Yates Algorithm to Analyze the Performance of MANET Routing Protocol

A. Nabou1, MD. Laanaoui 2, M. Ouzzif 1 and MA. El Houssaini3

1RITM Laboratory, CED Engineering Sciences, EST, ENSEM, Hassan II University of Casablanca, Morocco
2Department of Computer Sciences, Faculty of Sciences and Techniques, Cadi Ayyad University of Marrakech, Morocco
3Laboratory STIC, ESEF, Chouaib Doukkali University, El Jadida, Morocco

E-mail: d.laanaoui@uca.ma

Abstract. To test the performance of any routing protocol in Mobile Ad hoc Network (MANET), the re-searchers simulate their scenarios several times with different simulators to get either positive or negative results. This operation of the simulation can last many hours and sometimes several days depending on the performance either of the software or the hardware, and the number of factors used to analyze. In this paper, we propose a new method reckons on the Yates algorithm that are considered as a solution to evaluate the performance of any MANET routing protocols under the effect of any number of factors. This approach allows creating a simulation model in the form of mathematical formulas. To check the efficiency of our proposed method we chose Optimized Link State Routing Protocol (OLSR) as MANET routing protocol and the effect of four factors which are: The Black Hole attack, Worm Hole attack, Node Speed and the Pause Time.

1. Introduction

Mobile Ad hoc Network (MANET) can be defined as a network that connects differ-ent wireless devices between them without any central equipment like access points or router, without any admin intervention. In MANET, each wireless device named as a node can play two roles at the same time: host and router. In literature, there are various MANET routing protocols that take some constraints to ensure the connectivity of nodes like the mobility, consumption of energy and the threat of security, both the researchers and the company that works in MANET subject use different simulators to analyze the performance of each protocol under different factors and parameters. For that reason, the evaluation can take many days to test the effect of one factor. Moreover, this delay of simulations can increase in large density of the network or in big areas of simulation. In this paper, we propose a new method to test to effeteness of any MANET protocol under different factors in a simultaneous manner based on the concept of experimental plan, which used in some other industry subjects like chemical or mechanical research. The main idea of our proposition is building a model that presented as a mathematical formula and can be used to analyze the performance of any parameters like throughput, end-to-end delay, and so on, without any additional simulations. To calculate the model of each parameter by Yates algorithm [1] we are obliged to realize real simulations for the two levels Min (-1) and Max (+1) of each factor we want to study its effects. The outcome we create the formula
that gathers the relations between the result of the performance parameter and the effect of its factors. By the end, we find the result of parameter Y in the form of an equation that contains the coefficients of all factors. To test the effeteness of the Yates method in MANET, we chose OLSR [2] as the routing protocol and we test its performance under four different factors, in principle we select two factors in security (the Blackhole attack and Wormhole attack), and two other factors in Random Waypoint Mobility [3] (The Node Speed and Pause Time). The rest of this paper is organized as follows: in section II, we discuss to OLSR routing protocols in detail. Section III discuss some related work followed by the section IV that presents the concept of the experimental plan with the Yates algorithm. Section V defines the factors used in our model, then we propose our work in section VI following by the experimental results in section VII. Finally, we conclude our work.

2. Description of OLSR Routing Protocol
Optimized Link State Routing Protocol (OLSR) classified into proactive MANET protocols, they kept the routing paths for all destination nodes in the network, and generally, they use the same principle of function in classical wired routing protocols. However OLSR uses a new technic called by ”MultiPoint Relays” (MPR), MPRs are selective neighbors that allow for each node in the network to reach all its 2-hop neighbors, this new method of routing allows to avoid the overhead of the control routing messages, and to form a route from the source node to any destination in the network [2]. In addition, only MPRs nodes are responsible for forwarding broadcast messages during the flooding process. MPRs enable a better scalability in the distribution of topology information [4].

HELLO message and Topology Control (TC) message are two principal control messages used by OLSR for calculating the routing table. HELLO message is used to detect neighbors’ nodes, which it is have direct symmetric links, defines a list of 1-hop neighbors address, and list of MPR nodes [2]. However, HELLO messages are forwarded only between the 1-hop neighbors due to Time-to-Life (TTL) of the message that fixed at one. For TC messages they are generating and forwarding only by the MPR nodes and they are flooded to all nodes in the network. The information diffused in the network by HELLO and TC messages will help each node in the network to calculate its routing table. The standard version of OLSR uses the number of hops as a metric for selecting the route of destination. There are also two other control messages that can be generated in OLSR protocol: MID messages are sent by a node in the network to declare its multiple interfaces. The information broadcast in the network by these MID messages will help to build the routing table; generally, a node that has only a single interface address participating in the MANET must not generate any MID message [2].

The last control message that can be used in the OLSR protocol is HNA messages: It considered as a generalized version of the TC-message, the difference between TC and HNA messages is that a TC message may have a canceling effect on the previous information whereas information in HNA messages is removed only upon expiration [2].

The protocol is especially useful for large and dense networks, as optimization through MPR is working well in this situation. The larger and denser the network, the more optimizing can be done compared to the traditional link-state algorithm [5].

3. Related Work
In the literature the researches analyze the performance of any MANET routing protocol by using different simulators in the following we present some works that evaluate OLSR routing protocol in mobility and security effects:

the authors [6] evaluate three MANET routing protocols under two factors the first scenario analyzes their performance depends on the number of nodes and the second scenario under the pause time, the comparison is made according to five metrics of performance. The results of all
Simulations show the superiority of OLSR compared to other protocols. The paper [7] compares the performance of two proactive routing protocols according to different performance matrices, i.e., throughput, average jitter, average end-to-end delay, first packet reception (FPR), last packet reception (LPR), total byte reception (TBR), and total packet reception (TPR), varying the number of nodes; finally, all the simulations in a mobile environment show that the performance of the OLSR routing protocol is better than that of the STAR routing protocol.

The authors [8] compare two MANET routing protocols, AODV and OLSR, taking into account two factors: pause time and network density. The simulation results show that the OLSR protocol is more efficient in networks with high density and very sporadic traffic.

The work [9] the authors evaluated the four performance measures control overhead, PDR, end-to-end delay, and throughput for four MANET routing protocols as follows: DSDV, AODV, OLSR, and DSR in three scenarios of simulation: number of nodes as the first parameter, pause time as second and finally the size of network the conclusion of work confirms that OLSR protocol is the better solution for high mobility condition. [10] Study the effects of Black Hole Attack in MANET by using both proactive and reactive routing protocol, they choose OLSR protocol as a proactive routing protocol and AODV is a reactive routing protocol for simulation. They conclude that the AODV protocol is more vulnerable to a black hole attack than OLSR protocol by analyzing the performance parameters of end-to-end delay, throughput, and network load. [11] Present comparative analysis of performance parameters of Packet Delivery Ratio and average Throughput by using AODV protocol and OLSR protocol. As a result of the simulation, they observe important decreasing of values in PDR and decreasing also of average Throughput for both routing protocol OLSR protocol and AODV protocol. [12] Present an analytical approach to analysis AODV and OLSR routing protocols under the Black Hole attack, they proposed the packet end-to-end delay, network load, and throughput as performance metrics, in a result, there is a higher number of nodes and more route requests, the Blackhole attack affects the network performance more. In addition, they conclude that the AODV protocol is more vulnerable more than OLSR protocol under the Blackhole attack.

In [13] the authors present an analysis of the effect of the Wormhole attack on AODV and OLSR routing protocols in four scenarios and they used traffic simulation results and mathematical formula to show that AODV protocol is more vulnerable to wormhole attack compared to OLSR, the authors utilize OPNET for simulation.

The researchers [14] test the performance of three MANET routing protocols under the effect of node speed, all simulations were done in the NS3 simulator, for the experimental results, OLSR is more performance compared to AODV and DSDV for all metrics of analysis, however, when node speed increases the performance of OLSR become decreased.

4. The Experimental Plans and Yates method.

The experimental plan makes it possible to organize better the tests to accompany scientific research or industrial studies, to get the most information with the minimum of experiences. This methodology can be used in industries like chemical, petrochemicals, and pharmaceuticals or in the mechanical, automotive, and metallurgical industries [7]. One of the methods used in the experimental plan is the Yates method [1]. The Yates algorithm is a process used to calculate the main effects and interaction estimators in a factorial experiment. This method is used mainly in the statistic domain and in the chemical industry for the design and analysis of industrial experiments. This method gives a quantitative estimate of the effect of changing levels of a dependent variable [1]. It can be applied to experiments with factors having more than two levels.

We consider a factorial experiment with n factors each having two levels. We note this experience as 2n, by using Yates algorithms we can find the sums of squares corresponding to the main
effects and interactions of the factorial experiment 2n. The algorithm is present as a matrix of experiments that is the table which indicates the number of experiments to be carried out with the way to vary the factors and the order in which the experiments must be carried out. This table is composed of a +1 and -1 level. Two essential concepts must define before starting the calculating of each model: the overall effect and average effect of a factor:

The overall effect of a factor is the variation of the response when the factor goes from level -1 to level +1. This parameter can help us in the representation graphic of the factors to know their effects. The average effect of a factor is the half-variation of the response when the factor goes from level -1 to level +1. Thus, the average effect is defined as half of the overall effect.

The building of the experimental model in Yates’s algorithm is done by the matrix of the effect, in follow we present its goals:

The matrix of the effects used to calculate the coefficients of the model is obtained by adding to the left of the experiment matrix a column containing only +1 and the combination between the level of all factors. For calculating the coefficients of the experimental model, we use the matrix of Hadamard [15], it demonstrated that to obtain in n experiments a minimum variance, the matrix of effects X must verify the relation:

$$tXX = nI_n$$

Where In is the identity matrix of order n, and tX is the transposed matrix of X.

The matrix of the effects presents all the combinations possible between the level Min and Max of the factors and, we put the results of any performance parameter depending on the level of each factor in the matrix.

To calculate the experimental model in Yates’s method we use equation 2 that links the response to the factors we explain it as: for k factors, taking two levels the complete plan is noted as 2k:

$$Y = \alpha_0 + \alpha_1X1 + \alpha_2X2 + \ldots + \alpha_kXk$$ (2)

Where Y is the response of the experiment and $\alpha_0 , \alpha_1 , \alpha_2 \ldots \alpha_k$ are reals called coefficients of the model in the experiments section we explain the method used to calculate them.

Yates’ algorithm can be used to calculate the effects in a simple and systematic way and can be executed on an electronic spreadsheet [16]. The next section we define the factors used in our analysis.

The next section we define the factors used in our analysis.

5. The Factors of analysis

There are several constraints to ensure good communication in MANET; we can cite for example two essential constraints, which are the security of the routing protocols and the mobility of the nodes, these factors are taken into consideration in our proposed method to test the performance of OLSR protocol. We start by mobility factors (pause time and node speed), usually, each simulator has several mobility models that define how the nodes move in simulation, for example, speed, direction, destination, etc... In our study we use the Random Waypoint Mobility Model (RWM), it considers as one of the most popular mobility models [17], thanks to its simplicity and wide availability. In RWM the nodes of the network mobile randomly and freely without restrictions, we can say in a simple manner that the parameters of destination, speed, and direction are chosen in a random way and independently of other nodes. The mobility of nodes
in the RWM model is governed as follow: In the beginner each node waits for a fixed second called by the Pause Time (PT), then it selects a random destination in the network by also a random speed varies from 0 that generally excluded and some maximum speed [18] named by Node Speed (NS).

In the random waypoint model, speed and pause time are the two key parameters that define the mobility behavior of the nodes [19].

The second factor used in our analysis is the security, for that we will launch two routing attacks that affect the Ad hoc routing protocols, the first one is the Blackhole attack (BH) that promotes itself as a best and fresh node path to reach the destination, unfortunately, the attacker drops all routing packets received from its neighbors and stop forwarding them to the next router node, in the other meaning of black hole attack, the attacker will drop routing messages instead of relaying them to the corresponding nodes, which contrasts with the normal feature of the routing protocol [5]. The second one is the Wormhole attack (WH) that requires at least two attackers called by colluding nodes and they create a virtual link and tunnel the data between them in order the reduce the performance of routing protocol.

A wormhole attack is organized by two (distant) attackers in collusion who have an out-of-band connection between them. By transmitting data coming from one side of the wormhole to the other and vice versa, the neighboring nodes come to the false conclusion that such a link exists and is more efficient than other options. Manet traffic is then routed through the malicious nodes, creating virtual traffic in the network [20].

6. Proposed Work

In our work, we propose a new method for analyzing the effect of four factors on OLSR routing protocols is performance by using Yates’s method. After a modest reading of literature, we can say that our method was the first to evaluate any MANET protocol with any number of factors. In our case we use four factors (k = 4) that mean plan of $2^4 = 16$ experiments. In the other hand, we determine the response Y (parameters of performance); four responses of performance are cited in our method, which are:

(i) Throughput (TH): Define as the total of bites that received successfully by the destination node in a specified time is expressed in kilobits per second (Kbps). For best performance, the throughput should be higher.

(ii) Packet delivery ratio (PDR): is the ratio of total packets received to total packets dispatched, expressed as a percentage. The higher output of PDR means a better performance of the network.

(iii) End to End Delay (EED): is the average time it takes for the data to reach the nation. It also comprises the delay caused by the process of route discovery and queuing in the transfer of data packets. Only data packets that have been successfully delivered to the destinations that have counted. It is expressed in milliseconds (ms). The lower value of the end-to-end delay indicates that the protocol performs better.

(iv) Jitter Delay: is the variation in delay between each data packet received. The variation in the arrival time of packets must be minimal to achieve the best performance in mobile ad-hoc networks [21].

Before starting the experiment, we describe the levels Min (-1) and Max (+1) for each factor (Table 1).

For the Black hole and Worm hole attacks, we propose to use logical values (0 or 1), in +1 level the value of both factors becomes 1 and considers them are launching in the network. On the contrary, -1 levels set 0 value of their factor when they are not present in the network.
Table 1. The values of +1 and -1 levels of each factor.

| N | Factor          | +1 level | -1 level         |
|---|----------------|----------|------------------|
| 1 | Node speed     | 20       | 5                |
| 2 | Pause time     | 20       | 0                |
| 3 | Black Hole attack | With attack | Without attack |
| 4 | Worm Hole attack | With attack | Without attack |

In the section of experimental results, we explain in detail how to calculate the coefficients of all models either with or without interaction.

7. Experimental Results

To apply the experimental plan in MANET by the Yates method, we simulate 50 nodes under the effect of four factors of analysis. The first step starts by determining the value of k (number of factors), the second part begins with the realization of the real experiments. In our case, we simulate 24 =16 experiments in order to calculate the coefficient of the Yates model. Table 2 describes all the other parameters of the simulation:

Table 2. Parameters of Simulation in NS3.

| No | Parameter          | Value                                |
|----|--------------------|--------------------------------------|
| 1  | PC Simulator       | Dell Intel Xeon CPU ES-2407          |
| 2  | Simulator          | NS3 (V3.25)                          |
| 3  | Number of Nodes    | 50                                   |
| 4  | Simulation Time    | 200                                  |
| 5  | Pause Time         | 0 -20                                |
| 6  | Wi-Fi mode         | Ad-hoc                               |
| 7  | Transmit Power     | 7.5 dBm                              |
| 8  | Mobility model     | Random Waypoint mobility model       |
| 9  | Wifi rate          | 2Mbps                                |
| 10 | N. of Source/Sink  | 10                                   |
| 11 | Packet Size        | 64 Bytes                             |
| 12 | Node Speed         | 5-20 m/s                             |
| 13 | Protocol           | OLSR                                 |
| 14 | Network size       | 1000x1000 m                          |
| 15 | Network Attacks    | Black Hole AttackWorm Hole Attack     |

7.1. The matrix of the effects:

To calculate the coefficient of each factor by applying the Yates method, we utilize the matrix of Hadamard, this matrix contains all possible combinations of low/high levels for all the factors, and we add four other columns to mention the results of responses Y of all metrics. Table 3 describes the Matrix of effects with the results of experiments.
### Table 3. The matrix of the effects with experiments results.

| Nº  | Av. | BH   | WH   | NS   | PTc  | Y(TH) | Y(PDR) | Y(EED) | Y(Jitter) |
|-----|-----|------|------|------|------|-------|--------|--------|-----------|
| 1   | +1  | -1   | -1   | -1   | -1   | 15.23 | 76.65  | 18.80  | 17.19     |
| 2   | +1  | -1   | -1   | -1   | -1   | 10.42 | 52.45  | 32.74  | 27.47     |
| 3   | +1  | -1   | +1   | -1   | -1   | 13.61 | 68.49  | 22.04  | 24.10     |
| 4   | +1  | +1   | -1   | -1   | -1   | 8.80  | 44.28  | 19.01  | 16.15     |
| 5   | +1  | -1   | -1   | +1   | -1   | 16.31 | 78.26  | 15.69  | 13.82     |
| 6   | +1  | +1   | -1   | +1   | -1   | 14.72 | 74.06  | 18.69  | 15.79     |
| 7   | +1  | -1   | +1   | +1   | -1   | 11.06 | 55.67  | 34.53  | 31.23     |
| 8   | +1  | +1   | -1   | +1   | -1   | 13.52 | 68.64  | 22.85  | 21.82     |
| 9   | +1  | -1   | -1   | -1   | +1   | 15.23 | 76.65  | 18.80  | 17.19     |
| 10  | +1  | +1   | -1   | -1   | +1   | 13.52 | 68.64  | 22.85  | 21.82     |
| 11  | +1  | -1   | +1   | -1   | +1   | 11.06 | 55.67  | 34.53  | 31.23     |
| 12  | +1  | +1   | -1   | -1   | +1   | 9.35  | 47.66  | 38.58  | 35.86     |
| 13  | +1  | -1   | +1   | +1   | +1   | 13.80 | 69.47  | 21.64  | 18.64     |
| 14  | +1  | +1   | -1   | +1   | +1   | 15.39 | 77.45  | 25.02  | 21.09     |
| 15  | +1  | -1   | +1   | +1   | +1   | 11.03 | 55.52  | 27.17  | 26.61     |
| 16  | +1  | +1   | +1   | +1   | +1   | 12.62 | 63.50  | 30.56  | 29.01     |
| SUM |     |      |      |      |      | 210.66 | 1061.13 | 397.54 | 363.92   |

#### 7.2. Coefficients of the model:

Each estimate of a coefficient of the model is equal to the algebraic sum of the experimental responses $Y_i$ affected by the signs of the column of the matrix $X$ corresponding to the factor $X_i$ divided by the number of experiments. The estimation of the coefficients of the model is given by [22]:

$$A=\sum_{1}^{n}\frac{XY_{rep}}{n}$$

This result makes it possible to dispense with any matrix calculation and makes it possible to obtain the coefficients of the model with a simple calculator or better with a spreadsheet.

We explain the method to calculate the coefficient for one respond $Y$ (Throughput) and it is the same way to calculate all coefficients for other responds (PDR, EED and Jitter). For a plan of $2^4$ experiments built with Yates algorithm, the coefficients of the model are $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ and $\alpha_4$.

(i) For $\alpha_0$ is the average of Throughput from the table 3 it is equal as :

$$\frac{210.66}{16} = 13.166$$

(ii) $\alpha_1$ is the average of Throughput for all levels for the factor Black Hole from the matrix it equal :

$$\frac{-11.395}{16} = -0.71$$

(iii) $\alpha_2$ is the average of Throughput for all levels for the factor Worm Hole:

$$\frac{-20.295}{16} = -1.26$$
(iv) $\alpha_3$ is the average of Throughput for all levels for the factor Node Speed:

$$\frac{16.165}{16} = 1.01$$  \hspace{2cm} (7)

(v) $\alpha_4$ is the average of Throughput for all levels for the factor Pause Time:

$$\frac{-6.585}{16} = -0.41$$  \hspace{2cm} (8)

At the end, we create the model of Throughput parameter as follow:

$$Y(Throughput) = 13.166 - 0.71X_1 - 1.26X_2 + 1.01X_3 - 0.41X_4$$  \hspace{2cm} (9)

Where:
- $X_1$ is the factor of Black hole attack, in our model it takes two logical values (1 with attack and 0 without attack)
- $X_2$ is the factor of Worm hole attack, in our model it also takes two logical values (1 with attack and 0 without attack)
- $X_3$ is the factor of Node Speed
- $X_4$ is the factor of Pause Time

We apply the same procedure for the other parameters to find these results:

$$Y(PDR) = 66.32 - 3.5X_1 - 1.48X_2 + 5X_3 + 1.99X_4$$  \hspace{2cm} (10)

$$Y(EED) = 24.84 + 2.25X_1 + 0.23X_2 - 3.19X_3 + 2.55X_4$$  \hspace{2cm} (11)

$$Y(Jitter) = 22.74 + 1.87X_1 + 0.33X_2 - 3.41X_3 + 2.44X_4$$  \hspace{2cm} (12)

7.3. The representation of the effects:

The graphical presentation of the effect of factors is made from the average of each level i.e. -1 and +1. From the results of table 3, we calculate the average of each level with respect to each factor and it represents as follow:

Figure 1. Throughput of OLSR protocol depend to level of the factor.
From figure 1, we note that the performance of OLSR protocol decreases in +1 level for Black hole attack, Worm hole attack, and Pause Time. The explanation of these results is that the presence of Black Hole and Worm hole attacks with a high pause time can degrade the OLSR protocol performance. We can also classify the effect of each factor according to the difference between the low and high levels. We start the ranking of effects on the OLSR throughput either positively or negatively: the effect of Worm hole comes first, followed by the effect of node speed, the effect of Black hole comes in 3rd position, and finally the effect of pause time. The results of the Throughput metric by yates method are similar to other previous works in literature, for example, the throughput in work [5] under the effect of pause time shows that the level +1 when pause time is value equal 20 was more performance than the level -1 when it values fixed at 5 seconds. The effect of node speed that has already been analyzed at work [13] gives the same result compared to our method of analysis: the effect of -1 level is more than the level, Max. Now the result found in the work [9] to analyze the effect of the black hole gives the same logical conclusion compared to analyze by Yates algorithm; the performance of throughput goes degraded when the attack Black hole is present in the network. In other meaning, the level +1 in our case. The study to analyze the effect of worm hole in the paper [12] confirm the results of our method of analysis, the throughput of OLSR is more performance in low level than the high level when the attack was launched in the network.

![Figure 2. PDR of OLSR protocol depend to level of the factor.](image)

The results obtained for the Packet Delivery Ratio are similar to the Throughput metric. The node speed factor has a positive effect on its +1 level, unlike the three other factors, which decrease the percentage of the PDR metric at their higher level. The classification in the effect between all the factors can be mentioned as firstly, the Worm Hole attack with negativity effect, followed by node speed factor in positivity outcome, then the Black hole attack decreases the performance in PDR in a third case, the last negative factor noted is the pause time.

When we compare the result of PDR realized by the Yates method with other studies that use different simulators, the conclusion is the same, for example, the works [5] and [8] show that the PDR in it -1 level is more performance than +1 level under pause time factor. The same remark when we analyze the effect of speed node in paper [13] the performance of OLSR protocol decreases in Max level compared to Min level of node speed. The average of End-to-End (figure3 ) takes more delays in the +1 level for the three factors Black hole attack, Worm Hole attack, and pause time, these results can be considerate as legitimate due to the effect of Black hole and
Wormhole attacks, which work as DOS attacks, modify the routing protocols by dropping packets or selecting a longer path to reach the destination. For higher pause time values, we show that the EED of the OLSR protocol was increased. The exception here is the factor of node speed; it takes less delay when the speed of nodes was close to the Max level (20 m/s) in our case.

The average EED in work [12], [5], and [9] under respectively the effect of Wormhole, pause time, and black hole, all results are closing to the results of our method. The metric of EED of all these three factors is more performance in their -1 level compared to Max’s level. The exception found by Yates method in the effect of node speed in its -1 level is like the work [13]. Figure 4 shows that the Jitter metric has a bigger delay when the Black hole and Wormhole

Figure 3. EED of OLSR protocol depend to level of the factor.

Figure 4. Jitter delay of OLSR protocol depends to level of the factor.
attacks are launching in the network, the same observation for the pause time when it fixed at Max level. All these factors decrease the performance of OLSR protocol in their higher level; on the other hand, we find that the high level of speed node factor gives a good result in this metric compared to its low level.

These results found by Yates algorithm for the effect of pause time are similar to other performance analysis, for example [23] and [8] confirm that Jitter delay is more performance in less value of the pause time, for the effect of routing attacks it very logical that jitter delay becomes increasing in it value when these attacks are launching in the network, in other meaning when they were in +1 level for our method of analyzing.

8. Conclusion
In our work, we propose the use of the experiment plan in MANET by using the Yates method that applying in industrial studies. This method can help the researchers to build a model that relates the respond Y and the effect of factors. In our case, we chose OLSR protocol as MANET routing protocols to test its performance under four factors: The Black hole and Worm hole attacks as security factors, and node speed, pause time as mobility factors. By using just 16 real experiments that present the total combination of +1 and -1 levels for all factors, we can construct the Yates model by calculating the coefficient of factors. The results obtained from our method of the analysis show that the performance of OLSR protocol is decreasing when Black hole and Worm hole attacks are present in the network, with higher pause time. On contrary OLSR is more performance when the speed of nodes moves with a higher value. Finally, the experiment plan gives estimated results of each respond Y under the effect of many factors without any additional simulations.

References
[1] YADOLAH DODGE, Yates’ Algorithm, The Concise Encyclopedia of Statistics, Springer, (2008).
[2] P. JACQUET, P. MULETHALER, T. CLAUSEN, A. LAOUTI, A. QAYYUM, L. VIENNOT, Optimized Link State Routing Protocol for AdHoc Networks, 0-7803-7406-1/01/ 17.00 IEEE, (2001).
[3] ESA HYYTIÄ, JORMA VIRTAMO, Random waypoint mobility model in cellular networks, Pringer Sci. Bus. Media LLC 2007, (2007).
[4] P. JACQUET, P. MINET, P. MULETHALER, ET N. RIVIERRE, Increasing reliability in cable free radio LANs: Low level forwarding in HIPERLAN, Wirel. Pers. Commun, (1996).
[5] R. BHUVANESWARI ET R. RAMACHANDRAN, Denial of service attack solution in OLSR based manet by varying number of fictitious nodes, Clust. Comput., vol. 22, no 5, p. 12689-12699, (2019), doi: 10.1007/s10586-018-1723-0.
[6] LAKSHMAN NAIK, L. R.U.KHAN, ET R.B.MISHRA, Analysis of Node Density andPause Time Effects in MANET Routing Protocols using NS-3, J Comput. Netw. Inf. Secur., (2016).
[7] PANKAJ KUMAR VARSHNEY, G.S. AGRAWAL, ET SUDHIR KUMAR SHARMA, Relative Performance Analysis of Proactive Routing Protocols in Wireless Ad hoc Networks using Varying Node Density, Invertis J. Sci. Technol., vol. 9, no 3, p. 1-9, (2016).
[8] DILPREET KAUR ET NAESH KUMAR, Comparative Analysis of AODV, OLSR, TORA, DSR and DSDV Routing Protocols in Mobile Ad-Hoc Networks, J Comput. Netw. Inf. Secur., no 3, p. 39-46, (2013), doi: 10.5815/iijnis.2013.03.05.
[9] S. MOHAPATRA ET P. KANUNGO, Performance analysis of AODV, DSR, OLSR and DSDV Routing Protocols using NS2 Simulator, Int. Conf. Commun. Technol. Syst. Des., (2011).
[10] IRSHAD ULLAH ET SHAHZAD ANWAR, Effects of Black Hole Attack on MANET Using Reactive and Proactive Protocols, IJCSI Int. J. Comput. Sci. Issues, vol. 10, no 1, mai (2013).
[11] PRAVEEN K S, GURURAJ H L, ET RAMESH B, Comparative Analysis of Black Hole Attack in Ad Hoc Network Using AODV and OLSR Protocols, International Conference on Computational Modeling and Security (CMS 2016), (2016).
[12] D. C. SANJAY SINGH, AODV vs. OLSR: An Analytical Approach to Study Black Hole Attack, Int. J. Comput. Appl. 0975 – 8887, vol. 172, no 9, août (2017).
[13] Mohammad Sadeghi et Prof. Dr Saadiah Yahya, *Analysis of Wormhole Attack on MANETs Using Different MANET Routing Protocols*, the Fourth International Conference on Ubiquitous and Future Networks.

[14] Lakshman Naik L., R. U. Khan, et R. B. Mishra, *Analysis of Node Velocity Effects in MANET Routing Protocols using Network Simulator (NS3)*, Int. J. Comput. Appl., vol. 144, no 4, p. 0975 – 8887, juin (2016).

[15] H. Kharaghani, *A Hadamard matrix of order 428*, Journal of combinatorial Designs, p. 393–470, nov. 2005.

[16] A. Gonzalez-Pocino, F. Alvarez-Antolin, et J. Asensio-Lozano, *Improvement of Adhesive Wear Behavior by Variable Heat Treatment of a Tool Steel for Sheet Metal Forming*, Materials, vol. 12, no 17, Art. no 17, janv. (2019), doi: 10.3390/ma12172831.

[17] Tracy Camp, Jeff Boleng, et Vanessa Davies, *A survey of mobility models for ad hoc network research*, Wirel. Commun. Mob. Comput., p. 483–502, 2002, doi: 10.1002/wcm.72.

[18] Josh Broch, David A. Maltz, David B. Johnson, Yih-Chun Hu, et Jorjeta Jetcheva, *A performance comparison of multi-hop wire-less ad hoc network routing protocols*, 4th Annu. ACMIEEE Int. Conf. Mob. Comput. Netw., p. 85-97, oct. (1998), doi: 10.1145/288235.288256.

[19] Devarajan Krishnamoorthy et Vaiyapuri Padmathilagam, *Performance Evaluation of MANET Routing Protocol Using Random Way Point and Manhattan Mobility Models*, Middle-East J. Sci. Res., vol. 24, no 8, p. 2523-2530, (2016), doi: 10.5829/idosi.mejr.2016.24.08.23810.

[20] N. Schweitzer, A. Stulman, T. Hirst, R. D. Margalit, et A. Shaftai, *Network bottlenecks in OLSR based ad-hoc networks*, Ad Hoc Netw., vol. 88, p. 36-54, mai 2019, doi: 10.1016/j.adhoc.(2018).12.002.

[21] Abdellah Nabou, My Driss Laanaoui, et Mohammed Ouzzif, *The effect of Transmit Power on MANET routing protocols using AODV, DSDV, DSR and OLSR in NS3*, Advances in Intel-ligent Systems and Computing, p. 274–286, (2018).

[22] Yadolah Dodge, *Statistique, Dictionnaire encyclopédique.*, (2007).

[23] Raaid Alubady, Mohammed Al-Samman, Adib Habbal, Suhaidi Hassan, et Suki Arif, *PERFORMANCE ANALYSIS OF REACTIVE AND PROACTIVE ROUTING PROTOCOLS IN MANET*, ARPN J. Eng. Appl. Sci., vol. 10, no 3, févr. (2015).