Elizondo, T. Watson, "Application of Artificial Neural Networks and Related Techniques to Intrusion Detection", IEEE World Congress on Computational Intelligence (WCCI, 2010), pp. 949 – 954; L. Ondrej, T. Vollmer, M. Manic, "Neural Network Based Intrusion Detection System for Critical Infrastructures", Proceedings of International Joint Conference on Neural Networks, (2009) pp. 1827-1834.

(7) C. H. Wu, "Behavior-based spam detection using a hybrid method of rule-based techniques and neural networks," Expert Systems with Applications, Vol. 36, Issue.3, Part: 1, (2009) pp. 4321–4330.

(8) A. Iftikhar, B.A. Azween, A. S. Alghamdi, "Application of artificial neural network in detection of dos attacks," Proceedings of the 2nd ACM international conference on Security of information and networks, (2009), pp. 229–234.

(9) P. Salvador, A. Nogueira, U. Franca, R. Valadas, "Framework for Zombie Detection using Neural Networks", Fourth International Conference on Internet Monitoring and Protection (ICIMP '09), (2009) pp.14– 20.

(10) D. K. Barman, G. Khataniar, "Design Of Intrusion Detection System Based On Artificial Neural Network And Application Of Rough Set", International

## المطلب الثاني
## إثبات الجرائم السيبرانية بواسطة العميل المحقق الذكي

العميل المحقق الذكي عبارة عن قوى مستقلة يولدها الكمبيوتر وتتواصل مع بعضها البعض حيث يحدث تبادل للبيانات وتتعاون فيما بينها من أجل تنفيذ الاستجابات المناسبة فى حالة وقوع أحداث غير متوقعة، وتُعد هذه التقنية مناسبة لإثبات ومكافحة الهجمات الإلكترونية نظرا لقابليتها للانتقال والقدرة على التكيف فى البيئات التي يتم نشرها فيها[١١].

- فى عام (٢٠٠٣) تم تطوير نظام "مخطط" يمكنه إثبات ومنع خطط معينة للهجوم السيبراني باستخدام تخطيط متعدد الجوانب[١٢]، وفى عام (٢٠٠٦) ظهر نظام جديد يعرف بائتلاف العملاء المحققين الموزعين الذى يحافظ على نظام التشغيل العادي، حيث يثبت ويتعامل مع الأحداث الطارئة والتي لا يمكن توقعها، ويحمى من المطلعين الخبثاء والأخطاء والهجمات فى شبكات الطاقة الكهربائية الموزعة[١٣]، وفى عام (٢٠٠٧) تم اقتراح إطار لآليات الدفاع التعاوني ضد هجمات الإنترنت، واعتمد ذلك على النمذجة والمحاكاة الذكية للعديد من العملاء المحققين، حيث تتفاعل مجموعات من العملاء الأذكياء وتضبط تكوينهم وسلوكهم حسب حالة الشبكة وطبقا لشدة الهجمات، وبعد اختبار هذا الاقتراح فى التحقيق فى الهجمات الموزعة وآليات الدفاع ضدها، تبين وجود فعالية كبيرة والتعاون والقدرة على التكيف فى مجموعات العميل المحقق الذكي[١٤]. وفى ذات العام تم تقديم نموذج أولى

---

Journal of Computer Science and Communication Networks, Vol. 2, No. 4, (2012), pp. 548-552.

(11) Selma Dilek, applications of artificial intelligence techniques to combating cyber-crimes: a review, op, cit, P. 26

(12) N. C. Rowe, "Counter-planning Deceptions To Foil Cyber-Attack Plans", Proceedings of the 2003 IEEE Workshop on Information Assurance, United States Military Academy, West Point, Information Assurance Workshop, 2003, pp. 203- 210.

(13) L. Phillips, H. Link, R. Smith, L. Weiland, Agent-Based Control of Distributed Infrastructure Resources, U.S. Department of Energy, Sandia National Laboratories, USA. (2006)

(14) I. Kotenko, A. Ulanov, "Multi-Agent Framework fo Simulation of Adaptive Cooperative Defense Against Internet Attacks", International Workshop on

(ISSN: 2537 - 0758)

لأمان متعدد الطبقات يوفر حماية من الإدخال غير الصحيح والقدرة على إثبات استراتيجيات الهجوم غير المعروفة والاسترداد منها[١٥].

- فى عام (٢٠٠٦) ظهر نظام- متعدد العملاء المحققين- متنقل قائم على التوليف بغرض إثبات ومكافحة جرائم الاختراق الإلكتروني دون حاجة لتدخل بشري[١٦]، وفى وفى عام (٢٠٠٧) ظهر نظام تصوير متنقل مترابط ومرن ومرتكز على عميل محقق ذكي لإثبات جرائم الاختراق الإلكتروني فى الشبكات الحيوية، وهذا النظام مدعم كذلك بشبكة عصبية اصطناعية[١٧]. وفى عام (٢٠١١) تم اقتراح نظام لإثبات الاختراق الإلكتروني الموزع بناءً على التعاون بين عملاء محققين متعددين لإثبات جرائم الاختراق الإلكتروني فى شبكات التحكم الإشرافي ومعرفة البيانات **(SCADA)**، وتشمل تلك البنية كذلك القيود الهيكلية للشبكة والقيود على الاتصال[١٨]. وفى عام (٢٠١٣) ظهرت مقاربة ذكية متعددة العملاء بغرض إثبات جرائم الاختراق الإلكتروني للشبكة باستخدام استخراج البيانات[١٩].
- فى عام (٢٠٠٦) تم تصميم نظام متعدد العملاء المحققين لإثبات جرائم دودة الكمبيوتر واحتوائها فى شبكات مدينة العاصمة، وأظهرت التجارب أن هذا النظام

---

Autonomous Intelligent Systems: Agents and Data Mining (AIS-ADM), Springer-Verlag, Berlin Heidelberg, vol. 4476, 2007, pp. 212–228.

(15) D. Edwards, S. Simmons, N. Wilde, "Prevention, Detection and Recovery from Cyber-Attacks Using a Multilevel Agent Architecture", IEEE International Conference on System of Systems Engineering (SoSE '07), (2007) pp. 1 – 6.

(16) J. Helano, M. Nogueira, "Mobile Intelligent Agents to Fight Cyber Intrusions", the International Journal of Forensic Computer Science (IJoFCS), Vol. 1, 2006, pp. 28-32.

(17) E. Herrero, M. Corchado, A. Pellicer, A. Abraham, "Hybrid multi agent-neural network intrusion detection with mobile visualization", Innovations in Hybrid Intelligent Systems, Vol. 44, (2007) pp. 320- 328.

(18) A. F. Shosha, P. Gladyshev, W. Shinn-Shyan, L. Chen-Ching, "Detecting cyber intrusions in SCADA networks using multi-agent collaboration," 16th International Conference on Intelligent System Application to Power Systems (ISAP), (2011) pp.1-7.

(19) I. Ionita, L. Ionita, "An agent-based approach for building an intrusion detection system," 12th International Conference on Networking in Education and Research (RoEduNet), (2013) pp.1-6.

يثبت ثم يحبط انتشار دودة الكمبيوتر computer worm بشكل فعال حتى مع ارتفاع معدلات الإصابة بها[٢٠].

- فى عام (٢٠٠٧) ظهر نموذج تجريدي من أجل إثبات جرائم الحالات الشاذة في الشبكات كالفيروسات، وقد استوحِيَ هذا النموذج من نظام المناعة البيولوجي، والذي يعتمد على تقنية متعددة العوامل تطبق على الشبكة والعائل لإثبات جرائم التطفل بما فيها عدوى الفيروسات[٢١].
- فى عام (٢٠١٠) تم تصميم بنية أمان شبكة مخصصة استنادا إلى أنظمة مناعة اصطناعية باستخدام عملاء محققين متنقلين وأذكياء بعضهم عملاء إثبات والآخر عملاء هجوم مضاد، وهي تجمع بين مزايا كل من أنظمة المناعة الاصطناعية وتقنية العميل المحقق الذكي، ولديها خصائص التوزيع والتكيف الذاتي والتعلم الذاتي والتوسع[٢٢].
- فى عام (٢٠١٠) تم تقديم منهج قائم على عملاء تحقيق متعددين من أجل التحقيق والدفاع ضد شبكات الروبوت التي تنتشر بسرعة عبر الإنترنت وتستخدم لارتكاب الجرائم السيبرانية المختلفة مثل إجراء عمليات فحص القابلية للتأثر، وإرسال كميات هائلة من رسائل البريد الإلكتروني العشوائي[٢٣].
- فى عام (٢٠١٠) تم اقتراح منهج نظري ذي طبقات لحماية أنظمة أتمتة شبكة الطاقة من الهجمات السيبرانية التي يكون مصدرها شبكة الإنترنت أو من مصادر داخلية على الشبكة، ويتمتع هذا المنهج بالقدرة على إثبات الأحداث والأنشطة المتطفلة داخل وحدات التحكم، وقد أثبتت تجربة واختبار نموذج أولي للمنهج

(20) X. Gou, W. Jin, D. Zhao, "Multi-agent system for worm detection and containment in metropolitan area networks", Journal of Electronics, Vol. 23, No. 2, (2006) pp. 259-265.
(21) H. Fu, X. Yuan, K. Zhang, X. Zhang, Q. Xie, “Investigating Novel Immune-Inspired Multi-Agent Systems for Anomaly Detection”, The 2nd IEEE Asia-Pacific Service Computing Conference, (2007) pp. 466- 472.
(22) X. Ye, J. Li, “A Security Architecture Based on Immune Agents for MANET”, International Conference on Wireless Communication and Sensor Computing (ICWCSC), 2010, pp. 1 5.
(23) I. Kotenko, A. Konovalov, A. Shorov, “Agent-Based modeling and Simulation of Botnets and Botnet Defence”, Proceeding of Conference on Cyber Conflict (CCD COE). (2010)

(ISSN: 2537 - 0758)

المقترح أنه قادر على إدارة وتخفيف بعض مشكلات الضعف الشائعة لأنظمة أتمتة شبكة الطاقة[٢٤].

- فى عام (٢٠١١) تم استحدث نظام أمان لإثبات وتدقيق حوادث السحابة كخدمة، ويعتمد على عملاء تحقيق يعملون بشكل تلقائي ويدركون تدفقات الأعمال الأساسية لحالات السحابة المنشورة؛ وهو ما يؤدي إلى توفير المرونة ومراقبة الأحداث المدعومة للبنية التحتية السحابية عن طريق هؤلاء العملاء[٢٥].

## المبحث الثاني

## إثبات الجرائم السيبرانية بواسطة الجيل الثاني من الذكاء الاصطناعي

يتم توظيف نظام المناعة الاصطناعية كما يحدث في نظام المناعة البيولوجية لدعم الاستقرار فى بيئة تتميز بالتغير المستمر، ويشتمل إثبات الاختراق الإلكتروني المستند إلى المناعة الاصطناعية على تطور الخلايا المناعية (التسامح الذاتي، والاستنساخ، والاختلاف... إلخ) واكتشاف المضادات فى وقت واحد، وينتج النظام المناعي الاصطناعي أجسامًا مضادة لمقاومة مسببات الجرائم، كما يمكن إثبات هذه الجرائم بواسطة الخوارزمية الوراثية والمجموعات الضبابية، ونتناول في هذا المبحث إثبات الجرائم السيبرانية بواسطة نظام المناعة الاصطناعية (مطلب أول) إثبات الجرائم السيبرانية بواسطة الخوارزمية الوراثية والمجموعات الضبابية (مطلب ثان) وذلك على النحو الآتي:-

### المطلب الأول

### إثبات الجرائم السيبرانية بواسطة نظام المناعة الاصطناعية

يمكن إثبات حجم الاقتحام الإلكتروني الإجرامي باختلاف تركيز الجسم المضاد، لذلك تؤدي هذه الأنظمة دورًا مهمًا فى إثبات الأمن السيبراني[٢٦].

---

(24) D. Wei, Y. Lu, M. Jafari, P. Skare, K. Rohde, "An Integrated Security System of Protecting Smart Grid against Cyber Attacks", Innovative Smart Grid Technologies (ISGT), (2010) pp. 1 7.

(25) F. Doelitzscher, C. Reich, M. Knahl, N. Clarke, "An Autonomous Agent Based Incident Detection System for Cloud Environments," IEEE Third International Conference on Cloud Computing Technology and Science (CloudCom), (2011) pp.197-204.

(26) Selma Dilek, applications of artificial intelligence techniques to combating cyber-crimes: a review, op, cit, P. 28

- فى عام (٢٠٠٧) تم تحليل نماذج نظام المناعة الاصطناعية التي تستخدم فى التعرف على الهوية ودخلت نظرية الخطر فى ذلك النظام باعتبارها وسيلة أو طريقة للاستجابة للخطر فى الشبكات اللاسلكية، وإثبات وتصنيف مخاطر الشبكة تم استخدام خرائط ذاتية التنظيم باعتبارها مصنفات، وتركت التجارب آثارا إيجابية لهذا النظام[٢٧].
- فى عام (٢٠٠٧) ظهر منهج يعتمد على نظام المناعة الاصطناعية لاستخراج خصائص ومواصفات البريد الإلكتروني لإثبات جرائم البريد العشوائي، وأثبتت نتائج تقييم الأداء فعالية الطريقة المقترحة فى إثبات الرسائل غير المرغوب فيها مقارنةً بالأنظمة الأخرى، مع وجود نسبة إيجابية خاطئة وكذلك معدلات سلبية كاذبة ضئيلة للغاية[٢٨].
- فى عام (٢٠٠٨) تم استحداث خوارزمية التعلم الهجين المستندة إلى نظام المناعة الاصطناعية لإثبات التشوه الإلكتروني[٢٩]. وبعد عامين وتحديدا فى عام (٢٠١٠) تم استحداث نموذج لتقييم الوضع الأمني للشبكة استنادا إلى نظام المناعة الاصطناعية، والذي يقيِّم حالة الأمان فى الوقت الفعلي والكمي للنظام، ويوفر الدعم اللازم لعمل تعديلات فى الوقت الفعلي لتدابير الدفاع، وتبين من التحليل النظري والعملي نجاعة النموذج فى إثبات التشوه الإلكتروني فى الوقت الملائم للحفاظ على أمن الشبكة[٣٠].

(27) M. A. Lebbe, J. I. Agbinya, Z. Chaczko, F. Chiang, "Self-Organized Classification of Dangers for Secure Wireless Mesh Networks", Australasian Telecommunication Networks and Applications Conference, (2007) pp. 322–327.
(28) B. Sirisanyalak, O. Sornil, "An artificial immunity-based spam detection system", IEEE Congress on Evolutionary Computation (CEC 2007), pp. 3392 3398.
(29) L. Hong, "Artificial Immune System for Anomaly Detection", IEEE International Symposium on Knowledge Acquisition and Modeling Workshop, (2008) pp. 340– 343.
(30) H. Qiang, T. Yiqian, "A Network Security Evaluate Method Base on AIS", International Forum on Information Technology and Applications (IFITA), Vol. 2, (2010) pp. 42– 45.

(ISSN: 2537 - 0758)

- فى عام (٢٠٠٩) تم اقتراح تمديد نموذج نظام المناعة الاصطناعية لأمن نظام الكمبيوتر إلى مجال أوسع بغرض توفير وظائف الإدراك الحسي وقدرات الإثبات مع ذكاء الجهاز[٣١].
- فى عام (٢٠٠٩) تم دراسة فوائد الذكاء الاصطناعي بشكل عام، ونظام المناعة الاصطناعية بشكل خاص، لتحسين إثبات جريمة الاختراق الإلكتروني من خلال التحقيق فى تصميمات النظم المختلفة لإثبات الاختراق اعتمادا على نظام المناعة الاصطناعية، ودلت النتائج على أن نظام المناعة الاصطناعية سيكون مثمرًا لتصميم تطبيقات خاصة بنظم إثبات جريمة الاختراق الإلكتروني[٣٢]. وفى عام (٢٠١١) تم استحداث نموذج لتقييم أمان الشبكة من أجل الإثبات الكمى لدرجة جرائم الاختراق وفقا لنظرية نظام المناعة الاصطناعية، وظهرت فعاليته ومميزاته مقارنة بالنماذج التقليدية لتقييم أمان الشبكة[٣٣]. وفى ذات العام ظهر نظام إثبات جرائم الاختراق الإلكتروني وفق تسلسل هرمى جديد بهدف تحسين الأمن السيبراني للشبكة الذكية، ويتكون النظام من وحدة ذكية تستخدم نظام المناعة الاصطناعية لإثبات البيانات الضارة والهجمات الإلكترونية المحتملة[٣٤] وفى عام (٢٠١٢) استحدث نموذج جديد يعتمد على نظام المناعة الاصطناعية، من أجل تصميم نموذج لإثبات جرائم الاختراق والتحكم فى الوصول وإثبات الحالات الشاذة فى الحالات الحرجة من البنى التحتية التي تعتمد على تكنولوجيا الإنترنت[٣٥]. وفى عام

(31) G. Gianini, M. Anisetti, A. Azzini, V. Bellandi, E. Damiani, S. Marrara, "An Artificial Immune System approach to Anomaly Detection in Multimedia Ambient Intelligence", 3rd IEEE International Conference on Digital Ecosystems and Technologies, (2009) pp. 502 – 506.

(32) A. EshghiShargh, "Using Artificial Immune System on Implementation of Intrusion Detection Systems", Third UK Sim. European Symposium on Computer Modeling and Simulation, (2009) pp. 164-168.

(33) J. Yang, T. F. Wang, C. M. Liu, B. Li, "Improved Agent Model for Network Security Evaluation Based on AIS", Fourth International Conference on Intelligent Computation Technology and Automation (ICICTA), Vol. 1, (2011) pp. 151 – 154.

(34) Y. Zhang, L. Wang, W. Sun, R. C. Green II, M. Alam, "Artificial Immune System based Intrusion Detection in A Distributed Hierarchical Network Architecture of Smart Grid", IEEE Power and Energy Society General Meeting, (2011) pp. 1 – 8.

(35) S. M. A. Mavee, E. M. Ehlers, "A Multi-Agent Immunologically-Inspired Model for Critical Information Infrastructure Protection", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, (2012) pp. 1089 – 1096.

(٢٠١٤) تم تطوير نظام فريد من نوعه للإثبات الجنائي للقرصنة يعتمد على العميل للشبكات اللاسلكية الذي يجمع المعلومات من العقد المختلفة ويستخدم هذه المعلومات مع نظام مناعي اصطناعي متطور لإثبات ذلك من خلال تجاوز أو تأخير عمليات الإرسال على طول مسار التسلل ولمنع التطفل، وقد بينت النتائج التجريبية أن النظام مناسب جدًا لإثبات جرائم القرصنة والوقاية في الشبكات اللاسلكية[٣٦].

- فى عام (٢٠٠٩) تم بحث إمكانية توسيع نظام المناعة الاصطناعية لإثبات هجمات خادم الويب، والتي يمكن أن تساعد مسئول النظام بالتحذير من خطورة جرائم الهجوم الإلكتروني والمساعدة فى التخفيف من الهجمات المباشرة[٣٧]. وفى ذات العام تم تقديم إطار أمنى يستند إلى نظام المناعة الاصطناعية لتأمين شبكات مخصصة للهاتف المحمول، قابلة للتطوير وقوية ولديها سمات مثل قابلية التوزيع والاستجابة الثانية واستعادة الذات[٣٨]. وفى عام (٢٠١٠) تم تقديم نموذج استجابة للتطفل على التعلم الذاتي قائم على نظام المناعة الاصطناعية بغرض إثبات الهجمات غير المعروفة وتصنيفها، وأظهرت التجارب أن هذا النموذج له صفات مثل التكيف الذاتي، والحساب الكمى، وأنه يوفر استجابة فعالة لجرائم الاقتحام[٣٩].
- فى عام (٢٠٠٩) تم اقتراح نظام جديد لإثبات جرائم الفيروسات استنادًا إلى نظام المناعة الاصطناعية، وأظهرت النتائج التجريبية أن هذا النظام له قدرة إثبات قوية وأداء تعميم جيد[٤٠].

---

(36) G.V.P. Kumar, D.K. Reddy"An Agent Based Intrusion Detection System for Wireless Network with Artificial Immune System (AIS) and Negative Clone Selection," International Conference on Electronic Systems, Signal Processing and Computing Technologies (ICESC), , (2014) pp. 429-433.

(37) M. Danforth "Towards a Classifying Artificial Immune System for Web Server Attacks", International Conference on Machine Learning and Applications, (2009) pp. 523– 527.

(38) Y. A. Mohamed, A. B. Abdullah, "Immune Inspired Framework for Ad Hoc Network Security", IEEE International Conference on Control and Automation, (2009) pp. 297– 302.

(39) L. Rui, L. Wanbo, "Intrusion Response Model based on AIS", International Forum on Information Technology and Applications (IFITA), Vol. 1, (2010) pp. 86– 90.

(40) R. Chao, Y. Tan, "A Virus Detection System Based on Artificial Immune System", International Conference on Computational Intelligence and Security, Vol. 1, (2009) pp. 6 – 10.

(ISSN: 2537 - 0758)

- فى عام (٢٠١٠) استخدمت الخرائط ذاتية التنظيم لتصور طوبولوجيا البيانات من بهدف إثبات وتحليل الوثائق النصية المتعلقة بالإرهاب السيبراني[٤١].
- فى عام (٢٠١١) تم الاستعانة بآلية مستندة إلى نظام المناعة الاصطناعية لإثبات جرائم الاقتحام في بيئة إنترنت الأشياء[٤٢]، والتي تحاكى آليات التكيف والتعلم الذاتي من خلال التكيف الديناميكى مع البيئة الافتراضية، وأظهر التحليل فعالية هذا النموذج في إثبات جرائم اقتحام إنترنت الأشياء[٤٣].
- فى عام (٢٠١١) اقتُرح نموذج تحسين لإثبات الحالات الشاذة استنادًا إلى نظام المناعة الاصطناعية، وأظهر ذلك النموذج تحسنا فى أداء المناعة الاصطناعية فى إثبات الحالات الشاذة، وضمان الأمن، وإجراء التنقيب عن البيانات فى الشبكات المخصصة للهاتف المحمول[٤٤].
- فى عام (٢٠١٢) قُدم نظام المناعة الاصطناعية لإثبات التصيد الاحتيالي الإلكتروني من خلال الذاكرة والكاشفات الناضجة، وقد ظهر تفرد هذا النظام ومرونته وقدرته على التكيف مع أنظمة اكتشاف الخداع الأخرى الموجودة[٤٥].

---

(41) E. Endy, C. Lim, K. I. Eng, A. S. Nugroho, "Implementation of intelligent searching using self-organizing map for webmining used in document containing information in relation to cyber terrorism", Second International Conference on Advances in Computing, Control, and Telecommunication Technologies, (2010) pp. 195 – 197.

(٤٢) إنترنت الأشياء (بالإنجليزية: Internet of Things- IoT)، مصطلح برز حديثا، يُقصد به الجيل الجديد من الإنترنت (الشبكة) الذى يتيح التفاهم بين الأجهزة المترابطة مع بعضها (عبر بروتوكول الإنترنت). وتشمل هذه الأجهزة الأدوات والمستشعرات والحساسات وأدوات الذكاء الاصطناعي المختلفة وغيرها، حيث تتخاطب وتتفاهم الأشياء عبر الإنترنت دون التدخل المباشر للبشر، فمثلاً يمكن للثلاجة التراسل مع مركز التسوق وشراء المستلزمات وتوصيلها بلا تدخل بشرى.

(43) C. Liu, J. Yang, Y. Zhang, R. Chen, J. Zeng, "Research on Immunity-based Intrusion Detection Technology for the Internet of Things", Seventh International Conference on Natural Computation (ICNC), Vol. 1, (2011) pp. 212 – 216.

(44) M. S. A. Ansari, M. Inamullah, "Misbehavior detection in mobile ad hoc networks using Artificial Immune System approach", IEEE 5th International Conference on Advanced Networks and Telecommunication Systems (ANTS), (2011) pp. 1 – 6.

(45) X. Fang, N. Koceja, J. Zhan, G. Dozier, D. Dipankar, "An Artificial Immune System for Phishing Detection", IEEE World Congress on Computational Intelligence (WCCI 2012), pp.1 7.

## المطلب الثاني

## إثبات الجرائم السيبرانية بواسطة الخوارزمية الوراثية والمجموعات الضبابية

يمكن إثبات الجرائم السيبرانية بواسطة الخوارزمية الوراثية والمجموعات الضبابة وذلك على النحو الآتي:-

- فى عام (٢٠٠٤) استحدثت خوارزمية التعلم لإثبات التشوه الإلكتروني والتي يمكنها كذلك إثبات الهجمات، وقد تم تطبيقها على نظام أمان كمبيوتر اصطناعي وأظهرت فعاليتها فى إثبات جرائم الاختراق(٤٦).
- فى عام (٢٠٠٩) ظهر نظام غامض لإثبات جرائم التطفل المستند إلى العائل باستخدام تقنية التنقيب عن البيانات، وأظهرت نتائج المحاكاة أن النظام المقترح يحسن الأداء ويقلل من حجم قاعدة البيانات، ومعدل الإنذارات الكاذبة(٤٧).
- فى عام (٢٠١١) تم وصف طريقة لإثبات اقتحام شبكة غامضة مبنية على أساس التنقيب عن القاعدة الصفية فى برمجة الشبكات الوراثية، وهي طريقة مرنة وفعالة لجرائم سوء استخدام وإثبات التشوه الإلكتروني فى الشبكات، وتستطيع التعامل مع قواعد البيانات المختلطة التي تحتوي على سمات منفصلة لقواعد ارتباط الطبقة اللازمة لإزالة إثبات جرائم الاختراق، وأثبتت التجارب العملية أن هذا النهج يوفر معدلات إثبات عالية تنافسية بالمقارنة مع تقنيات التعلم الآلي الأخرى(٤٨).
- فى عام (٢٠١٢) ظهر نظام إثبات جرائم الاختراق الإلكتروني القائم على قواعد الخوارزمية الوراثية لتحسين أمن النظام والسرية وتوافر الموارد فى الإعدادات الشبكية، ويستخدم مجموعة من قواعد التصنيف التي تم الحصول عليها من بيانات تدقيق الشبكة وإطار دعم الثقة، الذي يستخدم كدالة لياقة لتقييم جودة كل قاعدة(٤٩).

---

(46) D. W. Kim, J. W. Yang, K. B. Sim, "Adaptive Intrusion Detection Algorithm based on Learning Algorithm", The 30th Annual Conference of the IEEE Industrial Electronics Society, Vol. 3, (2004) pp. 2229 – 2233.

(47) M. A. Sekeh, M. A. Bin Maarof, "Fuzzy Intrusion Detection System via Data Mining Technique with Sequences of System Calls," Fifth International Conference on Information Assurance and Security (IAS '09.), Vol.1, (2009) pp.154-157.

(48) S. Mabu, C. Chen, L. Nannan, K. Shimada, K. Hirasawa, "An Intrusion-Detection Model Based on Fuzzy Class-Association-Rule Mining Using Genetic Network Programming," IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, Vol.41, No.1, (2011) pp.130-139.

(49) A.A. Ojugo, A.O. Eboka, O.E. Okonta, R.E Yoro (Mrs), F.O. Aghware, "Genetic Algorithm Rule-Based Intrusion Detection System (GAIDS)," Journal

(ISSN: 2537 - 0758)

وفى عام (٢٠١٣) تم تصميم نظام إثبات للجرائم السابقة بناءً على الخوارزمية الجينية والمنطق الضبابي للإثبات الفعال للأنشطة الإجرامية المتطفلة، وهذا النظام قابل للتكيف وفعال من حيث التكلفة، وأوضحت النتائج العملية أن النظام المقترح حقق معدل إثبات معقول لجرائم الاختراق[٥٠]. وفى ذات العام ظهر نظام إثبات جرائم الاختراق الإلكتروني للشبكة، وفيها تُستخدم قواعد غامضة لتصنيف بيانات الهجوم على الشبكة، بينما تعمل الخوارزمية الجينية على تحسين إيجاد قاعدة غامضة مناسبة للحصول على الحل الأمثل، أثبتت النتائج أن النظام المقترح يمكنه إثبات هجمات الشبكة فى الوقت المناسب (خلال ٢-٣ ثواني) عند وصول البيانات إلى نظام الإثبات بمعدل إثبات يتجاوز ٩٧.٥٪[٥١].

- فى عام (٢٠١٤) تم وضع نظام إثبات جرائم الاقتحام الغامض القائم على الشذوذ للكشف عن هجمات إسقاط الحزمة فى شبكات المحمول المخصصة، وأثبتت النتائج أن النظام المقترح لديه القدرة على إثبات جرائم هجمات إسقاط الرزم بإيجابية عالية مع انخفاض معدلات الإيجابية الكاذبة تحت جميع مستويات سرعة العقد المحمولة[٥٢]. وفى ذات العام تم تقديم نموذج لإثبات جرائم اقتحام الشبكة استنادًا إلى نهج الخوارزمية الجينية مع مُحسِّن أولى ومُحدد الاختيار اللذين يستخدمان لتحسين التفتيش عن سيناريوهات الهجوم فى ملفات التدقيق، واستخدم نهج الخوارزمية الجينية لأنه يعزز الأداء ويقلل من معدل الإيجابية الخاطئة[٥٣].
- فى عام (٢٠١٤) ظهر نظام لإثبات جرائم الاختراق الوراثي ذي الطبقات المستندة إلى الخوارزمية لأنشطة المراقبة فى بيئة معينة لتحديد ما إذا كانت شرعية أم ضارة

---

of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 8, 2012, pp. 1182 – 1194.

(50) M. Md. M. Hassan, "Network Intrusion Detection System Using Genetic Algorithm and Fuzzy Logic", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, (2013) No. 7.

(51) P. Jongsuebsuk, N. Wattanapongsakorn, C. Charnsripinyo, "Real-time intrusion detection with fuzzy genetic algorithm," 10th International Conference on Electrical Engineering/Electronics Computer, Telecommunications and Information Technology (ECTI-CON), 2013, pp.1-6.

(52) A. Chaudhary, V. N. Tiwari, A. Kumar, "Design an anomaly based fuzzy intrusion detection system for packet dropping attack in mobile ad hoc networks," IEEE International Conference on Advance Computing (IACC), (2014) pp. 256-261.

(53) S. E. Benaicha, L. Saoudi, S. E. Bouhouita Guermeche, O. Lounis, "Intrusion detection system using genetic algorithm," Science and Information Conference (SAI), (2014) pp. 564-568.

استنادًا إلى موارد المعلومات المتاحة، وأظهرت النتائج التجريبية أن النظام المقترح يثبت بكفاءة هجمات التي تأتى من على بُعد إلى موقع محلى Remote-to-Local attacks (R2L) بدقة ٩٠٪[٥٤].

**أولا: النتائج**:

١. يقدم الذكاء الاصطناعي العديد من أساليب الكمبيوتر (مثل الذكاء الحسابي، الشبكات العصبية، العملاء المحققين الأذكياء، نظم المناعة الصناعية، تعدين البيانات، التعرف على الأنماط، المنطق الغامض، إلخ) وهو ما لعب دورا هاما فى إثبات الجريمة السيبرانية والوقاية منها.

٢. الشبكات العصبية عبارة عن آلية إلكترونية تحاكى الجوانب الهيكلية والوظيفية للشبكات العصبية الموجودة فى النظم العصبية البيولوجية، وهى مثالية فى حالات التنبؤ أو التحكم فى البيئات السيبرانية الحيوية والمعقدة.

٣. عند تقسيم الدليل السيبرانى لا بد من مراعاة التطور المستمر الذي يطرأ على هذا النوع من الأدلة من جهة، وعلى البيئة الافتراضية من جهة أخرى، حتى يمكن الاعتماد عليها كدليل إثبات فى مختلف القضايا.

٤. العميل المحقق الذكي هو قوى مستقلة يولدها الكمبيوتر وتتواصل مع بعضها لتبادل البيانات والتعاون من أجل تخطيط وتنفيذ الاستجابات المناسبة فى حالة وقوع أحداث غير متوقعة، وتُعد تقنية العميل المحقق الذكي مناسبة لإثبات ومكافحة الهجمات الإلكترونية لقابليتها للانتقال والقدرة على التكيف فى البيئات التي يتم نشرها فيها، بالإضافة إلى طبيعتها التعاونية.

**ثانيا: التوصيات**

١. أهمية أن تنشئ الدولة– ممثلة فى وزارتى الداخلية والعدل– إدارة متخصصة فى الذكاء الاصطناعي لتفعيل دوره فى الإثبات الجنائى فى جميع مراحله من استدلال لتحقيق لمحاكمة.

٢. نوصي بإجراء المزيد من الأبحاث التى تتعلق بدور الذكاء الاصطناعي فى خدمة العدالة الجنائية.

٣. نوصي بزيادة الإنفاق على أبحاث الذكاء الاصطناعي بصفة عامة. إدراج مواد خاصة بالذكاء الاصطناعي فى القوانين ذات الصلة سواء كانت متعلقة بالنظم الالكترونية أو بالجرائم الالكترونية.

---

(54) M. Padmadas, N. Krishnan, J. Kanchana, M. Karthikeyan, "Layered approach for intrusion detection systems based genetic algorithm," IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), (2013) pp.1-4.

(ISSN: 2537 - 0758)

# قائمة المراجع


1. John Searle, 'Can Computers Think?' in David J Chalmers (ed), Philosophy of Mind: Classical and Contemporary Reading, Oxford University Press, 2002.
2. Christopher Rigano, using artificial intelligence to address criminal justice needs, NIJ Journal / Issue No. 280 January 2019.
3. Selma Dilek, Hüseyin Çakır and Mustafa Aydın, applications of artificial intelligence techniques to combating cyber-crimes: a review, DOI : 10.5121/ijaia.2015.6102, International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, No. 1, January 2015.
4. C. Bitter, D.A. Elizondo, T. Watson, "Application of Artificial Neural Networks and Related Techniques to Intrusion Detection", IEEE World Congress on Computational Intelligence (WCCI, 2010); L. Ondrej, T. Vollmer, M. Manic, "Neural Network Based Intrusion Detection System for Critical Infrastructures", Proceedings of International Joint Conference on Neural Networks, (2009).

A. Iftikhar, B.A. Azween, A. S. Alghamdi, "Application of artificial neural network in detection of dos attacks," Proceedings of the 2nd ACM international conference on Security of information and networks, (2009).

B. H. Wu, "Behavior-based spam detection using a hybrid method of rule-based techniques and neural networks," Expert Systems with Applications, Vol. 36, Issue.3, Part: 1, (2009).

5. P. Salvador, A. Nogueira, U. Franca, R. Valadas, "Framework for Zombie Detection using Neural Networks", Fourth International Conference on Internet Monitoring and Protection (ICIMP '09), (2009).
6. D. K. Barman, G. Khataniar, "Design Of Intrusion Detection System Based On Artificial Neural Network And Application Of Rough Set", International Journal of Computer Science and Communication Networks, Vol. 2, No. 4, (2012).
7. N. C. Rowe, "Counter-planning Deceptions To Foil Cyber-Attack Plans", Proceedings of the 2003 IEEE Workshop on Information

Assurance, United States Military Academy, West Point, Information Assurance Workshop, 2003.
8. (1) L. Phillips, H. Link, R. Smith, L. Weiland, Agent-Based Control of Distributed Infrastructure Resources, U.S. Department of Energy, Sandia National Laboratories, USA. (2006)
A. Kotenko, A. Ulanov, “Multi-Agent Framework fo Simulation of Adaptive Cooperative Defense Against Internet Attacks”, International Workshop on Autonomous Intelligent Systems: Agents and Data Mining (AIS-ADM), Springer-Verlag, Berlin Heidelberg, vol. 4476, 2007.
9. D. Edwards, S. Simmons, N. Wilde, “Prevention, Detection and Recovery from Cyber-Attacks Using a Multilevel Agent Architecture”, IEEE International Conference on System of Systems Engineering (SoSE '07), (2007).
10. X. Gou, W. Jin, D. Zhao, "Multi-agent system for worm detection and containment in metropolitan area networks", Journal of Electronics, Vol. 23, No. 2, (2006).
11. J. Helano, M. Nogueira, “Mobile Intelligent Agents to Fight Cyber Intrusions”, the International Journal of Forensic Computer Science (IJoFCS), Vol. 1, 2006.
12. E. Herrero, M. Corchado, A. Pellicer, A. Abraham, “Hybrid multi agent-neural network intrusion detection with mobile visualization”, Innovations in Hybrid Intelligent Systems, Vol. 44, (2007).
A. F. Shosha, P. Gladyshev, W. Shinn-Shyan, L. Chen-Ching, "Detecting cyber intrusions in SCADA networks using multi-agent collaboration," 16th International Conference on Intelligent System Application to Power Systems (ISAP).
B. Ionita, L. Ionita, "An agent-based approach for building an intrusion detection system," 12th International Conference on Networking in Education and Research (RoEduNet), (2013).
13. H. Fu, X. Yuan, K. Zhang, X. Zhang, Q. Xie, “Investigating Novel Immune-Inspired Multi-Agent Systems for Anomaly Detection”, The 2nd IEEE Asia-Pacific Service Computing Conference, (2007).
A. Kotenko, A. Konovalov, A.Shorov, “Agent-Based modeling and Simulation of Botnets and Botnet Defence”, Proceeding of Conference on Cyber Conflict (CCD COE). (2010)

(ISSN: 2537 - 0758)

14. X. Ye, J. Li, “A Security Architecture Based on Immune Agents for MANET”, International Conference on Wireless Communication and Sensor Computing (ICWCSC), 2010.
15. D. Wei, Y. Lu, M. Jafari, P. Skare, K. Rohde, “An Integrated Security System of Protecting Smart Grid against Cyber Attacks”, Innovative Smart Grid Technologies (ISGT), (2010).
16. F. Doelitzscher, C. Reich, M. Knahl, N. Clarke, "An Autonomous Agent Based Incident Detection System for Cloud Environments," IEEE Third International Conference on Cloud Computing Technology and Science (CloudCom), (2011).
17. B. Sirisanyalak, O. Sornil, “An artificial immunity-based spam detection system“, IEEE Congress on Evolutionary Computation (CEC 2007).
18. M. A. Lebbe, J. I. Agbinya, Z. Chaczko, F. Chiang, “Self-Organized Classification of Dangers for Secure Wireless Mesh Networks”, Australasian Telecommunication Networks and Applications Conference, (2007).
19. L. Hong, “Artificial Immune System for Anomaly Detection”, IEEE International Symposium on Knowledge Acquisition and Modeling Workshop, (2008).
20. H. Qiang, T. Yiqian, “A Network Security Evaluate Method Base on AIS”, International Forum on Information Technology and Applications (IFITA), Vol. 2, (2010).
21. G. Gianini, M. Anisetti, A. Azzini, V. Bellandi, E. Damiani, S. Marrara, “An Artificial Immune System approach to Anomaly Detection in Multimedia Ambient Intelligence”, 3rd IEEE International Conference on Digital Ecosystems and Technologies, (2009).
A. EshghiShargh, “Using Artificial Immune System on Implementation of Intrusion Detection Systems”, Third UK Sim. European Symposium on Computer Modeling and Simulation, (2009).
22. J. Yang, T. F. Wang, C. M. Liu, B. Li, “Improved Agent Model for Network Security Evaluation Based on AIS”, Fourth International Conference on Intelligent Computation Technology and Automation (ICICTA), Vol. 1, (2011).
23. Y. Zhang, L. Wang, W. Sun, R. C. Green II, M. Alam, “Artificial Immune System based Intrusion Detection in A Distributed

Hierarchical Network Architecture of Smart Grid", IEEE Power and Energy Society General Meeting, (2011).
24. S. M. A. Mavee, E. M. Ehlers, "A Multi-Agent Immunologically-Inspired Model for Critical Information Infrastructure Protection", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, (2012).
25. G.V.P. Kumar, D.K. Reddy"An Agent Based Intrusion Detection System for Wireless Network with Artificial Immune System (AIS) and Negative Clone Selection," International Conference on Electronic Systems, Signal Processing and Computing Technologies (ICESC), , (2014).
26. R. Chao, Y. Tan, "A Virus Detection System Based on Artificial Immune System", International Conference on Computational Intelligence and Security, Vol. 1, (2009).
27. M. Danforth "Towards a Classifying Artificial Immune System for Web Server Attacks", International Conference on Machine Learning and Applications, (2009).
28. Y. A. Mohamed, A. B. Abdullah, "Immune Inspired Framework for Ad Hoc Network Security", IEEE International Conference on Control and Automation, (2009).
29. L. Rui, L. Wanbo, "Intrusion Response Model based on AIS", International Forum on Information Technology and Applications (IFITA), Vol. 1, (2010).
30. C. Liu, J. Yang, Y. Zhang, R. Chen, J. Zeng, "Research on Immunity-based Intrusion Detection Technology for the Internet of Things", Seventh International Conference on Natural Computation (ICNC), Vol. 1, (2011).
31. M. S. A. Ansari, M. Inamullah, "Misbehavior detection in mobile ad hoc networks using Artificial Immune System approach", IEEE 5th International Conference on Advanced Networks and Telecommunication Systems (ANTS), (2011).
32. X. Fang, N. Koceja, J. Zhan, G. Dozier, D. Dipankar, "An Artificial Immune System for Phishing Detection", IEEE World Congress on Computational Intelligence (WCCI 2012).
33. D. W. Kim, J. W. Yang, K. B. Sim, "Adaptive Intrusion Detection Algorithm based on Learning Algorithm", The 30th Annual Conference of the IEEE Industrial Electronics Society, Vol. 3, (2004).

(ISSN: 2537 - 0758)

34. M. A. Sekeh, M. A. Bin Maarof, "Fuzzy Intrusion Detection System via Data Mining Technique with Sequences of System Calls," Fifth International Conference on Information Assurance and Security (IAS '09.), Vol.1, (2009).
35. S. Mabu, C. Chen, L. Nannan, K. Shimada, K. Hirasawa, "An Intrusion-Detection Model Based on Fuzzy Class-Association-Rule Mining Using Genetic Network Programming," IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, Vol.41, No.1, (2011).
36. A.A. Ojugo, A.O. Eboka, O.E. Okonta, R.E Yoro (Mrs), F.O. Aghware, "Genetic Algorithm Rule-Based Intrusion Detection System (GAIDS)," Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 8, 2012.
37. M. Md. M. Hassan, "Network Intrusion Detection System Using Genetic Algorithm and Fuzzy Logic", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, (2013) No. 7.
38. P. Jongsuebsuk, N. Wattanapongsakorn, C. Charnsripinyo, "Real-time intrusion detection with fuzzy genetic algorithm," 10th International Conference on Electrical Engineering/Electronics Computer, Telecommunications and Information Technology (ECTI-CON), 2013.
A. Chaudhary, V. N. Tiwari, A. Kumar, "Design an anomaly based fuzzy intrusion detection system for packet dropping attack in mobile ad hoc networks," IEEE International Conference on Advance Computing (IACC), (2014).
39. S. E. Benaicha, L. Saoudi, S. E. Bouhouita Guermeche, O. Lounis, "Intrusion detection system using genetic algorithm," Science and Information Conference (SAI), (2014).
40. M. Padmadas, N. Krishnan, J. Kanchana, M. Karthikeyan, "Layered approach for intrusion detection systems based genetic algorithm," IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), (2013).