Mobile Ad Hoc networks intrusion detection system against packet dropping attacks

Oussama Sbai, Mohamed Elboukhari
Department of Applied Engineering, ESTO (Higher School of Technology) Mohammed 1st University, Oujda, Morocco

Article Info

Article history:

Received Jul 30, 2021
Revised Feb 11, 2022
Accepted Mar 10, 2022

Keywords:

Blackhole attack
Grayhole attack
IDS
Machine learning
ns-3 simulator
Selfishness attack

ABSTRACT

Due to the extreme lack of a stable infrastructure, also self-organization of network components, unpredictable network topologies, and the lack of a central authority for routing, security assurance in mobile Ad Hoc networks (MANETs) is an important and difficult challenge. Among the famous threat that MANETs suffer from: blackhole, grayhole, and selfishness attacks, because the target of these attacks is to drop packets and disturb the routing operation of the network. A scalable, reliable, and robust network intrusion detection system (NIDS) should be created to effectively combat these families of network layer routing assaults in order to offer high availability for MANETs. In this paper, we present a MANETs-IDS based on machine learning algorithm against blackhole, grayhole, and selfishness attacks with Ad Hoc on-demand distance vector (AODV) routing protocol (RFC 3561) and optimized link state routing (OLSR) potocol (RFC 3626), using ns-3 simulation platform. Our simulation took into consideration the density of the network and a random mobility model of nodes. The obtained experimental results show that the proposed detection algorithm reached very promoting performances (in term of accuracy, processing time, time to build the model, precision, recall, F-measure).

Corresponding Author:

Oussama Sbai
Department of Applied Engineering, ESTO (Higher School of Technology) Mohammed 1st University
Oujda, Morocco
Email: o.sbai@ump.ac.ma

1. INTRODUCTION

Mobile Ad Hoc networks (MANETs) have gained a significant reputation and researchers' interest in recent years, on top of that is being a type of important future wireless networks generations. The MANETs are specifically used in homes and enterprise networking for information sharing, also in areas where wired and fixed infrastructure is not viable, like: Tactical networks (battlefields), calamity management, maritime communications, and rescue operations. In addition, MANETs are a back bone of the internet of things (IoT) [1], [2], and a key part of the intelligent transportation systems (ITS) [3]–[5]. The MANETs as their name defines them allow devices to communicate with each other through local wireless connections, what make them inexpensive to put up anywhere, because they do not require any special infrastructure for deployment.

In MANETs, the nodes are in permanent movement, the network is unstructured, and the communication medium is almost open, which means that the infiltration of the malicious nodes in the network is frequent and easy. Therefore, the routing protocols cannot determine the legitimacy of the intermediate nodes, and consequently several attacks appear, like the blackhole and grayhole attacks, overall data packets dropping attacks, or attacks that target privacy and confidentiality of information circulating in the network, or those that touch the integrity of data packets.

The blackhole, grayhole, selfishness are an active attacks, where the objective of the malicious node is to disrupt the network availability and service integrity [6]. Also, they produce the famous denial of service (DoS) problem [7]. In blackhole attack, the malicious node use the following technique: it sends out false routing information, pretending to have found the best path, causing other good nodes to route data packets via him, after that is dropping all received packets. The grayhole attack is the variety of the blackhole attack, which a malicious node's action is extremely unpredictable, it removes only packets from a specific source or destined for a specific destination, or the malicious node alternate between a benign behavior and other malicious. For selfishness attack, the malicious node will be selfish by refusing to collaborate with his neighbors to route the packets to their destination, consequently these latter will be dropped by malicious node. In the previous work [8], we studied the impact of the blackhole attack in both Ad Hoc on-demand distance vector (AODV) [9] and optimized link state routing (OLSR) [10] protocols by ns-3 simulator [11], and we deduced the blackhole attack has a significant negative impact on the network performance in term of packet delivery ratio (PDR) and routing overhead. To strength the underlying routing protocol of MANETs, they are forced to implement the intrusion detection systems (IDS). IDS are considered as the second layer of network protection, they are the plans responsible of perceiving spiteful exercises by overseeing executions made in the network. They spot the irregular execution or abnormal activity and take the appropriate response against it.

In MANETs intrusion detection literature, a number of important techniques that have been proposed [12]–[14]. More potential can be seen in machine learning approaches. The goal of machine learning (ML) algorithms is to create a system that consistently upgrade its performance based on previous outcomes, also based on the data acquired, they can also adapt to new archetype in the network. Wherefore, in this manuscript, we choose the technique of ML-based IDS to detect blackhole, grayhole, and selfishness attacks for network implemented Ad Hoc on-demand distance vector (AODV) [9] or optimized link state routing (OLSR) [10] protocols.

The reminder of this paper is organized as follows: section 1 presents MANET's environment, data packets dropping attacks of MANETs and the definition of IDS. Section 2 describes the related work. In section 3 we define proposed architecture and methodologies. Statistical measures are defined in section 4. The experimental environment set-up and the experimental results are given in section 5. Finally, a conclusion is in the last section.

2. LITERATURE REVIEW

In the last few years, several studies in IDS for MANETs and their derivate like vehicular Ad Hoc networks (VANETs) on adopting the ML approach have been done. Centered on the principle of distributed ensemble learning, this work [15] proposes a collaborative behavior-based intrusion detection system for VANETs on using random forest algorithm and NSL-KDD [16] dataset. A hybrid based IDS with the response action in the same framework are presented in [17] for MANETs against routing attacks, which are blackhole, grayhole, Sleep deprivation and rushing attacks. The technique used is a combination of ABID to detect the anomalies and KBID to identify the attack to lunch the adequate response action, and the data used to test the proposed system is generated by the ns-2 simulator. Rajalakshmi and Meena [18] presents a fuzzy based intrusion detection (FBID) system for MANETs, to identify, analyze and detect a malicious node in different circumstances. Basomingera and Choi [19] a supervised/unsupervised, cluster/host based intrusion detection system for MANETs is devloped, and the detection system gains knowledge from a dataset of route caches. In this work [20], the authors advance a distributed NIDS for DDoS attack detection based on random forest (RF) algorithm for VANETs. It uses a distributed architecture to collect and process network traffic. In addition, this proposed NIDS use Apache Spark for feature extraction and model training of the cleaned data. To test their solution, Moustafa and Slay use UNSW-NB15 [21] and NSL-KDD [16] datasets.

3. PROPOSED ARCHITECTURE ANDCORE FUNCTIONALITY

To insure the scalability of our proposed MANET-IDS, we use a clustering-based scheme in MANETs [22], with a security mechanism [23] to protect communication between cluster heads (CH) and cluster nodes (CNs). We suppose that is already made and the list of CH is available, the details of these mechanisms are outside the scope of the work in this paper, so in this work, we focus only on performing better IDS that will be employed on this CH. The proposed MANET-IDS collects periodically data to initiate intrusion detection and response actions for the duration of the network's life. During the data collection phase, the CHs collect data periodically from the CNs inside their virtual clusters see Figure 1. The features used reflect both the routing cache data selected from the routing table of nodes and the network performance: Round-trip time (RTT), percentage of packet loss and number of packets received. The Table 1 describes the features received to use in the machine learning process.

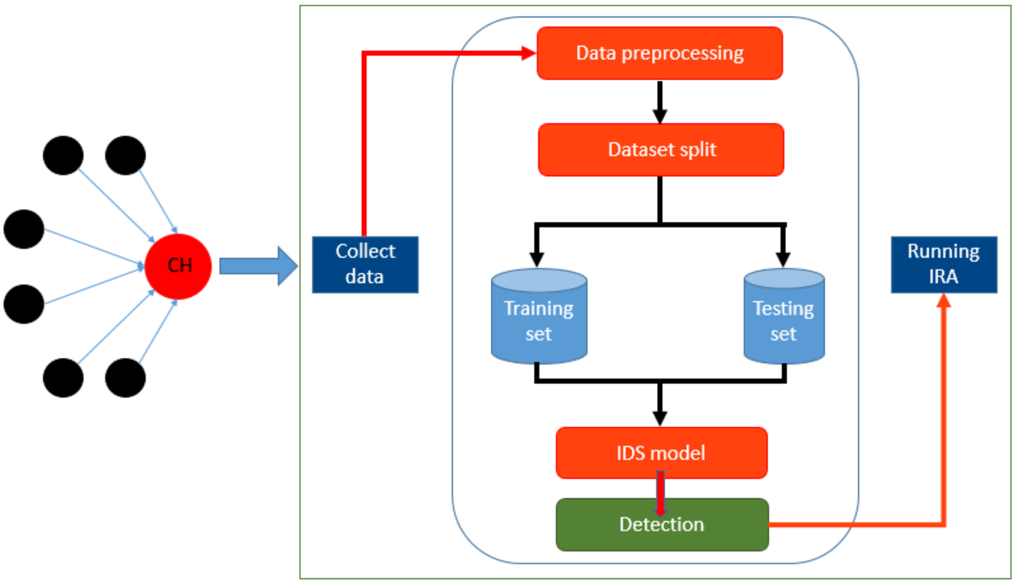

Figure 1. Architecture of proposed methodology

After detection of attacks, the next step is to launch an intrusion response action (IRA) [17]. In our case, and because the network performance has degraded considerably since the blackhole, grayhole and selfish attacks was existed in the network, we propose to adopt the solution of isolation of malicious nodes, by treating them as non-existent. For using this IRA, network nodes must enforce this restriction in reference to routing service and data sending: do not forward any data packets generated by or sent to the malicious nodes, or route them through these nodes; and do not send any routing packets to or through the malicious nodes, and ignore all routing packets originating from these nodes.

Table 1. Selected features

AODV features		OLSR features	
Feature	Description	Feature	Description
Destination	@IP of node destination	Source	@IP of node source
Gateway	@IP of node Gateway	Destination	@IP of node destination
Interface	@IP of node source	NextHop	@IP of next node
Flag	State and routing flags	Distance	The number of hops from the Originator @IP to the node destination
Expire	Expiration or deletion time of the route	Local time	The recording time of the route
Hops	The number of hops from the Originator @IP to the node destination	Number Packet received	Number Packet received by the route
Local time	The recording time of the route	RTT min	Minimum value of Round-trip time
Number Packet received	Number Packet received by the route	RTT avg	Average value of Round-trip time
RTT min	Minimum value of Round-trip time	RTT max	Maximum value of Round-trip time
RTT avg	Average value of Round-trip time	RTT mdev	Standard deviation value of Round-trip time
RTT max	Maximum value of Round-trip time	Packet loss %	Percentage Packet loss by the route
RTT mdev	Standard deviation value of Round-trip time	Label	Label of attack
Packet loss %	Percentage Packet loss by the route		
Label	Label of attack		

4. STATISTICAL MEASURES

To can evaluate the performance of the ML-IDS model, we use accuracy, precision, F-Measure and recall. In addition, we mesure the time taken to build the ML-IDS model or training time (Tr-time) plus the processing time (P-time) which is the amount of time that use for detecting the attack, in our case we measure the time taken to test the ML-IDS model.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{1}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP}+\text{FP}} \tag{2}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP}+\text{FN}} \tag{3}$$

$$\text{F} - \text{Measure} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{4}$$

5. EXPERIMENT RESULTS AND DISCUSSION

To simulate the MANETs network, we use ns-3 simulator [11]. The simulation runs for 60 seconds, on sending one packet per second, using IEEE 802.11ac protocol for MAC layer [24], in an area of 1000 x 1000 metre. The number of network nodes varies between 10 and 80 nodes which are randomly distributed and mobile on used the random way-point mobility model to have more general node mobility [25]. In addition, we use the parameter pause with constant random variable by 30th second for OLSR protocol, to reduce the mobility period nodes, because this protocol is used in network are not very mobile. On the other hand, for AODV protocol, we use the parameter pause with constant random variable by Constant=0, which means no pause period in this environment, because the AODV protocol is considered for hyper mobile network. Waikato environment for knowledge analysis (WEKA) toolbox [26], was used for running the different machine learning algorithm in the simulation experiments to evaluate the proposed dataset.

We apply most used supervised learning methods to be able to carry out a large-scale empirical comparison: J48 decision tree, random forest (RF), random tree (RT), Naïve Bayes (NB), Bayesian network (Bnet), sequential minimal optimization (SMO), support vector machine (SVM) and logistic regression. The machine learning algorithms used to detect studied attacks in a different network's topology: from 10 nodes in network to 80 nodes, for both AODV and OLSR protocols. Remember that this is a multiple classification of blackhole, grayhole and selfishness attacks and normal behavior of nodes. On comparing results of supervised learning algorithms shown in Tables 2 and 3 (see *Appendix)*, we found the results are in the interval 95% and 100% for accuracy, precision, recall and F-measure. The comparison of AODV and OLSR results denote the four algorithms: J48, RF, SMO and logistic give the best results with 100% in term of accuracy, precision, recall and F-measure. Then to decide, we take in consideration the results of the parameters time to build the model and processing time of machine learning algorithms (the both parameters are in second), by calculating the average of these parameters for each algorithm:

- In AODV: J48 (Tr-time 0.26 second, P-time 0.08 second); RF (Tr-time 7.72, P-time 0.55); SMO (Tr-time 52.16, P-time 0.22); Logistic (Tr-time 43, P-time 0.17).
- In OLSR: J48 (Tr-time 0.33 second, P-time 0.05 second); RF (Tr-time 10.43, P-time 0.67); SMO (Tr-time 60.93, P-time 0.32); Logistic (Tr-time 38.53, P-time 0.22).

We constat, for AODV protocol the J48 algorithm outperforms FR, SMO and Logistic based on Tr-time by 7.46 seconds, 51.9 seconds and 42.74 seconds, respectively. We can see that P-time of the J48 algorithm outperforms FR, SMO and Logistic, by 0.47 second, 0.14 second and 0.09 second, respectively. For OLSR protocol, the J48 algorithm outperforms FR, SMO and Logistic based on Tr-time by 10.1 seconds, 60.6 seconds and 38.2 seconds, respectively. Furthermore, in term of P-time we can see the J48 algorithm outperforms FR, SMO and Logistic, by 0.62 second, 0.27 second and 0.17 second, respectively. Ultimately, the last comparaison show the J48 give the best results in terme of performance and time (is the fastest).

6. CONCLUSION

In this paper, we proposed a MANETs-IDS based on the machine learning approach for detecting and preventing the effect of a blackhole, grayhole and selfishness attacks, the variety of dropped packet attack which suffers MANETs and their sub-class like VANETs. In our method, we use routing table information plus QoS metric as a feature to analyze network's performance and detect the attacks, by taking into consideration of a number of network's node. The effectiveness of J48 is evaluated by comparing it with other machine learning algorithms. According to the experimental results, J48 has a good detection efficiency against the four attacks sited above. As a future work, we are concentrating to extend our research to evaluate the effect of J48 in the experimental MANETs and to detect more attacks in a mobile Ad Hoc network.

APPENDIX

Table 2. AODV simulation results

Network	10 nodes	20	30	40	50	60	70	80
				AODV				
				Accuracy				
J48	100	100	100	100	100	100	100	100
RF	100	100	100	100	100	100	100	100
RT	99,2462	100	99,7424	99,651	99,5164	100	99,926	99,9268
NB	97,9899	97,02	98,0032	98,5294	99,445	99,6708	99,1428	99,516
SMO	100	100	100	100	100	100	100	100
SVM	95,2261	99,3649	99,3559	99,7757	99,9604	99,9029	99,9416	99,9346
Logistic	100	100	100	100	100	100	100	100
Bnet	98,995	99,8046	99,9034	99,7507	99,889	99,9083	99,9688	99,9608
				Precision				
J48	100	100	100	100	100	100	100	100
RF	100	100	100	100	100	100	100	100
RT	99,3	100	99,7	99,7	99,5	100	99,9	99,9
NB	98,1	97,3	98,3	98,8	99,5	99,7	99,4	99,7
SMO	100	100	100	100	100	100	100	100
SVM	95,6	99,4	99,4	99,8	100	99,9	99,9	99,9
Logistic	100	100	100	100	100	100	100	100
Bnet	99,1	99,8	99,9	99,8	99,9	99,9	100	100
				Recall				
J48	100	100	100	100	100	100	100	100
RF	100	100	100	100	100	100	100	100
RT	99,2	100	99,7	99,7	99,5	100	99,9	99,9
NB	98	97	98	98,5	99,4	99,7	99,1	99,5
SMO	100	100	100	100	100	100	100	100
SVM	95,2	99,4	99,4	99,8	100	99,9	99,9	99,9
Logistic	100	100	100	100	100	100	100	100
Bnet	99	99,8	99,9	99,8	99,9	99,9	100	100
				F-Measure				
J48	100	100	100	100	100	100	100	100
RF	100	100	100	100	100	100	100	100
RT	99,2	100	99,7	99,7	99,5	100	99,9	99,9
NB	98	97,1	98,1	98,6	99,5	99,7	99,2	99,6
SMO	100	100	100	100	100	100	100	100
SVM	95,1	99,4	99,3	99,8	100	99,9	99,9	99,9
Logistic	100	100	100	100	100	100	100	100
Bnet	99	99,8	99,9	99,8	99,9	99,9	100	100
				Time to build the model				
J48	0,04	0,1	0,08	0,21	0,21	0,26	0,38	0,84
RF	0,64	1,07	0,9	3,76	6,59	11,56	15,01	22,26
RT	0	0,01	0,03	0,04	0,09	0,16	0,18	0,27
NB	0,02	0,12	0,06	0,08	0,35	0,4	0,41	0,32
SMO	0,65	3,64	6,67	26,26	65,29	84,88	107,36	122,53
SVM	0,81	5,18	8,1	69,78	155,29	211,86	363,63	1088,04
Logistic	0,45	1,19	2,46	6,03	18,89	123,94	76,94	114,15
Bnet	0,16	0,26	0,08	0,23	0,34	0,69	0,87	1
				Time to test the model				
J48	0,01	0,01	0,01	0,01	0,04	0,26	0,34	0,03
RF	0,05	0,07	0,07	0,28	0,38	1,27	1,15	1,13
RT	0	0	0	0,02	0,02	0,04	0,21	0,05
NB	0,03	0,16	0,09	0,15	0,63	0,68	0,53	0,66
SMO	0,02	0,01	0,02	0,05	0,13	0,21	0,29	1,05
SVM	0,18	0,69	1,17	6,67	10,28	17,08	26,46	52,04
Logistic	0,02	0,01	0,04	0,04	0,05	0,17	0,22	0,84
Bnet	0,04	0,06	0,02	0,09	0,08	0,09	0,16	0,22

Table 3. OLSR simulation results

Network	10 nodes	20	30	40	50	60	70	80
				OLSR				
				Accuracy				
J48	100	100	100	100	100	100	100	100
RF	100	100	100	100	100	100	100	100
RT	99,789	99,8339	100	100	100	99,7633	99,6451	100
NB	99,3671	99,0864	99,5434	99,3379	99,7831	98,1959	99,7274	99,3736
SMO	100	100	100	100	100	100	100	100
SVM	96,8354	99,9169	99,3773	99,9172	99,9797	99,9316	99,9897	99,9944
Logistic	100	100	100	100	100	100	100	100
Bnet	99,789	99,6678	100	99,8581	99,9797	99,8843	99,9743	99,9574
				Precision				
J48	100	100	100	100	100	100	100	100
RF	100	100	100	100	100	100	100	100
RT	99,8	99,8	100	100	100	99,8	99,6	100
NB	99,4	99,1	99,6	99,3	99,8	98,5	99,8	99,5
SMO	100	100	100	100	100	100	100	100
SVM	97,3	99,9	99,4	99,9	100	99,9	100	100
Logistic	100	100	100	100	100	100	100	100
Bnet	99,8	99,7	100	99,9	100	99,9	100	100
				Recall				
J48	100	100	100	100	100	100	100	100
RF	100	100	100	100	100	100	100	100
RT	99,8	99,8	100	100	100	99,8	99,6	100
NB	99,4	99,1	99,5	99,3	99,8	98,2	99,7	99,4
SMO	100	100	100	100	100	100	100	100
SVM	96,8	99,9	99,4	99,9	100	99,9	100	100
Logistic	100	100	100	100	100	100	100	100
Bnet	99,8	99,7	100	99,9	100	99,9	100	100
				F-Measure				
J48	100	100	100	100	100	100	100	100
RF	100	100	100	100	100	100	100	100
RT	99,8	99,8	100	100	100	99,8	99,6	100
NB	99,4	99,1	99,5	99,3	99,8	98,3	99,7	99,4
SMO	100	100	100	100	100	100	100	100
SVM	96,7	99,9	99,3	99,9	100	99,9	100	100
Logistic	100	100	100	100	100	100	100	100
Bnet	99,8	99,7	100	99,9	100	99,9	100	100
				Time to build the model				
J48	0,08	0,09	0,09	0,2	0,22	0,27	0,6	1,1
RF	0,55	0,35	1,11	3,91	8,04	11,24	28,99	29,29
RT	0	0,01	0,02	0,07	0,15	0,15	0,17	0,38
NB	0,04	0,02	0,03	0,07	0,15	0,22	0,34	0,53
SMO	0,84	1,86	6,39	33,95	65,95	80,68	118,79	179
SVM	0,93	2	4,91	57,49	133,39	195,11	1097,3	3302,91
Logistic	0,28	0,55	1,82	22,88	53,01	21,03	59,15	149,54
Bnet	0,13	0,1	0,14	0,33	0,34	0,47	1,12	1,64
				Time to test the model				
J48	0,02	0,02	0	0,01	0,02	0,02	0,05	0,32
RF	0,07	0,04	0,05	0,23	0,55	0,56	1,39	2,51
RT	0,01	0	0	0,01	0,02	0,05	0,05	0,08
NB	0,03	0,04	0,05	0,21	0,22	0,3	0,7	1,3
SMO	0,02	0,01	0,02	0,07	0,13	0,2	1,22	0,89
SVM	0,11	0,46	0,66	6,69	14,13	12,53	74,13	93,9
Logistic	0,01	0,01	0,01	0,03	0,05	0,11	0,94	0,6
Bnet	0,02	0,01	0,03	0,04	0,06	0,13	0,19	0,4

REFERENCES

[1] J. Karlsson, L. S. Dooley, and G. Pulkkis, "Secure routing for MANET connected internet of things systems," *Proceedings - 2018 IEEE 6th International Conference on Future Internet of Things and Cloud, FiCloud 2018*, 2018, pp. 114–119, doi: 10.1109/FiCloud.2018.00024.

[2] B. K. Tripathy, S. K. Jena, V. Reddy, S. Das, and S. K. Panda, "A novel communication framework between MANET and WSN in IoT based smart environment," *International Journal of Information Technology (Singapore)*, vol. 13, no. 3, pp. 921–931, 2021, doi: 10.1007/s41870-020-00520-x.

[3] A. Lamssaggad, N. Benamar, A. S. Hafid, and M. Msahli, "A survey on the current security landscape of intelligent transportation systems," *IEEE Access*, vol. 9, no. Vlc, pp. 9180–9208, 2021, doi: 10.1109/ACCESS.2021.3050038.

[4] G. Li, Q. Sun, L. Boukhatem, J. Wu, and J. Yang, "Intelligent vehicle-to-vehicle charging navigation for mobile electric vehicles via vanet-based communication," *IEEE Access*, vol. 7, pp. 170888–170906, 2019, doi: 10.1109/ACCESS.2019.2955927.

[5] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected vehicles: Solutions and challenges," *IEEE Internet of Things Journal*, vol. 1, no. 4, pp. 289–299, 2014, doi: 10.1109/JIOT.2014.2327587.

[6] O. Sbai and M. Elboukhari, "Classification of mobile Ad Hoc networks attacks," *Colloquium in Information Science and Technology, CIST*, vol. 2018-October, pp. 618–624, 2018, doi: 10.1109/CIST.2018.8596391.
[7] Z. A. Zardari *et al*., "A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in MANETs," *Future Internet*, vol. 11, no. 3, 2019, doi: 10.3390/fi11030061.
[8] O. Sbai and M. Elboukhari, "Simulation of MANET's single and multiple blackhole attack with NS-3," *Colloquium in Information Science and Technology, CIST*, vol. 2018-October, pp. 612–617, 2018, doi: 10.1109/CIST.2018.8596606.
[9] C. Perkings, E. Belding-Royer, and S. Das, "Ad Hoc on-demand distance vector (AODV) routing," *Ietf Rfc 3561. RFC Editor*, pp. 1–37, 2003, [Online]. Available: http://tools.ietf.org/pdf/rfc3561.pdf
[10] T. Clausen and P. Jacquet, "Optimized link state routing protocol (OLSR)," Project Hipercom, INRIA, pp. 1–75, 2003, [Online]. Available: https://www.rfc-editor.org/info/rfc3626
[11] G. F. Riley and T. R. Henderson, "The ns-3 network simulator," in *Modeling and Tools for Network Simulation, Berlin, Heidelberg: Springer Berlin Heidelberg*, 2010, pp. 15–34.
[12] A. Nadeem and M. P. Howarth, "A survey of manet intrusion detection and prevention approaches for network layer attacks," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 4, pp. 2027–2045, 2013, doi: 10.1109/SURV.2013.030713.00201.
[13] S. Kumar and K. Dutta, "Intrusion detection in mobile Ad Hoc networks: techniques, systems, and future challenges," *Security and Communication Networks*, vol. 9, no. 14, pp. 2484–2556, Sep. 2016, doi: 10.1002/sec.1484.
[14] K. Khan, A. Mehmood, S. Khan, M. A. Khan, Z. Iqbal, and W. K. Mashwani, "A survey on intrusion detection and prevention in wireless ad-hoc networks," *Journal of Systems Architecture*, vol. 105, no. December 2019, p. 101701, 2020, doi: 10.1016/j.sysarc.2019.101701.
[15] F. A. Ghaleb *et al*., "Misbehavior-aware on-demand collaborative intrusion detection system using distributed ensemble learning for VANET," *Electronics (Switzerland)*, vol. 9, no. 9, pp. 1–17, 2020, doi: 10.3390/electronics9091411.
[16] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," *Wer sind Social Entrepreneurs in Deutschland?*, no. Cisda, pp. 21–38, 2009, doi: 10.1007/978-3-531-94152-3_2.
[17] A. Nadeem and M. P. Howarth, "An intrusion detection and adaptive response mechanism for MANETs," *Ad Hoc Networks*, vol. 13, no. PART B, pp. 368–380, 2014, doi: 10.1016/j.adhoc.2013.08.017.
[18] D. Rajalakshmi and K. Meena, "A hybrid intrusion detection system for mobile adhoc networks using fbid protocol," *Scalable Computing*, vol. 21, no. 1, pp. 137–145, 2020, doi: 10.12694/SCPE.V21I1.1642.
[19] R. Basomingera and Y. J. Choi, "Learning from routing information for detecting routing misbehavior in Ad Hoc networks," *Sensors (Switzerland)*, vol. 20, no. 21, pp. 1–22, 2020, doi: 10.3390/s20216275.
[20] Y. Gao, H. Wu, B. Song, Y. Jin, X. Luo, and X. Zeng, "A distributed network intrusion detection system for distributed denial of service attacks in vehicular Ad Hoc network," *IEEE Access*, vol. 7, pp. 154560–154571, 2019, doi: 10.1109/ACCESS.2019.2948382.
[21] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *2015 Military Communications and Information Systems Conference, MilCIS 2015 - Proceedings*, 2015, pp. 1–6, doi: 10.1109/MilCIS.2015.7348942.
[22] T. Rahman, I. Ullah, A. U. Rehman, and R. A. Naqvi, "Clustering schemes in MANETs: Performance evaluation, open challenges, and proposed solutions," *IEEE Access*, vol. 8, no. January, pp. 25135–25158, 2020, doi: 10.1109/ACCESS.2020.2970481.
[23] Y. Cai, H. Zhang, and Y. Fang, "A conditional privacy protection scheme based on ring signcryption for vehicular Ad Hoc networks," *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 647–656, 2021, doi: 10.1109/JIOT.2020.3037252.
[24] Cisco, "802.11ac: The Fifth Generation of Wi-Fi," in Cisco.Com, no. 1, 2018, pp. 1–20.
[25] M. A. Nisar, A. Mehmood, A. Nadeem, and K. Ahsan, "A two dimensional performance analysis of mobility models for MANETs and VANETs," *Research Journal of Recent Sciences*, vol. 3, no. 5, pp. 94–103, 2014, [Online]. Available: www.isca.me
[26] L. Vinet and A. Zhedanov, Data Mining, vol. 18, no. 10s. Elsevier, 2000.

BIOGRAPHIES OF AUTHORS

Oussama Sbai is a PhD candidate in computer science at Mohammed 1st University, Oujda, Morocco. His research interests include network security and network IDS using machine learning and deep learning. He can be contacted at email: o.sbai@ump.ac.ma.

Mohamed Elboukhari received the DESA (diploma of high study) degree in numerical analysis, computer science and treatment of signal in 2005 from the faculty of Science, Mohammed 1st University, Oujda, Morocco. He is currently professor, department of Applied Engineering, ESTO, Mohammed 1st University, Oujda, Morocco. His research interests include cryptography, quantum cryptography and wireless network security, Mobile Ad Hoc Networks (MANETs). He can be contacted at email: elboukharimohamed@gmail.com.