Neutrosophic Sets and Systems

Volume 23 Article 3

1-1-2018

# Intrusion Detection System and Neutrosophic theory for MANETs: A Comparative study

Haitham Elwahsh

Mona Gamal

A. A. Salama

I.M. El-Henawy

# Intrusion Detection System and Neutrosophic Theory for MANETs: A Comparative Study

**Haitham ElWahsh[1]*, Mona Gamal[2], A. A. Salama[3], and I.M. El-Henawy[4]**

[1] Computer Science Department, Faculty of Computers and Information, Kafrelsheikh University, Kafrelsheikh 33516, Egypt;
[2] Information System Department Faculty of Computers and Information, Kafrelsheikh University, Kafrelsheikh 33516, Egypt, Mona_Gafar@fci.kfs.edu.egm;
[3] Department of Mathematics and Computer Science, Faculty of Sciences, Port Said University, Port Said 522, Egypt; drsalama44@gmail.com.
[4] Computer Science Department, Faculty of Computers and Information, Zagazig University, Zagazig, Egypt; henawy2000@yahoo.com.
* Correspondence: Haitham.elwahsh@fci.kfs.edu.eg.

**Abstract**. Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organized in arbitrary and temporary network topologies without communication infrastructure. This network may change quickly and unforeseeable. The unique characteristics of MANET give an adversary the opportunity to launch numerous attacks against ad-hoc networks. So the security is an important role in MANETs. This article aims to present the concept of intrusion detection system (IDs) and surveys some of major intrusion detection approach against neutrosophic intrusion detection system in MANETs. Current IDS's corresponding to those architectures are also reviewed and compared. This paper introduces the accuracy rate and false alarm rate of four completely different classifiers to observe the percentage and the efficiency of the classifiers in detecting attacks in MANETs. Results show that Neutrosophic intelligent system based on genetic algorithm could facilitate significantly in detecting malicious activities in MANETs. Hence, neutrosophic techniques could be utilized to suit the ambiguity nature of the IDs.

**Keywords:** MANETs, Intrusion Detection, Neutrosophic, Security, Attacks.

## 1. Introduction

MANETs is a self-adapting network that's formed automatically by a group of mobile nodes without the needed of a hard and fast infrastructure or centralized control. Every node is supplied with a wireless transmitter and receiver, which permit it to contact with alternative nodes in its radio communication area. In order for a node to forward a packet to a node that's out of its radio area, the cooperation of alternative nodes within the network is needed; this can be referred to as a multi-hop communication. Therefore, every node must act as both a client and a router at the same time. The network topology often changes because of the mobility of nodes as they move at interval, into, or out of the network. A MANET with the features presented above was fit to military purposes.

In last years, MANETs have been expansion speedily and are progressively being used in several applications, starting from military to civilian and commercial uses, since forming such networks can be avoided the help of any infrastructure or interaction with a human. Several examples are: data collection, and virtual classrooms and conferences where laptops, or other mobile devices share wireless medium and connect to each other. As MANETs become widely spread, the security problem has become one of the fundamental attention. For example, a lot of the routing protocols designed for MANETs suppose that each node inside the network is cooperative and not pernicious [16, 31]. Therefore, just one node can cause the failure of the whole network. There are both passive and active attacks in MANETs. For passive attacks, packets containing secret data might be eavesdropped, that violates confidentiality. Active attacks, including sending data to incorrect destinations into the network, removing data, change the contents of data, and impersonating other nodes violate availability, integrity, authentication, and non-repudiation. Proactive approaches such as cryptography and authentication [21, 30, 29 and 8] were first brought into consideration,

and a lots of techniques have been proposed and implemented. However, these applications don't seem to be sufficient. If the flexibility to discover the attack once it comes into the network is got, these attacks can be stopped from doing any harm to the system or any data. Here is where the intrusion detection system comes in.

Intrusion detection as declared is a method of monitoring activities in a system, which may be a computer or network system. The mechanism that is achieved is named an IDs. An IDs gather activity data and then analyses it to determine whether or not there are any actions that assaulted the Protection rules. Once an IDs decide that an upnormal behavior or an action which recognize to be an attack occurs, it then makes an alarm to warn the security administrator. Additionally, IDs also can start a correct response to the malicious activity. Although there are many IDs techniques built for wired networks these days, they're not appropriate for wireless networks because of the variations in their characteristics. Therefore, those techniques should be changed or new techniques should be developed to form intrusion detection work effectively in MANETs. Because of the variations in the MANETs characteristics our research tend to use Neutrosophic Technique as a novel solution. In previous articles research [7 and 8] a neutrosophic intelligent system based on genetic algorithm was proposed, which the novelty in that technique is used three dimension (MEMBERSHIP- INDETERMENANCY - NONMEMEBRSHIP) all pervious technique used only two dimension (MEMBERSHIP- NONMEMEBRSHIP).

The concept of Neutrosophic Set (NS) was first introduced by Smarandache [12, 13] which is a generalization of classical sets, fuzzy set, intuitionistic fuzzy set etc. Salama et al. Work [2, 3, 4, 5, 6, 7, 8 and 11] formulated a beginning to new fields of neutrosophic theory in computer discipline. The neutrosophic indeterminacy assumption is very significant in many of circumstances such as information fusion (collecting data from various sensors). Also, NS is a conceivable common traditional system that generalize the principle of the traditional set, Fuzzy Set (FS) [23] and Intuitionistic Fuzzy Set (IFS)) [17], etc. NS 'A' determined on universe U. $\boldsymbol{x} = \boldsymbol{x}(\mathbf{T}, \mathbf{I}, \mathbf{F}) \in$ A with **T**, **I** and **F** are defined over the interval $]\mathbf{0}^{-}, \mathbf{1}^{+}[$. **T** is the truth-MEMEBERSHIP , **I** is the INDETERMINACY and F is the falsity-MEMEBERSHIP degrees on the set **A**.

Designing a neutrosophic IDS is a proper solution in handling vague circumstances. The neutrosophic IDS is formed of two sub phases: the preprocessing stage and the network attacks classification stage. The preprocessing stage is concerned by formulating the network features in a format appropriate for the classification. The KDD network data [18] is reformatted into neutrosophic form $(\mathbf{x}, \boldsymbol{\mu}_{\mathbf{A}}(\mathbf{x}), \boldsymbol{\sigma}_{\mathbf{A}}(\mathbf{x}), \boldsymbol{\nu}_{\mathbf{A}}(\mathbf{x}))$ where x is the value of feature, $\boldsymbol{\mu}_{\mathbf{A}}(\mathbf{x})$ is the MEMEBERSHIP (MEM), $\boldsymbol{\sigma}_{\mathbf{A}}(\mathbf{x})$ is the INDETERMINACY (I) and $\boldsymbol{\nu}_{\mathbf{A}}(\mathbf{x})$ is the NONMEMEBERSHIP (NON_MEM) degrees of the x in the feature space. This article extends a previous work [14 and 15] that compares how effectively intrusions in MANETs are detected by totally different classification algorithms. This paper is arranged as follows. Section 2 includes the Wireless technology. Section 3 proposes the Security in MANETs. The Literature Review of IDs in MANETs and conclusion are shown respectively in section 4 and 5.

## 2. Wireless technology

Wireless networks use the open medium as communication channel and electromagnetic waves to send data between participants. Nodes in wireless networks able to communicate with each different node placed inside a particular distance, known as transmission range. Once a node desires to send a packet to a different node that doesn't belong in its one-hop neighbourhood then it has to swear to intermediate nodes to forward the packets to the final destination. Thus, efficient routing protocols are needed in order to optimize the communication ways. Security problems in wireless communication may have a significant impact in different types of network architectures since many network architectures use wireless channels. As an example, a design using the 802.11 standard (usually referred as Wi-Fi or WLAN networks) uses a stationary infrastructure that communicates with different networks using a wired connection, however connects with the neighbors of its own network using a wireless channel. This design needs all the nodes to be placed inside the transmission area of the fixed infrastructure (access point), and any drawback concerning this central purpose might have an effect on the whole network. Wireless ad hoc networks or Mobile ad hoc Networks (MANETs) do not use a fixed infrastructure and all the nodes inside to the network could also be mobile. There's no central node acting as an access point, and mobile nodes share the responsibility of the proper functionality of the network, since a cooperative behaviour is required.

## 3. Security in MANETs

The fundamental nature of MANETs excite the emanation of recent security risks, whereas some present vulnerabilities in wired networks are accentuated. The use of security technologies built for wired networks to protect wireless networks isn't direct also not easy to perform. Within the absence of a wire connecting the nodes, any bad node might access the network without physical restraints. So as to stop dishonorable outsiders entering the network, cryptographic algorithms are often used to authenticate the nodes. However, additional difficult issues arise once an inside benign node is compromised, that is, if any assailant impersonates the identity of a node that's authorized in the network. Since the functionality of the network is typically based on a whole confidence between the participants, a bad node impersonating a trusty node might cause a significant security bridge. Most of the attacks in mobile environments focuses on routing protocols. These protocols were first off designed to be efficient without taking under consideration the protection problems. They typically need the collaboration between the entrants and assume confidence between them. Even so, a bad node might change its assumed benign functionality disturbing the general manner of the protocol. Below, a list of attacks is presented.

- Packet dropping attack: during this attack, the assailant rejects Route Error packets leading the truth nodes to forward packets in broken links [9].
- Flooding attack: The bad node broadcasts solid Route Request packets at random to any or all nodes each a hundred ms so as to overload the network [26].
- Black hole attack [20]: during this attack a bad node announces itself as having the shortest route to different nodes of the network. Nevertheless, as presently because it receives packets forwarded to different nodes, it drops them rather than forwarding to the ultimate destination. In our simulation situation, on every occasion a malicious black hole node receives a Route Request packet it sends a Route Reply packet to the destination on faith if it extremely contains a path towards the chosen destination. Thus, the black-hole node is always the primary node that responds to a Route Request packet. Moreover, the bad node falling all Route Reply and data packets it receives if the packets are destined to different nodes.
- Forging attack [25]: A bad node changes and broadcasts to the prey node Route Error packets resulting in repeated link features.

## 4. Intrusion Detection in MANETs

Nearly All researchers have two classify of attacks on the MANETs. They described attacks to passive and active. The passive attacks usually inclose only eaves dropping of data, while the active attacks inclose actions achieved by foes like replication, modification and deletion of changed data. Particularly, Attacks in MANET will cause congestion, propagate incorrect routing data, stop services from operating properly or termination them fully (Sharma & Sharma, 2011; Blazevic, et al., 2001).

Intrusion Detection systems (IDs) are software or hardware tools (even a combination of both) that automatically scan and monitor events in a laptop or network, searching for intrusive evidence [27]. Once planning an IDS to be utilized in a MANET, some considerations should be taken under consideration. There are many variations in the method the detection engine should behave with regard to a wired network IDS. A rather complete survey regarding this subject will be found in [11], wherever Anjum et al. present the most challenges to secure wireless mobile networks.

A lot of recently, Sen and Clark [28] have introduced a survey regarding existing intrusion detection approaches for MANETs. Traditional anomaly-based IDSs use predefined ‘‘normality’’ models to discover anomalies within the network. This can be an approach that cannot be simply deployed in MANETs, since the mobility and flexibility of MANET nodes, build hard the definition of ‘‘normal’’ and ‘‘malicious’’ behaviour. Moreover, the mobility of nodes leads to changes of the network topology, increasing the complexity of the detection method. In addition, since the MANET nodes haven't any fixed location, there's no central management and/or monitoring point wherever an IDS might be placed. This means that the detection method could also be distributed into many nodes, as well as the collection and analysis of data. Consequently, IDS are categorized into cooperative or independent (non-collaborative) [28].

Independent IDs are consist of IDs agents setted in the nodes of the network and be accountable for observing all nodes inside the network and sending alarms whenever they detect any suspect activity. the main trouble of this design is determining the place of the IDs agents, since nodes are moveable, and several domains of the network might not be monitored (for example, if the node hosting an IDs agent of one domain moves to another, the first remains

uncovered). Another drawback is that some resources such as bandwidth, central processing unit and/or power are scarce in these environments. Therefore, nodes hosting the IDs agents ought to be those having more resources and moreover, a bigger transmission vary. Maximizing the detection rate subject to resource limitation is a nondeterministic polynomial time (NP) complete problem and a few algorithms are planned to approximate the solution [11]. Several IDs architectures have been proposed to be used in mobile networks. The most updated IDs in the last three years ago are summarized.

Md Nasir Sulaiman, in 2015 [24] proposed a new classifier to enhance the abnormal attacks detection rate based on support vector machine (SVM) and genetic programming (GP). Depending on the experimental results, GPSVM classifier is controled to earn higher detection rate on the scarce abnormal attacks, without vital reduction on the general accuracy. This can be as a result of, GPSVM optimization mission is to confirm the accuracy is balanced between classes without reducing the generalization property of SVM, by an average accuracy of 88.51% .

Shankar Sriram V S, in 2017 [22], presented an adaptive, and a strong IDs technique using Hypergraph based Genetic algorithm (HG - GA) for parameter setting and feature selection in Support Vector Machine (SVM). Hyper – clique property of hypergraph was exploited for the generation of initial population to fasten the search for the optimum answer and to stop the trap at the local minima. HG-GA uses a weighted objective function to keep up the trade-off between increasing the detection rate and minimizing the false alarm rate, in conjunction with the optimum range of features. The performance of HG-GA SVM was evaluated using NSL-KDD intrusion dataset under two situations (i) All features and (ii) informative features obtained from HG – GA, with the Accuracy rate is 97.14% and the false rate is 0.83%.

Muder Almi'ani in 2018 [19], designed an intelligent IDs using clustered version of Self-Organized Map (SOM) network. The planned system consists of two subsequent stages: 1st, SOM network was designed, then a hierarchical agglomerative clustering using k-means was applied on SOM neurons. The proposed work in this research addressed the issues of sensitivity and time consumption for every connection record process. The proposed system was demonstrated using NSL-KDD benchmark dataset, wherever it's achieved superior sensitivity reached up to 96.66 you uninterested in less than 0.08 milliseconds per connection record.

The researches In 2017 and 2018 [14 and 15] tend to plan a novel approach for classifing MANETs attacks with a neutrosophic intelligent system based on genetic algorithm. Neutrosophic system could be a discipline that produces a mathematical formulation for the indeterminacy found in such complex situations. Neutrosophic rules compute with symbols rather than numeric values creating a good base for symbolic reasoning. These symbols ought to be carefully designed as they form the propositions base for the neutrosophic rules (NR) in the IDs. Every attack is set by MEM, NON_MEM and I degrees in neutrosophic system. The research proposed a MANETs attack inference by a hybrid framework of Self Organized Features Maps (SOFM) and the Genetic Algorithms (GA). The hybrid uses the unsupervised learning capabilities of the SOFM to determine the MANETs neutrosophic conditional variables. The neutrosophic variables along with the training information set are fed into the GA to find the most match neutrosophic rule set from a number of initial sub attacks according to the neutrosophic correlation coeffcient as a fitness function. This technique is designed to discover unknown attacks in MANETs. The simulation and experimental results are conducted on the KDD-99 network attacks data available in the UCI machine-learning repository for further process in knowledge discovery. The experiments cleared the feasibility of the proposed hybrid by an average accuracy of 99.3608 and false rate is 0.089.

It is clear that the neutrosophic IDs generated by GA takes highest precision percentage in comparision to all three classification based algorithms. Figure 1 refere to the corresponding chart for the result obtained in Table 1. Figure 2 shows the performance of existing and proposed neutrosophic IDs algorithm based on false alarm rate (FAR). Therefore our proposed neutrosophic IDs Algorithm [14 and 15] effectively detects attack with less false alarm rate.

| System name | Accuracy% | false rate% |
|---|---|---|
| GPSVM | 88.51 | 0.76 |
| HG-GA SVM | 97.14 | 0.83 |
| Clustered SOM | 96.66 | 0.08 |
| neutrosophic intelligent system based on genetic algorithm | 99.3608 | 0.089 |

**Table 1:** Performance of Neutrosophic genetic algorithm vs. existing algorithms

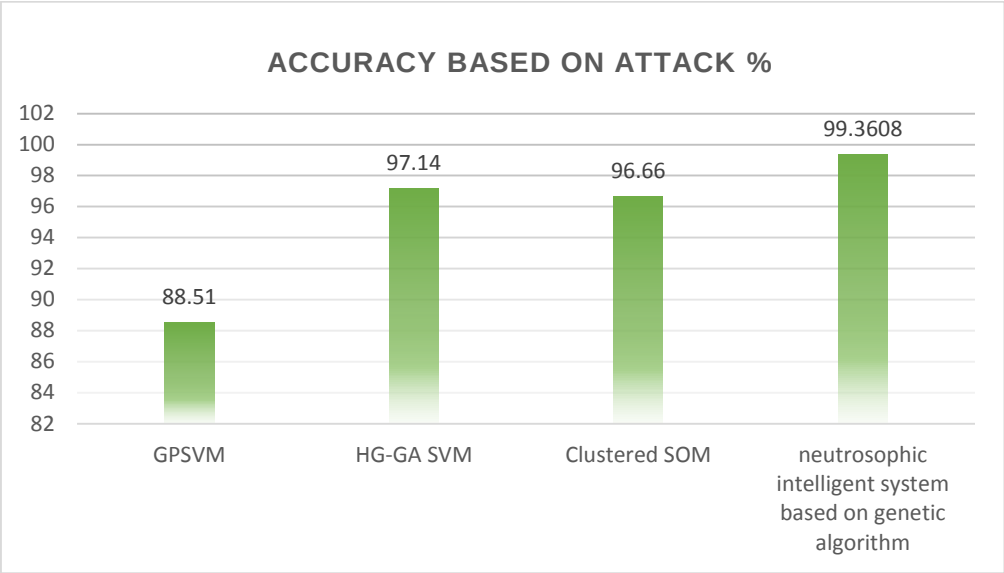


**Figure 1**: Results of neutrosophic genetic algorithm vs. existing algorithms

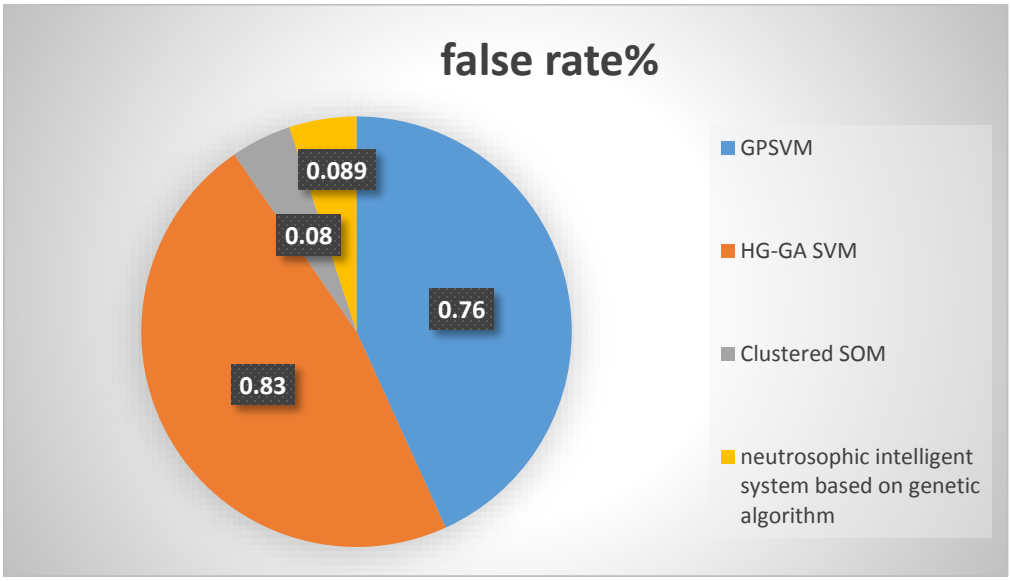


**Figure 2**. False alarm rate of proposed neutrosophic genetic algorithm vs. existing algorithms.

## 5. Conclusions

Detecting bad activities in MANETs might be a complicated mission because of the inherent features of those networks, like the mobility of the nodes, the shortage of a fixed design as well as the severe resource constraints. There's a pressing need to safeguard these communication networks and to propose efficient mechanisms in order to discover malicious behaviour. This article offers a comparison of the effectiveness of various classifiers which will use as intrusion detection algorithms in MANETs. Results show that Neutrosophic intrusion detection system relyied on GA could also be a good paradigm to use once the goal is to detect and to point that is the specific attack launched. The analysis of the classifiers is performed considering that the intrusion detection process is totally distributed and each node of the network hosts an independent intrusion detection agent.

## References:


[1] A. A. Salama, Florentin Smarandache, S. A. Alblowi, New Neutrosophic Crisp Topological Concepts, Neutrosophic Sets and Systems, 2014.

[2] A. A. Salama, Florentin Smarandache, Hewayda ElGhawalby : Neutrosophic Approach to Grayscale Images Domain, Neutrosophic Sets and Systems, vol. 21, 2018, pp. 13-19. https://doi.org/10.5281/zenodo.1408681.

[3] A. A. Salama, Florentin Smarandache, Mohamed Eisa: Introduction to Image Processing via Neutrosophic Techniques, Neutrosophic Sets and Systems, Vol. 5, 2014, pp. 59-64.doi.org/10.5281/zenodo.571456.

[4] A. A. Salama, Mohamed Eisa, S.A.El-Hafeez, M. M. Lotfy: Review of Recommender Systems Algorithms Utilized in Social Networks based e-Learning Systems & Neutrosophic System, Neutrosophic Sets and Systems, vol. 8, 2015, pp. 32-41. doi.org/10.5281/zenodo.571583.

[5] A. Salama, Haitham A. El-Ghareeb, Ayman M. Manie, Florentin Smarandache: Introduction to Develop Some Software Programs for Dealing with Neutrosophic Sets, Neutrosophic Sets and Systems, vol. 3, 2014, pp. 51-52. doi.org/10.5281/zenodo.571453.

[6] A.A.Salama,Mohamed Eisa, Hewayda ElGhawalby, A.E. Fawzy: Neutrosophic Features for Image Retrieval,Neutrosophic Sets and Systems, vol. 13, 2016, pp. 56-61.doi.org/10.5281/zenodo.570857.

[7] A. A. Salama, Basic Structure of Some Classes of Neutrosophic Crisp Nearly Open Sets and Possible Application to GIS Topology, Neutrosophic Sets and Systems, 2015, Volume 7, pp. 18-22.

[8] A. Perrig, R. Canetti, D. Tygar and D. Song, "The TESLA Broadcast Authentication Protocol," RSA CryptoBytes, 5 (Summer), 2002.

[9] D. Djenouri, O. Mahmoudi, M. Bouamama, D. Llewellyn-Jones, M. Merabti, On securing MANET routing protocol against control packet dropping, in: Proceedings of the International Conference on Pervasive Services, IEEE Computer Society, CA, USA, 2007, pp. 100–108.

[10] Eman.M.El-Nakeeb, Hewayda ElGhawalby, A.A. Salama, S.A.El-Hafeez: Neutrosophic Crisp Mathematical Morphology, Neutrosophic Sets and Systems, Vol. 16 (2017), pp. 57-69. doi.org/10.5281/zenodo.831936

[11] F. Anjum, P. Mouchtaris, Security for Wireless Ad Hoc Networks, Wiley-Interscience, 2007.

[12] F. Smarandache, Neutrosophy, Neutrosophic Probability, Set and Logic, Amer. Res. Press, Rehoboth, USA., (1998), p. 105, http://fs.gallup.unm.edu/eBook-neutrosophics4.pdf (fourth version).

[13] ] F. Smarandache, Neutrosophic set, a generalisation of the intuitionistic fuzzy sets, Inter. J. Pure Appl. Math., 24, (2005), 287-297.

[14] Haitham Elwahsh, Mona Gamal, A. A. Salama, Modeling Neutrosophic Data by Self-Organizing Feature Map: MANETs Data Case Study, Procedia Computer Science, 2017, Volume 121, pp 152-159, DOI.org/10.1016/j.procs.2017.11.021.

[15] Haitham Elwahsh, Mona Gamal, A. A. Salama, A Novel approach for classify MANETs attacks with a neutrosophic intelligent system based on genetic algorithm, , Security and Communication Networks, 2018, Accepted.

[16] Haitham Elwahsh, Mohamed Hashem , Mohamed Amin, "Secure Service Discovery Protocols for Ad Hoc Networks", Springer (LNCS) in Computer Science, Advances in Computer Science and Information Technology Communications in Computer and Information Science, 2011, Volume 131, Part 1, 147-157, DOI: 10.1007/978-3-642-17857-3_15

[17] K. Atanassov, Intuitionistic Fuzzy Set, Fuzzy Sets and Systems, 1986, Volume 20, pp. 87-96.

[18] KDD Cup 1999 Data, https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[19] Muder Almi'ani, Alia Abu Ghazleh, Amer Al-Rahayfeh, Abdul Razaque, Intelligent Intrusion Detection System Using Clustered Self Organized Map, 2018 Fifth International Conference on Software Defined Systems (SDS), DOI: 10.1109/SDS.2018.8370435.

[20] M. Al-Shurman, S.-M. Yoo, S. Park, Black-hole attack in mobile ad hoc networks, in: Proceedings of the 42nd Annual Southeast Regional Conference, ACM-SE 42, ACM, New York, NY, USA, 2004, pp. 96–97.

[21] M. G. Zapata, "Secure Ad Hoc On-Demand Distance Vector (SAODV) Routing," ACM Mobile Computing and Communication Review (MC2R), Vol. 6, No. 3, pp. 106-107, July 2002.

[22] M.R. Gauthama Raman , Nivethitha Somu , Kannan Kirthivasan , Ramiro Liscano , V.S. Shankar Sriram , An Effcient Intrusion Detection System based on Hypergraph - Genetic Algorithm for Parameter Optimization and Feature Selection in Support Vector Machine, Knowledge-Based Systems (2017), doi: 10.1016/j.knosys.2017.07.005

[23] Mitra. S, Pal. S.K., Self-organizing neural network as a fuzzy classifier, IEEE, 1994, Volume 24, pp 385–399.

[24] Muhammad Syafiq Mohd Pozi, Md Nasir Sulaiman, Norwati Mustapha, Thinagaran Perumal, Improving Anomalous Rare Attack Detection Rate for Intrusion Detection System Using Support Vector Machine and Genetic Programming. Neural Process Lett (2016) 44:279–290. DOI 10.1007/s11063-015-9457-y.

[25] P. Ning, K. Sun, How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols, Ad Hoc Networks 3 (2005) 795–819.

[26] P. Yi, Y.F. Hou, Y. Zhong, S. Zhang, Z. Dai, Flooding attack and defence in ad hoc networks, Journal of Systems Engineering and Electronics 17 (2006) 410–416.

[27] R. Bace, P. Mell, NIST Special Publication on Intrusion Detection Systems, Technical Report, National Institute of Standards and Technologies, 2001.

[28] S. Sen, J.A. Clark, Intrusion Detection in Mobile Ad Hoc Networks, Springer, 2008, pp. 427–454.

[29] Y. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks," Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MobiCom'02), pp. 12-23, September 2002.
[30] Y. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02), pp. 3-13, June 2002.
[31] Y. Zhang, W. Lee, and Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003.

Received: October 13, 2018. Accepted: November 6, 2018